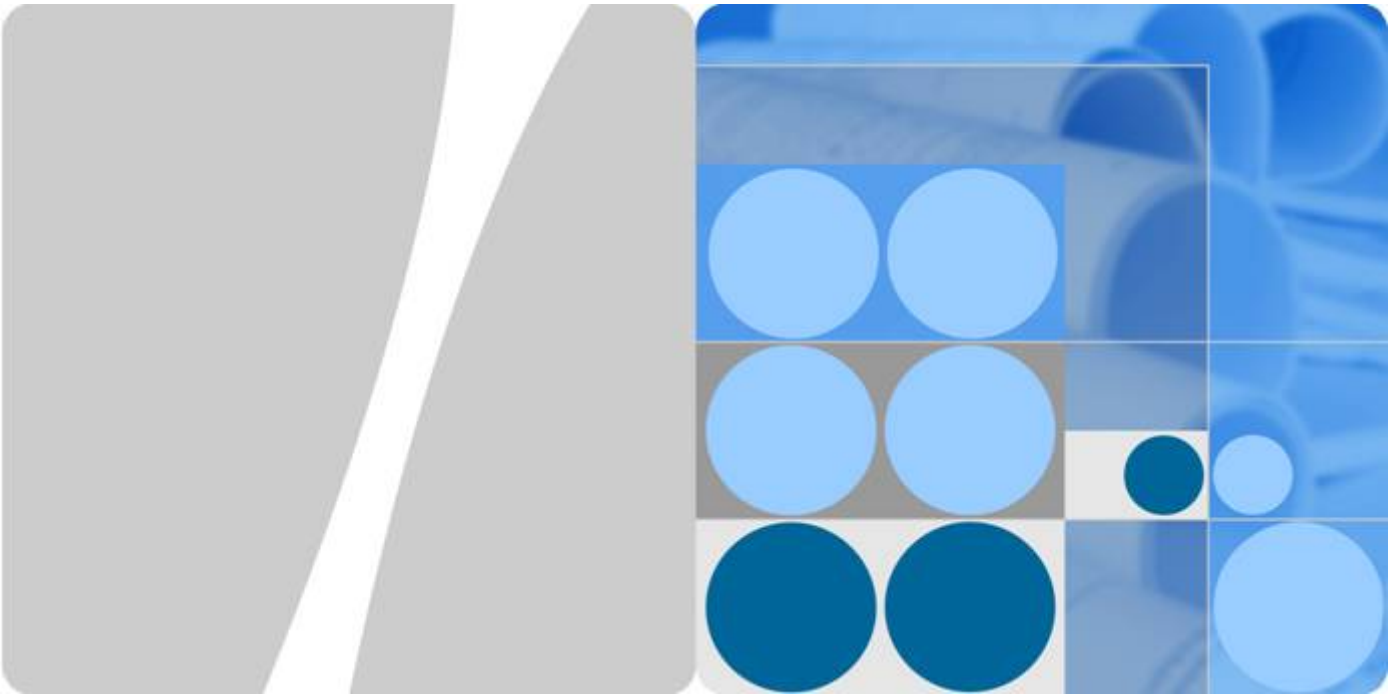


AC6605 无线接入控制器

V200R001C00

配置指南

文档版本　01

发布日期　2012-05-30

华为技术有限公司

HUAWEI

版权所有 © 华为技术有限公司 2012。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对 AC6605 设备，介绍了在不同应用场景中的配置过程和配置举例。

AC6605 设备分为有线侧和无线侧，有线侧特性与交换机相似。本文档中无线侧主要介绍了无线侧系统管理配置和 WLAN 配置，基础特性的配置与有线侧相似，文档中其它配置是有线侧的配置。

本文档主要适用于以下工程师：

- 网络规划工程师
- 硬件安装工程师
- 调测工程师
- 数据配置工程师
- 现场维护工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

版权所有 © 华为技术有限公司

符号	说明
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-05-30)

第一次正式发布。

版权所有 © 华为技术有限公司

目 录

前 言 ii
1 基础配置 1
1.1 登录交换机 2
1.1.1 简介 2
1.1.2 通过 Console 口登录交换机 2
1.1.3 通过 Telnet 登录交换机 4
1.1.4 配置举例 6
1.2 命令行介绍 10
1.2.1 命令行简介 10
1.2.2 在线帮助 13
1.2.3 命令行特性 15
1.2.4 快捷键 19
1.2.5 配置举例 20
1.3 如何使用接口 21
1.3.1 接口概述 21
1.3.2 配置接口基本参数 23
1.3.3 配置 Loopback 接口 26
1.3.4 维护接口 27
1.4 基本配置 27
1.4.1 基本配置简介 28
1.4.2 配置系统的基本环境 28
1.4.3 配置用户的基本环境 31
1.4.4 显示系统基本配置信息 33
1.5 用户管理 34
1.5.1 用户管理简介 34
1.5.2 通过 Console 口首次登录 AC6605 37
1.5.3 配置 Console 用户界面 41
1.5.4 配置 VTY 用户界面 44
1.5.5 管理用户界面 47
1.5.6 配置用户管理 49
1.5.7 配置举例 52
1.6 管理文件系统 54

版权所有 © 华为技术有限公司

1.6.1 文件系统简介.....54
1.6.2 管理存储设备.....55
1.6.3 管理目录.....56
1.6.4 管理文件.....58
1.7 管理配置文件.....62
1.7.1 管理配置文件简介.....62
1.7.2 管理配置文件.....63
1.8 FTP 和 TFTP.....66
1.8.1 FTP 和 TFTP 简介.....66
1.8.2 配置交换机作为 FTP 服务器.....67
1.8.3 配置 FTP 访问控制列表.....70
1.8.4 配置交换机作为 FTP 客户端.....72
1.8.5 配置交换机作为 TFTP 客户端.....77
1.8.6 限制对 TFTP 服务器的访问.....79
1.8.7 配置举例.....80
1.9 Telnet 及 SSH.....88
1.9.1 Telnet 及 SSH 简介.....88
1.9.2 配置 Telnet 终端服务.....90
1.9.3 配置 SSH 用户.....93
1.9.4 配置 SSH 服务器功能.....98
1.9.5 配置 STelnet 客户端功能.....102
1.9.6 配置 SFTP 客户端功能.....105
1.9.7 配置 SCP 客户端功能.....111
1.9.8 配置举例.....113
1.10 SSL 配置.....144
1.10.1 SSL 概述.....144
1.10.2 AC6605 支持的 SSL 特性.....146
1.10.3 通过用户终端登录 FTPS 服务器.....146
1.10.4 通过 FTPS 客户端登录 FTPS 服务器.....150
1.10.5 配置安全 Web 网管.....156
1.10.6 配置举例.....160
2 设备管理.....172
2.1 NAP 配置.....173
2.1.1 NAP 简介.....173
2.1.2 配置 NAP 远程开局.....173
2.1.3 配置举例.....177
2.2 使用 display 命令查看设备的状态.....180
2.2.1 简介.....180
2.2.2 查看 AC6605 设备的状态.....180
2.3 硬件管理.....184
2.3.1 简介.....184
2.3.2 AC6605 支持的硬件管理特性.....184

版权所有 © 华为技术有限公司

2.3.3 备份电子标签.....185
2.3.4 配置电口自动节能功能.....185
2.4 使用信息中心监控设备.....186
2.4.1 信息中心简介.....187
2.4.2 配置信息中心.....191
2.4.3 输出信息中心的信息.....193
2.4.4 维护.....196
2.4.5 配置举例.....196
2.5 监控口配置.....198
2.5.1 监控口概述.....198
2.5.2 配置监控口与网管的关联.....199
2.5.3 配置监控口与声光报警设备的关联.....200
2.5.4 配置举例.....202
2.6 使用镜像监控设备.....204
2.6.1 简介.....205
2.6.2 建立基于接口的本地镜像.....208
2.6.3 建立基于接口的远程镜像.....209
2.6.4 删除基于接口的镜像.....211
2.6.5 建立基于 VLAN 的本地镜像.....212
2.6.6 建立基于 VLAN 的远程镜像.....214
2.6.7 删除基于 VLAN 的镜像.....215
2.6.8 建立基于 MAC 地址的本地镜像.....216
2.6.9 建立基于 MAC 地址的远程镜像.....217
2.6.10 删除基于 MAC 地址的镜像.....219
2.6.11 建立基于流的本地流镜像.....220
2.6.12 建立基于流的远程流镜像.....222
2.6.13 删除基于流的镜像.....224
2.6.14 删除或变更观察接口.....225
2.6.15 配置 CPU 镜像.....227
2.6.16 删除 CPU 镜像.....228
2.6.17 配置举例.....229
2.7 PoE 配置.....241
2.7.1 PoE 供电简介.....241
2.7.2 AC6605 支持的 PoE 特性.....241
2.7.3 配置 PoE.....242
2.7.4 配置举例.....245
2.8 ALS 配置.....247
2.8.1 ALS 简介.....247
2.8.2 AC6605 支持的 ALS 特性.....247
2.8.3 配置 ALS.....249
2.8.4 配置举例.....252
2.9 重新启动和复位.....254

版权所有 © 华为技术有限公司

2.9.1 简介.....254
2.9.2 立即重新启动 AC6605 设备.....256
2.9.3 定时重新启动 AC6605 设备.....257
3 以太网配置.....258
3.1 以太网接口配置.....260
3.1.1 以太网接口概述.....260
3.1.2 AC6605 支持的以太网接口特性.....260
3.1.3 配置以太网接口的基本属性.....261
3.1.4 配置以太网接口的高级属性.....264
3.1.5 维护.....268
3.1.6 配置举例.....269
3.2 链路聚合配置.....270
3.2.1 链路聚合概述.....270
3.2.2 AC6605 支持的链路聚合特性.....270
3.2.3 配置手工负载分担模式链路聚合.....272
3.2.4 配置静态 LACP 模式链路聚合.....276
3.2.5 配置 E-Trunk.....282
3.2.6 维护.....288
3.2.7 配置举例.....289
3.3 VLAN 配置.....295
3.3.1 VLAN 概述.....295
3.3.2 AC6605 支持的 VLAN 特性.....301
3.3.3 划分 VLAN.....303
3.3.4 创建 VLANIF 接口.....312
3.3.5 配置 VLAN 间通信.....315
3.3.6 配置 VLAN 聚合节约 IP 地址.....318
3.3.7 配置 MUX VLAN 实现二层流量隔离.....322
3.3.8 配置 Voice VLAN 传输语音流量.....326
3.3.9 配置管理 VLAN 实现网管集中管理设备.....333
3.3.10 维护 VLAN.....334
3.3.11 配置举例.....335
3.4 VLAN Mapping 配置.....359
3.4.1 VLAN Mapping 概述.....359
3.4.2 AC6605 支持的 VLAN Mapping 特性.....359
3.4.3 配置单层 Tag 的 VLAN Mapping.....359
3.4.4 配置双层 Tag 的 VLAN Mapping.....361
3.4.5 配置举例.....362
3.5 QinQ 配置.....369
3.5.1 QinQ 概念.....369
3.5.2 AC6605 支持的 QinQ 特性.....369
3.5.3 配置基于接口的 QinQ.....370
3.5.4 配置灵活 QinQ.....371

版权所有 © 华为技术有限公司

3.5.5 配置 VLANIF 接口支持 QinQ Stacking 功能.....373
3.5.6 配置外层 VLAN Tag 的协议类型.....375
3.5.7 配置举例.....377
3.6 GVRP 配置.....389
3.6.1 GVRP 概述.....389
3.6.2 AC6605 支持的 GVRP 特性.....392
3.6.3 配置 GVRP 功能.....392
3.6.4 维护.....395
3.6.5 配置举例.....396
3.7 MAC 表配置.....399
3.7.1 MAC 表概述.....399
3.7.2 AC6605 支持的 MAC 表特性.....400
3.7.3 配置静态 MAC 表项.....402
3.7.4 配置黑洞 MAC 表项.....403
3.7.5 配置动态 MAC 表项的老化时间.....404
3.7.6 配置禁止 MAC 地址学习功能.....404
3.7.7 配置限制 MAC 地址学习数量.....407
3.7.8 配置接口安全.....409
3.7.9 配置 MAC 地址防漂移.....412
3.7.10 配置 MAC 地址漂移检测功能.....414
3.7.11 配置丢弃全零 MAC 地址报文功能.....416
3.7.12 配置 MAC 刷新 ARP 功能.....417
3.7.13 配置端口桥功能.....418
3.7.14 配置举例.....419
3.8 STP/RSTP 配置.....427
3.8.1 STP/RSTP 简介.....427
3.8.2 配置 STP/RSTP 基本功能.....433
3.8.3 配置 STP/RSTP 影响拓扑收敛的参数.....438
3.8.4 配置 RSTP 保护功能.....443
3.8.5 配置 STP/RSTP 支持和其他制造商设备互通的参数.....447
3.8.6 维护 STP/RSTP.....449
3.8.7 配置举例.....449
3.9 MSTP 配置.....458
3.9.1 MSTP 简介.....458
3.9.2 配置 MSTP 基本功能.....469
3.9.3 配置 MSTP 多进程.....476
3.9.4 配置 MSTP 影响拓扑收敛的参数.....480
3.9.5 配置 MSTP 保护功能.....484
3.9.6 配置 MSTP 支持和其他制造商设备互通的参数.....489
3.9.7 维护 MSTP.....492
3.9.8 配置举例.....492
3.10 SEP 配置.....506

版权所有 © 华为技术有限公司

3.10.1 SEP 简介.....506
3.10.2 配置 SEP 基本功能.....521
3.10.3 灵活指定阻塞端口.....526
3.10.4 配置 SEP 多实例.....529
3.10.5 配置网络拓扑变化通告.....532
3.10.6 维护 SEP.....535
3.10.7 配置举例.....536
3.11 二层协议透明传输配置.....581
3.11.1 二层协议透明传输概述.....581
3.11.2 AC6605 支持的二层协议透明传输特性.....582
3.11.3 配置基于接口的二层协议透明传输.....587
3.11.4 配置基于 VLAN 的二层协议透明传输.....590
3.11.5 配置基于 QinQ 的二层协议透明传输.....592
3.11.6 维护二层协议透明传输.....595
3.11.7 配置举例.....596
3.12 Loopback Detection 配置.....623
3.12.1 Loopback Detection 概述.....623
3.12.2 配置 Loopback Detection 功能.....623
3.12.3 配置举例.....628
4 IP 业务配置.....630
4.1 IP 地址配置.....631
4.1.1 IP 地址概述.....631
4.1.2 AC6605 支持的 IP 地址特性.....631
4.1.3 配置接口的 IP 地址.....631
4.1.4 配置举例.....633
4.2 ARP 配置.....635
4.2.1 ARP 概述.....635
4.2.2 AC6605 支持的 ARP 特性.....635
4.2.3 配置静态 ARP.....636
4.2.4 优化动态 ARP.....639
4.2.5 配置路由式 Proxy ARP.....640
4.2.6 配置 VLAN 内 Proxy ARP.....642
4.2.7 配置 VLAN 间 Proxy ARP.....644
4.2.8 维护 ARP.....645
4.2.9 配置举例.....647
4.3 DHCP 配置.....662
4.3.1 DHCP 概述.....662
4.3.2 AC6605 支持的 DHCP 特性.....663
4.3.3 配置基于全局地址池的 DHCP 服务器.....664
4.3.4 配置基于 VLANIF 接口地址池的 DHCP 服务器.....671
4.3.5 配置 DHCP 中继.....677
4.3.6 维护 DHCP.....682

版权所有 © 华为技术有限公司

4.3.7 配置举例.....682
4.4 DHCPv6 配置.....693
4.4.1 DHCPv6 概述.....693
4.4.2 AC6605 支持的 DHCPv6 特性.....694
4.4.3 配置 DHCPv6 中继.....695
4.4.4 维护 DHCPv6.....698
4.4.5 配置举例.....699
4.5 IP 性能配置.....702
4.5.1 IP 性能概述.....702
4.5.2 AC6605 支持的 IP 性能.....702
4.5.3 配置 IP 性能优化.....702
4.5.4 维护 IP 性能.....705
4.5.5 配置举例.....708
4.6 DHCP 策略 VLAN 配置.....711
4.6.1 DHCP 策略 VLAN 概述.....711
4.6.2 AC6605 支持的 DHCP 策略 VLAN 特性.....711
4.6.3 配置基于 MAC 地址的 DHCP 策略 VLAN.....711
4.6.4 配置基于接口的 DHCP 策略 VLAN.....712
4.6.5 配置普通 DHCP 策略 VLAN.....714
4.6.6 维护.....715
4.6.7 配置举例.....715
4.7 DNS 配置.....719
4.7.1 DNS 概述.....719
4.7.2 AC6605 支持的 DNS 特性.....719
4.7.3 配置 DNS.....719
4.7.4 维护 DNS.....722
4.7.5 配置举例.....723
4.8 IPv6 基础配置.....727
4.8.1 IPv6 概述.....727
4.8.2 AC6605 支持的 IPv6 特性.....727
4.8.3 配置接口的 IPv6 地址.....728
4.8.4 配置 IPv6 邻居发现.....731
4.8.5 维护 IPv6.....735
4.8.6 配置举例.....737
4.9 IPv6 DNS 配置.....740
4.9.1 IPv6 DNS 概述.....740
4.9.2 AC6605 支持的 IPv6 DNS 特性.....740
4.9.3 配置 IPv6 DNS.....740
4.9.4 维护 IPv6 DNS.....743
4.9.5 配置举例.....744
4.10 IPv6 over IPv4 隧道配置.....747
4.10.1 IPv6 over IPv4 概述.....747

版权所有 © 华为技术有限公司

4.10.2 AC6605 支持的 IPv6 over IPv4 特性.....747
4.10.3 配置 IPv4/IPv6 双协议栈.....751
4.10.4 配置 IPv6 over IPv4 隧道.....753
4.10.5 配置举例.....757
5 IP 路由配置.....771
5.1 静态路由配置.....772
5.1.1 静态路由概述.....772
5.1.2 AC6605 支持的静态路由特性.....772
5.1.3 配置 IPv4 静态路由.....773
5.1.4 配置 IPv6 静态路由.....775
5.1.5 配置 BFD for 公网 IPv4 静态路由.....777
5.1.6 配置静态路由举例.....778
5.2 RIP 配置.....787
5.2.1 RIP 概述.....787
5.2.2 AC6605 支持的 RIP 特性.....788
5.2.3 配置 RIP 的基本功能.....788
5.2.4 配置 RIP 的路由属性.....792
5.2.5 控制 RIP 路由信息的发布.....794
5.2.6 控制 RIP 路由信息的接收.....797
5.2.7 配置 RIP-2 特性.....800
5.2.8 调整和优化 RIP 网络.....803
5.2.9 配置 RIP 的网管功能.....807
5.2.10 配置 RIP 举例.....808
5.3 RIPng 配置.....816
5.3.1 RIPng 概述.....816
5.3.2 AC6605 支持的 RIPng 特性.....817
5.3.3 配置 RIPng 的基本功能.....817
5.3.4 配置 RIPng 的路由属性.....819
5.3.5 控制 RIPng 路由信息的发布.....822
5.3.6 控制 RIPng 路由信息的接收.....824
5.3.7 调整优化 RIPng 网络.....826
5.3.8 配置举例.....828
5.4 OSPF 配置.....832
5.4.1 OSPF 概述.....832
5.4.2 AC6605 中支持的 OSPF 特性.....834
5.4.3 配置 OSPF 的基本功能.....837
5.4.4 建立或维持 OSPF 邻居或邻接关系.....840
5.4.5 配置 OSPF 的 STUB 区域.....843
5.4.6 配置 OSPF 的 NSSA 区域.....845
5.4.7 配置 OSPF 在不同网络类型中的属性.....848
5.4.8 配置 OSPF 的路由属性.....851
5.4.9 控制 OSPF 的路由信息.....854

版权所有 © 华为技术有限公司

5.4.10 调整优化 OSPF 网络.....859
5.4.11 配置 OSPF 网管功能.....864
5.4.12 提高 OSPF 网络的安全性.....865
5.4.13 维护 OSPF.....867
5.4.14 配置 OSPF 举例.....869
5.5 OSPFv3 配置.....894
5.5.1 OSPFv3 概述.....894
5.5.2 AC6605 支持的 OSPFv3 特性.....895
5.5.3 配置 OSPFv3 基本功能.....895
5.5.4 建立或维持 OSPFv3 邻居或邻接关系.....898
5.5.5 配置 OSPFv3 的区域属性.....900
5.5.6 配置 OSPFv3 的路由属性.....901
5.5.7 控制 OSPFv3 的路由信息.....903
5.5.8 调整和优化 OSPFv3 网络.....906
5.5.9 配置举例.....908
5.6 IS-IS 配置.....912
5.6.1 IS-IS 基本概念.....912
5.6.2 AC6605 支持的 IS-IS 特性.....914
5.6.3 配置 IS-IS 的基本功能.....919
5.6.4 建立或维持 IS-IS 邻居或邻接关系.....922
5.6.5 配置 IS-IS 在不同网络类型中的属性.....927
5.6.6 配置 IS-IS 的路由属性.....929
5.6.7 控制 IS-IS 路由信息的发布.....933
5.6.8 控制 IS-IS 路由信息的接收.....935
5.6.9 调整和优化 IS-IS.....937
5.6.10 提高 IS-IS 网络的安全性.....943
5.6.11 维护 IS-IS 配置.....946
5.6.12 配置 IS-IS 举例.....949
5.7 BGP 配置.....969
5.7.1 BGP 概述.....969
5.7.2 AC6605 中支持的 BGP 特性.....970
5.7.3 配置 BGP 的基本功能.....974
5.7.4 配置 BGP 的路由属性.....977
5.7.5 配置 BGP 过滤器.....984
5.7.6 控制路由信息的发布.....989
5.7.7 控制路由信息的引入.....991
5.7.8 配置 BGP 对等体间连接参数.....993
5.7.9 配置 BFD for BGP.....997
5.7.10 配置 BGP 负载分担.....999
5.7.11 配置 BGP 安全性.....1001
5.7.12 BGP 维护.....1002
5.7.13 配置 BGP 举例.....1003

版权所有 © 华为技术有限公司

5.8 路由策略配置.....1017
5.8.1 路由策略概述.....1017
5.8.2 AC6605 支持的路由策略特性.....1018
5.8.3 配置地址前缀列表.....1019
5.8.4 配置 Route-Policy.....1021
5.8.5 对接收的路由应用路由过滤器.....1024
5.8.6 对发布的路由应用路由过滤器.....1027
5.8.7 对引入的路由应用路由过滤器.....1031
5.8.8 控制路由策略生效时间.....1033
5.8.9 路由策略维护.....1035
5.8.10 配置路由策略举例.....1036
5.9 MCE 配置.....1045
5.9.1 MCE 概述.....1045
5.9.2 AC6605 支持的 MCE 特性.....1047
5.9.3 配置 VPN 实例.....1047
5.9.4 在 MCE 与 Site 间配置路由多实例.....1049
5.9.5 在 MCE 与 PE 间配置路由多实例.....1053
5.9.6 MCE 配置举例.....1056
6 组播配置.....1063
6.1 IP 组播配置指导.....1065
6.1.1 IP 组播概述.....1065
6.1.2 AC6605 支持的 IP 组播特性.....1065
6.1.3 IPv4 组播配置指导.....1065
6.2 IGMP Snooping 配置.....1068
6.2.1 IGMP Snooping 概述.....1068
6.2.2 AC6605 支持的 IGMP Snooping 特性.....1069
6.2.3 配置基于 VLAN 的 IGMP Snooping.....1070
6.2.4 配置静态组播 MAC 地址.....1081
6.2.5 配置二层组播 SSM Mapping 功能.....1082
6.2.6 维护.....1084
6.2.7 配置举例.....1086
6.3 组播 VLAN 配置.....1092
6.3.1 组播 VLAN 概述.....1092
6.3.2 AC6605 支持的组播 VLAN 特性.....1092
6.3.3 配置基于用户 VLAN 的组播 VLAN 复制.....1094
6.3.4 配置基于接口的组播 VLAN 复制.....1096
6.3.5 配置组播 VLAN 多对多.....1098
6.3.6 配置举例.....1101
6.4 可控组播配置.....1110
6.4.1 概述.....1110
6.4.2 基本原理.....1110
6.4.3 配置可控组播功能.....1111

版权所有 © 华为技术有限公司

6.4.4 配置举例.....1114
6.5 IGMP 配置.....1117
6.5.1 IGMP 概述.....1117
6.5.2 AC6605 支持的 IGMP 特性.....1118
6.5.3 配置 IGMP 基本功能.....1119
6.5.4 配置 IGMP 性能参数.....1122
6.5.5 配置 SSM Mapping.....1128
6.5.6 维护 IGMP.....1130
6.5.7 配置举例.....1132
6.6 PIM-DM（IPv4）配置.....1142
6.6.1 PIM-DM 概述.....1142
6.6.2 AC6605 支持的 PIM-DM 特性.....1143
6.6.3 配置 PIM-DM 基本功能.....1144
6.6.4 调整组播源控制参数.....1146
6.6.5 调整邻居控制参数.....1148
6.6.6 调整剪枝控制参数.....1151
6.6.7 调整状态刷新控制参数.....1154
6.6.8 调整嫁接控制参数.....1158
6.6.9 调整 Assert 控制参数.....1159
6.6.10 配置防止主机恶意攻击功能（PIM Silent）.....1161
6.6.11 维护 PIM-DM（IPv4）.....1164
6.6.12 配置举例.....1165
6.7 PIM-SM（IPv4）配置.....1171
6.7.1 PIM-SM 概述.....1171
6.7.2 AC6605 支持的 PIM-SM 特性.....1172
6.7.3 配置 PIM-SM 基本功能.....1173
6.7.4 调整组播源控制参数.....1177
6.7.5 调整 C-RP 和 C-BSR 的控制参数.....1179
6.7.6 配置 BSR 管理域.....1183
6.7.7 调整邻居控制参数.....1186
6.7.8 调整源注册控制参数.....1190
6.7.9 调整转发控制参数.....1192
6.7.10 调整 Assert 控制参数.....1196
6.7.11 调整 SPT 切换控制参数.....1198
6.7.12 配置 PIM BFD.....1200
6.7.13 配置防止主机恶意攻击功能（PIM Silent）.....1202
6.7.14 维护 PIM-SM（IPv4）.....1204
6.7.15 配置举例.....1206
6.8 MSDP 配置.....1215
6.8.1 MSDP 概述.....1215
6.8.2 AC6605 支持的 MSDP 特性.....1216
6.8.3 配置 PIM-SM 域间组播.....1218

版权所有 © 华为技术有限公司

6.8.4 配置 PIM-SM 域内 Anycast RP....1221
6.8.5 管理 MSDP 对等体连接....1226
6.8.6 配置 SA 缓存....1228
6.8.7 配置 SA 请求....1230
6.8.8 配置过滤 SA 消息的规则....1233
6.8.9 配置 MSDP 认证....1236
6.8.10 维护 MSDP....1239
6.8.11 配置举例....1241
6.9 IPv4 组播路由管理....1250
6.9.1 IPv4 组播路由管理概述....1250
6.9.2 AC6605 支持的 IPv4 组播路由管理特性....1251
6.9.3 配置组播静态路由....1253
6.9.4 配置组播路由策略....1254
6.9.5 配置组播转发范围....1257
6.9.6 配置组播转发表限制参数....1258
6.9.7 维护 IPv4 组播路由管理....1260
6.9.8 配置举例....1263
6.10 MLD Snooping 配置....1267
6.10.1 MLD Snooping 概述....1267
6.10.2 AC6605 支持的 MLD Snooping 特性....1268
6.10.3 配置 MLD Snooping 基本功能....1268
6.10.4 配置 VLAN 的组播策略....1272
6.10.5 配置接口快速离开功能....1273
6.10.6 配置 MLD Snooping 查询器....1274
6.10.7 （可选）调整 MLD Snooping 的性能....1277
6.10.8 维护....1280
6.10.9 配置举例....1281
7 QoS 配置....1284
7.1 基于类的 QoS 配置....1285
7.1.1 基于类的 QoS 概述....1285
7.1.2 AC6605 支持的基于类的 QoS 特性....1285
7.1.3 配置基于简单流分类的优先级映射....1288
7.1.4 配置基于复杂流分类的流策略....1292
7.1.5 配置基于简化 QoS 命令的流策略....1303
7.1.6 维护基于类的 QoS....1310
7.1.7 配置举例....1311
7.2 流量监管和流量整形配置....1323
7.2.1 流量监管和流量整形概述....1323
7.2.2 配置基于接口的流量监管....1326
7.2.3 配置基于类的流量监管....1328
7.2.4 配置流量整形....1332
7.2.5 维护流量监管和流量整形....1334

版权所有 © 华为技术有限公司

7.2.6 配置举例.....1335
7.3 拥塞避免和拥塞管理配置.....1350
7.3.1 拥塞避免和拥塞管理概述.....1350
7.3.2 配置拥塞避免.....1353
7.3.3 配置拥塞管理.....1356
7.3.4 维护拥塞避免和拥塞管理.....1359
7.3.5 配置举例.....1359
8 安全配置.....1364
8.1 AAA 及用户管理配置.....1366
8.1.1 AAA 及用户管理概述.....1366
8.1.2 AC6605 支持的 AAA 及用户管理特性.....1366
8.1.3 配置 AAA 方案.....1368
8.1.4 配置 RADIUS 服务器模板.....1372
8.1.5 配置 HWTACACS 服务器模板.....1379
8.1.6 配置业务方案.....1384
8.1.7 配置域.....1386
8.1.8 配置本地用户管理.....1390
8.1.9 维护 AAA 及用户管理.....1394
8.1.10 配置举例.....1395
8.2 NAC 配置.....1402
8.2.1 NAC 概述.....1402
8.2.2 AC6605 支持的 NAC 特性.....1404
8.2.3 配置 Web 认证.....1404
8.2.4 配置 802.1x 认证.....1408
8.2.5 配置 MAC 认证.....1417
8.2.6 维护 NAC.....1422
8.2.7 配置举例.....1423
8.3 DHCP Snooping 配置.....1433
8.3.1 DHCP Snooping 概述.....1433
8.3.2 AC6605 支持的 DHCP Snooping 特性.....1433
8.3.3 配置防止 DHCP Server 仿冒者攻击.....1436
8.3.4 配置防止改变 CHADDR 值的 DoS 攻击.....1438
8.3.5 配置防止仿冒 DHCP 续租报文攻击.....1440
8.3.6 配置 DHCP Snooping 用户数限制.....1445
8.3.7 配置限制 DHCP 报文上送速率.....1448
8.3.8 配置丢弃报文告警功能.....1451
8.3.9 维护 DHCP Snooping.....1454
8.3.10 配置举例.....1455
8.4 ARP 安全配置.....1469
8.4.1 ARP 安全概述.....1469
8.4.2 AC6605 支持的 ARP 安全特性.....1471
8.4.3 配置 ARP 报文源 MAC 地址检查功能.....1472

版权所有 © 华为技术有限公司

8.4.4 配置防 ARP DOS 攻击.....1473
8.4.5 配置防 ARP 欺骗攻击.....1481
8.4.6 维护 ARP 安全.....1487
8.4.7 配置举例.....1489
8.5 IP 源防攻击配置.....1495
8.5.1 IP 源防攻击概述.....1495
8.5.2 AC6605 支持的 IP 源防攻击特性.....1496
8.5.3 配置 IP Source Guard.....1496
8.5.4 配置 URPF.....1499
8.5.5 配置举例.....1500
8.6 本机防攻击配置.....1502
8.6.1 本机防攻击概述.....1502
8.6.2 AC6605 支持的本机防攻击特性.....1503
8.6.3 配置防攻击策略.....1503
8.6.4 配置攻击溯源.....1508
8.6.5 维护防攻击策略.....1512
8.6.6 配置举例.....1513
8.7 MFF 配置.....1515
8.7.1 MFF 概述.....1515
8.7.2 AC6605 支持的 MFF 特性.....1516
8.7.3 配置 MFF.....1517
8.7.4 配置举例.....1521
8.8 流量抑制配置.....1525
8.8.1 流量抑制概述.....1525
8.8.2 AC6605 支持的流量抑制特性.....1525
8.8.3 配置流量抑制.....1525
8.8.4 配置风暴控制功能.....1528
8.8.5 配置举例.....1529
8.9 ACL 配置.....1532
8.9.1 ACL 概述.....1532
8.9.2 AC6605 支持的 ACL 分类.....1533
8.9.3 配置 ACL.....1534
8.9.4 配置 ACL6.....1539
8.9.5 配置举例.....1543
8.10 ND Snooping 配置.....1556
8.10.1 ND Snooping 概述.....1556
8.10.2 AC6605 支持的 ND Snooping 特性.....1556
8.10.3 配置 ND Snooping.....1557
8.10.4 维护 ND Snooping.....1560
8.10.5 配置举例.....1561
9 可靠性配置.....1565
9.1 DLDP 配置.....1566

版权所有 © 华为技术有限公司

9.1.1 DLDP 概述.....1566
9.1.2 配置 DLDP 功能.....1567
9.1.3 重置 DLDP 状态.....1572
9.1.4 维护.....1573
9.1.5 配置举例.....1574
9.2 Smart Link 和 Monitor Link 配置.....1577
9.2.1 Smart Link 和 Monitor Link 概述.....1577
9.2.2 配置 Smart Link 组基本功能.....1577
9.2.3 配置 Smart Link 组数据流策略.....1583
9.2.4 配置 Monitor Link 组功能.....1586
9.2.5 维护.....1590
9.2.6 配置举例.....1590
9.3 RRPP 配置.....1602
9.3.1 RRPP 概述.....1603
9.3.2 AC6605 支持的 RRPP 特性.....1603
9.3.3 配置 RRPP 基本功能.....1607
9.3.4 配置 RRPP 多实例.....1614
9.3.5 维护 RRPP.....1623
9.3.6 配置举例.....1624
9.4 以太网 OAM 配置.....1692
9.4.1 以太网 OAM 概述.....1692
9.4.2 AC6605 支持的以太网 OAM 特性.....1693
9.4.3 配置 EFM OAM 基本功能.....1697
9.4.4 配置 EFM OAM 链路监控.....1700
9.4.5 配置物理链路丢包率检测.....1704
9.4.6 配置 EFM OAM 和接口联动.....1708
9.4.7 配置 EFM OAM 与接口联动（触发与 EFM OAM 联动的接口物理状态变为 Down）.....1711
9.4.8 配置 EFM OAM 和 EFM OAM 联动.....1714
9.4.9 配置以太网 CFM 基本功能.....1716
9.4.10 配置以太网 CFM 的相关参数.....1725
9.4.11 配置以太网的故障确认.....1728
9.4.12 配置以太网的故障定位.....1730
9.4.13 配置以太网 CFM 和接口联动.....1733
9.4.14 配置以太网 CFM 与接口联动（触发与以太网 CFM 联动的接口物理状态变为 Down）.....1736
9.4.15 配置 EFM OAM 和以太网 CFM 之间的联动.....1739
9.4.16 配置以太网 CFM 和以太网 CFM 联动.....1741
9.4.17 配置以太网 CFM 和 SEP 联动.....1743
9.4.18 维护以太网 OAM.....1745
9.4.19 配置举例.....1745
9.5 Y.1731 配置.....1793
9.5.1 Y.1731 概述.....1793
9.5.2 AC6605 支持的 Y.1731 特性.....1794

版权所有 © 华为技术有限公司

9.5.3 配置 VLAN 的单向时延统计功能.....1795
9.5.4 配置 VLAN 的双向时延统计功能.....1799
9.5.5 配置举例.....1802
9.6 BFD 配置.....1811
9.6.1 BFD 概述.....1811
9.6.2 AC6605 支持的 BFD 特性.....1811
9.6.3 配置 BFD 单跳检测.....1813
9.6.4 配置 BFD 多跳检测.....1817
9.6.5 配置静态标识符自协商 BFD.....1820
9.6.6 调整 BFD 检测参数.....1822
9.6.7 配置 Trap 消息定时器的时间间隔.....1826
9.6.8 维护 BFD.....1827
9.6.9 配置举例.....1828
9.7 VRRP 和 VRRP6 配置.....1837
9.7.1 VRRP 概述.....1837
9.7.2 AC6605 支持的 VRRP 特性.....1838
9.7.3 配置 VRRP 备份组.....1839
9.7.4 配置 VRRP 监视接口状态.....1844
9.7.5 配置 VRRP 监视 BFD 会话状态.....1847
9.7.6 配置 VRRP 安全功能.....1850
9.7.7 调整优化 VRRP.....1852
9.7.8 配置管理 VRRP 备份组.....1858
9.7.9 配置 VRRP 协议版本升级.....1862
9.7.10 维护 VRRP.....1863
9.7.11 配置举例.....1864
9.8 联动配置举例集.....1886
9.9 MAC SWAP 环回测试配置.....1887
9.9.1 MAC SWAP 环回测试概述.....1887
9.9.2 AC6605 支持的 MAC SWAP 环回测试特性.....1887
9.9.3 本端 MAC SWAP 环回测试配置.....1888
9.9.4 远端 MAC SWAP 环回测试配置.....1891
9.9.5 配置举例.....1894
10 网络管理配置.....1898
10.1 SNMP 配置.....1899
10.1.1 SNMP 简介.....1899
10.1.2 配置设备使用 SNMPv1 与网管通信.....1903
10.1.3 配置设备使用 SNMPv2c 与网管通信.....1910
10.1.4 配置设备使用 SNMPv3 与网管通信.....1917
10.1.5 SNMP 配置举例.....1924
10.2 LLDP 配置.....1935
10.2.1 LLDP 概述.....1935
10.2.2 AC6605 支持的 LLDP 特性.....1938

版权所有 © 华为技术有限公司

10.2.3 配置 LLDP 功能.....1942
10.2.4 维护.....1949
10.2.5 配置举例.....1949
10.3 HGMP 配置.....1964
10.3.1 HGMP 概述.....1965
10.3.2 AC6605 支持的 HGMP 特性.....1966
10.3.3 配置 HGMP 的基本功能.....1969
10.3.4 配置 HGMP 的高级功能.....1977
10.3.5 维护 HGMP.....1985
10.3.6 配置举例.....1986
10.4 NTP 配置.....2082
10.4.1 NTP 概述.....2082
10.4.2 AC6605 支持的 NTP 特性.....2084
10.4.3 配置 NTP 基本功能.....2085
10.4.4 配置 NTP 安全机制.....2092
10.4.5 维护 NTP.....2097
10.4.6 配置举例.....2097
10.5 Ping 和 Tracert 配置.....2113
10.5.1 Ping.....2113
10.5.2 Tracert.....2114
10.5.3 配置 Ping 和 Tracert.....2115
10.5.4 调试.....2117
10.5.5 配置举例.....2117
10.6 NQA 配置.....2119
10.6.1 NQA 概述.....2119
10.6.2 NQA 与 Ping 的比较.....2119
10.6.3 NQA 客户端和服务器.....2119
10.6.4 AC6605 支持的 NQA 特性.....2120
10.6.5 配置 ICMP 测试.....2121
10.6.6 配置 FTP 下载测试.....2123
10.6.7 配置 FTP 上载测试.....2126
10.6.8 配置 HTTP 测试.....2129
10.6.9 配置 DNS 测试.....2131
10.6.10 配置 Traceroute 测试.....2133
10.6.11 配置 SNMP 查询测试.....2135
10.6.12 配置 TCP 测试.....2138
10.6.13 配置 UDP 测试.....2140
10.6.14 配置 Jitter 测试.....2143
10.6.15 配置 ICMP Jitter 测试.....2146
10.6.16 配置 NQA 测试例的通用参数.....2149
10.6.17 配置 NQA 双向传输延迟阈值.....2153
10.6.18 配置 NQA 测试的 Trap 开关.....2154

版权所有 © 华为技术有限公司

10.6.19 维护 NQA....2158
10.6.20 配置举例....2159
10.7 RMON 配置....2187
10.7.1 RMON 概述....2187
10.7.2 AC6605 支持的 RMON 特性....2187
10.7.3 配置 RMON....2189
10.7.4 维护 RMON....2194
10.7.5 配置举例....2194
11 无线侧系统管理配置....2199
11.1 配置用户登录....2200
11.1.1 用户通过 Console 口登录系统....2200
11.1.2 用户通过终端 Telnet 登录到系统....2202
11.1.3 检查配置结果....2203
11.2 配置用户界面....2204
11.2.1 配置 Console 用户界面....2204
11.2.2 配置 VTY 用户界面....2206
11.2.3 检查配置结果....2207
11.3 设置启动文件....2207
11.3.1 配置交换机下次启动时加载的系统软件....2207
11.3.2 配置交换机下次启动时加载的配置文件....2208
11.3.3 检查配置结果....2208
11.4 重新启动....2209
11.4.1 （可选）通过按键立即重新启动 AC6605....2209
11.4.2 （可选）通过命令行定时重新启动 AC6605....2210
11.4.3 检查配置结果....2210
11.5 设备升级....2211
11.5.1 AC 设备升级....2211
11.5.2 升级 AP 设备....2212
11.5.3 检查配置结果....2213
11.6 查看设备状态....2214
11.6.1 查看设备信息....2214
11.6.2 查看版本信息....2214
11.6.3 查看诊断信息....2215
11.6.4 显示系统配置信息....2215
11.6.5 显示系统运行状态....2215
11.7 （可选）激活 License....2215
12 WLAN 配置....2218
12.1 WLAN 基本业务配置....2219
12.1.1 WLAN 业务简介....2219
12.1.2 AC6605 支持的 WLAN 特性....2222
12.1.3 配置 AC 基本功能....2223

版权所有 © 华为技术有限公司

12.1.4 配置 AP 与 AC 互通.....2225
12.1.5 配置 WLAN 射频.....2229
12.1.6 配置无线用户接入.....2236
12.1.7 管理 AP.....2244
12.1.8 维护.....2247
12.1.9 配置举例.....2250
12.2 WLAN WDS 配置.....2272
12.2.1 WDS 简介.....2272
12.2.2 AC6605 支持的 WLAN WDS 特性.....2274
12.2.3 配置 WDS 业务.....2276
12.2.4 配置网桥白名单.....2278
12.2.5 配置 AP 有线口参数.....2279
12.2.6 配置 STP 功能.....2280
12.2.7 配置参数下发.....2281
12.2.8 配置举例.....2281
12.3 WLAN 安全配置.....2290
12.3.1 WLAN 安全简介.....2290
12.3.2 AC6605 支持的 WLAN 安全特性.....2292
12.3.3 配置用户接入安全策略.....2293
12.3.4 配置 STA 黑白名单.....2296
12.3.5 配置用户隔离.....2297
12.3.6 配置示例.....2299
12.4 WLAN QoS 配置.....2306
12.4.1 WLAN QoS 简介.....2306
12.4.2 AC6605 支持的 WLAN QoS 特性.....2307
12.4.3 配置射频的 QoS 策略.....2308
12.4.4 配置 VAP 的 QoS 策略.....2310
12.4.5 配置用户优先级和用户 CAR.....2312
12.4.6 通过 QoS 模板配置用户优先级和用户 CAR.....2314
12.4.7 配置示例.....2315

版权所有 © 华为技术有限公司

1 基础配置

关于本章

本文档针对 AC6605 基础特性，从配置过程和配置举例两方面对特性进行介绍。

1.1 登录交换机
配置交换机之前需要首先登录交换机。

1.2 命令行介绍
用户对设备的日常操作，主要通过输入命令行来实现。用户通过命令行对设备下发各种命令来实现对设备的配置与日常维护操作。

1.3 如何使用接口
介绍接口的概念及接口的常用基础配置。

1.4 基本配置
基本配置包括系统基本环境和用户基本环境的配置。

1.5 用户管理
用户管理包括用户界面和用户登录时的配置。

1.6 管理文件系统
介绍了文件系统的基础知识，主要包括管理文件、管理目录和管理存储设备的方法。

1.7 管理配置文件
管理配置文件包括当前配置和配置文件，以及主备配置一致性检测和恢复。

1.8 FTP 和 TFTP
FTP 和 TFTP 是常用的文件传输协议。

1.9 Telnet 及 SSH
Telnet 及 SSH 提供通过终端远程登录并访问服务器的方式。

1.10 SSL 配置
安全套接层 SSL（Secure Sockets Layer）可对用户和服务器之间传送的数据进行加密和鉴别，实现合法用户安全登录服务器。

华为专有和保密信息
版权所有 © 华为技术有限公司

1.1 登录交换机

配置交换机之前需要首先登录交换机。

1.1.1 简介

可以通过 Console 口、Telnet 登录交换机。

通过 Console 口登录交换机

通过 Console 口登录主要用于交换机第一次上电或本地配置。

有两种情况，只能通过 Console 口对交换机进行配置：

- 交换机第一次上电；
- 无法通过 Telnet 登录交换机。

通过 Telnet 登录交换机

如果已知待登录交换机的 IP 地址，用户可以通过 Telnet 方式登录到交换机上，进行本地或者远程配置。

用户需要通过 Console 口方式预先正确配置交换机接口的 IP 地址，配置用户账号以及正确的登录验证方式和呼入呼出受限规则，并且终端与交换机之间直连或有可达路由。

目标交换机根据配置的登录参数对用户进行验证，包括三种方式：

- password 验证：登录用户需要输入正确的口令
- AAA 本地验证：登录用户需要输入正确的用户名和口令
- 不验证：登录用户不需要输入用户名或口令

登录成功后，Telnet 客户端界面上出现命令行提示符（如<Quidway>）。此时可以键入命令，查看交换机运行状态，或对交换机进行配置，需要帮助可以随时键入“?”。

说明

通过 Telnet 配置交换机时，请不要轻易改变交换机的 IP 地址（修改可能导致 Telnet 连接断开）。如有必要修改，须在修改后输入交换机的新 IP 地址，重新建立连接。

1.1.2 通过 Console 口登录交换机

通过 Console 口配置终端与交换机的连接，搭建配置环境。

建立配置任务

在进行通过 Console 口登录交换机配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

通过 Console 口登录主要用于交换机第一次上电或本地配置。

版权所有 © 华为技术有限公司

说明

当交换机无法远程访问时，可通过 Console 口登录。

前置任务

在配置通过 Console 口登录交换机之前，需要完成以下任务：

- 准备好 PC/终端（含串口和 RS-232 电缆）
- PC 已安装终端仿真程序（如 Windows XP 的超级终端）

数据准备

在通过 Console 口登录交换机之前，需要准备以下数据。

说明

如果通过 Console 口登录交换机时配置了 AAA 验证方式，需要登录用户名和密码。

序号	数据
1	终端通信参数（包括波特率、数据位、奇偶校验、停止位和流量控制）
2	（可选）AAA 验证方式下的登录用户名和密码

建立物理连接

通过 Console 口登录交换机的物理连接方法。

背景信息

请在登录的交换机上进行以下配置。

操作步骤

步骤 1 使用配置电缆将 PC 的 COM 口和交换机的 Console 口连接。

步骤 2 所有设备上电，自检正常。

----结束

配置终端

通过 Console 口登录交换机配置终端的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 在 PC 上运行终端仿真程序，设置终端通信参数为：

- 波特率：9600 bps

版权所有 © 华为技术有限公司

- 数据位：8
- 停止位：1
- 校验：无
- 流控：无

----结束

登录交换机

通过 Console 口登录交换机的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 按 Enter 键，直到出现用户视图的命令行提示符，如<Quidway>；至此用户进入了用户视图配置环境。

说明

如果通过 Console 口登录交换机时配置了 AAA 或 Password 验证方式，需要在登录之前输入登录用户名和密码。

----结束

1.1.3 通过 Telnet 登录交换机

通过 Telnet 配置终端与交换机的连接，搭建配置环境。

建立配置任务

在进行通过 Telnet 登录交换机配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

如果已知待登录交换机的 IP 地址，用户可以通过 Telnet 方式登录到交换机上，进行本地或者远程配置。

前置任务

在配置通过 Telnet 登录交换机之前，需要完成以下任务：

- 设备上电自检正常
- 准备好 PC（含串口和 GigabitEthernet 交叉/直通网线）

数据准备

在配置通过 Telnet 登录交换机之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	PC 的 IP 地址
2	待配置交换机以太网接口的 IP 地址
3	Telnet 访问的用户信息（用户名、口令和验证方式）

建立物理连接

通过 Telnet 登录交换机的物理连接方法。

前提条件

完成物理连接的建立。

操作步骤

步骤 1 通过网线把交换机和 PC 直连或 PC 和交换机分别通过网线连接入网络中。

----结束

配置登录用户参数

通过 Telnet 登录交换机配置登录用户参数的方法。

背景信息

请在登录的交换机上进行以下配置。

操作步骤

步骤 1 配置登录用户的验证方式。

步骤 2 配置登录用户的权限限制。

配置的具体步骤请参见 **1.5.4 配置 VTY 用户界面**和 **1.5.6 配置用户管理**。

----结束

从 Telnet 客户端登录

通过 Telnet 登录交换机的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 在 PC 上运行 Telnet 客户端程序，键入目标交换机提供 Telnet 服务的接口 IP 地址。

版权所有 © 华为技术有限公司

步骤 2 在登录窗口输入用户名和口令，验证通过后，出现用户视图的命令行提示符，如<Quidway>。至此用户进入了用户视图配置环境。

----结束

1.1.4 配置举例

配置通过 Console 口、Telnet 登录交换机的实例分析。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

配置通过 Console 口登录示例

配置通过 Console 口登录交换机的示例。在本示例中，在 PC 端进行登录的设置，实现通过 Console 口登录交换机。

组网需求

交换机第一次上电，需要通过串口对交换机进行初始的配置。

图 1-1 配置通过 Console 口登录组网图



配置思路

1. 通过 Console 口连接 PC 和交换机。
2. 在 PC 端进行登录的设置。
3. 登录交换机。

数据准备

终端通信参数（包括波特率、数据位、奇偶校验、停止位和流量控制）。

操作步骤

步骤 1 建立本地配置环境，只需将 PC（或终端）的串口通过标准 RS-232 配置电缆与交换机的 Console 口连接。

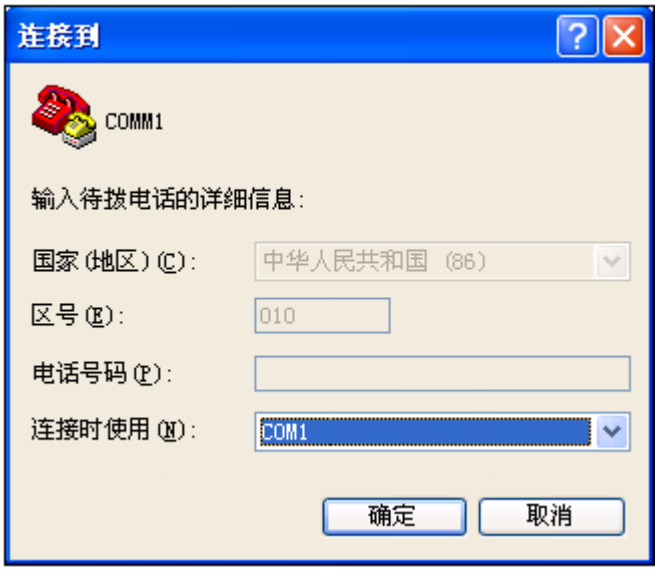
步骤 2 在 PC 上运行终端仿真程序。设置终端通信参数为 9600bps、8 位数据位、1 位停止位、无校验和无流控，如图 1-2 至图 1-4 所示。

版权所有 © 华为技术有限公司

图 1-2 新建连接

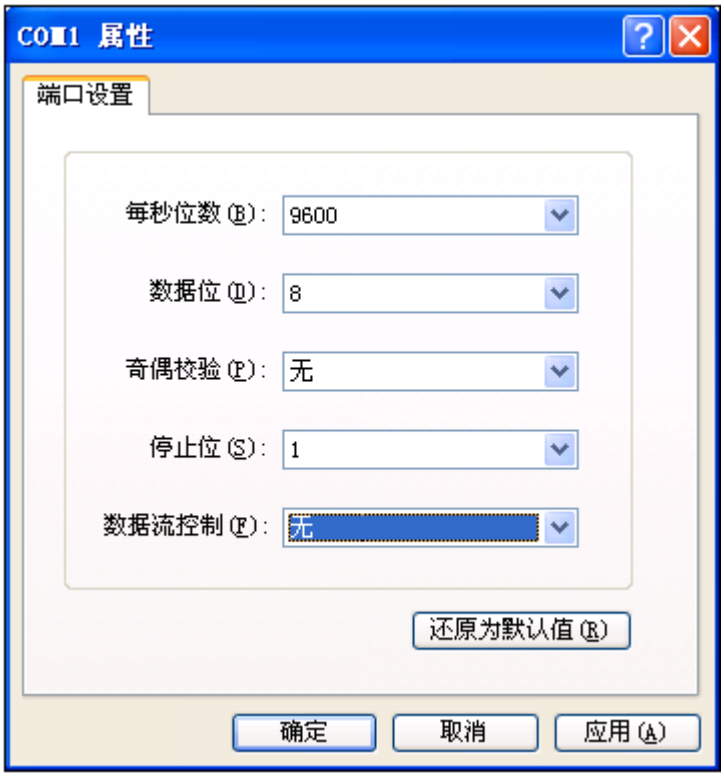


图 1-3 连接端口设置



版权所有 © 华为技术有限公司

图 1-4 端口通信参数设置



步骤 3 交换机上电自检，系统自动进行配置，自检结束后提示用户键入回车，直到出现命令行提示符（如<Quidway>）。

此时可以键入命令，查看交换机运行状态，或对交换机进行配置，需要帮助可以随时键入“?”。

----结束

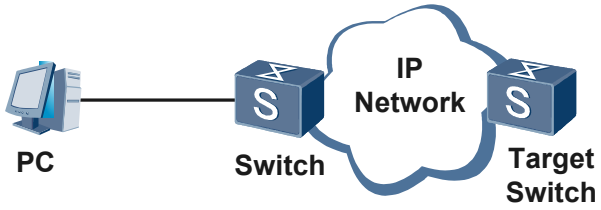
配置通过 Telnet 登录示例

配置通过 Telnet 登录交换机的示例。在本示例中，通过配置用户登录参数，实现从客户端登录交换机。

组网需求

用户可以通过 PC 等配置终端登录到其它网段上的交换机，进行远程维护。

图 1-5 配置通过 Telnet 登录组网图



华为专有和保密信息
版权所有 © 华为技术有限公司

配置思路

1. 建立物理连接
2. 配置用户登录参数
3. 从客户端登录交换机

数据准备

- PC 的 IP 地址
- 待配置交换机以太网接口的 IP 地址
- Telnet 访问的用户信息（用户名、口令和验证方式）

操作步骤

步骤 1 在 PC 端和交换机端分别和网络连接。

步骤 2 在 Target 交换机端配置登录用户参数。

配置登录地址

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type hybrid
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway]interface vlanif 10
[Quidway-vlanif10] ip address 202.38.160.92 255.255.0.0
[Quidway-vlanif10] quit
```

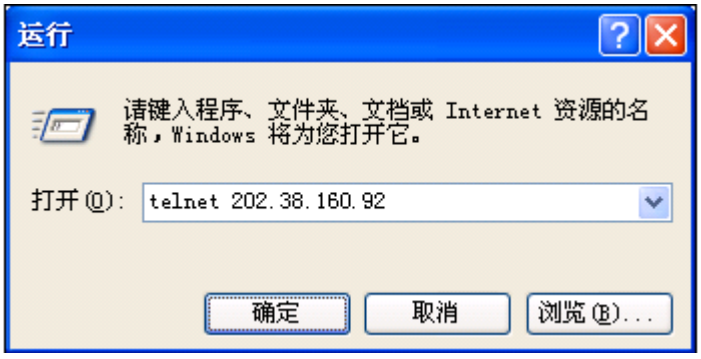
配置登录验证方式

```
[Quidway] aaa
[Quidway-aaa] local-user huawei password cipher hello
[Quidway-aaa] local-user huawei service-type telnet
[Quidway-aaa] local-user huawei level 3
[Quidway-aaa] quit
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
```

步骤 3 配置客户端登录

在 PC 上运行 Telnet，如下图所示。

图 1-6 PC 上的 Telnet 界面



版权所有 © 华为技术有限公司

单击<确定>。

在登录窗口输入用户名和口令，验证通过后，出现用户视图的命令行提示符，如<Quidway>。至此用户进入了用户视图配置环境。

说明

登录交换机前，需要保证 PC 和交换机能够 ping 通，否则无法登录交换机。

----结束

1.2 命令行介绍

用户对设备的日常操作，主要通过输入命令行来实现。用户通过命令行对设备下发各种命令来实现对设备的配置与日常维护操作。

1.2.1 命令行简介

命令行接口是用户对命令行使用的常用工具。

命令行接口

通过命令行接口输入命令，您可以对交换机进行配置和管理。

用户登录到交换机出现命令行提示符后，即进入命令行接口 CLI（Command Line Interface）。命令行接口是用户与交换机进行交互的常用工具。

系统向用户提供一系列命令，用户可以通过命令行接口输入命令，对交换机进行配置和管理。

命令行接口有如下特性：

- 允许通过 Console 口进行本地配置。
- 允许通过 Telnet、SSH 进行本地或远程配置。
- 提供 User-interface 视图，管理各种终端用户的特定配置。
- 命令分级保护，不同级别的用户只能执行相应级别的命令。
- 通过不认证、password、AAA 三种验证方式，确保未授权用户无法侵入交换机，保证系统的安全。
- 用户可以随时键入“?”而获得在线帮助。
- 提供网络测试命令，如 **tracert**、**ping** 等，迅速诊断网络是否正常。
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障。
- 用 **telnet** 命令直接登录并管理其它交换机。
- 提供 FTP 服务，方便用户上传、下载文件。
- 提供类似 DosKey 的功能，可以执行某条历史命令。
- 命令行解释器提供不完全匹配和上下文关联等多种智能命令解析方法，方便用户输入。

版权所有 © 华为技术有限公司

说明

- 系统可正确执行的命令长度最大为 512 个字符，包括使用不完整格式的情况。
- 如果使用不完整格式进行配置，由于命令保存到配置文件中时使用的是完整格式，可能导致配置文件中存在长度超过 512 个字符的命令。系统重启时，这类命令将无法恢复。因此，在使用不完整格式的命令进行配置时，也需要注意命令的总长度。

命令级别

系统命令采用分级保护方式，命令从低到高划分为 16 个级别。

缺省情况下，命令按如下 0 ～ 3 级进行注册：

- 0 级，参观级：网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（Telnet 客户端）等。
- 1 级，监控级：用于系统维护，包括 display 等命令。
- 2 级，配置级：业务配置命令，包括路由、各个网络层次的命令，向用户提供直接网络服务。
- 3 级，管理级：用于系统基本运行的命令，对业务提供支撑作用，包括文件系统、FTP、TFTP、Xmodem 下载、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令；用于业务故障诊断的 debugging 命令等。

注意

并不是所有 display 命令都是监控级，比如管理配置文件中的 **display current-configuration** 命令和 **display saved-configuration** 命令是 3 级管理级。各命令的级别请参见《AC6605 命令参考》手册。

如果用户需要实现权限的精细管理，可以将命令级别提升到 0 ～ 15 级。关于命令级别的提升请参见“**设置命令级别**”。

说明

- 实际实现中，根据命令的重要程度，有可能出现某些命令的缺省级别要高于本命令按照命令规则定义所对应的级别。
- 登录用户也划分为 16 级，与命令级别对应。不同级别的用户登录后，只能使用等于或低于自己级别的命令。关于用户分级请参见“**用户管理**”。

命令视图

命令行接口分为若干个命令视图，所有命令都注册在某个（或某些）命令视图下，通常情况下，必须先进入命令所在的视图才能执行该命令。

命令视图基本概念

与交换机建立连接，如果此交换机是缺省配置，则进入用户视图，在屏幕上显示：

```
<Quidway>
```

键入 **system-view** 后回车，进入系统视图。

```
<Quidway> system-view
[Quidway]
```


版权所有 © 华为技术有限公司

在系统视图下键入 **aaa**，则可进入 AAA 视图。

```
[Quidway] aaa
[Quidway-aaa]
```

说明

命令行提示符“Quidway”是缺省的主机名（sysname）。通过提示符可以判断当前所处的视图，例如：“<>”表示用户视图，“[]”表示除用户视图以外的其它视图。

有些在系统视图下实现的命令，在其它视图下也可以实现，但实现的功能与命令视图密切相关。

常用视图

AC6605 的命令视图有很多，下面提到的视图是最常用的视图。其他视图的进入方式在具体的命令中都有说明，请参见*《Quidway AC6605 T 比特路由交换机 命令参考》*。

- 用户视图

项目	解释
功能	查看 AC6605 的简单运行状态和统计信息。
进入命令	连接建立后直接进入
进入后提示符	<Quidway>
退出命令	<Quidway> **quit**
退出后提示符	无

- 系统视图

项目	解释
功能	配置 AC6605 的系统参数，并通过该视图进入其他功能配置视图。
进入命令	<Quidway> **system-view**
进入后提示符	[Quidway]
退出命令	[Quidway] **quit**
退出后提示符	<Quidway>

- 以太网接口视图
  - 千兆以太网接口视图

项目	解释
功能	配置 AC6605 千兆以太网接口的相关参数，管理千兆以太网接口。
进入命令	[Quidway] **interface GigabitEthernet** *X/Y/Z*
进入后提示符	[Quidway-GigabitEthernet*X/Y/Z*]

版权所有 © 华为技术有限公司

项目	解释
退出命令	[Quidway-GigabitEthernet*X/Y/Z*] **quit**
退出后提示符	[Quidway]

说明

X/Y/Z 为需要配置的千兆以太网接口的接口编号，分别对应“槽位号/子卡号/接口序号”。

如果是千兆和万兆以太网接口的混合板，区别在于万兆接口所在子卡不同，其中万兆以太网接口对应的接口序号通常只对应一个序号为 1；如果接口板上全是万兆以太网接口，则和千兆以太网接口视图进入方法一样。

1.2.2 在线帮助

输入命令行或进行配置业务时，在线帮助可以提供在配置手册之外的实时帮助。

背景信息

AC6605 的命令行接口提供如下三种在线帮助：

- 完全帮助
- 部分帮助
- 命令行错误信息

完全帮助

应用完全帮助，系统可以协助您在输入命令行时，给予全部关键字或参数的提示。

命令行的完全帮助可以通过以下 3 种方式获取：

- 在所有命令视图下，键入“?”获取该命令视图下所有的命令及其简单描述。
  ```
  <Quidway> ?
  ```
- 键入命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其描述。举例如下。
  ```
  [Quidway-ui-vty0] authentication-mode ?
    aaa       AAA authentication
    none      Login without checking
    password  Authentication through the password of a user terminal interface
  [Quidway-ui-vty0] authentication-mode aaa ?
  <cr>
  [Quidway-ui-vty0] authentication-mode aaa
  ```
  其中 aaa、none 和 password 是关键字，AAA authentication、Login without checking 和 Authentication through the password of a user terminal interface 是对关键字的分别描述。

  <cr>表示该位置没有关键字或参数，在紧接着的下一个命令行该命令被复述，直接键入回车即可执行。
- 键入命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数名和参数描述。举例如下。
  ```
  <Quidway> system-view
  [Quidway] sysname ?
  TEXT  Host name(1 to 246 characters)
  ```


版权所有 © 华为技术有限公司

其中 TEXT 是参数名，Host name(1 to 246 characters)是对参数的描述。

部分帮助

应用部分帮助，系统可以协助您在输入命令行时，给予以该字符串开头的所有关键字或参数的提示。

背景信息

命令行的部分帮助可以通过以下三种方式获取。

操作步骤

- 键入一字符串，其后紧接“?”，列出以该字符串开头的所有关键字。

```
<Quidway> d?
  debugging                               delete
  dir                                     display
```

- 键入一命令，后接一字符串紧接“?”，列出命令以该字符串开头的所有关键字。

```
<Quidway> display b?
  bfd                                     bgp
  bootrom                                 bpdu
  bpdu-tunnel                             buffer
```

- 输入命令的某个关键字的前几个字母，按下<tab>键，可以显示出完整的关键字，前提是这几个字母可以唯一标示出该关键字，否则，连续按下<tab>键，可出现不同的关键字，用户可以从中选择所需要的关键字。

----结束

命令行错误信息

所有用户键入的命令，如果通过语法检查，则正确执行，否则系统将会向用户报告错误信息。

常见错误信息参见**表 1-1**。

表 1-1 命令行常见错误信息表

英文错误信息	错误原因
Unrecognized command	没有查找到命令
	没有查找到关键字
Wrong parameter	参数类型错
	参数值越界
Incomplete command	输入命令不完整
Too many parameters	输入参数太多
Ambiguous command	输入命令不明确

版权所有 © 华为技术有限公司

1.2.3 命令行特性

命令行的特性包括编辑特性、显示特性、正则表达式的使用以及历史命令。

编辑特性

命令行编辑功能有助于您利用某些特定的键进行命令的编辑或者获得帮助。

AC6605 的命令行接口提供基本的命令编辑功能，支持多行编辑，每条命令最大长度为 512 个字符。

一些常用的编辑功能如表 1-2 所示。

表 1-2 编辑功能表

功能键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标，否则，响铃告警。
退格键 BackSpace	删除光标位置的前一个字符，光标左移，若已经到达命令首，则响铃告警。
左光标键←或<Ctrl_B>	光标向左移动一个字符位置，若已经到达命令首，则响铃告警。
右光标键→或<Ctrl_F>	光标向右移动一个字符位置，若已经到达命令尾，则响铃告警。
Tab 键	输入不完整的关键字后按下 Tab 键，系统自动执行部分帮助： ● 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示，光标距词尾空一格； ● 对于不匹配或者匹配的关键字不唯一的情况，首先显示前缀，继续按 Tab 键循环翻词，此时光标距词尾不空格，按空格键输入下一个单词； ● 如果输入错误关键字，按 Tab 键后，换行显示，输入的关键字不变。

显示特性

所有的命令行有共同的显示特性，并且可以根据用户的需求，灵活构建显示方式。

AC6605 的命令行接口提供如下显示特性：

- 提示信息和帮助信息提供中、英文两种语言显示。
- 在一次显示信息超过一屏时，提供暂停功能，在暂停显示时用户可以有三种选择，如表 1-3 所示。

版权所有 © 华为技术有限公司

表 1-3 显示功能表

功能键	功能
键入<Ctrl_C>	停止显示和命令执行。 **说明** 也可以键入除空格键、回车键等的其他键停止显示和命令执行。
键入空格键	继续显示下一屏信息。
键入回车键	继续显示下一行信息。

正则表达式

正则表达式是一种模式匹配工具，用户根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。

正则表达式描述了一种字符串匹配的模式，由普通字符（例如字符 a 到 z）和特殊字符（或称“元字符”）组成。正则表达式作为一个模板，将某个字符模式与所搜索的字符串进行匹配。

正则表达式一般具有以下功能：

- 检查字符串中符合某个规则的子字符串，并可以获取该子字符串。
- 根据匹配规则对字符串进行替换操作。

正则表达式的语法规则

正则表达式由普通字符和特殊字符组成。

- 普通字符

  普通字符匹配的对象是普通字符本身。包括所有的大写和小写字母、数字、标点符号以及一些特殊符号。例如：a 匹配 abc 中的 a，202 匹配 202.113.25.155，@匹配 xxx@xxx.com 中的@。

- 特殊字符

  特殊字符配合普通字符匹配复杂或特殊的字符串组合。表 1-4 是对特殊字符及其语法意义的使用描述。

表 1-4 特殊字符及其语法意义描述

特殊字符	功能	举例
\	转义字符。将下一个字符（特殊字符或者普通字符）标记为普通字符。	*匹配*
^	匹配行首的位置。	^10 匹配 10.10.10.1，不匹配 20.10.10.1
$	匹配行尾的位置。	1$匹配 10.10.10.1，不匹配 10.10.10.2

版权所有 © 华为技术有限公司

特殊字符	功能	举例
*	匹配前面的子正则表达式零次或多次。	10*可以匹配 1、10、100、1000、…… (10)*可以匹配空、10、1010、101010、……
+	匹配前面的子正则表达式一次或多次。	10+可以匹配 10、100、1000、…… (10)+可以匹配 10、1010、101010、……
?	匹配前面的子正则表达式零次或一次。	10?可以匹配 1 或者 10 (10)?可以匹配空或者 10
.	匹配任意单个字符。	0.0 可以匹配 0x0、020、…… .oo.可以匹配 book、look、tool、……
()	一对圆括号内的正则表达式作为一个子正则表达式，匹配子表达式并获取这一匹配。圆括号内也可以为空。	100(200)+可以匹配 100200、100200200、……
x|y	匹配 x 或 y。	100|200 匹配 100 或者 200 1(2|3)4 匹配 124 或者 134，而不匹配 1234、14、1224、1334
[xyz]	匹配正则表达式中包含的任意一个字符。	[123]匹配 255 中的 2
[^xyz]	匹配正则表达式中未包含的字符。	[^123]匹配除 123 之外的任何字符
[a-z]	匹配正则表达式指定范围内的任意字符。	[0-9]匹配 0 到 9 之间的所有数字
[^a-z]	匹配正则表达式指定范围外的任意字符。	[^0-9]匹配所有非数字字符
_	匹配一个逗号（,）、左花括号（{）、右花括号（}）、左圆括号、右圆括号。 匹配输入字符串的开始位置。 匹配输入字符串的结束位置。 匹配一个空格。	_2008_可以匹配 2008、空格 2008 空格、空格 2008、2008 空格、,2008,、{2008}、(2008)、{2008、(2008}

说明

除非特别说明，上表中涉及到的字符指的是可以打印的字符。

- 特殊字符的退化

  某些特殊字符如果处在如下的正则表达式的特殊位置时，会引起退化，成为普通字符。

版权所有 © 华为技术有限公司

- 特殊字符处在转义符号‘\’之后，则发生转义，变为匹配该字符本身。
- 特殊字符“*”、“+”、“?”，处于正则表达式的第一个字符位置。例如：+45匹配+45，abc(*def)匹配 abc*def。
- 特殊字符“^”，不在正则表达式的第一个字符位置。例如：abc^匹配 abc^。
- 特殊字符“$”，不在正则表达式的最后一个字符位置。例如：12$2 匹配 12$2。
- 右括号“)”或者“]”没有对应的左括号“(”或“[”。例：abc)匹配 abc)，0-9]匹配 0-9]。

说明

除非特别说明，以上正则表达式包括括号“（）”内包含的子正则表达式。

- 普通字符与特殊字符的组合使用

  实际应用中，往往不是一个普通字符加上一个特殊字符配合使用，而是由多个普通字符和特殊字符组合，匹配某些特征的字符串。

在命令中指定过滤方式

注意

AC6605 采用正则表达式实现管道符的过滤功能。并非所有 display 命令均支持管道符。当显示信息内容很多时，此 display 命令支持管道符；当显示信息内容很少时，此 display 命令不支持管道符。

按过滤条件进行查询时，显示内容的第一行信息中，以包含该字符串的整条信息作为起始，而非过滤字符串作为起始。

系统支持使用| **count**，显示使用过滤条件后输出的结果的行数。可以与过滤方式配合使用。

在支持正则表达式的命令中，有三种过滤方式可供选择：

- | **begin** *regular-expression*：输出以匹配指定正则表达式的行开始的所有行。
- | **exclude** *regular-expression*：输出不匹配指定正则表达式的所有行。
- | **include** *regular-expression*：只输出匹配指定正则表达式的所有行。

说明

regular-expression 为字符串形式，长度范围是 1 ~ 255。

在分屏显示时指定过滤方式

采用分屏显示时，可以在分屏提示符“---- More ----”中指定过滤类型：

- /*regular-expression*：输出以匹配指定正则表达式的行开始的所有行。
- -*regular-expression*：输出不匹配指定正则表达式的所有行。
- +*regular-expression*：只输出匹配指定正则表达式的所有行。

历史命令

命令行接口提供类似 Doskey 功能，能够自动保存用户键入的历史命令，用户可以随时调用命令行接口保存的历史命令，并重复执行。

版权所有 © 华为技术有限公司

缺省情况下，为每个登录用户保存 10 条历史命令。对历史命令的操作如表 1-5 所示。

表 1-5 访问历史命令

操作	命令或功能键	结果
显示历史命令	**display history-command**	显示用户键入的历史命令。
访问上一条历史命令	上光标键或者<Ctrl_P>	如果还有更早的历史命令，则取出上一条历史命令，否则响铃警告。
访问下一条历史命令	下光标键或者<Ctrl_N>	如果还有更新的历史命令，则取出下一条历史命令，否则清空命令，响铃警告。

说明

对于 Windows 9X 的超级终端，↑光标键无效，这是由于 Windows 9x 的超级终端对这个键作了不同解释，这时可以用组合键<Ctrl_P>代替↑光标键达到同样目的。

在使用历史命令功能时，需要注意：

- AC6605 保存的历史命令与用户输入的命令格式相同，如果用户使用了命令的不完整形式，保存的历史命令也是不完整形式。
- 如果用户多次执行同一条命令，AC6605 的历史命令中只保留最早的一次。但如果执行时输入的形式不同，将作为不同的命令对待。

  例如：多次执行 **display ip routing-table** 命令，历史命令中只保存一条。如果执行 **display ip routing** 和 **display ip routing-table**，将保存为两条历史命令。

1.2.4 快捷键

可以通过使用系统快捷键，完成对应命令的输入，简化操作。

系统快捷键

系统快捷键是系统中固定的快捷键，不由用户定义，代表固定功能。系统包括的主要快捷键如表 1-6 所示。

说明

由于不同的终端软件对于某些键的解释不同，具体终端上实际可用的快捷键与本节所列举的按键组合可能略有差异。

表 1-6 系统快捷键

功能键	功能
CTRL_A	将光标移动到当前行的开头。
CTRL_B	将光标向左移动一个字符。
CTRL_C	停止当前正在执行的功能。

版权所有 © 华为技术有限公司

功能键	功能
CTRL_D	删除当前光标所在位置的字符。
CTRL_E	将光标移动到当前行的末尾。
CTRL_F	将光标向右移动一个字符。
CTRL_H	删除光标左侧的一个字符。
CTRL_K	在连接建立阶段终止呼出的连接。
CTRL_N	显示历史命令缓冲区中的后一条命令。
CTRL_P	显示历史命令缓冲区中的前一条命令。
CTRL_R	重新显示当前行信息。
CTRL_T	终止呼出的连接。
CTRL_V	粘贴剪贴板的内容。
CTRL_W	删除光标左侧的一个字符串（字）。
CTRL_X	删除光标左侧所有的字符。
CTRL_Y	删除光标右侧所有的字符。
CTRL_Z	返回到用户视图。
CTRL_]	终止呼入的连接或重定向连接。
ESC_B	将光标向左移动一个字（word）。
ESC_D	删除光标右侧的一个字（word）。
ESC_F	将光标向右移动一个字（word）。
ESC_N	将光标向下移动一行。
ESC_P	将光标向上移动一行。

1.2.5 配置举例

通过以下几个举例，您可以了解到命令行的基本使用。

Tab 键使用示例

输入 Tab 键可以提示所有相关的关键字，或者检查关键字是否正确。

操作步骤

- 如果与不完整的关键字匹配的关键字唯一。
  请在 AC6605 上执行以下配置。
  1. 输入不完整的关键字。

版权所有 © 华为技术有限公司

```
[Quidway] info-
```

2. 按下 Tab 键。

   则系统用此完整的关键字替代原输入并换行显示，光标距词尾空一格。

```
[Quidway] info-center
```

- 如果不匹配或者匹配的关键字不唯一。

  请在 AC6605 上进行以下配置。

  # 关键字 info-center 后面可以跟如下 2 个关键字。

```
[Quidway] info-center log?
  logbuffer                              loghost
```

1. 输入不完整的关键字。

```
[Quidway] info-center l
```

2. 按下 Tab 键。

   则系统首先显示所有匹配的关键字的前缀，本例中前缀是“log”。

```
[Quidway] info-center log
```

3. 继续按 Tab 键循环翻词，此时光标距词尾不空格。

```
[Quidway] info-center loghost
[Quidway] info-center logbuffer
```

   找到所需要的关键字 **logbuffer** 后，停止按 Tab 键。

4. 按空格键，然后输入下一个单词 channel。

```
[Quidway] info-center logbuffer channel
```

----结束

1.3 如何使用接口

介绍接口的概念及接口的常用基础配置。

1.3.1 接口概述

接口是 AC6605 提供给用户操作或配置的单元，主要用于接收和发送数据。

接口从功能上可以划分为管理接口和业务接口，从物理形态上可以划分为物理接口和逻辑接口。

说明

物理接口有时也被称为端口，为便于描述，在本手册中，统一描述为接口。

管理接口

管理接口，是一种人为的划分，主要是相对于业务接口而言的。管理接口主要为用户提供配置管理支持，也就是用户通过此类接口可以登录到 AC6605，并进行配置和管理操作。管理接口不承担业务传输。

AC6605 的管理接口为 Console 口。

版权所有 © 华为技术有限公司

表 1-7 各管理接口介绍

接口名称	接口描述	接口用途
Console 口	遵循 EIA/TIA-232 标准，接口类型是 DCE。	该接口和配置终端的 COM 串口连接，用于搭建现场配置环境。

管理接口的编号规则如下：

表 1-8 各管理接口编号

接口名称	管理接口编号
Console 口	通常描述为用户界面接口“console 0”

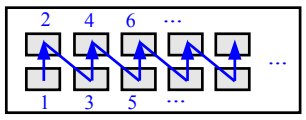
业务接口分类

业务接口就是承担业务传输的各类接口，按照接口速率可以分为百兆接口、千兆接口和万兆接口；按照接口电气属性可以分为电接口、光接口。

业务接口的编号规则如下：

- 槽位号：表示当前交换机的槽位，取值为 0。
- 子卡号：表示业务接口板支持的子卡号，值为 0。
- 接口序号：表示设备上各接口的编排顺序号。

表 1-9 以太网接口编号规则

接口编排规则示意图	说明
	设备有两排业务接口，左下接口从 1 起始编号，依据从下到上，再从左到右的规则依次递增编号。 例如，左上第一个接口编号为 0/0/2。

物理接口

物理接口是实际存在的接口。

物理接口包括各管理接口和各业务接口。

AC6605 目前支持物理接口包括：

- Console 口
- 千兆以太网 GE（Gigabit Ethernet）接口

逻辑接口

逻辑接口是指物理上不存在且需要通过配置建立的接口。

版权所有 © 华为技术有限公司

AC6605 目前支持的逻辑接口包括：

- Eth-Trunk 接口

  Eth-Trunk 只能由以太网链路构成。

  Eth-Trunk 技术有如下优点：

  - 增加带宽：Eth-Trunk 接口的带宽是各成员接口带宽的总和。
  - 提高可靠性：当某个成员链路出现故障时，流量会自动的切换到其他可用的链路上，从而提高整个 Eth-Trunk 链路的可靠性。

  具体配置方法请参见《AC6605 无线接入控制器 配置指南-以太网》中的“链路聚合配置”。

- Loopback 接口

  Loopback 是一种虚拟接口。TCP/IP 协议规定，127.0.0.0 网段的地址属于环回地址，包含这类地址的接口属于环回接口。

  系统在启动时自动创建一个使用环回地址 127.0.0.1 的接口，用来接收所有发送给本机的数据包。

  但是有些应用（如配置 VPN 互访）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口；要求该本地接口的 IP 地址为 32 位掩码（节约 IP 地址），并且能够被路由协议发布出去。

  利用 Loopback 接口永远 Up 的特性，还可以用做 Router ID、LSR ID、Tunnel 隧道借用 Loopback 的 IP 地址等。

  具体的配置方法请参见**配置 Loopback 接口**。

- NULL 接口

  Null 接口类似于一些操作系统中支持的空设备（Null Devices），任何送到该接口的网络数据报文都会被丢弃。 Null 接口主要应用在路由选择和策略路由中。比如在路由选择的过程，如果匹配不到路由，就会把报文送到该接口。

- Tunnel 接口

  Tunnel 接口是一种逻辑接口，可以用于其他接口的备份接口、建立 GRE 隧道或 MPLS TE 隧道。

- VLANIF 接口

  当 AC6605 需要与网络层的设备通信时，可以在 AC6605 上创建基于 VLAN 的逻辑接口，即 VLANIF 接口。VLANIF 接口是网络层接口，可以配置 IP 地址。借助 VLANIF 接口，AC6605 就能与其它网络层的设备互相通信。

  具体配置方法请参见《AC6605 无线接入控制器 配置指南-以太网》中的“配置 VLANIF 接口”。

1.3.2 配置接口基本参数

介绍如何对接口进行初步配置。

建立配置任务

在配置接口工作方式、路由等高级配置前，需要对接口进行基本配置。

应用环境

为了便于对接口进行配置和维护，在 AC6605 中配置了接口视图，与接口有关的各种命令都必须在相应的接口视图下使用。

版权所有 © 华为技术有限公司

接口的基础配置包括：进入接口、配置接口描述信息、启动和关闭接口等。

前置任务

在 AC6605 上正确安装接口板卡。

数据准备

在配置接口之前，需准备以下数据：

序号	数据
1	需配置接口的接口类型和接口编号
2	接口的描述信息

进入接口视图

对接口进行基本配置前，需要进入接口视图。

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。

其中，*interface-type* 为接口类型；*interface-number* 为接口编号。

----结束

查看接口下所有命令

进入接口视图后，可以查看接口视图下的所有命令。

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* 进入指定的接口视图。

步骤 3 执行命令**?**，查看指定接口视图下所有命令。

----结束

版权所有 © 华为技术有限公司

配置接口描述

AC6605 对于接口有一个接口描述，用来帮助识别和记忆接口的用途，以便管理。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。

步骤 3 执行命令 **description** *description*，配置接口描述。

----结束

启动和关闭接口

当某物理接口闲置，没有连接电缆时，请使用关闭该接口，以防止由于干扰导致接口异常；当需要使用关闭的接口时，请启动相应的接口。

背景信息

说明

- Null 接口一直处于 Up 状态，不能使用命令关闭 Null 接口。
- Loopback 接口一旦被创建，将一直保持 Up 状态，不能使用命令关闭 Loopback 接口。

操作步骤

- 关闭接口

  请在 AC6605 上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。
  3. 执行命令 **shutdown**，关闭接口。

  说明

  缺省情况下，接口处于打开状态。

- 启动接口

  请在 AC6605 上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。
  3. 执行命令 **undo shutdown**，启动接口。

----结束

进一步配置接口

配置完基本参数后，请根据需要进一步配置接口。

背景信息

用户要通过接口访问网络，除了需要完成接口的基本配置外，还需要详细了解组网需求，进一步配置接口的多项参数（高级配置）。

版权所有 © 华为技术有限公司

进一步配置接口包括：

- 配置接口工作方式
- 配置路由配置

具体配置请参见《AC6605 无线接入控制器 配置指南-以太网》和《AC6605 无线接入控制器 配置指南-IP 路由》

检查配置结果

基本参数配置完后，可以使用相关的 display 命令显示配置结果。

操作步骤

步骤 1 执行命令 **display interface** [*interface-type* [*interface-number*]]，查看接口当前运行状态和统计信息。

步骤 2 执行命令 **display interface description**，查看接口的描述信息。

步骤 3 执行命令 **display ip interface** [*interface-type interface-number*]，查看接口 IP 的主要配置信息。

步骤 4 执行命令 **display ip interface brief** [*interface-type interface-number*]，查看接口 IP 的简要状态信息。

----结束

1.3.3 配置 Loopback 接口

介绍初步配置 Loopback 接口的方法。

建立配置任务

用户可以创建或删除 Loopback 接口。Loopback 接口一旦被创建，将一直保持 Up 状态，直到被删除。

应用环境

有些应用（如配置 VPN 互访）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且需要将这个接口上的地址通过路由协议发布出去。Loopback 接口也常用来提高配置的可靠性。

前置任务

在配置 Loopback 接口之前，需完成 AC6605 加电启动正常。

数据准备

在配置 Loopback 接口之前，需准备以下数据。

序号	数据
1	Loopback 接口的接口编号

版权所有 © 华为技术有限公司

序号	数据
2	Loopback 接口的 IP 地址

配置 Loopback 接口 IPv4 相关项

Loopback 接口可以配置 IPv4 地址，可以用于绑定 VPN 实例、对源 IPv4 地址进行校验。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface loopback** *interface-number*，创建 Loopback 接口。

interface-number 取值范围为 0 ～ 1023，最多可创建 1024 个 Loopback 接口。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 Loopback 接口的 IPv4 地址。

步骤 4 （可选）执行命令 **ip verify source-address**，配置 Loopback 接口对源 IPv4 地址校验。

----结束

检查配置结果

配置完 Loopback 接口后，请检查配置是否正确。

操作步骤

步骤 1 执行命令 **display interface loopback** [*number*]，查看 Loopback 接口的状态信息。

----结束

1.3.4 维护接口

介绍如何维护接口。

清除接口统计信息

接口统计信息清除后，不能恢复。操作前请仔细确认。

操作步骤

步骤 1 在确认需要清除接口的统计信息后，请在用户视图下，执行命令 **reset counters interface** [*interface-type* [*interface-number*]]清除接口信息。

----结束

1.4 基本配置

基本配置包括系统基本环境和用户基本环境的配置。

版权所有 © 华为技术有限公司

1.4.1 基本配置简介

基本配置的意义和范围。

在配置业务之前，用户往往需要根据系统运行时的环境要求进行一些基本配置，以满足运行维护需求。

AC6605 提供两方面的基本环境配置：

- 系统基本环境：主要包括语言模式、主机名、系统时间、标题文字和命令级别。
- 用户基本环境：主要包括级别切换的口令设置和终端锁定设置。

1.4.2 配置系统的基本环境

配置系统基本配置环境，以符合用户使用习惯或实际环境的需求。

建立配置任务

在进行系统的基本环境配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在配置业务前，用户需要进行系统的基本环境配置，以便符合实际环境的要求。

缺省情况下，AC6605 支持的命令级别为 0 ～ 3 级，依次分别为：访问级、监控级、配置级和管理级。

如果用户需要在设备端定义更多级别，实现权限的更精细管理，可以采用命令行级别扩展功能，将命令级别由 0 ～ 3 级批量提升到 0 ～ 15 级。

前置任务

在配置系统环境之前，需要完成以下任务：

- 交换机上电自检正常

数据准备

在配置系统环境之前，需要准备以下数据。

序号	数据
1	系统时间
2	主机名称
3	登录信息
4	命令级别

版权所有 © 华为技术有限公司

设置设备名称

设备名称可以根据需要进行更改，更改后立即生效。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **sysname** *host-name*，设置设备名称。

设备名称会出现在命令提示符中，用户可以根据需要更改设备名称。

缺省情况下，交换机主机名为 Quidway。

----结束

设置系统时钟

为了保证网络中的设备在同一时钟下工作，需要设置或更改系统时钟。

背景信息

为了保证与其他设备协调工作，需要准确设置系统的时间。AC6605 支持时区和夏时制的设置。

说明

UTC（Universal Time Coordinated）指通用协调时间。

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **clock datetime** *HH:MM:SS YYYY-MM-DD*，设置当前时间。

步骤 2 执行命令 **clock timezone** *time-zone-name* { **add** | **minus** } *offset*，设置所在的时区。

- **add** 将在 UTC 标准时间的基础上增加指定的时区偏移量。即，在系统默认的 UTC 时区的基础上，加上 *offset*，就可以得到 *time-zone-name* 所标识的时区时间。
- **minus** 将在 UTC 标准时间的基础上减去指定的时区偏移量。即，在系统默认的 UTC 时区的基础上，减去 *offset*，就可以得到 *time-zone-name* 所标识的时区时间。

步骤 3 执行命令 **clock daylight-saving-time** *time-zone-name* **one-year** *start-time start-date end-time end-date offset* 或 **clock daylight-saving-time** *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date* } *offset* [*start-year* [*end-year*]]，设置夏令时。

配置周期夏令时，夏令时开始时间和结束时间支持日期+日期、星期+星期、日期+星期、星期+日期四种配置方式。配置方法请参考 **clock daylight-saving-time** 命令。

版权所有 © 华为技术有限公司

说明

当当前时间处在夏令时时，执行命令 **clock timezone** *time-zone-name* { **add** | **minus** } *offset* 设置时区名是可以成功的。但此时执行命令 **display clock** 显示的时区名为夏令时名，当夏令时结束之后，就会显示之前设置的时区名。

----结束

设置标题文本

如果用户需要对登录的用户提供警示或说明信息，可以设置登录时或登录成功后的标题文本。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **header login** { **information** *text* | **file** *file-name* }，设置登录时的标题文本。

执行命令 **header shell** { **information** *text* | **file** *file-name* }，设置登录成功后的标题文本。

标题文本是用户在连接到交换机、进行登录验证以及开始交互配置时系统显示的一段提示信息。为用户登录提供明确的指示信息时，使用此配置。

说明

- 如果在客户端使用 SSH1.X 版本登录交换机，则用户登录时不显示参数 **login** 设置的标题信息，但可以显示参数 **shell** 设置的信息。
- 如果在客户端使用 SSH2.0 版本登录交换机，则设置的登录时和登录成功后的标题信息都可以显示。

----结束

设置命令级别

缺省情况下，命令按 0 ～ 3 级进行注册，如果用户需要实现权限的精细管理，可以将命令级别提升到 0 ～ 15 级。

背景信息

如果用户没有对某条命令单独调整过命令级别，命令级别批量提升后，原注册的所有命令行按以下原则自动调整：

- 0 级和 1 级命令保持级别不变。
- 2 级命令提升到 10 级；3 级命令提升到 15 级。
- 2 ～ 9 级和 11 ～ 14 级这些命令级别中没有命令行。用户可以单独调整命令行到这些级别中，以实现权限的精细化管理。

说明

2 级提升到 10 级，3 级提升到 15 级，并不是两次单独提升，而是一次批量提升。

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **command-privilege level rearrange**，批量提升命令的级别。

如果用户没有设置相应切换到 15 级用户级别的密码，系统会提示用户设置 15 级用户的 super 密码，并询问用户是否继续执行命令级别提升，此时应选择“N”，设置密码。如果选择了“Y”，那么命令的级别就会直接批量提升，导致非 Console 口用户无法提升自己的级别。

步骤 3 执行命令 **command-privilege level** *level* **view** *view-name command-key*，设置命令级别。

command-privilege level 命令可以一次指定多条命令（*command-key*）的级别及所在视图。

所有的命令都有默认的视图和优先级，一般不需要用户进行重新设置。

----结束

1.4.3 配置用户的基本环境

配置用户基本配置环境，以切换用户级别。

建立配置任务

在进行用户的基本环境配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

用户可以以较低级别身份登录到交换机，进行简单配置或者查看。当需要较复杂配置时，需要切换到较高级别身份。因此，需要配置用户进行此切换的基本环境。

前置任务

在配置用户的基本环境之前，需要完成以下任务：

- 交换机上电自检正常

数据准备

在配置用户的基本环境之前，需要准备以下数据。

序号	数据
1	用户级别切换密码

配置切换用户级别的口令

用户由低级别切换到高级别前，需要设置口令。

背景信息

如果用户以较低级别的身份登录到交换机后，需要切换到较高级别的用户身份进行操作，必须输入正确的级别切换口令。该口令需要事先配置。

版权所有 © 华为技术有限公司

注意

如果使用 **simple** 选项，密码将以明文形式保存在配置文件中，以低级别登录的用户可以通过查看配置方式获取切换密码，造成安全问题。因此，一般情况下，应使用 cipher 选项，将密码加密保存。

同时，使用 **cipher** 选项设置了密码后，无法从系统取回。请妥善保管，以免遗忘或者遗失。

在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **super password** [**level** *user-level*] { **simple** | **cipher** } *password*，配置切换用户级别的口令。

----结束

切换用户级别

用户由低级别切换到高级别，需要输入设置好的口令。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **super** [*level*]，切换用户级别。

步骤 2 根据系统提示，输入切换口令。

如果输入的口令正确，将切换到更高级别。如果连续三次输入错误的口令，将退回用户视图，仍保持现有登录级别。

说明

当以低级别登录的用户通过 **super** 命令切换到高级别时，系统会自动发送 **trap** 信息，并记录在日志中。如果切换到的级别低于当前级别，则仅记录日志。

----结束

锁定用户界面

用户可以使用设置好的口令，锁定用户界面。

背景信息

在用户需要暂时离开操作终端时，为防止未授权的用户操作该终端界面，可以锁定用户界面。

请在交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **lock**，锁定用户界面。

步骤 2 根据系统提示，输入解除锁定的口令，并确认口令。

```
<Quidway> lock
Enter Password:
Confirm Password:
```

锁定成功后，系统将提示终端界面已经锁定。

锁定用户界面时，需要输入口令并确认。解除锁定时，必须输入正确的口令。

----结束

1.4.4 显示系统基本配置信息

显示系统基本配置信息有相应的 display 命令。

背景信息

利用 display 命令可以收集系统状态信息，根据功能可以划分为以下几类：

- 显示系统配置信息的 display 命令
- 显示系统运行状态的 display 命令
- 显示系统诊断信息的 display 命令
- 显示主控板重启信息的 display 命令

有关各协议和各种接口的 display 命令请参见相关章节。下面只介绍一些有关系统的 display 命令。

可在所有视图下进行下面的操作。

显示系统配置信息

用户可以查看系统版本、系统时钟、起始配置信息、当前配置信息等信息。

背景信息

已完成基本配置。

操作步骤

- 执行命令 **display version**，显示系统版本。
- 执行命令 **display clock** ，显示系统时钟。
- 执行命令 **display saved-configuration**，显示起始配置信息。
- 执行命令 **display current-configuration**，显示当前配置信息。

----结束

显示系统运行状态

用户可以查看当前视图的运行配置等信息。

版权所有 © 华为技术有限公司

背景信息

已完成基本配置。

操作步骤

步骤 1 执行命令 **display this**，显示当前视图的运行配置。

----结束

收集系统诊断信息

用户可以查看系统诊断信息。

背景信息

已完成基本配置。

操作步骤

步骤 1 执行命令 **display diagnostic-information** [*file-name*]，显示系统诊断信息。

在系统出现故障或日常维护时，为了便于问题定位，需要收集很多的信息，但相应的 **display** 命令很多，很难一次把信息收集全，这时可以使用 **display diagnostic-information** 命令进行系统当前各个模块的运行信息收集。

display diagnostic-information 命令一次性收集了如下命令后的终端显示的信息，包括：**display clock**、**display version**、**display cpu-usage**、**display interface**、**display current-configuration**、**display saved-configuration**、**display history-command** 等。

----结束

1.5 用户管理

用户管理包括用户界面和用户登录时的配置。

1.5.1 用户管理简介

用户界面和用户管理的基本概念。

用户界面

用户界面 UI（User Interface）是 AC6605 提供用户登录服务的一种视图。借助用户界面视图，可以配置和管理所有工作在异步、交互方式下的物理接口和逻辑接口参数，实现对登录用户的管理、验证和验证后的授权级别。

用户界面的类型

AC6605 支持的用户界面类型如表 1-10 所示。

版权所有 © 华为技术有限公司

表 1-10 用户界面类型

类型	用途	说明
CON	适用于从 Console 接口进行本地登录	CON 表示一种线设备接口，符合 EIA/TIA-232 标准，接口类型为 DCE。每个设备上提供一个 Console 接口。
VTY	适用于通过 Telnet 或 SSH 方式进行本地或远程登录	VTY 是一种虚拟接口，表示逻辑终端线。当用户终端以 Telnet、FTP 或 SSH 方式登录到 AC6605，就建立了一条 VTY 连接。

用户界面的编号

同一用户界面可以采用两种编号方式：相对编号和绝对编号。

- 相对编号

  相对编号是在每种类型用户界面的内部进行编号。相对编号方式只能唯一指定某种类型的用户界面中的一个或一组，而不能跨类型操作。

  用户界面的相对编号的形式为“用户界面类型+编号”。相对编号规则如下：

  - CON 的相对编号为 console0
  - VTY 缺省的相对编号分别为 vty0、vty1、vty2、vty3 和 vty4

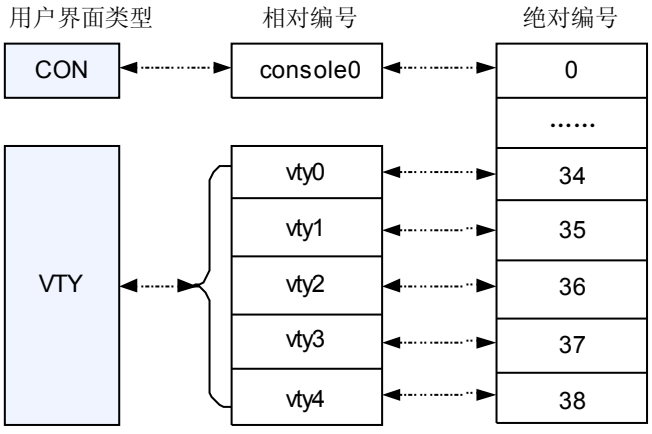
- 绝对编号

  AC6605 为 CON 和各 VTY 用户界面分别指定了唯一的缺省固定编号，分别命名为 0、34、……、38，通过缺省固定编号可以进入指定的用户界面视图。

- 相对编号和绝对编号之间的关系

  同一用户界面的相对编号和绝对编号之间的对应关系如图 1-7 所示。

图 1-7 AC6605 用户界面的编号



从图中可以看出，相对编号和绝对编号之间存在对应关系，例如相对编号 console0 和绝对编号 0 对应相同的用户界面，vty1 和 35 对应相同的用户界面。

说明

在 AC6605 上，用户界面绝对编号的取值范围是 0、34 ~ 48。

版权所有 © 华为技术有限公司

用户验证

对于登录到 AC6605 的用户，系统需要根据配置对其进行验证以保证系统的安全性。

首次启动 AC6605 时，系统内没有预存登录验证信息，此时从 Console 接口登录 AC6605 时无需用户验证。

如果不是初次登录，而是从以太网口通过 Telnet 方式登录，出于安全性考虑，需要对登录用户进行验证。只有验证通过的用户才能登录到 AC6605，并进行各种配置和维护操作。

因此，需要在 AC6605 上规划登录用户，为用户设置登录密码和登录级别，从而实现对登录用户的管理。

规划登录用户的类型

按照用户登录到 AC6605 后获得的服务类型和权限，可以将登录用户按照表 1-11 进行划分。

表 1-11 登录用户的类型

用户类型	登录描述	用户验证需求
超级用户	从 Console 接口通过配置电缆直接登录，拥有所有权限。	初次不验证登录用户，后续建议验证。
Telnet 用户	从以太网口通过 Telnet 方式登录，拥有受控权限。在用户终端和 AC6605 之间建立 Telnet 连接。	建议验证登录用户。
SSH 用户	从以太网口通过 SSH 方式登录，拥有受控权限。在用户终端和 AC6605 之间建立 SSH 连接。	建议验证登录用户。
FTP 用户	从以太网口通过 FTP 方式登录，拥有受控权限。在用户终端和 AC6605 之间建立 FTP 连接。	建议验证登录用户。

用户通过 Telnet、SSH 和 FTP 等方式登录，能获得的权限取决于登录连接所在用户界面的优先级。同时，AC6605 支持同一用户能同时获得多种服务。因此，需要合理的规划登录用户类型和用户级别，兼顾登录便捷性和安全性。

用户的优先级

系统支持对超级用户和 Telnet 用户进行分级管理。

与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越高则优先级越高。

说明

如果不对用户进行优先级规划，默认用户登录级别为 0 ~ 3 级，四个级别。

用户所能访问命令的级别由用户的级别决定。

- 如果对用户采用不验证或 password 验证，登录到 AC6605 的用户所能访问的命令级别由登录时的用户界面级别决定。

版权所有 © 华为技术有限公司

- 如果对用户采用 AAA 验证，登录到 AC6605 的用户所能访问的命令级别由 AAA 配置信息中本地用户的优先级级别决定。

用户所能访问的命令包括用户所在用户级别的命令以及低于用户级别的命令。

例如：如果目前系统中用户级别只有 0 ～ 3 级，级别为 2 的用户可以访问级别为 0、1、2 的命令。级别为 3 的用户可以访问所有命令。

验证登录用户

在 AC6605 上配置了用户后，系统会对新登录用户进行身份验证。AC6605 提供了三种验证方式，如表 1-12 所示。

表 1-12 登录用户的验证方式

验证方式	登录描述
不验证	登录用户不需要输入用户名和密码，就可以直接登录 AC6605。存在很大的安全隐患。
Password 验证	登录用户只需要输入密码，无需用户名，可以获得一定的安全性。
AAA 验证	登录用户需要提供用户名和密码，由 AC6605 根据本地配置的用户信息进行验证。进一步改善了安全性，提供了基于用户的安全管理，适用于通过 Console 接口和 Telnet 登录的用户。

1.5.2 通过 Console 口首次登录 AC6605

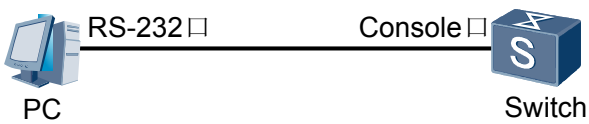
介绍如何通过 Console 口登录 AC6605。

建立登录任务

应用环境

用户需要通过 Console 口登录到 AC6605，如图 1-8 所示。图中，AC6605 用 Switch 表示。

图 1-8 通过 Console 口登录到 AC6605



说明

如果 AC6605 是首次上电，并且用户需要管理和配置 AC6605，则用户只能通过 Console 口登录到 AC6605。

版权所有 © 华为技术有限公司

前置任务

在通过 Console 口登录到 AC6605 前，需要完成以下任务：

- 正确连接 PC 机和 AC6605
- AC6605 正常启动

数据准备

无

通过 Console 口登录 AC6605

背景信息

在通过 Console 口搭建本地配置环境时，用户可以在 PC 上通过 Windows 系统中的“超级终端”与 AC6605 建立连接。

操作步骤

步骤 1 请在 PC 上启动超级终端

选择“开始 > 程序 > 附件 > 通讯 > 超级终端”菜单项，Windows 系统启动超级终端。

步骤 2 新建连接

如图 1-9 所示。在“名称”文本框中输入新建连接的名称；选择图标。然后单击“确定”按钮。

图 1-9 新建连接

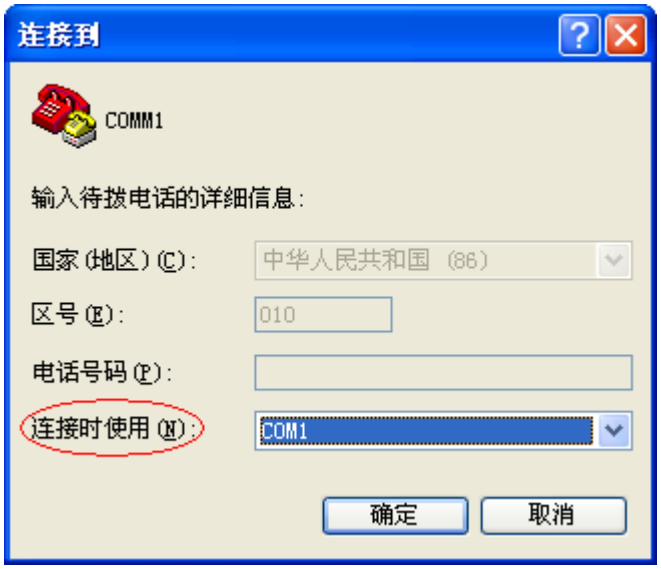


步骤 3 设置连接端口

进入如图 1-10 所示的 [连接到] 窗口后，请根据 PC（或配置终端）实际使用的端口在“连接时使用”下拉列表框中进行选择。然后单击“确定”按钮。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 1-10 连接端口设置



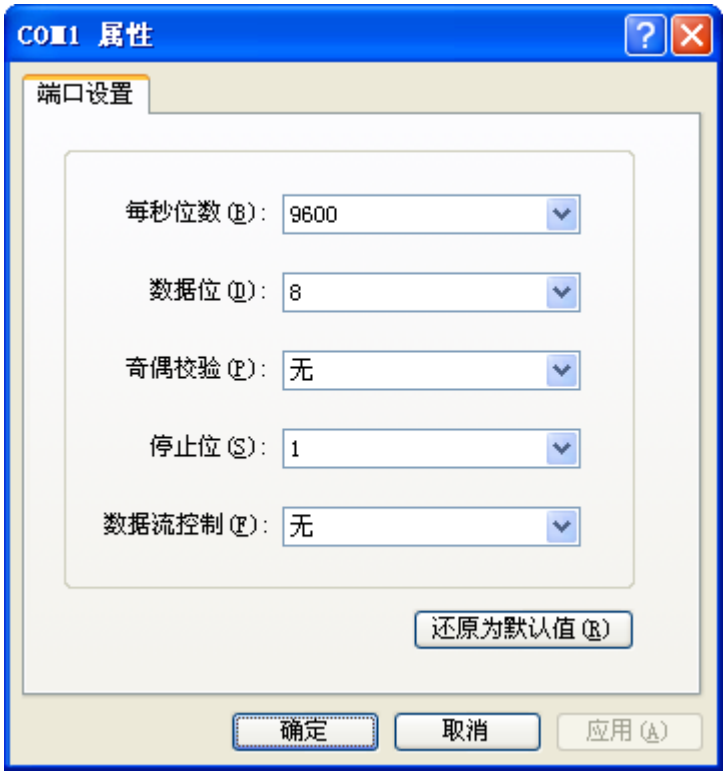
步骤 4 设置通信参数

进入如图 1-11 所示的 [端口属性] 窗口后，请按表 1-13 中的描述进行通信参数的设置。

说明

在其它的 Windows 操作系统中，“每秒位数”可能被描述为“波特率”；“数据流控制”可能被描述为“流量控制”。

图 1-11 端口通信参数设置



版权所有 © 华为技术有限公司

表 1-13 通信参数

参数	取值
每秒位数（波特率）	9600
数据位	8
奇偶校验	无
停止位	1
数据流控制（流量控制）	无

步骤 5 启动超级终端后，选择“文件 > 属性”菜单项，进入如图 1-12 所示的 [连接属性] 窗口。选择“设置”页签，在“终端仿真”下拉列表框中选择“自动检测”或“VT100”。单击“确定”按钮结束设置。

图 1-12 终端类型选择



按照以上 5 个步骤结束设置后，按下“Enter”键，屏幕出现<Quidway>提示符，表示登录到 AC6605。此时就可输入命令，配置或管理 AC6605。

----结束

版权所有 © 华为技术有限公司

1.5.3 配置 Console 用户界面

配置 Console 用户界面，实现在本地维护交换机。

建立配置任务

在进行 Console 用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要在本地维护交换机时，需要配置 Console 用户界面。

前置任务

在配置 Console 用户界面之前，需要完成以下任务：

- 交换机上电并启动正常
- PC 机与交换机通过异步接口连接正常

数据准备

在配置 Console 用户界面之前，需要准备以下数据。

序号	数据
1	传输速率、流控方式、校验方式、停止位、数据位
2	流控方式、终端屏幕的一屏长度、终端屏幕显示的列数、历史命令缓冲区大小
3	用户优先级
4	用户验证方式、用户名、口令

说明

以上数据交换机除用户名和口令外，其他均有缺省值，一般不需要单独配置。

配置 Console 接口属性

用户可以配置 Console 接口的传输速率、流控方式、校验位、停止位和数据位。

背景信息

请在用户端登录到的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **user-interface console** *interface-number*，进入 console 用户界面视图。

步骤 3 （可选）执行命令 **speed** *speed-value*，设置传输速率。

缺省情况下，传输速率为 9600bit/s。

步骤 4 （可选）执行命令 **flow-control** { **hardware** | **none** | **software** }，设置流控方式。

缺省情况下，流控方式为 None。

步骤 5 （可选）执行命令 **parity** { **even** | **mark** | **none** | **odd** | **space** }，设置校验位。

缺省情况下，校验位为 None。

步骤 6 （可选）执行命令 **stopbits** { **1.5** | **1** | **2** }，设置停止位。

缺省情况下，停止位为 1bit。

步骤 7 （可选）执行命令 **databits** { **5** | **6** | **7** | **8** }，设置数据位。

缺省情况下，数据位为 8。

说明

当用户通过 Console 接口登录交换机时，超级终端的上述属性要和交换机的接口属性保持一致，否则不能登录到交换机。

----结束

配置 Console 终端属性

用户可以配置 Console 接口的用户超时断连功能、终端屏幕的显示长度或宽度以及历史命令缓冲区大小。

背景信息

请在用户端登录的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface console** *interface-number* ，进入 console 用户界面视图。

步骤 3 执行命令 **shell**，启动终端服务。

步骤 4 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

缺省情况下，用户界面断连的超时时间为 10 分钟。

步骤 5 执行命令 **screen-length** *screen-length*，设置终端屏幕每屏显示的行数。

缺省情况下，终端屏幕显示的行数为 24 行。

执行命令 **screen-length** *screen-length* **temporary** 可以指定终端屏幕的临时显示行数。

步骤 6 执行命令 **screen-width** *screen-width*，设置当前终端屏幕显示的列数。

缺省情况下，终端屏幕显示的列数为 80 列。

步骤 7 执行命令 **history-command max-size** *size-value*，设置历史命令缓冲区大小。

版权所有 © 华为技术有限公司

缺省情况下，用户界面历史命令缓冲区大小为 10 条历史命令。

----结束

配置用户的优先级

用户可以配置通过 Console 接口登录的用户优先级。

背景信息

请在用户端登录的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface console** *interface-number*，进入 console 用户界面视图。

步骤 3 执行命令 **user privilege level** *level*，设置用户的优先级。

用户的优先级和命令的优先级是相对应的，即用户只能使用和自己级别相对应的命令。

命令优先级请参见命令级别。

----结束

配置用户验证方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

操作步骤

- 设置 AAA 本地验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **quit**，退出 Console 用户界面视图。
  5. 执行命令 **aaa**，进入 AAA 视图。
  6. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。
- 设置密码验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证。
  4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置 password 验证的口令。
- 设置不对用户验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。

版权所有 © 华为技术有限公司

3. 执行命令 **authentication-mode none**，设置用户验证方式为不验证。

----结束

检查配置结果

Console 用户界面配置成功后，可以查看到用户界面的使用信息、物理属性和配置、本地用户列表和在线用户等内容。

前提条件

已完成 Console 用户界面的所有配置。

操作步骤

- 使用 **display users** [**all**]命令显示用户界面的使用信息。
- 使用 **display user-interface console** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。
- 使用 **display local-user** 命令查看本地用户列表。
- 使用 **display access-user** 命令查看在线用户。

----结束

1.5.4 配置 VTY 用户界面

配置 VTY 用户界面，实现在远程维护交换机。

建立配置任务

在进行 VTY 用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要配置和管理 Telnet 或 SSH 登录交换机时，需要配置 VTY 用户界面。

前置任务

在配置 VTY 用户界面之前，需要完成以下任务：

- 交换机上电并启动正常
- PC 机与交换机连接正常

数据准备

在配置 VTY 用户界面之前，需要准备以下数据。

序号	数据
1	VTY 类型用户界面的最大个数
2	（可选）对 VTY 类型用户界面呼入呼出进行限制的 ACL 号

版权所有 © 华为技术有限公司

序号	数据
3	终端用户超时断开时间、终端屏幕的一屏长度、终端屏幕显示的列数和历史命令缓冲区大小
4	用户验证方式、用户名、口令

配置 VTY 用户界面的最大个数

用户可以配置同时登录到交换机的 VTY 类型用户界面的最大个数。

背景信息

请在用户端登录到的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface maximum-vty** *number*，配置可以同时登录到交换机的 VTY 类型用户界面的最大个数。

说明

当配置 VTY 用户界面最大个数为 0 时，任何用户（包括网管用户）都无法登录到交换机。

如果要配置的 VTY 用户接口的最大数小于当前的最大数量，则不需要其它配置。

如果要配置的 VTY 用户接口的最大数量大于当前的最大数量，就需要为新增加的用户接口配置验证方式和密码。因为对于新增用户接口系统默认为使用密码验证。

例如：当前允许最多 5 个 VTY 用户同时在线，现在配置为允许 15 个 VTY 用户同时在线，那么 VTY 用户接口 5 ～ 14 就需要使用 **authentication-mode** 和 **set authentication password** 命令配置验证方式和密码，配置如下：

```
<Quidway> system-view
[Quidway] user-interface maximum-vty 15
[Quidway] user-interface vty 5 14
[Quidway-ui-vty5-14] authentication-mode password
[Quidway-ui-vty5-14] set authentication password cipher huawei
```

----结束

（可选）配置呼入呼出限制

用户可以配置 VTY 类型用户界面的呼入呼出限制。

背景信息

请在用户端登录到的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **acl** *acl-number* { **inbound** | **outbound** }，配置 VTY 类型用户界面的呼入呼出限制。

当需要限制某个地址或地址段的用户登录到交换机时，使用 **inbound**；当需要限制已经登录的用户登录到其它交换机时，使用 **outbound**。

----结束

配置 VTY 终端属性

用户可以配置 VTY 接口的用户超时断连功能、终端屏幕的显示长度或宽度以及历史命令缓冲区的大小。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **shell**，启用 VTY 终端服务。

步骤 4 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

步骤 5 执行命令 **screen-length** *screen-length*，设置终端屏幕每屏显示的行数。

缺省情况下，终端屏幕显示的行数为 24 行。

执行命令 **screen-length** *screen-length* **temporary** 可以指定终端屏幕的临时显示行数。

步骤 6 执行命令 **screen-width** *screen-width*，设置当前终端屏幕显示的列数。

缺省情况下，终端屏幕显示的列数为 80 列。

步骤 7 执行命令 **history-command max-size** *size-value*，设置历史命令缓冲区的大小。

缺省情况下，用户界面历史命令缓冲区大小为 10 条历史命令。

----结束

配置用户验证方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

背景信息

交换机提供三种验证方式：

- AAA 验证：需要设置用户名和密码。
- 密码验证（password）：不需要设置用户名，但一定要设置密码，否则将只能通过 Console 口登录交换机。
- 不验证（none）：不需要设置用户名和密码，登录交换机时也不进行验证。

版权所有 © 华为技术有限公司

操作步骤

- 设置 AAA 验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **quit**，退出 VTY 用户界面视图。
  5. 执行命令 **aaa**，进入 AAA 视图。
  6. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。
- 设置密码验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证。
  4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置密码验证的口令。
- 设置不对用户验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode none**，设置用户验证方式为不验证。

----结束

检查配置结果

VTY 用户界面配置成功后，可以查看到用户界面的使用信息、VTY 类型用户界面的最大个数以及物理属性和配置等内容。

前提条件

已完成 VTY 用户界面的所有配置。

操作步骤

- 使用 **display users** [**all**]命令查看用户界面的使用信息。
- 使用 **display user-interface maximum-vty** 命令查看 VTY 类型用户界面的最大个数。
- 使用 **display user-interface** [[*ui-type*] *ui-number1* | *ui-number*] [**summary**]命令查看用户界面的物理属性和配置。

----结束

1.5.5 管理用户界面

配置用户管理，保证操作用户能够安全管理交换机。

建立配置环境

在进行管理用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

为了保证操作用户能够安全管理交换机，可以在用户界面间发送消息、清除指定用户等。

前置任务

在管理用户界面之前，需要完成以下任务：

- 交换机上电并正常启动
- PC 机与交换机连接正常

数据准备

在管理用户界面之前，需要准备以下数据。

序号	数据
1	用户界面类型和编号
2	要发送的消息内容

发送消息给其它用户界面

用户可以通过配置实现在用户界面间传递消息。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **send** { **all** | *ui-type ui-number* | *ui-number1* }，设置在用户界面间传递消息。

步骤 2 根据系统提示，输入要传递的消息。使用“Ctrl_Z”或回车键结束输入，使用“Ctrl_C”中止本次操作。

----结束

清除在线用户

用户可以通过配置实现清除指定的在线用户。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **free user-interface** { *ui-number* | *ui-type ui-number1* }，清除在线用户。

版权所有 © 华为技术有限公司

步骤 2 根据系统提示，确定是否清除指定的在线用户。

----结束

检查配置结果

管理用户界面配置成功后，可以查看用户界面的使用信息。

前提条件

已完成管理用户界面的所有配置。

操作步骤

- 使用 **display users [all]**命令显示用户界面的使用信息。

----结束

1.5.6 配置用户管理

配置用户管理，实现为交换机创建用户，并为用户设置口令，对用户进行管理。

建立配置任务

在进行用户管理的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当配置了主控板或接口板的 IP 地址后，任何远端用户均可使用 Telnet 登录到交换机，或与交换机建立 PPP 连接而访问网络，增加了不安全性。为防止这种现象，需要为交换机创建用户，并为用户设置口令，对用户进行管理。

前置任务

在配置用户之前，需要完成以下任务：

- 交换机上电并正常启动
- PC 机与交换机连接正常

数据准备

在配置用户之前，需要准备以下数据。

序号	数据
1	验证用户的方式
2	用户名和口令
3	用户优先级

版权所有 © 华为技术有限公司

配置验证用户的方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode** { **aaa** | **password** | **none** }，设置用户验证方式。

----结束

配置 Password 方式的口令

用户可以配置密码验证的口令，以及明文或密文的显示方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode password**，设置用户验证方式为 Password 验证。

步骤 4 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置密码验证的密文口令或明文口令。

说明

交换机默认的验证方式是密码验证。

----结束

配置 AAA 方式用户名和密码

用户可以配置 AAA 本地验证的口令，以及明文或密文的显示方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **aaa**，进入 AAA 视图。

步骤 6 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

配置登录不验证

用户可以配置登录交换机的方式为不验证方式。

背景信息

注意

设置登录方式为不验证，会引起交换机的安全问题。

请在用户端需要登录的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode none**，配置用户登录不验证。

说明

- 如果配置的验证方式为采用不验证或 password 验证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。
- 如果配置的验证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

----结束

配置用户的优先级

用户可以配置优先级。

背景信息

具体请参见《AC6605 无线接入控制器 配置指南-安全》。

检查配置结果

用户管理配置成功后，可以查看用户界面的使用信息、本地用户列表和在线用户等信息。

版权所有 © 华为技术有限公司

前提条件

已完成用户管理的所有配置。

操作步骤

- 使用 **display users [all]**命令显示用户界面的使用信息。
- 使用 **display local-user** 命令查看本地用户列表。
- 使用 **display access-user** 命令查看在线用户。

----结束

1.5.7 配置举例

配置用户通过不同方式登录交换机的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

注意

以下第一个和第二个配置举例执行完毕后，当前用户 VTY0，不能对设备进行优先级为 2 以上的配置命令的操作，请确认可以通过其他方式登录交换机并删除配置。

配置用户通过 Password 方式登录交换机示例

配置通过 Password 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、验证方式和断开连接的时间，实现使用 Password 方式登录交换机。

组网需求

PC 机的 COM 口与交换机的 Console 口相连。

配置 VTY0 的优先级为 2，对从 VTY0 登录的用户进行 password 验证，用户登录时需要输入口令“huawei”。

登录后，如果用户超过 30 分钟未对交换机进行操作，将断开与交换机的连接。

配置思路

采用如下的思路配置登录交换机：

1. 进入用户接口视图，配置 VTY0 的优先级为 2。
2. 配置明文验证和断开连接的时间。

数据准备

为完成此配置例，需准备如下的数据：

- 验证方式密码
- 断开连接的时间

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 VTY0 的优先级为 2。

```
<Quidway> system-view
[Quidway] user-interface vty0
[Quidway-ui-vty0] user privilege level 2
```

步骤 2 配置明文验证和断开连接的时间。

```
[Quidway-ui-vty0] authentication-mode password
[Quidway-ui-vty0] set authentication password simple huawei
[Quidway-ui-vty0] idle-timeout 30
```

----结束

配置文件

```
#
 sysname Quidway
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
#
user-interface vty 0
 user privilege level 2
 set authentication password simple huawei
 idle-timeout 30
#
return
```

配置用户通过 AAA 方式登录交换机示例

配置通过 AAA 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、断开连接的时间以及打开本地用户的闲置切断开关等操作，实现使用 AAA 方式登录交换机。

组网需求

PC 机的 COM 口与交换机的 Console 口相连。

配置 VTY0 的优先级为 2，对从 VTY0 登录的用户进行 AAA 验证，用户登录时需要输入用户名“huawei”，密码“huawei”。

登录后，如果用户超过 30 分钟未对交换机进行操作，将断开与交换机的连接。

配置思路

采用如下的思路配置登录交换机：

1. 进入用户接口视图，配置 VTY0 的优先级为 2 和断开连接的时间。
2. 进入 AAA 视图，配置用户名、密码和用户等级。
3. 在 AAA 视图下打开本地用户的闲置切断开关。

数据准备

为完成此配置例，需准备如下的数据：

- 验证时需要的用户名和密码

版权所有 © 华为技术有限公司

- 断开连接的时间

操作步骤

步骤 1 交换机上配置 VTY0 的优先级为 2，验证方式为 aaa，断开连接时间为 30 分钟。

```
<Quidway> system-view
[Quidway] user-interface vty0
[Quidway-ui-vty0] user privilege level 2
[Quidway-ui-vty0] authentication-mode aaa
[Quidway-ui-vty0] idle-timeout 30
[Quidway-ui-vty0] quit
```

步骤 2 配置用户名、密码和用户等级。

```
[Quidway] aaa
[Quidway-aaa] local-user huawei password cipher huawei
[Quidway-aaa] local-user huawei privilege level 2
```

----结束

配置文件

```
#
 sysname Quidway
#
aaa
local-user huawei password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user huawei privilege level 2
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
#
user-interface vty 0
 authentication-mode aaa
 user privilege level 2
 idle-timeout 30
#
return
```

1.6 管理文件系统

介绍了文件系统的基础知识，主要包括管理文件、管理目录和管理存储设备的方法。

1.6.1 文件系统简介

简单介绍文件系统的概念。

基本概念

文件系统包括对存储设备中的文件、目录的管理，包括创建文件系统，创建、删除、修改、更名文件和目录，以及显示文件的内容。

文件系统实现两类功能：管理存储设备、管理保存在存储设备中的文件。

存储设备

存储设备是指用于存储数据的硬件。

版权所有 © 华为技术有限公司

AC6605 目前支持的存储设备为 Flash Memory。

文件

文件是系统存储信息，并对信息进行管理的一种机制。

目录

目录是一种将整个文件集合进行组织的机制，目录是文件逻辑上的容器。

1.6.2 管理存储设备

介绍格式化存储设备的方法。

建立配置任务

需要清空 AC6605 的信息时，可以对存储设备进行格式化。

前置任务

在配置管理存储设备之前，需要完成以下任务：

- AC6605 安装完毕并加电启动正常
- 客户端可以登录到 AC6605 上

数据准备

在配置管理存储设备之前，需要准备以下数据。

序号	数据
1	设备的名称

修复文件系统异常的存储设备

当某存储设备上的文件系统出现异常时，交换机的终端会给出提示信息，建议修复。

背景信息

请在交换机上执行如下的配置。

操作步骤

步骤 1 执行命令 **fixdisk** *device-name*，修复文件系统异常的存储设备。

说明

执行此命令后，如果仍然收到系统建议修复的信息，则表示物理介质可能已经损坏。

----结束

版权所有 © 华为技术有限公司

（可选）格式化存储设备

格式化会清空存储器中的所有文件和目录。

背景信息



注意

执行 **format flash:**命令后，AC6605 会清空 Flash 存储器中的所有文件和目录，并且不可恢复，请谨慎使用此命令！

操作步骤

步骤 1 在用户视图下执行 **format flash:**命令，格式化存储设备。

----结束

1.6.3 管理目录

可以通过管理目录在逻辑上将文件分级存放。

建立配置任务

在管理目录之前，完成前置任务和数据准备，有助于快速、准确地完成各项属性的配置任务。

应用环境

当需要在客户端与服务器端进行文件传输时，需要使用文件系统对目录进行配置。

前置任务

在配置文件系统的基本功能之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 已正确连接客户端与服务器端

数据准备

在配置管理目录的基本功能之前，需要准备以下数据。

序号	数据
1	需要创建的目录名
2	需要删除的目录名

版权所有 © 华为技术有限公司

查看当前的工作目录

当需要了解当前所在的目录节点信息时，可以进行查看当前工作目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **pwd**，屏幕上显示当前所处的目录。

----结束

改变当前目录

当需要变更到别的目录节点时，可以进行改变当前目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前所处的目录。

步骤 2 执行命令 **pwd**，查看当前所处的目录。

----结束

显示目录或文件信息

当需要查看某一目录及该目录下的文件时，可以进行显示目录或文件信息的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，进入想要显示的文件所在的目录。

步骤 2 执行命令 **dir** [/**all**] [*filename* | **flash:**]，显示目录中的文件和子目录的列表。

所有路径都支持绝对路径或相对于当前工作路径的相对路径。

----结束

创建目录

当希望新建一个目录时，可以进行创建目录的操作，在指定存储设备的指定目录下创建目录。

版权所有 © 华为技术有限公司

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到所要创建目录的父目录。

步骤 2 执行命令 **mkdir** *directory*，创建目录。

----结束

删除目录

当需要舍弃某一目录时，可以进行删除目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到所要删除目录的父目录。

步骤 2 执行命令 **rmdir** *directory*，删除目录。

----结束

1.6.4 管理文件

可以通过管理文件，对其进行查看、删除、重命名等操作。

建立配置任务

在管理文件之前，完成前置任务和数据准备，有助于快速、准确地完成各项属性的配置任务。

应用环境

如需要查看、删除、重命名交换机上的文件时，需要使用文件系统对文件进行配置。

前置任务

在配置文件系统之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 已正确连接客户端与服务器端

数据准备

在配置文件系统之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	需要查看的文件名
2	需要删除的文件名
3	需要重命名的文件名

显示文件的内容

当需要查看文件内容时，可以进行显示文件内容的操作，系统将以文本形式显示。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **more** *filename*，显示文件的内容。

----结束

拷贝文件

当需要复制某一文件时，可以进行拷贝文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **copy** *source-filename destination-filename*，拷贝文件。

----结束

移动文件

当需要将文件转移存放路径时，可以进行移动文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **move** *source-filename destination-filename*，移动文件。

----结束

版权所有 © 华为技术有限公司

重新命名文件

当需要修改某一文件名称时，可以进行重新命名文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **rename** *source-filename destination-filename*，重新命名文件。

----结束

压缩文件

当需要减小某一文件大小时，可以进行压缩文件的操作。

操作步骤

步骤 1 执行命令 **zip** *source-filename destination-filename*，压缩文件。

----结束

删除文件

当需要丢弃某一文件时，可以进行删除文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **delete** [**/unreserved**] *filename*，删除文件。

----结束

彻底删除回收站中的文件

当需要永久删除某一已丢弃的文件时，可以进行彻底删除回收站中的文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **reset recycle-bin** [*filename*]，删除文件。

----结束

版权所有 © 华为技术有限公司

恢复删除文件

当需要还原某一已丢弃的文件时，可以进行恢复删除文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **undelete** *filename*，恢复删除的文件。

说明

- 如果当前目录不是根目录，对文件的操作要使用绝对路径。
- 对于执行删除命令行时使用参数[**/unreserved**]后的文件不可恢复。

----结束

运行批处理文件

当需要对文件一次进行多项处理时，可以进行运行批处理文件的操作。

前提条件

在客户端编辑的批处理文件，已经上传到交换机。

背景信息

如果已经建立好批处理文件，那么可以执行该文件，以实现执行固定任务的自动化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **execute** *filename*，运行批处理文件。

----结束

配置文件系统提示方式

当在设备上进行操作时，系统可以给予提示或警示信息。如果需要修改系统对文件操作的提醒方式时，可以进行配置文件系统提示方式的操作。

前提条件

在配置文件系统之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 客户端可以登录到交换机上

背景信息

在操作文件时，如可能导致数据丢失或破坏，则需配置系统给出提示信息。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行 **system-view** 命令，进入到系统视图。

步骤 2 执行 **file prompt** { **alert** | **quiet** }命令，配置文件系统提示方式。

缺省情况下，提示方式为 **alert**。

注意

如果将文件操作的提醒方式设置为 quiet，则对由于用户误操作（比如删除文件操作）而导致数据丢失的情况不作提示，请慎用。

----结束

1.7 管理配置文件

管理配置文件包括当前配置和配置文件，以及主备配置一致性检测和恢复。

1.7.1 管理配置文件简介

配置文件是本次或下次启动交换机时加载的配置项。

配置文件

配置文件的基本概念。

配置文件是本次或下次启动交换机时加载的配置项。

配置文件为一文本文件，其格式如下：

- V200R001 版本的配置文件必须以类似“!Software Version V200R001C00SPC001”的版本信息开头。
- 以命令格式保存。
- 为了节省空间，只保存非缺省的参数（各配置参数的缺省值请详见以后各章节）。
- 命令的组织以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以#开始的为注释行）。空行或注释行可以是一行或多行。
- 节的顺序安排通常为：全局配置、逻辑接口配置、物理接口配置、路由协议配置等。

说明

- 系统可正确执行的命令长度最大为 512 个字符，包括使用不完整格式的情况。
- 如果使用不完整格式进行配置，由于命令保存到配置文件中时使用的是完整格式，可能导致配置文件中存在长度超过 512 个字符的命令。系统重启时，这类命令将无法恢复。

配置文件和当前配置

配置文件和当前配置的基本概念。

版权所有 © 华为技术有限公司

- 起始配置：交换机上电时，从默认存储路径中读取配置文件进行交换机的初始化工作，因此该配置文件中的配置称为起始配置，如果默认存储路径中没有配置文件，则交换机用缺省参数初始化。
- 当前配置：与起始配置相对应，交换机运行过程中正在生效的配置称为当前配置。
- 用户通过命令行接口可以修改交换机当前配置，为了使当前配置能够作为交换机下次上电时的起始配置，需要用 **save** 命令保存当前配置到默认存储设备中，形成配置文件。

1.7.2 管理配置文件

管理配置文件，保证交换机正常启动。

建立配置任务

在进行管理配置文件的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

如下情况下，用户会进行管理配置文件的操作。

- 为了让交换机正常启动，用户需要正确选择交换机在启动时加载的 AC6605 系统软件和配置文件。
- 用户在修改当前配置后，需要保存修改的内容。
- 用户需要查看交换机的配置信息。

前置任务

在对配置文件进行管理之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常

数据准备

管理配置文件之前，需准备以下数据。

序号	数据
1	AC6605 系统软件及其文件名
2	配置文件及其文件名
3	配置文件比较的开始行数

配置交换机下次启动时加载的系统软件

用户在需要升级设备的系统软件等情况时，可以指定交换机下次启动时加载的系统软件。

版权所有 © 华为技术有限公司

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *system-file* [**slave-board**]，配置交换机下次启动时加载的 AC6605 系统软件。

系统软件的文件名必须以“.cc”作为扩展名，而且必须存放在 Flash 的根目录下。

指定 AC6605 下次启动加载的系统文件时，如果待升级的软件对应的 BOOTROM 版本和当前设备 BOOTROM 版本不一致，设备会自动提醒升级设备 BOOTROM。

----结束

配置交换机下次启动时加载的配置文件

用户在重启设备之前，可以指定交换机下次启动时加载的配置文件。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行 **startup saved-configuration** *configuration-file* 命令，配置交换机下次启动时加载的配置文件。

配置文件的文件名必须以.cfg 或.zip 作为扩展名，而且必须存放在存储设备的根目录下。

交换机上电时，默认从 Flash 存储器中读取配置文件进行初始化，因此该配置文件中的配置称为初始配置。如果 Flash 中尚没有配置文件，则交换机用缺省参数初始化。

与初始配置相对应，交换机运行过程中正在生效的配置称为当前配置。

----结束

保存配置文件

为了降低由于交换机掉电或者意外重启导致配置信息的丢失，系统提供实时保存配置的功能。

操作步骤

- 执行命令 **save** [**all**] [*configuration-file*]，保存当前配置。

  配置文件必须以“.cfg”或“.zip”作为扩展名，而且系统启动配置文件必须存放在存储设备的根目录下。

  用户通过命令行接口可以修改交换机的当前配置，为了使当前配置能够作为交换机下次上电时的初始配置，需要用 **save** 命令保存当前配置到 Flash 存储器中，形成配置文件。

  执行命令 **save all**，将会保存当前所有的配置，包括不在位的板卡的配置，至系统默认的存储路径中。

版权所有 © 华为技术有限公司

说明

在第一次保存配置文件时，如果不指定可选参数 *configuration-file*，则交换机将提示是否将文件名保存为“vrpcfg.zip”。

----结束

清除配置文件的内容

用户可以清除当前设备上加载的配置文件的内容。

背景信息

在以下两种情况下，需要擦除 Flash 存储器中的配置文件：

- 在交换机软件升级之后，软件和配置文件不匹配。
- 发现配置文件遭到破坏，或加载了错误的配置文件。

操作步骤

- 清除当前加载的配置文件的内容

  在用户视图下，执行命令 **reset saved-configuration**，清除当前加载的配置文件的内容。

  - 如果交换机当前启动与下次启动的配置文件一致，执行该命令将同时清除这两个配置文件。交换机下次启动采用缺省配置文件。
  - 如果交换机当前启动与下次启动的配置文件不一致，执行该命令将清除当前启动的配置文件。
  - 如果交换机当前启动的配置文件为空，执行该命令后，系统将提示配置文件不存在。

  配置文件被清除后，如果不使用 **startup saved-configuration** *configuration-file* 命令重新指定含有正确配置信息的配置文件，或者不使用 **save** 命令保存配置文件，则交换机下次启动时，将采用缺省的配置参数进行初始化。

----结束

比较配置文件

用户可以比较当前配置和初始配置。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **compare configuration** [*configuration-file*] [*current-line-number save-line-number*]，比较当前的配置与下次启动的配置文件内容是否一致。

如果不输入参数，表示从配置文件的首行开始进行比较。*current-line-number* 和 *save-line-number* 这两个参数用来在发现配置文件不同之处后，跳过该不同处继续进行比较。

系统在比较出不同之处时，将从不同的行开始，分别对当前配置文件和保存的配置文件，显示一定数量字符的文件内容（默认显示 150 个字符），如果该不同之处到文件末尾不足 150 个字符，将显示到文件尾为止。

版权所有 © 华为技术有限公司

比较当前配置和下次配置文件时，如果下次配置文件为空，或者下次启动的配置文件存在，但是内容为空，系统将提示读文件失败。

----结束

检查配置结果

管理配置文件配置成功后，可以查看到当前配置文件、交换机下次启动时加载的配置文件的内容、设备启动时使用的文件信息和存储设备中的文件信息等内容。

前提条件

已完成管理配置文件的所有配置

操作步骤

- 使用 **display current-configuration** 命令查看当前配置文件。
- 使用 **display saved-configuration** [**last**]命令配置交换机下次启动时加载的配置文件的内容。
- 使用 **display startup** 命令查看设备启动时使用的文件信息。
- 使用 **dir** [/**all**] [*filename*]命令查看存储设备中的文件信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 交换机的当前配置信息正确，无多余配置。
- 交换机的当前配置信息已经被保存在存储设备中。
- 交换机下次启动时加载的 AC6605 系统软件和配置文件正确，且已经保存在存储设备的根目录中。

1.8 FTP 和 TFTP

FTP 和 TFTP 是常用的文件传输协议。

1.8.1 FTP 和 TFTP 简介

介绍 FTP 和 TFTP 的基本概念。

FTP

FTP 向用户提供本地和远程主机之间的文件传输，尤其在进行版本升级、日志下载、文件传输和配置保存等业务操作中广泛应用。

FTP（File Transfer Protocol）在 TCP/IP 协议族中属于应用层协议，主要向用户提供本地与远程主机之间的文件传输。FTP 协议基于相应的文件系统实现。

系统提供的 FTP 服务包括：

版权所有 © 华为技术有限公司

- FTP Server：用户可以运行 FTP 客户端程序登录到交换机，访问交换机上的文件。
- FTP Client：用户在 PC 上通过终端仿真程序或 Telnet 程序建立与交换机的连接后，可以输入 FTP 命令建立与远程 FTP Server 的连接并访问远程主机上的文件。

TFTP

TFTP 不具有复杂的交互存取接口和认证控制，适用于客户端和服务器之间不需要复杂交互的环境。

TFTP（Trivial File Transfer Protocol）是一种简单文件传输协议。

与 FTP 相比，TFTP 不具有复杂的交互存取接口和认证控制，适用于客户机和服务器之间不需要复杂交互的环境。例如，系统启动时使用 TFTP 获取系统内存映像。

TFTP 协议在 UDP 基础上实现。

TFTP 协议传输由客户端发起。当需要下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据包，并向服务器发送确认；当需要上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据包，并接收服务器的确认。

TFTP 传输文件有两种模式：

- 二进制模式：用于传输程序文件
- ASCII 码模式：用于传输文本文件

目前，AC6605 只能作为 TFTP 客户端，且只能使用二进制模式传输文件。

1.8.2 配置交换机作为 FTP 服务器

配置 FTP 服务器的基本功能。

建立配置任务

在进行交换机作为 FTP 服务器的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

把交换机作为 FTP 服务器。客户端通过 FTP 登录到交换机以后，可以在客户端与服务器端之间实现远程传输文件。

前置任务

在配置交换机作为 FTP 服务器之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 客户端与交换机路由可达

数据准备

如果配置交换机作为 FTP 服务器，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	（可选）FTP 服务器指定监听端口号
2	（可选）FTP 服务器的超时断开连接时间
3	FTP 用户名和口令
4	FTP 用户的授权工作目录

（可选）指定 FTP 服务器端口号

用户可以配置或变更 FTP 服务器监听端口号。变更后，只有用户知道 FTP 服务使用的当前端口号，确保安全性。

背景信息

FTP 服务未使能情况下，可以按照用户指定端口进行 FTP 端口变更。

如果变更端口前 FTP 服务已经启动，需执行 **undo ftp server** 命令关闭 FTP 服务，再进行端口变更。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp** [**ipv6**] **server port** *port-number*，变更 FTP 服务器端口。

如果配置了新的监听端口号，FTP 服务器端先断开当前已经建立的所有 FTP 连接，然后使用新的端口号开始监听。缺省情况下，FTP 服务器端监听端口号是 21。

----结束

使能 FTP 服务器

缺省情况下 FTP 服务器功能关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp** [**ipv6**] **server enable**，启动 FTP 服务器。

说明

当客户端与交换机之间的文件操作结束后，请执行 **undo ftp** [**ipv6**] **server** 命令，及时关闭 FTP 服务器功能，从而保证交换机的安全。

----结束

版权所有 © 华为技术有限公司

（可选）配置 FTP 服务器超时断开连接的时间

用户可以配置 FTP 连接空闲时间，长时间没有操作的时候释放 FTP 连接资源。

背景信息

在设定的时间内，FTP 连接始终处于空闲状态时，系统将自动断开 FTP 连接。

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp** [**ipv6**] **timeout** *minutes*，配置 FTP 服务器超时断连时间。

缺省情况下，系统的连接空闲时间为 30 分钟。

----结束

配置本地用户名和口令

用户可以配置 FTP 用户的验证信息，保证安全性，无权限的用户将不能操作设备。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

配置服务类型及授权信息

用户可以配置 FTP 用户的授权方式和授权目录，保证安全性，无权限的用户将不能访问受限目录。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2（可选）执行命令 **set default ftp-directory** *directory*，配置 FTP 用户的缺省工作目录。

步骤 3 执行命令 **aaa**，进入 AAA 视图。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **local-user** *user-name* **service-type ftp**，配置 FTP 服务类型。

步骤 5 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的授权目录。

----结束

检查配置结果

交换机作为 FTP 服务器配置成功后，可以查看到 FTP 服务器的配置和状态信息、登录的 FTP 用户信息等内容。

前提条件

已完成交换机作为 FTP 服务器的所有配置。

操作步骤

- 使用 **display [ipv6] ftp-server** 命令查看 FTP 服务器的配置和状态信息。
- 使用 **display ftp-users** 命令查看登录的 FTP 用户信息。

----结束

任务示例

执行命令 **display [ipv6] ftp-server**，可以看到当前 FTP 服务器的各项参数。

```
<Quidway> display ftp-server
  FTP server is running
  Max user number                 5
  User count                      0
  Timeout value(in minute)        30
  Listening port                  21
  Acl number                      0
```

执行命令 **display ftp-users**，可以看到当前配置的 FTP 用户的用户名、端口号、授权目录等信息。

```
<Quidway> display ftp-users
  username  host                                    port  idle  topdir
  zll       100.2.150.226                           1383  3     flash:
```

1.8.3 配置 FTP 访问控制列表

配置 FTP 访问控制列表，实现只允许指定的客户端登录到交换机。

建立配置任务

在进行 FTP 访问控制列表的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当交换机作为 FTP 服务器时，为提高安全性，可以通过配置 ACL 实现只允许满足匹配条件的客户端访问服务器。

版权所有 © 华为技术有限公司

前置任务

在配置 FTP 访问控制列表之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常。
- 客户端和作为 FTP 服务器的交换机路由可达。

数据准备

在配置 FTP 访问控制列表之前，需要准备以下数据。

序号	数据
1	访问控制列表号

使能 FTP 服务器

FTP 服务器缺省情况下关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp** [**ipv6**] **server enable**，启动 FTP 服务器。

----结束

配置基本访问控制列表

用户可以配置 ACL 规则。使用源地址信息，作为定义 ACL 规则的信息。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，进入 ACL 视图。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *，配置 ACL 规则。

说明

FTP 只支持基本访问控制列表。

----结束

版权所有 © 华为技术有限公司

配置 FTP 基本访问控制列表

用户可以配置 FTP 基本访问控制列表。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp** [**ipv6**] **acl** *acl-number*，配置 FTP 基本访问控制列表。

----结束

检查配置结果

FTP 访问控制列表配置成功后，可以查看到 FTP 服务器的配置和状态信息、登录的 FTP 用户信息等内容。

前提条件

已完成 FTP 访问控制列表的所有配置

操作步骤

- 使用 **display** [**ipv6**] **ftp-server** 命令查看 FTP 服务器的配置和状态信息。

----结束

任务示例

配置 FTP 服务器完毕，执行命令 **display** [**ipv6**] **ftp-server**，可以看到 FTP 基本访问控制列表号是 2345。

```
<Quidway> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening Port               1080
  Acl number                   2345
```

1.8.4 配置交换机作为 FTP 客户端

配置交换机作为 FTP 客户端，登录 FTP 服务器。

建立配置任务

在进行交换机作为 FTP 客户端的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

可以配置交换机作为 FTP 客户端，然后从交换机登录到 FTP 服务器，执行诸如传输文件、管理服务器目录等操作。

前置任务

在配置交换机作为 FTP 客户端之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机与服务器路由可达

数据准备

如果配置交换机作为 FTP 客户端，需要准备以下数据：

序号	数据
1	FTP 服务器的主机名或 IP 地址
2	建立 FTP 连接使用的端口号
3	FTP 协议命令
4	本地的文件名和远程 FTP 服务器上的文件名
5	远程 FTP 服务器上的工作路径名、FTP 客户端的本地工作路径或远程 FTP 服务器目录名
6	登录时需要的用户名及密码

登录 FTP 服务器

用户视图和 FTP 视图下，用户均可以登录 FTP 服务器。

背景信息

请在作为客户端的交换机上进行如下的配置。

在不同的视图下，与 FTP 服务器建立连接的方式也不同。

操作步骤

- 根据服务器端 IP 地址类型不同，进行如下操作。
  - 服务器端是 IPv4 地址。
    - 用户视图下，建立与 FTP 服务器的连接。

      执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
    - FTP 视图下，建立与 FTP 服务器的连接。

      1. 执行命令 **ftp**，进入 FTP 视图。

版权所有 © 华为技术有限公司

2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。

说明

在登录 FTP 服务器之前，可以执行命令 **set net-manager vpn-instance**，设置默认的 VPN 实例。执行该命令后，进行 FTP 操作时所使用的 VPN 实例即用户配置的默认 VPN 实例。

- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

----结束

配置文件传输方式

用户可以配置传输的文件的数据类型和文件传输方式。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **ascii** 或 **binary**，配置传输的文件的数据类型为 ASCII 码或者二进制。

FTP 支持 ASCII 码、二进制文件类型。二者的区别是：

- ASCII 传输使用 ASCII 字符，把回车键和换行符分开。
- 二进制不用转换或格式化就可传字符。

FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。客户端可使用模式切换命令进行切换（ASCII 和 Binary）。传输文本文件使用 ASCII 方式，传输二进制文件使用 Binary 方式。

步骤 2 执行命令 **passive**，配置文件传输方式为被动方式。

步骤 3 执行命令 **verbose**，打开 verbose 开关。

打开 verbose 开关，将显示所有 FTP 响应，在文件传送完成后，将同时显示与传送效率有关的统计信息。

----结束

查看 FTP 命令的在线帮助

用户可以在 FTP 客户端视图下查看 FTP 命令的在线帮助。

背景信息

请在作为客户端的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 FTP 客户端视图执行命令 **remotehelp** [*command*]，查看 FTP 命令的在线帮助。

----结束

上传、下载文件

用户可以将本地的文件上传到远程 FTP 服务器，也可以从 FTP 服务器下载文件并保存在本地。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 上传或者下载文件。

- 在 FTP 客户端视图执行命令 **put** *local-filename* [*remote-filename*]，将本地的文件上传到远程 FTP 服务器。
- 在 FTP 客户端视图执行命令 **get** *remote-filename* [*local-filename*]，从 FTP 服务器下载文件并保存在本地。

----结束

管理目录

用户可以在 FTP 服务器上进行创建、删除目录等管理操作。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 在 FTP 客户端视图进行如下一种或多种操作来管理目录。

- 执行命令 **cd** *pathname*，改变远程 FTP 服务器上的工作路径。
- 执行命令 **cdup**，改变 FTP 服务器端的工作路径到上一级目录。
- 执行命令 **pwd**，显示 FTP 服务器端工作路径。
- 执行命令 **lcd** [*local-directory*]，显示或者改变 FTP 客户端的工作路径。
- 执行命令 **mkdir** *remote-directory*，在 FTP 服务器上创建目录。
- 执行命令 **rmdir** *remote-directory*，在 FTP 服务器上删除目录。

说明

- 创建的目录可以为字母和数字等的组合，但不可以为<、>、?、\、：等特殊字符。
- 如果执行命令 **mkdir /abc**，则是在根目录下创建一个名为“abc”的子目录。

----结束

版权所有 © 华为技术有限公司

管理文件

用户可以显示 FTP 服务器上指定远程目录或文件的信息，或者删除 FTP 服务器上的指定文件。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 在 FTP 客户端视图进行如下一种或多种操作来管理文件。

- 执行命令 **ls** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的信息。

  如果指定远程文件时没有指定路径名称，那么系统将在工作目录下搜索指定的文件。
- 执行命令 **dir** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的详细信息。

  如果指定远程文件时没有指定路径名称，那么系统将在工作目录下搜索指定的文件。
- 执行命令 **delete** *remote-filename*，删除 FTP 服务器上指定文件。

  如果指定远程文件时没有指定路径名称，那么系统将在工作目录下搜索指定的文件。

当指定 *local-filename* 时，可以把显示的文件的相关信息下载到本地。

----结束

更改登录用户

用户可以更改当前的登录用户，重新进行登录 FTP 服务器。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 在 FTP 客户端视图执行命令 **user** *user-name* [*password*]，更改当前的登录用户，重新进行登录。

更改当前的登录用户后，原用户的连接将断开。

----结束

断开 FTP 连接

用户可以终止与服务器的连接，并退回到用户视图或 FTP 视图。

背景信息

请在作为客户端的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 根据不同配置需要，选择执行如下操作。

- 退回到用户视图。

  执行命令 **bye** 或 **quit**，终止与服务器的连接，并退回到用户视图。

- 退回到 FTP 视图。

  执行命令 **close** 或 **disconnect**，终止与服务器的连接，并退回到 FTP 视图。

说明

上述配置步骤只能在 FTP 客户端视图下执行。

----结束

1.8.5 配置交换机作为 TFTP 客户端

配置交换机作为 TFTP 客户端，登录 TFTP 服务器。

建立配置任务

在进行 TFTP 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要在服务器端与客户端传送文件且不需要复杂的交互环境时，可以使用 TFTP 协议。

前置任务

在配置 TFTP 之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机和 TFTP 服务器路由可达

数据准备

在配置 TFTP 之前，需要准备以下数据。

序号	数据
1	TFTP 服务器 IP 地址
2	TFTP 服务器中特定文件的文件名
3	文件所在的目录

（可选）配置 TFTP 客户端源地址

用户可以配置 TFTP 客户端的源地址信息，从指定的客户端源地址和路由建立 TFTP 连接，保证安全性。

版权所有 © 华为技术有限公司

背景信息

请在作为 TFTP 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 TFTP 客户端的源地址信息。

配置了 TFTP 客户端源地址信息后，在服务器端显示的 TFTP 客户端的源地址信息与该步骤中配置的一致。

----结束

使用 TFTP 下载文件

用户可以在 TFTP 客户端下载服务器上的文件。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 根据服务器端 IP 地址类型不同，进行如下操作。

- 服务器端是 IPv4 地址，执行命令 **tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **get** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。
- 服务器端是 IPv6 地址，执行命令 **tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-i** *interface-type interface-number*] **get** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。

----结束

使用 TFTP 上传文件

用户可以在 TFTP 客户端上传文件至服务器。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 根据服务器端 IP 地址类型不同，进行如下操作。

- 服务器端是 IPv4 地址，执行命令 **tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **put** *source-filename* [*destination-filename*]，使用 TFTP 上传文件。

版权所有 © 华为技术有限公司

- 服务器端是 IPv6 地址，执行命令 **tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-i** *interface-type interface-number*] **put** *source-filename* [*destination-filename*]，使用 TFTP 上传文件。

----结束

1.8.6 限制对 TFTP 服务器的访问

配置限制客户端登录 TFTP 交换机，实现允许本设备以 TFTP 方式登录到哪些 TFTP 服务器。

建立配置任务

在进行限制对 TFTP 服务器的访问配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

交换机作为 TFTP 客户端时，可以在交换机上配置访问控制列表，控制允许本设备以 TFTP 方式登录到哪些 TFTP 服务器。

前置任务

在配置限制对 TFTP 服务器的访问之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机和 TFTP 服务器路由可达

数据准备

在配置限制对 TFTP 服务器的访问之前，需要准备以下数据。

序号	数据
1	TFTP 服务器 IP 地址
2	访问控制列表号

配置基本访问控制列表

用户可以配置 ACL 规则。

背景信息

说明

TFTP 只支持基本访问控制列表。

请在作为 TFTP 客户端的设备进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，进入 ACL 视图。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *，配置 ACL 规则。

----结束

配置 TFTP 基本访问控制列表

用户可以配置 TFTP 基本访问控制列表。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 TFTP 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **tftp-server acl** *acl-number*，使用访问控制列表限制本设备端对 TFTP 服务器的访问。

- 如果是 IPv6 类型的地址

  执行命令 **tftp-server ipv6 acl** *acl6-number*，使用访问控制列表限制本设备端对 TFTP 服务器的访问。

----结束

1.8.7 配置举例

通过示例介绍 FTP 和 TFTP 的常见应用。

配置 FTP 服务器端示例

在本示例中，通过使用正确的用户名和密码以 FTP 方式登录到 FTP 服务器，实现下载文件到交换机的存储器。

组网需求

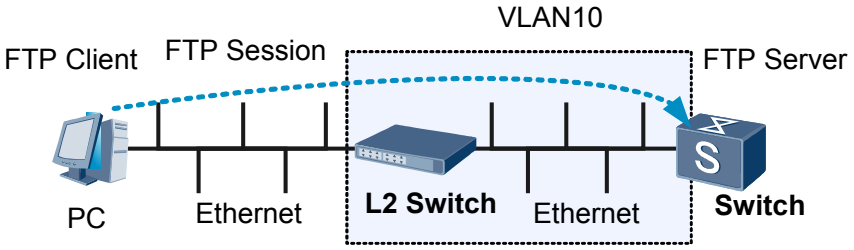
如图 1-13 所示。本端 PC 作为 FTP 客户端，IP 地址为 10.1.1.1/24。

Switch 作为 FTP Server。在 Switch 上配置 VLAN 10，将端口 GigabitEthernet0/0/1 加入 VLAN 10。配置 VLAN 10 的接口 IP 地址为 10.1.1.2/24。

PC 向 Switch 上传文件。

版权所有 © 华为技术有限公司

图 1-13 Switch 作为 FTP 服务器的组网图



Switch	接口	对应的 VLANIF	IP 地址
FTP Server	GigabitEthernet0/0/1	VLANIF 10	10.1.1.2/24

配置思路

采用如下的思路配置 FTP 服务器功能：

1. 在 FTP 服务器端 Switch 上建立正确的 FTP 用户名和密码。
2. PC 以 FTP 方式登录到 Switch 上。
3. 上传文件到 FTP 服务器端。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器端的 IP 地址。
- 在服务器端设置 FTP 用户名为 u1，密码为 ftppwd。
- 源文件在 PC 上正确的路径。
- 目标文件名和在 Switch 存放的位置。

操作步骤

步骤 1 在 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.1.1.2/24

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.2 24
```

步骤 2 在 Switch 上启动 FTP 服务，并配置 FTP 用户名 u1，口令 ftppwd

```
[Quidway] ftp server enable
[Quidway] aaa
[Quidway-aaa] local-user u1 password simple ftppwd
[Quidway-aaa] local-user u1 service-type ftp
[Quidway-aaa] local-user u1 ftp-directory flash:/
[Quidway-aaa] return
```

步骤 3 在 PC 机上，向 Switch 发起 FTP 连接，输入用户名 u1 和口令 ftppwd

PC 机上的 FTP 客户端以 Window XP 操作系统为例说明。

版权所有 © 华为技术有限公司

```
C:\WINDOWS\Desktop> ftp 10.1.1.2
Connected to 10.1.1.2.
220 FTP service ready.
User (10.1.1.1:(none)): u1
331 Password required for u1
Password:
230 User logged in.
ftp>
```

步骤 4 在 PC 机上，配置二进制传输格式和 PC 机本地目录

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

步骤 5 在 PC 上，向 Switch 上传文件 d006.cc 和 vrpcfg.cfg

```
ftp> put d006.cc d006.cc
200 Port command okay.
150 Opening BINARY mode data connection for d006.cc.
ftp> put vrpcfg.cfg vrpcfg.cfg
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.cfg.
ftp> quit
C:\WINDOWS\Desktop>
```

----结束

配置文件

```
#
 sysname Quidway
#
 FTP server enable
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
aaa
 local-user u1 password simple ftppwd
 local-user u1 ftp-directory flash:/
 local-user u1 service-type ftp
Return
```

配置 FTP 访问控制列表示例

在本示例中，通过配置 ACL，实现 FTP 服务器只允许某一主机登录。

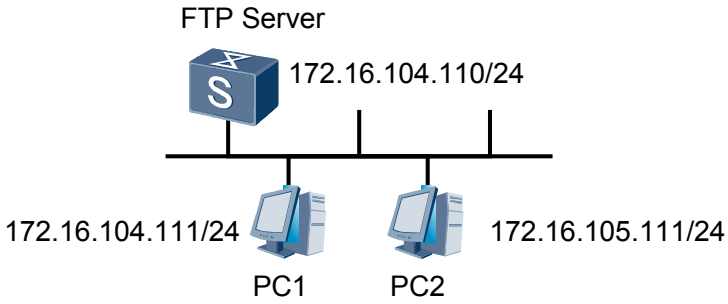
组网需求

如图 1-14 所示，FTP 服务器 IP 地址为 172.16.104.110/24。

客户端 PC1，PC2 和 FTP 服务器路由可达，在作为 FTP 服务器的 Switch 中，配置 ACL 后，实现 FTP 服务器只允许主机地址为：172.16.104.111 的 PC1 可以通过 FTP 方式下载和上传文件，PC2 无法连接 FTP 服务器。

版权所有 © 华为技术有限公司

图 1-14 配置 FTP 访问控制列表组网图



配置思路

采用如下的思路配置 FTP 服务器访问控制列表功能：

1. 在 FTP 服务器端进行基础配置。
2. 在 FTP 服务器端配置访问控制列表。

数据准备

为完成此配置举例，需准备如下的数据：

- 在服务器端设置 FTP 用户名为 u1，密码为 huawei。
- 访问控制列表号。

操作步骤

步骤 1 配置 FTP 基本功能

请参见**配置 FTP 服务器端示例**。

步骤 2 配置 ACL 基本访问控制列表

```
<Quidway> system-view
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 172.16.104.111 0.0.0.0
[Quidway-acl-basic-2001] quit
```

步骤 3 配置 FTP 支持的 ACL 列表

```
[Quidway] ftp acl 2001
```

步骤 4 从 PC1 连接 FTP Server

```
c:\ ftp 172.16.104.110
Connected to 172.16.104.110.
220 FTP service ready.
User (100.2.150.40:(none)):u1
331 Password required for u1
Password:
230 User logged in.
ftp>
```

步骤 5 从 PC2 连接 FTP Server

```
c:\ ftp 172.16.104.110
Connected to 172.16.104.110.
```


版权所有 © 华为技术有限公司

```
Info:Connection was denied by remote host according to ACL!
Connection closed by remote host.
```

----结束

配置文件

FTP 服务器的配置文件

```
#
 sysname Quidway
#
 FTP server enable
 FTP acl 2001
#
acl number 2001
 rule 5 permit source 172.16.104.111 0
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 local-user u1 password simple huawei
 local-user u1 ftp-directory flash:/
 local-user u1 service-type ftp
#
return
```

配置 FTP 客户端示例

在本示例中，通过登录 FTP 服务器，实现从 FTP 服务器中下载系统软件和配置软件到客户端中。

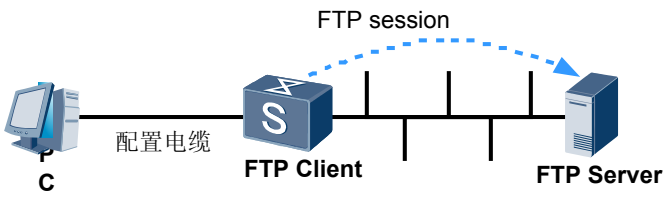
组网需求

如图 1-15 所示。远端服务器提供 FTP 服务器功能，IP 地址为 10.1.1.2。

Switch 与 FTP Server 在直连网段，路由可达。Switch 作为 FTP 客户端，从端口 GigabitEthernet0/0/1 到 GigabitEthernet0/0/4 都可以向外发起 FTP 连接请求，这些端口对应的 IP 地址为 10.1.1.3/24。

Switch 从 FTP 服务器下载文件。

图 1-15 Switch 作为 FTP 客户端的组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 FTP 客户端功能：

1. 从 FTP 客户端登录到 FTP 服务器中。
2. 从服务端下载文件到客户端的存储设备中。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 客户端的接口所属的 VLAN 号为 VLAN10，对应 VLANIF 接口的 IP 地址为 10.1.1.3/24。
- 目标文件名及在 Switch 中的位置。
- 客户端用于登录的用户名 u1 和密码 ftppwd。

操作步骤

步骤 1 在远端服务器上启动 FTP Server 服务应用，添加 FTP 用户名 u1，密码 ftppwd。

步骤 2 在 Switch 上创建 VLAN，并配置 IP 地址为 10.1.1.3/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/4] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/4] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.3 24
```

步骤 3 在 Switch 上，向 FTP Server 发起连接，FTP Server 的 IP 地址为 10.1.1.2，输入用户名 u1 和口令 ftppwd。

```
<Quidway> ftp 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
User(10.1.1.2:(none)):u1
331 Password required for u1.
Enter password:
230 User logged in.

[ftp]
```

步骤 4 在 Switch 上，配置二进制传输格式和 Flash 工作目录。

```
[ftp] binary
```


版权所有 © 华为技术有限公司

```
200 Type set to I.
[ftp] lcd flash:/
The current local directory is flash:.
```

步骤 5 在 Switch 上，从远端 FTP 服务器下载 vrpcfg.cfg 文件。

```
[ftp] get vrpcfg.cfg vrpcfg.cfg
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.cfg.

226 Transfer complete.
FTP: 9124 byte(s) received in 3.100 second(s) 2.94Kbyte(s)/sec.
[ftp] quit
<Quidway>
```

----结束

配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.3 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置 TFTP 客户端示例

在本示例中，Switch 作为 TFTP 客户端实现从服务器端下载文件。

组网需求

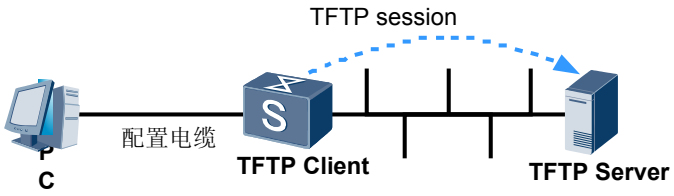
如图 1-16 所示。Switch 不能作为 TFTP 的服务器端。远端服务器提供 TFTP Server 功能，IP 地址为 10.1.1.2/24。

Switch 作为 TFTP 客户端。在 Switch 上配置 VLAN 10，将端口 GigabitEthernet0/0/1 加入 VLAN 10。配置 VLAN 10 的接口 IP 地址为 10.1.1.1/24。

Switch 从 TFTP 服务器端下载文件。

版权所有 © 华为技术有限公司

图 1-16 配置 TFTP 组网图



配置思路

采用如下的思路配置 TFTP 传输文件功能：

1. 在 TFTP 服务器端运行 TFTP 软件，并设置源文件在服务器中的位置。
2. 在 Switch 上使用 TFTP 命令下载文件。

数据准备

为完成此配置例，需准备如下的数据：

- TFTP 服务器端安装 TFTP 软件。
- 源文件在 TFTP 服务器中的路径。
- 目标文件名及在 Switch 上存放的路径。

操作步骤

步骤 1 在远端服务器上启动 TFTP Server 服务，确保 TFTP 服务应用软件处于启动状态

步骤 2 在 Switch 上创建 VLAN 10，并配置 VLAN 10 接口的 IP 地址为 10.1.1.1/24

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
```

步骤 3 在 Switch 上，向 TFTP Server 发起连接，下载 8031.cc 文件

```
<Quidway> tftp 10.1.1.2 get 8031.cc 8031new.cc
Info:  Transfer file in binary mode.
Downloading the file from the remote tftp server, please wait...
```

----结束

配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
Return
```

1.9 Telnet 及 SSH

Telnet 及 SSH 提供通过终端远程登录并访问服务器的方式。

1.9.1 Telnet 及 SSH 简介

用户登录、Telnet 及 SSH 基本概念。

用户登录概述

用户可以通过 Console 口、Telnet 或 SSH 进行本地或远程登录。

配置了用户界面、用户管理和终端服务后，用户才能登录到设备，对本地或远端的 AC6605 进行配置、监控和维护。

用户界面提供登录入口，用户管理确保登录安全，终端服务则提供登录协议支持。

目前 AC6605 支持的登录方式包括：

- 通过 Console 口登录。
- 通过 Telnet 或 SSH 进行本地或远程登录。

Telnet 终端服务基本概念

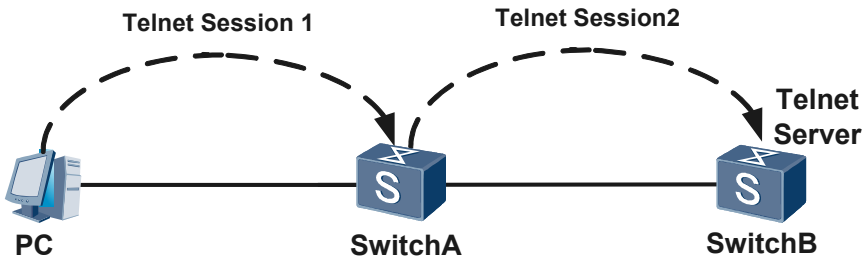
AC6605 提供的 Telnet 服务包括 Telnet Server 和 Telnet Client。

Telnet 协议在 TCP/IP 协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。

AC6605 提供的 Telnet 服务包括：

- Telnet server：用户在 PC 上运行 Telnet 客户端程序登录到交换机，对交换机进行配置管理。此时，交换机提供 Telnet server 服务。
- Telnet client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与交换机的连接后，再执行 **telnet** 命令登录到其它交换机，对其进行配置管理。如图 1-17 所示，SwitchA 此时既作为 Telnet server，也同时提供 Telnet client 服务。

图 1-17 提供 Telnet client 服务



版权所有 © 华为技术有限公司

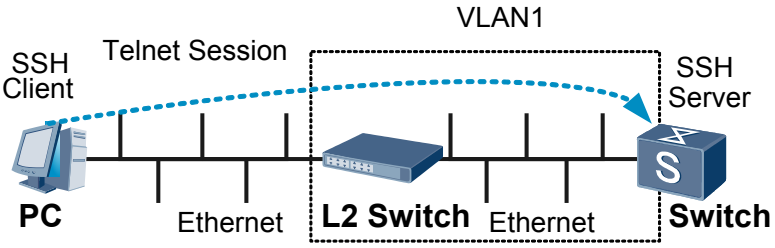
SSH 终端服务基本概念

AC6605 支持基本的 SSH 协议、客户端功能、SCP 功能、SFTP 协议、STelnet 协议。

SSH 简介

SSH（Secure Shell）在 TCP/IP 协议族中属于应用层协议，主要用于在需要保证安全的网络环境中提供远程登录和虚拟终端功能。SSH 基于 TCP 连接为传输信息提供强大的安全保障和验证功能，从而有效地抵御 IP 地址欺骗、明文密码截取、DoS（Denial of Service）等攻击。如图 1-18 所示。图中，AC6605 用 Switch 表示。

图 1-18 PC 与 AC6605 建立本地 SSH 连接



SSH 采用了客户/服务器体系模型，通过建立 SSH 连接构建多条安全的传输通路。例如，Switch 作为 SSH Server，可以接受来自多个用户 PC 机（SSH Client）的连接，用户 PC 机和 SSH Server 之间可能存在其它 L2 Switch 设备。实际组网时，要求 PC 和 Switch 之间有可达路由。

SSH 的优势

SSH 的应用包括 STelnet 和 SFTP，相对 Telnet、FTP 等终端服务，SSH 可以在没有安全保障的网络上提供安全的远程访问，优势如下：

- STelnet 客户端功能

  Telnet 缺少安全的认证方式，而且传输过程采用 TCP 进行明文传输，存在很大的安全隐患。单纯提供 Telnet 服务容易招致 DoS（Denial of Service）、主机 IP 地址欺骗、路由欺骗等恶意攻击。

  相对于 Telnet，SSH 通过以下措施实现在不安全网络上提供安全的远程访问：

  - 支持 RSA（Revest-Shamir-Adleman Algorithm）验证方式
  - 支持 DES（Data Encryption Standard）、3DES 数据加密方式
  - 支持用户名/口令的加密传输
  - 支持交互数据的加密传输

  SSH 终端服务采用 RSA 算法，可以遵照非对称加密体系的加密原则，通过生成公钥和私钥，以加密方式传递密钥、用户名/口令、交互数据，最终实现了整个会话信息的端到端安全传递。
- SFTP 客户端功能

  SFTP 是 Secure FTP 的简称，存在两种应用。

版权所有 © 华为技术有限公司

- 用户可以从远端安全地通过 AC6605 登录到远程设备上，进行文件管理，应用于远程系统升级等需要文件传送的地方，增加了数据传输的安全性。
- AC6605 本身可以作为客户端，在本设备上安全 FTP 到远程设备，进行文件的安全传输。

- SCP 客户端功能

  SCP 是 Secure Copy 的简称，使得用户可以从远端安全的登录到设备上进行文件上传或下载，这样使远程系统升级等需要文件传送的地方，增加了数据传输的安全性。同时，由于提供了客户端功能，可以在本设备上连接到远程设备，进行文件的安全传输。

  与 SFTP 协议相比，SCP 协议可以简化用户传输文件的操作，将用户身份认证、文件传输等步骤合并，提高配置效率。

SSH 连接的建立过程

SSH 连接的建立过程包括如下五个阶段：

1. 协商 SSH 版本号
2. 协商密钥
3. 验证用户身份
4. 请求会话
5. 交互会话

1.9.2 配置 Telnet 终端服务

通过 Telnet 协议远程登录到交换机，对交换机进行配置。

建立配置任务

在进行 Telnet 终端服务的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户通过 Telnet 协议远程登录到交换机进行维护管理时，需要配置 Telnet 终端服务。

前置任务

在配置 Telnet 终端服务之前，需要完成以下任务：

- 交换机运行正常
- 正确配置交换机接口的 IP 地址
- 配置了用户账号以及正确的登录验证方式和呼入呼出受限规则
- 终端与交换机之间有可达路由

数据准备

在配置 Telnet 终端服务之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	交换机 IP 地址
2	VPN 实例名
3	远端交换机的 IPv4/IPv6 地址或主机名
4	远端交换机提供 Telnet 服务的 TCP 端口号
5	（可选）用户界面断开连接的超时时间
6	（可选）设备作为 Telnet 客户端时的源地址（或者源接口）

使能 Telnet 服务

建立与服务器的 Telnet 连接之前，需要首先开启 Telnet 服务。

背景信息

请在作为 Telnet 服务器的交换机上进行如下的配置。

根据网络协议基于 IPv4 还是 IPv6，选择执行如下步骤之一。

操作步骤

- 网络协议基于 IPv4
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **telnet server enable**，使能 Telnet 服务。

     说明

     - 缺省情况下，系统的 Telnet 服务功能是开启的。
     - 执行命令 **undo telnet server enable** 关闭 Telnet 服务器时，如果有通过 telnet 登录的用户在线，该命令执行不成功。
     - 关闭 Telnet 服务功能后，将不能通过 Telnet 方式登录设备，只能通过 SSH 或异步串口等其他方式登录设备。
- 网络协议基于 IPv6
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **telnet ipv6 server enable**，使能 Telnet 服务。

     说明

     - 缺省情况下，系统的 Telnet 服务功能是开启的。
     - 执行命令 **telnet ipv6 server enable** 关闭 Telnet 服务器时，如果有通过 telnet 登录的用户在线，该命令执行不成功。
     - 关闭 Telnet 服务功能后，将不能通过 Telnet 方式登录设备，只能通过 SSH 或异步串口等其他方式登录设备。

----结束

建立 Telnet 连接

用户可以通过 Telnet 连接，登录并管理交换机。

版权所有 © 华为技术有限公司

背景信息

请在作为 Telnet 客户端的交换机上进行如下的配置。

根据网络协议基于 IPv4 还是 IPv6，选择执行如下 2 个步骤之一：

操作步骤

- 执行命令 **telnet** [**vpn-instance** *vpn-instance-name*] *host-name* [*port-number*]，登录并管理其他交换机。
- 执行命令 **telnet ipv6** *host-name* [*port-number*]，登录并管理其他交换机。

----结束

（可选）配置 Telnet 服务器端口号

用户可以配置或变更 Telnet 服务器监听端口号。变更后，只有用户知道 Telnet 服务使用的当前端口号，确保安全性。

背景信息

请在作为 Telnet 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **telnet server port** *port-number*，设置 Telnet 服务器的监听端口号。

如果配置了新的监听端口号，Telnet 服务器端先断开当前已经建立的所有 Telnet 连接，然后使用新的端口号开始监听。缺省情况下，Telnet 服务器端监听端口号是 23。

----结束

（可选）Telnet 连接的定时断开

用户可以配置 Telnet 连接空闲时间。在设定的时间内，如果 Telnet 连接始终处于空闲状态，系统将自动断开该 Telnet 连接。

背景信息

请在作为 Telnet 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **idle-timeout** *minutes* [*seconds*]，允许定时断开 Telnet 连接。

----结束

版权所有 © 华为技术有限公司

检查配置结果

Telnet 终端服务配置成功后，可以查看到当前用户界面连接情况、每个用户界面连接情况、以及当前建立的所有 TCP 连接情况等内容。

前提条件

已完成 Telnet 终端服务的所有配置。

背景信息

- 使用 **display users** 命令查看当前用户界面连接情况。
- 使用 **display users all** 命令查看每个用户界面连接情况。
- 使用 **display tcp status** 命令查看当前建立的所有 TCP 连接情况。
- 使用 **display telnet server status** 命令查看 Telnet 服务器的状态和配置信息。

任务示例

执行命令 **display tcp status**，可以看到 TCP 连接状态。**Established** 表示一个 TCP 连接已经建立。

```
<Quidway> display tcp status
TCPCB      Tid/Soid    Local Add:port         Foreign Add:port      VPNID     State
39952df8   36 /1509     0.0.0.0:0              0.0.0.0:0             0         Closed
32af9074   59 /1        0.0.0.0:21             0.0.0.0:0             14849     Listening
34042c80   73 /17       10.164.39.99:23        10.164.6.13:1147      0         Established
```

执行命令 **display telnet server status**，可以看到 Telnet 服务器的状态和配置信息。

```
<Quidway> display telnet server status
 TELNET IPV4 server                      :Enable
 TELNET IPV6 server                      :Enable
 TELNET server port                      :23
```

1.9.3 配置 SSH 用户

配置 SSH 用户，保证 STelnet 或 SFTP 客户端能够登录到 SSH 服务器。

建立配置任务

在进行 SSH 用户的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

只有在 SSH 服务器端完成对 SSH 用户的正确配置后，STelnet 或 SFTP 客户端才能登录到 SSH 服务器，完成到相应的操作。

前置任务

在配置 SSH 用户之前，需完成以下任务：

- 创建本地用户
- SSH 服务器端配置客户端的 RSA 公钥

版权所有 © 华为技术有限公司

数据准备

在配置 SSH 用户之前，需准备以下数据。

序号	数据
1	SSH 用户的用户名和密码
2	SSH 用户的认证方式
3	SSH 用户的服务方式
4	为 SSH 用户分配的对端 RSA 公钥名
5	SSH 用户的 SFTP 工作目录

创建 SSH 用户

AAA 无法提供 RSA 认证，因此当认证方式为 RSA 或 password-rsa 时，用户需要创建 SSH 用户。如果认证方式为 password，可以使用 AAA 视图同名的 local-user 用户。

背景信息

说明

如果不单独创建 SSH 用户，还可以在进行如下配置的同时新建 SSH 用户：

- **配置 SSH 用户的认证方式**
- **配置 SSH 用户的服务方式**

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh user** *user-name*，创建 SSH 用户。

如果创建认证方式为 password 或 password-rsa 的 SSH 用户，则还需要在 AAA 视图下创建同名的 local-user 用户。

1. 执行命令 **aaa**，进入 AAA 视图。
2. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

配置 VTY 用户界面支持 SSH 协议

用户可以在 VTY 用户界面配置 SSH。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-interface** [**vty**] *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **authentication-mode aaa**，设置验证方式为 AAA 验证。

步骤 4 执行命令 **protocol inbound ssh**，配置 VTY 支持 SSH 协议。

说明

必须设置 VTY 用户界面验证方式为 AAA 验证，否则 **protocol inbound ssh** 将不能配置成功。

----结束

生成本地 RSA 密钥对

在进行 SSH 配置之前，需要首先配置 RSA 密钥。

背景信息

请在作为客户端和服务器端的交换机上分别进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rsa local-key-pair create**，产生本地 RSA 密钥对。

说明

成功完成 SSH 登录的首要操作是配置并产生本地 RSA 密钥对。在进行其它 SSH 配置之前，必须完成 **rsa local-key-pair create** 配置，生成本地密钥对。

----结束

配置 SSH 用户的认证方式

用户可以配置对 SSH 用户进行 Password 验证或者 RSA 验证。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** }，配置 SSH 用户的认证方式。

根据实际配置需要，选择如下操作之一：

- 配置对 SSH 用户进行 Password 验证

版权所有 © 华为技术有限公司

- 执行命令 **ssh user** *user-name* **authentication-type password**，对 SSH 用户配置 Password 验证。
- 执行命令 **ssh authentication-type default password**，对 SSH 用户配置缺省密码验证。

采用本地认证或 HWTACACS 服务器认证时，如果用户数量少可以采用第一种配置；如果用户数量比较多，对 SSH 用户使用缺省密码验证方式可以简化配置。

- 配置对 SSH 用户进行 RSA 验证

1. 执行命令 **ssh user** *user-name* **authentication-type rsa**，对 SSH 用户配置 RSA 验证。
2. 执行命令 **rsa peer-public-key** *key-name*，进入公共密钥视图。
3. 执行命令 **public-key-code begin**，进入公共密钥编辑视图。
4. 输入 *hex-data*，编辑公共密钥。

   键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持 SSH 的客户端软件随机生成。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。
5. 执行命令 **public-key-code end**，退出公共密钥编辑视图。

   如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥；如果步骤 b 中指定的密 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。
6. 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。
7. 执行命令 **ssh user** *user-name* **assign rsa-key** *key-name*，为 SSH 用户分配公钥。

说明

- 进入公共密钥编辑视图后，即可将客户端上产生的 RSA 公共密钥传送到服务器端。请采用拷贝粘贴方式将 RSA 公共密钥配置到作为 SSH 服务器的交换机上。
- 在为 SSH 用户分配对端 RSA 公共密钥之前，所分配的对端 RSA 公共密钥必须是在 SSH 服务器端已经配置完成且来自 SSH 客户端的 RSA 公共密钥。

----结束

（可选）配置 SSH 用户基本验证信息

用户可以配置服务器密钥的更新时间、SSH 认证超时时间以及 SSH 验证重试次数。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh server rekey-interval** *interval*，设置服务器密钥的更新时间。

缺省情况下，SSH 服务器密钥对的更新时间间隔为 0，表示永不更新。

步骤 3 执行命令 **ssh server timeout** *seconds*，设置 SSH 认证超时时间。

缺省情况下，SSH 连接认证超时时间为 60 秒。

步骤 4 执行命令 **ssh server authentication-retries** *times*，设置 SSH 验证重试次数。

版权所有 © 华为技术有限公司

缺省情况下，SSH 连接的验证重试次数为 3。

----结束

（可选）配置 SSH 用户按命令行授权

配置验证方式为 RSA 时，需要配置 SSH 用户按命令行授权。

背景信息

说明

SSH 用户有 4 种验证方式：password、rsa、password-rsa 和 all 方式。password 方式的命令行授权配置请参见《AC6605 无线接入控制器 配置指南-安全》“AAA 及用户管理配置”。本节介绍 RSA 方式的命令行授权。

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh user** *user-name* **authorization-cmd aaa**，对指定 SSH 用户配置按命令行授权。

----结束

后续处理

对进行 RSA 验证的 SSH 用户配置命令行授权后，请再进行相关 AAA 授权配置。否则该 SSH 用户的命令行授权配置不能生效。

配置 SSH 用户的服务方式

用户可以配置 SSH 用户的服务方式为 sftp 或 stelnet 或 all。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh user** *username* **service-type** { **sftp** | **stelnet** | **all** }，配置 SSH 用户的服务方式。

缺省情况下，SSH 用户的服务方式是空，即不支持任何服务方式。

----结束

（可选）配置 SSH 用户的 SFTP 服务授权目录

用户配置某一目录为授权目录，允许 SSH 用户使用 SFTP 服务。

版权所有 © 华为技术有限公司

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh user** *username* **sftp-directory** *directoryname*，配置 SSH 用户的 SFTP 服务授权目录。

缺省情况下，SSH 用户的 SFTP 服务授权目录为 Flash。

----结束

检查配置结果

SSH 用户配置成功后，可以查看到 SSH 用户信息等内容。

前提条件

已完成 SSH 用户的所有配置

背景信息

- 使用 **display ssh user-information** 命令在 SSH 服务器端查看所有 SSH 用户信息。
- 使用 **display ssh user-information** *username* 命令在 SSH 服务器端查看指定 SSH 用户信息。

任务示例

运行命令 **display ssh user-information** *username*，可以看到名为 **client001** 的 SSH 用户的验证方式为 **password**，服务方式为 **sftp**。

```
<Quidway> display ssh user-information client001
      User Name              : client001
      Authentication-type    : password
      User-public-key-name   : -
      Sftp-directory         : -
      Service-type           : sftp
      Authorization-cmd      : No
```

1.9.4 配置 SSH 服务器功能

SSH 服务器的配置方法。首先在 SSH 服务器上使能 STelnet 或者 SFTP，保证 STelnet 和 SFTP 功能的使用。

建立配置任务

在进行 SSH 服务器功能的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

必须在 SSH 服务器上使能 STelnet、SFTP 或者 SCP，才能完成到相应的操作。SSH 服务器还支持监听端口号的设定。通过设定 SSH 服务器端的监听端口号为其他端口，攻

版权所有 © 华为技术有限公司

击者不知道 SSH 监听端口号的更改，有效防止攻击者对 SSH 服务标准端口访问消耗带宽和系统资源。

前置任务

在配置 SSH 服务器功能之前，需完成以下任务：

- SSH 客户端和服务器正确连接
- SSH 客户端和服务器之间有可达的路由
- SSH 服务器端配置 VTY 用户界面支持 SSH 协议
- SSH 服务器端配置 SSH 用户
- SSH 服务器端生成本地 RSA 密钥对

数据准备

在配置 SSH 服务器功能之前，需准备以下数据。

序号	数据
1	SSH 服务器端监听端口号

使能 STelnet 服务

使用 STelnet 服务之前，需要首先进行使能操作。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stelnet server enable**，使能 STelnet 服务。

缺省情况下，STelnet 服务为关闭状态。

----结束

使能 SFTP 服务

使用 SFTP 服务之前，需要首先进行使能操作。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **sftp server enable**，使能 SFTP 服务。

缺省情况下，SFTP 服务为关闭状态。

----结束

使能 SCP 服务

使用 SCP 服务之前，需要首先进行使能操作。

请在作为 SCP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **scp server enable**，使能 SCP 服务。

缺省情况下，SSH 服务器端的 SCP 服务为关闭状态。

----结束

（可选）使能兼容低版本功能

用户可以配置是否使能兼容低版本 SSH 协议。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh server compatible-ssh1x enable**，使能兼容低版本功能。

缺省情况下，SSH2.0 协议的服务器是兼容 SSH1.X 服务器功能的。如果不允许 SSH1.3 ～ SSH1.99（SSH 的协议版本号大于等于 1.3 且小于等于 1.99）的客户端登录，则执行 **undo ssh server compatible-ssh1x enable**，去使能兼容低版本功能。

说明

- SSH2.0 协议相比 SSH1.X 协议来说，在结构上做了扩展，可以支持更多的认证方法和密钥交换方法，同时提高了服务能力（如 SFTP）。
- AC6605 支持大于等于 1.3 且小于等于 2.0 之间的 SSH 协议版本。

----结束

（可选）配置 SSH 服务器端监听端口号

用户可以配置或变更 SSH 服务器监听端口号。变更后，只有用户知道 SSH 服务使用的当前端口号，确保安全性。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh server port** *port-number*，配置 SSH 服务器监听端口号。

如果配置了新的监听端口号，SSH 服务器端先断开当前已经建立的所有 STelnet 和 SFTP 连接，然后使用新的端口号开始监听。缺省情况下，SSH 服务器端监听端口号是 22。

----结束

（可选）配置服务器密钥对更新时间

用户可以配置服务器密钥对更新时间，更新密钥可以保证安全性。

背景信息

请在作为 SSH 服务器的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh server rekey-interval** *interval*，配置服务器密钥对更新时间。

缺省情况下，SSH 服务器密钥对的更新时间间隔为 0，表示永不更新。

----结束

检查配置结果

SSH 服务器功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

前提条件

已经完成 SSH 服务器功能的所有配置。

背景信息

使用 **display ssh server status** 命令查看 SSH 服务器的全局配置信息。

任务示例

执行命令 **display ssh server status**，可以看到 SSH 会话连接的协议版本号为 1.99、建立 SSH 会话连接的重试次数为 5 等信息。

```
<Quidway> display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval :2 hours
 SSH Authentication retries           :5 times
 SFTP server                          :Enable
 Stelnet server                       :Enable
 Scp server                           :Enable
 SSH server port                      :55535
```

说明

如果当前监听端口号是缺省值，不显示当前监听端口号信息。

版权所有 © 华为技术有限公司

1.9.5 配置 STelnet 客户端功能

STelnet 客户端的配置方法。客户端和服务器之间经过协商，建立安全连接，客户端可以像操作 Telnet 一样登录服务器。

建立配置任务

在进行 Stelnet 客户端功能的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

STelnet 是一种安全的 Telnet 服务，SSH 用户可以像使用 Telnet 服务一样操作 STelnet 服务。

前置任务

在 STelnet 客户端连接 SSH 服务器之前，需完成以下任务：

- SSH 服务器端生成本地 RSA 密钥对
- SSH 服务器端配置 STelnet 用户
- SSH 服务器端 STelnet 服务使能

数据准备

在配置 STelnet 客户端连接 SSH2 服务器之前，需准备以下数据。

序号	数据
1	SSH 服务器名称
2	SSH 服务器当前监听的端口号
3	STelnet 客户端到 SSH 服务器端的首选加密算法
4	SSH 服务器端到 STelnet 客户端的首选加密算法
5	STelnet 客户端到 SSH 服务器端的首选 HMAC 算法
6	SSH 服务器端到 STelnet 客户端的首选 HMAC 算法
7	首选密钥交换算法
8	出接口名称
9	源地址

使能 SSH 客户端首次认证功能

使能 SSH 客户端首次认证功能后，当 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。

版权所有 © 华为技术有限公司

背景信息

如果配置了使能 SSH 客户端首次认证功能，那么在 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。登录后，系统将自动分配并保存 RSA 公钥，为下次登录时认证。

推荐使用使能 SSH 客户端首次认证功能，简化用户操作。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh client first-time enable**，使能 SSH 客户端首次认证功能。

缺省情况下，SSH 客户端首次认证功能为关闭状态。

说明

- 使能 SSH 客户端首次认证功能的目的，是为了当 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查，因为此时 STelnet 客户端还没有保存 SSH 服务器的 RSA 公钥。
- 如果没有使能 SSH 客户端首次认证功能，则当 STelnet 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，而导致登录服务器失败。

窍门

除了使能 SSH 客户端首次认证功能之外，如果 STelnet 客户端想第一次就能成功登录 SSH 服务器，还可以通过事先在客户端为 SSH 服务器分配 RSA 公钥来实现。

----结束

（可选）SSH 客户端为 SSH 服务器分配 RSA 公钥

用户可以在 SSH 客户端为 SSH 服务器分配 RSA 公钥。

背景信息

如果没有使能 SSH 客户端首次认证功能，那么需要在 STelnet 客户端登录 SSH 服务器之前分配 RSA 公钥。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rsa peer-public-key** *key-name*，进入公共密钥视图。

步骤 3 执行命令 **public-key-code begin**，进入公共密钥编辑视图。

步骤 4 输入 *hex-data*，编辑公共密钥。

键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持 SSH 的客户端软件随机生成。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。

步骤 5 执行命令 **public-key-code end**，退出公共密钥编辑视图。

版权所有 © 华为技术有限公司

如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥；如果步骤 2 中指定的 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。

步骤 6 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。

步骤 7 执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配 RSA 公钥。

说明

- 在为 SSH 服务器分配对端 RSA 公钥之前，所分配的对端 RSA 公钥必须是在 SSH 客户端已经配置完成且来自 SSH 服务器端的 RSA 公钥，这样 STelnet 客户端对 SSH 服务器的 RSA 公钥进行有效性检查才会通过。
- 如果 SSH 客户端保存的 SSH 服务器公钥失效，执行命令 **undo ssh client** *servername* **assign rsa-key**，解除 SSH 客户端与 SSH 服务器的绑定关系，再执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配新的 RSA 公钥。

----结束

启动 STelnet 客户端

用户可以从 SSH 客户端以 STelnet 方式登录到 SSH 服务器上。

背景信息

说明

STelnet 客户端访问 SSH 服务器时可以携带源地址、VPN 实例名，选择密钥交换算法、加密算法和 HMAC 算法。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **stelnet** *host-ipv4* [*port*] [[**-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 STelnet 方式登录到 SSH 服务器上。

- 如果是 IPv6 类型的地址

  执行命令 **stelnet ipv6** *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 STelnet 方式登录到 SSH 服务器上。

----结束

检查配置结果

Stelnet 客户端功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

版权所有 © 华为技术有限公司

前提条件

已完成 STelnet 客户端功能的所有配置

背景信息

- 使用 **display ssh server-info** 命令在 SSH 客户端查看 SSH 服务器与 RSA 公钥之间的对应关系。
- 使用 **display ssh server session** 命令在 SSH 服务器端查看 SSH 客户端连接会话信息。

任务示例

运行命令 **display ssh server session**，可以看到客户端从 VTY3 登录上来，采用的服务方式是 Stelent，验证方式是 password 等信息。

```
<Quidway> display ssh server session
Session 1:
       Conn                : VTY 3
       Version             : 2.0
       State               : started
       Username            : client001
       Retry               : 1
       CTOS Cipher         : aes128-cbc
       STOC Cipher         : aes128-cbc
       CTOS Hmac           : hmac-sha1-96
       STOC Hmac           : hmac-sha1-96
       Kex                 : diffie-hellman-group1-sha1
       Service Type        : stelnet
       Authentication Type : password
```

1.9.6 配置 SFTP 客户端功能

SFTP 客户端的配置方法。服务器通过对客户端的认证及双向的数据加密，为网络文件传输提供了安全的服务。

建立配置任务

在进行 SFTP 客户端功能的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

SFTP 使得用户可以从远端安全的登入设备进行文件管理，这样使远程系统升级等需要文件的传送的地方，增加了数据传输的安全性。同时，由于提供了 Client 功能，可以在本设备上安全 FTP 到远程设备，进行文件的安全传输。

前置任务

在 SFTP 客户端连接 SSH2 服务器之前，需完成以下任务：

- SSH 服务器端生成本地 RSA 密钥对
- SSH 服务器端配置 SFTP 用户
- SSH 服务器端 SFTP 服务使能

版权所有 © 华为技术有限公司

数据准备

在 SFTP 客户端连接 SSH2 服务器之前，需准备以下数据。

序号	数据
1	SSH 服务器名称
2	SSH 服务器当前监听的端口号
3	SFTP 客户端到 SSH 服务器端的首选加密算法
4	SSH 服务器端到 SFTP 客户端的首选加密算法
5	SFTP 客户端到 SSH 服务器端的首选 HMAC 算法
6	SSH 服务器端到 SFTP 客户端的首选 HMAC 算法
7	首选密钥交换算法
8	出接口名称
9	目录名称
10	文件名称

使能 SSH 客户端首次认证功能

使能 SSH 客户端首次认证功能后，当 SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。

背景信息

如果配置了使能 SSH 客户端首次认证功能，那么在 SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。登录后，系统将自动分配并保存 RSA 公钥，为下次登录时认证。

推荐使用使能 SSH 客户端首次认证功能，简化用户操作。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssh client first-time enable**，使能 SSH 客户端首次认证功能。

缺省情况下，SSH 客户端首次认证功能为关闭状态。

说明

- 使能 SSH 客户端首次认证功能的目的，是为了当 SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查，因为此时 SFTP 客户端还没有保存 SSH 服务器的 RSA 公钥。
- 如果没有使能 SSH 客户端首次认证功能，则当 SFTP 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，而导致登录服务器失败。

版权所有 © 华为技术有限公司

窍门

除了使能 SSH 客户端首次认证功能之外，如果 SFTP 客户端想第一次就能成功登录 SSH 服务器，还可以通过事先在客户端为 SSH 服务器分配 RSA 公钥来实现。

----结束

（可选）SSH 客户端为 SSH 服务器分配 RSA 公钥

用户可以在 SSH 客户端为 SSH 服务器分配 RSA 公钥。

背景信息

如果没有使能 SSH 客户端首次认证功能，那么需要在 SFTP 客户端登录 SSH 服务器之前分配 RSA 公钥。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rsa peer-public-key** *key-name*，进入公共密钥视图。

步骤 3 执行命令 **public-key-code begin**，进入公共密钥编辑视图。

步骤 4 输入 *hex-data*，编辑公共密钥。

键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持 SSH 的客户端软件随机生成。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。

步骤 5 执行命令 **public-key-code end**，退出公共密钥编辑视图。

如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥；如果步骤 2 中指定的 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。

步骤 6 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。

步骤 7 执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配 RSA 公钥。

说明

- 在为 SSH 服务器分配对端 RSA 公钥之前，所分配的对端 RSA 公钥必须是在 SSH 客户端已经配置完成且来自 SSH 服务器端的 RSA 公钥，这样 SFTP 客户端对 SSH 服务器的 RSA 公钥进行有效性检查才会通过。
- 如果 SSH 客户端保存的 SSH 服务器公钥失效，执行命令 **undo ssh client** *servername* **assign rsa-key**，解除 SSH 客户端与 SSH 服务器的绑定关系，再执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配新的 RSA 公钥。

----结束

启动 SFTP 客户端

用户可以从 SSH 客户端以 SFTP 方式登录到 SSH 服务器上。

版权所有 © 华为技术有限公司

背景信息

说明

SFTP 客户端启动命令跟 STelnet 客户端启动命令很相似，支持访问 SSH 服务器时携带源地址，选择密钥交换算法、加密算法和 HMAC 算法，以及设置 keepalive 功能。

在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **sftp** [**-a** *source-address*] *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 SFTP 方式登录到 SSH 服务器上。

----结束

（可选）管理目录

用户可以在 SFTP 客户端上创建、删除服务器上的目录。

背景信息

说明

当 SFTP 客户端登录到 SSH 服务器之后，在 SFTP 客户端可以创建并删除 SSH 服务器上的目录，以及显示当前的工作目录，显示指定目录下的文件或目录信息。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **sftp** [**-a** *source-address*] *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] |

版权所有 © 华为技术有限公司

[**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 SFTP 方式登录到 SSH 服务器上。

步骤 3 可根据需要，执行如下一个或多个操作：

- 执行命令 **cd** [*remote-directory*]，改变用户的当前工作目录。
- 执行命令 **cdup**，改变用户的工作目录为当前工作目录的上一级目录。
- 执行命令 **pwd**，显示用户的当前工作目录。
- 执行命令 **dir / ls** [*remote-directory*]，显示指定目录下的文件列表。
- 执行命令 **rmdir** *remote-directory* & <1-10>，删除服务器上目录。
- 执行命令 **mkdir** *remote-directory*，在服务器上创建新目录。

----结束

（可选）管理文件

用户可以在 SFTP 客户端上显示 SFTP 服务器指定远程目录或文件的信息，或者删除 SFTP 服务器上的指定文件。

背景信息

说明

当 SFTP 客户端登录到 SSH 服务器之后，在 SFTP 客户端可以改变文件名、删除文件、显示文件列表、上传，下载文件。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **sftp** [**-a** *source-address*] *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** |

版权所有 © 华为技术有限公司

sha1_96 | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 SFTP 方式登录到 SSH 服务器上。

步骤 3 可根据需要，执行如下一个或多个操作：

- 执行命令 **rename** *old-name new-name*，改变服务器上指定的文件的名字。
- 执行命令 **get** *remote-filename* [*local-filename*]，下载远程服务器上的文件。
- 执行命令 **put** *local-filename* [*remote-filename*]，上传本地文件到远程服务器。
- 执行命令 **remove** *remote-filename*，删除服务器上文件。

----结束

（可选）SFTP 客户端命令帮助

用户而可以查看 SFTP 客户端命令帮助。

背景信息

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **sftp** [**-a** *source-address*] *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 SFTP 方式登录到 SSH 服务器上。

步骤 3 执行命令 **help** [**all** | *command-name*]，显示 SFTP 客户端命令帮助。

----结束

检查配置结果

SFTP 客户端功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

前提条件

已完成 SFTP 客户端功能的所有配置

版权所有 © 华为技术有限公司

背景信息

- 使用 **display ssh server-info** 命令在 SSH 客户端查看 SSH 服务器与 RSA 公钥之间的对应关系。
- 使用 **display ssh server session** 命令在 SSH 服务器端查看 SSH 客户端连接会话信息。

任务示例

运行命令 **display ssh server session**，可以看到客户端从 VTY4 登录上来，服务方式是 **sftp**，验证方式是 **rsa** 等。

```
<Quidway> display ssh server session
Session 2:
       Conn                 : VTY 4
       Version              : 2.0
       State                : started
       Username             : client002
       Retry                : 1
       CTOS Cipher          : aes128-cbc
       STOC Cipher          : aes128-cbc
       CTOS Hmac            : hmac-sha1-96
       STOC Hmac            : hmac-sha1-96
       Kex                  : diffie-hellman-group1-sha1
       Service Type         : sftp
       Authentication Type  : rsa
```

1.9.7 配置 SCP 客户端功能

SCP 客户端的配置方法。SCP 客户端和服务器之间经过协商，建立安全连接，客户端可以上传文件至服务器或从服务器下载文件至本地。

建立配置任务

在进行 SCP 客户端功能的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

SCP 是基于 SSH2 的安全文件传输方式。与使用 SFTP 协议传输文件相比，使用 SCP 方式上传或下载文件，可以减少用户认证、分配公钥等操作步骤，同时支持批量操作。

前置任务

在配置 SCP 客户端功能之前，需完成以下任务：

- SCP 服务器端生成本地 RSA 密钥对
- SCP 服务器端配置 SCP 用户
- SCP 服务器端 SCP 服务使能

数据准备

在配置 SCP 客户端之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	（可选）本端交换机的源 IPv4 或 IPv6 地址、源接口
2	远端 SCP 服务器的端口号、VPN 实例名、文件上传或下载时的加密算法、上传或下载的源文件、上传或下载的目的文件

（可选）配置 SCP 客户端源地址

用户可以配置 SCP 客户端的源地址信息，从指定的客户端源地址建立 SCP 连接，保证安全性。

背景信息

请在作为 SCP 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 SCP 客户端的源 IP 地址或源接口。

当前源接口只支持 LoopBack 接口，增强安全性。

----结束

拷贝文件

用户可以从客户端通过 SCP 方式上传文件至服务器或下载服务器上的文件至本地。

背景信息

说明

SCP 客户端访问 SCP 服务器时可以携带源地址、VPN 实例名，选择加密算法。

请在作为 SCP 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 上传文件至远端 SCP 服务器或下载远端 SCP 服务器上的文件至本地

- 基于 IPv4

  scp [**-port** *port-number* | **public-net** | **vpn-instance** *vpn-instance-name* | **-a** *sourceaddress* | **-i** *interface-type interface-number* | **-r** | **-cipher** { **des** | **3des** | **aes128** } | **-c**]* *sourcefile destinationfile*

- 基于 IPv6

版权所有 © 华为技术有限公司

scp ipv6 [**-port** *port-number* | **public-net** | **vpn-instance** *vpn-instance-name* | **-a** *sourceipv6address* | **-r** | **-cipher** { **des** | **3des** | **aes128** } | **-c**]* *sourcefile destinationfile* [**-i** *interface-type interface-number*]

----结束

检查配置结果

SCP 客户端功能配置成功后，可以查看到 SCP 连接的配置信息。

前提条件

已完成 SCP 客户端功能的所有配置

背景信息

- 使用 **display scp-client** 命令在 SCP 客户端查看源配置信息。

任务示例

执行命令 **display scp-client**，可以看到源 IP 地址的配置信息。

```
<Quidway> display scp-client
 The source of SCP ipv4 client: 1.1.1.1
 The source of SCP ipv6 client: --
```

1.9.8 配置举例

配置 Telnet 及 SSH 的应用的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

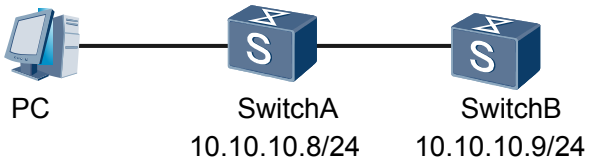
配置 Telnet 终端服务示例

在本示例中，通过配置用户验证方式和密码，实现 Telnet 登录。

组网需求

如图 1-19，用户登录到 Switch 后，通过在 Switch 上的 Telnet 程序登录到 SwitchB（使用默认接口号 23）。

图 1-19 Ethernet 网络用户远程登录组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GigabitEthernet0/0/1	VLANIF 2	10.10.10.8/24
SwitchB	GigabitEthernet0/0/1	VLANIF 2	10.10.10.9/24

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 Telnet 终端服务：

1. 在 SwitchA 和 SwitchB 上配置 IP 地址。
2. 在 SwitchB 上配置 Telnet 验证方式和密码。
3. 从 SwitchA 登录到 SwitchB 上。

数据准备

为完成此配置举例，需准备以下数据：

- VLAN 的 ID
- Telnet 客户端 SwitchA 的 IP 地址和接口号
- Telnet 服务器 SwitchB 的 IP 地址和接口号
- SwitchB Telnet 登录的验证方式和密码

操作步骤

步骤 1 配置 IP 地址

配置 Telnet 客户端 SwitchA 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 2
[SwitchA-Vlanif2] ip address 10.10.10.8 255.255.255.0
[SwitchA-Vlanif2] quit
[SwitchA]
```

配置 Telnet 服务器 SwitchB 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 2
[SwitchB-Vlanif2] ip address 10.10.10.9 255.255.255.0
[SwitchB-Vlanif2] quit
[SwitchB]
```

步骤 2 配置 Telnet 服务器 SwitchB 的 Telnet 验证方式和密码

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode password
[SwitchB-ui-vty0-4] set authentication password simple 123456
[SwitchB-ui-vty0-4] quit
[SwitchB]
```

步骤 3 检查配置结果

从 SwitchA 上 Telnet 到 SwitchB。

```
<SwitchA> telnet 10.10.10.9
Trying 10.10.10.9 ...
```


版权所有 © 华为技术有限公司

```
Press CTRL+K to abort
Connected to 10.10.10.9 ...

Login authentication


Password:
info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<SwitchB>
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2
#
interface Vlanif2
 ip address 10.10.10.8 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2
#
interface Vlanif2
 ip address 10.10.10.9 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
user-interface vty 0 4
set authentication password simple 123456
#
return
```

配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例

配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例。在本示例中，通过在 SSH 服务器端生成本地密钥对，并在 SSH 服务器端配置 SSH 用户的用户名和密码，使能 Stelnet 服务，实现 Stelnet 客户端连接 SSH 服务器。

组网需求

如图 1-20 所示，SSH 服务器端 STelnet 服务使能后，STelnet 客户端可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

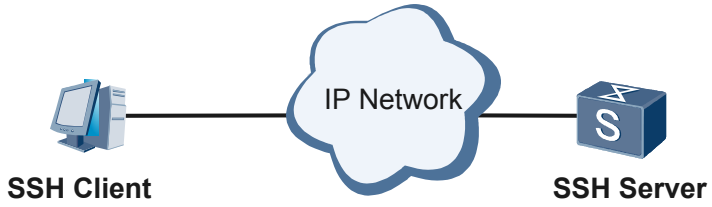
配置登录用户 Client001，密码为“huawei”，登录验证方式为 password。

服务器端 IP 地址是 192.168.1.1。

用户界面仅支持 SSH 协议。

版权所有 © 华为技术有限公司

图 1-20 配置 PC 作为 STelnet 客户端连接 SSH 服务器组网图



配置思路

采用如下的思路配置 PC 作为 STelnet 客户端连接 SSH 服务器：

1. 用户 Client001 的配置在 SSH 服务器上完成。
2. SSH 服务器端 STelnet 服务使能。
3. 配置 SSH 服务器端缺省的认证方式为 password。

数据准备

为完成此配置例，需准备如下的数据：

- SSH 用户名及认证方式。
- SSH 用户密码。
- SSH 服务器名。

操作步骤

步骤 1 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.......++++++++++++
..........++++++++++++
.....................................++++++++
......++++++++
```

步骤 2 在服务器端配置 VTY 用户界面

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

说明

若配置登录协议为 SSH，则 AC6605 设备将自动禁止 Telnet 功能。

步骤 3 在服务器端配置 SSH 用户的用户名和密码

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password cipher huawei
[SSH Server-aaa] local-user client001 privilege level 3
```


版权所有 © 华为技术有限公司

```
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
```

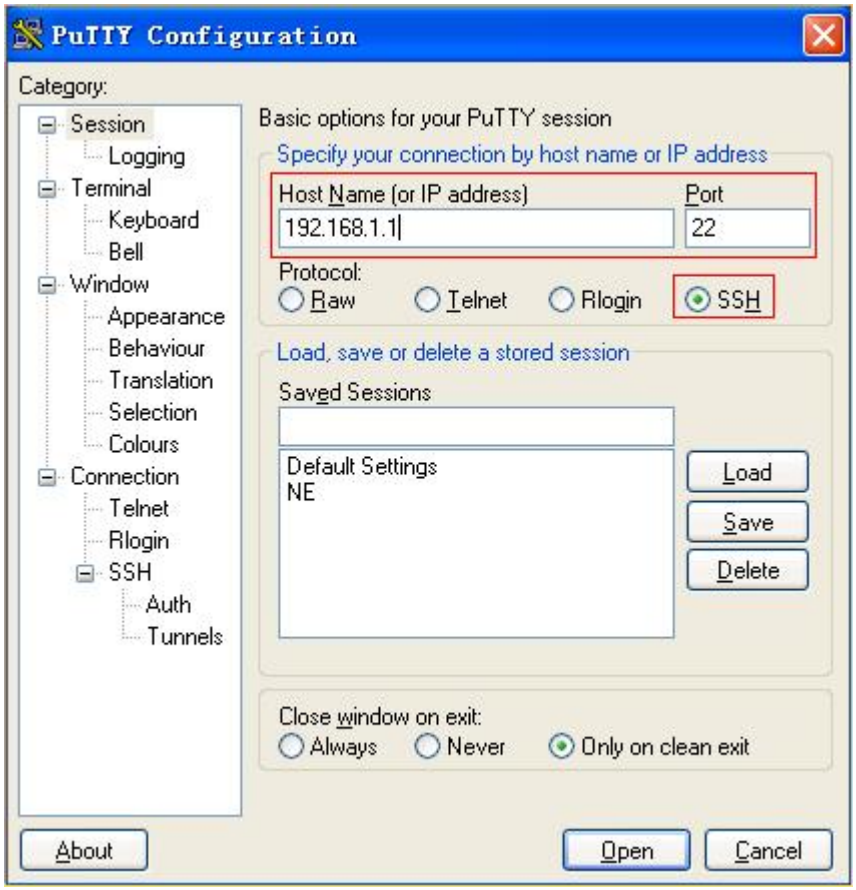
步骤 4 使能 STelent 功能，并配置用户的服务类型为 STelnet

```
[SSH Server] stelnet server enable
[SSH Server] ssh authentication-type default password
```

步骤 5 验证配置结果

通过 putty 软件登录设备，指定设备的 IP 地址 192.168.1.1，并指定登录方式为 SSH。

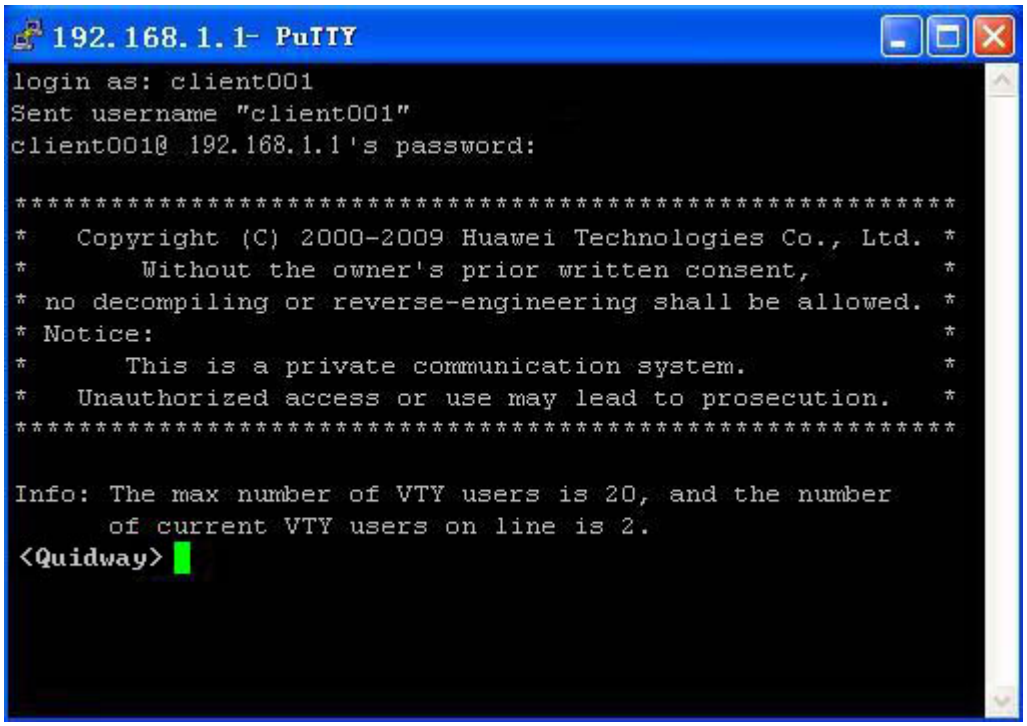
图 1-21 putty 软件配置界面



通过 putty 软件登录设备，输入用户名和密码，用户名 client001，密码 huawei。

版权所有 © 华为技术有限公司

图 1-22 putty 软件登录界面



----结束

配置文件

- SSH 服务器的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
 stelnet server enable
 ssh authentication-type default password
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

配置交换机作为 STelnet 客户端连接 SSH 服务器的示例

在本示例中，通过在 STelnet 客户端和 SSH 服务器端生成本地密钥对，在 SSH 服务器端生成 RSA 公钥、并为用户绑定该 RSA 公钥，实现 Stelnet 客户端连接 SSH 服务器。

组网需求

当需要从一台交换机登录到其他交换机进行配置时，可以配置交换机作为 STelnet 客户端连接待配置的交换机。

版权所有 © 华为技术有限公司

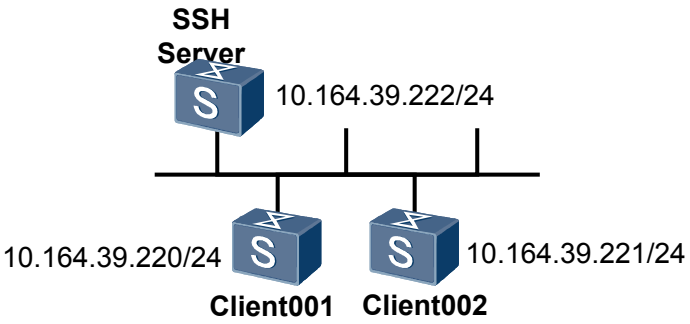
如图 1-23 所示，SSH 服务器端 STelnet 服务使能后，STelnet 客户端可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

配置两个登录用户：

- 用户 Client001，密码为 huawei，登录验证方式为 password。
- 用户 Client002，验证方式为 RSA，并为其分配公钥 RsaKey001。

用户界面仅支持 SSH 协议。

图 1-23 配置 STelnet 客户端连接 SSH 服务器组网图



Switch	接口	对应的 VLANIF	IP 地址
SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

配置思路

采用如下的思路配置 STelnet 客户端连接 SSH 服务器：

1. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。
2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 STelnet 客户端和 SSH 服务器端生成本地密钥对。
4. 在 SSH 服务器端生成 RSA 公钥，并为用户 Client002 绑定 SSH 客户端的 RSA 公钥。
5. SSH 服务器端 STelnet 服务使能。
6. 用户 Client001 和 Client002 分别以 STelnet 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 1-23。
- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- SSH 服务器名。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置接口 VLANIF10 的 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.......++++++++++++
..........++++++++++++
.................................++++++++
......++++++++
```

步骤 3 在服务器端创建 SSH 用户

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式:

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户;
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

- 创建 SSH 用户 Client001。

  # 新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

  ```
  [Quidway] ssh user client001
  [Quidway] ssh user client001 authentication-type password
  ```

  # 为 SSH 用户 Client001 配置密码为 huawei。

  ```
  [Quidway] aaa
  [Quidway-aaa] local-user client001 password simple huawei
  [Quidway-aaa] local-user client001 service-type ssh
  ```

- 新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA。

  ```
  [Quidway] ssh user client002
  [Quidway] ssh user client002 authentication-type rsa
  ```

步骤 4 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname client002
[client002] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001

Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b rsa-key

=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client002]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 5 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥

```
[Quidway] ssh user client002 assign rsa-key RsaKey001
```


版权所有 © 华为技术有限公司

步骤 6 SSH 服务器端 STelnet 服务使能

使能 STelnet 服务功能。

```
[Quidway] stelnet server enable
```

步骤 7 配置 SSH 用户 Client001、Client002 的服务方式为 STelnet

```
[Quidway] ssh user client001 service-type stelnet
[Quidway] ssh user client002 service-type stelnet
```

步骤 8 STelnet 客户端连接 SSH 服务器

第一次登录，需要使能 SSH 客户端首次认证功能。

```
[client001] ssh client first-time enable
[client002] ssh client first-time enable
```

STelnet 客户端 Client001 用 password 认证方式连接 SSH 服务器，输入配置的用户名和密码。

```
<client001> system-view
[client001] stelnet 10.164.39.222
Please input the username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
The server is not authenticated. Continue to access it?(Y/N):y
Save the server's public key?(Y/N):y
The server's public key will be saved with the name: 10.164.39.222. Please wait...
Enter password:
```

输入密码 huawei，显示登录成功信息如下：

```
info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

STelnet 客户端 Clent002 用 RSA 认证方式连接 SSH 服务器。

```
<client002> system-view
[client002] stelnet 10.164.39.222
Please input the username: client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...

info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

步骤 9 检查配置结果

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令和 **display ssh server session** 命令，可以查看到 STelnet 服务已经使能，并且 STelnet 客户端已经成功连接到 SSH 服务器。

查看 SSH 状态信息。

```
[Quidway] display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP server                          :Disable
 Stelnet server                       :Enable
 Scp server                           :Disable
```


版权所有 © 华为技术有限公司

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: password
Session 1:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: rsa
```

查看 SSH 用户信息。

```
[Quidway] display ssh user-information
User 1:
       User Name: client001
       Authentication-type: password
       User-public-key-name: -
       Sftp-directory: -
       Service-type: stelnet
       Authorization-cmd: No
  User 2:
       User Name: client002
       Authentication-type: rsa
       User-public-key-name: RsaKey001
       Sftp-directory: -
       Service-type: stelnet
       Authorization-cmd: No
```

----结束

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 rsa peer-public-key rsakey001
  public-key-code begin
    3047
      0240
BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB 203C8FCB BBC8FDF2 F7CB674E
       519E8419 0F6B97A8 EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43 1D7E3E1B      0203
       010001
```


版权所有 © 华为技术有限公司

```
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password simple huawei
 local-user client001 service-type ssh
#
stelnet server enable
 ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
 ssh user client001 service-type stelnet
 ssh user client002 service-type stelnet
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Client001 的配置文件

```
#
 sysname client001
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Client002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置 SFTP 客户端连接 SSH 服务器的示例

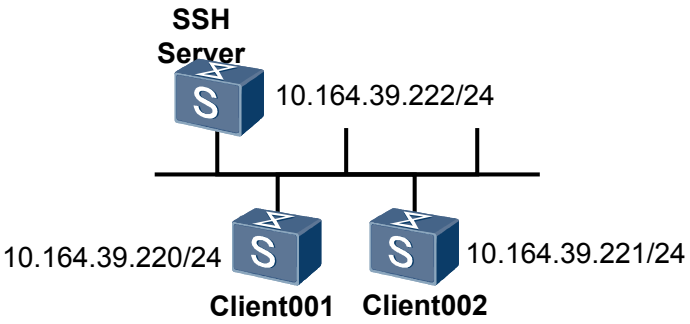
在本示例中，通过在 SFTP 客户端和 SSH 服务器端生成本地密钥对，在 SSH 服务器端生成 RSA 公钥、并为用户绑定该 RSA 公钥，实现 SFTP 客户端连接 SSH 服务器。

版权所有 © 华为技术有限公司

组网需求

如图 1-24 所示，SSH 服务器端 SFTP 服务使能后，SFTP Client 端可以通过 Password、RSA、password-rsa、all 认证的方式登录到 SSH 服务器端。

图 1-24 配置 SFTP 客户端连接 SSH 服务器组网图



Switch	接口	对应的 VLANIF	IP 地址
SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

配置思路

采用如下思路配置 SFTP 客户端连接 SSH 服务器的示例：

1. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。
2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 SFTP 客户端和 SSH 服务器端生成本地密钥对。
4. 在 SSH 服务器端生成 RSA 公钥，并为用户 Client002 绑定 SSH 客户端的 RSA 公钥。
5. SSH 服务器端 SFTP 服务使能。
6. 配置 SSH 用户的服务方式和授权目录。
7. 用户 Client001 和 Client002 分别以 SFTP 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 1-24。
- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- SSH 服务器名。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
```

步骤 3 在服务器端创建 SSH 用户

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式:

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户;
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

- 创建 SSH 用户 Client001。

  # 新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

  ```
  [Quidway] ssh user client001
  [Quidway] ssh user client001 authentication-type password
  ```

  # 为 SSH 用户 Client001 配置密码为 huawei。

  ```
  [Quidway] aaa
  [Quidway-aaa] local-user client001 password simple huawei
  [Quidway-aaa] local-user client001 service-type ssh
  ```

- 新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA。

  ```
  [Quidway] ssh user client002
  [Quidway] ssh user client002 authentication-type rsa
  ```

步骤 4 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname client002
[client002] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b rsa-key

=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 5 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥

```
[Quidway] ssh user client002 assign rsa-key RsaKey001
```

步骤 6 SSH 服务器端 SFTP 服务使能

使能 SFTP 服务功能

版权所有 © 华为技术有限公司

```
[Quidway] sftp server enable
```

步骤 7 在 SSH 服务器端配置 SSH 用户的服务方式和授权目录

目前 SSH 服务器端已配置了两个 SSH 用户：Client001 和 Client002，Client001 的认证方式是 password，Client002 的认证方式是 RSA。

```
[Quidway] ssh user client001 service-type sftp
[Quidway] ssh user client001 sftp-directory flash:/
[Quidway] ssh user client002 service-type sftp
[Quidway] ssh user client002 sftp-directory flash:/
```

步骤 8 SFTP 客户端连接 SSH 服务器

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client001] ssh client first-time enable
[client002] ssh client first-time enable
```

SFTP 客户端 Client001 用 password 认证方式连接 SSH 服务器。

```
<client001> system-view
[client001] sftp 10.164.39.222
Input Username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Enter password:
sftp-client>
```

SFTP 客户端 Client002 用 RSA 认证方式连接 SSH 服务器。

```
<client002> system-view
[client002] sftp 10.164.39.222
Input Username: client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
sftp-client>
```

步骤 9 检查配置结果

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令和 **display ssh server session** 命令，可以查看到 SFTP 服务已经使能，并且 SFTP 客户端已经成功连接到 SSH 服务器。

查看 SSH 状态信息。

```
[Quidway] display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP server                          :Enable
 Stelnet server                       :Disable
 Scp server                           :Disable
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
```


版权所有 © 华为技术有限公司

```
       Kex: diffie-hellman-group1-sha1
       Service Type: sftp
       Authentication Type: password
Session 2:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: sftp
       Authentication Type: rsa
```

查看 SSH 用户信息。

```
[Quidway] display ssh user-information
User 1:
       User Name: client001
       Authentication-type: password
       User-public-key-name: -
       Sftp-directory: flash:
       Service-type: sftp
       Authorization-cmd: No
  User 2:
       User Name: client002
       Authentication-type: rsa
       User-public-key-name: RsaKey001
       Sftp-directory: flash:
       Service-type: sftp
       Authorization-cmd: No
```

----结束

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 rsa peer-public-key rsakey001
  public-key-code begin
   3047
     0240
       C4989BF0 416DA8F2 2675910D 7F2997E8 5573A35D 0163FD4A FAC39A6E 0F45F325
       A4E3AA1D 54692B04 C6A28D3D C58DE2E8 E0D58D65 7A25CF92 A74D21F9 E917182B
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password simple huawei
 local-user client001 service-type ssh
#
sftp server enable
 ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type rsa
```


版权所有 © 华为技术有限公司

```
 ssh user client002 assign rsa-key RsaKey001
 ssh user client001 service-type sftp
 ssh user client002 service-type sftp
 ssh user client001 sftp-directory flash:/
 ssh user client002 sftp-directory flash:/
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Clien001 的配置文件

```
#
 sysname client001
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Clien002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置 SSH 服务器支持其他端口号访问的示例

配置 SSH 服务器支持其他端口号访问的示例。在本示例中，通过设定 SSH 服务器端的监听端口号为其他端口号，实现只有合法的用户才能建立 SSH 连接。

组网需求

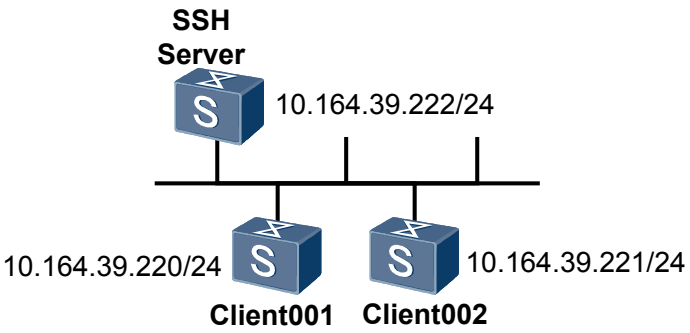
SSH 协议的标准监听端口号为 22，如果攻击者不断访问标准端口，将导致带宽和服务器性能的下降，从而导致其他正常用户无法访问。

通过设定 SSH 服务器端的监听端口号为其他端口号，攻击者不知道 SSH 监听端口号的更改，仍然发送标准端口号 22 的 socket 连接，SSH 服务器检测发现请求连接端口号不是监听的端口号，就不建立 socket 连接。

版权所有 © 华为技术有限公司

这样只有合法的用户采用 SSH 服务器设定的非标准监听端口才能建立 socket 连接，进行 SSH 协议的版本号协商、算法协商及会话密钥生成、认证、会话请求、会话阶段等过程。

图 1-25 配置 SSH 服务器支持其他端口号访问组网图



Switch	接口	对应的 VLANIF	IP 地址
SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

配置思路

采用如下的思路配置 SSH 服务器支持其他端口号访问的示例：

1. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。
2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 SFTP 客户端和 SSH 服务器端生成本地密钥对。
4. 在 SSH 服务器端生成 RSA 公钥，并为用户 Client002 绑定 SSH 客户端的 RSA 公钥。
5. SSH 服务器端 STelnet 和 SFTP 服务使能。
6. 配置 SSH 用户的服务方式和授权目录。
7. 设置 SSH 服务器端监听端口号。
8. 用户 Client001 和 Client002 分别以 STelnet 和 SFTP 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 1-25。
- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- 服务器名。
- SSH 服务器端监听端口号。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
[Quidway-Vlanif10] quit
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
```

步骤 3 配置服务器端 RSA 公钥

在客户端生成客户端的本地密钥对

```
<Quidway> system-view
[Quidway] sysname client002
[client002] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001

Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
```


版权所有 © 华为技术有限公司

```
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b rsa-key

=============================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Server
Key type: RSA encryption Key
=============================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client002]
```

在服务器端将客户端上产生的 RSA 公钥传送到服务器端。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 4 在服务器端创建 SSH 用户

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式。

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户；
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

创建 SSH 用户 Client001，新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

```
[Quidway] ssh user client001
[Quidway] ssh user client001 authentication-type password
```

为 SSH 用户 Client001 配置密码为 huawei。

```
[Quidway] aaa
[Quidway-aaa] local-user client001 password simple huawei
[Quidway-aaa] local-user client001 service-type ssh
[Quidway-aaa] quit
```

配置 Client001 的服务方式为 STelnet。

```
[Quidway] ssh user client001 service-type stelnet
```


版权所有 © 华为技术有限公司

新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA，并绑定 SSH 客户端 RSA 公钥。

```
[Quidway] ssh user client002
[Quidway] ssh user client002 authentication-type rsa
[Quidway] ssh user client002 assign rsa-key RsaKey001
```

配置 Client002 的服务方式为 SFTP，授权目录为 flash:/。

```
[Quidway] ssh user client002 service-type sftp
[Quidway] ssh user client002 sftp-directory flash:/
```

步骤 5 SSH 服务器端使能 STelent 和 SFTP 服务

```
[Quidway] stelnet server enable
[Quidway] sftp server enable
```

步骤 6 配置 SSH 服务端新的监听端口号

```
[Quidway] ssh server port 1025
```

步骤 7 SSH 客户端连接 SSH 服务器

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client001] ssh client first-time enable
[client002] ssh client first-time enable
```

STelnet 客户端用新端口号连接 SSH 服务器。

```
[client001] stelnet 10.164.39.222 1025
Please input the username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
he server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
he server's public key will be saved with the name: 10.164.39.222. Please wait...
Enter password:
```

输入密码 huawei，显示登录成功信息如下：

```
info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

SFTP 客户端用新端口号连接 SSH 服务器。

```
[client002]sftp 10.164.39.222 1025
Please input the username:client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
The server's public key does not match the one we cached.
The server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to update the server's public key we cached?(Y/N):y
sftp-client>
```

步骤 8 检查配置结果

攻击者使用原端口号 22 访问 SSH 服务器，不能成功。

```
[client002] sftp 10.164.39.222
Please input the username:client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
Can't establish tcp connection to server
```


版权所有 © 华为技术有限公司

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令和 **display ssh server session** 命令，可以查看到 SSH 服务器端当前监听端口号，并且 STelnet 客户端或 SFTP 客户端已经成功连接到 SSH 服务器。

查看 SSH 状态信息。

```
[Quidway] display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP server                          :Enable
 Stelnet server                       :Enable
 Scp server                           :Disable
 SSH server port                      :1025
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: password
Session 2:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: sftp
       Authentication Type: rsa
```

----结束

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 rsa peer-public-key rsakey001
  public-key-code begin
   3047
     0240
       C4989BF0 416DA8F2 2675910D 7F2997E8 5573A35D 0163FD4A FAC39A6E 0F45F325
       A4E3AA1D 54692B04 C6A28D3D C58DE2E8 E0D58D65 7A25CF92 A74D21F9 E917182B
     0203
       010001
```


版权所有 © 华为技术有限公司

```
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password simple huawei
 local-user client001 service-type ssh
#
 sftp server enable
 stelnet server enable
 ssh server port 1025
 ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
 ssh user client001 service-type stelnet
 ssh user client002 service-type sftp
 ssh user client002 sftp-directory flash:/
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Clien001 的配置文件

```
#
 sysname client001
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
 ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Clien002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
 ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置 SSH 支持 RADIUS 认证的示例

配置 SSH 支持 RADIUS 认证的示例。在本示例中，通过 RADIUS 服务器认证用户信息，实现 SSH 服务器根据认证结果决定是否允许 SSH 客户端建立连接。

版权所有 © 华为技术有限公司

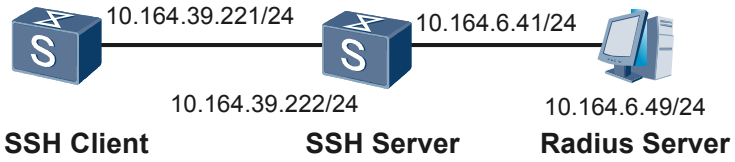
组网需求

如果 RADIUS 用户连接 SSH 服务器，那么在 SSH 认证过程中，SSH 服务器将 SSH 客户端的认证信息（用户名、密码）发送给 RADIUS 服务器（兼容 TACACS 服务器）进行认证。

RADIUS 服务器认证该用户，将认证结果（成功、失败，如果成功还包含用户等级）返回给 SSH 服务器。SSH 服务器根据认证结果决定是否允许 SSH 客户端建立连接。

组网图如图 1-26 所示。

图 1-26 配置 SSH 支持 RADIUS 认证组网图



配置思路

采用如下的思路配置 SSH 支持 RADIUS 认证的示例：

1. SSH 服务器端配置 RADIUS 模板。
2. SSH 服务器端配置域。
3. RADIUS 服务器创建用户。
4. 分别在 STelnet 客户端和 SSH 服务器端生成本地密钥对。SSH 服务器端监听端口号。
5. 分别在客户端和 SSH 服务器端生成本地密钥对。
6. 在 SSH 服务器端生成 RSA 公钥，并为用户 ssh2@ssh.com 绑定 SSH 客户端的 RSA 公钥。
7. SSH 服务器端 STelnet 和 SFTP 服务使能。
8. 配置 SSH 用户的服务方式和授权目录。
9. 用户 ssh1@ssh.com 和 ssh2@ssh.com 分别以 STelnet 和 SFTP 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- 配置两个 SSH 用户采用的认证方式是 Password。
- 认证模式为 RADIUS。
- RADIUS 模板名称。
- RADIUS 域名称。
- RADIUS 用户名称和密码。

操作步骤

步骤 1 在 SSH 服务器端生成本地密钥对

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.......++++++++++++
..........++++++++++++
.................................++++++++
......++++++++
```

步骤 2 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

```
<Quidway> system-view
[Quidway] sysname client
[client] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client] display rsa local-key-pair public
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: Quidway_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b rsa-key
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: Quidway_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
```


版权所有 © 华为技术有限公司

```
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 3 创建 SSH 用户

在 RADIUS 服务器端，添加两个用户，用户名分别为 ssh1@ssh.com 和 ssh2@ssh.com；另外还须指定 NAS 的地址 10.164.39.222 和密钥 huawei。NAS 的地址是指和 RADIUS 服务器连接的 SSH 服务器的地址。

在 SSH 服务器端配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

在 SSH 服务器端创建 SSH 用户 ssh1@ssh.com 和 ssh2@ssh.com。

```
[Quidway] ssh user ssh1@ssh.com
[Quidway] ssh user ssh1@ssh.com authentication-type password
[Quidway] ssh user ssh1@ssh.com service-type stelnet
[Quidway] ssh user ssh2@ssh.com
[Quidway] ssh user ssh2@ssh.com authentication-type password
[Quidway] ssh user ssh2@ssh.com service-type sftp
[Quidway] ssh user client001 sftp-directory flash:/
```

步骤 4 配置 RADIUS 模板

配置认证方案 newscheme，认证方法为 RADIUS。

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme newscheme
[Quidway-aaa-authen-newscheme] authentication-mode radius
[Quidway-aaa-authen-newscheme] quit
```

配置 SSH 服务端的 RADIUS 模板为 ssh。

```
[Quidway] radius-server template ssh
```

配置 RADIUS 认证服务器的 IP 地址为 10.164.6.49 和端口 1812。

```
[Quidway-radius-ssh] radius-server authentication 10.164.6.49 1812
```

配置 RADIUS 服务器密钥为 huawei。

```
[Quidway-radius-ssh] radius-server shared-key huawei
[Quidway-radius-ssh] quit
```

步骤 5 配置 RADIUS 域名

配置 SSH 服务端的 RADIUS 域名为 ssh.com，在域下应用认证方案 newscheme、RADIUS 模板 ssh。

```
[Quidway] aaa
[Quidway-aaa] domain ssh.com
[Quidway-aaa-domain-ssh.com] authentication-scheme newscheme
[Quidway-aaa-domain-ssh.com] radius-server ssh
[Quidway-aaa-domain-ssh.com] quit
[Quidway-aaa] quit
```

步骤 6 SSH 客户端连接 SSH 服务器。

版权所有 © 华为技术有限公司

使能 SSH 服务器端的 STelnet 和 SFTP 服务功能。

```
[Quidway] stelnet server enable
[Quidway] sftp server enable
```

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client] ssh client first-time enable
[client] quit
```

STelnet 客户端采用 RADIUS 认证连接 SSH 服务器。

```
<client> system-view
[client] stelnet 10.164.39.222
Please input the username: ssh1@ssh.com
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
The server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
The server's public key will be saved with the name: 10.164.39.222. Please wait...
Enter password:
```

输入密码 huawei，显示登录成功信息如下：

```
Info: The max number of VTY users is 10, and the current number
      of VTY users on line is 2.
<Quidway>
```

SFTP 客户端采用 RADIUS 认证连接 SSH 服务器。

```
<client> system-view
[client] sftp 10.164.39.222
Please input the username: ssh2@ssh.com
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
Enter password:
sftp-client>
```

步骤 7 检查配置结果

配置完成后，在 SSH 服务器端执行 **display radius-server configuration** 命令和 **display ssh server session** 命令，可以查看到 SSH 服务器端关于 RADIUS 服务器的配置，并且看到 STelnet 客户端或 SFTP 客户端采用 RADIUS 认证已经成功连接到 SSH 服务器。

查看 RADIUS 服务器的配置信息。

```
[Quidway-aaa] display radius-server configuration
-------------------------------------------------------------------
  Server-template-name            :  ssh
  Protocol-version                :  standard
  Traffic-unit                    :  B
  Shared-secret-key               :  huawei
  Timeout-interval(in second)     :  5
  Primary-authentication-server   :  10.164.6.49   :1812    LoopBack:NULL
  Primary-accounting-server       :  0.0.0.0       :0       LoopBack:NULL
  Secondary-authentication-server :  0.0.0.0       :0       LoopBack:NULL
  Secondary-accounting-server     :  0.0.0.0       :0       LoopBack:NULL
  Retransmission                  :  3
  Domain-included                 :  YES
  Calling-station-id MAC-format   :  xxxx-xxxx-xxxx
  -----------------------------------------------------------------
  Total of radius template :1
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
```


版权所有 © 华为技术有限公司

```
      Conn                : VTY 0
      Version             : 2.0
      State               : started
      Username            : ssh1@ssh.com
      Retry               : 1
      CTOS Cipher         : aes128-cbc
      STOC Cipher         : aes128-cbc
      CTOS Hmac           : hmac-sha1-96
      STOC Hmac           : hmac-sha1-96
      Kex                 : diffie-hellman-group1-sha1
      Service Type        : stelnet
      Authentication Type : password
  Session 2:
      Conn                : VTY 1
      Version             : 2.0
      State               : started
      Username            : ssh2@ssh.com
      Retry               : 1
      CTOS Cipher         : aes128-cbc
      STOC Cipher         : aes128-cbc
      CTOS Hmac           : hmac-sha1-96
      STOC Hmac           : hmac-sha1-96
      Kex                 : diffie-hellman-group1-sha1
      Service Type        : sftp
      Authentication Type : password
```

----结束

配置文件

SSH 服务器的配置文件

```
#
 sysname Quidway
#
radius-server template ssh
 radius-server authentication 10.164.6.49 1812
#
 rsa peer-public-key rsakey001
  public-key-code begin
   3047
     0240
       C4989BF0 416DA8F2 2675910D 7F2997E8 5573A35D 0163FD4A FAC39A6E 0F45F325
       A4E3AA1D 54692B04 C6A28D3D C58DE2E8 E0D58D65 7A25CF92 A74D21F9 E917182B
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
authentication-scheme newscheme
authentication-mode  radius
 #
 domain ssh.com
  authentication-scheme newscheme
  radius-server ssh
 #
#
sftp server enable
stelnet server enable
 ssh user ssh1@ssh.com
 ssh user ssh2@ssh.com
 ssh user ssh1@ssh.com authentication-type password
 ssh user ssh2@ssh.com authentication-type password
 ssh user ssh2@ssh.com assign rsa-key RsaKey001
 ssh user ssh1@ssh.com service-type stelnet
 ssh user ssh2@ssh.com service-type sftp
ssh user client001 sftp-directory flash:/
#
```


版权所有 © 华为技术有限公司

```
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

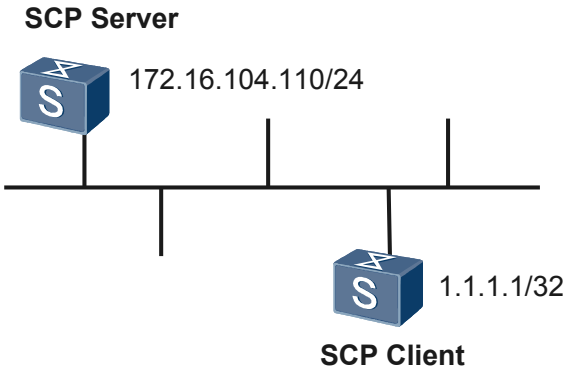
配置 SCP 客户端示例

配置 SCP 客户端的示例。在本示例中，通过登录 SCP 服务器，实现从 SCP 服务器中下载文件至客户端。

组网需求

如图 1-27 所示，作为 SCP 客户端的交换机和服务器路由可达，并从 SCP 服务器中下载文件至客户端。

图 1-27 配置 SCP 客户端组网图



配置思路

采用如下的思路配置 SCP 客户端功能：

1. 在 SSH 服务器端生成本地密钥对。
2. 在 SSH 服务器端创建 SSH 用户。
3. 在 SSH 服务器端使能 SCP 功能。
4. 使能客户端首次认证功能。
5. 在 SCP 客户端指定源接口 IP 地址，从 SSH 服务器下载文件至本地。

数据准备

为完成此配置例，需准备如下的数据：

- SSH 用户名、认证方式和认证密码。
- SCP 客户端源接口 IP 地址。
- 源文件名及路径和目标文件名及路径。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: SSH Server_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 512
Generating keys...
.....++++++++++++
....++++++++++++
......++++++++
..............................++++++++
```

步骤 2 在服务器端创建 SSH 用户

配置 VTY 用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

```
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
```

为 SSH 用户 Client001 配置密码为 huawei。

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password cipher huawei
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
```

配置 SSH 用户 client001 的服务方式为 all。

```
[SSH Server] ssh user client001 service-type all
```

步骤 3 在服务器端使能 SCP 服务

```
[SSH Server] scp server enable
```

步骤 4 从 SCP 客户端下载服务器上的文件。

第一次登录，需要使能 SSH 客户端首次认证功能。

```
<Quidway> system-view
[Quidway] sysname SCP Client
[SCP Client] ssh client first-time enable
```

设置 SCP 客户端的源地址为 LoopBack 接口 IP 地址 1.1.1.1。

```
[SCP Client] scp client-source -a 1.1.1.1
```

使用 3des 加密算法将文件 license.txt 从 IP 地址为 172.16.104.110 的远端 SCP 服务器下载至本地用户目录下。

```
[SCP Client] scp -a 1.1.1.1 -cipher 3des client001@172.16.104.110:license.txt license.txt
```

步骤 5 验证配置结果

在 SCP 客户端执行 **display scp-client** 命令，查看结果如下：

```
<Quidway> display scp-client
```


版权所有 © 华为技术有限公司

```
The source of SCP ipv4 client: 1.1.1.1
```

可以看到 SCP 客户端源 IP 地址为 1.1.1.1。

----结束

配置文件

- SCP 服务器上的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password simple huawei
 local-user client001 service-type ssh
#
 scp server enable
 ssh user client001
 ssh user client001 authentication-type password
 ssh user client001 service-type all
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SCP 客户端上的配置文件

```
#
 sysname SCP Client
#
 ssh client first-time enable
 scp client-source 1.1.1.1
#
return
```

1.10 SSL 配置

安全套接层 SSL（Secure Sockets Layer）可对用户和服务器之间传送的数据进行加密和鉴别，实现合法用户安全登录服务器。

1.10.1 SSL 概述

当前，SSL 只支持应用于 FTPS 和 HTTPS（安全 Web 网管）。

概述

SSL 协议是在 Internet 基础上提供的一种保证私密性的安全协议。它能使客户端与服务器之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 利用数据加密、身份验证和消息完整性验证机制，为基于 TCP 可靠连接的应用层协议提供安全性保证。SSL 具有以下优点：

- 提供较高的安全性保证。SSL 利用数据加密、身份验证和消息完整性验证机制，保证网络上数据传输的安全性。
- 支持各种应用层协议。虽然 SSL 设计的初衷是为了解决万维网安全性问题，但是由于 SSL 位于应用层和传输层之间，它可以为任何基于 TCP 等可靠连接的应用层协议提供安全性保证。

版权所有 © 华为技术有限公司

- 部署简单。目前 SSL 已经成为网络中用来鉴别网站和网页浏览者身份，在浏览器使用者及 Web 服务器之间进行加密通信的全球化标准。

SSL 从以下几方面提高了设备的安全性：

- 通过 SSL 协议保证合法客户端可以安全地访问服务器，禁止非法的客户端访问服务器。
- 客户端与服务器之间交互的数据需要经过加密和摘要，加密保证了传输的安全性，摘要保证了数据的完整性，从而实现了对设备的安全管理。
- 为设备制定基于证书属性的访问控制策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击。

基本概念

- CA（Certificate Authority）

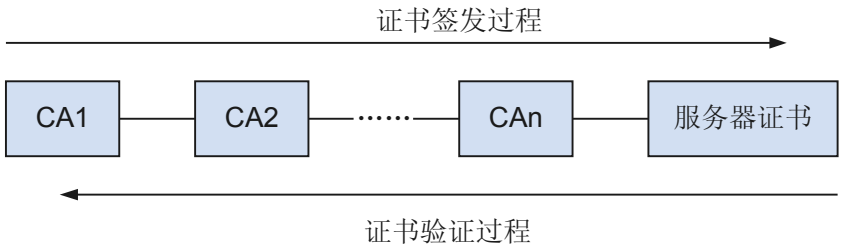
  CA 是发放、管理、废除数字证书的机构。CA 的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的 CA，被称之为根 CA。根 CA 可授权其它 CA 为其下级 CA。CA 的身份也需要证明，而证明信息在信任证书机构文件中描述。

  例如：CA1 作为最上级 CA 也叫根证书，签发下一级 CA2 证书，CA2 又可以给它的下一级 CA3 签发证书，以此下去，最终由 CAn 签发服务器的证书。

  如果服务器端的证书由 CA3 签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。先由 CA3 证书验证服务器端证书的有效性，如果通过则再由 CA2 证书验证 CA3 证书的有效性，最后由最上级 CA1 证书验证 CA2 证书的有效性。只有通过最上级 CA 证书即根证书的验证，服务器证书才会验证成功。

  证书签发过程与证书验证过程如图 1-28 所示。

  图 1-28 证书签发过程与证书验证过程示意图

- 数字证书

  数字证书实际上是存于计算机上的一个记录，是由 CA 签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的 CA 的数字签名及数字证书的有效期等内容。数字证书的作用使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

  用户必须事先获取信息发送者的公钥证书，以便对信息进行解码认证，同时还需要 CA 发送给发送者的证书，以便用户验证发送者的身份。

- 证书撤销列表 CRL（Certificate Revocation List）

  CRL 由 CA 发布，它指定了一套证书发布者认为无效的证书。

  数字证书的寿命是有限的，但 CA 可通过证书撤销过程缩短证书的寿命。CRL 指定的寿命通常比数字证书指定的寿命要短。由 CA 撤销数字证书，意味着 CA 在数字

版权所有 © 华为技术有限公司

证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL 中的有关数据被删除，以缩短 CRL 列表的大小。

在使用每个数字证书前，客户端一定会检查相应的 CRL。如果检查到数字证书在 CRL 中指定，CA 在数据库中将该数字证书标记为作废标志，并在下次发布 CRL 时加入证书作废列表。在 CRL 中的证书作废列表到期后即可删除。

1.10.2 AC6605 支持的 SSL 特性

当前，SSL 只支持应用于 FTPS 和 HTTPS（安全 Web 网管）。

FTPS

FTPS 是基于 SSL 安全连接的 FTP 协议。

FTPS 通过 SSL 提供的数据加密、身份验证和消息完整性验证等安全机制，为 FTP 服务器访问提供了安全性保证。

- 通过用户终端登录 FTP 服务器

  在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能后，用户在终端通过支持 SSL 的 FTP 客户端软件登录安全 FTP 服务器，在终端与服务器之间实现文件的安全管理操作。
- 通过 FTP 客户端登录 FTP 服务器
  - 在作为 FTP 客户端的设备上部署 SSL 策略并加载信任证书机构文件，检查证书持有者身份的合法性，并签发证书，以防证书被伪造或篡改，以及对证书和密钥进行管理。
  - 在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能，检查信任证书机构文件的合法性，保证合法客户端安全登录服务器。

HTTPS

HTTPS 是基于 SSL 安全连接的 HTTP 协议。

HTTPS 通过 SSL 提供的数据加密、身份验证和消息完整性验证等安全机制，为 Web 访问提供了安全性保证。

在作为 HTTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 HTTP 服务器功能后，用户可通过 HTTPS 登录服务器，利用 Web 页面安全管理远程设备。

1.10.3 通过用户终端登录 FTPS 服务器

FTPS 将 FTP 和 SSL（Secure Sockets Layer，安全套接层）结合，通过 SSL 对客户端身份和服务器进行验证，对传输的数据进行加密，从而实现了对设备的安全管理。

建立配置任务

在配置通过用户终端登录 FTPS 服务器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

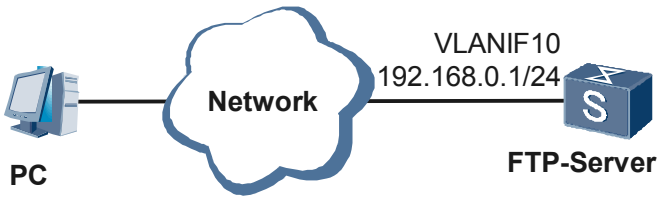
传统的 FTP 不具备安全机制，采用明文的形式传输数据。如果 FTP 服务器设置了登录用户名和密码，则 FTP 服务器可以验证客户端的身份，但是客户端不能验证服务器的身

版权所有 © 华为技术有限公司

份，无法防止传输的数据被篡改等，存在很大的安全隐患。在 FTP 服务器上部署 SSL 策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL 可以为 FTP 服务器提供安全连接，从而很大程度上改善了 FTP 服务器安全性问题。

如图 1-29 所示，在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能后，用户在终端通过支持 SSL 的 FTP 客户端软件登录安全 FTP 服务器，在终端与服务器之间实现文件的安全管理操作。

图 1-29 通过终端登录 FTPS 服务器组网图



前置任务

在配置通过用户终端登录 FTPS 服务器之前，需要完成以下任务：

- 数字证书已经上传到作为 FTPS 服务器的设备上，并已经拷贝到系统目录下名为 security 的子目录内。
- PC 上已经安装支持 SSL 的 FTP 客户端软件。

数据准备

在配置通过用户终端登录 FTPS 服务器之前，需要准备以下数据。

序号	数据
1	SSL 策略名称、数字证书
2	FTPS 服务器的 IP 地址

配置 SSL 策略并加载数字证书

数字证书主要用来客户端对服务器端身份的验证，保证安全通信。

背景信息

FTPS 服务器需要从证书颁发中心 CA（Certificate Authority）获得数字证书，访问服务器的客户端也需要从 CA 得到 CA 证书，用来验证服务器数字证书的有效性。

说明

CA 是负责发放和管理数字证书的权威机构，当前 FTPS 服务器上加载的数字证书必须向 CA 申请。

数字证书格式分为 PEM 格式、ASN1 格式和 PFX 格式。虽然证书的格式不相同，但是证书的内容一样。

版权所有 © 华为技术有限公司

- PEM 格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem。
  PEM 格式适用于系统之间的文本模式传输。
- ASN1 是通用的数字证书格式之一，文件的扩展名是.der。
  ASN1 格式是大多数浏览器的默认格式。
- PFX 是通用的数字证书格式之一，文件的扩展名是.pfx。
  PFX 格式是可移植的格式，是二进制格式。

请在作为 FTPS 服务器的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name*，配置 SSL 策略并 SSL 策略视图。

步骤 3 加载数字证书。

以下步骤请根据数字证书格式任选其一执行：

- 执行命令 **certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书。
- 执行命令 **certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*，加载 ASN1 格式的证书。
- 执行命令 **certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac** *mac-code* | **key-file** *key-filename* } **auth-code** *auth-code*，加载 PFX 格式的证书。
- 执行命令 **certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书链。

说明

一个 SSL 策略只能加载一个证书或者证书链。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先卸载旧证书或者证书链。

----结束

使能 FTPS 功能

在 FTP 服务器上部署 SSL 策略，并使能安全 FTP 功能，FTPS 服务器将提供以 SSL 为基础的 FTP 服务功能。

背景信息

说明

使能 FTPS 服务功能，必须去使能普通 FTP 服务器功能。

请在作为 FTPS 服务器的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp secure-server ssl-policy** *policy-name*，为 FTP 服务器配置 SSL 策略。

步骤 3 执行命令 **ftp secure-server enable**，使能 FTPS 服务器功能。

版权所有 © 华为技术有限公司

缺省情况下，未使能 FTPS 服务器。

----结束

访问 FTPS 服务器

用户可以通过支持 SSL 的 FTP 客户端软件从 PC 访问 FTPS 服务器，或通过 FTPS 客户端访问 FTPS 服务器，实现对 FTPS 服务器进行文件的安全管理。

需要在用户终端安装支持 SSL 的 FTP 客户端软件，通过第三方软件从用户终端登录 FTPS 服务器，实现对 FTPS 服务器进行文件的安全管理。

检查配置结果

通过用户终端登录 FTPS 服务器成功配置后，可以查看到 FTPS 服务器上的 SSL 策略、加载的数字证书，及 FTPS 服务器状态信息等内容。

前提条件

已完成通过用户终端登录 FTPS 服务器的所有配置。

操作步骤

- 使用 **display ssl policy** 命令，查看配置的 SSL 策略及加载的数字证书。
- 使用 **display ftp-server** 命令，查看 SSL 策略名称、FTPS 服务器的状态。

----结束

任务示例

在 FTP 服务器上执行命令 **display ssl policy**，可以看到配置的 SSL 策略及加载的数字证书详细信息。

```
<Quidway> display ssl policy
       SSL Policy Name: ftp_server
     Policy Applicants: FTP secure-server
         Key-pair Type: RSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_rsa.pem
     Key-file Filename: 1_serverkey_pem_rsa.pem
             Auth-code: 123456
                   MAC:
              CRL File:
       Trusted-CA File:
```

在 FTP 服务器上执行命令 **display ftp-server**，可以看到 SSL 策略名称、FTPS 服务器的状态是 running。

```
<Quidway> display ftp-server
  FTP server is stopped
  Max user number                 5
  User count                      1
  Timeout value(in minute)        30
  Listening port                  21
  Acl number                      0
  FTP server's source address     0.0.0.0
  FTP SSL policy                  ftp_server
  FTP Secure-server is running
```


版权所有 © 华为技术有限公司

1.10.4 通过 FTPS 客户端登录 FTPS 服务器

FTPS 客户端和 FTPS 服务器互相验证身份，保证合法客户端可以安全地访问服务器，提高了访问可靠性。

建立配置任务

在配置通过 FTPS 客户端登录 FTPS 服务器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

传统的 FTP 不具备安全机制，采用明文的形式传输数据。如果 FTP 服务器设置了登录用户名和密码，则 FTP 服务器可以验证客户端的身份，但是客户端不能验证服务器的身份，无法防止传输的数据被篡改等，存在很大的安全隐患。

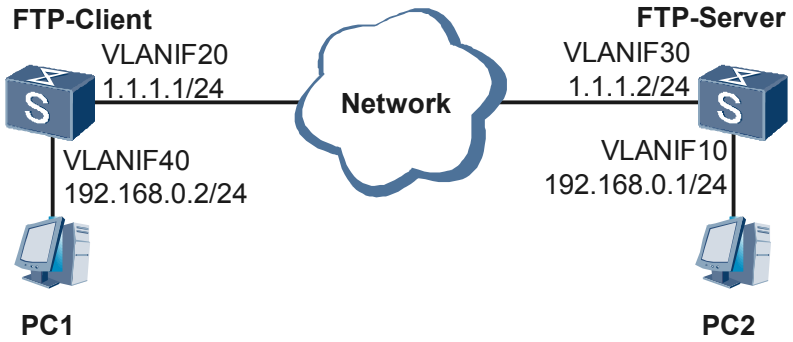
- 在 FTP 客户端配置 SSL 策略，并加载信任证书机构文件。
- 在 FTP 服务器配置 SSL 策略，并加载数字证书。

客户端通过信任证书机构文件和数字证书对服务器进行身份验证，保证合法客户端访问正确的服务器

如图 1-30 所示：

- 在作为 FTP 客户端的设备上部署 SSL 策略并加载信任证书机构文件，检查证书持有者身份的合法性，并签发证书，以防证书被伪造或篡改，以及对证书和密钥进行管理。
- 在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能，检查信任证书机构文件的合法性，保证合法客户端安全登录服务器。

图 1-30 配置通过 FTPS 访问其他设备文件组网图



在 FTP 客户端和 FTP 服务器之间路由可达的情况下，从 FTP 客户端登录到安全 FTP 服务器上实现远程管理文件。

前置任务

在配置通过 FTPS 客户端登录 FTPS 服务器之前，需要完成以下任务：

版权所有 © 华为技术有限公司

- 信任证书机构文件已经上传到作为 FTPS 客户端的设备上，并已经拷贝到系统目录下名为 security 的子目录内。
- 数字证书已经上传到作为 FTPS 服务器的设备上，并已经拷贝到系统目录下名为 security 的子目录内。

数据准备

在配置通过 FTPS 客户端登录 FTPS 服务器之前，需要准备以下数据。

序号	数据
1	SSL 策略名称、信任证书机构文件、（可选）CRL 文件、FTPS 客户端的 IP 地址
2	数字证书、FTPS 服务器的 IP 地址

配置 FTPS 客户端

在作为 FTP 客户端的设备上部署 SSL 策略，并加载信任证书机构文件。通过信任证书机构文件，FTPS 客户端可验证 FTPS 服务器，保证合法用户安全登录 FTPS 服务器。

背景信息

信任证书机构文件的类型分为 PEM 格式、ASN1 格式和 PFX 格式。虽然证书的格式不相同，但是证书的内容一样。

- PEM 格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem。
- ASN1 是通用的数字证书格式之一，文件的扩展名是.der。
- PFX 是通用的数字证书格式之一，文件的扩展名是.pfx。

CRL 文件支持 ASN1 和 PEM 两种类型，虽然格式不一样，但是文件的内容一样。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name*，配置 SSL 策略并 SSL 策略视图。

步骤 3 加载信任证书机构文件。

以下步骤请根据信任证书机构文件格式任选其一执行：

- 执行命令 **trusted-ca load pem-ca** *ca-filename*，加载 PEM 格式的信任证书机构文件。
- 执行命令 **trusted-ca load asn1-ca** *ca-filename*，加载 ASN1 格式的信任证书机构文件。
- 执行命令 **trusted-ca load pfx-ca** *ca-filename* **auth-code** *auth-code*，加载 PFX 格式的信任证书机构文件。

一个 SSL 策略最多可以同时加载 4 个信任证书机构文件。如果多次加载不同的信任证书机构文件，信任证书机构文件会被增加到现有的信任证书机构文件列表中。

版权所有 © 华为技术有限公司

说明

- 如果 FTPS 服务器端配置的证书文件包含的是单个证书，则需要在客户端配置此证书以上的各级 CA 证书，直接到根证书为止。
- 如果 FTPS 服务器端配置的是证书链，则只需在客户端配置根证书即可。

步骤 4 （可选）执行命令 **crl load** { **pem-crl** | **asn1-crl** } *crl-filename*，加载证书撤销列表。

一个 SSL 策略最多可以同时加载 2 个 CRL 文件。如果多次加载不同的 CRL 文件，CRL 文件会被增加到现有的 CRL 文件列表中。

----结束

配置 FTPS 服务器

FTPS 将 FTP 和 SSL（Secure Sockets Layer，安全套接层）结合，通过 SSL 对客户端身份和服务器进行验证，对传输的数据进行加密，从而实现了对设备的安全管理。

背景信息

FTPS 服务器需要从证书颁发中心 CA（Certificate Authority）获得数字证书，访问服务器的客户端也需要从 CA 得到 CA 证书，用来验证服务器数字证书的有效性。

说明

CA 是负责发放和管理数字证书的权威机构，当前 FTPS 服务器上加载的数字证书必须向 CA 申请。

数字证书格式分为 PEM 格式、ASN1 格式和 PFX 格式。虽然证书的格式不相同，但是证书的内容一样。

- PEM 格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem。
  PEM 格式适用于系统之间的文本模式传输。
- ASN1 是通用的数字证书格式之一，文件的扩展名是.der。
  ASN1 格式是大多数浏览器的默认格式。
- PFX 是通用的数字证书格式之一，文件的扩展名是.pfx。
  PFX 格式是可移植的格式，是二进制格式。

请在作为 FTPS 服务器的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name*，配置 SSL 策略并 SSL 策略视图。

步骤 3 加载数字证书。

以下步骤请根据数字证书格式任选其一执行：

- 执行命令 **certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书。
- 执行命令 **certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*，加载 ASN1 格式的证书。
- 执行命令 **certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac** *mac-code* | **key-file** *key-filename* } **auth-code** *auth-code*，加载 PFX 格式的证书。

版权所有 © 华为技术有限公司

- 执行命令 **certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书链。

说明

一个 SSL 策略只能加载一个证书或者证书链。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先卸载旧证书或者证书链。

步骤 4 执行命令 **quit**，返回到系统视图。

步骤 5 执行命令 **ftp secure-server ssl-policy** *policy-name*，为 FTP 服务器配置 SSL 策略。

步骤 6 执行命令 **ftp secure-server enable**，使能 FTPS 服务器功能。

缺省情况下，未使能安全 FTP 服务器。

说明

使能安全 FTP 服务功能，必须去使能普通 FTP 服务器功能。

----结束

访问 FTPS 服务器

在 FTPS 客户端通过 FTP 命令登录 FTPS 服务器，实现远程管理 FTPS 服务器。

操作步骤

- 基于 IPv4 网络

  在用户视图下执行命令 **ftp ssl-policy** *policy-name* [[**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]]，与远端 FTPS 服务器建立控制连接，并进入 FTP 客户端视图。

- 基于 IPv6 网络

  在用户视图下执行命令 **ftp ssl-policy** *policy-name* **ipv6** *host* [*port-number*]，与远端 FTPS 服务器建立控制连接，并进入 FTP 客户端视图。

----结束

后续处理

登录 FTPS 服务器时，经过验证并正确输入用户名和密码后，才能成功登录。登录 FTPS 服务器后，可对 FTPS 服务器中的文件进行操作（与普通 FTP 方式一样），如表 1-14 所示。

表 1-14 文件操作

文件操作		操作
管理文件操作	配置传输文件的文件类型	● 执行命令 **ascii** 设置传输的数据类型为 ASCII 格式。 ● 执行命令 **binary** 设置传输的数据类型为二进制模式。 FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。

版权所有 © 华为技术有限公司

文件操作		操作
	配置传输文件的连接模式	● 执行命令 **passive** 设置数据传输的方式为被动方式。 ● 执行命令 **undo passive** 设置数据传输的方式为主动方式。 缺省情况下，数据传输方式是被动方式。
	上传文件	● 执行命令 **put** *local-filename* [*remote-filename*]，从本地设备上传文件至远端服务器。 ● 执行命令 **mput** *local-filenames*，从本地设备上传多个文件至远端服务器。
	下载文件	● 执行命令 **get** *remote-filename* [*local-filename*]，从远端服务器下载文件并存储在本地。 ● 执行命令 **mget** *remote-filenames*，从远端服务器下载多个文件并存储在本地。
	使能系统的提示功能	● 如果在客户端视图下执行命令 **prompt** 使能文件传输提示功能，则用户在进行文件上传或下载时，系统会提示是否确认执行此操作。 ● 如果在客户端视图下再次执行命令 **prompt**，则去使能文件传输提示功能。 **说明** 本命令只应用在使用 **mput** 命令和 **mget** 命令的多文件传输场景中。其中对于使用 **mget** 命令的场景，如果被传输的文件已经在本地存在，无论系统提示的功能被使能还是被禁止，系统都会提示用户是否覆盖本地已存在的文件。
	打开 FTP verbose 开关	执行命令 **verbose** 打开 verbose 开关，将显示所有的 FTP 响应信息。在文件传送完成后，将显示与传输速率相关的统计信息。
管理目录操作	改变远程 FTP 服务器上的工作路径	执行命令 **cd** *pathname*
	改变 FTP 服务器端的工作路径到上一级目录	执行命令 **cdup**
	显示 FTP 服务器端工作路径	执行命令 **pwd**
	显示目录中的文件和子目录的列表	执行命令 **dir** [*remote-directory* [*local-filename*]] 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
	显示 FTP 服务器上指定远程目录或文件的信息	执行命令 **ls** [*remote-directory* [*local-filename*]]

版权所有 © 华为技术有限公司

文件操作		操作
	显示或者改变FTP 客户端的工作路径	执行命令 **lcd** [*directory*] 与 **pwd** 不同的是，**lcd** 命令执行后显示的是 FTP 客户端的本地工作路径，而 **pwd** 显示的则是远端 FTP 服务器的工作路径。
	在 FTP 服务器上创建目录	执行命令 **mkdir** *remote-directory* 创建的目录可以为字母和数字等的组合，但不可以为<、>、?、\、：等特殊字符。
	在 FTP 服务器上删除目录	执行命令 **rmdir** *remote-directory*
查看 FTP 命令的在线帮助		执行命令 **remotehelp** [*command*]
更改登录用户		执行命令 **user** *username* [*password*]

检查配置结果

通过 FTPS 客户端登录 FTPS 服务器成功配置后，可以查看到 FTPS 客户端、FTPS 服务器上的 SSL 策略，FTPS 客户端上加载的信任证书机构文件，FTPS 服务器上加载的数字证书等内容。

前提条件

已完成通过 FTPS 客户端登录 FTPS 服务器的所有配置。

操作步骤

- 使用 **display ssl policy** 命令，分别查看 FTP 客户端配置的 SSL 策略、加载的信任证书机构文件，FTP 服务器端配置的 SSL 策略、加载的数字证书。
- 使用 **display ftp-server** 命令，查看 SSL 策略名称、FTPS 服务器的状态。

----结束

任务示例

在 FTP 客户端上执行命令 **display ssl policy**，可以看到配置的 SSL 策略及加载的信任证书机构文件详细信息。

```
<Quidway> display ssl policy
       SSL Policy Name: ftp_client
     Policy Applicants:
         Key-pair Type:
 Certificate File Type:
      Certificate Type:
  Certificate Filename:
     Key-file Filename:
             Auth-code:
                   MAC:
              CRL File:
       Trusted-CA File:
     Trusted-CA File 1: Format = PEM, Filename = 1_cacert_pem_rsa.pem
     Trusted-CA File 2: Format = PEM, Filename = 1_rootcert_pem_rsa.pem
```


版权所有 © 华为技术有限公司

在 FTP 服务器上执行命令 **display ssl policy**，可以看到配置的 SSL 策略及加载的数字证书详细信息。

```
<Quidway> display ssl policy
       SSL Policy Name: ftp_server
     Policy Applicants: FTP secure-server
         Key-pair Type: RSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_rsa.pem
     Key-file Filename: 1_serverkey_pem_rsa.pem
             Auth-code: 123456
                   MAC:
              CRL File:
       Trusted-CA File:
```

在 FTP 服务器上执行命令 **display ftp-server**，可以看到 SSL 策略名称、FTPS 服务器的状态是 running。

```
<Quidway> display ftp-server
  FTP server is stopped
  Max user number                5
  User count                     1
  Timeout value(in minute)       30
  Listening port                 21
  Acl number                     0
  FTP server's source address    0.0.0.0
  FTP SSL policy                 ftp_server
  FTP Secure-server is running
```

1.10.5 配置安全 Web 网管

在作为 HTTP 服务器的设备上部署 SSL 策略，并加载数字证书，数字证书主要用来客户端对服务器端身份的验证。

建立配置任务

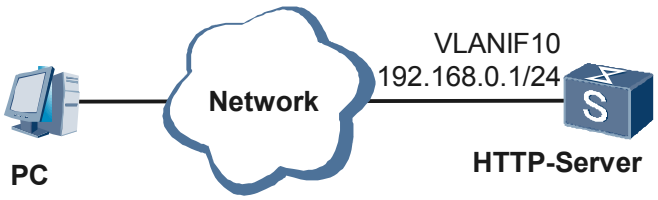
在配置设备作为 HTTPS 服务器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

对于支持 Web 网管功能的设备，开启 HTTP 服务后，设备可以作为 Web 服务器，允许用户通过 HTTP 协议登录，并利用 Web 页面实现对设备的访问和控制。但是 HTTP 协议本身不能对 Web 服务器的身份进行验证，也不能保证数据传输的私密性，无法提供安全性保证。为此，可在设备上部署 HTTPS 功能，将 HTTP 和 SSL 结合，通过 SSL 对客户端身份和服务器进行验证，对传输的数据进行加密，从而实现了对设备的安全管理。

如图 1-31 所示，在作为 HTTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 HTTP 服务器功能后，用户可通过 HTTPS 登录服务器，利用 Web 页面安全管理远程设备。

图 1-31 配置通过 HTTPS 访问其他设备文件组网图



版权所有 © 华为技术有限公司

前置任务

在配置设备作为 HTTPS 服务器之前，需要完成以下任务：

- 数字证书已经上传到作为 HTTPS 服务器的设备上，并已经拷贝到系统目录下名为 security 的子目录内。
- PC 上已经安装 Web 浏览器。

数据准备

在配置设备作为 HTTPS 服务器之前，需要准备以下数据。

序号	数据
1	SSL 策略名称、数字证书
2	HTTPS 服务器的 IP 地址、网页文件、网管帐号

配置 SSL 策略并加载数字证书

数字证书对用户终端-HTTPS 服务器进行双方身份验证，保证安全通信。

背景信息

使用 HTTPS 实现文件的安全操作前，HTTPS 服务器需要从证书颁发中心 CA（Certificate Authority）获得数字证书，通过数字证书对客户端进行身份验证，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备。

说明

CA 是负责发放和管理数字证书的权威机构。当前 HTTPS 服务器上加载的数字证书可以由第三方工具生成，比如 OpenSSL。OpenSSL 可以看作一个 CA，生成证书的具体步骤请参见相关软件的使用手册。

数字证书包括证书申请者的名称及相关信息、申请者的公钥、签发证书的 CA 的数字签名及证书的有效期等内容。发送数字证书时，可同步发布证书链。这时，接收者拥有证书链上的每一个证书。

数字证书格式分为 PEM 格式、ASN1 格式和 PFX 格式。虽然证书的格式不相同，但是证书的内容一样。

- PEM 格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem。PEM 类型的证书仅含公钥不含私钥，密钥一般被加密。

  PEM 格式适用于系统之间的文本模式传输。
- ASN1 是通用的数字证书格式之一，文件的扩展名是.der。ANS1 类型的证书仅含公钥不含私钥，密钥不加密。

  ASN1 格式是大多数浏览器的默认格式。
- PFX 是通用的数字证书格式之一，文件的扩展名是.pfx。PFX 类型的证书可含私钥，密钥一般被加密。

  PFX 格式是可移植的格式，是二进制格式。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name*，配置 SSL 策略。

步骤 3 加载数字证书

以下步骤请任选其一执行：

- 执行命令 **certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书。
- 执行命令 **certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*，加载 ASN1 格式的证书。
- 执行命令 **certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac** *mac-code* | **key-file** *key-filename* } **auth-code** *auth-code*，加载 PFX 格式的证书。
- 执行命令 **certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*，加载 PEM 格式的证书链。

说明

一个 SSL 策略只能加载一个证书或者证书链。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先卸载旧证书或者证书链。

----结束

加载 Web 网页文件

用户希望在图形界面下直观地管理和维护设备时，可以配置 Web 网管功能实现。用户使用 Web 网管功能时，必须加载 Web 网页文件。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **http server load** *file-name*，加载 Web 网页文件。

----结束

使能安全 HTTP 功能

在 HTTP 服务器上部署 SSL 策略，并使能安全 HTTP 功能，HTTPS 服务器将提供以 SSL 为基础的安全 HTTP 服务功能。

背景信息

说明

使能安全 HTTP 服务功能，必须去使能普通 HTTP 服务器功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **http secure-server ssl-policy** *policy-name*，为 HTTP 服务器配置 SSL 策略。

步骤 3 执行命令 **http secure-server enable**，使能安全 HTTP 服务器功能。

版权所有 © 华为技术有限公司

缺省情况下，未使能安全 HTTP 服务功能。

步骤 4 （可选）**http secure-server port** *port-number*，配置安全 HTTP 服务器监听的端口号。

缺省情况下，安全 HTTP 服务器端监听端口号是 443，此时用户通过 WEB 功能访问和控制设备可以不指定端口号。但如果使用缺省的监听端口号，可能会有攻击者不断访问此端口，导致带宽和服务器性能的下降，造成其他正常用户无法访问。所以可以执行本命令重新配置安全 HTTP 服务器的监听端口号，攻击者不知道安全 HTTP 服务器监听端口号的更改，有效防止了攻击者对安全 HTTP 服务器标准端口的访问。

----结束

创建 Web 网管帐号

为了保证用户安全登录 Web 服务器，建议设置 HTTP 用户名和密码。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置 HTTP 用户名和密码。

说明

实际应用时，建议使用 **cipher** 形式的密码，用户名和密码不要设置的过于简单，以保证安全性。

步骤 4 执行命令 **local-user** *user-name* **service-type http**，配置用户的访问类型是 HTTP。

----结束

登录 Web 网管

用户登录 Web 网管后，通过 Web 网管，可在图形界面下非常直观地管理和维护设备。

在 PC 上打开 Web 浏览器，在地址栏中输入 HTTPS 服务器的 IP 地址，按回车键后将显示登录对话框，如图 1-32 所示。

图 1-32 登录界面示意图



版权所有 © 华为技术有限公司

请正确输入 HTTP 用户名、密码和验证码，单击登录或直接按回车键即可进入 Web 网管系统主页面。

检查配置结果

安全 Web 网管成功配置后，可以查看到 HTTPS 服务器上的 SSL 策略、加载的数字证书，及 HTTPS 服务器状态信息等内容。

前提条件

已完成安全 Web 网管的所有配置。

操作步骤

- 使用 **display ssl policy** 命令，查看配置的 SSL 策略及加载的数字证书。
- 使用 **display http server** 命令，查看 SSL 策略名称、HTTP 服务器的状态。

----结束

任务示例

执行命令 **display ssl policy**，可以看到配置的 SSL 策略及加载的数字证书详细信息。

```
<Quidway> display ssl policy
       SSL Policy Name: http_server
     Policy Applicants: WEB secure-server
         Key-pair Type: RSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_rsa.pem
     Key-file Filename: 1_serverkey_pem_rsa.pem
             Auth-code: 123456
                   MAC:
              CRL File:
       Trusted-CA File:
```

执行命令 **display http server**，可以看到 SSL 策略名称、HTTPS 服务器的状态。

```
<Quidway> display http server
   HTTP Server Status              : disabled
   HTTP Server Port                : 80(80)
   HTTP Timeout Interval           : 20
   Current Online Users            : 0
   Maximum Users Allowed           : 5
   HTTP Secure-server Status       : enabled
   HTTP Secure-server Port         : 443(443)
   HTTP SSL Policy                 : http_server
```

1.10.6 配置举例

配置通过用户终端登录 FTPS 服务器示例

用户在终端可以通过支持 SSL 的 FTP 客户端软件登录到有 FTPS 服务器功能的设备，在用户终端与服务器之间实现安全文件管理操作。

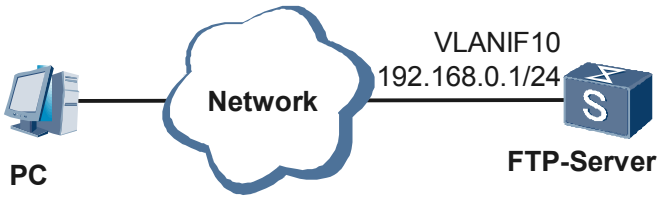
版权所有 © 华为技术有限公司

组网需求

传统的 FTP 不具备安全机制，采用明文的形式传输数据。如果 FTP 服务器设置了登录用户名和密码，则 FTP 服务器可以验证客户端的身份，但是客户端不能验证服务器的身份，无法防止传输的数据被篡改等，存在很大的安全隐患。在 FTP 服务器上部署 SSL 策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL 可以为 FTP 服务器提供安全连接，从而很大程度上改善了 FTP 服务器安全性问题。

如图 1-33 所示，在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能后，用户在终端通过支持 SSL 的 FTP 客户端软件登录安全 FTP 服务器，在终端与服务器之间实现文件的安全管理操作。

图 1-33 通过 FTPS 进行文件操作组网图



配置思路

采用如下的思路配置通过 FTPS 进行文件操作：

1. 上传数字证书。
   将 PC 机上存储的数字证书上传到作为 FTP 服务器的设备上。
2. 加载数字证书。
   将 FTP 服务器根目录下的数字证书拷贝到 security 子目录中，再配置 SSL 策略并加载数字证书。
3. 使能安全 FTP 服务器功能。
4. 在 PC 上安装支持 SSL 的 FTP 客户端软件。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器的 IP 地址
- FTP 的用户名及密码
- SSL 数字证书

操作步骤

步骤 1 上传数字证书

在作为 FTP 服务器的设备上配置 IP 地址，实现用户终端和 FTP 服务器路由可达。

```
<Quidway> system-view
[Quidway] sysname FTP-Server
[FTP-Server] interface gigabitethernet0/0/1
[FTP-Server-GigabitEthernet0/0/1] port link-type access
```


版权所有 © 华为技术有限公司

```
[FTP-Server-GigabitEthernet0/0/1] quit
[FTP-Server] vlan 10
[FTP-Server-vlan10] port gigabitethernet0/0/1
[FTP-Server-vlan10] quit
[FTP-Server] interface vlanif 10
[FTP-Server-Vlanif10] ip address 192.168.0.1 24
[FTP-Server-Vlanif10] quit
```

使能 FTP 服务器功能。

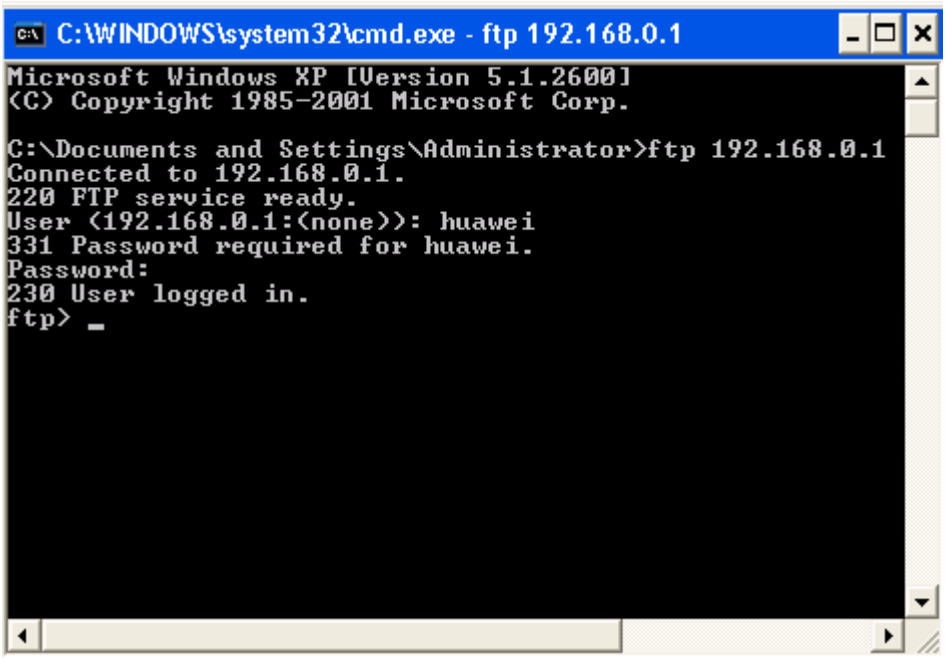
```
[FTP-Server] ftp server enable
```

在 FTP 服务器上配置 FTP 用户的验证信息、授权方式和授权目录。

```
[FTP-Server] aaa
[FTP-Server-aaa] local-user huawei password simple huawei
[FTP-Server-aaa] local-user huawei service-type ftp
[FTP-Server-aaa] local-user huawei ftp-directory flash:
[FTP-Server-aaa] quit
[FTP-Server] quit
```

在 PC 机上进入 windows 命令行提示符输入，执行 ftp 命令指定 FTP 服务器的连接地址。然后输入正确的用户名和密码与 FTP 服务器建立 FTP 连接。如图 1-34 所示。

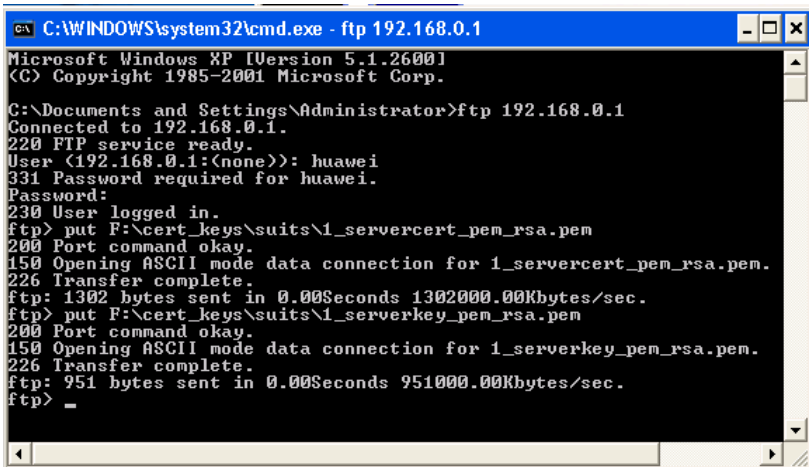
图 1-34 从用户终端登录 FTP 服务器示意图



在用户终端将数字证书上传到 FTP 服务器上，如图 1-35 所示。

版权所有 © 华为技术有限公司

图 1-35 上传数字证书示意图



上述步骤成功执行后，在 FTP 服务器端执行命令 **dir**，可看到成功上传的数字证书。

```
<FTP-Server> dir
Directory of flash:/

Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
   0  drw-              -  May 10 2011 05:05:40   src
   1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
   2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
   3  -rw-          1,302  May 10 2011 05:32:05   1_servercert_pem_rsa.pem
   4  -rw-            951  May 10 2011 05:32:44   1_serverkey_pem_rsa.pem

304,292 KB total (303,770 KB free)
```

步骤 2 配置 SSL 策略并加载数字证书

创建 security 子目录，并将安全证书拷贝到 security 子目录。

```
<FTP-Server> mkdir security/
<FTP-Server> copy 1_servercert_pem_rsa.pem security/
<FTP-Server> copy 1_serverkey_pem_rsa.pem security/
```

上述步骤成功执行后，在 security 子目录下执行命令 **dir**，可看到拷贝成功的数字证书。

```
<FTP-Server> cd security/
<FTP-Server> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          1,302  May 10 2011 05:44:34   1_servercert_pem_rsa.pem
    1  -rw-            951  May 10 2011 05:45:22   1_serverkey_pem_rsa.pem

304,292 KB total (303,766 KB free)
```

创建 SSL 策略，并加载 PEM 格式的数字证书。

```
<FTP-Server> system-view
[FTP-Server] ssl policy ftp_server
[FTP-Server-ssl-policy-ftp_server] certificate load pem-cert 1_servercert_pem_rsa.pem key-pair rsa
key-file 1_serverkey_pem_rsa.pem auth-code 123456
[FTP-Server-ssl-policy-ftp_server] quit
```

步骤 3 使能安全 FTP 服务器功能

说明

使能安全 FTP 服务功能，必须去使能普通 FTP 服务器功能。

```
[FTP-Server] undo ftp server
```


版权所有 © 华为技术有限公司

```
[FTP-Server] ftp secure-server ssl-policy ftp_server
[FTP-Server] ftp secure-server enable
```

步骤 4 在 PC 上安装支持 SSL 的 FTP 客户端软件

具体操作过程请参见第三方软件的帮助文档。

步骤 5 检查配置结果

在安全 FTP 服务器端执行命令 **display ssl policy**，可以看到加载的证书详细信息。

```
[FTP-Server] display ssl policy
       SSL Policy Name: ftp_server
     Policy Applicants: FTP secure-server
         Key-pair Type: RSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_rsa.pem
     Key-file Filename: 1_serverkey_pem_rsa.pem
             Auth-code: 123456
                   MAC:
              CRL File:
       Trusted-CA File:
```

在安全 FTP 服务器端执行命令 **display ftp-server**，可以看到 SSL 策略名称、安全 FTP 服务器的状态是 running。

```
[FTP-Server] display ftp-server
   FTP server is stopped
   Max user number                 5
   User count                      1
   Timeout value(in minute)        30
   Listening port                  21
   Acl number                      0
   FTP server's source address     0.0.0.0
   FTP SSL policy                  ftp_server
   FTP Secure-server is running
```

用户可以通过支持 SSL 的 FTP 客户端软件与安全 FTP 服务器建立连接，并实现文件的上传和下载。

----结束

安全 FTP 服务器的配置文件

```
#
 sysname FTP-Server
#
 FTP secure-server enable
 ftp secure-server ssl-policy ftp_server
#
 vlan batch 10
#
ssl policy ftp_server
 certificate load pem-cert 1_servercert_pem_rsa.pem key-pair rsa key-file 1_serverkey_pem_rsa.pem
auth-code 123456
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 local-user huawei password simple huawei
 local-user huawei service-type ftp
 local-user huawei ftp-directory flash:/
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
return
```

配置通过 FTPS 客户端登录 FTPS 服务器示例

用户通过 FTPS 客户端登录到 FTPS 服务器功能的设备，在客户端与服务器之间实现安全文件管理操作。

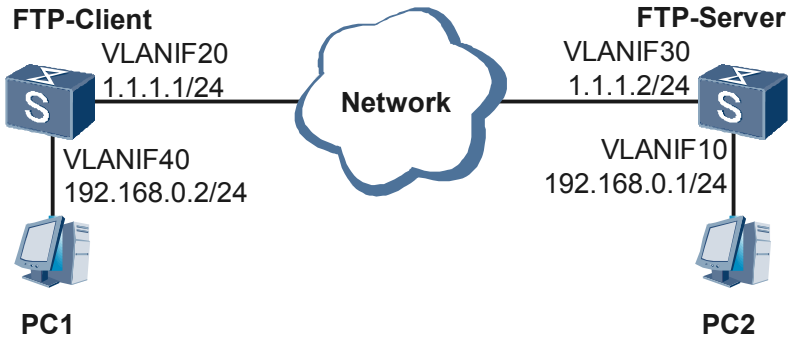
组网需求

传统的 FTP 不具备安全机制，采用明文的形式传输数据。如果 FTP 服务器设置了登录用户名和密码，则 FTP 服务器可以验证客户端的身份，但是客户端不能验证服务器的身份，无法防止传输的数据被篡改等，存在很大的安全隐患。在 FTP 服务器上部署 SSL 策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL 可以为 FTP 服务器提供安全连接，从而很大程度上改善了 FTP 服务器安全性问题。

如图 1-36 所示：

- 在作为 FTP 客户端的设备上部署 SSL 策略并加载信任证书机构文件，检查证书持有者身份的合法性，并签发证书，以防证书被伪造或篡改，以及对证书和密钥进行管理。
- 在作为 FTP 服务器的设备上部署 SSL 策略，加载数字证书并使能安全 FTP 服务器功能，检查信任证书机构文件的合法性，保证合法客户端安全登录服务器。

图 1-36 配置通过 FTPS 访问其他设备文件组网图



在 FTP 客户端和 FTP 服务器之间路由可达的情况下，从 FTP 客户端登录到安全 FTP 服务器上实现远程管理文件。

配置思路

采用如下的思路配置通过 FTPS 访问其他设备文件：

1. 上传证书。
   - 将 PC2 上存储的数字证书上传到作为 FTP 服务器的设备上。
   - 将 PC1 上存储的信任证书机构文件上传到作为 FTP 客户端的设备上。

版权所有 © 华为技术有限公司

2. 加载证书，并配置 SSL 策略。
   - 将 FTP 服务器根目录下的数字证书拷贝到 security 子目录中，再配置 SSL 策略并加载数字证书。
   - 将 FTP 客户端根目录下的信任证书机构文件拷贝到 security 子目录中，再配置 SSL 策略并加载信任证书机构文件。
3. 在 FTP 服务器端使能安全 FTP 服务器功能。
4. 配置 FTP 客户端和 FTP 服务器相连的接口 IP 地址，保证路由可达。
5. 在 FTP 客户端通过 FTP 命令登录安全 FTP 服务器，实现远程文件管理。

数据准备

为完成此配置示例，需准备如下的数据：

- FTP 客户端、FTP 服务器的 IP 地址
- FTP 的用户名及密码
- SSL 信任证书机构文件、数字证书

操作步骤

步骤 1 上传证书

- 在 FTP 服务器上进行如下配置

  # 在作为 FTP 服务器的设备上配置 IP 地址，实现用户终端和 FTP 服务器路由可达。

```
<Quidway> system-view
[Quidway] sysname FTP-Server
[FTP-Server] interface gigabitethernet0/0/1
[FTP-Server-GigabitEthernet0/0/1] port link-type access
[FTP-Server-GigabitEthernet0/0/1] quit
[FTP-Server] vlan 10
[FTP-Server-vlan10] port gigabitethernet0/0/1
[FTP-Server-vlan10] quit
[FTP-Server] interface vlanif 10
[FTP-Server-Vlanif10] ip address 192.168.0.1 24
[FTP-Server-Vlanif10] quit
```

  # 使能 FTP 服务器功能。

```
[FTP-Server] ftp server enable
```

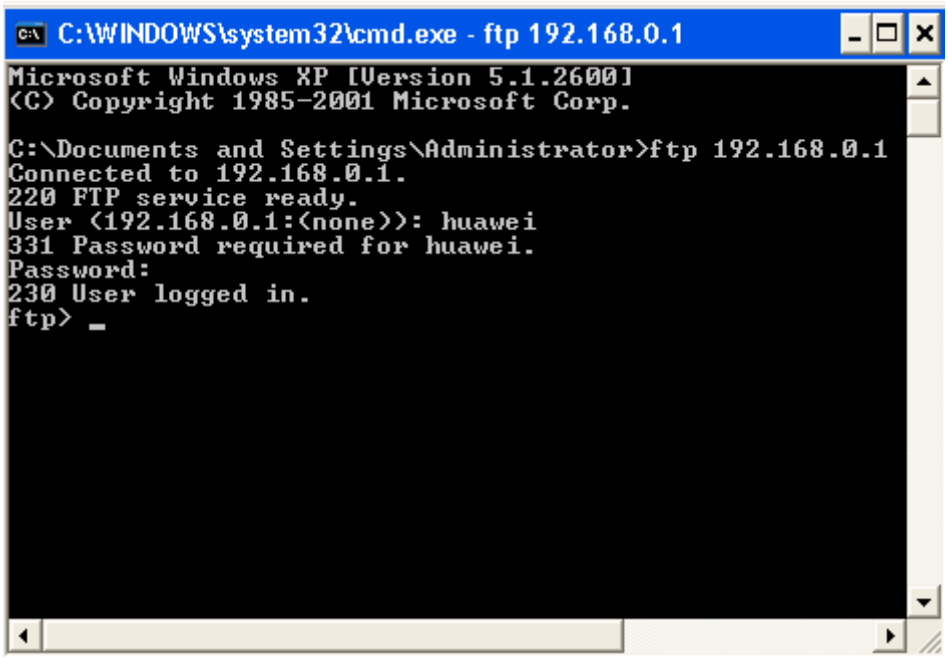
  # 在 FTP 服务器上配置 FTP 用户的验证信息、授权方式和授权目录。

```
[FTP-Server] aaa
[FTP-Server-aaa] local-user huawei password simple huawei
[FTP-Server-aaa] local-user huawei service-type ftp
[FTP-Server-aaa] local-user huawei ftp-directory flash:
[FTP-Server-aaa] quit
[FTP-Server] quit
```

  # 在 PC 机上进入 windows 命令行提示符输入，执行 ftp 命令指定 FTP 服务器的连接地址。然后输入正确的用户名和密码与 FTP 服务器建立 FTP 连接。如图 1-37 所示。

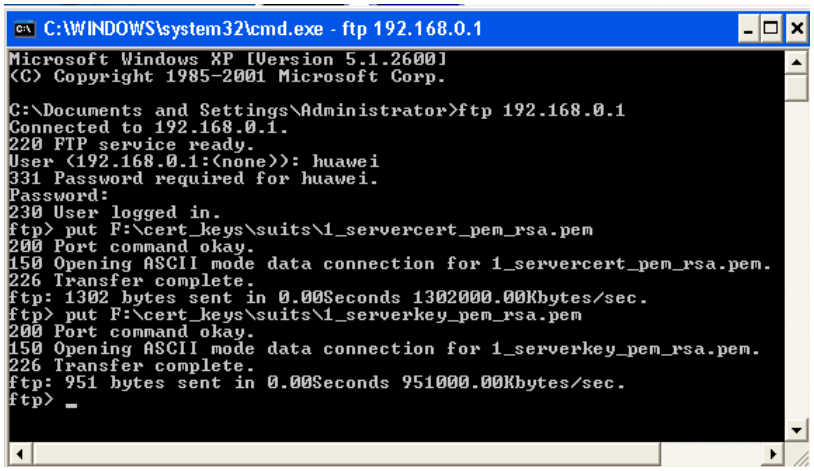
版权所有 © 华为技术有限公司

图 1-37 从用户终端登录 FTP 服务器示意图



在用户终端将数字证书上传到 FTP 服务器上，如图 1-38 所示。

图 1-38 上传数字证书示意图



上述步骤成功执行后，在 FTP 服务器端执行命令 **dir**，可看到成功上传的数字证书。

```
<FTP-Server> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  drw-              -  May 10 2011 05:05:40   src
    1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
    2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
    3  -rw-          1,302  May 10 2011 05:32:05   1_servercert_pem_rsa.pem
    4  -rw-            951  May 10 2011 05:32:44   1_serverkey_pem_rsa.pem
    5  drw-              -  May 10 2011 05:43:39   security
```


版权所有 © 华为技术有限公司

```
304,292 KB total (303,766 KB free)
```

- 在 FTP 客户端上进行如下配置

  将信任证书机构文件上传到 FTP 客户端的步骤与配置 FTP 服务器类似，这里不再赘述。详细配置请见本示例 FTP 客户端的配置文件。

  信任证书机构文件上传到 FTP 客户端后，在 FTP 客户端可执行命令 **dir**，可看到成功上传的信任证书机构文件。

```
<FTP-Client> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-        524,558  May 10 2011 04:50:39   private-data.txt
    1  -rw-          1,237  May 10 2011 05:55:33   l_cacert_pem_rsa.pem
    2  -rw-          1,241  May 10 2011 05:55:44   l_rootcert_pem_rsa.pem
    3  drw-              -  Apr 09 2011 19:46:14   src
    4  -rw-            421  Apr 09 2011 19:46:14   vrpcfg.zip
    5  -rw-      1,308,478  Apr 14 2011 19:22:45   web.zip
    6  drw-              -  Apr 10 2011 01:35:54   logfile
    7  -rw-              4  Apr 19 2011 04:24:28   snmpnotilog.txt
    8  drw-              -  Apr 11 2011 16:18:53   security
    9  drw-              -  Apr 13 2011 11:37:40   lam

304,292 KB total (300,270 KB free)
```

步骤 2 配置 SSL 策略并加载证书

- 在 FTP 服务器上进行如下配置

  # 创建 security 子目录，并将安全证书拷贝到 security 子目录。

```
<FTP-Server> mkdir security/
<FTP-Server> copy l_servercert_pem_rsa.pem security/
<FTP-Server> copy l_serverkey_pem_rsa.pem security/
```

  上述步骤成功执行后，在 security 子目录下执行命令 **dir**，可看到拷贝成功的数字证书。

```
<FTP-Server> cd security/
<FTP-Server> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          1,302  May 10 2011 05:44:34   l_servercert_pem_rsa.pem
    1  -rw-            951  May 10 2011 05:45:22   l_serverkey_pem_rsa.pem

304,292 KB total (303,766 KB free)
```

  # 创建 SSL 策略，并加载 PEM 格式的数字证书。

```
<FTP-Server> system-view
[FTP-Server] ssl policy ftp_server
[FTP-Server-ssl-policy-ftp_server] certificate load pem-cert l_servercert_pem_rsa.pem key-pair
rsa key-file l_serverkey_pem_rsa.pem auth-code 123456
[FTP-Server-ssl-policy-ftp_server] quit
```

  上述步骤成功配置后，在 FTP 服务器端执行命令 **display ssl policy**，可以看到加载的证书详细信息。

```
[FTP-Server] display ssl policy
       SSL Policy Name: ftp_server
     Policy Applicants: FTP secure-server
        Key-pair Type: RSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: l_servercert_pem_rsa.pem
     Key-file Filename: l_serverkey_pem_rsa.pem
             Auth-code: 123456
                   MAC:
              CRL File:
       Trusted-CA File:
```


版权所有 © 华为技术有限公司

- 配置 FTP 客户端

  # 创建 security 子目录，并将信任证书机构文件拷贝到 security 子目录。

  具体配置步骤与 FTP 服务器上的配置类似，这里不再赘述。详细配置请见本示例 FTP 客户端的配置文件。

  信任证书机构文件拷贝到 security 子目录后，在 security 子目录下执行命令 **dir**，可看到拷贝成功的信任证书机构文件。

```
<FTP-Client> cd security/
<FTP-Client> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          1,237  May 10 2011 05:57:15   1_cacert_pem_rsa.pem
    1  -rw-          1,241  May 10 2011 05:57:29   1_rootcert_pem_rsa.pem

304,292 KB total (300,266 KB free)
```

  # 创建 SSL 策略，并加载信任证书机构文件。

```
<FTP-Client> system-view
[FTP-Client] ssl policy ftp_client
[FTP-Client-ssl-policy-ftp_client] trusted-ca load pem-ca 1_cacert_pem_rsa.pem
[FTP-Client-ssl-policy-ftp_client] trusted-ca load pem-ca 1_rootcert_pem_rsa.pem
[FTP-Client-ssl-policy-ftp_client] quit
```

  上述步骤成功配置后，在 FTP 客户端执行命令 **display ssl policy**，可以看到加载的信任证书机构文件详细信息。

```
[FTP-Client] display ssl policy
      SSL Policy Name: ftp_client
    Policy Applicants:
        Key-pair Type:
 Certificate File Type:
     Certificate Type:
  Certificate Filename:
    Key-file Filename:
            Auth-code:
                 MAC:
             CRL File:
      Trusted-CA File:
    Trusted-CA File 1: Format = PEM, Filename = 1_cacert_pem_rsa.pem
    Trusted-CA File 2: Format = PEM, Filename = 1_rootcert_pem_rsa.pem
```

步骤 3 使能安全 FTP 服务器功能

说明

使能安全 FTP 服务功能，必须去使能普通 FTP 服务器功能。

```
[FTP-Server] undo ftp server
[FTP-Server] ftp secure-server ssl-policy ftp_server
[FTP-Server] ftp secure-server enable
```

步骤 4 配置 FTP 客户端和 FTP 服务器相连的接口 IP 地址

配置 FTP 服务器。

```
[FTP-Server] interface gigabitethernet 0/0/2
[FTP-Server-GigabitEthernet0/0/2] port link-type access
[FTP-Server-GigabitEthernet0/0/2] quit
[FTP-Server] vlan 30
[FTP-Server-vlan30] port gigabitethernet 0/0/2
[FTP-Server-vlan30] quit
[FTP-Server] interface vlanif 30
[FTP-Server-Vlanif30] ip address 1.1.1.2 24
[FTP-Server-Vlanif30] quit
```

配置 FTP 客户端。

```
[FTP-Client] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[FTP-Client-GigabitEthernet0/0/2] port link-type access
[FTP-Client-GigabitEthernet0/0/2] quit
[FTP-Client] vlan 20
[FTP-Client-vlan20] port gigabitethernet 0/0/2
[FTP-Client-vlan20] quit
[FTP-Client] interface vlanif 20
[FTP-Client-Vlanif20] ip address 1.1.1.1 24
[FTP-Client-Vlanif20] quit
[FTP-Client] quit
```

步骤 5 在 FTP 客户端通过 FTP 命令登录安全 FTP 服务器实现远程文件管理

```
<FTP-Client> ftp ssl-policy ftp_client 1.1.1.2
Trying 1.1.1.2 ...
Press CTRL+K to abort
Connected to 1.1.1.2.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(1.1.1.2:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

在客户端需要正确输入用户名和密码，才能通过 FTP 方式成功登录 FTP 服务器。

步骤 6 检查配置结果

在安全 FTP 服务器端执行命令 **display ftp-server**，可以看到 SSL 策略名称、安全 FTP 服务器的状态是 running。

```
[FTP-Server] display ftp-server
  FTP server is stopped
  Max user number                 5
  User count                      1
  Timeout value(in minute)        30
  Listening port                  21
  Acl number                      0
  FTP server's source address     0.0.0.0
  FTP SSL policy                  ftp_server
  FTP Secure-server is running
```

在 FTP 客户端，用户可远程管理 FTP 服务器上的文件。

----结束

配置文件

- FTP 服务器上的配置文件

```
#
 sysname FTP-Server
#
 FTP secure-server enable
 ftp secure-server ssl-policy ftp_server
#
 vlan batch 10 30
#
ssl policy ftp_server
 certificate load pem-cert 1_servercert_pem_rsa.pem key-pair rsa key-file
1_serverkey_pem_rsa.pem auth-code 123456
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
```


版权所有 © 华为技术有限公司

```
 local-user huawei password simple huawei
 local-user huawei service-type ftp
 local-user huawei ftp-directory flash:/
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif30
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 30
#
return
```

- FTP 客户端上的配置文件

```
#
 sysname FTP-Client
#
 FTP server enable
#
 vlan batch 20 40
#
ssl policy ftp_client
 trusted-ca load pem-ca l_cacert_pem_rsa.pem
 trusted-ca load pem-ca l_rootcert_pem_rsa.pem
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 local-user huawei password simple huawei
 local-user huawei service-type ftp
 local-user huawei ftp-directory flash:/
#
interface Vlanif20
 ip address 1.1.1.1 255.255.255.0
#
interface Vlanif40
 ip address 192.168.0.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 20
#
return
```


版权所有 © 华为技术有限公司

2 设备管理

关于本章

本文档针对 AC6605 的设备管理特性，从配置过程和配置举例两方面对特性进行介绍。

2.1 NAP 配置
介绍 NAP（Neighbor Access Protocol）功能在 AC6605 的配置方法。

2.2 使用 display 命令查看设备的状态
介绍了设备相关的维护和查看操作。

2.3 硬件管理
介绍 AC6605 与硬件管理相关的配置。

2.4 使用信息中心监控设备
介绍了信息中心的基础知识，还介绍了管理信息中心和监控 AC6605 设备时的配置步骤和相应的配置举例。

2.5 监控口配置
配置监控口，对设备的环境进行监控。

2.6 使用镜像监控设备
镜像主要用来监控观察设备上符合某种要求的报文。

2.7 PoE 配置
介绍 PoE 的基本概念和配置方法。

2.8 ALS 配置
介绍 ALS（Automatic Laser Shutdown）功能在 AC6605 的配置方法。

2.9 重新启动和复位
介绍了 BootROM 软件和 VRP 系统软件的基础知识，以及重新启动 AC6605 设备的方法。

版权所有 © 华为技术有限公司

2.1 NAP 配置

介绍 NAP（Neighbor Access Protocol）功能在 AC6605 的配置方法。

2.1.1 NAP 简介

NAP 协议用来实现空配置开局功能。利用现网设备与空配置设备的物理直接连接，从现网设备登录空配置设备，实现远程开局的功能。

通常，设备在发货时只加载软件版本，没有配置数据。在对设备进行开局调测时，工程师必须到现场进行配置和互通联调，无法从远程登录，对工程开局造成不便，提高了运作和交付成本。

目前华为提供的 HGMP（Huawei Group Management Protocol）协议可以解决部分问题，但 HGMP 仅适用于二层网络，主要应用于以太网的组网环境下。NAP 协议应用于三层网络，利用现网设备与空配置设备的物理直接连接，在二者之间建立临时的邻居关系，从现网设备登录空配置设备，实现远程开局的功能。该协议的广泛使用，将大大降低网络的运行维护和交付成本。

2.1.2 配置 NAP 远程开局

使用 NAP 协议，用户可以从现网设备登录空配置设备，实现远程开局的功能。

背景信息

注意

空配置设备在上电启动之后，必须保证与现网设备的相连接口处于 Up 状态，且支持 NAP 协议，否则 NAP 远程开局功能不可用。

建立配置任务

在进行 NAP 远程开局的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当需要对空配置设备进行开局配置时，可以使用 NAP 协议，通过现网设备远程登录，建立临时的邻居关系，实现远程配置。

前置任务

在配置 NAP 远程开局功能之前，需要完成以下任务：

- 空配置设备已经通过缆线与现网设备直接单跳相连
- 空配置设备与现网设备的相连接口均处于 Up 状态，且均支持 NAP 协议

版权所有 © 华为技术有限公司

数据准备

说明

- 如果采用手工方式配置 NAP 连接的 IP 地址，那么在配置 NAP 功能之前，需要准备以下数据。
- 如果采用自动分配 IP 地址方式，可忽略此项。

在配置 NAP 远程开局功能之前，需要准备以下数据。

序号	数据
1	两个主 IP 地址。分别用于主从接口上的主 IP 地址，要求两个地址在同一个网段。
2	两个从 IP 地址。分别用于主从接口上的从 IP 地址，要求两个地址在同一个网段。

配置启动 NAP 主接口

用户可以采用系统分配 IP 地址的方式或者指定 IP 地址的方式，配置启动 NAP 的主接口。

背景信息

注意

如果 NAP 的主接口端设备上有影响 IP 地址配置或 IP 报文转发的命令（如 VPN、Eth-Trunk 或二层接口的相关配置），会导致 NAP 功能不可用。建议删除此类命令后，重新启用 NAP 功能。

请在需要配置并启动 NAP 主接口功能的交换机上进行下面的配置。

NAP 的 IP 地址分配分为自动分配和手工配置两种方式。

操作步骤

- 自动分配 IP 地址
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **nap port master**，配置并启动 NAP 主接口。
- 手工配置 IP 地址

  如果采用手工配置 IP 地址的方式，有如下两种方式，用户可以根据需要进行选择。

  手工指定 NAP 的 IP 地址池，IP 地址在该地址池中自动分配。请按如下步骤执行操作。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **nap ip-pool** *ip-address mask-length*，配置 NAP 的 IP 地址池。

     默认 NAP 连接的 IP 地址池是 10.167.253.0/24，可以通过命令 **nap ip-pool** *ip-address mask-length* 修改该值，进行手工配置。

版权所有 © 华为技术有限公司

说明

主节点设备启动 NAP 功能后，不能再更改 IP 地址池。

3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
4. 执行命令 **nap port master**，配置并启动 NAP 主接口。

手工指定 NAP 的 IP 地址。请按如下步骤执行操作。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **nap port master**，配置并启动 NAP 主接口。
4. 执行命令 **nap local-ip** *mast-inter-mast-ip* **sub-ip** *mast-inter-sub-ip* **peer-ip** *sub-inter-mast-ip* **sub-ip** *sub-inter-sub-ip mask-length*，手工配置 NAP 的 IP 地址。

   默认 NAP 连接的 IP 地址池是 10.167.253.0/24。

   配置时请遵循主从接口主 IP 地址属于同一网段，主从接口从 IP 地址属于同一网段。

----结束

远程登录

邻居关系建立后，用户可以从 NAP 主节点登录从节点。

背景信息

执行命令 **display nap interface**，查看接口的 NAP 状态信息，确保 IP 地址已经分配成功。

请在配置为 NAP 主接口的交换机上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **nap login neighbor**，由主节点登录从节点。

- 在从节点设备空配置情况下，NAP 主节点登录到对端的从节点时，不需要用户名密码验证。
- 如果从节点设备配置了用户名和密码等登录信息，那么通过 NAP 远程登录到从节点设备的时候需要进行用户密码认证。

说明

为保证 NAP 的安全性，对于远程的 Telnet 连接，空配置的从节点设备会检查 Telnet 的源地址，如果是对端主节点设备的 NAP 协议地址，默认级别将和 Console 口登录级别相同，即最高用户级别，不需要进行验证直接登录，否则无法登录。

如果在接口下配置了 **ip source check user-bind enable** 命令，则无法登录到 NAP 邻居端。

----结束

关闭从节点 NAP 功能

当 NAP 功能完成后，需要关闭从节点设备从接口的 NAP 功能。

版权所有 © 华为技术有限公司

背景信息

主节点设备通过 Telnet 的方式登录从节点设备。此时 NAP 功能已经完成，为保证系统安全性，应该对从节点设备从接口的 NAP 功能全局去使能。

请在配置为 NAP 从节点的交换机上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **undo nap slave enable**，关闭从节点设备 NAP 功能。

----结束

检查配置结果

NAP 远程开局功能配置成功后，可以查看到 NAP 协议配置的当前状态信息、接口的 NAP 状态信息等内容。

前提条件

已完成 NAP 远程开局的所有配置。

操作步骤

步骤 1 使用 **display nap status** 命令查看 NAP 协议配置的当前状态信息。

步骤 2 使用 **display nap interface** [*interface-type interface-number*]命令查看接口的 NAP 状态信息。

----结束

任务示例

执行命令 **display nap status**，查看 NAP 协议配置的当前状态信息。

```
<Quidway> display nap status
 Slave port status         : Enable
 Nap ip-pool/Mask          : 12.12.12.0/24
```

执行命令 **display nap interface** *interface-type interface-number* 命令，查看指定接口下的 NAP 状态信息。

```
<Quidway> display nap interface gigabitethernet0/0/1
```

- 如果 IP 地址没有分配成功，显示信息为：

```
-------------------------------------------------------
 NAP master port list:
 Port count          : 2
-------------------------------------------------------
 Port property                          : Master
 Current status                         : DETECTING
 Local port                             : GigabitEthernet0/0/1
 Peer port                              : GigabitEthernet0/0/1
 Local primary ip                       : NULL
 Peer primary ip                        : NULL
 Local secondary ip                     : NULL
 Peer secondary ip                      : NULL
 Hello time                             : 3s
```


版权所有 © 华为技术有限公司

```
Linked time                              : 00:00:00
-------------------------------------------------------
Port property                            : Master
Current status                           : DETECTING
Local port                               : GigabitEthernet0/0/2
Peer port                                : GigabitEthernet0/0/2
Local primary ip                         : NULL
Peer primary ip                          : NULL
Local secondary ip                       : NULL
Peer secondary ip                        : NULL
Hello time                               : 3s
Linked time                              : 00:00:00
-------------------------------------------------------
```

- 如果 IP 地址分配成功，显示信息为：

```
-------------------------------------------------------
NAP master port list :
Port count           : 2
-------------------------------------------------------
Port property                            : Master
Current status                           : IP-ASSIGNED
Local port                               : GigabitEthernet0/0/1
Peer port                                : GigabitEthernet0/0/1
Local primary ip                         : 12.12.12.5
Peer primary ip                          : 12.12.12.6
Local secondary ip                       : 12.12.12.9
Peer secondary ip                        : 12.12.12.10
Hello time                               : 3s
Linked time                              : 00:09:12
-------------------------------------------------------
Port property                            : Master
Current status                           : IP-ASSIGNED
Local port                               : GigabitEthernet0/0/2
Peer port                                : GigabitEthernet0/0/2
Local primary ip                         : 10.10.10.5
Peer primary ip                          : 10.10.10.6
Local secondary ip                       : 10.10.10.9
Peer secondary ip                        : 10.10.10.10
Hello time                               : 3s
Linked time                              : 00:03:41
-------------------------------------------------------
```

2.1.3 配置举例

配置升级维护的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

配置手工方式的 NAP 远程开局示例

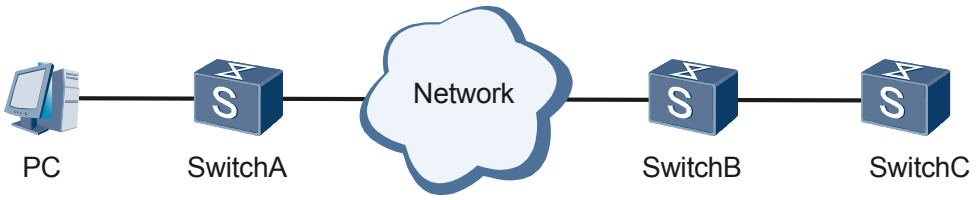
配置手工方式的 NAP 远程开局的示例。在本示例中，通过建立与空配置设备的临时邻居关系，为两端设备设置指定的 IP 地址，实现手工方式下的远程开局。

组网需求

如图 2-1 所示，用户从 SwitchA 远程登录到 SwitchB，以 SwitchB 为本端设备，建立与空配置 SwitchC 的临时邻居关系。SwitchB 和 SwitchC 的相连接口单跳直连，均处于 Up 状态，且均支持 NAP 功能。

版权所有 © 华为技术有限公司

图 2-1 配置 NAP 远程开局组网图



配置思路

采用如下的思路配置 NAP 远程开局的基本功能：

1. 在 SwitchB 上配置 NAP 主接口。
2. 在 SwitchB 上指定 NAP 连接的 IP 地址。
3. 从 SwitchB 使用 NAP 功能通过 Telnet 方式登录到 SwitchC。

数据准备

为完成此配置例，需准备如下的数据：

- 两个主 IP 地址。分别用于主从接口上的主 IP 地址，要求两个地址在同一个网段。
- 两个从 IP 地址。分别用于主从接口上的从 IP 地址，要求两个地址在同一个网段。

操作步骤

步骤 1 在 SwitchB 上配置 NAP 主接口

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] nap port master
```

步骤 2 在 SwitchB 上指定 NAP 连接的 IP 地址

```
[SwitchB-GigabitEthernet0/0/1] nap local-ip 12.12.12.5 sub-ip 12.12.12.9 peer-ip 12.12.12.6 sub-ip
12.12.12.10 30
Are you sure to continue?[Y/N] y
```

完成以上配置后，在 SwitchB 上执行 **display nap status** 命令可以看到当前 NAP 协议配置已经使能，执行 **display nap interface** 命令可以看到主从接口的主 IP 地址和从 IP 地址分配成功。如下所示。

```
[SwitchB-GigabitEthernet0/0/1] display nap status
Slave port status         : Enable
 Nap ip-pool/Mask          : 10.167.253.0/24
[SwitchB-GigabitEthernet0/0/1] display nap interface
-------------------------------------------------------
 NAP master port list
 Port count           : 1
-------------------------------------------------------
 Port property                          : Master
 Current status                         : IP-ASSIGNED
 Local port                             : GigabitEthernet0/0/1
 Peer port                              : GigabitEthernet0/0/1
 Local primary ip                       : 12.12.12.5
 Peer primary ip                        : 12.12.12.6
 Local secondary ip                     : 12.12.12.9
 Peer secondary ip                      : 12.12.12.10
```


版权所有 © 华为技术有限公司

```
 Hello time                                : 3s
 Linked time                               : 00:02:33
-------------------------------------------------------
```

步骤 3 主节点设备远程登录到从节点设备

```
[SwitchB-GigabitEthernet0/0/1] nap login neighbor
Trying 12.12.12.10 ...
Press CTRL+K to abort
Connected to 12.12.12.10 ...

Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
```

步骤 4 关闭从节点 NAP 功能

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] undo nap slave enable
```

----结束

配置文件

无

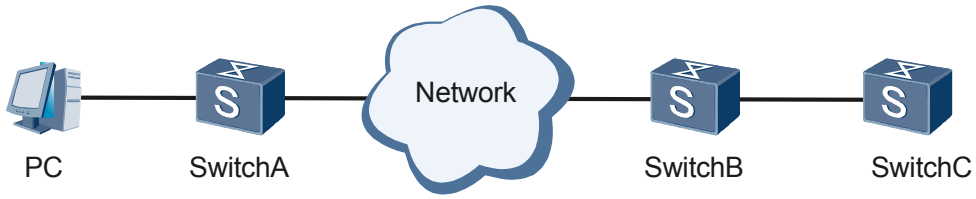
配置自动方式的 NAP 远程开局示例

配置自动方式的 NAP 远程开局的示例。在本示例中，通过建立与空配置设备的临时邻居关系，实现自动方式下的远程开局。

组网需求

如图 2-2 所示，用户从 SwitchA 远程登录到 SwitchB，以 SwitchB 为本端设备，建立与空配置 SwitchC 的临时邻居关系。SwitchB 和 SwitchC 的相连接口单跳直连，均处于 Up 状态，且均支持 NAP 功能。

图 2-2 配置 NAP 远程开局组网图



配置思路

采用如下的思路配置 NAP 远程开局的基本功能：

1. 在 SwitchB 上分配主 IP 地址和从 IP 地址。
2. 在 SwitchB 上配置 NAP 主接口。
3. 从 SwitchB 使用 NAP 功能通过 Telnet 方式登录到 SwitchC。

版权所有 © 华为技术有限公司

数据准备

无

操作步骤

步骤 1 配置 NAP 主接口

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] nap port master
```

步骤 2 配置主节点设备远程登录到从节点设备

配置 SwitchB。

```
[SwitchB-GigabitEthernet0/0/1] nap login neighbor
Trying 10.167.253.10 ...
Press CTRL+K to abort
Connected to 10.167.253.10 ...

Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
```

步骤 3 关闭从节点 NAP 功能

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] undo nap slave enable
```

----结束

配置文件

无

2.2 使用 display 命令查看设备的状态

介绍了设备相关的维护和查看操作。

2.2.1 简介

介绍了设备相关的维护和查看操作。

管理员可以通过相关的 display 命令查看设备的当前状态，判断设备当前的运行状态是否正常。

2.2.2 查看 AC6605 设备的状态

介绍通过 display 命令查看 AC6605 设备的运行状态。

查看设备信息

管理员可以查看设备的部件类型和状态信息。

版权所有 © 华为技术有限公司

背景信息

在实际操作中，在任意视图下使用该命令查看 AC6605 设备的部件类型及状态信息。

操作步骤

步骤 1 执行命令 **display device** [**slot** *slot-id*] ，查看设备信息。

----结束

查看版本信息

管理员可以查看设备的版本信息，包括：板卡类型、设备启动时长、硬件版本和软件版本。

背景信息

在实际操作中，在任意视图下使用该命令查看 AC6605 设备的版本信息。

操作步骤

步骤 1 执行命令 **display version** [**slot** *slot-id*] ，查看版本信息。

----结束

查看电子标签

管理员可以查看设备的电子标签信息，包括：板卡型号、条码、BOM 编码、英文描述、生产日期、供应商名称、发行号、CLEI 码、销售 BOM 编码。

背景信息

在实际操作中，在任意视图下使用该命令查看 AC6605 设备的电子标签信息。

该命令可以显示标识硬件代码的相关信息，为网络安装、升级、扩容以及设备维护管理和批量更换提供必要的依据。

操作步骤

步骤 1 执行命令 **display elabel** [**slot** *slot-id* [*subcard-id*]]，查看电子标签。

----结束

任务示例

```
<Quidway> display elabel slot 0
/$[System Integration Version]
/$SystemIntegrationVersion=3.0


[Slot_0]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0
```


版权所有 © 华为技术有限公司

```
[Main_Board]

/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=CX22EOFEA
BarCode=2102351377107C800132
Item=03020KAQ
Description=AC6605 Mainframe(24 10/100 BASE-T ports and 2 Combo GE(10/100/10
00 BASE-T+100/1000 BASE-X) ports and 2 SFP GE (100/1000 BASE-X) ports (SFP Req.)
 and AC 110/220V)
Manufactured=2008-06-02
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=02351377



[Port_1]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=
BarCode=
Item=
Description=
Manufactured=
/$VendorName=
IssueNumber=
CLEICode=
BOM=02351397


[Port_2]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=
BarCode=
Item=
Description=
Manufactured=
/$VendorName=
IssueNumber=
CLEICode=
BOM=02351347
```

查看温度

管理员可以查看设备的环境温度，包括：设备当前温度和设备硬件允许的温度上下限。

背景信息

在实际操作中，可以在任意视图下使用该命令查看 AC6605 设备目前的工作温度。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **display environment** [**slot** *slot-id*]，查看支持温度传感的单板的温度信息。

----结束

查看风扇的状态

当设备温度过高时，请先检查风扇的运行状态。

操作步骤

步骤 1 执行命令 **display fan** [**slot** *slot-id* | **verbose**]，查看风扇状态。

----结束

查看电源模块状态

需要更换电源模块前或需要检查电源模块状态时，请先查看电源模块状态。

操作步骤

步骤 1 在任意视图下，执行命令 **display power**，查看电源模块的状态。

----结束

查看 CPU 占用率

管理员可以查看 CPU 占用率的统计信息和配置信息。

操作步骤

步骤 1 执行命令 **display cpu-usage** [**configuration** | **slave** | **slot** *slot-id*]，查看 CPU 占用率的统计信息和配置信息。

----结束

查看内存占用率

管理员可以查看内存占用率，包括：统计时间、总内存、已用内存和内存占用率。

背景信息

在实际操作中，在任意视图下使用该命令查看 AC6605 设备内存占用率的统计信息。

操作步骤

步骤 1 执行命令 **display memory-usage** [**slave** | **slot** *slot-id*]，查看内存占用率的统计信息。

----结束

版权所有 © 华为技术有限公司

查看告警信息

管理员可以查看设备的告警信息，包括：告警名称、告警日期、告警时间、发生告警的部件。

背景信息

在实际操作中，在任意视图下使用该命令查看 AC6605 设备上的各事件的告警信息。

操作步骤

步骤 1 执行命令 **display alarm urgent** [**slot** *slot-id* | **time** *interval*]，查看设备运行中的告警信息。

----结束

查看接口状态信息

管理员可以查看接口状态信息，包括：接口当前运行状态、接口基本配置和发送接收报文的统计信息。

查看指定接口的状态信息

1. 执行命令 **display interface** *interface-type interface-number*，查看指定接口的状态信息。

查看当前接口视图的状态信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **display this interface**，查看当前接口的状态信息。

2.3 硬件管理

介绍 AC6605 与硬件管理相关的配置。

2.3.1 简介

简介 AC6605 的硬件管理。

硬件管理指硬件安装完毕后在运行过程中通过命令对硬件资源进行的操作。

2.3.2 AC6605 支持的硬件管理特性

介绍 AC6605 硬件管理的支持情况。

AC6605 支持如下几种硬件管理：

- 备份电子标签
- 配置电口自动节能

版权所有 © 华为技术有限公司

2.3.3 备份电子标签

介绍如何备份电子标签。

建立配置任务

在备份电子标签前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

电子标签在处理网络故障工作中具有重要的作用，因此需要对电子标签进行备份：网络出现故障时，通过电子标签能很方便、准确地获得相关的硬件信息。

前置任务

在备份电子标签之前，需要保证 AC6605 与 FTP 服务器之间网络互通并有可达路由。

数据准备

在备份电子标签之前，需要准备以下数据。

序号	数据
1	需备份的电子标签文件名称
3	FTP 服务器地址、用户名和密码（可选，针对备份到 FTP 服务器）

备份电子标签

AC6605 支持将电子标签备份到 FTP 服务器或 Flash 中。

操作步骤

- 备份电子标签到 CF 卡
  1. 在用户视图下执行命令 **backup elabel** [**slot** *slot-id*]，备份电子标签到 Flash 中。
- 备份电子标签到 FTP 服务器
  1. 在用户视图下执行命令 **backup elabel** [**ftp** *ip-address filename username password*] [**slot** *slot-id* [*subcard-id*]]，备份电子标签到 FTP 服务器。

----结束

2.3.4 配置电口自动节能功能

介绍如何配置电口自动节能功能。

建立配置任务

在配置电口自动节能功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

在设备正常工作的情况下，使用电口自动节能能在一定程度上实现设备节能。

前置任务

无

数据准备

在配置电口自动节能之前，需要准备以下数据。

序号	数据
1	需要配置电口自动节能的电接口号。

使能电口自动节能功能

需要使用电口自动节能时，需要先使能该功能。

操作步骤

步骤 1 执行 **system-view** 命令进入系统视图。

步骤 2 执行 **interface** { *interface-type interface-number* }命令，进入指定接口的接口视图。

步骤 3 执行 **port-auto-sleep enable** 命令，使能电口自动节能功能。

缺省情况下，以太网端口未使能自动节能功能。

----结束

检查配置结果

使能电口自动节能功能后，可以通过命令检查配置是否正确。

操作步骤

步骤 1 执行 **system-view** 命令进入系统视图。

步骤 2 执行 **interface** { *interface-type interface-number* }命令，进入指定接口的接口视图。

步骤 3 执行 **display this** 命令，检查接口下的自动节能功能是否使能。

----结束

2.4 使用信息中心监控设备

介绍了信息中心的基础知识，还介绍了管理信息中心和监控 AC6605 设备时的配置步骤和相应的配置举例。

版权所有 © 华为技术有限公司

2.4.1 信息中心简介

信息中心是控制日志、告警、调试信息输出的通道。

信息中心概述

信息中心是交换机的信息枢纽，通过对系统输出信息进行分类和筛选，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供强有力的支持。

AC6605 支持的信息中心特性

AC6605 系统中可以支持将 3 种信息（日志、告警和调试信息），按照 8 个严重等级，分配到 10 个信息通道中，再输出到多个方向。

信息的分类

信息中心可以接收和处理 3 类信息：

- log 类：即日志信息
- debug 类：即调试信息
- trap 类：即告警信息

信息的严重等级

根据信息的严重等级或紧急程度，信息分为 8 个等级，信息越严重，其严重等级值越小。详细信息见表 2-1。

表 2-1 信息严重等级的定义

显示值	严重等级	描述
0	Emergency	设备致命的异常，系统已经无法恢复正常，必须重启设备。如程序异常导致设备重启，内存的使用被检测出错误等。
1	Alert	设备重大的异常，需要立即采取措施。如设备内存占用率达到极限等。
2	Critical	设备重大的异常，需要采取措施进行处理或原因分析。如设备内存占用率超过低界线，温度超过低温告警线，BFD 探测出设备不可达，检测出错误的消息（消息是由本设备内部生成）等。
3	Error	错误的操作或设备的异常流程，不会影响后续业务，但是需要关注和原因分析。如用户的错误指令，用户密码错误，检测出错误协议报文（报文是由其他设备获得）。
4	Warning	设备的异常运转的异常点，可能引起业务故障的流程，需要引起注意。如用户关闭路由进程，BFD 探测的一次报文丢失，检测出错误协议报文等。

版权所有 © 华为技术有限公司

显示值	严重等级	描述
5	Notice	用于设备正常运转的关键操作信息。如用户执行 **shutdown** 命令，邻居发现，协议状态机的正常跳转等。
6	Informational	用于设备正常运转的一般性操作信息。如用户使用 **display** 命令等。
7	Debugging	设备正常运转的一般性信息，用户无需关注。

根据严重等级过滤信息时，仅输出严重等级值小于或等于所配置的严重等级值的信息，即，输出所配置级别和比所配置级别更严重的信息。

例如，当配置严重等级阈值为 6 时，仅输出严重等级值为 0 ～ 6 的信息。

信息中心的工作过程

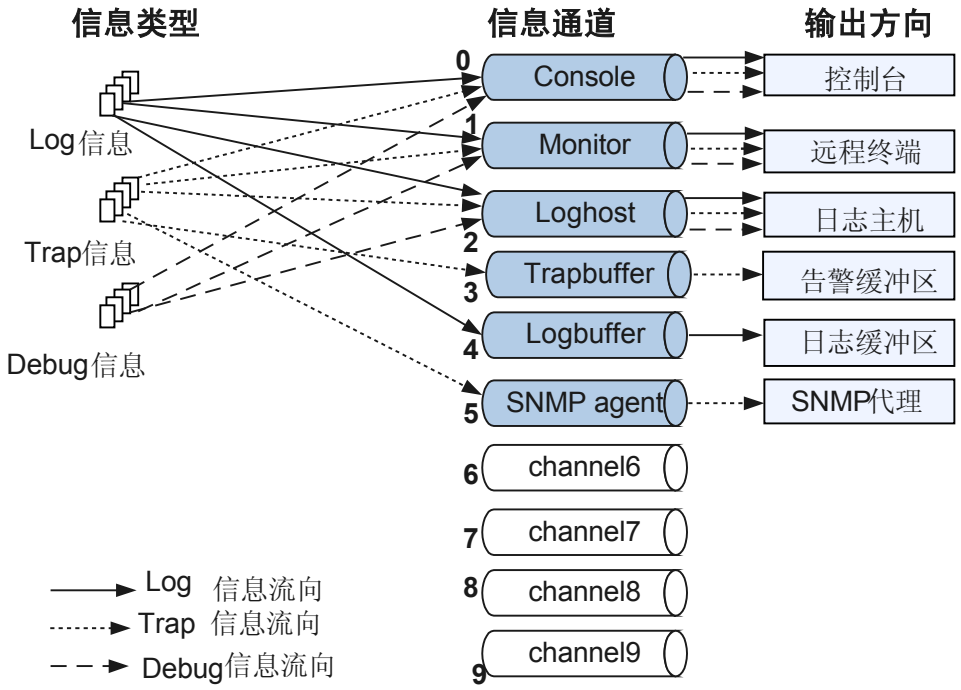
信息中心的工作过程如下：

- 接收各模块输出的日志信息（log）、告警信息（trap）和调试信息（debug）。
- 根据用户的设置，将不同重要程度的信息输出到不同的信息通道。
- 根据信息通道和输出方向的关联，将信息输出到不同方向。

概括来说，信息中心的主要工作就是将 3 种信息，按照 8 个严重等级，分配到 10 个信息通道中，再输出到多个方向。

如下图 2-3 所示。缺省情况下，日志、告警、调试信息都从缺省的信息通道输出。用户也可以指定从其他的通道进行输出，例如，用户配置发往日志缓存区的日志信息使用通道 6，则发送到日志缓存区的日志都会从通道 6 输出，不再从通道 4 输出。

图 2-3 信息中心的功能



版权所有 © 华为技术有限公司

信息通道和输出方向

信息中心支持 10 个通道，其中，通道 0 ～ 5 有缺省通道名。并且，这 6 个信息通道缺省与 6 个输出方向分别关联。

缺省通道和输出方向的对应关系请见表 2-2。

表 2-2 信息通道和输出方向

通道号	缺省通道名	输出方向	描述
0	console	console	本地控制台，可以接收日志、告警、调试信息。
1	monitor	monitor	VTY 终端，可以接收日志、告警、调试信息。方便远程维护。
2	loghost	loghost	日志主机，可以接收日志、告警、调试信息。信息在日志主机上以文件形式保存，供随时查看。
3	trapbuffer	trapbuffer	告警缓冲区，可以接收告警信息。在交换机内部分配，用于记录信息。
4	logbuffer	logbuffer	日志缓冲区，可以接收日志信息。在交换机内部分配，用于记录信息。
5	snmpagent	snmpagent	SNMP 代理，可以接收告警信息。
6	未指定	未指定	保留。
7	未指定	未指定	保留。
8	未指定	未指定	保留。
9	未指定	未指定	保留。

在配置多日志主机的情况下，用户可以配置日志信息通过一个通道或多个通道输出到不同的日志主机中。例如配置部分日志信息通过通道 2（loghost）输出到日志主机，部分日志信息从通道 6 输出到日志主机，还可以更改通道 6 的名称，便于对信息通道的管理。

日志信息的输出格式

Syslog 是信息中心（info-center）的一个子功能。Syslog 使用 UDP 进行传输，使用端口号 514 将日志信息输出到日志主机中。

日志格式如图 2-4 所示：

图 2-4 日志输出格式

<Int_16>TIMESTAMP HOSTNAME %%ddAAA/B/CCC(l):slot=XXX; YYYY

华为专有和保密信息
版权所有 © 华为技术有限公司

各字段的详细说明见表 2-3。

表 2-3 日志记录格式说明

字段	字段含义	说明
<Int_16>	前导符	在向日志主机发送的时候添加前导符，在设备本机保存的日志不保存前导符。
TIMESTAMP	时间戳，信息输出的时间	时间戳有 5 种格式可供选择。 ● short-date 型：与 date 型的唯一区别是，short-date 型时间戳不含年份。 ● format-date 型：另一种系统时间形式。 ● none 型：信息中不包含时间戳。 时间戳与主机名之间用一个空格隔开。
HOSTNAME	主机名	缺省是“Quidway”。
%%	华为公司的标识	标识该日志是由华为公司的产品输出的。
dd	版本号	用来标识该日志格式的版本。
AAA	模块名	向信息中心输出信息的模块名称。
B	日志的级别	表示日志信息的级别。
CCC	简要描述	用以进一步说明信息的类型。
(L)	信息的类别	L：用户日志标识。
slot=XXX	定位信息	slot：表示发送定位信息的槽位号。
YYYY	描述符	各个模块向信息中心输出的信息的具体内容。由各个模块在每次输出时填充，详细描述该日志的具体内容。

告警信息的输出格式

图 2-5 告警输出格式

TimeStamp HostName ModuleName/Severity/BriefDescription

各字段的详细说明见表 2-4。

版权所有 © 华为技术有限公司

表 2-4 告警记录格式说明

字段	字段含义	说明
TimeStamp	时间戳，信息输出的时间	时间戳有 5 种格式可供选择。 ● boot 型：相对时间类型。调试信息缺省采用 boot 型时间戳。 ● date 型：系统时间类型。告警信息和日志信息缺省采用 date 型时间戳。 ● short-date 型：与 date 型的唯一区别是，short-date 型时间戳不含年份。 ● format-date 型：另一种系统时间形式。 ● none 型：信息中不包含时间戳。 时间戳与主机名之间用一个空格隔开。
HostName	主机名	缺省是“Quidway”。主机名与模块名之间用一个空格隔开。
ModuleName	模块名	用来表示产生告警的模块名。
Severity	严重级别	告警的严重级别。 ● Critical（紧急） ● Major（重要） ● Minor（次要） ● Warning（提示） ● Indeterminate（不确定） ● Cleared（已清除）
Brief	简要描述	告警信息的简要描述。
Description	描述信息	告警信息的描述信息。

2.4.2 配置信息中心

介绍管理、配置信息中心的方法。

建立配置任务

在配置信息中心前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

需要记录 AC6605 设备运行时的调试信息、日志信息或告警信息，而且需要重定向输出到终端界面、缓冲区或主机以备存储和查阅时，则可以配置信息中心。

前置任务

无

版权所有 © 华为技术有限公司

数据准备

管理信息中心之前，需要准备以下数据。

序号	数据
1	（可选）信息通道的编号和名称
2	（可选）信息的时间戳格式
3	（可选）信息的级别
4	（可选）日志信息的语言、日志主机的地址
5	（可选）日志缓冲区、告警缓冲区的大小

使能信息中心的功能

只有在使能信息中心后，系统才会向日志主机、控制台等方向输出系统信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，使能信息中心功能。

----结束

（可选）命名信息通道

为方便记忆，管理员可以为信息通道命名。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel** *channel-number* **name** *channel-name*，为输出 Debug 信息、Log 信息或者 Trap 信息的通道命名。

----结束

定义信息通道的内容

管理员可以指定具体模块向信息通道中输出信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **debug** | **log** | **trap** } { **state** { **off** | **on** } | **level** *severity* } *] *，指定某个模块或所有模块向信息通道中添加 Debug 信息、Log 信息或者 Trap 信息。

版权所有 © 华为技术有限公司

说明

命令 **undo info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }可以用来禁用不需要的模块，只选择特定的某个或某几个模块向信息通道中输出信息。

----结束

（可选）设置输出信息的时间戳

管理员可以配置输出信息的时间戳格式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center timestamp debugging** { **boot** | **none** | { **short-date** | **format-date** | **date** } [**precision-time** { **tenth-second** | **second** }] }，配置输出 Debugging 信息的时间戳格式。

步骤 3 执行命令 **info-center timestamp** { **trap** | **log** } { **boot** | **none** | { **short-date** | **format-date** | **date** } [**precision-time** { **tenth-second** | **millisecond** }] }，配置输出 Log 信息或者 Trap 信息的时间戳格式。

----结束

检查配置结果

信息中心配置完成后，管理员可以通过命令行检查配置结果。

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看通道配置的内容	**display channel** [*channel-number* | *channel-name*]
查看信息中心记录的信息	**display info-center** [**statistics**]
查看内存日志缓冲区记录的信息	**display logbuffer** [**level** *severity* | **module** *module-name* | **size** *value* | **slot** *slot-id*]*
查看概要的日志缓冲区信息	**display logbuffer summary** [**level** *severity* | **slot** *slot-id*]*
查看告警缓冲区记录的信息	**display trapbuffer** [**size** *value*]

2.4.3 输出信息中心的信息

介绍将信息中心的信息输出到指定方向的方法。

向 Console 方向输出信息

管理员配置向 Console 方向输出信息。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center console channel** { *channel-number* | *channel-name* }，配置向 Console 方向输出信息。

步骤 3 执行命令 **quit**，返回到用户视图。

步骤 4 执行命令 **terminal monitor**，使能终端显示信息的功能，缺省情况下该功能处于开启状态。

步骤 5 执行命令 **terminal debugging**、**terminal logging** 或 **terminal trapping**，分别使能终端显示 Debug 信息、Log 信息或者 Trap 信息。

说明

步骤**步骤 4** 和**步骤 5** 在配置时没有先后顺序要求。

----结束

向 Telnet 终端输出信息

管理员配置向 Telnet 终端输出信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置向 Telnet 终端输出信息。

步骤 3 执行命令 **quit**，返回到用户视图。

步骤 4 执行命令 **terminal monitor**，使能终端显示信息的功能。

步骤 5 执行命令 **terminal debugging**、**terminal logging** 或 **terminal trapping**，分别使能终端显示 Debug 信息、Log 信息或者 Trap 信息。

说明

步骤**步骤 4** 和**步骤 5** 在配置时没有先后顺序要求。

----结束

向 SNMP 输出信息

管理员配置向 SNMP 输出信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center snmp channel** { *channel-number* | *channel-name* }，配置向 SNMP 输出信息。

步骤 3 执行命令 **snmp-agent**，启动 SNMP 代理功能。

版权所有 © 华为技术有限公司

有关 SNMP 代理的配置，请参见《AC6605 无线接入控制器 配置指南 网络管理》中的“SNMP 配置”章节。

----结束

向日志缓冲区输出信息

管理员配置向日志缓冲区输出信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *，配置向日志缓冲区输出信息。

----结束

向告警缓冲区输出信息

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *，配置向告警缓冲区输出信息。

----结束

向日志主机输出信息

管理员配置向日志主机输出信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置向 IPv4 日志主机输出信息。

步骤 3 执行命令 **info-center loghost ipv6** *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] }] *，配置向 IPv6 日志主机输出信息。

步骤 4 执行命令 **info-center loghost source** *interface-type interface-number*，配置发送日志信息的源接口。

----结束

版权所有 © 华为技术有限公司

检查配置结果

配置完信息中心的各通道输出信息后，可以查看信息中心的统计信息。

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看信息中心的统计信息	**display info-center [statistics]**

在配置成功时，执行上面的命令，应能得到以下结果：信息中心能够向目的终端输出统计信息。

2.4.4 维护

介绍清除统计信息的功能。

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作	命令
清除信息中心的统计信息	**reset info-center statistics**
清除日志缓冲区中的信息	**reset logbuffer**
清除告警缓冲区中的信息	**reset trapbuffer**

2.4.5 配置举例

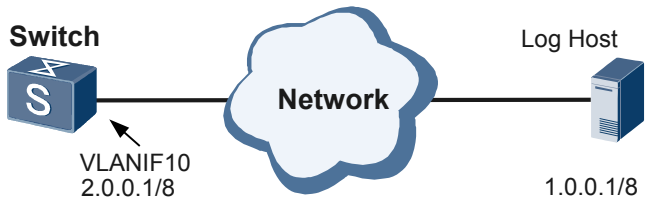
介绍常见的使用信息中心监控设备配置实例。

配置信息中心的示例

通过示例介绍如何配置信息中心。配置示例中包括组网需求、配置注意事项、配置思路等。

组网需求

图 2-6 向日志主机输出日志信息的组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置本举例：

1. 使能信息中心。
2. 配置信息通道，保证 AC6605 设备能正确的向日志主机发送日志信息。同时，关闭 AC6605 设备向日志主机输出调试信息和告警信息的输出开关。
3. 配置日志主机侧。

数据准备

为完成此配置例，需准备如下的数据：

- 日志主机的 IP 地址是 1.0.0.1/8。

配置步骤

说明

配置举例中，只列出了与监控相关的命令。日志主机侧的配置请参考日志主机的帮助文件。

1. 使能信息中心

   # 使能信息中心。缺省情况下，AC6605 设备的信息中心处于使能状态。

```
<Quidway> system-view
[Quidway] info-center enable
Info:Information center is enabled
```

2. 配置信息通道

   # 配置 AC6605 设备从 loghost 信息通道向日志主机输出所有模块的严重等级是 0 ～ 7 级的日志信息。同时，关闭 loghost 信息通道中调试信息和告警信息的输出开关。

```
[Quidway] info-center source default channel loghost log level debugging state on trap state off debug state off
```

   # 检查配置结果。

```
[Quidway] display channel loghost
channel number:2, channel name:loghost
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     N      debugging     N      debugging
```

3. 配置日志主机

   # 配置日志主机的 IP 地址是 1.0.0.1。

```
[Quidway] info-center loghost 1.0.0.1
```

   # 配置 AC6605 设备上向日志主机输出日志信息的接口是 VLANIF10。

```
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type hybrid
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-vlanif10] ip address 2.0.0.1 255.0.0.0
[Quidway-vlanif10] quit
[Quidway] info-center loghost source vlanif 10
```

   # 检查配置结果。

```
[Quidway] display info-center
Information Center:enabled
```


版权所有 © 华为技术有限公司

```
Log host:
         the interface name of the source address:vlanif 10
         1.0.0.1, channel number 2, channel name loghost,
                                    language English , host facility local7
Console:
         channel number : 0, channel name : console
Monitor:
         channel number : 1, channel name : monitor
SNMP Agent:
         channel number : 5, channel name : snmpagent
Log buffer:
         enabled,max buffer size 1024, current buffer size 512,
current messages 440, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 0
Trap buffer:
         enabled,max buffer size 1024, current buffer size 256,
current messages 1, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
Information timestamp setting:
         log - date, trap - date, debug - boot

 Sent messages = 499, Received messages = 499

 IO Reg messages = 0 IO Sent messages = 0
```

4. 打开 Console 终端的屏幕显示开关

   # 打开 Console 终端的屏幕显示开关。根据需要查看的信息类型，打开相应的屏幕显示开关。

```
[Quidway] info-center console channel 0
[Quidway] quit
<Quidway> terminal monitor
Info:Current terminal monitor is on
<Quidway> terminal logging
Info:Current terminal logging is on
```

配置文件

```
#
 info-center source default channel 2 log level debugging state on trap state off debug state off
 info-center loghost source vlanif 10
 info-center loghost 1.0.0.1
 #
 vlan batch 10
#
interface vlanif10
 ip address 2.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 10
#
return
```

2.5 监控口配置

配置监控口，对设备的环境进行监控。

2.5.1 监控口概述

监控口可以用于监控机柜门、设备电源、电池电量和空调电源。

AC6605 交换机在硬件上提供 4 个开关量输入，可以用于监控机柜门、设备电源、电池电量和空调电源，具体检测哪些设备由用户决定。根据 AC6605 这 4 个开关量状态的变

版权所有 © 华为技术有限公司

化生成 Trap 告警发送给网管（此时可以不用配置输出规则）。此外，AC6605 硬件上还提供 3 个开关量输出，可以连接声光报警设备，实现对设备周围环境的监控。

2.5.2 配置监控口与网管的关联

介绍如何配置监控口与网管的关联。

建立配置任务

在配置监控口与网管的关联前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 硬件上提供 4 个开关量输入，分别用于监控机柜门、设备电源、电池电量和空调电源，据 AC6605 这 4 个开关量状态的变化生成 Trap 告警发送给网管（此时可以不用配置输出规则）。每个输入的开关量对应 2 条 Trap 告警，4 个开关量分别对应 8 条告警：

Line ID	Normal Status	Trap(Warning)	Trap(Cancel)
1	low-level	InputLine1 abnormal	InputLine1 normal
2	high-level	InputLine2 abnormal	InputLine2 normal
3	low-level	InputLine3 abnormal	InputLine3 normal
4	low-level	InputLine4 abnormal	InputLine4 normal

前置任务

在配置监控口之前，需完成以下任务：

- 设备已经正常启动。
- 监控卡正常运行。

数据准备

在配置监控口之前，需准备以下数据。

序号	数据
1	由用户设定监控口输入线路 1 ～ 4 分别是以低电平为正常状态还是以高电平为正常状态。
2	确定各输入线路的名称。

配置监控口的输入线路

介绍如何配置监控线路的名称及正常状态的值。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor input** *id-number* **enable**，使能对各线路的监控。

步骤 3 执行命令 **monitor input** *id-number* **name** *line-name* **normal-state** { **low-level** | **high-level** }，设置所监控线路的名称以及正常状态的值。

----结束

检查配置结果

配置完监控口输入线路，可以使用命令行检查配置结果。

前提条件

已经完成对监控口输入线路的所有配置。

操作步骤

- 使用 **display monitor input** { *id-number* | **all** }命令查看之前所做的配置。

----结束

任务示例

在配置成功时，执行 **display monitor input all** 命令，能够查看到监控板上所有输入线路的信息。

```
<Quidway> display monitor input all
--------------------------------------------------------------------------
LineID  LineName              Enable  NormalStatus  CurrentStatus
--------------------------------------------------------------------------
1       Inputline1            enable  low-level     abnormal
2       Inputline2            enable  high-level    normal
3       Inputline3            enable  high-level    normal
4       Inputline4            enable  low-level     normal
--------------------------------------------------------------------------
```

分别改变输入线路 1 ～ 4 的高/低电平状态，告警上报正常：

- 对于输入线路 1 和 4 为高电平时上报输入线路不正常的告警，为低电平时恢复；
- 对于输入线路 2 和 3 为低电平时上报输入线路不正常的告警，为高电平时恢复。

2.5.3 配置监控口与声光报警设备的关联

管理员可以配置设备与声光报警设备的连接，当有异常情况时声光报警便会发出告警。

建立配置任务

在配置监控口与声光报警设备的关联前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 硬件上提供 4 个开关量输入，分别用于监控机柜门、设备电源、电池电量和空调电源，同时提供 3 个开关量输出，可以连接声光报警设备，当有异常情况发生时声光

版权所有 © 华为技术有限公司

报警便会发出告警。根据 AC6605 这 4 个开关量状态的变化控制 3 个开关量的输出，开关量输入与输出之间的关系可以通过命令灵活配置。

前置任务

在配置监控口之前，需完成以下任务：

- 设备已经正常启动。
- 监控卡正常运行。

数据准备

在配置监控口之前，需准备以下数据。

序号	数据
1	由用户设定监控口输入线路 1 ～ 4 分别是以低电平为正常状态还是以高电平为正常状态。
2	确定各输入线路的名称。

配置输入线路

介绍如何配置输入监控线路的名称及正常状态的值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor input** *id-number* **enable**，使能对各线路的监控。

步骤 3 执行命令 **monitor input** *id-number* **name** *line-name* **normal-state** { **low-level** | **high-level** }，设置所监控线路的名称以及正常状态的值。

----结束

配置输出线路

介绍如何配置输出端口所监控的输入端口以及输出端口和输入端口的逻辑关系。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor output** *id-number*，创建一个输出线路的输出控制列表，并进入 Output 视图。

步骤 3 执行命令 **rule** *rule-id* **match-input** *line-mask* **key** *level-value*，配置输出端口所监控的输入端口以及输出端口和输入端口的逻辑关系。

----结束

版权所有 © 华为技术有限公司

检查配置结果

配置完成后，可以使用命令行检查配置结果。

前提条件

已经完成对监控口输入线路和输出线路的所有配置。

操作步骤

- 使用 **display monitor output** *id-number* 命令查看之前所做的配置。

----结束

任务示例

在配置成功时，执行 **display monitor output 1** 命令，能够查看到监控口指定输出线路的匹配规则。

```
<Quidway> display monitor output 1
-------------------------------------------------------------------------------
RuleID    InputMask          LevelValue
-------------------------------------------------------------------------------
1            1001               1000
2            1100               0100
-------------------------------------------------------------------------------
```

2.5.4 配置举例

举例说明对监控口实际使用的配置。

配置监控口示例

通过示例介绍如何配置监控口。配置示例中包括组网需求、配置注意事项、配置思路等。

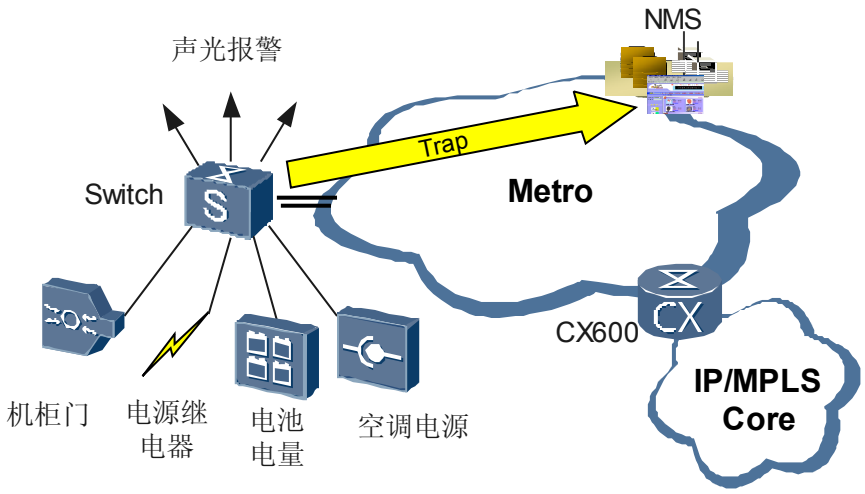
组网需求

如图 2-7 所示，AC6605 硬件上提供 4 个开关量输入，分别用于监控机柜门、设备电源、电池电量和空调电源，同时提供 3 个开关量输出，可以连接声光报警设备，当有异常情况发生时声光报警便会发出告警。Switch 依据这 4 个开关量状态的变化控制 3 个开关量的输出，开关量输入与输出之间的关系可以通过命令灵活配置。

监控输入口线路 1 ～ 4 分别连接监控机柜门、设备电源、电池电量和空调电源四个开关，设定正常状态下这 4 个输入线路都是高电平，若为低电平则表示相应设备出现异常。同时设定对机柜门和设备电源的监控分别对应输出电路 1 和 2，而输出线路 1、2 分别连接 2 个声光报警器，某一路发生异常时对应的报警器变亮。电池电量和空调电源两路异常时都对应输出线路 3，只要有任意一路发生异常，则与输出线路 3 连接的报警器变亮。

版权所有 © 华为技术有限公司

图 2-7 配置监控口示例组网图



配置思路

配置监控口的思路如下：

1. 配置输入线路。
2. 配置输出线路。
3. 配置输入线路与输出线路的逻辑关系。

数据准备

为完成此配置例，需准备如下的数据：

- 各输入线路的名称。
- 各输入线路在正常状态时的电平值，在本例中 1 ～ 4 路在正常状态下都为高电平。

操作步骤

步骤 1 在 Switch 上配置输入线路。

使能对 1 ～ 4 路输入线路的监控。

```
<Quidway> system-view
[Quidway] monitor input 1 enable
[Quidway] monitor input 2 enable
[Quidway] monitor input 3 enable
[Quidway] monitor input 4 enable
```

各输入线路的名称以及在正常状态时的电平值。

```
[Quidway] monitor input 1 name input1 normal-state high-level
[Quidway] monitor input 2 name input2 normal-state high-level
[Quidway] monitor input 3 name input3 normal-state high-level
[Quidway] monitor input 4 name input4 normal-state high-level
```

步骤 2 在 Switch 上配置输出线路。

配置输出线路 1 与输入线路 1 相关联，正常状态为高电平。

版权所有 © 华为技术有限公司

```
[Quidway] monitor output 1
[Quidway-monitor-output1] rule 1 match-input 1000 key 1000
[Quidway-monitor-output1] quit
```

配置输出线路 2 与输入线路 2 相关联，正常状态为高电平。

```
[Quidway] monitor output 2
[Quidway-monitor-output2] rule 1 match-input 0100 key 0100
[Quidway-monitor-output2] quit
```

配置输出线路 3 与输入线路 3、4 相关联，正常状态为高电平。

```
[Quidway] monitor output 3
[Quidway-monitor-output3] rule 1 match-input 0010 key 0010
[Quidway-monitor-output3] rule 2 match-input 0001 key 0001
[Quidway-monitor-output3] quit
```

步骤 3 验证配置结果

通过观察声光报警器验证上述配置是否生效：

- 当输入线路 1 由高电平变为低电平时，上报输入线路 1 异常告警，并且输出线路 1 的报警器亮；
- 当输入线路 2 由高电平变为低电平时，上报输入线路 2 异常告警，并且输出线路 2 的报警器亮；
- 当输入线路 3 和 4 任意一路变为低电平时，上报输入线路 3 异常告警，并且输出线路 3 的报警器亮。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
 monitor input 1 enable
 monitor input 1 name input1 normal-state high-level
 monitor input 2 enable
 monitor input 2 name input2 normal-state high-level
 monitor input 3 enable
 monitor input 3 name input3 normal-state high-level
 monitor input 4 enable
 monitor input 4 name input4 normal-state high-level
#
monitor output 1
 rule 1  match-input 1000 key 1000
monitor output 2
 rule 1  match-input 0100 key 0100
monitor output 3
 rule 1  match-input 0010 key 0010
 rule 2  match-input 0001 key 0001
#
return
```

2.6 使用镜像监控设备

镜像主要用来监控观察设备上符合某种要求的报文。

版权所有 © 华为技术有限公司

2.6.1 简介

介绍关于镜像的基本知识。

镜像功能

镜像是指在不影响报文正常处理流程的情况下，通过复制报文到观察端口，以便对报文进行监控观察的一种功能。管理员可以通过镜像功能进行网络检测和故障排除。

镜像分为接口镜像、流镜像、基于 VLAN 的镜像、基于 MAC 的镜像、CPU 镜像。

基本概念

- 观察接口

  观察接口是连接监控主机的接口，用于输出从镜像接口或流镜像接口所复制过来的报文。
- 镜像接口

  镜像接口是被观察的接口。从镜像接口输入或输出的所有报文都将被复制到观察接口。
- 流镜像接口

  流镜像接口是应用了包含流镜像行为的流策略的接口。从流镜像接口输入的报文，如果匹配此接口上流策略中的流分类，则将被复制到观察接口。
- 镜像流

  镜像流是输入到流镜像接口，并被观察的报文流。当某报文流成为镜像流后，此镜像流将被复制到观察接口。
- 镜像 VLAN

  镜像 VLAN 是被观察的 VLAN。从镜像 VLAN 输入的所有报文都将被复制到观察接口。
- 镜像 MAC

  镜像 MAC 是指用户需要镜像的报文的源或者目的 MAC 地址，AC6605 将符合镜像 MAC 地址的流量复制到观察接口。
- RSPAN VLAN

  RSPAN（Remote Switched Port Analyzer：远程交换接口分析器） VLAN 是指远程镜像 VLAN,当被镜像的报文和观察接口不是同一个交换机时，此时镜像接口的报文需要通过远程镜像 VLAN，以广播的方式传递到观察接口。
- 本地镜像

  当观察接口和镜像接口在同一个交换机上时，此时的镜像称为本地镜像。
- 远端镜像

  当观察接口和镜像接口不在同一交换机上时，此时的镜像称为远端镜像。

说明

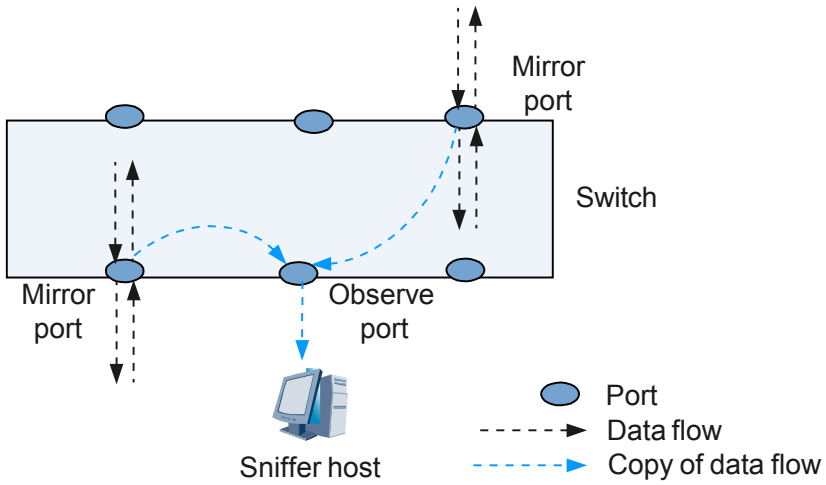
AC6605 不支持一条流同时镜像到多个观察接口。

基于接口的镜像

如图 2-8 所示，所谓基于接口的镜像，就是 AC6605 设备复制一份从镜像接口输入或输出的报文，并将此报文传送到指定的观察接口。

版权所有 © 华为技术有限公司

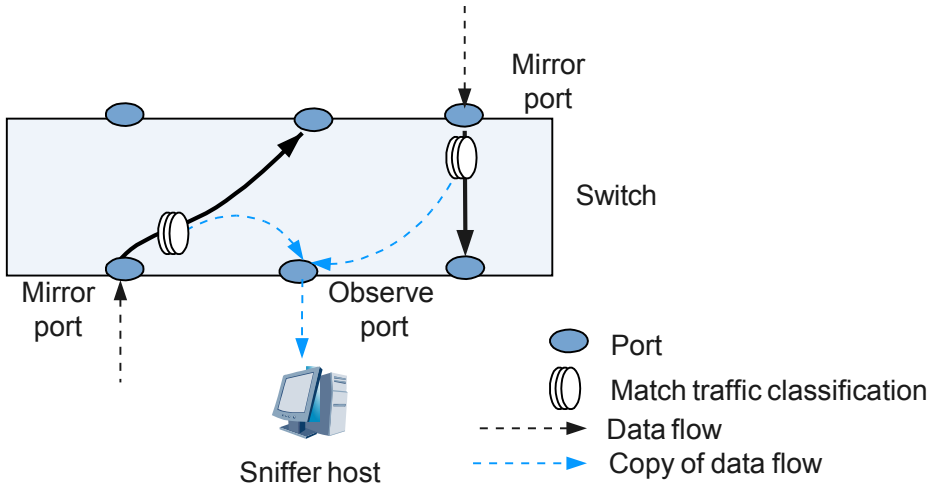
图 2-8 接口镜像示意图



流镜像

如图 2-9 所示，所谓流镜像，就是 AC6605 设备将镜像流（可能来自多个接口）复制到指定的观察接口。

图 2-9 流镜像示意图



流镜像是流行为中的一个动作，当配置了流镜像的流策略被应用在某接口上时，从这个接口输入的报文将与此流策略中的流分类进行匹配，如果报文流符合流分类，则复制此报文流到指定的观察接口。

基于 VLAN 的镜像

基于 VLAN 的镜像是指将指定 VLAN 内所有活动接口的入方向上的报文镜像到目的接口。配置了基于 VLAN 的镜像后，设备将 VLAN 内所有活动接口接收到的入方向所有

版权所有 © 华为技术有限公司

报文镜像到目的接口。与接口镜像相比，基于 VLAN 的镜像提供了一种更加广泛的镜像方式，用户可以对某个 VLAN 或者某些 VLAN 内的报文进行监控。

基于 MAC 的镜像

基于 MAC 地址的镜像提供了一种更加精确的镜像方式，用户可以对网络中特定设备的报文进行监控。在 VLAN 内匹配源或者目的 MAC 地址的报文会被镜像到指定接口。

CPU 镜像

CPU 镜像是对 CPU 接收到的报文进行镜像：

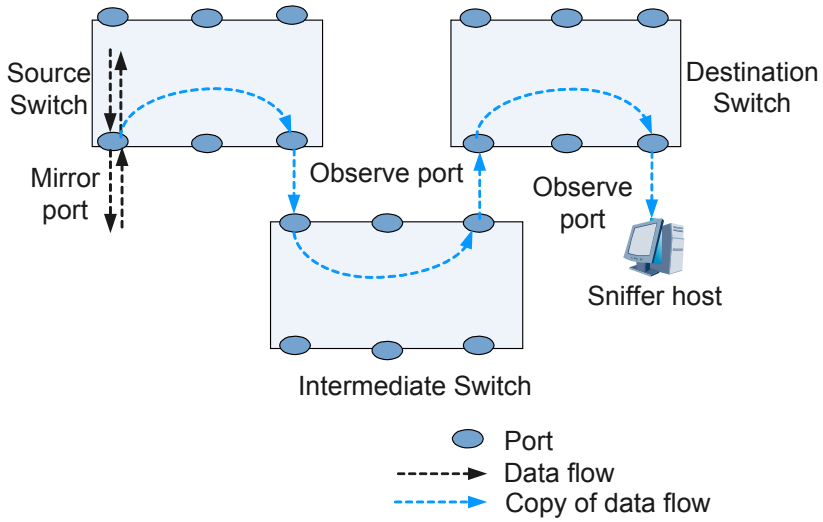
- 如果指定了 **acl** 参数，则将匹配指定 ACL 规则的报文镜像到指定的观察接口。
- 如果没有指定 **acl** 参数，则将 CPU 接收到的所有报文镜像到指定的观察接口。

CPU 镜像功能提供了一种调试方法，方便用户调试和定位问题。

远程镜像

接口镜像是 AC6605 设备复制一份从镜像接口输入或输出的报文，并将此报文传送到指定的观察接口。当观察接口和镜像接口不在同一交换机上时，需要使用远程镜像（Remote Switched Port Analyzer：远程交换接口分析器）技术来满足这一需求。

图 2-10 远程镜像示意图



如图 2-10 所示，其中：

- **Source Switch** 为镜像接口所在的 Switch。
- **Destination Switch** 为观察接口所在的 Switch。
- **Intermediate Switch** 为连接 **Source Switch** 和 **Destination Switch** 的中间设备。

说明

在远程镜像中如果 Source Switch 和 Destination Switch 直接连接，则没有 Intermediate Switch 设备。

华为专有和保密信息
版权所有 © 华为技术有限公司

远程镜像是将镜像报文在 RSPAN VLAN 中，以广播的方式从 Source Switch 传递到 Destination Switch。其中 Source Switch、Intermediate Switch 和 Destination Switch 互连的接口都属于 RSPAN VLAN。

在 Source Switch 设备上，被镜像的报文通过 observe port 转发到 **Intermediate Switch**，最终在 RSPAN VLAN 以广播的方式转发到 Destination Switch 的 observe port。

在 **Destination Switch** 设备上的 observe port 负责接收被镜像的远端报文。

通过 RSPAN 的功能，可以将基于接口镜像、VLAN 镜像、MAC 地址镜像、接口流镜像的流量转发到目标观察接口。

2.6.2 建立基于接口的本地镜像

介绍基于接口的本地镜像的配置方法。

建立配置任务

应用环境

监控 AC6605 设备上某接口所有的输入或输出报文时，如果镜像接口和观察接口在同一个 AC6605，可以配置基于接口的本地镜像功能。

前置任务

无

数据准备

在配置接口镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号
2	镜像接口的类型和编号

配置基于接口的本地镜像

背景信息

配置镜像的接口可以是物理接口，也可以是 Eth-Trunk 接口。

若镜像端口为 Eth-trunk 类型，需要预先使用命令 **interface eth-trunk** *trunk-id* 创建 Eth-trunk。

- 若已经配置 Eth-trunk 为镜像端口，则不能再单独配置其成员接口为镜像端口。
- 若已经配置 Eth-trunk 下某成员接口为镜像端口，则不能再配置 Eth-trunk 为镜像端口。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number* ，配置观察接口。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入镜像接口的接口视图。

步骤 4 执行命令 **port-mirroring to observe-port** *index* { **both** | **inbound** | **outbound** } ，配置接口镜像。

当需要同时监控多个接口的入方向或出方向的报文时，可以重复执行步骤**步骤 3** 和步骤**步骤 4**。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看接口镜像信息列表	**display port-mirroring**
查看观察端口的使用情况	**display observe-port**

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察接口的编号。
- 正确配置了镜像接口的编号和镜像的方向。

2.6.3 建立基于接口的远程镜像

介绍基于接口的远程镜像配置方法。

建立配置任务

应用环境

监控 AC6605 设备上某个或某些接口的输入或输出报文时，当被监控接口和观察接口不在同一个 AC6605 上时，可以配置基于接口的远程镜像功能。

前置任务

无

数据准备

在配置接口镜像之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	观察接口的类型和编号
2	镜像接口编号
3	远程镜像 VLAN 的编号

配置基于接口的远程镜像

背景信息

配置镜像的接口可以是物理接口，也可以是 Eth-Trunk 接口。

若镜像端口为 Eth-trunk 类型，需要预先使用命令 **interface eth-trunk** *trunk-id* 创建 Eth-trunk。

- 若已经配置 Eth-trunk 为镜像端口，则不能再单独配置其成员接口为镜像端口。
- 若已经配置 Eth-trunk 下某成员接口为镜像端口，则不能再配置 Eth-trunk 为镜像端口。

操作步骤

- 在 Source Switch 设备上配置需要远程镜像的接口和远程镜像 VLAN

  说明

  镜像端口不允许加入到远程镜像 VLAN。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 RSPAN VLAN 并进入 VLAN 视图。
  3. 执行命令 **mac-address learning disable**，关闭 MAC 地址学习功能。

     说明

     如果在此 VLAN 上关闭了 MAC 地址的学习功能，则不能在该 VLAN 上配置其它业务。
  4. 执行命令 **quit** 返回系统视图。
  5. 执行命令 **observe-port** *index* **interface** *interface-type interface-number* [**vlan** *vlan-id*]，配置观察接口并指定远程镜像 VLAN。
  6. 执行命令 **interface** *interface-type interface-number*，进入远程镜像接口的接口视图。
  7. 执行命令 **port-mirroring to observe-port** *index* { **both** | **inbound** | **outbound** }，配置接口镜像。

     当需要同时监控多个接口的入方向或出方向的报文时，可以重复执行步骤**步骤 6** 和步骤**步骤 7**。
- 在 Intermediate Switch 设备上配置远程镜像 VLAN 和远程镜像 VLAN 的接口属性

  说明

  镜像端口不允许加入到远程镜像 VLAN。

  在 Intermediate Switch 设备上进行如下配置，其中 Intermediate Switch 与 Source Switch 和 Destination Switch 连接的接口的配置相同。如果没有 Intermediate Switch 则取消该步骤配置。

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，创建远程镜像 VLAN 并进入 VLAN 视图。
3. 执行命令 **quit** 返回系统视图。
4. 执行命令 **interface** *interface-type interface-number*，进入 Intermediate Switch 与 Source Switch 和 Destination Switch 连接的接口的接口视图。
5. 执行命令 **port link-type trunk** 将接口的链路类型配置为 Trunk。
6. 执行命令 **port trunk allow-pass vlan** *vlan-id*，配置接口加入 RSPAN VLAN。
7. 执行命令 **quit** 返回系统视图。

- 在 Destination Switch 设备上配置远程镜像的观察接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，创建远程镜像 VLAN 并进入 VLAN 视图。
3. 执行命令 **quit** 返回系统视图。
4. 执行命令 **interface** *interface-type interface-number*，进入 Intermediate Switch 和 Destination Switch 连接的接口的接口视图。

   说明

   如果没有 Intermediate Switch 设备，此时进入 Source Switch 与 Destination Switch 连接的接口的接口视图。
5. 执行命令 **port link-type trunk** 将接口的链路类型配置为 Trunk。
6. 执行命令 **port trunk allow-pass vlan** *vlan-id*，配置接口加入 RSPAN VLAN。
7. 执行命令 **interface** *interface-type interface-number*,进入观察接口的接口视图。
8. 执行命令 **port hybrid untagged vlan** *vlan-id*，将观察接口配置为 Hybrid 类型并允许远端镜像 VLAN 的报文通过。
9. 执行命令 **quit** 返回系统视图。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置 RSPAN VLAN。
- 正确配置了观察接口的编号。
- 正确配置了观察端口的类型。
- 正确配置了镜像接口的编号和镜像的方向。

2.6.4 删除基于接口的镜像

介绍删除接口的镜像的方法。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

当不需要监控 AC6605 设备上某接口所有的输入或输出报文，而当前该监控功能又处于使能状态时，或是在删除、变更被绑定的观察接口前，都需要先删除接口镜像。

前置任务

无

数据准备

在删除接口镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号
2	待删除的镜像接口的类型和编号

删除接口镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入镜像接口的接口视图。

步骤 3 执行命令 **undo port-mirroring** { **both** | **inbound** | **outbound** }，删除接口镜像。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在删除成功时，执行上面的命令，应能得到如下结果：已配置的接口镜像被正确删除。

2.6.5 建立基于 VLAN 的本地镜像

介绍基于 VLAN 本地镜像的配置方法。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

当需要监控 AC6605 设备上某个或某些 VLAN 所有活动接口的输入报文时，如果被监控的数据和观察接口在同一个 AC6605 时，可以配置基于 VLAN 的本地镜像功能。

前置任务

需要监控的 VLAN 已经被建立，并且该 VLAN 中已经加入了物理接口。

数据准备

在配置基于 VLAN 的本地镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号
2	镜像 VLAN 编号

配置基于 VLAN 的本地镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number*，配置观察接口。

步骤 3 执行命令 **vlan** *vlan-id*，进入镜像 VLAN 的 VLAN 视图。

步骤 4 执行命令 **mirroring to observe-port** *index* **inbound**，配置 VLAN 镜像。

当需要同时监控多个 VLAN 的入方向的报文时，可以重复执行步骤**步骤 3** 和步骤**步骤 4**。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在配置成功时，执行上面的命令，应能得到以下结果：

版权所有 © 华为技术有限公司

- 正确配置了观察端口的类型。
- 正确配置了观察接口的编号。

2.6.6 建立基于 VLAN 的远程镜像

介绍了基于 VLAN 的远程镜像配置方法。

建立配置任务

应用环境

需要监控 AC6605 设备上某个或某些 VLAN 所有活动接口的输入报文时，当被监控 VLAN 和观察接口不在同一个 AC6605 时，可以配置基于 VLAN 的远程镜像功能。

前置任务

被监控的 VLAN 已经建立，并且该 VLAN 中已经加入了物理接口。

数据准备

在配置基于 VLAN 的远程镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号
2	镜像 VLAN 编号
3	RSPAN VLAN 的编号

配置基于 VLAN 的远程镜像

操作步骤

- 在 Source Switch 设备上配置基于 VLAN 的远程镜像

  说明

  镜像端口不允许加入到 RSPAN VLAN。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 RSPAN VLAN 并进入 VLAN 视图。
  3. 执行命令 **mac-address learning disable**，关闭 MAC 地址学习功能。

     说明

     如果在此 VLAN 上关闭了 MAC 地址的学习功能，则不能在该 VLAN 上配置其它业务。
  4. 执行命令 **quit** 返回系统视图。
  5. 执行命令 **observe-port** *index* **interface** *interface-type interface-number* [**vlan** *vlan-id*]，配置观察接口并指定 RSPAN VLAN。
  6. 执行命令 **vlan** *vlan-id*，进入镜像 VLAN 的 VLAN 视图。

版权所有 © 华为技术有限公司

7. 执行命令 **mirroring to observe-port** *index* **inbound**，配置基于 VLAN 的远程镜像。

   当需要同时监控多个 VLAN 的入方向的报文时，可以重复执行步骤**步骤 6** 和步骤**步骤 7**。

- 在 Intermediate Switch 设备上配置 RSPAN VLAN 和 RSPAN VLAN 的接口属性

  Intermediate Switch 设备上配置和基于接口的远程镜像中的 Intermediate Switch 设备上配置相同。对于 Intermediate Switch 设备上配置请参见**配置基于接口的远程镜像**。

- 在 Destination Switch 设备上配置远程镜像的观察接口

  Destination Switch 设备上配置和基于接口的远程镜像中的 Destination Switch 设备上配置相同。对于 Destination Switch 设备上配置请参见**配置基于接口的远程镜像**。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察端口的类型。
- 正确配置了观察接口的编号。

2.6.7 删除基于 VLAN 的镜像

介绍删除基于 VLAN 的本地和远程镜像的方法。

建立配置任务

应用环境

当不需要监控 AC6605 设备上某 VLAN 所有的输入报文，而当前该监控功能又处于使能状态时，或是在删除、变更被绑定的观察接口前，都需要先删除基于 VLAN 的镜像。

前置任务

无

数据准备

在删除基于 VLAN 的镜像之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	待删除的镜像 VLAN 的编号

删除基于 VLAN 的镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入被监控 VLAN 的 VLAN 视图。

步骤 3 执行命令 **undo mirroring inbound**，删除基于 VLAN 的镜像。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在删除成功时，已配置的基于 VLAN 的镜像被正确删除。

2.6.8 建立基于 MAC 地址的本地镜像

介绍基于 MAC 地址的本地镜像配置方法。

建立配置任务

应用环境

监控 AC6605 设备上某 VLAN 的源或目的 MAC 地址为指定 MAC 地址的输入报文时，如果被监控的指定 MAC 地址的报文和观察接口在同一个 AC6605 时，可以配置基于 MAC 地址的本地镜像功能。

前置任务

无

数据准备

在配置 MAC 镜像之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	观察接口的类型和编号
2	镜像 MAC 地址
3	镜像 MAC 地址所在 VLAN 的编号

配置基于 MAC 地址的本地镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number*，配置观察接口。

步骤 3 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 4 执行命令 **mac-mirroring** *mac-address* **to observe-port** *index* **inbound**，配置基于 MAC 地址的镜像。

当需要同时监控多个 VLAN 中多个 MAC 地址的入方向报文时，可以重复执行步骤步骤 3 和步骤步骤 4。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口镜像信息列表	**display port-mirroring**

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察端口的类型。
- 正确配置了观察接口的编号。

2.6.9 建立基于 MAC 地址的远程镜像

介绍基于 MAC 地址的远程镜像配置方法。

华为专有和保密信息
版权所有 © 华为技术有限公司

建立配置任务

应用环境

监控 AC6605 设备上某 VLAN 的源或目的 MAC 为指定 MAC 地址的输入报文时，当被监控指定 MAC 的报文和观察接口不在同一个 AC6605 上时，可以配置基于 MAC 的远程镜像功能。

前置任务

无

数据准备

在配置 MAC 地址镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号
2	镜像 MAC 地址
3	镜像 MAC 地址所在 VLAN 的编号
4	RSPAN VLAN 的编号

建立基于 MAC 地址的远程镜像

介绍基于 MAC 地址的远程镜像配置方法。

操作步骤

- 在 Source Switch 设备上配置基于 MAC 地址的远程镜像

  说明

  镜像端口不允许加入到 RSPAN VLAN。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 RSPAN VLAN 并进入 VLAN 视图。
  3. 执行命令 **mac-address learning disable**，关闭 MAC 地址学习功能。

     说明

     如果在此 VLAN 上关闭了 MAC 地址的学习功能，则不能在该 VLAN 上配置其它业务。
  4. 执行命令 **quit** 返回系统视图。
  5. 执行命令 **observe-port** *index* **interface** *interface-type interface-number* [**vlan** *vlan-id*]，配置观察接口并指定 RSPAN VLAN。
  6. 执行命令 **vlan** *vlan-id*，进入被监控 MAC 地址所在 VLAN 的 VLAN 视图。
  7. 执行命令 **mac-mirroring** *mac-address* **to observe-port** *index* **inbound**，配置远程 MAC 地址镜像并指定 RSPAN VLAN。

版权所有 © 华为技术有限公司

当需要同时监控多个源或目的为指定 MAC 地址的入方向的报文时，可以重复执行步骤**步骤 6** 和步骤**步骤 7**。

- 在 Intermediate Switch 设备上配置 RSPAN VLAN 和 RSPAN VLAN 的接口属性

  Intermediate Switch 设备上配置和基于接口的远程镜像中的 Intermediate Switch 设备上配置相同。对于 Intermediate Switch 设备上配置请参见**配置基于接口的远程镜像**。

- 在 Destination Switch 设备上配置远程镜像的观察接口

  Destination Switch 设备上配置和基于接口的远程镜像中的 Destination Switch 设备上配置相同。对于 Destination Switch 设备上配置请参见**配置基于接口的远程镜像**。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看基于 MAC 地址镜像信息列表	**display port-mirroring**

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察端口的类型。
- 正确配置 RSPAN VLAN。
- 正确配置了观察接口的编号。

2.6.10 删除基于 MAC 地址的镜像

介绍删除基于 MAC 地址镜像的配置方法。

建立配置任务

应用环境

当不需要监控 AC6605 设备上 VLAN 中特定 MAC 的输入报文，而当前该监控功能又处于使能状态时，或是在删除、变更被绑定的观察接口前，都需要先删除基于 MAC 地址的镜像。

前置任务

无

数据准备

在删除基于 MAC 地址的镜像之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	待删除的镜像 MAC 地址

删除基于 MAC 地址的镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入被监控 MAC 地址的报文所在 VLAN 的 VLAN 视图。

步骤 3 执行命令 **undo mac-mirroring** *mac-address* **inbound**，删除基于 MAC 地址的镜像。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看镜像端口的配置情况	**display port-mirroring**

在删除成功时，已配置的基于 MAC 地址的镜像被正确删除。

2.6.11 建立基于流的本地流镜像

介绍本地流镜像的配置方法。

建立配置任务

应用环境

当需要监控输入 AC6605 设备的具有某些相同属性的报文流时，如果被监控数据和观察接口在同一个 Switch，可以配置基于流的本地镜像功能。

前置任务

无

数据准备

在配置流镜像之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	观察接口的类型和编号
2	流镜像接口的类型和编号
3	流分类、流行为和流策略的名称

配置流分类规则

说明

流分类视图下各流分类匹配规则之间没有先后次序，可以叠加和组合使用，共同提供流分类依据。

配置流分类规则的具体步骤请参见《*AC6605 无线接入控制器 配置指南-QoS*》的**配置复杂流分类**。

配置流镜像动作

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number*，配置观察接口。

步骤 3 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。

步骤 4 执行命令 **mirroring to observe-port** *index*，配置基于流分类的流镜像。

----结束

后续处理

在流行为中配置了流镜像动作后，需要在流策略中将该流行为与某个流分类进行绑定，最后在接口上应用该策略。具体的配置步骤请参见**创建和应用策略**。

创建和应用策略

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic policy** *policy-name*，创建流策略，并进入流策略视图。

步骤 3 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定类配置流行为。

本步骤中参数 *class-name* 的取值必须与**配置流分类规则**中所创建的流分类名相同。

本步骤中参数 *behavior-name* 的取值必须与**配置流镜像动作**中步骤**步骤 3** 的参数 *behavior-name* 相同。

步骤 4 执行命令 **quit**，返回系统视图。

版权所有 © 华为技术有限公司

步骤 5 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 6 执行命令 **traffic-policy** *policy-name* **inbound**，在接口上应用包含了流镜像动作的流策略。

当需要同时监控多个接口的，且具有某些相同属性的入方向的报文流时，可以重复执行步骤步骤 5 和步骤步骤 6。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口的镜像信息	**display port-mirroring**
查看在接口上应用流策略中的流镜像配置	**display traffic policy interface** [*interface-type interface-number*] [**inbound**]

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察接口的接口编号。
- 在需要监控入方向报文流的接口上应用了正确的流策略。
- 被应用的流策略中包含了正确的流分类和流行为，且流行为中包含流镜像。

2.6.12 建立基于流的远程流镜像

介绍远程流镜像的配置方法。

建立配置任务

应用环境

当需要监控输入 AC6605 设备的具有某些相同属性的报文流时，如果被监控的数据和观察接口不在同一个 AC6605 时，可以配置基于流的远程镜像功能。

前置任务

无

数据准备

在配置基于流的远程镜像之前，需要准备以下数据。

序号	数据
1	观察接口的类型和编号

版权所有 © 华为技术有限公司

序号	数据
2	流镜像接口的类型和编号
3	流分类、流行为和流策略的名称
4	RSPAN VLAN 的编号

配置流分类规则

背景信息

关于配置流分类规则请参见**配置流分类规则**

建立基于流分类的远程镜像

操作步骤

- 在 Source Switch 设备上配置基于流分类的远程镜像

  说明

  镜像端口不允许加入到 RSPAN VLAN。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 RSPAN VLAN 并进入 VLAN 视图。
  3. 执行命令 **mac-address learning disable**，关闭 MAC 地址学习功能。

     说明

     如果在此 VLAN 上关闭了 MAC 地址的学习功能，则不能在该 VLAN 上配置其它业务。
  4. 执行命令 **quit** 返回系统视图。
  5. 执行命令 **observe-port** *index* **interface** *interface-type interface-number* [**vlan** *vlan-id*]，配置观察接口并指定 RSPAN VLAN。
  6. 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
  7. 执行命令 **mirroring to observe-port** *index*，配置基于流分类远程镜像。

     在流行为中配置了流镜像动作后，需要在流策略中将该流行为与某个流分类进行绑定，最后在接口上应用该策略。具体的配置步骤请参见**创建和应用策略**。
- 在 Intermediate Switch 设备上配置远程镜像 VLAN 和远程镜像 VLAN 的接口属性

  Intermediate Switch 设备上配置和基于接口的远程镜像中的 Intermediate Switch 设备上配置相同。对于 Intermediate Switch 设备上配置请参见**配置基于接口的远程镜像**。
- 在 Destination Switch 设备上配置远程镜像的观察接口

  Destination Switch 设备上配置和基于接口的远程镜像中的 Destination Switch 设备上配置相同。对于 Destination Switch 设备上配置请参见**配置基于接口的远程镜像**。

----结束

创建和应用策略

版权所有 © 华为技术有限公司

背景信息

关于在 Source Switch 设备上配置流分类规则的方法请参见创建和应用策略

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口的镜像信息	**display port-mirroring**
查看在接口上应用流策略中的流镜像配置	**display traffic policy interface** [*interface-type interface-number*] [**inbound**]

在配置成功时，执行上面的命令，应能得到以下结果：

- 正确配置了观察接口的接口编号。
- 正确配置了观察端口的类型。
- 正确配置 RSPAN VLAN。
- 在需要监控入方向报文流的接口上应用了正确的流策略。
- 被应用的流策略中包含了正确的流分类和流行为，且流行为中包含流镜像。

2.6.13 删除基于流的镜像

介绍删除流镜像的方法。

建立配置任务

应用环境

当不需要监控输入 AC6605 设备的具有某些相同属性的报文流，而当前该监控功能又处于使能状态时，可以删除流镜像。

前置任务

无

数据准备

在删除流镜像之前，需要准备以下数据。

序号	数据
1	待删除的流镜像接口的类型和编号
2	流策略的名称

版权所有 © 华为技术有限公司

删除流镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name* 进入流行为视图。

步骤 3 执行命令 **undo mirroring** 取消该流的镜像动作。

步骤 4 执行命令 **quit** 退出流行为视图。

步骤 5 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 6 执行命令 **undo traffic-policy inbound**，在该接口上取消已被创建的流策略，删除流镜像。

若要删除这个流策略，须在所有已经应用该流策略的接口上执行取消操作，然后在系统视图下执行 **undo traffic policy** *policy-name* 命令删除该流策略。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口的镜像信息	**display port-mirroring**
查看在接口上应用流策略中的流镜像配置	**display traffic policy interface** [*interface-type interface-number*] [**inbound**]

在删除成功时，执行上面的命令，应能得到以下结果：

已配置过某流策略的接口上的相应流策略被正确删除。

2.6.14 删除或变更观察接口

介绍删除或变更观察接口的方法。

建立配置任务

应用环境

当不需要对流量进行监控或需要指定观察接口为设备上另外的接口时，可以删除或变更观察接口。

前置任务

在执行此任务前，需要先在该观察接口上执行 **2.6.4 删除基于接口的镜像**、**2.6.7 删除基于 VLAN 的镜像**、**2.6.10 删除基于 MAC 地址的镜像**、**2.6.13 删除基于流的镜像**。

版权所有 © 华为技术有限公司

数据准备

在删除或变更观察接口之前，需要准备以下数据。

序号	数据
1	新观察接口的类型和编号

（可选）删除观察接口

前提条件

删除观察接口前，请确保观察接口没有被引用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入镜像接口的接口视图。

步骤 3 执行命令 **undo port-mirroring** { **both** | **inbound** | **outbound** }，删除接口镜像。

步骤 4 执行命令 **quit**，退出到系统视图。

步骤 5 执行命令 **undo observe-port** *index*，删除观察接口。

----结束

（可选）变更观察接口

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number*，变更观察接口，指定于新的接口。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看观察端口的使用情况	**display observe-port**
查看接口的镜像信息	**display port-mirroring**

在删除或变更成功时，执行上面的命令，应能得到以下结果：观察接口被删除或被成功指定于新的接口。

版权所有 © 华为技术有限公司

2.6.15 配置 CPU 镜像

介绍配置 CPU 镜像的方法。

建立配置任务

应用环境

在调试 AC6605 设备时，如果需对 CPU 接收报文的情况进行监控时，可配置 CPU 镜像功能。

前置任务

无

数据准备

在配置 CPU 镜像之前，需要准备以下数据。

序号	数据
1	（可选）进行 ACL 过滤的 ACL 编号和 ACL 规则
2	观察接口的索引、类型和编号

（可选）配置 ACL 规则

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number*，创建一个 ACL，并进入 ACL 视图。

关于 **acl** 命令的详细解释，请参见《AC6605 无线接入控制器 命令参考》。

步骤 3 执行 **rule** 命令，创建基本 ACL 或高级 ACL 规则。

关于 **rule** 命令的详细解释，请参见《AC6605 无线接入控制器 命令参考》。

----结束

配置观察接口

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **observe-port** *index* **interface** *interface-type interface-number*，配置全局观察接口。

----结束

版权所有 © 华为技术有限公司

配置 CPU 镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **port-mirroring cpu** [**acl** *acl-number*] **to observe-port** *index* **inbound** ，配置 CPU 镜像。

缺省情况下，没有使能 CPU 镜像功能。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看接口的镜像信息	**display port-mirroring**
查看 CPU 镜像信息	**display cpu port-mirroring**

在配置成功时，执行 **display cpu port-mirroring** 命令，可以查看 CPU 接收到的报文所匹配的 ACL 编号和镜像所指定的观察接口。

2.6.16 删除 CPU 镜像

介绍删除 CPU 镜像的配置方法。

建立配置任务

应用环境

当不需要对 AC6605 设备 CPU 接收报文的情况进行监控时，可以删除 CPU 镜像配置。

前置任务

无

数据准备

在删除 CPU 镜像之前，需要准备以下数据。

序号	数据
1	观察接口的编号

版权所有 © 华为技术有限公司

删除 CPU 镜像

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **undo port-mirroring cpu**，删除 CPU 镜像配置。

步骤 3 **可选:** 执行命令 **undo observe-port** *index*，删除观察接口和对应的索引。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看接口的镜像信息	**display port-mirroring**
查看 CPU 镜像信息	**display cpu port-mirroring**

2.6.17 配置举例

介绍与镜像相关的组网举例。

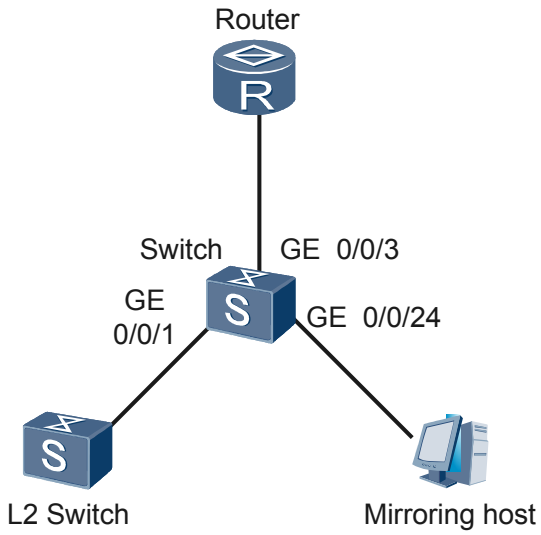
配置基于接口的本地镜像示例

配置需求

如图 2-11 所示，Switch 与 L2 Switch、PC 及路由器相连，现需要使用 PC 对 L2 Switch 发往 Switch 的报文进行监控，以检查该类报文的转发是否正常。此时，可以在 Switch 上配置基于接口的本地镜像。

将 GigabitEthernet0/0/1 接口作为镜像接口，将 GigabitEthernet0/0/24 接口作为观察接口。

图 2-11 基于接口的本地镜像组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置接口镜像的基本功能：

1. 将 GigabitEthernet0/0/24 接口配置为观察接口。
2. 将 GigabitEtherner0/0/1 接口配置为镜像接口。

数据准备

配置时需要准备如下数据：

- 接口加入的 VLAN ID。

配置步骤

1. 在 Switch 上创建 VLAN，把相应接口以 Trunk 方式加入 VLAN

   # 将接口 GigabitEthernet0/0/1 和 GigabitEthernet0/0/3 以 Trunk 方式加入同一 VLAN。（以下配置以接口 GigabitEthernet0/0/1 为例，同理配置接口 GigabitEthernet0/0/3）

   ```
   <Switch> system-view
   [Switch] vlan 10
   [Switch-vlan10] quit
   [Switch] interface gigabitethernet 0/0/1
   [Switch-GigabitEthernet0/0/1] port link-type trunk
   [Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
   [Switch-GigabitEthernet0/0/1] quit
   ```

2. 配置观察接口

   # 将 GigabitEthernet0/0/24 接口配置为观察接口。

   ```
   <Switch> system-view
   [Switch] observe-port 1 interface gigabitethernet 0/0/24
   ```

3. 配置镜像接口

   # 将 GigabitEthernet0/0/1 接口配置为镜像接口。

   ```
   [Switch] interface gigabitethernet 0/0/1
   [Switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
   [Switch-GigabitEthernet0/0/1] quit
   ```

4. 检查配置结果

   # 执行 **display port-mirroring** 命令查看观察接口和镜像接口的配置情况。

   ```
   [Switch] display port-mirroring
     Port-mirror:
     ------------------------------------------------------------------------
     Mirror-port              Direction     Observe-port
     ------------------------------------------------------------------------
     GigabitEthernet0/0/1            Inbound       GigabitEthernet0/0/24
     ------------------------------------------------------------------------
   ```

配置文件

Switch 的配置文件。

```
#
 sysname Switch
#
 observe-port 1 interface GigabitEthernet0/0/24
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 port-mirroring to observe-port 1 inbound
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

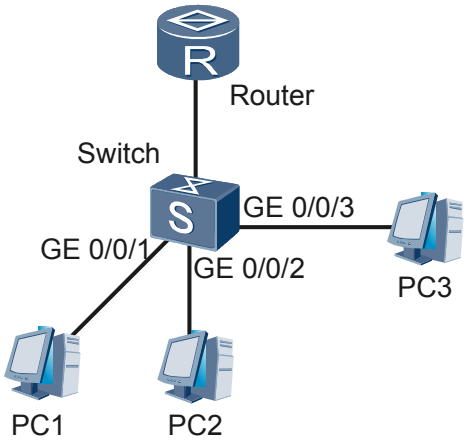
配置基于 VLAN 的本地镜像示例

配置需求

如图 2-12 所示，GigabitEthernet0/0/1 接口连接 PC1,GigabitEthernet0/0/2 连接 PC2，PC1 与 PC2 同属于 VLAN10。现在需要监控 VLAN10 的所有活动接口的入流量。此时，可以在 Switch 设备上配置基于 VLAN 的本地镜像。

其中 GigabitEthernet0/0/3 接口作为观察接口。

图 2-12 基于 VLAN 的本地镜像组网图



配置思路

采用如下的思路配置基于 VLAN 的本地镜像的基本功能：

1. 将 GigabitEthernet0/0/3 接口配置为观察接口。
2. 将 VLAN10 配置为镜像 VLAN。

数据准备

无

配置步骤

1. 配置观察接口

   # 将 GigabitEthernet0/0/3 接口配置为观察接口。

版权所有 © 华为技术有限公司

```
<Switch> system-view
<Switch> interface GigabitEthernet 0/0/3
<Switch-GigabitEthernet0/0/3> quit
[Switch] observe-port 1 interface gigabitethernet 0/0/3
```

2. 配置镜像 VLAN

   # 将 VLAN10 配置为镜像 VLAN。

```
[Switch] vlan 10
[Switch-vlan10] mirroring to observe-port 1 inbound
[Switch-vlan10] quit
```

3. 检查配置结果

   # 执行 **display port-mirroring** 命令查看观察接口的配置情况。

```
[Switch] display port-mirroring
  Vlan-mirror:
  ------------------------------------------------------------------------------
  Mirror-vlan              Direction     Observe-port
  ------------------------------------------------------------------------------
  10                       Inbound       GigabitEthernet0/0/3
  ------------------------------------------------------------------------------
```

配置文件

Switch 的配置文件。

```
#
sysname Switch
#
 vlan batch 1 10
#
 observe-port 1 interface GigabitEthernet0/0/3
#
vlan 10
 mirroring to observe-port 1 inbound
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10

#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#

#
return
```

配置基于 MAC 地址的本地镜像示例

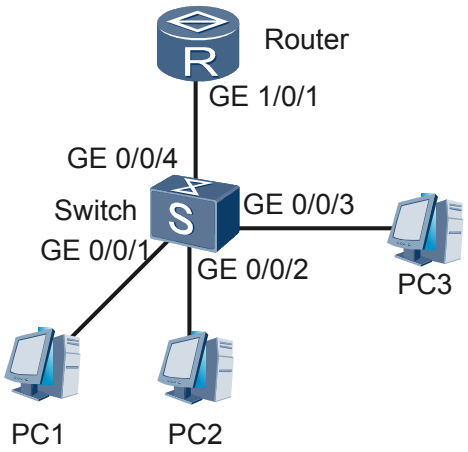
配置需求

如图 2-13 所示，GigabitEthernet0/0/1 接口连接 PC1,GigabitEthernet0/0/2 连接 PC2，GigabitEthernet0/0/4 连接路由器，其中 GigabitEthernet0/0/1、GigabitEthernet0/0/2 和 GigabitEthernet0/0/4 同属于 VLAN10。现在需要监控 VLAN10 中源或目的 MAC 地址是路由器 GigabitEthernet1/0/1 接口的 MAC 地址的所有入方向流量。此时，可以在 Switch 设备上配置基于 MAC 的本地镜像。

其中 GigabitEthernet0/0/3 接口作为观察接口。路由器 GigabitEthernet1/0/1 的 MAC 地址为 0001-0001-0001。

版权所有 © 华为技术有限公司

图 2-13 基于 MAC 地址的本地镜像组网图



配置思路

采用如下的思路配置基于 MAC 地址的本地镜像的基本功能：

1. 将 GigabitEthernet0/0/3 接口配置为观察接口。
2. 在 VLAN10 视图下配置基于 MAC 地址的本地镜像。

数据准备

无

配置步骤

1. 配置 VLAN10，并将接口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 和 GigabitEthernet0/0/4 加入 VLAN10（略）。
2. # 将 GigabitEthernet0/0/3 接口配置为观察接口。

```
<Switch> system-view
[Switch] observe-port 1 interface gigabitethernet 0/0/3
```

3. 配置镜像 MAC

   # 在 VLAN10 视图下配置基于 MAC 地址的本地镜像。

```
[Switch] vlan 10
[Switch-vlan10] mac-mirroring 0001-0001-0001 to observe-port 1 inbound
[Switch-vlan10] quit
```

4. 检查配置结果

   # 执行 **display port-mirroring** 命令查看观察接口的配置情况。

```
[Switch] display port-mirroring
  Mac-mirror:
  ------------------------------------------------------------------------
  Mirror-mac       Vlan    Direction     Observe-port
  ------------------------------------------------------------------------
  0001-0001-0001   10      Inbound       GigabitEthernet0/0/3
  ------------------------------------------------------------------------
```

配置文件

Switch 的配置文件。

版权所有 © 华为技术有限公司

```
#
sysname Switch
#
 vlan batch 1 10
#
 observe-port 1 interface GigabitEthernet0/0/3
#
vlan 10
 mac-mirroring 0001-0001-0001 to observe-port 1 inbound
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 1
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 10
#
return
```

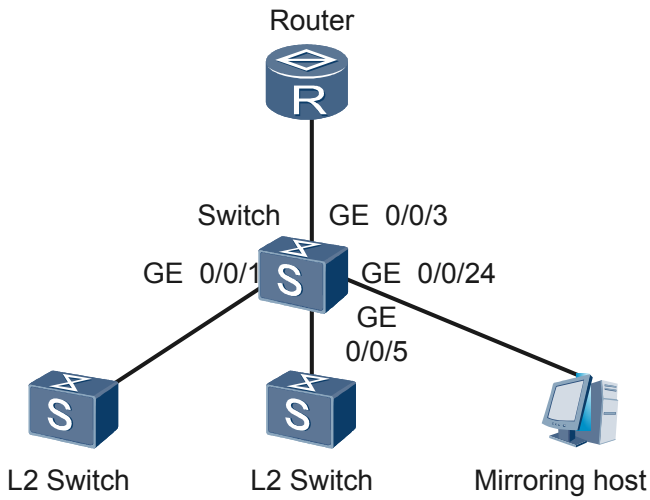
配置基于流的本地流镜像示例

配置需求

如图 2-14 所示，Switch 设备的 GigabitEthernet0/0/1 接口和 GigabitEthernet0/0/5 接口各与一台 L2 Switch 连接。现在需要监控 GigabitEthernet0/0/1 接口和 GigabitEthernet0/0/5 接口的入方向上符合某些相同属性的报文，报文的出接口为 GigabitEthernet0/0/3。在本例中，需要监控 802.1p 优先级为 6 的报文流。

将 GigabitEthernet0/0/24 接口作为观察接口。

图 2-14 流镜像的组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置基于流的本地流镜像的基本功能：

1. 将 GigabitEthernet0/0/24 接口配置为观察接口。
2. 创建流分类，并配置流分类规则是匹配 802.1p 优先级为 6 的报文。
3. 创建流行为，并在流行为中配置流镜像。
4. 创建流策略，绑定之前创建的流分类和流行为。
5. 在 GigabitEthernet0/0/1 接口和 GigabitEthernet0/0/5 接口上应用流策略。
6. 在 Switch 上创建 VLAN，将接口 GigabitEthernet0/0/1、GigabitEthernet0/0/3 和 GigabitEthernet0/0/5 以 Trunk 方式加入同一 VLAN。

数据准备

完成此配置举例，需要准备如下的数据：

- 流分类的名称是 c1。
- 流行为的名称是 b1。
- 流策略的名称是 p1。
- 在 Switch 上创建的 VLAN 编号为 10。

配置步骤

1. 在 Switch 上创建 VLAN，把相应接口以 Trunk 方式加入 VLAN

   # 将接口 GigabitEthernet0/0/1、GigabitEthernet0/0/3 和 GigabitEthernet0/0/5 以 Trunk 方式加入同一 VLAN。（以下配置以接口 GigabitEthernet0/0/1 为例，同理配置接口 GigabitEthernet0/0/3 和 GigabitEthernet0/0/5）

   ```
   <Switch> system-view
   [Switch] vlan 10
   [Switch-vlan10] quit
   [Switch] interface gigabitethernet 0/0/1
   [Switch-GigabitEthernet0/0/1] port link-type trunk
   [Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
   [Switch-GigabitEthernet0/0/1] quit
   ```

2. 配置观察接口

   # 将 GigabitEthernet0/0/24 接口配置为观察接口。

   ```
   [Switch] observe-port 1 interface gigabitethernet 0/0/24
   ```

3. 创建流分类

   # 创建流分类 c1，并配置流分类规则为匹配 802.1p 优先级为 6 的报文。

   ```
   [Switch] traffic classifier c1
   [Switch-classifier-c1] if-match 8021p 6
   [Switch-classifier-c1] quit
   ```

4. 创建流行为

   # 创建流行为 b1，并在流行为中配置流镜像。

   ```
   [Switch] traffic behavior b1
   [Switch-behavior-b1] mirroring to observe-port 1
   [Switch-behavior-b1] quit
   ```

5. 创建流策略

   # 创建流策略，绑定流分类 c1 和流行为 b1。

   ```
   [Switch] traffic policy p1
   [Switch-trafficpolicy-p1] classifier c1 behavior b1
   ```


版权所有 © 华为技术有限公司

```
[Switch-trafficpolicy-p1] quit
```

6. 应用流策略并使能信任报文携带的 802.1p 优先级

   # 在 GigabitEthernet0/0/1 接口和 GigabitEthernet0/0/5 接口上应用流策略 p1，并使能 **trust 8021p**。

```
[Switch]  interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] trust 8021p inner
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/5
[Switch-GigabitEthernet0/0/5] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/5] trust 8021p inner
[Switch-GigabitEthernet0/0/5] quit
```

7. 检查配置结果

   # 执行 **display port-mirroring** 命令查看观察接口。

```
[Switch] display port-mirroring
  Stream-mirror:
  ------------------------------------------------------------------------
  Behavior                Direction     Observe-port
  ------------------------------------------------------------------------
  b1                      -             GigabitEthernet0/0/24
  ------------------------------------------------------------------------
```

   # 执行 **display traffic policy interface** 命令查看 GigabitEthernet0/0/1 接口和 GigabitEthernet0/0/5 接口上应用的流策略。

```
[Switch] display traffic policy interface
  Interface: GigabitEthernet0/0/1
  Direction: Inbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
        if-match 8021p 6
     Behavior: b1
         Mirroring to observe-port 1
  Interface: GigabitEthernet0/0/5
  Direction: Inbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
        if-match 8021p 6
     Behavior: b1
         Mirroring to observe-port 1
```

配置文件

Switch 的配置文件。

```
#
sysname Switch
#
vlan batch 10
#
 observe-port 1 interface GigabitEthernet0/0/24
#
traffic classifier c1 operator and
 if-match 8021p 6
#
traffic behavior b1
 mirroring to observe-port 1
#
traffic policy p1
 classifier c1 behavior b1
#
```


版权所有 © 华为技术有限公司

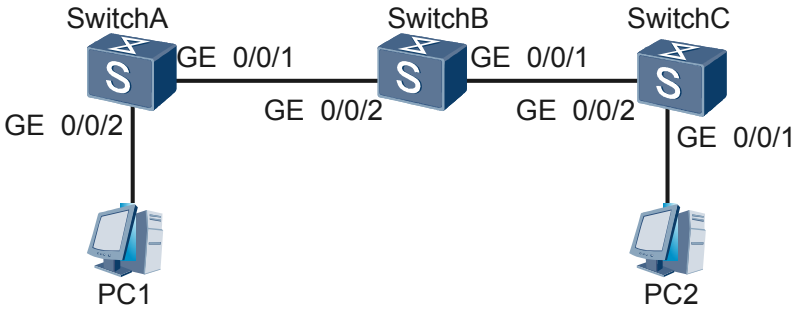
```
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 10
 traffic-policy p1 inbound
 trust 8021p inner
#
interface GigabitEthernet0/0/3
port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/5
port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
 trust 8021p inner
#
interface GigabitEthernet0/0/24
#
return
```

配置基于接口的远程镜像示例

配置需求

如图 2-15 所示，SwitchA 连接 PC1，SwitchC 连接 PC2，现在需要在 PC2 上监控 SwitchA 的 GigabitEthernet0/0/2 接口的入流量，可以在 SwitchA 上配置基于接口的远程镜像。

图 2-15 基于接口的远程镜像组网图



配置思路

采用如下的思路配置基于接口的远程镜像的基本功能：

1. 将 SwitchA 的 GigabitEthernet0/0/1 接口配置为观察接口，并指定 RSPAN VLAN。
2. 将 SwitchA 的 GE0/0/2 接口配置为镜像接口。
3. 将 SwitchC 的 GE0/0/1 接口配置为观察接口。

数据准备

配置基于接口的远程镜像时需要准备如下数据：

- SwitchA 上观察接口的索引编号为 1。
- SwitchA、SwitchB 和 SwitchC 上 RSPAN VLAN 的 VLAN 编号为 2。

版权所有 © 华为技术有限公司

- SwitchC 上观察接口的索引编号为 1。

配置步骤

1. 在 SwitchA 上完成如下配置：

   #配置 RSPAN VLAN。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

   # 配置 GE0/0/1 接口为观察接口，并指定 RSPAN VLAN 的编号为 2。

```
[SwitchA] observe-port 1 interface gigabitethernet 0/0/1 vlan 2
```

   # 配置将 GE0/0/1 以 Trunk 方式加入 RSPAN VLAN。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
```

   # 在 GE0/0/2 接口入方向上配置远程接口镜像。

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port-mirroring to observe-port 1 inbound
[SwitchA-GigabitEthernet0/0/2] quit
```

2. 在 SwitchB 上完成如下配置:

   # 创建 RSPAN VLAN。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] quit
```

   # 配置将 GE0/0/1 和 GE0/0/2 以 Trunk 方式加入 RSPAN VLAN。

```
[SwitchB] interface GigabitEthernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface GigabitEthernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet0/0/2] quit
```

3. 在 SwitchC 上完成如下配置:

   # 创建 RSPAN VLAN。

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

   # 配置将 GE0/0/2 以 Trunk 方式加入 RSPAN VLAN。

```
[SwitchC] interface GigabitEthernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet0/0/2] quit
```

   # 配置将 GE0/0/1 配置为 Hybrid 类型并允许远端镜像 VLAN 的报文通过。

```
[SwitchC] interface GigabitEthernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[SwitchC-GigabitEthernet0/0/1] quit
```

配置文件

SwitchA 的配置文件。

```
#
```


版权所有 © 华为技术有限公司

```
sysname SwitchA
#
vlan 2
#
 observe-port 1 interface GigabitEthernet0/0/1 vlan 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port-mirroring to observe-port 1 inbound
#

#
return
```

SwitchB 的配置文件。

```
#
sysname SwitchB
#
vlan 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#

#
return
```

SwitchC 的配置文件。

```
#
sysname SwitchC
#
vlan 2
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#

#
return
```

变更观察接口的示例

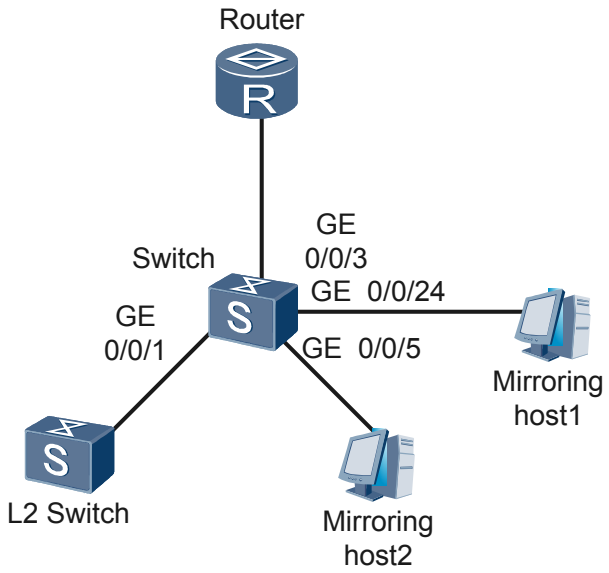
配置需求

如图 2-16 所示，Switch 设备 GigabitEthernet0/0/1 接口连接了一台 L2 Switch，GigabitEthernet0/0/24 连接主机 1，GigabitEthernet0/0/5 连接主机 2。为了监控 GigabitEthernet0/0/1 接口的入方向上的流量，在 Switch 设备上配置了接口镜像，将 GigabitEthernet0/0/1 接口作为镜像接口，将连接主机 1 的 GigabitEthernet0/0/24 接口作为观察接口，由主机 1 来收集 GigabitEthernet0/0/1 接口入方向上的流量。

目前需要由主机 2 来收集 GigabitEthernet0/0/1 接口入方向上的流量，因此需要将观察接口由 GigabitEthernet0/0/24 变更为 GigabitEthernet0/0/5。

版权所有 © 华为技术有限公司

图 2-16 变更观察接口的组网图



配置思路

采用如下的思路变更观察接口：

1. 删除镜像接口 GigabitEthernet0/0/1。
2. 变更观察接口 GigabitEthernet0/0/24 为 GigabitEthernet0/0/5。
3. 将 GigabitEtherner0/0/1 接口重新配置为镜像接口。

数据准备

完成此配置举例，需要准备如下的数据：

- 新观察接口的类型和编号为 GigabitEthernet0/0/5。

配置步骤

1. 显示当前观察接口和镜像接口的配置情况。

   # 执行 **display port-mirroring** 命令查看当前的观察接口和镜像接口的配置情况。

```
<Switch> display port-mirroring
Port-mirror:
  ------------------------------------------------------------------------
  Mirror-port              Direction     Observe-port
  ------------------------------------------------------------------------
  GigabitEthernet0/0/1           Inbound       GigabitEthernet0/0/24
  ------------------------------------------------------------------------
```

2. 删除镜像接口

   # 删除镜像接口 GigabitEthernet0/0/1。

```
<Switch> system-view
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] undo port-mirroring inbound
[Switch-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

3. 将观察接口变更为 GigabitEthernet0/0/5

   # 变更观察接口为 GigabitEthernet0/0/5。

   ```
   [Switch] observe-port 1 interface gigabitethernet 0/0/5
   ```

4. 配置镜像接口

   # 将 GigabitEthernet0/0/1 接口重新配置为镜像接口。

   ```
   [Switch] interface gigabitethernet 0/0/1
   [Switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
   [Switch-GigabitEthernet0/0/1] quit
   ```

5. 检查配置结果

   # 执行 **display port-mirroring** 命令查看变更后的观察接口和镜像接口的配置情况。

   ```
   [Switch] display port-mirroring
   Port-mirror:
     ------------------------------------------------------------------------
     Mirror-port              Direction     Observe-port
     ------------------------------------------------------------------------
     GigabitEthernet0/0/1            Inbound       GigabitEthernet0/0/5
     ------------------------------------------------------------------------
   ```

配置文件

Switch 的配置文件。

```
#
 sysname Switch
#
 observe-port 1 interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/1
 port-mirroring to observe-port 1 inbound
#
return
```

2.7 PoE 配置

介绍 PoE 的基本概念和配置方法。

2.7.1 PoE 供电简介

介绍远程 PoE 供电的基本原理和概念。

PoE 全称为 Power over Ethernet，是指通过 10BASE-T、100BASE-TX、1000BASE-T 以太网网络进行供电。通过这种方式，终端设备在接入网络的同时就可以实现受电，可以有效的解决 IP 电话、无线 AP(Access Point)、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电，不再需要考虑这些设备的室内电源系统布线的问题。在兼容性方面，PoE 供电的统一标准是 IEEE 802.3at 和 802.3af 标准，可以解决不同厂家设备之间的适配性的问题。

2.7.2 AC6605 支持的 PoE 特性

介绍 AC6605 支持的 PoE 功能。

Switch PoE 交换机的下行电口支持 PoE 供电。每端口最大供电功率为 30W，最大供电距离 100m。PoE 交换机使用信号线耦合供电方式，即在同一对线上同时传输电流和数据。

版权所有 © 华为技术有限公司

PoE 电源分为两种：500W 均流电源和 250W 均流电源。其中 500W 电源只有 369.6W 可用于 PoE 供电，250W 电源只有 123.2W 可用于 PoE 供电。

目前 AC6605 系列产品中支持 PoE 功能的设备包括：

- AC6605

  PoE 交换机支持 2 个电源槽位，每个电源槽位支持 500W 功率电源或 250W 功率电源供电。这两种电源的搭配关系如下表所示：

电源搭配		PoE 实际可用功率
250W 均流	-	123.2W
500W 均流	-	369.6W
250W 均流	250W 均流	246.4W
250W 均流	500W 均流	492.8W
500W 均流	500W 均流	739.2W

2.7.3 配置 PoE

介绍全局和接口视图下配置 PoE 相关功能的方法。

建立配置任务

在配置 PoE 前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 可以自动检测连接的设备是否需要远程供电，并对需要远程供电的设备进行供电。

根据实际组网需要，用户可以：

- 通过命令行设置交换机整机对外提供的 PoE 最大功率、预留功率。
- 可以通过命令行分别控制不同 PoE 端口远程供电特性（使能/关闭端口的远程供电特性、设置端口的最大供电功率、设置端口供电方式、设置端口供电优先级）。

前置任务

确认 AC6605 上有 PoE 电源。

配置全局 PoE

用户可以在系统视图下配置 AC6605 的最大供电能力、配置供电的管理方式、配置 PoE 电源预留功率占 PoE 电源总功率的比例以及给某个接口上的 PD 上下电。

操作步骤

- **可选:** 配置设备的最大供电能力。

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **poe max-power** *maximum-power* [**slot** *slot-id*]，配置设备的最大对外输出功率。

   取值范围为 15400 ～ 739200mW。

- **可选:** 配置供电的管理方式。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **poe power-management** { **auto** | **manual** } [**slot** *slot-id*]，配置交换机供电的管理方式。
- **可选:** 手动给某个接口上的外部设备 PD 上下电。

  说明

  当设备的供电管理方式为 **manual** 时，需要手动给某个接口上的外部设备 PD 上下电。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **poe power-on interface** *interface-type interface-number* 或命令 **poe power-off interface** *interface-type interface-number*，手动给某个接口上的 PD 设备上下电。
- **可选:** 使能允许上电瞬间的高冲击电流。

  不规范的 PD 上电瞬间会产生高冲击电流，导致 PSE 侧自我保护从而将 PD 断电。在这种情况下，若一定要给此 PD 供电，需要允许上电瞬间的高冲击电流。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **poe high-inrush enable** 使能允许 PD 上电瞬间的高冲击电流。

     缺省情况下，未使能允许上电瞬间的高冲击电流。
- **可选:** 配置 PoE 电源预留功率占 PoE 电源总功率的比例。

  AC6605 会根据每个接口实际消耗的功率动态地给每个接口分配功率，每个 PD 设备在运行过程中，其功率消耗会不断变化，系统会定期计算当前接入的所有的 PD 所需总功率是否超过分配的功率上限，如果超过，系统会自动给优先级比较低的接口上的 PD 设备断电，保证其他 PD 设备的正常运行。

  但是有时候会出现突发性的功率消耗激增，系统剩余可用功率无法支撑这种需求激增，而软件系统还未来得及计算出消耗总功率超限，作断开优先级较低的接口供电的处理时，PoE 电源会因为过载而导致过载保护断电，所有的 PD 设备下电。

  如果合理设置系统预留功率，在发生突发功率需求激增的情况下，系统预留功率可以支撑突发需求，保证软件系统有时间通过给优先级低的接口上的设备下电的方法保证其他设备的稳定运行。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **poe power-reserved** *reserved-power-percent* [**slot** *slot-id*]，配置 PoE 电源管理模式，配置 PoE 电源预留功率占 PoE 电源总功率的比例。

     缺省情况下，预留功率比例为 20%。
- **可选:** 配置 PoE 电源的告警阈值功率百分比。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **poe power-threshold** *thresholdvalue* [**slot** *slot-id*] 配置 PoE 电源的告警阈值功率百分比。

版权所有 © 华为技术有限公司

缺省情况下，告警阈值功率百分比为 90%，即当消耗的功率为电源总功率的 90%时，产生告警。

----结束

配置接口 PoE 功能

用户可以在接口视图下使能接口的 PoE 功能、配置设备接口的最大对外输出功率、PoE 接口供电的优先级和 PoE 接口的下电时间段。

操作步骤

- 接口下使能 PoE 功能。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number* 进入接口视图。
  3. 执行命令 **poe enable** 使能 PoE 功能。

     缺省情况下，接口使能 PoE 供电功能。
- **可选:** 设置设备接口的最大对外输出功率。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number* 进入接口视图。
  3. 执行命令 **poe power** *maximum-power* 设置接口的最大对外输出功率。

     缺省情况下，接口对外提供的最大功率为 30000 毫瓦。
- **可选:** 配置 PoE 接口供电的优先级。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **poe priority** { **critical** | **high** | **low** }，配置该接口的供电的优先级。

     优先级从高到低依次为：**critical**、**high**、**low**。

     默认接口的供电优先级是 Low。
- **可选:** 配置 PoE 接口的下电时间段。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **time-range** *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }，配置 PoE 的下电时间段。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  4. 执行命令 **poe power-off time-range** *time-range-name*，在接口下生效已配置的 PoE 下电时间段规则。
- **可选:** 配置 PSE 设备接口对 PD 设备接口的兼容性检测功能。

  说明

  在使能对 PD 设备接口的兼容性检测前，必须先使能设备接口的 PoE 功能。使能 PD 设备的兼容性检测功能，可以使交换机检测到不符合 802.3af 或 802.3at 标准的 PD 设备。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **poe legacy enable** 使能设备接口对非标准 PD 设备的兼容性检测功能。

     缺省情况下，接口对 PD 设备接口的兼容性检测功能为关闭状态。

版权所有 © 华为技术有限公司

- **可选:** 配置接口强制供电功能。

  在系统功率充足的情况下，连接 PD 后，如果 PSE 无法检测到 PD，可以使能接口强制供电功能强制给 PD 供电。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **poe force-power** 使能接口强制供电功能。

     缺省情况下，接口未使能 PoE 强制供电功能。

----结束

检查配置结果

在完成 PoE 配置后，可以查看 PoE 电源的状态和设备信息以及接口下的 PoE 配置。

前提条件

PoE 设备已经安装，已经完成了 PoE 的相关配置。

操作步骤

步骤 1 执行命令 **display poe-power**，查看 PoE 电源的状态。

步骤 2 执行命令 **display poe device**，查看所有支持 PoE 功能的设备信息。

步骤 3 执行命令 **display poe information**，查看设备的 PoE 信息。

步骤 4 执行命令 **display poe power interface** *interface-type interface-number*，查看指定接口的输出功率。

步骤 5 执行命令 **display poe power-state interface** *interface-type interface-number*，查看指定接口的 PoE 供电状态。

----结束

2.7.4 配置举例

介绍 Switch 上配置 PoE 功能的举例。

配置 Switch PoE 功能示例

配置需求

如图 2-17 所示，Switch 支持 PoE 功能。SwitchA、SwitchB 和 AP(Access Point)支持 PoE 受电。

说明

SwitchA、SwitchB 和 AP 为其他厂商的设备，要求其支持 PoE 受电。

其中：

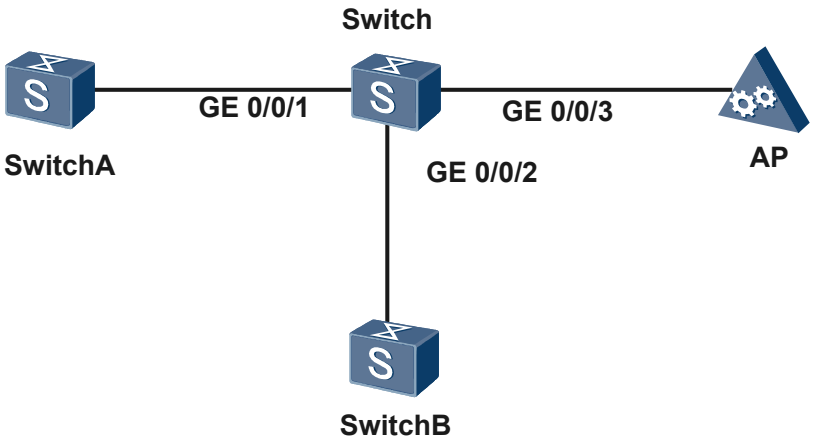
- SwitchA 与 Switch 的 GigabitEthernet0/0/1 接口连接，SwitchA 的最大功耗为 12000mW，SwitchA 连接公司数据服务器，需要优先保证其供电。

版权所有 © 华为技术有限公司

- SwitchB 与 Switch 的 GigabitEthernet0/0/2 接口连接，SwitchB 的最大功耗为 20000mW，SwitchB 连接普通上网用户。
- AP 与 Switch 的 GigabitEthernet0/0/3 接口连接，AP 的最大功耗为 2500mW，AP 连接无线上网用户。

Switch 采用自动供电管理方式给 SwitchA、SwitchB 和 AP 供电。

图 2-17 PoE 组网图



配置思路

采用如下的思路配置：

1. 使能 Switch 和 SwitchA 连接接口的 PoE 功能，配置其对外供电的最大功率和供电优先级。
2. 使能 Switch 和 SwitchB 连接接口的 PoE 功能并配置其对外供电的最大功率。
3. 使能 Switch 和 AP 连接接口的 PoE 功能并配置其对外供电的最大功率。
4. 配置 Switch 的供电管理方式为自动方式。

数据准备

配置时需要准备如下数据：

- 需要使能 PoE 功能的接口的编号。
- 接口对外供电的最大功耗。

配置步骤

1. #在 Switch 上使能 GigabitEthernet0/0/1 接口 PoE 功能，配置 GigabitEthernet0/0/1 接口对外供电的最大功率和供电优先级。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] poe enable
[Switch-GigabitEthernet0/0/1] poe power 12000
[Switch-GigabitEthernet0/0/1] poe priority critical
[Switch-GigabitEthernet0/0/1] quit
```

2. #在 Switch 上使能 GigabitEthernet0/0/2 接口 PoE 功能，配置 GigabitEthernet0/0/2 接口对外供电的最大功耗为 20000mW。

版权所有 © 华为技术有限公司

```
<Switch> system-view
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] poe enable
[Switch-GigabitEthernet0/0/2] poe power 20000
[Switch-GigabitEthernet0/0/2] quit
```

3. # 在 Switch 上使能 GigabitEthernet0/0/3 接口 PoE 功能，配置 GigabitEthernet0/0/3 接口对外供电的最大功耗为 2500mW。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] poe enable
[Switch-GigabitEthernet0/0/3] poe power 2500
[Switch-GigabitEthernet0/0/3] quit
```

4. # 配置 Switch 的供电管理方式为自动方式。

```
[Switch] poe power-management auto
```

配置文件

```
#
 sysname Switch

#
interface GigabitEthernet0/0/1
 poe power 12000
 poe priority critical
#
interface GigabitEthernet0/0/2
 poe power 20000
#
interface GigabitEthernet0/0/3
 poe power 2500
#
return
```

2.8 ALS 配置

介绍 ALS（Automatic Laser Shutdown）功能在 AC6605 的配置方法。

2.8.1 ALS 简介

ALS 功能通过检测光口的 LOS（Loss of Signal）信号来控制光模块激光器的发光。

未使能 ALS 功能时，当光纤链路发生故障，虽然数据通讯中断，但是交换机的光接口没有被关闭，光模块激光器的发光功能是打开的。光模块激光器在数据通讯中断时的持续发光不仅造成能源的浪费，激光射入人眼也会造成一定危害。

使能 ALS 功能后，当光纤链路故障时，软件检测到光口的 LOS 信号后，自动关闭光模块激光器；当光纤链路恢复后，软件检测到光口的 LOS 信号被清除，自动打开光模块激光器。ALS 功能为用户提供安全保护的同时，也能为用户节能。

2.8.2 AC6605 支持的 ALS 特性

介绍 AC6605 支持的 ALS 功能。

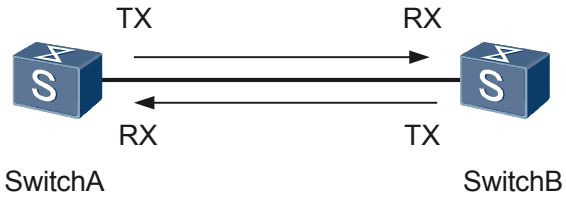
ALS 应用环境

- 交换机和交换机之间通过光纤互联

版权所有 © 华为技术有限公司

在交换机和交换机之间通过光纤互相连接时，通过启动交换机接口的 ALS 功能，可以对交换机用户起到安全防护作用，避免用户受到激光的伤害，连接如图 2-18 所示。

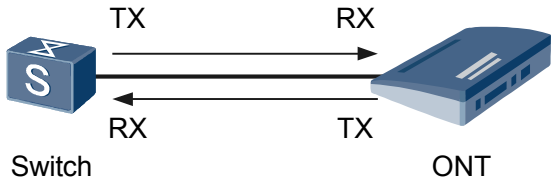
图 2-18 交换机之间通过光纤互联组网图



- 交换机和光网络终端 ONT（Optical Network Terminal）之间通过光纤互联

  在光纤到户的应用中，通过启动交换机接口的 ALS 功能，可以对光网络终端用户起到安全防护作用，避免用户因为对激光危害不够了解，或者孩童玩耍光纤，造成激光对人眼的伤害，连接如图 2-19 所示。

图 2-19 交换机与光网络终端通过光纤互联组网图



ALS 功能对链路数据通讯恢复的影响

未使能 ALS 功能时，交换机的光模块激光器始终为打开，光纤链路恢复后接口 LOS 信号被清除，接口状态快速变为“up”。使能 ALS 功能后，通过检查接口的 LOS 信号来控制激光器的发光，会延缓链路数据通讯的恢复。

- 光纤链路两端均使能 ALS 功能

  如图 2-18 所示，两台交换机通过光纤连接。接口 ALS 功能均为使能状态，且重启模式为自动。光纤链路恢复后，SwitchA 和 SwitchB 接口状态由“down”变为“up”的过程如下：

  1. SwitchA 周期性的发送光脉冲。
  2. SwitchB 在光纤链路恢复后，收到 SwitchA 发送的光脉冲。
  3. SwitchB 接口的 LOS 信号被清除，接口状态为“up”并开始发送信号。
  4. SwitchA 收到 SwitchB 发送的信号。
  5. SwitchA 接口的 LOS 信号被清除，接口状态为“up”，数据通讯恢复。

- 光纤链路仅有一端使能 ALS 功能

  如图 2-18 所示，两台交换机通过光纤连接。SwitchA 接口未使能 ALS 功能，SwitchB 接口使能 ALS 功能，且重启模式为自动。光纤链路恢复后，SwitchA 和 SwitchB 接口状态由“down”变为“up”的过程如下：

  1. SwitchA 的光模块激光器始终保持发光状态。
  2. SwitchB 在光纤链路恢复后，立即收到 SwitchA 发送的光信号。
  3. SwitchB 接口的 LOS 信号被清除，接口状态为“up”并开始发送信号。

版权所有 © 华为技术有限公司

4. SwitchA 收到 SwitchB 发送的信号。
5. SwitchA 接口的 LOS 信号被清除，接口状态为“up”，数据通讯恢复。

接口使能 ALS 功能后，接口恢复通讯的速度会受到影响，在有流量的情况下会导致接口丢包。

2.8.3 配置 ALS

在接口视图下配置光模块激光器的 ALS 功能可以为用户提供安全保护，并实现能源的节约。

建立配置任务

在进行 ALS 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 可以通过检测光口的 LOS 信号来控制光口光模块激光器是否发光，从而为用户提供安全保护，并实现能源的节约。

根据实际组网需要，在使能 ALS 功能后，用户可以：

- 通过命令行设置光模块激光器的重启模式。
- 通过命令行设置光模块激光器的发光间隔和发光时间。
- 通过命令行查看不同光模块接口的 ALS 配置。

前置任务

在配置 ALS 功能之前，需完成以下任务：

确认 AC6605 上有光模块。

数据准备

在配置 ALS 之前，需准备以下数据。

序号	数据
1	激光器的发光间隔 激光器的发光时间

使能接口的 ALS 功能

使能接口的 ALS 功能后，ALS 相关配置才能生效。

背景信息

ALS 功能的约束条件：

版权所有 © 华为技术有限公司

- 只有光口支持 ALS 功能，电口不支持 ALS 功能。
  - 光口在单方向通讯应用时，不支持 ALS 功能。
  - 硬件需要支持软件对光口的 LOS 信号检测和对接口激光器的发光控制。
- 端口聚合组不支持 ALS 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **als enable**，使能接口的 ALS 功能。

缺省情况下，所有接口未使能 ALS 功能。

----结束

（可选）配置激光器的重启模式

激光器重启模式分为自动重启和手动重启模式，缺省情况下为自动重启模式。

前提条件

接口使能 ALS 功能。

背景信息

光模块激光器为自动重启模式时，将以配置的发光间隔定期自动打开激光器；配置为手动重启模式后，必须由用户手动打开激光器，激光器发送一个光脉冲。

用户在能及时知道光纤链路恢复的情况下，使用手动重启模式可使激光器立即发光，实现数据通讯的快速恢复。

缺省情况下，所有接口使能 ALS 功能后，激光器的重启模式为自动重启。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。

步骤 3 执行命令 **als restart mode manual**，配置接口激光器的重启模式为手动重启。

手动重启模式下发光时间与之前自动重启模式下的发光时间一致。

----结束

（可选）手动打开激光器

当激光器重启模式为手动重启模式时，需要手动打开光模块的激光器，使得激光器发送一个光脉冲。

前提条件

接口使能 ALS 功能，且重启模式为手动重启。

版权所有 © 华为技术有限公司

背景信息

当接口检测到 LOS 信号，光模块激光器停止发光，若不执行 **als restart** 命令，激光器不会再次打开。若手动打开激光器，仍然检测到 LOS 信号，则激光器再次关闭；若检测到 LOS 信号被清除，则打开光口激光器发光，恢复数据通讯。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **als restart**，手动打开光模块的激光器，激光器发送一个光脉冲。

----结束

（可选）配置激光器的发光间隔与发光时间

合理配置激光器的发光间隔与发光时间，做到节能减排与及时探测到光纤链路恢复的平衡。

前提条件

接口使能 ALS 功能，且重启模式为自动重启。

背景信息

发光时间为激光器持续发光的时间长度，间隔时间为激光器前次发光结束到下次发光开始的时间长度。发光时间越小，发光间隔越大，越有利于节能减排，但不利于及时探测到光纤链路的恢复。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **als restart pulse-interval** *pulse-interval*，配置指定接口激光器的发光间隔。

缺省配置时，发光间隔的缺省值为 100s。

步骤 4 执行命令 **als restart pulse-width** *pulse-width*，配置指定接口激光器的发光时间。

缺省配置时，发光时间的缺省值为 2s。

----结束

检查配置结果

完成 ALS 配置后，可以查看指定接口或指定槽位的 ALS 配置信息，包括是否使能 ALS、激光器是否处于发光状态、ALS 重启模式、激光器发光间隔和发光时间。

前提条件

AC6605 已经完成了 ALS 的相关配置。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **display als configuration slot** *slot-id*，查看指定成员交换机的 ALS 配置信息。
- 执行命令 **display als configuration interface** *interface-type interface-number*，查看指定接口 ALS 的配置信息。

----结束

2.8.4 配置举例

举例说明 ALS 的配置。

配置 ALS 示例

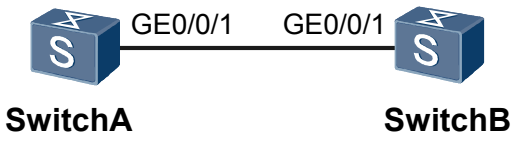
通过配置 ALS 功能，激光器能在链路故障时自动终止发光，在链路恢复后恢复发光。

组网需求

如图 2-20 所示，SwitchA 的 GigabitEthernet0/0/1 与 SwitchB 的 GigabitEthernet0/0/1 之间通过光纤互连。

当光纤链路发生故障导致数据传输中断时，光模块激光器的持续发光会造成能源的浪费和潜在的危险性。在光纤链路的两端接口使能 ALS 功能后，激光器能在链路故障时自动终止发光，在链路恢复后恢复发光。

图 2-20 ALS 应用组网图



配置思路

采用如下的思路配置基本 ALS 功能：

1. 使能 SwitchA 与 SwitchB 的 GigabitEthernet0/0/1 接口 ALS 功能。
2. 配置 SwitchA 与 SwitchB 的 GigabitEthernet0/0/1 接口激光器的重启模式为自动重启。
3. 配置 SwitchA 与 SwitchB 的 GigabitEthernet0/0/1 接口激光器的发光间隔和发光时间。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 的 GigabitEthernet0/0/1 接口的光模块激光器发光间隔和发光时间。
- SwitchB 的 GigabitEthernet0/0/1 接口的光模块激光器发光间隔和发光时间。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 SwitchA 上使能 GigabitEthernet0/0/1 接口的 ALS 功能，配置该接口激光器重启模式为自动重启，发光间隔为 200s，发光时间为 3s。

使能 ALS 功能

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] als enable
```

配置激光器的发光间隔和发光时间

```
[SwitchA-GigabitEthernet0/0/1] undo als restart mode manual
[SwitchA-GigabitEthernet0/0/1] als restart pulse-interval 200
[SwitchA-GigabitEthernet0/0/1] als restart pulse-width 3
```

步骤 2 在 SwitchB 上使能 GigabitEthernet0/0/1 接口的 ALS 功能，配置该接口激光器重启模式为自动重启，发光间隔为 200s，发光时间为 3s。

使能 ALS 功能

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] als enable
```

配置激光器的发光间隔和发光时间

```
[SwitchB-GigabitEthernet0/0/1] undo als restart mode manual
[SwitchB-GigabitEthernet0/0/1] als restart pulse-interval 200
[SwitchB-GigabitEthernet0/0/1] als restart pulse-width 3
```

步骤 3 验证配置结果。

#在 SwitchA 和 SwitchB 上执行 **display als configuration interface** *interface-type interface-number* 命令，查看 ALS 的配置情况。

```
<SwitchA> display als configuration interface gigabitethernet0/0/1

-------------------------------------------------------------------------------
Interface              ALS       Laser     Restart    Interval(s)   Width(s)
                       Status    Status    Mode
-------------------------------------------------------------------------------
GigabitEthernet0/0/1   Enable    Off       Auto       200           3
-------------------------------------------------------------------------------
<SwitchB> display als configuration interface gigabitethernet0/0/1

-------------------------------------------------------------------------------
Interface              ALS       Laser     Restart    Interval(s)   Width(s)
                       Status    Status    Mode
-------------------------------------------------------------------------------
GigabitEthernet0/0/1   Enable    Off       Auto       200           3
-------------------------------------------------------------------------------
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
interface GigabitEthernet0/0/1
 als enable
 als restart pulse-interval 200
 als restart pulse-width 3
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
interface GigabitEthernet0/0/1
 als enable
 als restart pulse-interval 200
 als restart pulse-width 3
#
return
```

2.9 重新启动和复位

介绍了 BootROM 软件和 VRP 系统软件的基础知识，以及重新启动 AC6605 设备的方法。

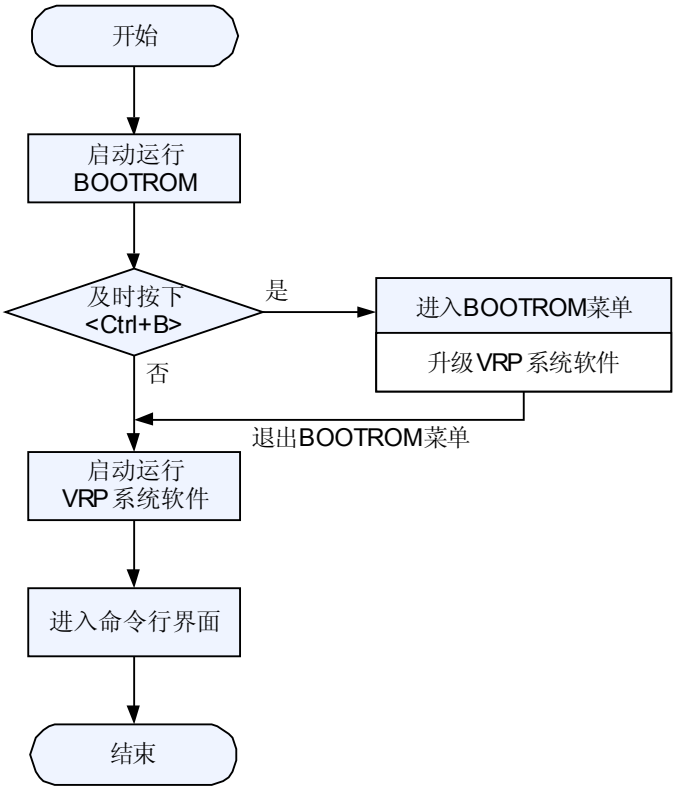
2.9.1 简介

介绍重新启动及复位 AC6605 设备时所需要了解的知识。

AC6605 设备的启动过程

AC6605 设备的软件包括 BOOTROM 软件和 VRP 系统软件。AC6605 设备上电后，各软件的启动运行顺序如图 2-21 所示。

图 2-21 AC6605 设备的启动过程



版权所有 © 华为技术有限公司

BOOTROM 主系统软件负责引导运行 VRP 系统软件。

BOOTROM 软件的启动过程

说明

在终端上观察 BOOTROM 软件的启动过程前，需要先用串口线将设备的 Console 口与终端直接相连。

BOOTROM 主系统比较当前配置和配置文件的一致性并提示是否进行 reboot 操作。显示信息如下：

```
Info: The system is now comparing the configuration, please wait.
System will reboot! Continue?[Y/N]:y

BIOS LOADING ...
Copyright (c) 2008-2010 HUAWEI TECH CO., LTD.
CX22EFFE (Ver124, Jun  9 2010, 17:41:46)

Press Ctrl+B to enter BOOTROM menu ... 0
```

如果用户在 2 秒钟内按下<Ctrl+B>快捷键，则 AC6605 设备提示用户输入 BOOTROM 主系统菜单的密码（缺省密码是 huawei），屏幕显示如下信息。

```
password:
          BOOTROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Modify BOOTROM password
    7. Reboot
Enter your choice(1-7):
```

通过 BOOTROM 主系统菜单，用户可以升级 VRP 系统软件，或指定 AC6605 设备启动时加载的 VRP 系统软件。

BOOTROM 系统软件初始化串口和 Console 控制台，解压缩逻辑芯片的逻辑程序和 VRP 系统软件，并引导运行 VRP 系统软件。AC6605 的屏幕显示以下信息。

```
Decompressing Image file ... done

PPI DEV SysInit......OK
Hard system init.................OK
Begin to start the system, please waiting ......

VOS VFS init.....................OK
VOS monitor init.................OK
CFM init advance.................OK
PAT init ........................OK
VOS VFS init hind ...............OK

VRP_Root begin...
VRP_InitializeTask begin...
Init the Device Link.............OK
CFG_PlaneInit begin..............OK
CFM_Init begin...................OK
CLI_CmdInit begin................OK
VRP_RegestAllLINKCmd begin.......OK
create task begin................
task init begin...

Recover configuration...OK!done
```


版权所有 © 华为技术有限公司

```
Press ENTER to get started.
```

当屏幕显示以上信息时，表明 VRP 系统软件的启动过程完成，此时用户可以按下回车键进入命令行接口。

2.9.2 立即重新启动 AC6605 设备

介绍立即重新启动 AC6605 设备的方法。

通过命令行

背景信息

注意

一般情况下，不要轻易使用 **reboot** 命令，因为它将导致网络工作在短时间内瘫痪。

在需要重启 AC6605 设备时，请确认是否需要保存配置文件，同时确保重新启动时的文件信息正确。有关保存配置文件的操作，请参见《AC6605 无线接入控制器 配置指南 基础配置》。

操作步骤

步骤 1 执行命令 **reboot**，立刻重新启动 AC6605 设备。

----结束

通过 AC6605 设备上的按键

背景信息

注意

一般情况下，不要轻易执行此操作，因为它将导致网络工作在短时间内瘫痪。

在需要重启 AC6605 设备时，请确认是否需要保存配置文件，同时确保重新启动时的文件信息正确。有关保存配置文件的操作，请参见《AC6605 无线接入控制器 配置指南-基础配置》。

操作步骤

步骤 1 按动 AC6605 设备上的电源按钮，关闭当前处于运行状态的 AC6605 设备。

步骤 2 再次按动电源按钮，立刻重新启动 AC6605 设备。

----结束

版权所有 © 华为技术有限公司

2.9.3 定时重新启动 AC6605 设备

介绍定时重新启动 AC6605 设备的方法。

操作步骤

步骤 1 执行命令 **schedule reboot** { **at** *time* | **delay** *interval* [**force**] }，使能定时重启功能。

缺省情况下，未配置重新启动 AC6605 设备的时间，即不支持定时重启功能。

----结束

版权所有 © 华为技术有限公司

3 以太网配置

关于本章

本文档针对 AC6605 的以太网业务，主要包括以太网接口配置、链路聚合配置、VLAN 配置、VLAN Mapping 配置、QinQ 配置、GVRP 配置、MAC 表配置、STP/RSTP、MSTP 配置、SEP 配置、二层协议透明传输配置、Loopback Detection 配置。

本文档从配置过程和配置举例两大方面介绍了此业务的配置方法和应用场景。

3.1 以太网接口配置
介绍以太网接口的基本知识、配置方法和配置实例。

3.2 链路聚合配置
介绍链路聚合的基本知识、配置方法和配置实例。

3.3 VLAN 配置
VLAN（Virtual Local Area Network）具有隔离广播域、增强保密性、组网灵活和良好的扩展性等特点。

3.4 VLAN Mapping 配置
介绍了 VLAN Mapping 配置的基本知识、配置方法，配置实例。

3.5 QinQ 配置
介绍 QinQ 的基本知识、配置方法和配置实例。

3.6 GVRP 配置
介绍了 GVRP 的基本知识、GVRP 配置方法和配置实例。

3.7 MAC 表配置
介绍了 MAC 表的基本知识、配置方法和配置实例。

3.8 STP/RSTP 配置
STP（Spanning Tree Protocol，生成树协议）将环形网络修剪成为一个无环的树型网络，避免报文在环形网络中的增生和无限循环；RSTP（Rapid Spanning Tree Protocol，快速生成树协议）在 STP 基础上实现了快速收敛，并增加了边缘端口的概念及保护功能。

3.9 MSTP 配置
MSTP（Multiple Spanning Tree Protocol，多生成树协议）将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

华为专有和保密信息
版权所有 © 华为技术有限公司

3.10 SEP 配置

SEP（Smart GigabitEthernet Protection）作为以太网保护协议，通过选择性地阻塞网络中冗余链路，阻止网络形成逻辑环路，达到消除环路的目的。

3.11 二层协议透明传输配置

介绍了二层协议透明传输的基本知识、配置方法和配置实例。

3.12 Loopback Detection 配置

介绍 Loopback Detection 的基本知识、配置方法和配置实例。

版权所有 © 华为技术有限公司

3.1 以太网接口配置

介绍以太网接口的基本知识、配置方法和配置实例。

3.1.1 以太网接口概述

简要介绍以太网接口。

以太网以其高度灵活、相对简单、易于实现的特点，成为重要的局域网组网技术。

以太网接口分为：以太网电接口和以太网光接口。

以太网电接口和以太网光接口的属性如表 3-1 所示。

表 3-1 以太网接口属性

接口类型	速率（Mbit/s）	自协商模式		非自协商模式	
		全双工	半双工	全双工	半双工
以太网电接口	10	√	√	√	√
	100	√	√	√	√
	1000	√	×	√	×
以太网光接口	100	×	×	√	×
	1000	√	×	√	×

如果本端接口配置为自协商模式，那么对端接口也一定要配置为自协商模式，否则可能会产生丢包现象。

3.1.2 AC6605 支持的以太网接口特性

介绍以太网接口特性在 AC6605 中的支持情况。

端口组功能

AC6605 支持的端口组功能主要是为了方便用户同时对端口组中的多个端口进行配置。在端口组视图下，用户只需输入一次配置命令，则该端口组内的所有端口都会配置该功能，以减少重复配置工作。

自协商功能

自协商的主要功能就是使物理链路两端的端口通过协商能力信息交互来自动选择同样的工作参数。自协商端口发送本端的协商能力信息并检测对端的信息。一旦本端收到对端的协商能力信息，并且得知对端也收到本端发送的协商信息，就比较两端的能力来建立起双方具有的最高性能的工作模式。

自动协商的内容主要包括双工模式、运行速率以及流控参数。一旦协商通过，链路两端的端口就以同样的双工模式、运行速率和流控参数来工作。

版权所有 © 华为技术有限公司

端口隔离功能

端口隔离功能是指使能了端口隔离功能的端口之间相互隔离，可以隔离同一 VLAN 内不同端口之间的二三层报文。通过配置端口隔离功能，可以灵活地限制端口间的报文互通，为用户提供了更安全、更灵活的组网方案。

3.1.3 配置以太网接口的基本属性

介绍配置以太网接口的描述信息、网线类型、双工模式、速率、自协商、光接口与电接口切换的过程与步骤。

建立配置任务

应用环境

在以下情况，需执行本配置任务：

- 为了便于识别、维护接口，配置接口的描述信息。
- 缺省情况下，快速以太网电接口自动识别它所连接的网线的类型。当自动识别发生错误时，可手动配置快速以太网电接口的网线类型。
- 缺省情况下，快速以太网电接口和它直接连接的接口自协商确定双方共同的双工模式和速率。如果对端接口不具备自协商功能，可手动配置快速以太网电接口的双工模式和速率，以和对端接口匹配。

前置任务

无

数据准备

在配置以太网接口的基本属性之前，需要准备以下数据。

序号	数据
1	以太网接口的编号
2	（可选）接口的描述信息
3	（可选）以太网电接口的网线类型
4	（可选）以太网电接口的双工状态
5	（可选）以太网接口的速率

（可选）配置描述信息

背景信息

请在需要配置以太网接口描述信息的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **description** *description*，配置接口的描述信息。

缺省情况下，接口的描述信息是“HUAWEI, Quidway Series, X Interface”，X 由实际的接口类型和接口编号代替。

----结束

（可选）配置网线类型

背景信息

请在需要配置以太网接口网线类型的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太网电接口视图。

步骤 3 执行命令 **mdi** { **across** | **auto** | **normal** }，配置以太网电接口的网线类型。

缺省情况下，以太网电接口自动识别所连接网线的类型。

电接口可识别的网线类型可以分为交叉网线和直通网线两种。**across** 表示接口可识别交叉网线；**normal** 表示接口可识别直通网线；**auto** 表示自动识别网线，即与该接口实际连接的网线类型既可以使用直通网线也可以使用交叉网线。

----结束

（可选）配置双工模式

背景信息

请在需要配置以太网接口双工模式的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太网电接口视图。

步骤 3 执行命令 **undo negotiation auto**，配置以太网电接口工作在非自协商模式。

步骤 4 执行命令 **duplex** { **full** | **half** }，配置以太网电接口的双工模式。

缺省情况下，当以太网电接口工作在非自协商模式时，它的双工模式为全双工模式。

----结束

版权所有 © 华为技术有限公司

（可选）配置速率

背景信息

请在需要配置以太网接口速率的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **undo negotiation auto**，配置以太网接口工作在非自协商模式。

步骤 4 执行命令 **speed** { **10** | **100** | **1000** }，配置以太网接口的速率。

缺省情况下，当以太网接口工作在非自协商模式时，它的速率为接口支持的最大速率。

----结束

（可选）使能自协商功能

背景信息

请在需要配置以太网接口自协商功能的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **negotiation auto**，配置接口工作在自协商模式。

缺省情况下，接口工作在自协商模式。

接口的自协商模式需要与对端设备接口保持一致。

说明

100M 光接口不支持配置自协商模式。

1000M 光接口的自协商功能不能协商接口速率。

----结束

（可选）配置光接口与电接口切换

背景信息

请在需要配置以太网光口与电口切换的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface gigabitethernet** *interface-number*，进入 GigabitEthernet 接口视图。

步骤 3 执行命令 **combo-port** { **auto** | **copper** | **fiber** }，配置以太网光口与电口切换。

缺省情况下，自动切换光口模式与电口模式。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display interface** [*interface-type* [*interface-number*]] 查看以太网接口的描述信息、双工模式和速率。

----结束

3.1.4 配置以太网接口的高级属性

介绍配置以太网接口的端口环回、端口组、最大帧长、流量控制、流量控制自协商、电缆检测、环回测试、端口隔离的过程与步骤。

建立配置任务

应用环境

在以下情况，需执行本配置任务：

- AC6605 上使用端口组功能实现一次配置多个端口，以减少重复配置工作。
- 当 AC6605 上的某个接口接收到的流量可能超过该接口的处理能力，且和它直接相连的接口也支持流量控制功能，可打开本端接口的流量控制开关。当接口上的流量控制开关打开后，如果接口接收流量达到最大值，接口会向对端发送 Pause 帧（全双工模式下）或通过反压方式（半双工模式下）来通知对方本端的处理能力已经达到极限。如果对方接口也支持流量控制功能，就会自动降低发送速率，和本端端口的转发能力一致，从而保证本端接口能够正常处理接收到的帧。
- AC6605 上的端口隔离功能是指使能了端口隔离功能的端口之间两两隔离，可以实现同一 VLAN 内端口之间的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

前置任务

无

数据准备

在配置以太网接口的高级属性之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	接口的编号
2	（可选）接口允许通过的最大帧长

（可选）配置以太网接口环回功能

背景信息

请在需要配置以太网接口环回的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **loopback internal**，配置以太网端口的环回功能。

缺省情况下，以太网接口环回功能处于关闭状态。

----结束

（可选）配置端口组

背景信息

请在需要配置以太网端口组的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **port-group** *port-group-name*，进入端口组视图。

步骤 3 执行命令 **group-member** *interface-type interface-number*，添加以太网端口到指定端口组中。

----结束

（可选）配置接口允许通过的最大帧长

背景信息

请在需要配置以太网接口最大帧长的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太网接口视图。

步骤 3 执行命令 **jumboframe enable** [*value*]，设置允许通过以太网接口的最大帧长。

缺省情况下，AC6605 允许通过的最大帧长度为 9216 字节。

----结束

（可选）使能流量控制

背景信息

请在需要配置流量控制功能的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **flow-control**，打开以太网接口的流量控制开关。

缺省情况下，以太网接口的流量控制开关处于关闭状态。

对端设备接口也需要打开流量控制开关才能实现流量控制。

----结束

（可选）使能流量控制自协商功能

背景信息

请在需要配置以太网接口流量控制自协商功能的 AC6605 上进行如下配置。

千兆以太网接口支持流量控制自协商功能，快速以太网接口不支持此功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface gigabitethernet** *interface-number*，进入 GE 接口视图。

步骤 3 执行命令 **flow-control negotiation**，打开千兆以太网接口的流量控制自协商功能。

缺省情况下，以太网接口的流量控制自协商功能处于关闭状态。

对端设备接口也需要配置流量控制自协商才能实现流量控制自协商成功。

----结束

（可选）使能端口隔离功能

版权所有 © 华为技术有限公司

背景信息

请在需要配置端口隔离功能的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **port-isolate mode** { **l2** | **all** }，配置端口隔离模式。

缺省情况下，端口隔离模式为二层隔离三层互通。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入以太网接口视图。

步骤 4 （可选）执行命令 **am isolate** *interface-type interface-number* [**to** *interface-number*]，配置端口单向隔离。

说明

接口 A 配置与接口 B 单向隔离，即接口 A 发送的报文不能到达接口 B，但从接口 B 发送的报文可以到达接口 A。

步骤 5 执行命令 **port-isolate enable** [**group** *group-id*]，使能端口隔离功能。

说明

同一端口隔离组的端口之间互相隔离，不同端口隔离组的端口之间不隔离。如果不指定 *group-id* 参数时，默认加入的端口隔离组为 1。

----结束

（可选）使能电缆检测功能

背景信息

电缆检测功能可用于检测接口所连的电缆是否存在故障。当电缆状态为正常时，检测信息中的长度是指该电缆的总长度。当电缆状态非正常时，检测信息中的长度是指从本端口到故障位置的长度。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **virtual-cable-test**，配置接口电缆检测功能。

说明

- 测试结果不能保证对所有厂商生产的网线都准确，测试结果仅供参考。
- 执行本命令时，可能会在短时间内影响该接口的业务正常使用。
- Combo 电口支持电缆检测功能。
- 建议将对端端口 shutdown 或拔掉对端端口的网线，以免对端信号对测试结果产生影响。

----结束

（可选）配置接口环回测试

版权所有 © 华为技术有限公司

背景信息

请在需要进行以太网接口环回测试的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **loopbacktest internal**，配置以太网接口的环回测试功能。

缺省情况下，接口没有配置环回测试功能。

----结束

检查配置结果

操作步骤

- 使用命令 **display port-group** [**all** | *port-group-name*] 查看配置的端口组。
- 使用命令 **display interface** [*interface-type* [*interface-number*]] 查看接口的自协商功能。
- 使用命令 **display virtual-cable-test** *interface-type interface-number* 查看以太网接口的电缆检测结果。

----结束

3.1.5 维护

介绍维护以太网接口的相关命令和方法。

调试以太网接口

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现以太网接口或 Eth-Trunk 运行故障时，请在用户视图下执行 **debugging** 命令对以太网接口或 Eth-Trunk 进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

步骤 1 使用命令 **debugging l2if** [**error** | **event** | **msg** | **updown**] 打开数据链路层特性的调试开关。

----结束

版权所有 © 华为技术有限公司

3.1.6 配置举例

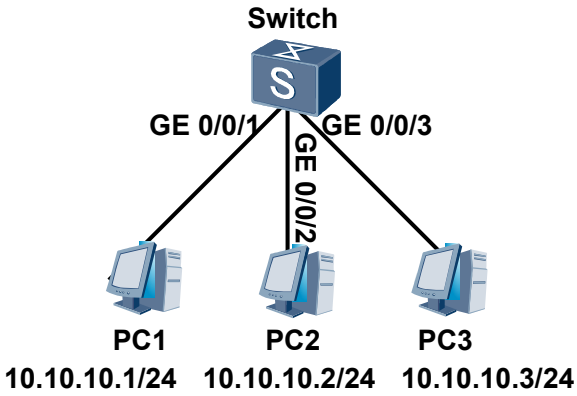
介绍以太网接口的各种组网举例。

配置端口隔离示例

组网需求

如图 3-1 所示，要求 PC1 与 PC2 之间不能互相访问，PC1 与 PC3 之间可以互相访问，PC2 与 PC3 之间可以互相访问。

图 3-1 配置端口隔离示例组网图



配置思路

采用如下的思路配置端口隔离：

1. 使能 PC1 和 PC2 相连端口的端口隔离功能，使 PC1 与 PC2 不能互相访问。

数据准备

为完成此配置例，需准备如下的数据：

- Switch 与 PC1 之间连接的端口号。
- Switch 与 PC2 之间连接的端口号。
- 配置 Switch 的端口隔离模式为二层隔离三层互通（此配置为缺省配置）。
- 配置连接 PC1、PC2、PC3 的端口属于同一 VLAN（缺省情况下属于 VLAN1）。
- 配置连接 PC1、PC2 的端口属于同一隔离组（缺省情况下属于隔离组 1）。

操作步骤

步骤 1 配置端口隔离功能

配置端口隔离模式为二层隔离三层互通。

```
<Quidway> system-view
[Quidway] port-isolate mode l2
```


版权所有 © 华为技术有限公司

配置 GigabitEthernet0/0/1 的端口隔离功能。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port-isolate enable
[Quidway-GigabitEthernet0/0/1] quit
```

配置 GigabitEthernet0/0/2 的端口隔离功能。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port-isolate enable
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 验证配置结果

PC1 和 PC2 不能互相 ping 通。

PC1 和 PC3 可以互相 ping 通。

PC2 和 PC3 可以互相 ping 通。

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
interface GigabitEthernet0/0/1
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
#
return
```

3.2 链路聚合配置

介绍链路聚合的基本知识、配置方法和配置实例。

3.2.1 链路聚合概述

简要介绍链路聚合的基本概念。

链路聚合（Link Aggregation）是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽的一种方法，又称为多接口负载均衡组（Load Sharing Group）或链路聚合组（Link Aggregation Group），相关的协议标准请参考 IEEE802.3ad。

通过在两台设备之间建立链路聚合组，可以提供更高的通讯带宽和更高的可靠性。链路聚合不仅为设备间通信提供了冗余保护，而且不需要对硬件进行升级。

3.2.2 AC6605 支持的链路聚合特性

介绍链路聚合特性在 AC6605 中的支持情况。

版权所有 © 华为技术有限公司

手工负载分担模式

手工负载分担模式允许在聚合组中手工加入多个成员接口，所有的接口均处于转发状态，分担负载的流量。AC6605 支持的负载分担方式包括目的 MAC、源 MAC、源 MAC 异或目的 MAC、源 IP、目的 IP、源 IP 异或目的 IP。

Eth-Trunk 的创建、成员接口的加入都需要手工配置完成，没有 LACP（link Aggregation Control Protocol）协议报文的参与。

手工负载分担模式通常应用在对端设备不支持 LACP 协议的情况下。

静态 LACP 模式

静态 LACP 模式是一种利用 LACP 协议进行聚合参数协商、确定活动接口和非活动接口的链路聚合方式。该模式下，需手工创建 Eth-Trunk，手工加入 Eth-Trunk 成员接口，由 LACP 协议协商确定活动接口和非活动接口。

静态 LACP 模式也称为 M：N 模式。这种方式同时可以实现链路负载分担和链路冗余备份的双重功能。在链路聚合组中 M 条链路处于活动状态，这些链路负责转发数据并进行负载分担，另外 N 条链路处于非活动状态作为备份链路，不转发数据。当 M 条链路中有链路出现故障时，系统会从 N 条备份链路中选择优先级最高的接替出现故障的链路，同时这条替换故障链路的备份链路状态变为活动状态开始转发数据。

静态 LACP 模式与手工负载分担模式的主要区别为：静态 LACP 模式有备份链路，而手工负载分担模式所有成员接口均处于转发状态，分担负载流量。

和静态 LACP 模式相对应的还包括动态 LACP 模式。动态 LACP 模式的链路聚合，从 Eth-Trunk 的创建到加入成员接口都不需要人工的干预，由 LACP 协议自动协商完成。虽然这种方式对于用户来说很简单，但由于这种方式过于灵活，不便于管理，所以 AC6605 上不支持动态 LACP 模式链路聚合。

活动接口与非活动接口

处于活动状态并负责转发数据的接口称作活动接口。相反，处于非活动状态禁止转发数据的接口称作非活动接口。根据配置的工作模式不同，角色分工如下：

- 手工负载分担模式。正常情况下，所有的成员接口均为活动接口，除非这些接口出现链路故障。
- 静态 LACP 模式。M 条链路对应的接口为活动接口负责转发数据，N 条链路对应的接口为非活动接口负责冗余备份。

主动端与被动端

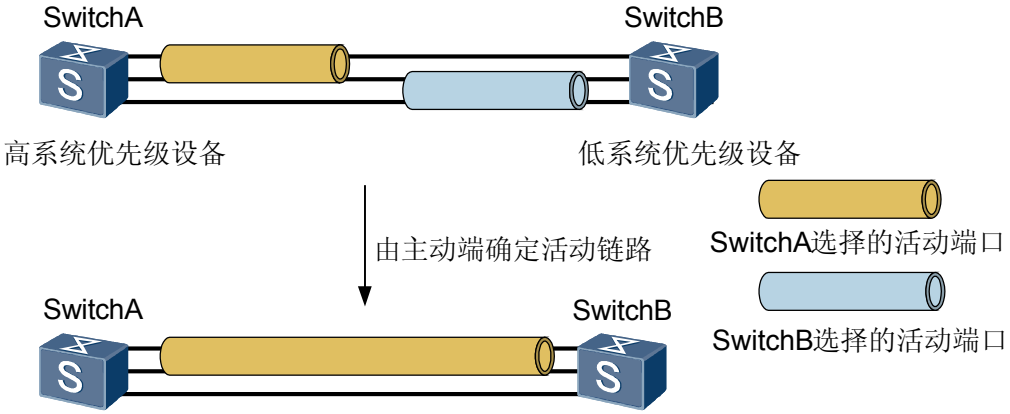
在静态 LACP 模式下，聚合组两端的设备中 LACP 优先级较高的一端为主动端，LACP 优先级较低的一端为被动端。

如果两端设备的 LACP 优先级一样时,需要按照系统 MAC 来选择主动端，系统 MAC 小的一端优先。

区分主动端与被动端的目的是为了保证两端设备最终确定的活动接口一致，如果两端都按照本端各自的接口优先级来选择活动接口，两端所确定的活动接口很可能不一致，活动链路也就无法建立。因此首先确定主动端，被动端按照主动端侧的接口优先级来选择活动接口。如图 3-2 所示。

版权所有 © 华为技术有限公司

图 3-2 静态 LACP 模式下主动端确定活动链路



3.2.3 配置手工负载分担模式链路聚合

介绍了手工负载分担模式链路聚合配置场景、步骤及注意事项。

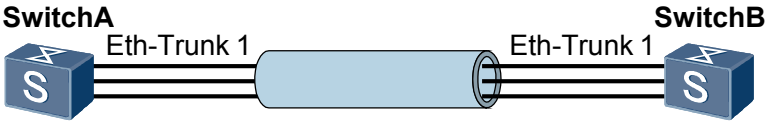
建立配置任务

应用环境

当需要增加两台设备之间的带宽或可靠性，而两台设备中有一台不支持 LACP 协议时，可在 Switch 设备上创建手工负载分担模式的 Eth-Trunk，并加入多个成员接口增加设备间的带宽及可靠性。

如图 3-3 所示，SwitchA 和 SwitchB 之间创建 Eth-Trunk。

图 3-3 手工负载分担模式链路聚合组网图



前置任务

在配置手工负载分担模式链路聚合之前，需完成以下任务：

- 设备正常上电。
- 创建 Eth-Trunk。

数据准备

在配置手工负载分担模式链路聚合之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	负载分担模式 Eth-Trunk 的编号
2	成员接口的类型和编号

配置 Eth-Trunk 工作模式为手工负载分担模式

背景信息

说明

改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。删除已存在的成员接口请在相应接口视图下执行命令 **undo eth-trunk** 或在 Eth-Trunk 视图下执行命令 **undo trunkport** *interface-type interface-number*。

在需要配置手工负载分担模式 Eth-Trunk 的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **mode manual load-balance**，配置当前 Eth-Trunk 工作模式为手工负载分担模式。

缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

如果本端配置手工负载分担模式 Eth-Trunk，那么对端设备也必须要配置手工负载分担模式 Eth-Trunk。

----结束

向 Eth-Trunk 中加入成员接口

背景信息

在需要配置 Eth-Trunk 成员接口的 AC6605 上进行如下配置。

操作步骤

- 在 Eth-Trunk 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>，增加成员接口。
- 在成员接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

3. 执行命令 **eth-trunk** *trunk-id*，将当前接口加入 Eth-Trunk。

将成员接口加入 Eth-Trunk 时，需要注意以下问题：

- 每个 Eth-Trunk 接口下最多可以包含 8 个成员接口。
- 成员接口不能配置任何业务和静态 MAC 地址。
- 成员接口加入 Eth-Trunk 时，必须为缺省的 hybrid 类型接口。
- Eth-Trunk 接口不能嵌套，即成员接口不能是 Eth-Trunk。
- 一个以太网接口只能加入到一个 Eth-Trunk 接口，如果需要加入其它 Eth-Trunk 接口，必须先退出原来的 Eth-Trunk 接口。
- 一个 Eth-Trunk 接口中的成员接口必须是同一类型，例如：FE 口和 GE 口不能加入同一个 Eth-Trunk 接口。
- 可以将不同接口板上的以太网接口加入到同一个 Eth-Trunk。
- 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。
- 当成员接口的速率不一致时，实际使用中速率小的接口可能会出现拥塞，导致丢包。
- 当成员接口加入 Eth-Trunk 后，学习 MAC 地址时是按照 Eth-Trunk 来学习的，而不是按照成员接口来学习。

----结束

（可选）配置负载分担方式

背景信息

在需要配置 Eth-Trunk 负载分担方式的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

缺省情况下，AC6605 上 Eth-Trunk 接口的负载分担模式为 **src-dst-ip**。

AC6605 支持以下负载分担模式：

- dst-ip（目的 IP 地址）模式：从目的 IP 地址、出端口的 TCP/UDP 端口号中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- dst-mac（目的 MAC 地址）模式：从目的 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-ip（源 IP 地址）模式：从源 IP 地址、入端口的 TCP/UDP 端口号中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。

版权所有 © 华为技术有限公司

- src-mac（源 MAC 地址）模式：从将源 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-dst-ip（源 IP 地址与目的 IP 地址的异或）模式：从目的 IP 地址、源 IP 地址两种负载分担模式的运算结果进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-dst-mac（源 MAC 地址与目的 MAC 地址的异或）模式：从目的 MAC 地址、源 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。

Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

----结束

（可选）配置活动接口数阈值

背景信息

在需要配置活动接口数阈值的 AC6605 上进行如下配置。

操作步骤

- 配置链路聚合带宽的上限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **max bandwidth-affected-linknumber** *link-number*，配置影响链路聚合带宽的接口数上限阈值。

     缺省情况下，链路聚合带宽的上限阈值为 8。

  说明

  - 本端 AC6605 设备和对端 AC6605 设备的链路聚合带宽的上限阈值可以不同。如果两端配置链路聚合带宽的上限阈值不同，则以上限阈值数值较小的一端为准。
- 配置活动接口数下限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **least active-linknumber** *link-number*，配置活动接口数下限阈值。

     缺省情况下，活动接口数下限阈值为 1。

  配置手工模式活动接口数目下限阈值可以决定 Eth-Trunk 中活动接口数的最小值，如果手工模式下活动接口数目小于该值，Eth-Trunk 的接口状态将变为 DOWN 的状态。

  说明

  - 本端 AC6605 设备和对端 AC6605 设备的活动接口数下限阈值可以不同。如果下限阈值不同，以下限阈值数值较大的一端为准。

----结束

版权所有 © 华为技术有限公司

检查配置结果

操作步骤

- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口。
- 使用命令 **display eth-trunk** *trunk-id* 查看 Eth-Trunk 的手工负载分担模式。

----结束

3.2.4 配置静态 LACP 模式链路聚合

介绍了静态 LACP 模式链路聚合配置场景、步骤及注意事项。

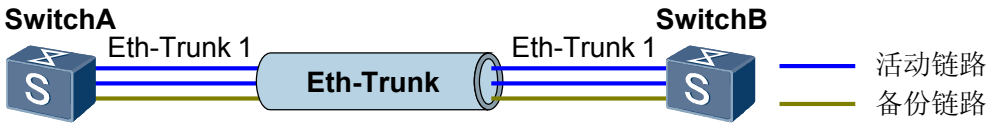
建立配置任务

应用环境

在两台直接相连 Switch 设备上配置链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

- 两设备间的链路具有冗余备份的能力，当部分链路故障时使用备份链路替代故障链路，保持数据传输的不中断。
- 活动链路具有负载分担的能力。

图 3-4 静态 LACP 模式链路聚合组网图



前置任务

在配置手工负载分担模式链路聚合之前，需完成以下任务：

- 设备正常上电。
- 创建 Eth-Trunk。

数据准备

在配置静态 LACP 模式链路聚合的基本功能之前，需要准备以下数据。

序号	数据
1	Eth-Trunk 的编号
2	成员接口的类型和编号
3	活动接口上限阈值

版权所有 © 华为技术有限公司

配置 Eth-Trunk 的工作模式为静态 LACP 模式

背景信息

说明

改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。删除已存在的成员接口请在相应接口视图下执行命令 **undo eth-trunk** 或在 Eth-Trunk 视图下执行命令 **undo trunkport** *interface-type interface-number*。

在需要配置静态 LACP 模式 Eth-Trunk 的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **bpdu enable**，配置接口上送 BPDU 报文到 CPU 处理。

步骤 4 执行命令 **mode lacp-static**，配置 Eth-Trunk 的工作模式为静态 LACP 模式。

缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

如果本端配置静态 LACP 模式 Eth-Trunk，那么对端设备也必须要配置静态 LACP 模式 Eth-Trunk。

----结束

向 Eth-Trunk 中加入成员接口

背景信息

在需要配置 Eth-Trunk 成员接口的 AC6605 上进行如下配置。

操作步骤

- 在 Eth-Trunk 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>，增加成员接口。
- 在成员接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **eth-trunk** *trunk-id*，将当前接口加入 Eth-Trunk。

  将成员接口加入 Eth-Trunk 时，需要注意以下问题：

  - 每个 Eth-Trunk 接口下最多可以包含 8 个成员接口。

版权所有 © 华为技术有限公司

- 成员接口不能配置任何业务和静态 MAC 地址。
- 成员接口加入 Eth-Trunk 时，必须为缺省的 hybrid 类型接口。
- Eth-Trunk 接口不能嵌套，即成员接口不能是 Eth-Trunk。
- 一个以太网接口只能加入到一个 Eth-Trunk 接口，如果需要加入其它 Eth-Trunk 接口，必须先退出原来的 Eth-Trunk 接口。
- 一个 Eth-Trunk 接口中的成员接口必须是同一类型，即 FE 口和 GE 口不能加入同一个 Eth-Trunk 接口。
- 可以将不同接口板上的以太网接口加入到同一个 Eth-Trunk。
- 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。
- 当成员接口的速率不一致时，实际使用中速率小的接口可能会出现拥塞，导致丢包。
- 当成员接口加入 Eth-Trunk 后，学习 MAC 地址时是按照 Eth-Trunk 来学习的，而不是按照成员接口来学习。
- 当成员接口全部都是半双工模式时，Eth-Trunk 不能协商成 UP 状态。

----结束

（可选）配置负载分担方式

背景信息

在需要配置 Eth-Trunk 负载分担方式的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

缺省情况下，AC6605 上 Eth-Trunk 接口的负载分担模式为 **src-dst-ip**。

AC6605 支持以下负载分担模式：

- dst-ip（目的 IP 地址）模式：从目的 IP 地址、出端口的 TCP/UDP 端口号中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- dst-mac（目的 MAC 地址）模式：从目的 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-ip（源 IP 地址）模式：从源 IP 地址、入端口的 TCP/UDP 端口号中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-mac（源 MAC 地址）模式：从将源 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。

版权所有 © 华为技术有限公司

- src-dst-ip（源 IP 地址与目的 IP 地址的异或）模式：从目的 IP 地址、源 IP 地址两种负载分担模式的运算结果进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。
- src-dst-mac（源 MAC 地址与目的 MAC 地址的异或）模式：从目的 MAC 地址、源 MAC 地址、VLAN ID、以太网类型及入端口信息中分别选择指定位的 3bit 数值进行异或运算，根据运算结果选择 Eth-Trunk 表中对应的出接口。

Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

----结束

（可选）配置活动接口数阈值

背景信息

在需要配置活动接口数阈值的 AC6605 上进行如下配置。

操作步骤

- 配置活动接口数上限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **max active-linknumber** *link-number* ，配置链路聚合活动接口数上限阈值。

     缺省情况下，活动接口数上限阈值为 8。

  配置静态 LACP 模式活动接口数目上限阈值可以控制 Eth-Trunk 中活动接口的最大数 M，剩余的成员接口处于备份状态。

  如果未配置上限阈值，Eth-Trunk 最多允许 8 个接口同时处于活动状态。

  说明

  - 活动接口数上限阈值必须大于等于活动接口数下限阈值。
  - 本端 AC6605 设备和对端 AC6605 设备的活动接口数上限阈值可以不同。如果两端配置活动接口数的上限阈值不同，则以上限阈值数值较小的一端为准。
- 配置活动接口数下限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **least active-linknumber** *link-number*，配置链路聚合活动接口数下限阈值。

     缺省情况下，活动接口数下限阈值为 1。

  配置静态 LACP 模式活动接口数目下限阈值可以决定 Eth-Trunk 中活动接口数的最小值，如果静态模式下活动接口数目小于该值，Eth-Trunk 的接口状态将变为 DOWN 的状态。

版权所有 © 华为技术有限公司

说明

- 活动接口数下限阈值必须小于等于活动接口数上限阈值。
- 本端 AC6605 设备和对端 AC6605 设备的活动接口数下限阈值可以不同。如果下限阈值不同，以下限阈值数值较大的一端为准。

----结束

（可选）配置系统 LACP 优先级

背景信息

在需要配置系统 LACP 优先级的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lacp priority** *priority*，配置当前 AC6605 设备的系统 LACP 优先级。

系统 LACP 优先级值越小优先级越高，缺省情况下，系统 LACP 优先级为 32768。

在两端设备中选择系统 LACP 优先级较小一端作为主动端，如果系统 LACP 优先级相同则选择 MAC 地址较小的一端作为主动端。

----结束

（可选）配置接口 LACP 优先级

背景信息

在需要配置接口 LACP 优先级的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **lacp priority** *priority*，配置当前接口的 LACP 优先级。

缺省情况下，接口的 LACP 优先级是 32768。*priority* 取值越小，表明接口的 LACP 优先级越高。

----结束

（可选）使能 LACP 抢占并配置抢占等待时间

背景信息

在需要配置 LACP 抢占的 AC6605 上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **lacp preempt enable**，使能当前 Eth-Trunk 接口的 LACP 抢占功能。

缺省情况下，LACP 抢占功能处于禁止状态。

说明

为保证 Eth-Trunk 正常工作，要求 Eth-Trunk 两端统一配置使能 LACP 抢占或不使能 LACP 抢占。

步骤 4 执行命令 **lacp preempt delay** *delay-time*，配置当前 Eth-Trunk 接口的 LACP 抢占等待时间。

缺省情况下，LACP 抢占等待时间为 30 秒。

使能 LACP 抢占功能可以保持接口 LACP 优先级最高的接口为活动接口。例如：当一条高优先级的接口因故障切换为非活动状态而后又恢复时，如果使能了抢占，则高优先级的接口将重新成为活动接口；如果未使能抢占，该接口不能重新成为活动接口。

抢占等待时间是指在静态 LACP 模式的 Eth-Trunk 中非活动接口切换为活动接口需要等待的时间。

----结束

（可选）配置接收 LACP 协议报文超时时间

背景信息

在需要配置接收 LACP 协议报文超时时间的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **lacp timeout** { **fast** | **slow** }，配置当前接口接收 LACP 协议报文的超时时间。

说明

- 配置此命令后，本端将接收报文的超时时间通过 LACP 报文通知对端。配置为 **fast**，对端发送 LACP 报文的周期为 1 秒。配置为 **slow**，对端发送 LACP 报文的周期为 30 秒。
- LACP 协议报文的超时时间为 LACP 报文发送周期的 3 倍，即：配置为 **fast**，接收 LACP 协议报文的超时时间为 3 秒。配置为 **slow**，接收 LACP 协议报文的超时时间为 90 秒。
- 两端配置的超时时间可以不一致。但为了便于维护，建议用户配置一致的 LCAP 协议报文超时时间。

----结束

检查配置结果

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口。
- 使用命令 **display eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 查看 Eth-Trunk 信息、活动接口信息以及非活动接口信息。

----结束

3.2.5 配置 E-Trunk

E-Trunk 是一种实现跨设备链路聚合的控制协议，基于 LACP（单台设备链路聚合的标准）进行了扩展，能够实现多台设备间的链路聚合。从而把链路可靠性从单板级提高到了设备级。

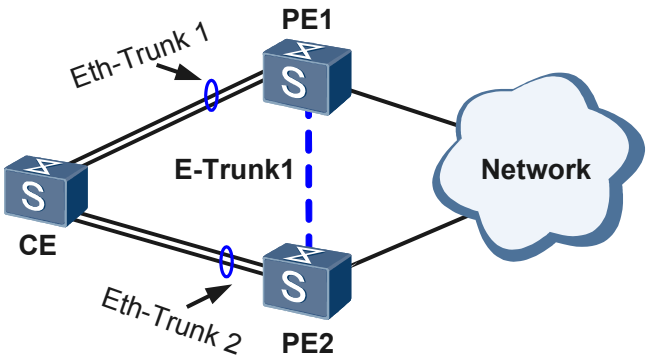
建立配置任务

在进行 E-Trunk 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 3-5 所示，E-Trunk（Enhanced Trunk）应用于 CE 接入网络时，在 CE 与双 PE 间实现链路保护。CE 分别通过一条静态 LACP 模式的 Eth-Trunk 与 PE1、PE2 相连。这两个 Eth-Trunk 构成一个 E-Trunk，在 PE1 与 PE2 之间实现链路聚合组的备份，提高网络可靠性。

图 3-5 配置 E-Trunk 组网图



前置任务

在配置 E-Trunk 之前，需要完成以下任务：

- 正确连接设备之间的物理链路。
- 配置静态 LACP 模式 Eth-Trunk 接口。

数据准备

在配置 E-Trunk 之前，需准备以下数据：

版权所有 © 华为技术有限公司

序号	数据
1	LACP 系统 ID 和优先级
2	E-Trunk 的 ID、优先级
3	Eth-Trunk 接口号和工作模式
4	源端和对端的 IP 地址
5	加密密码
6	Hello 报文发送周期和检测 Hello 报文的时间倍数

配置 E-Trunk 的 LACP 系统 ID 和优先级

在 E-Trunk 中，为了使 CE 设备认为对端的两台 PE 设备是一台设备，E-Trunk 中主、备两台 PE 设备的 LACP 优先级、系统 ID 都需要保持一致。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lacp e-trunk system-id** *mac-address*，配置 E-Trunk 的 LACP 系统 ID。

缺省情况下，使用主控板的以太口 MAC 地址作为 E-Trunk 的 LACP 系统 ID。

E-Trunk 中主备两台设备的 LACP 系统 ID 需要保持一致。

步骤 3 执行命令 **lacp e-trunk priority** *priority*，配置 E-Trunk 的 LACP 优先级。

缺省情况下，E-Trunk 的 LACP 优先级是 32768。

E-Trunk 中主备两台设备的 LACP 优先级需要保持一致。

----结束

创建 E-Trunk 并配置优先级

E-Trunk 的优先级用于在聚合组中决策两台设备的主备状态。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，创建 E-Trunk。

版权所有 © 华为技术有限公司

当 E-Trunk 存在时，执行本命令直接进入 E-Trunk 视图。

在一个 E-Trunk 内，两端设备上配置的 *e-trunk-id* 必须相同。

一台设备上最多创建 16 个 E-Trunk。

步骤 3 执行命令 **priority** *priority*，配置 E-Trunk 的优先级。

优先级用于两台设备间进行主备协商，优先级高的为主用设备，值越小优先级越高。

如果优先级相同，那么比较两台设备的系统 ID，ID 较小的为主用设备。

缺省情况下，E-Trunk 的优先级为 100。

----结束

配置本端和对端的 IP 地址

E-Trunk 协议报文采用本端配置的 Source IP 及协议端口号发送。如果要修改地址则两台设备需要同时修改，否则会导致协议报文丢弃。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，进入 E-Trunk 视图。

步骤 3 执行命令 **peer-address** *peer-ip-address* **source-address** *source-ip-address*，配置对端和本端的 IP 地址。

对端和本端上的 IP 地址互为对端和源端。例如，设备 A 和设备 B 之间建立 E-Trunk，设备 A 上的对端 IP 为 2.2.2.2，源端 IP 为 1.1.1.1。那么，设备 B 上的对端 IP 为 1.1.1.1，源端 IP 为 2.2.2.2。

----结束

配置 E-Trunk 与 BFD 会话绑定

通过报文接收超时无法快速感知对端是否故障，可以使用快速检测协议 BFD 快速感知。每个 E-Trunk 都需要指定对端的 IP，通过创建检测对端路由是否可达的 BFD 会话，E-Trunk 可感知到 BFD 通告的故障，并快速处理。

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，进入 E-Trunk 视图。

步骤 3 执行命令 **e-trunk track bfd-session** *session-id*，绑定 BFD 会话。

版权所有 © 华为技术有限公司

BFD 用于实现 E-Trunk 的两台设备之间控制协议链路的快速故障检测。

----结束

将 Eth-Trunk 加入 E-Trunk

当 E-Trunk 配置成功，必须向 E-Trunk 中加入成员 Eth-Trunk，才能实现两台设备上的链路聚合协议。从而实现跨设备的链路聚合组冗余，提高网络可靠性。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

仅静态 LACP 模式的 Eth-Trunk 才能加入 E-Trunk。

步骤 3 执行命令 **e-trunk** *e-trunk-id*，将 Eth-Trunk 加入到指定 E-Trunk 中。

一个 Eth-Trunk 只能加入一个 E-Trunk。

一个 E-Trunk 中，两端设备上所加入的 Eth-Trunk ID 必须一致。例如，设备 A 上加入 E-Trunk1 中的有 Eth-Trunk 1 和 Eth-Trunk 2。那么在设备 B 上加入 E-Trunk1 中的必须是 Eth-Trunk 1 和 Eth-Trunk 2。

----结束

（可选）配置 Eth-Trunk 在 E-Trunk 中的工作模式

只能对已经加入 E-Trunk 的 Eth-Trunk 配置工作模式，Eth-Trunk 的工作模式分为：自动模式、强制主用模式和强制备用模式。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

仅静态 LACP 模式的 Eth-Trunk 才能加入 E-Trunk。

步骤 3 执行命令 **e-trunk mode** { **auto** | **force-master** | **force-backup** }，配置 Eth-Trunk 在 E-Trunk 中的工作模式。

缺省情况下，Eth-Trunk 在 E-Trunk 中工作在自动模式。

只能对已经加入 E-Trunk 的 Eth-Trunk 执行本命令。当 Eth-Trunk 退出 E-Trunk 时，该配置将自动清除。

版权所有 © 华为技术有限公司

当设置工作模式为自动模式或者工作模式由强制模式切换为自动模式后，根据本端 E-Trunk 的主备状态和对端 Eth-Trunk 的故障信息决定本端成员 Eth-Trunk 的状态。

- 本端 E-Trunk 状态为主用，则本端 Eth-Trunk 的工作模式为主用。
- 本端 E-Trunk 状态为备用，对端成员 Eth-Trunk 为故障，则本端 Eth-Trunk 的工作模式为主用。当本端收到对端 Eth-Trunk 故障恢复消息后，该 Eth-Trunk 进入备用状态。

在 E-Trunk 正常工作期间，改变报文发送周期或超时时间，会引起主备状态振荡。因此建议在改变报文发送周期或超时时间前，先将成员 Eth-Trunk 的工作模式设置为强制主/备模式，待新的配置生效后，再恢复自动模式。

----结束

（可选）配置密码

为了提高系统的安全性可配置加密密码。E-Trunk 中的两端设备上的加密密码必须配置为一致。

背景信息

用户可以选择采用明文加密或密文加密。

- 明文加密时，在配置文件中采用明文形式显示。
- 密文加密时，在配置文件中采用加密后的乱码显示，不显示真正的密码。

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，进入 E-Trunk 视图。

步骤 3 执行命令 **security-key** { **simple** *simple-key* | **cipher** *cipher-key* }，配置加密报文的密码。



注意

如果使用 simple 选项，密码将以明文形式保存在配置文件中，以低级别登录的用户可以通过查看配置方式获取密码，造成安全隐患。因此，建议使用 cipher 选项，将密码加密保存。

----结束

（可选）配置超时时间

如果处于备用状态的 E-Trunk 在超时时间内没有收到对端发送的 Hello 报文，则在定时器超时后进入主用状态。此处的超时时间是对端报文中所携带的超时时间，而不是本端设置的超时时间。

背景信息

请在组成 E-Trunk 的两端设备上分别进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，进入 E-Trunk 视图。

步骤 3 执行命令 **timer hello** *hello-times*，配置 Hello 报文的发送周期。

缺省情况下，Hello 报文发送周期值为 10，单位为 100 毫秒，即 1 秒。

步骤 4 执行命令 **timer hold-on-failure multiplier** *multiplier*，配置检测 Hello 报文的时间倍数。

对端利用接收到的报文中携带的超时时间来检测本端是否超时。如果对端处于备用状态，在超时时间内没有收到由本端发送的 Hello 报文，则在定时器超时后进入主用状态。

超时时间 = 发送周期 × 时间倍数。建议将时间倍数设置为 3 倍以上。

缺省情况下，检测 Hello 报文的时间倍数为 20。

----结束

（可选）配置延时回切时间

配置 E-Trunk 的延时回切时间后，必须等待延时回切定时器超时，本端 E-Trunk 的成员 Eth-Trunk 恢复为主用状态。从而延迟了 E-Trunk 成员的流量回切时间，保证业务流量不会中断。

背景信息

当 E-Trunk 与其他业务配合使用时，如果 E-Trunk 状态为主用的设备发生故障恢复后，成员 Eth-Trunk 状态恢复早于其他相关业务恢复。如果马上将 E-Trunk 成员的流量回切，将会导致业务流量中断。

配置 E-Trunk 的延时回切时间后，必须等待延时回切定时器超时，本端成员 Eth-Trunk 状态才能 Up，E-Trunk 的本端设备才能恢复为主用状态。从而延迟了 E-Trunk 成员的流量回切时间，保证业务流量不会中断。

请在组成 E-Trunk 的两端设备上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **e-trunk** *e-trunk-id*，进入 E-Trunk 视图。

步骤 3 执行命令 **timer revert delay** *delay-value*，配置回切延迟时间。

缺省情况下，E-Trunk 延时回切的时间为 120 秒。

----结束

检查配置结果

E-Trunk 配置成功后，您可以查看到 E-Trunk 优先级、系统 ID、源 IP、对端 IP、延时回切时间、主备状态、主备状态的原因等内容。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **display e-trunk** *e-trunk-id*，查看 E-Trunk 的信息。

----结束

3.2.6 维护

清除 LACP 统计信息、调试链路聚合组、监控链路聚合组运行状况。

清除 LACP 统计信息

背景信息

注意

清除 LACP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在用户视图下使用命令 **reset lacp statistics eth-trunk** [*trunk-id*] 清除 LACP 收发报文的统计信息。

----结束

调试链路聚合组

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行命令 undo debugging all 关闭调试开关。

当链路聚合组出现运行故障时，请在用户视图下执行命令 **debugging** 对链路聚合进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

- 使用命令 **debugging trunk error** 打开 Eth-Trunk 差错信息调试开关。
- 使用命令 **debugging trunk event** 打开 Eth-Trunk 事件通知调试开关。
- 使用命令 **debugging trunk lacp-pdu** 打开 LACP 报文调试开关。
- 使用命令 **debugging trunk lagmsg** 打开 LACP 协议消息调试开关。
- 使用命令 **debugging trunk msg** 打开 Eth-Trunk 消息调试开关。

版权所有 © 华为技术有限公司

- 使用命令 **debugging trunk state-machine** 打开 Eth-Trunk 状态机调试开关。
- 使用命令 **debugging trunk updown** 打开 Eth-TrunkUp/Down 信息调试开关。
- 使用命令 **debugging trunk** 打开 Eth-Trunk 信息调试开关。

----结束

监控链路聚合组运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解链路聚合组的运行状况。

操作步骤

- 使用命令 **display eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 查看链路聚合组状态信息。
- 使用命令 **display lacp statistics eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 查看 LACP 收发报文统计信息。
- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口信息。

----结束

3.2.7 配置举例

介绍了手工负载分担模式和静态 LACP 模式下的典型应用场景举例。

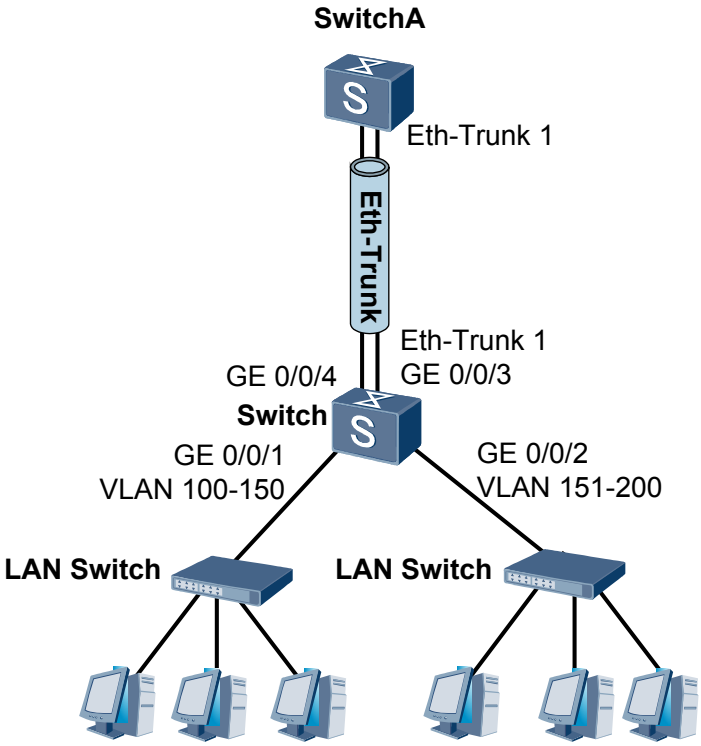
配置手工负载分担模式链路聚合示例

组网需求

如图 3-6 所示，Switch 和 SwitchA 之间用 Eth-Trunk 链路连接。要求 Switch 和 SwitchA 之间的链路有较高的可靠性。

版权所有 © 华为技术有限公司

图 3-6 配置手工负载分担模式链路聚合组网图



配置思路

采用如下的思路配置负载分担链路聚合：

1. 创建 Eth-Trunk。
2. 加入成员接口。

数据准备

为完成此配置例，需准备的数据：

- 链路聚合组编号。
- Eth-Trunk 的成员接口类型和编号。

操作步骤

步骤 1 创建 Eth-Trunk

创建 Eth-Trunk 1。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] interface eth-trunk 1
[Switch-Eth-Trunk1] quit
```

步骤 2 向 Eth-Trunk 中加入成员接口

将 Eth0/0/3 加入 Eth-Trunk 1。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] eth-trunk 1
[Switch-GigabitEthernet0/0/3] quit
```

将 Eth0/0/4 加入 Eth-Trunk 1。

```
[Switch] interface gigabitethernet 0/0/4
[Switch-GigabitEthernet0/0/4] eth-trunk 1
[Switch-GigabitEthernet0/0/4] quit
```

步骤 3 配置 Eth-Trunk 1

配置 Eth-Trunk 1 允许 VLAN100-200 的报文通过。

```
[Switch] interface eth-trunk 1
[Switch-Eth-Trunk1] port link-type trunk
[Switch-Eth-Trunk1] port trunk allow-pass vlan 100 to 200
[Switch-Eth-Trunk1] quit
```

步骤 4 验证配置结果

在任意视图下执行 **display trunkmembership** 命令，检查 Eth-Trunk 1 是否创建成功，及成员接口是否正确加入。

```
[Switch] display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: gigabitethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of UP Ports in Trunk = 2
operate status: up
Interface GigabitEthernet0/0/3, valid, operate up, weight=1,
Interface GigabitEthernet0/0/4, valid, operate up, weight=1,
```

显示 Eth-Trunk 1 的配置信息。

```
[Switch] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL          Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName               Status      Weight
GigabitEthernet0/0/3           Up        1
GigabitEthernet0/0/4           Up        1
```

从以上信息看出 Eth-Trunk 1 中包含 2 个成员接口 Eth0/0/3 和 Eth0/0/4。成员接口的状态都为 Up。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Switch
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100 to 200
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface GigabitEthernet0/0/4
```


版权所有 © 华为技术有限公司

```
 eth-trunk 1
#
return
```

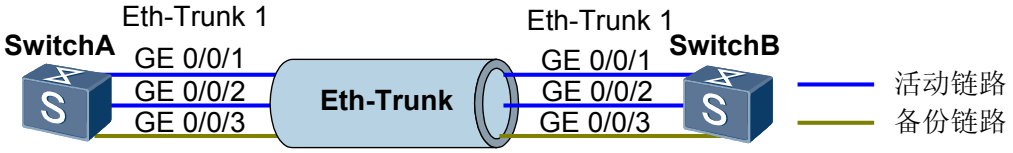
配置静态 LACP 模式链路聚合示例

组网需求

如图 3-7 所示，在两台 Switch 设备上配置静态 LACP 模式链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

- 2 条活动链路具有负载分担的能力。
- 两设备间的链路具有 1 条冗余备份链路，当活动链路出现故障链路时，备份链路替代故障链路，保持数据传输的可靠性。

图 3-7 配置静态 LACP 模式链路聚合组网图



配置思路

采用如下的思路配置静态 LACP 模式链路聚合：

1. 在 Switch 设备上创建 Eth-Trunk，配置 Eth-Trunk 为静态 LACP 模式。
2. 将成员接口加入 Eth-Trunk。
3. 配置系统优先级确定主动端。
4. 配置活动接口上限阈值。
5. 配置接口优先级确定活动链路。

数据准备

为完成此配置例，需准备如下的数据：

- 两端 Switch 设备链路聚合组编号。
- SwitchA 系统优先级。
- 活动接口上限阈值。
- 活动接口 LACP 优先级。

操作步骤

步骤 1 创建编号为 1 的 Eth-Trunk，配置它的工作模式为静态 LACP 模式

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
```


版权所有 © 华为技术有限公司

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] bpdu enable
[SwitchA-Eth-Trunk1] mode lacp-static
[SwitchA-Eth-Trunk1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface eth-trunk 1
[SwitchB-Eth-Trunk1] bpdu enable
[SwitchB-Eth-Trunk1] mode lacp-static
[SwitchB-Eth-Trunk1] quit
```

步骤 2 将成员接口加入 Eth-Trunk

配置 SwitchA。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] eth-trunk 1
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] eth-trunk 1
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] eth-trunk 1
[SwitchA-GigabitEthernet0/0/3] quit
```

配置 SwitchB。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] eth-trunk 1
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] eth-trunk 1
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] eth-trunk 1
[SwitchB-GigabitEthernet0/0/3] quit
```

步骤 3 在 SwitchA 上配置系统优先级为 100，使其成为 LACP 主动端

[SwitchA] **lacp priority 100**

步骤 4 在 SwitchA 上配置活动接口上限阈值为 2

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] max active-linknumber 2
[SwitchA-Eth-Trunk1] quit
```

步骤 5 在 SwitchA 上配置接口优先级确定活动链路

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] lacp priority 100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] lacp priority 100
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤 6 验证配置结果

查看各 Switch 设备的 Eth-Trunk 信息，查看链路是否协商成功。

```
[SwitchA] display eth-trunk 1
 Eth-Trunk1's state information is:
 Local:
 LAG ID: 1                 WorkingMode: STATIC
 Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
 System Priority: 100         System ID: 00e0-fca8-0417
Least Active-linknumber: 1  Max Active-linknumber: 2
```


版权所有 © 华为技术有限公司

```
Operate status: Up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName          Status    PortType  PortPri   PortNo PortKey   PortState Weight
GigabitEthernet0/0/1          Selected  100M       100      6145    2865      11111100     1
GigabitEthernet0/0/2          Selected  100M       100      6146    2865      11111100     1
GigabitEthernet0/0/3          Unselect  100M       32768    6147    2865      11100000     1

Partner:
--------------------------------------------------------------------------------
PartnerPortName        SysPri    SystemID    PortPri PortNo PortKey   PortState
GigabitEthernet0/0/1          32768  00e0-fca6-7f85  32768     6145   2609      11111100
GigabitEthernet0/0/2          32768  00e0-fca6-7f85  32768     6146   2609      11111100
GigabitEthernet0/0/3          32768  00e0-fca6-7f85  32768     6147   2609      11110000

[SwitchB] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                 WorkingMode: STATIC
Preempt Delay: Disabled         Hash arithmetic: According to SA-XOR-DA
System Priority: 32768          System ID: 00e0-fca6-7f85
Least Active-linknumber: 1      Max Active-linknumber: 8
Operate status: Up              Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName          Status    PortType  PortPri   PortNo  PortKey   PortState Weight
GigabitEthernet0/0/1          Selected  100M       32768      6145    2609      11111100     1
GigabitEthernet0/0/2          Selected  100M       32768      6146    2609      11111100     1
GigabitEthernet0/0/3          Unselect  100M       32768      6147    2609      11100000     1

Partner:
--------------------------------------------------------------------------------
PartnerPortName        SysPri    SystemID     PortPri  PortNo  PortKey   PortState
GigabitEthernet0/0/1          100    00e0-fca8-0417  100       6145     2865      11111100
GigabitEthernet0/0/2          100    00e0-fca8-0417  100       6146     2865      11111100
GigabitEthernet0/0/3          100    00e0-fca8-0417  32768     6147     2865      11110000
```

通过以上显示信息可以看到，SwitchA 的系统优先级为 100，高于 SwitchB 的系统优先级。Eth-Trunk 的成员接口中 GigabitEthernet 0/0/1、GigabitEthernet 0/0/2 成为活动接口，处于“Selected”状态，接口 GigabitEthernet 0/0/3 处于“Unselect”状态，同时实现 M 条链路的负载分担和 N 条链路的冗余备份功能。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 lacp priority 100
#
interface Eth-Trunk1
 mode lacp-static
 max active-linknumber 2
#
interface GigabitEthernet0/0/1
 eth-trunk 1
 lacp priority  100
#
interface GigabitEthernet0/0/2
 eth-trunk 1
 lacp priority  100
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
return
```


版权所有 © 华为技术有限公司

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
interface Eth-Trunk1
 mode lacp-static
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
return
```

3.3 VLAN 配置

VLAN（Virtual Local Area Network）具有隔离广播域、增强保密性、组网灵活和良好的扩展性等特点。

3.3.1 VLAN 概述

从 VLAN 技术的出现、VLAN 的优点到 VLAN 如何工作等，描述了 VLAN 技术是二层网络中重要转发技术之一。

VLAN 概述

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机可实现 LAN（Local Area Network）互联，由于交换机采用交换方式将来自入接口的信息转发到指定出接口上，克服了共享介质上的访问冲突问题，有效的解决了冲突严重问题。但是，当来自入接口的信息无法确定指定的出接口时，此信息会通过交换机上其他所有接口转发（除接收该信息的接口），形成了广播域。

为了解决广播域问题，可将网络分段，把大的广播域划分为若干个小的广播域，从而限制广播报文的影响范围。通常采用路由器在网络层进行网络隔离，但是存在规划复杂、组网方式不灵活，且成本较高。作为替代的 LAN 分段方法，VLAN（Virtual Local Area Network，虚拟局域网）技术被引入，用于解决大型的二层网络所面临的广播风暴、安全等问题。

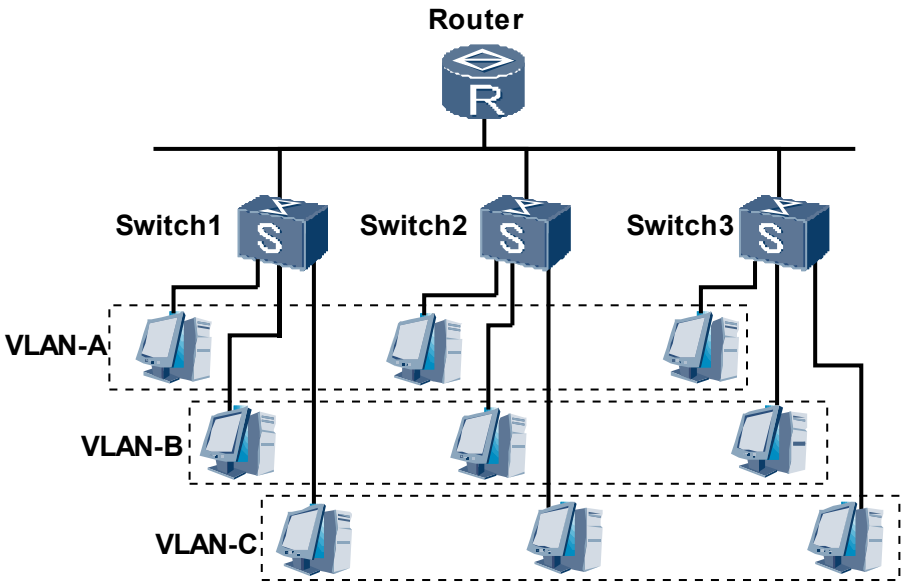
VLAN 定义

VLAN 是将一个物理的 LAN 在逻辑上划分成多个广播域（多个 VLAN）的通信技术。每一个 VLAN 都包含一组拥有相同需求的计算机，与物理上形成的 LAN 具有相同的属性。但是由于 VLAN 是在逻辑划分而不是在物理上划分，所有同一个 VLAN 内的各个工作站无需放置在同一个物理空间。即使两台计算机有着同样的网段，如果它们不属于同一个 VLAN，它们各自的广播流不会互相转发，从而实现了控制流量、减少设备投资、简化网络管理、提高网络的安全性。

图 3-8 是一个典型的 VLAN 应用。3 台交换机放置在不同的地点，比如写字楼的不同楼层。采用 VLAN，可以实现各企业客户共享 LAN 设施，同时保证各自的网络信息安全。

版权所有 © 华为技术有限公司

图 3-8 VLAN 的典型应用示意图



从上述应用可以看出 VLAN 具有以下优势：

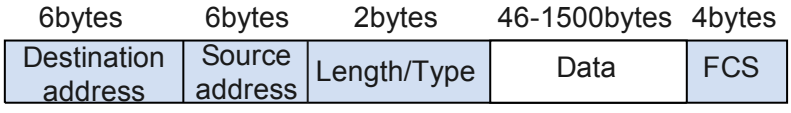
- 限制广播域。广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强局域网的安全性。不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其它 VLAN 内的用户直接通信。
- 提高了网络的健壮性。故障被限制在一个 VLAN 内，本 VLAN 内的故障不会影响其他 VLAN 的正常工作。
- 灵活构建虚拟工作组。用 VLAN 可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

VLAN 相关术语和基本原理

- 802．1Q 简介和 VLAN 帧格式

  传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如图 3-9 所示。

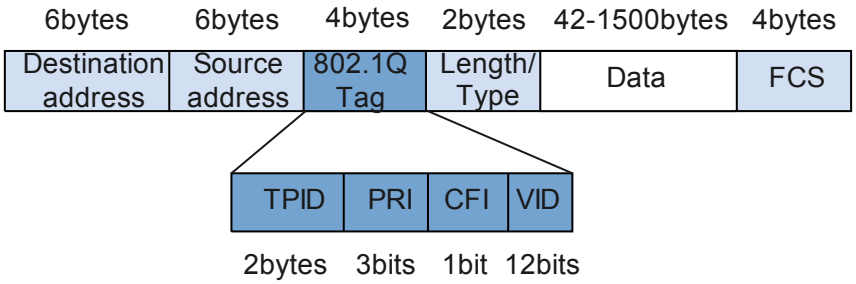
  图 3-9 传统的以太网数据帧格式



  IEEE 802.1Q 是虚拟桥接局域网的正式标准，对 Ethernet 帧格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 字节的 802.1Q Tag，如图 3-10 所示。

版权所有 © 华为技术有限公司

图 3-10 802.1Q 帧格式



- TPID：长度为 2 字节，表示帧类型。取值为 0x8100 时表示 802.1Q Tag 帧。如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃。
- PRI：Priority，长度为 3 比特，表示帧的优先级，取值范围为 0 ～ 7，值越大优先级越高。用于当交换机阻塞时，优先发送优先级高的数据帧。
- CFI：Canonical Format Indicator，长度为 1 比特，表示 MAC 地址是否是经典格式。CFI 为 0 说明是经典格式，CFI 为 1 表示为非经典格式。用于兼容以太网和令牌环网。在以太网中，CFI 的值为 0。
- VID：VLAN ID，长度为 12 比特，表示该帧所属的 VLAN。在 AC6605 中，VLAN ID 取值范围是 0 ～ 4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的有效取值范围是 1 ～ 4094。

  每台支持 802.1Q 协议的交换机发送的数据包都会包含 VLAN ID，以指明自己属于哪一个 VLAN。因此，在一个 VLAN 交换网络中，以太网帧有以下两种形式：
  - 有标记帧（tagged frame）：加入了 4 字节 802.1Q Tag 的帧
  - 无标记帧（untagged frame）：原始的、未加入 4 字节 802.1Q Tag 的帧

- VLAN 的划分方式

  VLAN 划分方式表 3-2 所示。

表 3-2 VLAN 划分方式

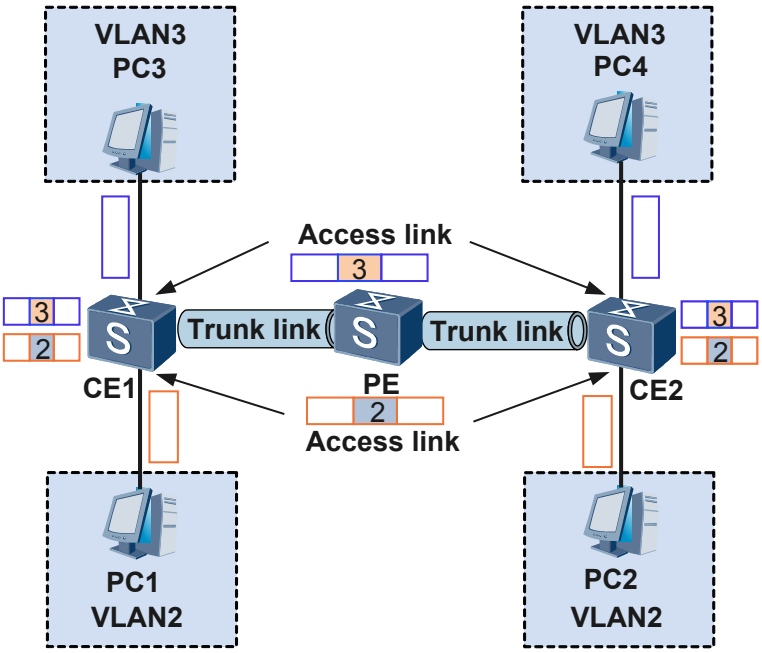
VLAN 划分方式	定义
基于端口划分	根据交换机的端口划分 VLAN。例如交换机的 1 ～ 4 端口划分到 VLAN2，5 ～ 8 端口划分到 VLAN3。 同一 VLAN 可以跨越多个以太网交换机，例如可以将交换机 A 的端口 1 ～ 4 和交换机 B 的端口 3 ～ 6 划分到同一个 VLAN。 交换机维护一张 VLAN 映射表，记录本机端口和 VLAN 的对应关系。
基于 MAC 地址划分	根据每个主机的 MAC 地址划分 VLAN，即根据主机的 MAC 地址配置主机属于哪个 VLAN。 交换机维护一张 VLAN 映射表，记录 MAC 地址和 VLAN 的对应关系。

华为专有和保密信息
版权所有 © 华为技术有限公司

VLAN 划分方式	定义
基于 IP 子网划分	根据主机的 IP 地址决定主机属于哪个 VLAN：同一个 IP 子网的所有主机属于同一个 VLAN。这样，同一个 IP 子网中的用户被划分在一个 VLAN 内。 交换机维护一张 VLAN 映射表，记录 IP 子网和 VLAN 的对应关系。
基于协议划分	根据二层数据帧中协议字段划分 VLAN。通过二层数据帧中的协议字段（目前可支持 IPv4、IPv6、IPX、AppleTalk 协议），可以判断出上层运行的网络协议，从而在相应的 VLAN 中传输。 交换机维护一张 VLAN 映射表，记录协议和 VLAN 的对应关系。
基于策略划分 VLAN	根据每个主机的 MAC 地址和 IP 地址划分 VLAN，即根据主机的 MAC 地址和 IP 地址配置主机属于哪个 VLAN。 交换机维护一张 VLAN 映射表，记录 MAC 地址、IP 地址、端口和 VLAN 的对应关系。

- VLAN 内的链路类型

图 3-11 VLAN 中的链路类型示意图



如图 3-11 所示，VLAN 中有以下两种链路类型：

- 接入链路（Access Link）：用于连接用户主机和交换机的链路。通常情况下，主机并不需要知道自己属于哪个 VLAN，主机硬件通常也不能识别带有 VLAN 标记的帧。因此，主机发送和接收的帧都是 untagged 帧。

版权所有 © 华为技术有限公司

- 干道链路（Trunk Link）：用于交换机间的互连或交换机与路由器之间的连接。干道链路可以承载多个不同 VLAN 数据，数据帧在干道链路传输时，干道链路的两端设备需要能够识别数据帧属于哪个 VLAN，所以在干道链路上传输的帧都是 Tagged 帧。

- 端口属性

  表 3-3 所示端口属性。

表 3-3 端口属性

端口属性	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	对发送报文的处理	用途
Access 端口	接收该报文，并打上缺省 VLAN 的 Tag。	● 当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文。 ● 当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。	去掉 Tag，发送该报文。	端口只能属于 1 个 VLAN，用于交换机与计算机直接连接。
Trunk 端口		● 当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文。 ● 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	● 当 VLAN ID 与缺省 VLAN ID 相同，且是该接口允许通过的 VLAN ID 时，去掉 Tag，发送该报文。 ● 当 VLAN ID 与缺省 VLAN ID 不同，且是该接口允许通过的 VLAN ID 时，保持原有 Tag，发送该报文。	端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般用于网络设备之间连接。
Hybrid 端口			当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。可以通过命令设置发送时是否携带 Tag。	端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于网络设备之间连接，也可以用于连接用户设备。

华为专有和保密信息
版权所有 © 华为技术有限公司

端口属性	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	对发送报文的处理	用途
QinQ 端口	QinQ 端口是使用 QinQ 协议的端口。QinQ 端口可以给帧加上双重 Tag，即在原来 Tag 的基础上，给帧加上一个新的 Tag，从而可以支持多达 4094 x 4094 个 VLAN，满足网络对 VLAN 数量的需求。			

每个 Access、Trunk、Hybrid、QinQ 类型的端口都可以配置一个缺省 VLAN（PVID：Port Default VLAN ID），表示端口所属的 VLAN。

- 对于 Access 类型端口，PVID 的数值表示当前端口所属的 VLAN。
- 对于 Trunk、Hybrid 类型端口，由于 Hybrid 类型端口和 Trunk 类型端口允许多个 VLAN 数据帧通过，也可理解为这两种类型的端口属于多个 VLAN，所以需要配置 PVID。

缺省情况下，端口将被划分到 VLAN1。

- VLAN 中的数据交换原理

  如图 3-11 所示，VLAN2 中的 PC1 发送数据到目的地 PC2，转发过程如下：

  1. CE1 的 Access 类型端口收到 PC1 发送的 untagged 帧，在帧上打上标记 PVID（VLAN 2）形成 tagged 帧。通过 MAC 地址表，找到对应的出接口，将此 tagged 帧发送出去。

     说明

     类似的，假设是基于 MAC 地址划分 VLAN。CE1 的 Acess 类型端口接收到 PC1 发送的 untagged 帧，在 VLAN 映射表中查询帧中源 MAC 地址所对应的 VLAN ID，并构造 tagged 帧。

  2. PE 的 Trunk 类型端口接收到帧后，先检查此帧携带的 VLAN ID 是否与自身已配置的 VLAN ID 一致。如果一致，直接将此数据帧透传到对端。否则，直接丢弃该帧。
  3. CE2 的 Trunk 类型端口接收到帧后，通过 MAC 地址表，找到对应的出接口，即 CE2 与 PC2 相连的 Access 端口。
  4. CE2 的 Access 类型端口收到帧后，确定帧中携带的 VLAN ID 和端口支持的 VLAN ID 一致，将帧中的标记剥掉，形成 untagged 帧，转发给目的主机 PC2。

- VLANIF 接口

  VLANIF 接口是逻辑接口、是三层接口，可以部署在三层交换机上，也可以部署在路由器上。

  三层交换技术是将路由技术与交换技术合二为一的技术，在交换机内部实现了路由，提高了网络的整体性能。三层交换机通过路由表传输第一个数据流后，会产生一个 MAC 地址与 IP 地址的映射表。当同样的数据流再次通过时，将根据此表直接从二层通过而不是通过三层。

  为了保证第一次数据流通过路由表正常转发，路由表中必须有正确的路由表项。因此必须在三层交换机上部署 VLANIF 接口并部署路由协议，实现三层路由可达。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

关键点总结：

- 对于主机来说，它不需要知道 VLAN 的存在。主机发出的是 untagged 报文。
- 交换设备接收到报文后，根据配置规则（如端口信息）判断出报文所属的 VLAN 后，再进行处理。
- 如果报文需要通过另一台交换机转发，则该报文必须通过干道链路传输透传到对端交换设备上。为了保证其它交换设备能够正确处理报文中的 VLAN 信息，在干道链路上传输的报文必须都打上了 VLAN 标记。
- 当交换设备最终确定报文出端口后，将报文发送给主机前，需要将 VLAN 标记从帧中删除，这样主机接收到的报文都是不带 VLAN 标记的以太网帧。

所以，一般情况下，干道链路上传输的都是 tagged 帧，接入链路上传送到的都是 untagged 帧。这样处理的好处是：网络中配置的 VLAN 信息可以被所有交换设备正确处理，而主机不需要了解 VLAN 信息。

3.3.2 AC6605 支持的 VLAN 特性

本章节从 VLAN 的配置逻辑角度介绍 AC6605 支持的 VLAN 特性，理解配置逻辑后，您可以更快速准确地完成配置任务。

通过 VLAN，可灵活构建虚拟工作组隔离广播域、实现 VLAN 内或 VLAN 间用户互相通信。

1. VLAN 最基本的配置是划分 VLAN，VLAN 划分成功后即可实现 VLAN 内的通信。
2. VLAN 内的通信实现后，还需要实现 VLAN 间的通信。

   说明

   上述两个步骤成功配置后，VLAN 的基本功能已经实现。
3. 为了满足特殊场合的应用和扩展功能，VLAN 还支持如下功能：
   - VLAN 聚合（VLAN aggregation）：解决了 IP 地址资源浪费问题，同时可实现不同 VLAN 间通信。
   - MUX VLAN：提供了一种在 VLAN 的接口间进行二层流量隔离的机制，可实现 VLAN 内的用户相互隔离。
   - Voice VLAN：从不同类型的用户流量中选出语音数据流，并自动修改语音数据报文的优先级，以提高语音数据的传输质量。
   - 管理 VLAN：用户可通过管理 VLAN 对应的 VLANIF 接口的 IP 地址 telnet 到管理交换机，从而实现通过远端设备集中管理。

划分 VLAN

划分 VLAN 是 VLAN 的基本配置，VLAN 划分成功后，即可实现同一 VLAN 中的用户可以互相通信。不同的场景采用不同的划分方式，如表 3-4 所示。

版权所有 © 华为技术有限公司

表 3-4 不同 VLAN 划分方式对应的应用场景

VLAN 划分方式	优点	缺点	应用场景
基于端口划分	配置过程简单明了，是最常用的 VLAN 划分方式。	配置不够灵活，当 VLAN 中的成员端口移动时需要重新配置 VLAN。这对于拥有众多移动用户的网络来说，网络管理者将会花费更多的时间进行维护。	适用于规模大、安全需求不高的场景中。
基于 MAC 地址划分	用户在变换物理位置时，不需要重新划分 VLAN。提高了终端用户的安全性和接入的灵活性。	网络管理者需要事先将归属到指定 VLAN 的终端 MAC 地址配置到交换机上。这对拥有大量终端的网络来说，初始配置时，配置工作量较大。	适用于安全和移动性需求较高的场景中。
基于子网划分	基于子网划分 VLAN 和基于协议划分 VLAN 统称为基于网络层划分 VLAN。 基于网络层划分 VLAN，不但大大减少了人工配置 VLAN 的工作量，同时保证了用户自由地增加、移动和修改。	交换机需要解析源 IP 地址并进行相应转换，导致交换机响应速度慢。	适用于对安全需求不高，对移动性和简易管理需求较高的场景中。
基于协议划分		交换机需要分析各种协议的地址格式并进行相应转换，导致交换机响应速度慢。	目前支持 at、ipv4、ipv6、ipx、llc 协议划分 VLAN。
基于策略划分 VLAN	安全性非常高，基于 MAC 地址+IP 地址、MAC 地址+IP 地址+接口成功划分 VLAN 后，禁止用户改变 IP 地址或 MAC 地址。 相较于其他 VLAN 划分方式，基于策略划分 VLAN 是优先级最高的 VLAN 划分方式。	针对每一条策略都需要手工配置。	适用于规模小，且对安全和移动性需求非常高的场景中。

VLAN 间的通信

划分 VLAN 后，同一 VLAN 内的用户可以互相通信，但是属于不同 VLAN 间的用户不能直接互相通信。为了实现 VLAN 间通信，可通过表 3-5 所示的方案实现。

华为专有和保密信息
版权所有 © 华为技术有限公司

表 3-5 实现 VLAN 间通信方案

VLAN 间通信方案	优点	缺点	应用场景
VLANIF 接口	属于不同 VLAN 且位于不同网段的用户，只要在路由可达的前提下，随时可以互相通信。	如果网络中存在多个用户属于不同 VLAN，那么需要为每一个 VLAN 创建对应的 VLANIF 接口，并分配 IP 地址，增加了配置工作量且占用大量 IP 地址资源。	适用于规模小、IP 地址固定的网络，且用户属于不同网段。 如果 VLAN 配置比较多，既要进行二层转发，又要进行三层转发，选择使用 VLANIF 接口。

VLAN 聚合

为了在交换机上实现 VLAN 间通信，需要为每个 VLANIF 接口配置一个 IP 地址，以实现 VLAN 间路由。如果 VLAN 很多，将占用许多 IP 地址资源。VLAN 聚合（VLAN aggregation）可以解决多个 VLAN 占用多个 IP 地址的问题。

VLAN 聚合是将多个 VLAN 集中在一起，形成一个 Super-VLAN。组成 Super-VLAN 的 VLAN 被称作 Sub-VLAN。

可以创建一个 VLANIF 接口，使其对应一个 Super-VLAN，只在该接口上配置 IP 地址，不必为每个 Sub-VLAN 分配 IP 地址，所有 Sub-VLAN 共用 IP 网段，从而解决 IP 地址使用效率的问题。

MUX VLAN

MUX VLAN 提供了一种在 VLAN 的接口间进行二层流量隔离的机制。比如在企业网络中，客户接口可以和服务器接口通讯，但客户接口间不能通讯。

MUX VLAN 分为主 VLAN 和从 VLAN，从 VLAN 又分为互通型从 VLAN 和隔离型从 VLAN。

主 VLAN 与从 VLAN 之间可以相互通信，不同从 VLAN 之间不能互相通信。互通型从 VLAN 接口之间可以互相通信，隔离型从 VLAN 接口之间不能互相通信。

当多台设备配置的 MUX VLAN 一致，且设备间允许 MUX VLAN 通过时，可以实现跨设备的 MUX VLAN 功能，功能实现与单台设备的 MUX VLAN 完全一致。

3.3.3 划分 VLAN

VLAN 划分成功后即可实现同一 VLAN 内的用户互相通信。目前 AC6605 支持以下 VLAN 划分方式，请根据实际情况选择合适的划分方式。

建立配置任务

在进行 VLAN 划分方式配置前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

目前，AC6605 支持以下方式划分 VLAN，用户可根据实际需要选择合适的划分方式。VLAN 的划分如表 3-6 所示。

表 3-6 不同 VLAN 划分方式对应的应用场景

VLAN 划分方式	优点	缺点	应用场景
基于端口划分	配置过程简单明了，是最常用的 VLAN 划分方式。	配置不够灵活，当 VLAN 中的成员端口移动时需要重新配置 VLAN。这对于拥有众多移动用户的网络来说，网络管理者将会花费更多的时间进行维护。	适用于规模大、安全需求不高的场景中。
基于 MAC 地址划分	用户在变换物理位置时，不需要重新划分 VLAN。提高了终端用户的安全性和接入的灵活性。	网络管理者需要事先将归属到指定 VLAN 的终端 MAC 地址配置到交换机上。这对拥有大量终端的网络来说，初始配置时，配置工作量较大。	适用于安全和移动性需求较高的场景中。
基于子网划分	基于子网划分 VLAN 和基于协议划分 VLAN 统称为基于网络层划分 VLAN。 基于网络层划分 VLAN，不但大大减少了人工配置 VLAN 的工作量，同时保证了用户自由地增加、移动和修改。	交换机需要解析源 IP 地址并进行相应转换，导致交换机响应速度慢。	适用于对安全需求不高，对移动性和简易管理需求较高的场景中。
基于协议划分		交换机需要分析各种协议的地址格式并进行相应转换，导致交换机响应速度慢。	目前支持 at、ipv4、ipv6、ipx、llc 协议划分 VLAN。
基于策略划分 VLAN	安全性非常高，基于 MAC 地址+IP 地址、MAC 地址+IP 地址+接口成功划分 VLAN 后，禁止用户改变 IP 地址或 MAC 地址。 相较于其他 VLAN 划分方式，基于策略划分 VLAN 是优先级最高的 VLAN 划分方式。	针对每一条策略都需要手工配置。	适用于规模小，且对安全和移动性需求非常高的场景中。

版权所有 © 华为技术有限公司

说明

如果设备同时支持多种方式划分 VLAN，AC6605 规定的优先使用顺序是:

1. 基于策略划分 VLAN

   基于策略划分 VLAN 的优先级最高，是不最常用的 VLAN 划分方式。

2. 基于 MAC 地址划分 VLAN 和基于子网划分 VLAN

   缺省情况下，优先基于 MAC 地址划分 VLAN。但是可以通过命令改变基于 MAC 地址划分 VLAN 和基于子网划分 VLAN 的优先级，从而决定优先划分 VLAN 的方式。

3. 基于协议划分 VLAN
4. 基于端口划分 VLAN

   基于端口划分 VLAN 的优先级最低，但是是最常用的 VLAN 划分方式。

前置任务

在划分 VLAN 之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在划分 VLAN 之前，需要准备以下数据。

序号	数据
1	VLAN ID、加入到 VLAN 的以太网接口编号、（可选）以太网接口属性
2	VLAN ID、关联 VLAN 的 MAC 地址、、（可选）MAC 地址对应 VLAN 的 802.1p 优先级
3	VLAN ID、（可选）IP 子网索引值、关联 VLAN 的 IP 地址、（可选）IP 地址或网段对应网段的 802.1p 优先级
4	VLAN ID、（可选）协议模板索引值、关联 VLAN 的协议、（可选）协议对应 VLAN 的 802.1p 优先级
5	VLAN ID、与 VLAN 相关联的 MAC 地址和 IP 地址、（可选）MAC 地址和 IP 地址组合策略应用的以太网接口编号

基于端口划分 VLAN

基于端口划分 VLAN 是最简单、最有效的划分方式。

背景信息

基于端口划分的 VLAN 可处理 tagged 报文，也可处理 untagged 报文。

- 当端口收到的报文为 untagged 报文时，在帧上打上标记缺省 VLAN 形成 tagged 帧。通过 MAC 地址表，找到对应出端口。
- 当端口收到的报文为 tagged 报文时：
  - 如果端口允许携带该 VLAN ID 的报文通过，则正常转发。
  - 如果端口不允许携带该 VLAN ID 的报文通过，则丢弃该报文。

基于端口划分 VLAN 的配置思路是：

版权所有 © 华为技术有限公司

1. 创建 VLAN。
2. 配置二层以太网端口属性。

   确定端口类型：Access、Trunk、Hybrid 或 QinQ。
3. 关联端口和 VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 配置二层以太网端口属性。

1. 执行命令 **interface** *interface-type interface-number*，进入需要加入 VLAN 的以太网接口视图。
2. 执行命令 **port link-type** { **access** | **hybrid** | **trunk** | **dot1q-tunnel** }，配置二层以太网端口属性。

   缺省情况下，端口属性是 Hybrid。
   - 如果二层以太网端口直接与终端连接，该端口类型可以是 Access 类型，也可使用缺省类型 Hybrid。
   - 如果二层以太网端口与另一台交换机设备的端口连接，那么对此端口类型没有限制，可使用任意类型的端口。

步骤 5 关联端口和 VLAN

以下步骤，请根据需要任选一种。

- Access 类型端口或 QinQ 类型端口

  执行命令 **port default vlan** *vlan-id*，将端口加入到指定的 VLAN 中。

  如果需要批量将端口加入 VLAN，可在 VLAN 视图下执行命令 **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>向 VLAN 中添加一个或一组端口。
- Trunk 类型端口
  - 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，将端口加入到指定的 VLAN 中。
  - （可选）执行命令 **port trunk pvid vlan** *vlan-id*，配置 Trunk 类型接口的缺省 VLAN。
- Hybrid 类型端口
  - 选择执行其中一个步骤配置 Hybrid 端口加入 VLAN 的方式：
    - 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，将 Hybrid 端口以 Untagged 方式加入 VLAN。

      Untagged 形式是指端口在发送帧时会将帧中的 Tag 剥掉，适用于二层以太网端口直接与终端连接。

版权所有 © 华为技术有限公司

- 执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，将 Hybrid 端口以 Tagged 方式加入 VLAN。

  Tagged 形式是指端口在发送帧时不将帧中的 Tag 剥掉，适用于二层以太网端口与另一台交换机设备的端口连接。
- （可选）执行命令 **port hybrid pvid vlan** *vlan-id*，配置 Hybrid 类型接口的缺省 VLAN ID。

缺省情况下，所有端口加入的 VLAN 和缺省 VLAN 都是 VLAN1。

----结束

基于 MAC 地址划分 VLAN

基于 MAC 地址划分 VLAN 不需要关注终端用户的物理位置，提高了终端用户的安全性和接入的灵活性。

背景信息

基于 MAC 地址划分的 VLAN 只处理 untagged 报文，对于 tagged 报文处理方式和基于端口的 VLAN 一样。

当接口收到的报文为 untagged 报文时，接口会以报文的源 MAC 地址为根据去匹配 MAC-VLAN 表项。

- 如果匹配成功，则按照匹配到的 VLAN ID 和优先级进行转发。
- 如果匹配失败，则按其它匹配原则进行匹配。

基于 MAC 地址划分 VLAN 的配置思路是：

1. 创建 VLAN。
2. 关联 MAC 地址和 VLAN，确定基于哪些 MAC 地址划分 VLAN。
3. 配置二层以太网端口属性。
   a. 确定端口类型：Hybrid
   b. 允许基于 MAC 地址的 VLAN 通过当前端口。
4. （可选）配置 VLAN 划分方式的优先级，确保优先基于 MAC 地址划分 VLAN。

   说明

   缺省情况下，优先基于 MAC 地址划分 VLAN，但是可通过配置改变优先划分的方式。
5. 使能基于 MAC 地址划分 VLAN，完成基于 MAC 地址划分 VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **mac-vlan mac-address** *mac-address* [*mac-address-mask* | *mac-address-mask-length*] [**priority** *priority*]，关联 MAC 地址和 VLAN。

版权所有 © 华为技术有限公司

- 参数 *mac-address* 格式是 H-H-H。其中 H 为 4 位的十六进制数，可以输入 1 ～ 4 位，如 00e0、fc01。当输入不足 4 位时，表示前面的几位为 0，如：输入 e0，等同于 00e0。MAC 地址不可设置为全 F 或全 0。
- 可选参数 *priority* 是 MAC 地址对应 VLAN 的 802.1p 优先级。取值范围是 0 ～ 7，值越大优先级越高。缺省值是 0。配置过程中，可以指定 MAC 地址对应 VLAN 的 802.1p 优先级，用于当交换机阻塞时，优先发送优先级高的数据包。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 配置二层以太网端口属性。

1. 执行命令 **interface** *interface-type interface-number*，进入允许基于 MAC 地址的 VLAN 通过的接口视图。
2. 执行命令 **port link-type hybrid**，配置当前接口类型是 Hybrid。

   缺省情况下，接口类型是 Hybrid。
3. 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，允许基于 MAC 地址划分的 VLAN 通过当前 Hybrid 端口。

步骤 6（可选）执行命令 **vlan precedence mac-vlan**，优先基于 MAC 地址划分 VLAN。

缺省情况下，优先基于 MAC 地址划分 VLAN。

步骤 7 执行命令 **mac-vlan enable**，使能基于 MAC 地址划分 VLAN。

缺省情况下，未使能基于 MAC 地址划分 VLAN 功能。

说明

MAC-VLAN 与 MUX-VLAN 冲突，不允许在同一接口配置。

----结束

基于子网划分 VLAN

基于子网划分 VLAN 和基于协议划分 VLAN 统称为基于网络层划分 VLAN，可减少手工配置 VLAN 的工作量，也可保证用户自由地增加、移动和修改。基于子网划分 VLAN 适用于对安全需求不高，对移动性和简易管理需求较高的场景中。

背景信息

基于 IP 子网的 VLAN 只处理 untagged 报文,对于 tagged 报文处理方式和基于端口的 VLAN 一样。

当设备端口接收到 untagged 报文时，设备根据报文的源 IP 地址或指定网段来确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。

基于 IP 子网划分 VLAN 的配置思路是：

1. 创建 VLAN。
2. 关联 IP 子网和 VLAN，确定基于哪些子网划分 VLAN。
3. 配置二层以太网端口属性。
   a. 确定端口类型：Hybrid
   b. 允许基于 IP 子网的 VLAN 通过当前端口。
4. （可选）配置 VLAN 划分方式的优先级，确保优先选择基于 IP 子网划分 VLAN。

版权所有 © 华为技术有限公司

说明

缺省情况下，优先基于 MAC 地址划分 VLAN，但是可通过配置改变优先划分的方式。

5. 使能基于 IP 子网划分 VLAN，完成基于 IP 子网划分 VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* { *mask* | *mask-length* } [**priority** *priority*]，关联 IP 子网和 VLAN。

- 可选参数 *ip-subnet-index* 是 IP 子网索引值。子网索引可以由用户指定，也可由系统根据 IP 子网划分 VLAN 的顺序自动编号产生。
- 参数 *ip-address* 是基于 IP 子网划分 VLAN 依据的源 IP 地址或网络地址。点分十进制格式。
- 可选参数 *priority* 是 IP 地址或网段对应 VLAN 的 802.1p 优先级。取值范围是 0 ～ 7，值越大优先级越高。缺省值是 0。配置过程中，可以指定 IP 地址或网段对应 VLAN 的 802.1p 优先级，用于当交换机阻塞时，优先发送优先级高的数据包。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 配置二层以太网端口属性。

1. 执行命令 **interface** *interface-type interface-number*，进入需要加入 VLAN 的以太网接口视图。
2. 执行命令 **port link-type hybrid**，配置当前接口类型是 Hybrid。

   缺省情况下，接口类型是 Hybrid。
3. 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，允许基于子网划分的 VLAN 通过当前 Hybrid 端口。

步骤 6（可选）执行命令 **vlan precedence ip-subnet-vlan**，优先基于 IP 子网划分 VLAN。

缺省情况下，优先基于 MAC 地址划分 VLAN。

步骤 7 执行命令 **ip-subnet-vlan enable**，使能基于 IP 子网划分 VLAN 的功能。

缺省情况下，未使能基于 IP 子网划分 VLAN 的功能。

----结束

基于协议划分 VLAN

基于子网划分 VLAN 和基于协议划分 VLAN 统称为基于网络层划分 VLAN，可减少手工配置 VLAN 的工作量，也可保证用户自由地增加、移动和修改。

版权所有 © 华为技术有限公司

背景信息

基于协议的 VLAN 只处理 untagged 报文,对于 tagged 报文处理方式和基于端口的 VLAN 一样。

当设备端口接收到 untagged 帧时，设备先识别帧的协议模板，然后确定报文所属的 VLAN。

- 如果端口配置了属于某些协议 VLAN，且报文的协议模板匹配其中某个协议 VLAN，则给报文打上该协议 VLAN 的 Tag。
- 如果端口配置了属于某些协议 VLAN，但报文的协议模板和所有协议 VLAN 不匹配，则给报文打端口 PVID 的 Tag。

基于 IP 协议划分 VLAN 的配置思路是：

1. 创建 VLAN。
2. 关联协议和 VLAN，确定基于哪些协议划分 VLAN。
3. 配置二层以太网端口属性。
   a. 确定端口类型：Hybrid
   b. 允许基于协议的 VLAN 通过当前端口。
   c. 关联接口和协议 VLAN。
      当有关联的协议进入关联的接口时，系统自动为该协议分配已经划分好的 VLAN ID。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **gigabitethernetii** | **llc** | **raw** | **snap** } | **mode** { **gigabitethernetii-etype** *etype-id1* | **llc dsap** *dsap-id* **ssap** *ssap-id* | **snap-etype** *etype-id2* } }，关联协议和 VLAN，并指定协议模板。

- 可选参数 *protocol-index* 是协议模板索引值。
  协议模板由协议类型+封装格式确定，一个协议 VLAN 可由一个协议模板定义。
- 配置源和目的服务接入点时，需要注意以下几点：
  - *dsap-id* 和 *ssap-id* 不能同时设置成 0xaa。
  - *dsap-id* 和 *ssap-id* 不能同时设置成 0xe0，0xe0 对应的是 IPX 报文的 llc 封装格式。
  - *dsap-id* 和 *ssap-id* 也不能同时设成 0xff，0xff 对应的是 IPX 报文的 raw 封装格式。

步骤 4 配置二层以太网端口属性。

1. 执行命令 **interface** *interface-type interface-number*，进入允许基于协议的 VLAN 通过的接口视图。
2. 执行命令 **port link-type hybrid**，配置当前接口类型是 Hybrid。
   缺省情况下，接口类型是 Hybrid。

版权所有 © 华为技术有限公司

3. 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，允许基于协议划分的 VLAN 通过当前 Hybrid 端口。
4. 执行命令 **protocol-vlan vlan** *vlan-id* { **all** | *protocol-index1* [**to** *protocol-index2*] } [**priority** *priority*]，关联接口和协议 VLAN。
   - 参数 *vlan-id* 必须是基于协议划分的 VLAN ID。
   - 可选参数 *priority* 是协议对应 VLAN 的 802.1p 优先级。取值范围是 0 ～ 7，值越大优先级越高。缺省值是 0。配置过程中，可以指定协议对应 VLAN 的 802.1p 优先级，用于当交换机阻塞时，优先发送优先级高的数据包。

----结束

基于策略划分 VLAN

基于策略划分 VLAN 也可称为 Policy VLAN，可实现用户终端的即插即用功能，同时可为终端用户提供安全的数据隔离。

背景信息

基于策略划分 VLAN 分为：包括基于 MAC 地址+IP 地址组合策略和基于 MAC 地址+IP 地址+接口组合策略。

基于策略划分 VLAN 是指在交换机上指定终端的 MAC 地址、IP 地址或接口，并与 VLAN 关联。只有符合条件的终端才能加入指定 VLAN。符合策略的终端加入指定 VLAN 后，严禁修改 IP 地址或 MAC 地址，否则会导致终端从指定 VLAN 中退出。

基于策略的 VLAN 只处理 untagged 报文,对于 tagged 报文处理方式和基于端口的 VLAN 一样。

当设备端口接收到 untagged 报文时，设备根据用户报文中的 MAC 地址和 IP 地址与配置的 MAC 地址和 IP 地址组合策略来确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。

基于策略划分 VLAN 的配置思路是：

1. 创建 VLAN。
2. 关联 MAC 地址和 IP 地址组合策略和 VLAN，确定基于哪些组合策略划分 VLAN。
3. 配置二层以太网端口属性。
   a. 确定端口类型：Hybrid
   b. 允许基于 MAC 地址和 IP 地址组合策略的 VLAN 通过当前端口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **policy-vlan mac-address** *mac-address* **ip** *ip-address* [**interface** *interface-type interface-number*] [**priority** *priority*]，配置 Policy VLAN。

版权所有 © 华为技术有限公司

如果不指定参数 **interface** *interface-type interface-number*，那么 MAC 地址和 IP 地址组合策略将应用到指定 VLAN 中所有的接口上。否则，MAC 地址和 IP 地址组合策略只应用到指定 VLAN中指定的接口上。

如果要删除被设置为 Policy VLAN 的 VLAN，需要先执行命令 **undo policy-vlan** 删除 Policy VLAN 后，才能够删除该 VLAN。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 配置二层以太网端口属性。

1. 执行命令 **interface** *interface-type interface-number*，进入允许基于 MAC 地址和 IP 地址组合策略的 VLAN 通过的接口视图。
2. 执行命令 **port link-type hybrid**，配置当前接口类型是 Hybrid。

   缺省情况下，接口类型是 Hybrid。
3. 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，允许基于 MAC 地址和 IP 地址组合策略划分的 VLAN 通过当前 Hybrid 端口。

----结束

检查配置结果

VLAN 划分方式配置成功后，您可以查看到基于不同方式划分 VLAN 的表项信息。如：哪些 VLAN 基于端口划分，哪些 VLAN 基于 MAC 地址划分等信息。

前提条件

已经完成 VLAN 划分方式的所有配置。

操作步骤

- 执行命令 **display vlan** [*vlan-id* [**verbose**]]，查看所有 VLAN 或指定 VLAN 的显示信息。
- 执行命令 **display mac-vlan** { **mac-address** { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] } | **vlan** *vlan-id* }，查看基于 MAC 地址划分 VLAN 的相关信息。
- 执行命令 **display ip-subnet-vlan vlan** { **all** | *vlan-id1* [**to** *vlan-id2*] }，查看基于 IP 子网划分 VLAN 的相关信息。
- 执行命令 **display protocol-vlan vlan** { **all** | *vlan-id1* [**to** *vlan-id2*] }，查看基于协议划分 VLAN 的相关信息。
- 执行命令 **display protocol-vlan interface** { **all** | *interface-type interface-number* }，查看接口关联基于协议划分 VLAN 的配置信息。
- 执行命令 **display policy-vlan** { **all** | **vlan** *vlan-id* }命令，查看策略 VLAN 的配置信息。

----结束

3.3.4 创建 VLANIF 接口

VLANIF 接口是三层逻辑接口，在 AC6605 上创建 VLANIF 接口后，可部署三层特性。

版权所有 © 华为技术有限公司

建立配置任务

在进行 VLANIF 接口配置前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

三层交换技术是将路由技术与交换技术合二为一的技术，在交换机内部实现了路由，提高了网络的整体性能。三层交换机通过路由表传输第一个数据流后，会产生一个 MAC 地址与 IP 地址的映射表。当同样的数据流再次通过时，将根据此表直接从二层通过而不是通过三层。

为了保证第一次数据流通过路由表正常转发，路由表中必须有正确的路由表项。因此必须在三层交换机上部署 VLANIF 接口并部署路由协议，实现三层路由可达。

前置任务

在创建 VLANIF 接口之前，需要完成以下任务：

- 已经成功创建 VLAN

数据准备

在创建 VLANIF 接口之前，需准备以下数据。

序号	数据
1	VLAN ID
2	VLANIF 接口的 IP 地址
3	（可选）延迟 VLANIF 接口状态变为 Down 的时间
4	（可选）VLANIF 接口的 MTU

创建 VLANIF 接口

在二层设备上部署三层特性，首要步骤是创建 VLANIF 接口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口，并进入 VLANIF 接口视图。

VLANIF 接口的编号必须对应一个已经创建的 VLAN ID。

说明

只有当 VLAN 内存在状态为 Up 的物理端口时，该 VLAN 对应的 VLANIF 接口状态才会 Up。

----结束

版权所有 © 华为技术有限公司

配置 VLANIF 接口的 IP 地址

VLANIF 接口是三层逻辑接口，只有配置了 IP 地址，才能实现网络层的设备互相通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，，进入 VLANIF 接口视图。

VLANIF 接口的编号必须对应一个已创建的 VLAN。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 VLANIF 接口的 IP 地址，实现三层互通。

----结束

（可选）延迟 VLANIF 接口状态变为 Down 的时间

延迟 VLANIF 接口状态变为 Down 的时间可避免由于 VLANIF 接口状态变化而引起的网络震荡，此功能也可称为 VLAN Damping 功能。

背景信息

当 VLAN 中接口状态变为 Down 而引起 VLAN 状态变为 Down 时，VLAN 会向 VLANIF 接口上报 Down 事件，从而引起 VLANIF 接口状态变化。

为避免由于 VLANIF 接口状态变化引起的网络震荡，可以在 VLANIF 接口上启动 VLAN Damping 功能。当 VLAN 中最后一个处于 Up 状态的成员端口变为 Down 后，启动 VLAN Damping 功能的设备会抑制设定的时间后再上报给 VLANIF 接口。如果在抑制的时间内 VLAN 中有成员口状态变为 Up，则 VLANIF 接口状态保持 Up 不变。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，，进入 VLANIF 接口视图。

VLANIF 接口的编号必须对应一个已创建的 VLAN。

步骤 3 执行命令 **damping time** *delay-time*，配置 VLAN Damping 功能的抑制时间。

参数 *delay-time* 取值范围是 0 ～ 20，单位是秒。缺省情况下，抑制时间是 0 秒，表示去使能 VLAN Damping 功能。

----结束

版权所有 © 华为技术有限公司

（可选）配置 VLANIF 接口的 MTU

背景信息

说明

- 使用 **mtu** 命令改变接口最大传输单元 MTU 后，需要重启接口以保证配置的 MTU 生效。可以先执行 **shutdown** 命令将接口关闭，再执行 **undo shutdown** 命令将接口重启；也可以在接口视图下执行 **restart** 命令重启接口。
- 如果使用 **mtu** 命令改变接口 MTU 的值，请同时修改与本设备相连的其他设备的 MTU 值，确保两端设备的 MTU 值匹配。否则，可能导致业务中断。
- VLANIF 接口下 **mtu** 的取值要小于该 VLAN 下的物理端口 **jumboframe** 的取值，以保证三层功能正常使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **mtu** *mtu*，配置 VLANIF 接口的 MTU。

最大传输单元 MTU（Maximum Transmission Unit）单位为字节，VLANIF 接口 MTU 的取值范围为 128 ～ 9216。缺省值为 1500。

说明

由于 QoS（Quality of Service）队列长度有限，如果 MTU 太小而报文尺寸较大，可能会造成分片过多，报文被 QoS 队列丢弃。为避免这种情况，可适当增大 QoS 队列的长度。

----结束

检查配置结果

VLANIF 接口实现三层互通配置成功后，您可以查看到指定 VLANIF 接口的 IP 地址配置是否正确、VLANIF 接口的状态等信息。

前提条件

已经完成 VLANIF 接口实现三层互通的所有配置。

操作步骤

- 执行命令 **display interface vlanif** [*vlan-id*]，查看 VLANIF 接口的使能状态、协议使能状态、接口描述信息和接口 IP 地址等。

----结束

3.3.5 配置 VLAN 间通信

VLAN 间通信配置成功后可实现不同 VLAN 内的用户互相通信。目前 AC6605 支持以下解决方案，请根据实际组网环境选择合适的方案部署。

建立配置任务

在进行 VLAN 间通信配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

目前，有表 3-7 所示的方案支持 VLAN 间通信，用户可根据实际组网环境选择合适的方案部署。

表 3-7 实现 VLAN 间通信方案

VLAN 间通信方案	优点	缺点	应用场景
VLANIF 接口	属于不同 VLAN 且位于不同网段的用户，只要在路由可达的前提下，随时可以互相通信。	如果网络中存在多个用户属于不同 VLAN，那么需要为每一个 VLAN 创建对应的 VLANIF 接口，并分配 IP 地址，增加了配置工作量且占用大量 IP 地址资源。	适用于规模小、IP 地址固定的网络，且用户属于不同网段。 如果 VLAN 配置比较多，既要进行二层转发，又要进行三层转发，选择使用 VLANIF 接口。

前置任务

在配置 VLAN 间通信之前，需完成以下任务：

- VLAN 已经创建

数据准备

在配置 VLAN 间通信之前，需要准备以下数据。

序号	数据
1	VLAN ID、VLANIF 接口编号、VLANIF 接口的 IP 地址及掩码

配置 VLANIF 接口支持 VLAN 间的通信

通过 VLANIF 接口实现 VLAN 间通信可节约成本，也可实现快速转发。

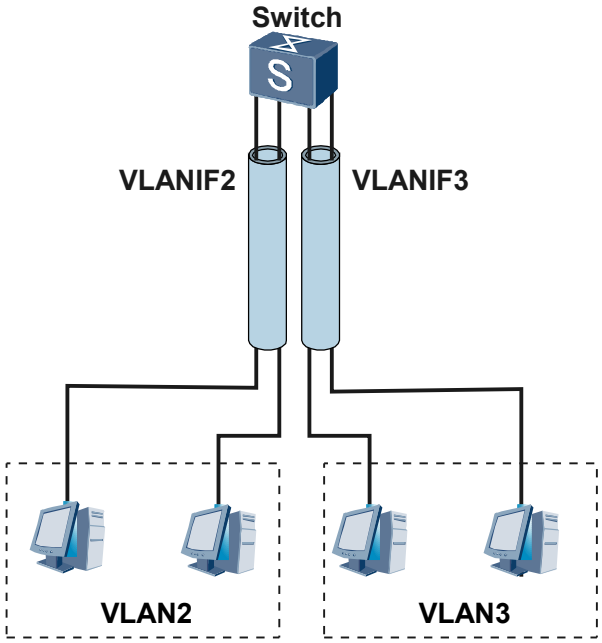
背景信息

VLANIF 是逻辑接口、是三层口，配置 IP 地址后可实现网络层互通。

通过 VLANIF 接口实现 VLAN 间通信需要为每个 VLAN 创建对应的逻辑接口 VLANIF 接口，并为每个 VLANIF 接口配置 IP 地址实现三层互通。

版权所有 © 华为技术有限公司

图 3-12 通过 VLANIF 接口实现 VLAN 间通信组网图



说明

为了成功实现 VLAN 间互通，VLAN 内主机的缺省网关必须是对应 VLANIF 接口的 IP 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口，并进入 VLANIF 接口视图。

VLANIF 接口的编号必须对应一个已经创建的 VLAN ID。

说明

只有当 VLAN 内存在状态为 Up 的物理端口时，该 VLAN 对应的 VLANIF 接口状态才会 Up。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 VLANIF 接口的 IP 地址。

不同的 VLANIF 接口所配置的 IP 地址应该在不同的网段。

----结束

检查配置结果

VLAN 间通信配置成功后，您可以查看到不同 VLAN 中的用户可以互相通信，及用户所属的 VLAN 等信息。

前提条件

已经完成 VLAN 间通信的所有配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **ping** [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-f** | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-n** | **-p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-system-time** | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*，查看不同 VLAN 间是否能够成功互相通信。

  若 Ping 不通，可执行以下命令进行故障定位。

  - 执行命令 **display vlan** [*vlan-id* [**verbose**]]，查看 VLAN 信息。
  - 执行命令 **display interface vlanif** [*vlan-id*]，查看 VLANIF 接口信息。

    执行此命令的前提是必须已经成功配置 VLANIF 接口。

----结束

3.3.6 配置 VLAN 聚合节约 IP 地址

VLAN 聚合解决了 IP 地址资源浪费问题，同时可实现不同 VLAN 间通信。

建立配置任务

在进行 VLAN 聚合配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

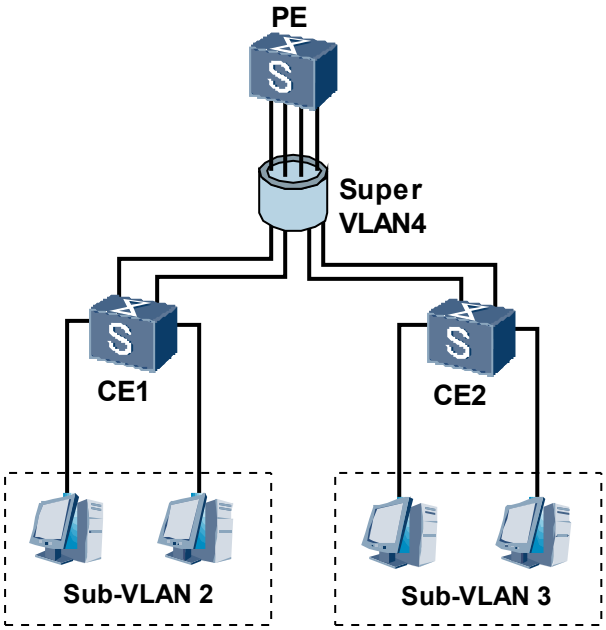
随着网络的发展，网络地址资源日趋紧张，为了节省 IP 地址，VLAN 聚合（VLAN aggregation）的概念被提出来。

VLAN 聚合的原理是一个 Super-VLAN 和多个 Sub-VLAN 关联，Super-VLAN 内不能加入物理端口，但可以创建对应的 VLANIF 接口，VLANIF 接口下可以配置 IP 地址。Sub-VLAN 可以加入物理端口，但不能创建对应的 VLANIF 接口，所有 Sub-VLAN 内的端口共用 Super-VLAN 的 VLANIF 接口 IP 地址，这既减少了一部分子网号、子网缺省网关地址和子网定向广播地址的消耗，又实现了不同广播域使用同一子网网段地址，消除了子网差异，增加了编址的灵活性，减少了闲置地址浪费。从而在保证了各个 Sub-VLAN 作为一个独立广播域实现了广播隔离的同时，将从前使用普通 VLAN 浪费掉的 IP 地址节省下来。

如图 3-13 所示是典型的 VLAN 聚合组网。

版权所有 © 华为技术有限公司

图 3-13 典型 VLAN 聚合组网图



前置任务

在配置 VLAN 聚合之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置 VLAN 聚合之前，需准备以下数据。

序号	数据
1	Sub-VLAN 的 VLAN ID 及其包含的端口编号
2	Super-VLAN 的 VLAN ID
3	VLANIF 接口的 IP 地址和掩码

创建 Sub-VLAN

Sub-VLAN 用于隔离广播域。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 3 执行命令 **port link-type access**，配置 Access 类型接口。

步骤 4 执行命令 **quit**，退出接口视图。

步骤 5 执行命令 **vlan** *vlan-id*，创建 Sub-VLAN，并进入 Sub-VLAN 视图。

步骤 6 执行命令 **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>，将端口加入 VLAN。

----结束

创建 Super-VLAN

Super-VLAN 由多个 Sub-VLAN 组成，不能加入物理端口，但可以创建 VLANIF 接口并配置 IP 地址。

背景信息

说明

在配置 Super-VLAN 之前必须已完成配置 Sub-VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

本配置步骤中的 *vlan-id* 与 Sub-VLAN 中的 *vlan-id* 必须使用不同的 VLAN ID。

步骤 3 执行命令 **aggregate-vlan**，创建 Super-VLAN。

Super-VLAN 中不能包含任何物理端口。

VLAN1 不能配置为 Super-VLAN。

步骤 4 执行命令 **access-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，将 Sub-VLAN 加入 Super-VLAN。

如果要将多个 Sub-VLAN 批量加入到 Super-VLAN 中，必须保证这些 Sub-VLAN 没有创建对应的 VLANIF 接口。

----结束

配置 Super-VLAN 对应的 VLANIF 接口的 IP 地址

Super-VLAN 对应的 VLANIF 接口的 IP 地址应包含各 Sub-VLAN 用户所在的子网段，所有 Sub-VLAN 共用 Super-VLAN 的 VLANIF 接口 IP 地址，从而解决 IP 地址资源问题。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，创建 Super-VLAN 对应的 VLANIF 接口，并进入 VLANIF 接口视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 VLANIF 接口的 IP 地址。

----结束

（可选）使能 Super-VLAN 对应的 VLANIF 接口的 ARP Proxy

不同 Sub-VLAN 之间相互二层隔离，如果需要三层互通，必须在 Super-VLAN 对应的 VLANIF 接口上使能 ARP Proxy。

背景信息

VLAN 聚合在实现不同 Sub-VLAN 间共用一个子网网段地址的同时也带来了 Sub-VLAN 间的三层转发问题。

普通 VLAN 实现方式中，VLAN 间的主机可以通过各自不同的网关进行三层转发达到互通的目的。但是 VLAN 聚合方式下，同一个 Super-VLAN 内的主机使用的是同一个网段的地址和共用同一个网关地址。即使是属于不同的 Sub-VLAN 的主机，由于它们同属一个子网，彼此通信时只会做二层转发，而不会通过网关进行三层转发。而实际上不同的 Sub-VLAN 的主机在二层是相互隔离的，这就造成了 Sub-VLAN 间无法通信。

为了实现 Sub-VLAN 间相互通信及 Sub-VLAN 与其他网络的互通，需要利用 ARP Proxy 功能。在创建好 Super-VLAN 和对应的 VLANIF 接口后，用户需要开启设备的 ARP Proxy 功能，Super-VLAN 利用 ARP Proxy 可以进行 ARP 请求和响应报文的转发与处理，从而实现 Sub-VLAN 之间的三层互通。

说明

Super-VLAN 对应的 VLANIF 接口配置 IP 地址后 ARP Proxy 才能生效。

当以太网存在大量 VLAN 时，不同的 VLAN 间需要通信，VLAN 聚合还可以简化配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 Super-VLAN 对应的 VLANIF 接口视图。

步骤 3 执行命令 **arp-proxy inter-sub-vlan-proxy enable**，使能 Sub-VLAN 间的 ARP Proxy 功能。

----结束

检查配置结果

VLAN 聚合配置成功后，您可以查看 VLAN 类型、VLANIF 接口物理状态、链路协议状态、IP 地址和掩码等内容。

前提条件

已经完成 VLAN 聚合功能的所有配置。

操作步骤

- 执行 **display vlan** [*vlan-id* [**verbose**]]命令，查看 VLAN 信息。

版权所有 © 华为技术有限公司

- 执行 **display interface vlanif** [*vlan-id*]命令，查看 VLANIF 接口信息

----结束

3.3.7 配置 MUX VLAN 实现二层流量隔离

MUX VLAN 可实现 VLAN 间通信，也可实现 VLAN 内的用户相互隔离。

建立配置任务

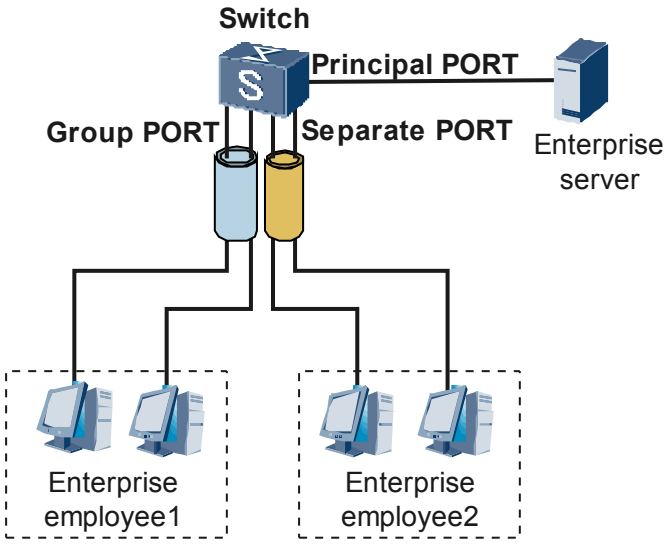
在进行 MUX VLAN 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在企业网络中，企业所有员工都可以访问企业的服务器。但对于企业来说，希望企业内部部分员工之间可以互相交流，而部分员工之间是隔离的，不能够互相访问。

为了解决此问题，可在连接终端的交换机上部署 MUX VLAN 特性。MUX VLAN 不但能够实现企业需求，同时也节约了 VLAN ID，便于网络管理者维护。

图 3-14 MUX VLAN 组网图



根据 MUX VLAN 特性，用 Principal port 连接企业服务器，Separate port 连接不需要互访的员工，Group port 连接需要互访的员工，如图 3-14 所示。对于不同的端口类型，MUX VLAN 划分如表 3-8 所示。

版权所有 © 华为技术有限公司

表 3-8 MUX VALN 划分表

MUX VLAN	VLAN 类型	所属端口	通信权限
Principal VLAN（主 VLAN）	-	Principal port	Principal port 可以和 MUX VLAN 内的所有端口进行通信。
Subordinate VLAN（从 VLAN）	Separate VLAN（隔离型从 VLAN）	Separate port	Separate port 只能和 Principal port 进行通信，和其他类型的端口实现完全隔离。 每个 Separate VLAN 必须绑定一个 Principal VLAN。
	Group VLAN（互通型从 VLAN）	Group port	Group port 可以和 Principal port 进行通信，在同一组内的端口也可互相通信，但不能和其他组端口或 Separate port 通信。 每个 Group VLAN 必须绑定一个 Principal VLAN。

前置任务

在配置 MUX VLAN 之前，需要完成以下任务：

- VLAN 已经成功创建

数据准备

在配置 MUX VLAN 之前，需准备以下数据。

序号	数据
1	Principal VLAN 的 VLAN ID 及其包含的端口编号
2	Group VLAN 的 VLAN ID 及其包含的端口编号
3	Separate VLAN 的 VLAN ID 及其包含的端口编号

配置 MUX VLAN 中的 Principal VLAN

加入 Principal VLAN 中的端口，可以与 MUX VLAN 内的所有端口进行通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

华为专有和保密信息
版权所有 © 华为技术有限公司

VLAN ID 的取值范围是 1 ～ 4094。如果需要批量创建 VLAN，可以先使用命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>批量创建，再使用命令 **vlan** *vlan-id* 进入相应的 VLAN 视图。

步骤 3 执行命令 **mux-vlan**，配置该 VLAN 为 MUX VLAN，即，Principal VLAN。

指定 VLAN ID 已经用于 Principal VLAN，那么该 VLAN 不能再用于 VLANIF 接口、super-VLAN、sub-VLAN。

----结束

配置 Subordinate VLAN 中的 Group VLAN

与 Group port 关联的 VLAN 称为 Group VLAN。Group VLAN 可实现同一组 VLAN 内的端口相互通信。

背景信息

同一 MUX VLAN 中 Group VLAN 和 Separate VLAN 的编号不能重叠。

请在需要实现 Group VLAN 的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入已经成功创建的 Principal VLAN 视图。

步骤 3 执行命令 **subordinate group** *vlan-id1* [**to** *vlan-id2*]，配置 Subordinate VLAN 中的 Group VLAN。

vlan-id1 和 *vlan-id2* 表示 VLAN 的编号。整数形式，取值范围是 1 ～ 4094。*vlan-id2* 的取值必须大于等于 *vlan-id1* 的取值。

如果该 VLAN ID 已经用于 Group VLAN，那么该 VLAN 不能再用于 VLANIF 接口、super-VLAN、sub-VLAN。

----结束

配置 Subordinate VLAN 中的 Separate VLAN

与 Separate port 关联的 VLAN 称为 Separate VLAN。Separate VLAN 可隔离端口间的流量，从而阻断端口间相互通信。

背景信息

同一 MUX VLAN 中 Group VLAN 和 Separate VLAN 的编号不能重叠。

请在需要实现 Separate VLAN 的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入已经成功创建的 Principal VLAN 视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **subordinate separate** *vlan-id*，配置 Subordinate VLAN 中的 Separate VLAN。

同一 MUX VLAN 中 Group VLAN 和 Separate VLAN 的编号不能重叠。

----结束

使能端口 MUX VLAN 功能

只有使能端口 MUX VLAN 功能后，才能实现 Principal VLAN 与 Subordinate VLAN 之间通信、Group VLAN 内的端口可以相互通信及 Separate VLAN 端口间不能相互通信的目的。

背景信息

使能端口 MUX VLAN 功能前：

- 端口只能允许一个普通 VLAN 通过。如果端口允许多个普通 VLAN 通过，那么端口将无法成功使能 MUX VLAN 功能。
- 端口必须先加入 Principal VLAN 或 Subordinate VLAN。

请在需要使能端口 MUX VLAN 功能的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入连接用户的以太网接口视图。

步骤 3 执行命令 **port mux-vlan enable**，使能端口的 MUX VLAN 功能。

使能 MUX VLAN 功能前，端口必须先加入 MUX VLAN，并且端口只能加入一个 VLAN。

端口使能 MUX VLAN 功能后，该端口不可以再用于 VLAN Mapping、VLAN Stacking 配置。

说明

- 禁止接口 MAC 地址学习功能或限制接口 MAC 地址学习数量会影响 MUX VLAN 功能的正常使用。
- 不能在同一接口上配置 MUX VLAN 和接口安全功能。
- 不能在同一接口上配置 MUX VLAN 和 MAC 认证功能。
- 不能在同一接口上配置 MUX VLAN 和 802.1x 认证功能。

----结束

检查配置结果

MUX VLAN 配置成功后，您可以查看到 Principal VLAN ID、Subordinate VLAN ID 和 VLAN 的类型等内容。

前提条件

已经完成 MUX VLAN 的所有配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **display mux-vlan**，查看所有 MUX VLAN 的相关信息。

----结束

3.3.8 配置 Voice VLAN 传输语音流量

Voice VLAN 是为用户的语音数据流而专门划分的 VLAN。

建立配置任务

在进行 Voice VLAN 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

网络中经常同时存在语音数据和非语音数据两种流量。语音数据在传输时需要具有比其他业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。提高语音数据传输优先级常用的处理方法是使用 ACL（Access Control List）对语音数据进行区分，并使用 QoS（Quality of Service）保证传输质量。

随着科技的发展，IP 电话应用越来越广泛。为了保证语音数据优先传输，可采用 ACL 区分语音数据和业务数据，并使用 Qos 保证传输质量。但是 ACL 规则需要针对每一个终端用户进行部署，这增大了网络管理者的工作量，且不利于维护。

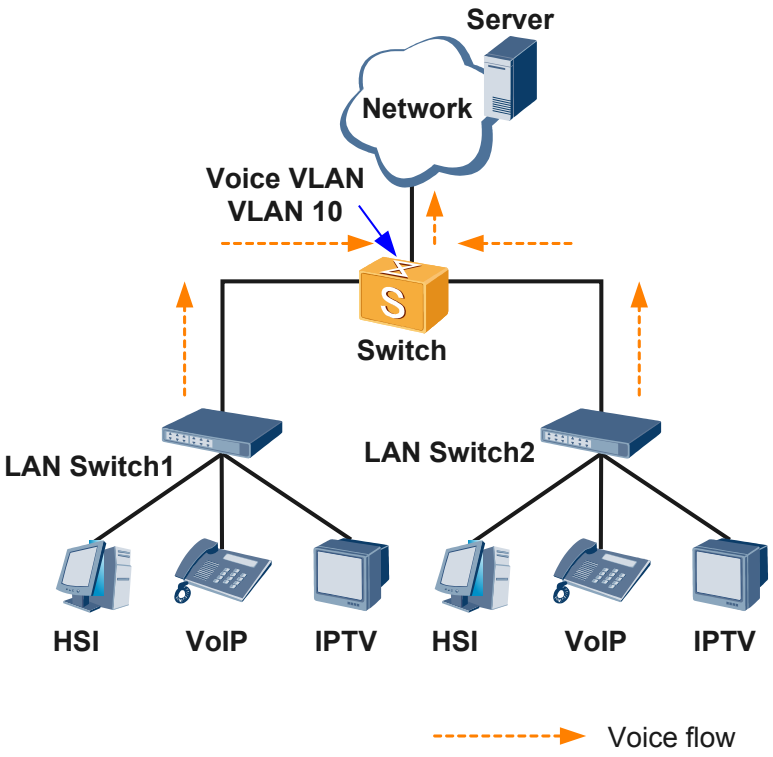
为了解决上述问题，Voice VLAN 应运而生。

Voice VLAN 通过识别收到的报文中的源 MAC 地址，判断是否是语音数据，并自动将收到语音数据的端口加入 Voice VLAN 中，同时自动部署优先级规则，保证语音数据的优先级和通话质量，从而简化了用户配置，且便于用户管理语音数据。

如图 3-15 所示某用户的三种业务 HSI（High Speed Internet）、VoIP（Voice over IP）和 IPTV（Internet Protocol Television）接入交换设备 Switch。为了对语音数据流进行针对性的 QoS 配置，提高语音数据流量的传输优先级，保证用户间的通话质量，可在 Switch 上部署 Voice VLAN 功能。

版权所有 © 华为技术有限公司

图 3-15 Voice VLAN 组网图



前置任务

在配置 Voice VLAN 之前，需要完成以下任务：

- VLAN 已经成功创建

数据准备

在配置 Voice VLAN 之前，需准备以下数据。

序号	数据
1	使能 Voice VLAN 功能的接口类型和编号、Voice VLAN ID
2	Voice VLAN 的 OUI 地址和掩码
3	（可选）Voice VLAN 的老化时间
4	（可选）Voice VLAN 的 8021p 和 DSCP 优先级
5	（可选）接口加入 Voice VLAN 的模式
6	（可选）Voice VLAN 的工作模式

华为专有和保密信息
版权所有 © 华为技术有限公司

使能 Voice VLAN 功能

当设备使能 Voice VLAN 功能后，设备会通过报文中的源 MAC 地址自动识别出语音数据流，并自动修改语音数据报文的优先级，以提高语音数据的传输质量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **voice-vlan** *vlan-id* **enable**，指定 VLAN 是 Voice VLAN，同时使能接口的 Voice VLAN 功能。

缺省情况下，Voice VLAN 功能处于去使能状态。

说明

- VLAN 1 不能指定为 Voice VLAN。
- 为保证各种功能的正常使用，请为 Voice VLAN、接口的缺省 VLAN 分配不同的 VLAN ID。
- 同一时刻，一个接口只能有一个 VLAN 被设置为 Voice VLAN。
- 当接口的 Voice VLAN 工作在自动模式时，需要使用 **port link-type** 命令将接口配置为 Trunk 或 Hybrid 类型。
- 如果要删除被设置为 Voice VLAN 的 VLAN，需要先使用 **undo voice-vlan enable** 命令去使能 Voice VLAN 功能后，才能够删除该 VLAN。
- 使能 Voice VLAN 功能的接口不允许再配置 VLAN Mapping、VLAN Stacking 和应用流策略。

----结束

配置 Voice VLAN 的 OUI

使能 Voice VLAN 功能的设备根据进入接口的数据流中的源 MAC 地址判断该数据流是否为语音数据流，如果源 MAC 地址与系统设置的 OUI（Organizationally Unique Identifier）地址相匹配，则认为该数据流是语音数据流。

背景信息

OUI 是 MAC 地址的前 24 位（二进制），是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符。

OUI 地址表示一个 MAC 地址段，将 48 位的 MAC 地址和掩码的对应位作与运算可以确定 OUI 地址。例如，MAC 地址为 1－1－1，掩码为 FFFF-FF00－0000，那么将 MAC 地址与其相应掩码位执行与运算的结果就是 OUI 地址 0001－0000－0000。只要接入设备的 MAC 地址前 24 位和 OUI 匹配，那么使能 Voice VLAN 功能的接口将认为此数据流是语音数据流，接入的设备是语音设备。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **voice-vlan mac-address** *mac-address* **mask** *oui-mask* [**description** *text*]，配置 OUI。

- *mac-address* 不可设置为全零、组播地址或广播地址。

版权所有 © 华为技术有限公司

- 系统只支持配置 16 个 OUI，即系统只支持配置 16 条本命令。当配置 OUI 的命令数量大于 16 时，将不能再增加配置。
- 当执行命令 **undo voice-vlan mac-address** 删除某一特定 OUI 时，*mac-address* 取值应为配置时 MAC 地址和 MASK 掩码进行逻辑与后的结果。

说明

当源 MAC 地址为 OUI 地址时，将根据**（可选）配置 Voice VLAN 的 802.1p 和 DSCP 优先级**中的配置修改报文中的 8021p 和 DSCP 优先级，以提高语音数据的传输质量。

----结束

（可选）配置 Voice VLAN 的老化时间

在自动模式下，使能 Voice VLAN 的设备通过学习语音设备发出的语音报文中的源 MAC 地址，将连接语音设备的接口自动加入到 Voice VLAN 中，并通过老化机制维护 Voice VLAN 内的接口数量。

背景信息

Voice VLAN 的老化时间只对接口以自动模式加入 Voice VLAN 的方式有效，对手动模式加入 Voice VLAN 的方式无效。

老化时间超时后，使能了 Voice VLAN 功能的接口未收到任何来自语音设备的语音报文时，连接语音设备的接口将自动从 Voice VLAN 中删除。如果使能了 Voice VLAN 功能的接口再次收到该语音设备发出的语音报文，连接语音设备的接口将再次自动加入 Voice VLAN，且老化时间重新开始计时。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **voice-vlan aging-time** *minutes*，配置 Voice VLAN 的老化时间。

Voice VLAN 的老化时间取值范围是 5 ～ 43200，单位是分钟。缺省值是 1440 分钟。

----结束

（可选）配置 Voice VLAN 的 802.1p 和 DSCP 优先级

通过配置 Voice VLAN 的 802.1p 和 DSCP 优先级，提高用户部署语音业务的灵活性。

背景信息

Voice-VLAN 特性的 802.1p 和 DSCP 优先级缺省值为 6 和 46，用户可以动态配置这两个参数，满足自由规划网络语音流量优先级的需求。

说明

- 802.1p 优先级就是 802.1Q VLAN 帧中的 PRI（Priority）字段值，长度为 3 比特，用于交换设备阻塞时，优先发送优先级高的数据包。
- IPv4 的数据报文头部里的 TOS（Type of Service）字节中的 6 位作为 DSCP（DiffServ Code Point）。DSCP 是 DiffServ 的信令，用于 IP 网络的 QoS 保证。网关的流量控制器的操作只决定于这 6 个比特。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **voice-vlan remark** { **8021p** *8021p-value* | **dscp** *dscp-value* } *，配置 Voice VLAN 的 802.1p 和 DSCP 优先级。

缺省情况下，Voice VLAN 的 802.1p 优先级是 6，DSCP 优先级是 46。

----结束

（可选）配置接口加入 Voice VLAN 的模式

交换设备上同一个接口只能指定一个 VLAN 为 Voice VLAN，接口加入 Voice VLAN 的模式分为自动模式和手工模式。

背景信息

接口加入 Voice VLAN 的模式有：

- 自动模式

  使能 Voice VLAN 功能的设备通过学习语音设备发出的语音报文中的源 MAC 地址，将连接语音设备的接口自动加入到 Voice VLAN 中，并通过老化机制维护 Voice VLAN 内的接口数量。在老化时间内，如果配置了 Voice VLAN 的设备未收到任何来自该语音设备的语音报文时，连接语音设备的接口将自动从 Voice VLAN 中删除。如果配置了 Voice VLAN 的设备再次收到该语音设备发出的语音报文，连接语音设备的接口将再次自动加入 Voice VLAN。

- 手工模式

  当使能 Voice VLAN 功能后，必须通过手工将连接语音设备的接口加入到 Voice VLAN 中，这样才能保证 Voice VLAN 功能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **voice-vlan mode** { **auto** | **manual** }，配置接口加入 Voice VLAN 的模式。

缺省情况下，接口加入 Voice VLAN 的模式为自动模式。

- 选择参数 **auto**，接口以自动模式加入 Voice VLAN。
- 选择参数 **manual**，接口以手工模式加入 Voice VLAN。
  - 如果接口类型是 Trunk，需要执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }手工将连接语音设备的接口加入到 Voice VLAN 中。
  - 如果接口类型是 Hybrid：
    - 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，手工将连接语音设备的接口以 Untagged 方式加入到 Voice VLAN 中。
    - 执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，手工将连接语音设备的接口以 Tagged 方式加入到 Voice VLAN 中。

版权所有 © 华为技术有限公司

说明

在自动模式下，不允许将 Access 类型接口加入到 Voice VLAN 中。如果接口类型为 Access，需要使用 **port link-type** 命令将接口配置为 Trunk 或 Hybrid 类型。

----结束

（可选）配置 Voice VLAN 的工作模式

传输数据包括传输语音和业务数据，为满足用户对 Voice VLAN 中传输数据的不同需求，Voice VLAN 在端口下定义了安全模式和普通模式两种传输模式。

背景信息

根据使能了 Voice VLAN 功能的端口对接收到的数据包的过滤机制又将 Voice VLAN 的工作模式分为安全模式和普通模式。

- 安全模式

  使能了 Voice VLAN 功能的入端口只允许源地址是可识别的 OUI 地址的语音报文通过，非该 Voice VLAN 内的语音报文将直接被丢弃，其他 VLAN 内的报文正常转发。

  安全模式用于防止 Voice VLAN 受到恶意数据流量的攻击，但是检查报文的工作会占用一定的系统资源。

- 普通模式

  使能了 Voice VLAN 功能的入端口允许同时传输语音报文和非语音报文。对每一个进入 Voice VLAN 的报文不进行源 MAC 地址匹配检查，容易受到恶意数据流量的攻击。

说明

建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。如确有此需要，请确认 Voice VLAN 工作在普通模式。

不同的 Voice VLAN 模式下处理报文的方式如**表 3-9** 所示。

表 3-9 不同的 Voice VLAN 模式下处理报文的方式

Voice VLAN 模式	处理报文的方式
安全模式	判断该报文源 MAC 地址和 OUI 地址不相同：不修改优先级并禁止数据在 Voice VLAN 内转发。
普通模式	判断该报文源 MAC 地址和 OUI 地址不相同：不修改优先级并允许数据在 Voice VLAN 内转发。

操作步骤

- 安全模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入连接用户语音设备的接口视图。
  3. 执行命令 **voice-vlan security enable**，配置 Voice VLAN 的工作模式是安全模式。

版权所有 © 华为技术有限公司

缺省情况下，Voice VLAN 的工作模式是安全模式。

- 普通模式

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入连接用户语音设备的接口视图。
  3. 执行命令 **undo voice-vlan security enable**，配置 Voice VLAN 的工作模式为普通模式。

     缺省情况下，Voice VLAN 的工作模式是安全模式。

----结束

（可选）使能接口与其他制造商的语音设备的互通功能

为了与其他制造商的语音设备互通，用户可以使能 Voice VLAN legacy 功能，使华为数据通信设备能够识别其他制造商的私有协议报文，实现互通。

背景信息

某些制造商的 IP 电话上电时，不会发送 DHCP 报文申请 IP 地址，而是发送私有协议报文申请 IP 地址。为了与其他制造商的语音设备互通，用户可以使能 Voice VLAN legacy 功能，使华为数据通信设备能够识别其他制造商的私有协议报文，实现互通。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **voice-vlan legacy enable**，使能接口与其他制造商的语音设备的互通功能。

缺省情况下，接口与其他制造商的语音设备的互通功能处于去使能状态。

----结束

检查配置结果

Voice VLAN 配置成功后，您可以查看到 Voice VLAN 的 OUI 地址、工作状态、安全模式、老化时间、802.1p 和 DSCP 优先级和使能了 Voice VLAN 功能接口等配置信息。

前提条件

已经完成 Voice VLAN 的所有配置。

操作步骤

- 使用命令 **display voice-vlan** [*vlan-id*] **status**，查看当前 Voice VLAN 的工作状态、安全模式、老化时间、802.1p 和 DSCP 优先级和使能 Voice VLAN 功能的接口等信息。
- 使用命令 **display voice-vlan oui**，查看 Voice VLAN 的 OUI 地址和相关属性，包括 OUI 掩码地址和 OUI 地址描述信息。

----结束

版权所有 © 华为技术有限公司

3.3.9 配置管理 VLAN 实现网管集中管理设备

配置管理 VLAN 功能，可实现用户通过管理 VLAN 对应的 VLANIF 接口实现网管集中管理设备。

建立配置任务

在进行管理 VLAN 实现网管集中管理设备配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当用户需要通过远端网管集中管理设备，可部署管理 VLAN 功能。

管理 VLAN 功能部署成功后，用户可通过管理 VLAN 对应的 VLANIF 接口的 IP 地址 telnet 到管理交换机，从而实现通过远端设备集中管理。

前置任务

在配置管理 VLAN 之前，需要完成以下任务：

- VLAN 已经成功创建

数据准备

在配置管理 VLAN 之前，需准备以下数据。

序号	数据
1	VLAN 编号

配置管理 VLAN

配置管理 VLAN 功能，用户通过管理 VLAN 的 VLANIF 接口登录到管理交换机，实现网管集中管理设备。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **management-vlan**，配置管理 VLAN。

配置管理 VLAN 后，加入该 VLAN 的端口类型必须是 trunk 或 hybrid 类型的接口。

执行命令 **undo management-vlan** 取消管理 VLAN 功能后，VLAN 将恢复为普通 VLAN。Access、Trunk 或 Hybrid 类型的端口都可以加入该 VLAN。

----结束

版权所有 © 华为技术有限公司

配置管理 VLAN 对应的 VLANIF 接口

用户需要通过管理 VLAN 对应的 VLANIF 接口的 IP 地址 telnet 到管理交换机，实现网管集中管理设备。

请在需要配置管理 VLAN 的设备上执行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口，并进入 VLANIF 接口视图。

VLANIF 接口的编号必须对应一个已经配置为管理 VLAN 的 ID。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 VLANIF 接口的 IP 地址。

管理 VLAN 对应的 VLANIF 接口 IP 地址配置成功后，可通过命令 telnet 登录到管理交换机实现网管集中管理设备。

----结束

检查配置结果

管理 VLAN 配置成功后，您可以查看到管理 VLAN 的配置信息。

前提条件

已经完成管理 VLAN 的所有配置。

操作步骤

- 执行命令 **display vlan** 查看管理 VLAN 的配置信息，带有*的 VLAN 为管理 VLAN。

----结束

3.3.10 维护 VLAN

使用清除统计信息命令，对定位 VLAN 产生的故障有帮助。

清除 VLAN 报文统计信息

当您需要统计一定时间内某 VLAN 的流量信息，这时必须在统计开始前清除该 VLAN 原有的统计信息，使 VLAN 重新进行统计。

背景信息



注意

清除 VLAN 报文统计信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 VLAN 报文统计信息后，请在用户视图下执行下面的 **reset** 命令。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **reset vlan** *vlan-id* **statistics**，清除指定 VLAN 的报文统计信息。

----结束

3.3.11 配置举例

介绍 VLAN 的各种组网举例。

配置基于接口划分 VLAN 示例

本示例中组网特点是配置过程简单，VLAN 划分后，属于不同 VLAN 的用户不能直接进行二层通信，同一 VLAN 内的用户可以直接互相通信。

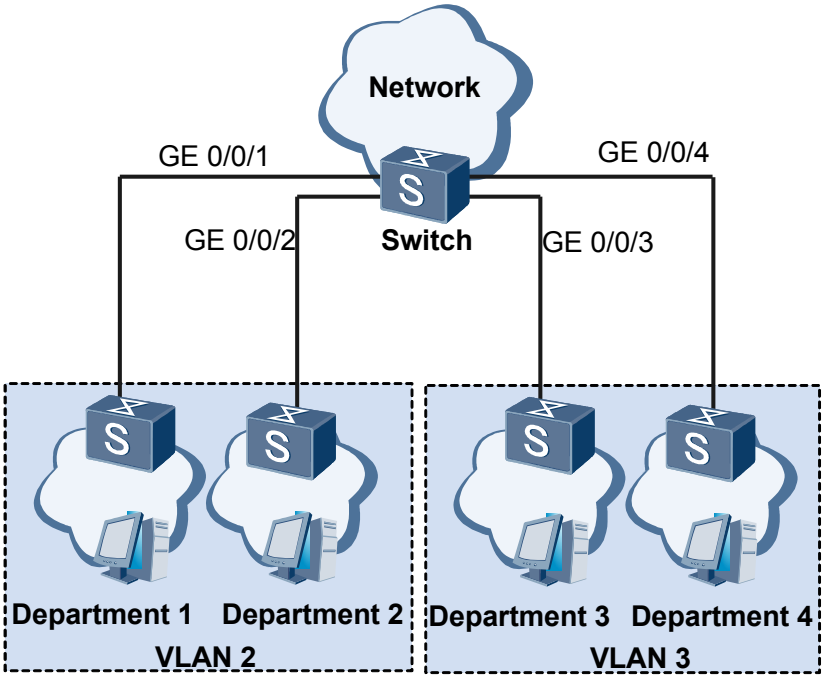
组网需求

某企业有很多部门，要求业务相同部门之间的员工可以互相访问，业务不同部门之间的员工不能互相访问。

如图 3-16 所示，现需要实现：

- 部门 1、部门 2 与部门 3、部门 4 互相隔离。
- 部门 1 与部门 2 可以互相访问。
- 部门 3 与部门 4 可以互相访问。

图 3-16 配置基于接口划分 VLAN 组网图



配置思路

采用如下的思路配置 VLAN：

版权所有 © 华为技术有限公司

1. 创建 VLAN，规划员工所属的 VLAN。
2. 配置端口属性，确定设备连接对象。
3. 关联端口和 VLAN，将连接部门 1 和部门 2 的交换机端口划分到 VLAN2，将连接部门 3 和部门 4 的交换机端口划分到 VLAN3，隔离部门 1、部门 2 和部门 3、部门 4 间的访问。

数据准备

为完成此配置例，需准备如下的数据：

- 接口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 属于 VLAN2。
- 接口 GigabitEthernet0/0/3、GigabitEthernet0/0/4 属于 VLAN3。

操作步骤

步骤 1 配置 Switch

创建 VLAN2。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

将接口 GigabitEthernet0/0/1 的类型为 Trunk，并加入到 VLAN2 中。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[Quidway-GigabitEthernet0/0/1] quit
```

配置接口 GigabitEthernet0/0/2 的类型为 Trunk，并加入到 VLAN2 中。

```
[Quidway]interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

创建 VLAN3。

```
[Quidway] vlan 3
[Quidway-vlan3] quit
```

配置接口 GigabitEthernet0/0/3 的类型为 Trunk，并加入到 VLAN3 中。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 3
[Quidway-GigabitEthernet0/0/3] quit
```

将接口 GigabitEthernet0/0/4 的类型为 Trunk，并加入到 VLAN3 中。

```
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type trunk
[Quidway-GigabitEthernet0/0/4] port trunk allow-pass vlan 3
[Quidway-GigabitEthernet0/0/4] quit
```

步骤 2 验证配置结果

部门 1、部门 2 所属的 VLAN2 内的任一台主机 ping 部门 3、部门 4 所属的 VLAN3 内的任一台主机，无法 ping 通，证明部门 1、部门 2 与部门 3、部门 4 已实现隔离。

部门 1 的任一台主机 ping 部门 2 的任一台主机，能 ping 通，证明部门 1 与部门 2 已实现互通。

版权所有 © 华为技术有限公司

部门 3 的任一台主机 ping 部门 4 的任一台主机，能 ping 通，证明部门 3 与部门 4 已实现互通。

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 3
#
return
```

配置基于 MAC 地址划分 VLAN 示例

配置基于 MAC 地址划分 VLAN 只适用于网卡不经常更换、网络环境较简单的场景中。

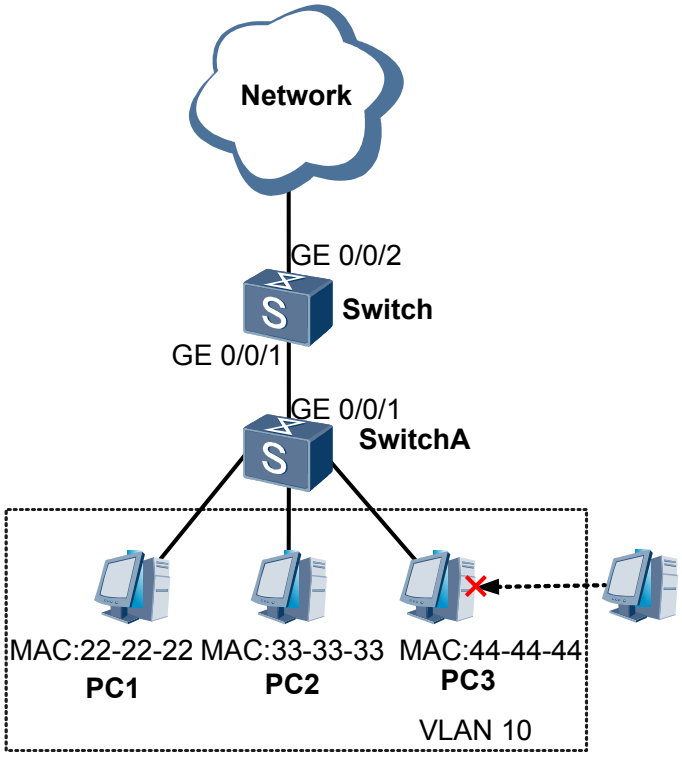
组网需求

某个公司的网络中，网络管理者将同一部门的员工划分到同一 VLAN。为了提高部门内的信息安全，要求只有本部门员工的 PC 才可以访问公司网络。

如**图 3-17** 所示，PC1、PC2、PC3 为本部门员工的 PC，要求这几台 PC 可以通过 SwitchA、Switch 访问公司网络，如换成其他 PC 则不能访问。

版权所有 © 华为技术有限公司

图 3-17 配置基于 MAC 地址的 VLAN 划分组网图



配置思路

采用如下的思路配置基于 MAC 地址的 VLAN 划分：

1. 创建 VLAN，确定员工所属的 VLAN。
2. 配置各以太网接口以正确的方式加入 VLAN。
3. 配置 PC1、PC2、PC3 的 MAC 地址与 VLAN 关联。交换机根据报文中的源 MAC 地址确定 VLAN。

数据准备

为完成此配置例，需准备如下的数据：

- 在 Switch 上配置接口 GE0/0/1 的 PVID 为 100。
- 在 Switch 上配置接口 GE0/0/1 以 untagged 方式加入 VLAN10。
- 在 Switch 上配置接口 GE0/0/2 以 tagged 方式加入 VLAN10。
- 在 SwitchA 上的接口使用默认配置，即所有接口以 untagged 方式加入 VLAN1。
- 获取 PC1、PC2、PC3 的 MAC 地址，配置 MAC 地址与 VLAN10 关联。

操作步骤

步骤 1 配置 Switch

创建 VLAN

华为专有和保密信息
版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] vlan batch 10 100
```

配置接口的 PVID 和加入 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid tagged vlan 10
[Quidway-GigabitEthernet0/0/2] quit
```

PC 的 MAC 地址与 VLAN10 关联

```
[Quidway] vlan 10
[Quidway-Vlan10] mac-vlan mac-address 22-22-22
[Quidway-Vlan10] mac-vlan mac-address 33-33-33
[Quidway-Vlan10] mac-vlan mac-address 44-44-44
[Quidway-Vlan10] quit
```

使能接口的基于 MAC 地址划分 VLAN 功能

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] mac-vlan enable
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 检查配置结果

PC1、PC2、PC3 可以访问公司网络，如换成其他外来人员的 PC 则不能访问。

----结束

配置文件

Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 10 100
#
vlan 10
 mac-vlan mac-address 0022-0022-0022
 mac-vlan mac-address 0033-0033-0033
 mac-vlan mac-address 0044-0044-0044
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10
#
return
```

配置基于 IP 子网划分 VLAN 示例

通过配置基于 IP 子网划分 VLAN，将指定网段或 IP 地址发出的报文在指定的 VLAN 中传输，减轻了网络管理者的初始配置任务量，且有利于管理。

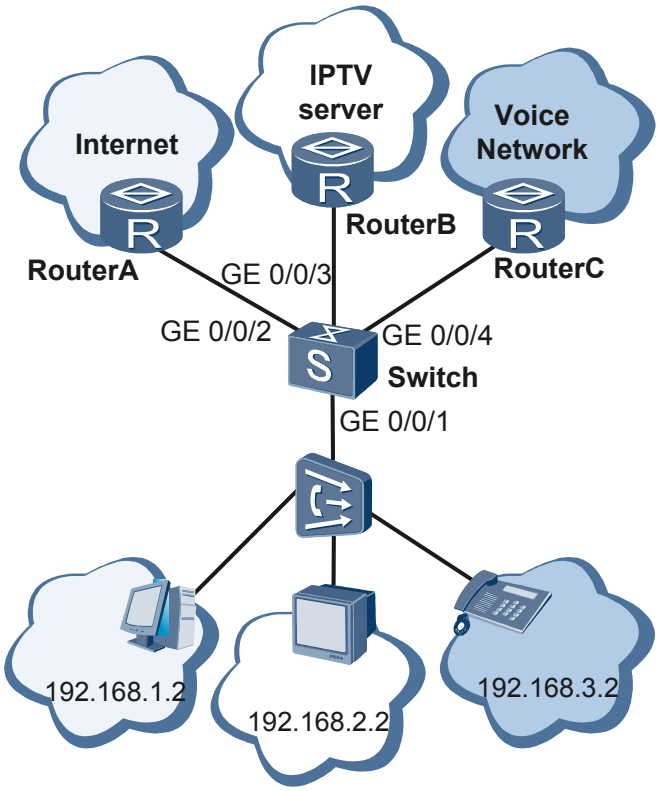
版权所有 © 华为技术有限公司

组网需求

某企业拥有多种业务，如 IPTV、VoIP、Internet 等，每种业务使用的 IP 地址各不相同。为了便于管理，现需要将同一种类型业务划分到同一 VLAN 中，不同类型的业务划分到不同 VLAN 中。

如图 3-18 所示，Switch 接收到用户报文有数据、IPTV、语音等多种业务，用户设备的 IP 地址各不相同。现需要将不同类型的业务划分到不同的 VLAN 中，通过不同的 VLAN ID 分流到不同的远端服务器上以实现业务互通。

图 3-18 基于 IP 子网划分 VLAN 组网图



配置思路

采用如下的思路配置基于 IP 子网划分 VLAN：

1. 创建 VLAN，确定每种业务所属的 VLAN。
2. 关联 IP 子网和 VLAN。

   交换机根据报文中的源 IP 地址或指定网段确定 VLAN。新站点在入网时无需进行太多配置，交换机则根据各站点网络地址自动将其划分到不同的 VLAN 中。
3. 允许基于 IP 子网的 VLAN 通过当前端口。
4. 配置 VLAN 划分方式的优先级，确保优先选择基于 IP 子网划分 VLAN。
5. 使能基于 IP 子网划分 VLAN。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据。

- 配置接口 GE0/0/1 以 untagged 方式加入 VLAN100、VLAN200、VLAN300。
- 配置接口 GE0/0/2、GE0/0/3 和 GE0/0/4 以 tagged 方式分别加入 VLAN100、VLAN200 和 VLAN300。
- IP 子网所需配置数据如表 3-10 所示。

表 3-10 基于 IP 子网划分 VLAN 的配置数据

VLAN ID	IP 子网索引	源 IP 地址	子网掩码	802.1p 优先级
100	1	192.168.1.2	255.255.255.0	2
200	1	192.168.2.2	255.255.255.0	3
300	1	192.168.3.2	255.255.255.0	4

操作步骤

步骤 1 创建 VLAN

在 Switch 上创建 VLAN100、VLAN200 和 VLAN300。

```
<Quidway> system-view
[Quidway] vlan batch 100 200 300
```

步骤 2 配置接口

在 Switch 上配置接口 GE0/0/1 为 Hybrid 类型，并加入 VLAN100、VLAN200 和 VLAN300。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabieEthernet0/0/1] port link-type hybrid
[Quidway-GigabieEthernet0/0/1] port hybrid untagged vlan 100 200 300
[Quidway-GigabieEthernet0/0/1] quit
```

在 Switch 上配置接口 GE0/0/2 加入 VLAN100。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabieEthernet0/0/2] port link-type trunk
[Quidway-GigabieEthernet0/0/2] port trunk allow-pass vlan 100
[Quidway-GigabieEthernet0/0/2] quit
```

在 Switch 上配置接口 GE0/0/3 加入 VLAN200。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabieEthernet0/0/3] port link-type trunk
[Quidway-GigabieEthernet0/0/3] port trunk allow-pass vlan 200
[Quidway-GigabieEthernet0/0/3] quit
```

在 Switch 上配置接口 GE0/0/4 加入 VLAN300。

```
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabieEthernet0/0/4] port link-type trunk
[Quidway-GigabieEthernet0/0/4] port trunk allow-pass vlan 300
[Quidway-GigabieEthernet0/0/4] quit
```

在 Switch 上配置接口 GE0/0/1 使能基于 IP 子网划分 VLAN 功能。

版权所有 © 华为技术有限公司

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabieEthernet0/0/1] ip-subnet-vlan enable
[Quidway-GigabieEthernet0/0/1] quit
```

步骤 3 配置基于 IP 子网划分 VLAN

在 Switch 上配置 VLAN100 与 IP 地址 192.168.1.2 关联，优先级为 2。

```
[Quidway] vlan 100
[Quidway-vlan100] ip-subnet-vlan 1 ip 192.168.1.2 24 priority 2
[Quidway-vlan100] quit
```

在 Switch 上配置 VLAN200 与 IP 地址 192.168.2.2 关联，优先级为 3。

```
[Quidway] vlan 200
[Quidway-vlan200] ip-subnet-vlan 1 ip 192.168.2.2 24 priority 3
[Quidway-vlan200] quit
```

在 Switch 上配置 VLAN300 与 IP 地址 192.168.3.2 关联，优先级为 4。

```
[Quidway] vlan 300
[Quidway-vlan300] ip-subnet-vlan 1 ip 192.168.3.2 24 priority 4
[Quidway-vlan300] quit
```

步骤 4 验证配置结果

在 Switch 上执行以下命令，显示信息如下：

```
[Quidway] display ip-subnet-vlan vlan all
-------------------------------------------------------------------
 Vlan    Index   IpAddress          SubnetMask          Priority
 ----------------------------------------------------------------
 100     1       192.168.1.2        255.255.255.0       2
 200     1       192.168.2.2        255.255.255.0       3
 300     1       192.168.3.2        255.255.255.0       4
 ----------------------------------------------------------------
 ip-subnet-vlan count: 3                 total count: 3
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Quidway
#
 vlan batch 100 200 300
#
vlan 100
 ip-subnet-vlan 1 ip 192.168.1.2 255.255.255.0 priority 2
#
vlan 200
 ip-subnet-vlan 1 ip 192.168.2.2 255.255.255.0 priority 3
#
vlan 300
 ip-subnet-vlan 1 ip 192.168.3.2 255.255.255.0 priority 4
#
interface GigabieEthernet0/0/1
 port hybrid untagged vlan 100 200 300
 ip-subnet-vlan enable
#
interface GigabieEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabieEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 200
```


版权所有 © 华为技术有限公司

```
#
interface GigabieEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 300
#
return
```

配置基于协议划分 VLAN 示例

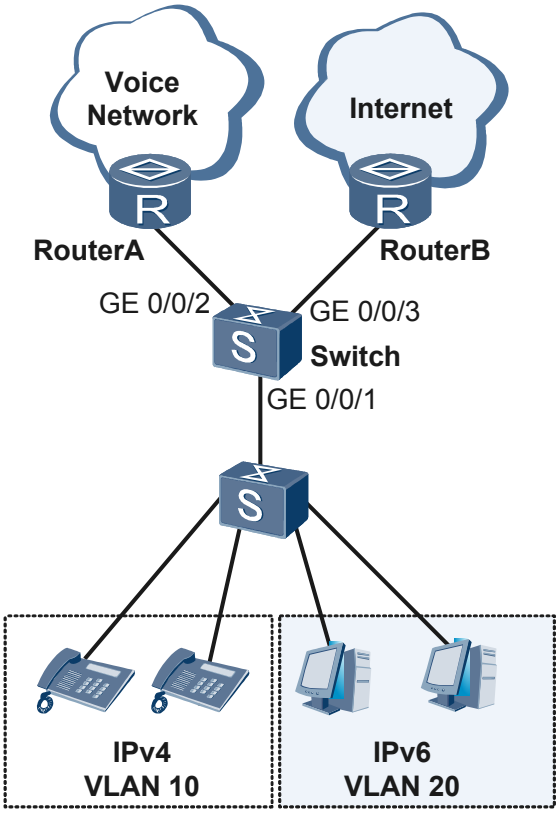
该示例的特点是减少了人工配置 VLAN 的工作量，同时保证了用户自由地增加、移动和修改。

组网需求

某企业拥有多种业务，如 IPTV、VoIP、Internet 等，每种业务所采用的协议各不相同。为了便于管理，减少人工配置 VLAN 的工作量，现需要将同一种类型业务划分到同一 VLAN 中，不同类型的业务划分到不同 VLAN 中。

如图 3-19 所示，Switch 收到的用户报文有多种业务，所采用的协议各不相同。VLAN10 中的用户采用 IPv4 协议与远端用户通信，而 VLAN20 中的用户采用 IPv6 协议与远端服务器通信。现需要将不同类型的业务划分到不同的 VLAN 中，通过不同的 VLAN ID 分流到不同的远端服务器上以实现业务互通。

图 3-19 基于协议划分 VLAN 组网图



配置思路

采用如下的思路配置基于协议划分 VLAN：

版权所有 © 华为技术有限公司

1. 创建 VLAN，确定每种业务所属的 VLAN。
2. 关联协议和 VLAN。

   Switch 根据端口接收到的报文所属的协议（族）类型给报文分配不同的 VLAN ID。无论用户物理位置是否移动、用户主机网卡是否更换、用户是否在同一网段、只要用户设备所采用的协议没有变换，VLAN 都不用再重新划分。
3. 关联接口和协议 VLAN。

   当有关联的协议进入关联的接口时，系统自动为该协议分配已经划分好的 VLAN ID。
4. 允许基于协议的 VLAN 通过当前端口。

数据准备

为完成此配置例，需准备如下的数据。

- 在 Switch 上配置接口 GE0/0/1 以 untagged 方式加入 VLAN10、VLAN20。
- 在 Switch 上配置接口 GE0/0/2、GE0/0/3 以 tagged 方式分别加入 VLAN10、VLAN20。
- 各个 VLAN 对应的协议。
  - VLAN10:IPv4
  - VLAN20:IPv6

操作步骤

步骤 1 创建 VLAN

配置 Switch。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 10 20
```

步骤 2 配置基于协议划分 VLAN

在 Switch 上配置 VLAN10 与协议 IPv4 关联。

```
[Switch] vlan 10
[Switch-vlan10] protocol-vlan ipv4
[Switch-vlan10] quit
```

在 Switch 上配置 VLAN20 与协议 IPv6 关联。

```
[Switch] vlan 20
[Switch-vlan20] protocol-vlan ipv6
[Switch-vlan20] quit
```

步骤 3 配置接口关联协议 VLAN

在 Switch 上配置接口与 VLAN10 关联，优先级是 5。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] protocol-vlan vlan 10 all priority 5
```

在 Switch 上配置接口与 VLAN20 关联，优先级是 6。

```
[Switch-GigabitEthernet0/0/1] protocol-vlan vlan 20 all priority 6
[Switch-GigabitEthernet0/0/1] quit
```

步骤 4 配置接口

版权所有 © 华为技术有限公司

在 Switch 上配置接口 GE0/0/1 允许 VLAN10 和 VLAN20 通过。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type hybrid
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 10 20
[Switch-GigabitEthernet0/0/1] quit
```

在 Switch 上配置接口 GE0/0/2 允许 VLAN10 通过。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/2] quit
```

在 Switch 上配置接口 GE0/0/3 允许 VLAN20 通过。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 20
[Switch-GigabitEthernet0/0/3] quit
```

步骤 5 验证配置结果

上述配置完成后，执行命令 **display protocol-vlan interface all**，可以查看接口关联基于协议划分 VLAN 的配置信息。例如：

以 Switch 上显示为例。

```
<Switch> display protocol-vlan interface all
-------------------------------------------------------------------------------
 Interface                VLAN    Index        Protocol Type           Priority
-------------------------------------------------------------------------------
 GigabitEthernet0/0/1           10      0            ipv4                    5
 GigabitEthernet0/0/1           20      0            ipv6                    6
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 10 20
#
vlan 10
 protocol-vlan 0 ipv4
vlan 20
 protocol-vlan 0 ipv6
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 10 20
 protocol-vlan vlan 10 0 priority 5
 protocol-vlan vlan 20 0 priority 6
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```


版权所有 © 华为技术有限公司

配置 VLAN 间通过 VLANIF 接口通信示例

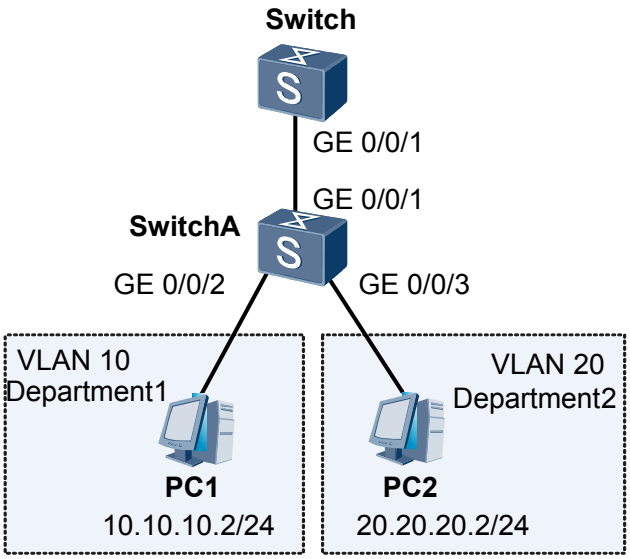
该组网的特点是将三层转发的设备由路由器替换为三层交换机，来实现了 VLAN 间互通。

组网需求

企业的不同部门拥有相同的业务，如上网、VoIP 等业务，且各个部门中的用户位于不同的网段。目前存在不同的部门中相同的业务所属的 VLAN 不相同，现需要实现不同 VLAN 中的用户相互通信。

如图 3-20 所示，部门 1 和部门 2 中拥有相同的业务上网业务，但是属于不同的 VLAN 且位于不同的网段。现需要实现部门 1 与部门 2 的用户互通。

图 3-20 配置 VLAN 间通过 VLANIF 接口通信组网图



配置思路

采用如下的思路配置 VLAN 间通过 VLANIF 接口通信：

1. 在交换机上创建 VLAN，确定用户所属的 VLAN。
2. 在交换机上配置允许用户所属的 VLAN 通过当前二层端口。
3. 在三层交换机上创建 VLANIF 接口并配置 IP 地址，实现三层互通。

说明

为了成功实现 VLAN 间互通，VLAN 内主机的缺省网关必须是对应 VLANIF 接口的 IP 地址。

数据准备

为完成此配置例，需准备如下的数据：

- 在 Switch 上配置接口 GE0/0/1 加入 VLAN10 和 VLAN20。
- 在 Switch 上配置 VLANIF10 的 IP 地址为 10.10.10.1/24。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 在 Switch 上配置 VLANIF20 的 IP 地址为 20.20.20.1/24。
- 在 SwitchA 上配置接口 GE0/0/1 加入 VLAN10 和 VLAN20。
- 在 SwitchA 上配置接口 GE0/0/2 加入 VLAN10。
- 在 SwitchA 上配置接口 GE0/0/3 加入 VLAN20。

操作步骤

步骤 1 配置 Switch

创建 VLAN

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

配置接口加入 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
[Quidway-GigabitEthernet0/0/1] quit
```

配置 VLANIF 接口的 IP 地址

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.10.10.1 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 20.20.20.1 24
[Quidway-Vlanif20] quit
```

步骤 2 配置 SwitchA

创建 VLAN

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

配置接口加入 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 10
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] port default vlan 20
[Quidway-GigabitEthernet0/0/3] quit
```

步骤 3 检查配置结果

在 VLAN10 中的 PC1 上配置缺省网关为 VLANIF10 接口的 IP 地址 10.10.10.1/24。

在 VLAN20 中的 PC2 上配置缺省网关为 VLANIF20 接口的 IP 地址 20.20.20.1/24。

配置完成后，VLAN10 内的 PC1 与 VLAN20 内的 PC2 能够相互访问。

----结束

版权所有 © 华为技术有限公司

配置文件

Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

SwitchA 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 10 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 20
#
return
```

配置 VLAN 聚合示例

该组网的特点是以较少的 IP 地址实现了 VLAN 间通信。

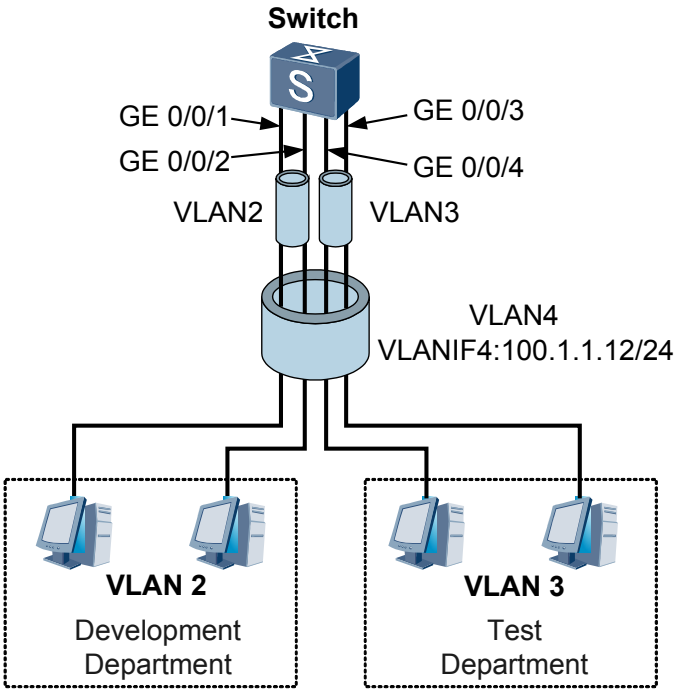
组网需求

某公司拥有多个部门且位于同一网段，为了提升业务安全性，将不同部门的员工划分到不同 VLAN 中。现由于业务需要，不同部门间的员工需要互通。

如图 3-21 所示，研发部和测试部分布在不同的 VLAN 中，现需要实现不同 VLAN 间的员工可以互相访问。

版权所有 © 华为技术有限公司

图 3-21 配置 VLAN 聚合组网图



配置思路

采用如下思路配置 VLAN 聚合：

1. 把 Switch 接口加入到相应的 sub-VLAN 中。
2. 把 sub-VLAN 聚合为 super-VLAN。
3. 配置 super-VLAN 的 IP 地址。
4. 配置 super-VLAN 的 Proxy ARP。

数据准备

为完成此配置例，需准备如下的数据：

- GE0/0/1 和 GE0/0/2 属于 VLAN2
- GE0/0/3 和 GE0/0/4 属于 VLAN3
- super-VLAN 的 ID 为 4
- super-VLAN 的 IP 地址为 100.1.1.12

操作步骤

步骤 1 配置接口类型

配置接口 GE0/0/1 为 Access 类型。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] quit
```


华为专有和保密信息
版权所有 © 华为技术有限公司

配置接口 GE0/0/2 为 Access 类型。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] quit
```

配置接口 GE0/0/3 为 Access 类型。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] quit
```

配置接口 GE0/0/4 为 Access 类型。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type access
[Quidway-GigabitEthernet0/0/4] quit
```

步骤 2 配置 VLAN2

创建 VLAN2。

```
[Quidway] vlan 2
```

向 VLAN2 中加入 GE0/0/1 和 GE0/0/2。

```
[Quidway-vlan2] port gigabitethernet 0/0/1 0/0/2
[Quidway-vlan2] quit
```

步骤 3 配置 VLAN3

创建 VLAN3。

```
[Quidway] vlan 3
```

向 VLAN3 中加入 GE0/0/3 和 GE0/0/4。

```
[Quidway-vlan3] port gigabitethernet 0/0/3 0/0/4
[Quidway-vlan3] quit
```

步骤 4 配置 VLAN4

配置 super-VLAN。

```
[Quidway] vlan 4
[Quidway-vlan4] aggregate-vlan
[Quidway-vlan4] access-vlan 2 to 3
```

配置 VLANIF。

```
[Quidway] interface vlanif 4
[Quidway-Vlanif4] ip address 100.1.1.12 255.255.255.0
[Quidway-Vlanif4] quit
```

步骤 5 配置 PC

分别为各 PC 配置 IP 地址，并使它们和 VLAN4 处于同一网段。

配置成功后，各 PC 与 Switch 之间可以相互 ping 通，但 VLAN2 的 PC 与 VLAN3 的 PC 间不可以相互 ping 通。

步骤 6 配置 Proxy ARP

```
[Quidway] interface vlanif 4
[Quidway-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
```


版权所有 © 华为技术有限公司

步骤 7 检查配置结果

配置完成后，VLAN2 的 PC 与 VLAN3 的 PC 间可以相互 ping 通。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
#
interface Vlanif4
 ip address 100.1.1.12 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 3
#
return
```

配置 MUX VLAN 示例

MUX VLAN 提供了一种在 VLAN 内的端口间进行二层流量隔离的机制，通过配置 MUX VLAN 可以实现企业内部部分员工之间可以互相交流，部分员工之间是相互隔离。

组网需求

在企业网络中，企业所有员工都可以访问企业的服务器。但对于企业来说，希望企业内部部分员工之间可以互相交流，而部分员工之间是隔离的，不能够互相访问。

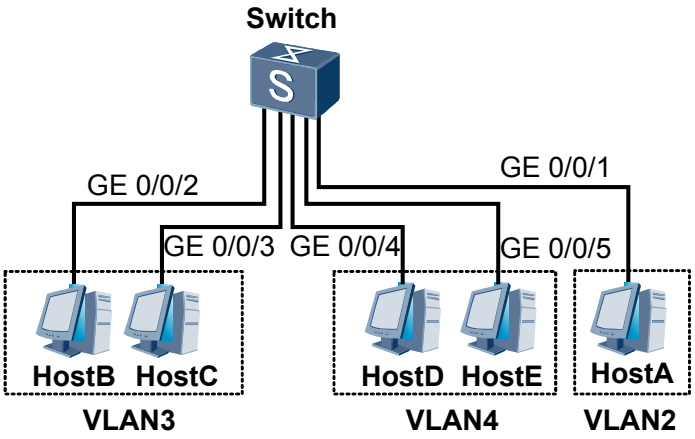
如图 3-22 所示，为了满足企业的需求，可将企业服务器、能够互相访问的员工分别划分到不同的两个 VLAN，将不能够互相访问的员工分别划分到不同的 VLAN（不能与企业服务器、互相访问的员工所在的 VLAN 相同）。由此，实现同一个 VLAN 内的用户可以相互通信，不同的 VLAN 间用户相互隔离。

为了实现所有员工都可访问企业服务器，可通过配置 VLAN 间通信实现。如果企业规模很大，拥有大量的员工，那么就要为不能互相访问的员工都分配 VLAN，这不但需要耗费大量的 VLAN ID，还增加了网络管理者的工作量同时也增加了维护量。

为了解决上述问题，可在连接终端的交换机上部署 MUX VLAN 特性。MUX VLAN 不但能够实现企业需求，同时也解决了 VLAN ID 紧缺问题，也便于网络管理者维护。

版权所有 © 华为技术有限公司

图 3-22 配置 MUX-VLAN 组网图



配置思路

采用如下思路配置 MUX-VLAN 功能：

1. 配置主 VLAN 的 MUX-VLAN 功能。
2. 配置 Group-VLAN 功能。
3. 配置 Separate-VLAN 功能。
4. 配置接口加入 VLAN 并使能 MUX-VLAN 功能。

数据准备

为完成此配置例，需准备如下的数据：

- GE0/0/1 属于 VLAN2
- GE0/0/2 和 GE0/0/3 属于 VLAN3
- GE0/0/4 和 GE0/0/5 属于 VLAN4

操作步骤

步骤 1 配置 MUX VLAN

创建 VLAN2、VLAN3 和 VLAN4。

```
<Quidway> system-view
[Quidway] vlan batch 2 3 4
[Quidway] quit
```

配置 MUX VLAN 中的主 VLAN 和从 VLAN。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] mux-vlan
[Quidway-vlan2] subordinate group 3
[Quidway-vlan2] subordinate separate 4
[Quidway-vlan2] quit
```

配置接口加入 VLAN 并使能 MUX VLAN 功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 2
[Quidway-GigabitEthernet0/0/1] port mux-vlan enable
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 3
[Quidway-GigabitEthernet0/0/2] port mux-vlan enable
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] port default vlan 3
[Quidway-GigabitEthernet0/0/3] port mux-vlan enable
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type access
[Quidway-GigabitEthernet0/0/4] port default vlan 4
[Quidway-GigabitEthernet0/0/4] port mux-vlan enable
[Quidway-GigabitEthernet0/0/4] quit
[Quidway] interface gigabitethernet 0/0/5
[Quidway-GigabitEthernet0/0/5] port link-type access
[Quidway-GigabitEthernet0/0/5] port default vlan 4
[Quidway-GigabitEthernet0/0/5] port mux-vlan enable
[Quidway-GigabitEthernet0/0/5] quit
```

步骤 2 检查配置结果

HostA 和 HostB、HostC、HostD、HostE 都可以互相 ping 通。

HostB 和 HostC 可以互相 ping 通。

HostD 和 HostE 不可以互相 ping 通。

HostB、HostC 和 HostD、HostE 不可以互相 ping 通。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate group 3
 subordinate separate 4
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
 port mux-vlan enable
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
return
```

配置自动模式下的 Voice VLAN 示例

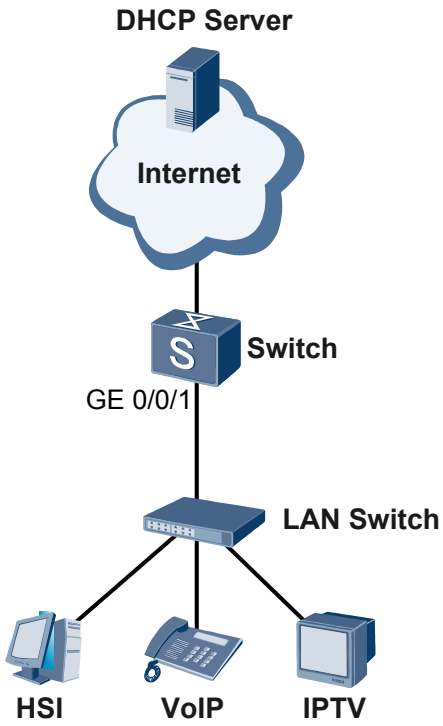
本示例组网的特点是语音流量可通过专属 VLAN（Voice VLAN）传输，在一段时间内，如果语音设备发生故障或语音设备退出网络，连接语音设备的端口会自动从 Voice VLAN 中退出。

组网需求

网络中有 HSI、VoIP 和 IPTV 等数据流，用户对语音通话质量较敏感，需要提高语音数据流的传输优先级，以保证用户的通话质量。

如图 3-23 所示，Switch 配置 Voice VLAN 功能后，根据进入接口 GigabitEthernet0/0/1 的数据流源 MAC 地址来判断是否为语音数据流，是则修改报文优先级且在 Voice VLAN 内传输，不是则不修改报文优先级且在普通 VLAN 内传输。并且要求接口 GigabitEthernet0/0/1 能自动加入和退出 Voice VLAN。

图 3-23 配置自动模式下的 Voice VLAN 的组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置自动模式下的 Voice VLAN：

1. 创建 VLAN。
2. 配置接口类型及缺省 VLAN。
3. 使能接口的 Voice VLAN 功能。
4. 配置接口加入 Voice VLAN 的模式。
5. 配置 Voice VLAN 的 OUI 地址。
6. 配置 Voice VLAN 的老化时间。
7. 配置 Voice VLAN 的工作模式。

数据准备

为完成此配置例，需准备如下的数据：

- 创建 Voice VLAN2 和 IP 电话申请 IP 地址的 VLAN6。
- OUI 地址为 0011-2200-0000，掩码地址为 ffff-ff00-0000。
- Voice VLAN 的老化时间为 100min。
- 接口 GigabitEthernet0/0/1 的缺省 VLAN 为 VLAN6。

操作步骤

步骤 1 配置 Switch 的 VLAN 和接口

创建 VLAN2、VLAN6

```
<Quidway> system-view
[Quidway] vlan batch 2 6
```

配置接口类型和缺省 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 6
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 6
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 配置 Switch 的 Voice VLAN 功能

配置接口 Voice VLAN 功能

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] voice-vlan 2 enable
```

配置接口加入 Voice VLAN 的模式

```
[Quidway-GigabitEthernet0/0/1] voice-vlan mode auto
[Quidway-GigabitEthernet0/0/1] quit
```

配置 OUI 地址

```
[Quidway] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

配置 Voice VLAN 的老化时间

```
[Quidway] voice-vlan aging-time 100
```

配置 Voice VLAN 的工作模式

版权所有 © 华为技术有限公司

```
[Quidway-GigabitEthernet0/0/1] voice-vlan security enable
```

步骤 3 检查配置结果

执行命令 **display voice-vlan oui**，查看 Voice VLAN 的 OUI 地址是否配置正确。

```
<Quidway> display voice-vlan oui
-------------------------------------------------
OuiAddress       Mask            Description
-------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

执行命令 **display voice-vlan 2 status**，查看 Voice VLAN 的工作状态、安全模式和老化时间是否配置正确。

```
<Quidway> display voice-vlan 2 status
Voice VLAN Configurations:
-------------------------------------------------
Voice VLAN ID            :  2
Voice VLAN status        : Enable
Voice VLAN aging time    : 100(minutes)
Voice VLAN 802lp remark  : 6
Voice VLAN dscp remark   : 46
-------------------------------------------------------------
Port Information:
-------------------------------------------------------------
Port                    Add-Mode  Security-Mode  Legacy
-------------------------------------------------------------
GigabitEthernet0/0/1            Auto      Security       Disable
```

----结束

配置文件

Switch 的配置文件。

```
#
sysname Quidway
#
 vlan batch 2 6
#
 voice-vlan aging-time 100
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 6
 port hybrid untagged vlan 6
 voice-vlan 2 enable
#
return
```

配置手动模式下的 Voice VLAN 示例

该组网的特点是使能了 Voice VLAN 功能的接口以手动模式加入 Voice VLAN。手动模式下配置了 Voice VLAN 功能后，必须通过手动将连接语音设备的接口加入到 Voice VLAN 中，这样才能保证接口正常转发 Voice VLAN 的语音报文。

组网需求

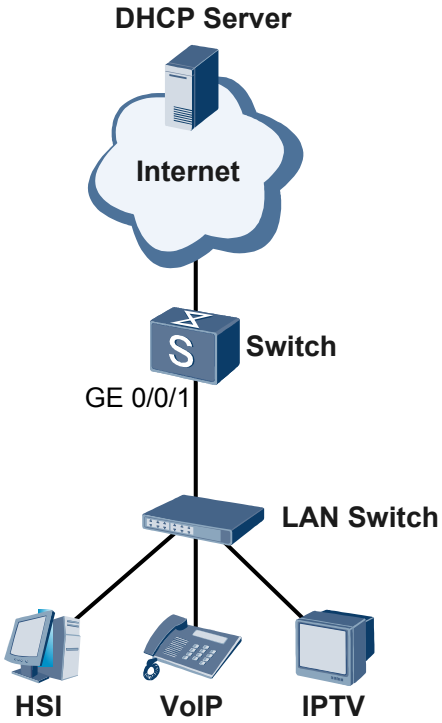
网络中有 HSI、VoIP 和 IPTV 等数据流，用户对语音通话质量较敏感，需要提高语音数据流的传输优先级，以保证用户的通话质量。

如图 3-24 所示，Switch 配置 Voice VLAN 功能后，根据进入接口 GigabitEthernet0/0/1 的数据流源 MAC 地址来判断是否为语音数据流，是则修改报文优先级且在 Voice VLAN

版权所有 © 华为技术有限公司

内传输，不是则不修改报文优先级且在普通 VLAN 内传输。接口 GigabitEthernet0/0/1 需要通过手动加入和退出 Voice VLAN。

图 3-24 配置手动模式下的 Voice VLAN 的组网图



配置思路

采用如下的思路配置自动模式下的 Voice VLAN：

1. 创建 VLAN。
2. 配置接口类型及缺省 VLAN。
3. 使能接口的 Voice VLAN 功能。
4. 配置接口加入 Voice VLAN 的模式。
5. 配置 Voice VLAN 的 OUI 地址。
6. 配置 Voice VLAN 的工作模式。
7. 配置接口加入 Voice VLAN。

数据准备

为完成此配置例，需准备如下的数据：

- 创建 Voice VLAN2 和 IP 电话申请 IP 地址的 VLAN6。
- OUI 地址为 0011-2200-0000，掩码地址为 ffff-ff00-0000。
- 接口 GigabitEthernet0/0/1 的缺省 VLAN 为 VLAN6。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 Switch 的 VLAN 和接口

创建 VLAN2、VLAN6

```
<Quidway> system-view
[Quidway] vlan batch 2 6
```

配置接口类型和缺省 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 6
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 6
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 配置 Switch 的 Voice VLAN 功能

配置接口 Voice VLAN 功能

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] voice-vlan 2 enable
```

配置接口加入 Voice VLAN 的模式

```
[Quidway-GigabitEthernet0/0/1] voice-vlan mode manual
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 2
[Quidway-GigabitEthernet0/0/1] quit
```

配置 OUI 地址

```
[Quidway] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

配置 Voice VLAN 的工作模式

```
[Quidway-GigabitEthernet0/0/1] voice-vlan security enable
```

步骤 3 检查配置结果

执行命令 **display voice-vlan oui**，查看 Voice VLAN 的 OUI 地址是否配置正确。

```
<Quidway> display voice-vlan oui
-------------------------------------------------
OuiAddress       Mask            Description
-------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

执行命令 **display voice-vlan 2 status**，查看 Voice VLAN 的工作状态、安全模式和老化时间是否配置正确。

```
<Quidway> display voice-vlan 2 status
Voice VLAN Configurations:
-------------------------------------------------
Voice VLAN ID           :  2
Voice VLAN status       : Enable
Voice VLAN aging time   : 1440(minutes)
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
-------------------------------------------------------------
Port Information:
-------------------------------------------------------------
Port                    Add-Mode  Security-Mode  Legacy
-------------------------------------------------------------
GigabitEthernet0/0/1            Manual    Security       Disable
```

----结束

版权所有 © 华为技术有限公司

配置文件

Switch 的配置文件。

```
#
sysname Quidway
#
 vlan batch 2 6
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 6
 port hybrid tagged vlan 2
 port hybrid untagged vlan 6
 voice-vlan 2 enable
 voice-vlan mode manual
#
return
```

3.4 VLAN Mapping 配置

介绍了 VLAN Mapping 配置的基本知识、配置方法，配置实例。

3.4.1 VLAN Mapping 概述

简要介绍 VLAN Mapping 的基本概念。

VLAN Mapping 即 VLAN 映射，它通过替换数据帧中的内外层 VLAN Tag 来实现用户 VLAN 与运营商 VLAN 的相互映射。通过替换 VLAN Tag 实现 VLAN 汇聚功能，使用户业务按照运营商的网络规划进行传输。

3.4.2 AC6605 支持的 VLAN Mapping 特性

介绍 VLAN Mapping 特性在 AC6605 中的支持情况。

AC6605 支持的 VLAN Mapping 特性：

- 支持接口+VLAN 方式的单层 VLAN Mapping 功能。
- 支持接口+VLAN 方式的双层 VLAN Mapping 功能。
- 支持接口+VLAN+802.1p 方式的单层 VLAN Mapping 功能。
- 支持全局的 VLAN Mapping 功能。

说明

AC6605 支持双层 VLAN Mapping 功能，不支持全局 VLAN Mapping 功能。。

3.4.3 配置单层 Tag 的 VLAN Mapping

介绍如何配置单层 Tag 的 VLAN Mapping 功能。

建立配置任务

应用环境

当两个用户私网间需要通过运营商公网进行通信，而且两个用户私网分别处在不同的 VLAN 范围内；用户的数据报文带有私网 VLAN Tag 进入公网。在公网上的边缘节点设

版权所有 © 华为技术有限公司

备可以配置 VLAN Mapping 功能，这样可以实现私网与公网的 VLAN 分离，节省公网的 VLAN资源。

前置任务

在配置单层 Tag 的 VLAN Mapping 之前，需完成配置 VLAN。

数据准备

在配置单层 Tag 的 VLAN Mapping 之前，需准备以下数据：

序号	数据
1	映射前的 VLAN 编号
2	映射后的 VLAN 编号

配置替换单层 Tag

背景信息

在需要配置单层 Tag 的 VLAN Mapping 功能的 AC6605 设备上进行以下操作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太网接口视图。

步骤 3 执行命令 **port link-type trunk**，配置接口的类型。

缺省情况下，接口的类型为 Hybrid。

步骤 4 执行命令 **port trunk allow-pass vlan** *vlan-id*，配置 Trunk 接口加入 **map-vlan**。

步骤 5 执行命令 **qinq vlan-translation enable**，使能接口 VLAN 转换功能。

步骤 6 执行命令 **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*]，配置接口的单层 Tag 的 VLAN Mapping 功能。

说明

- 配置 VLAN Mapping 功能的接口类型必须为 Trunk 或 Hybrid，接口必须以 Tagged 的方式加入映射后的 **map-vlan**。
- 当 **vlan** 的取值为 *vlan-id1* **to** *vlan-id2* 时，接口还需要以 Tagged 的方式加入映射前的 **vlan**，并且 **map-vlan** 不允许配置成 VLANIF 接口。
- 如果同时配置了 VLAN Mapping 和 DHCP 功能，接口需要以 Tagged 方式加入映射前 VLAN。
- MAC 地址学习限制可能会影响 N：1 的 VLAN Mapping 功能正常使用。

----结束

检查配置结果

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display vlan** *vlan-id* 查看接口是否加入映射后的本地 VLAN。
- 使用命令 **display current-configuration** 查看接口的单层 Tag 的 VLAN Mapping 配置。

  在配置成功时，执行上面的命令，应能得到如下的结果：

  - 接口已加入映射后的本地 VLAN；
  - 接口的单层 Tag 的 VLAN Mapping 配置正确。

----结束

3.4.4 配置双层 Tag 的 VLAN Mapping

介绍如何配置 VLAN Mapping 支持双层 Tag 交换功能。

建立配置任务

应用环境

当两个用户私网间需要通过运营商公网进行通信，而且两个用户私网分别处在不同的 VLAN 范围内；用户的数据报文可能带有一层或者两层 VLAN Tag 进入公网。在公网上的边缘节点设备可以配置双层 Tag 的 VLAN Mapping 功能，这样可以实现私网与公网的 VLAN 分离，节省公网的 VLAN 资源。而且相对于单层 Tag 的 VLAN Mapping 功能更加灵活，应用范围更广。

说明

AC6605 支持双层 VLAN Mapping 功能。

前置任务

- 在配置替换双层 Tag 中的外层 VLAN Tag 之前，需完成配置 VLAN。

数据准备

在配置双层 Tag 的 VLAN Mapping 功能之前，需准备以下数据：

序号	数据
1	映射前的外层 VLAN 编号
2	映射前的内层 VLAN 编号
3	映射后的外层 VLAN 编号

配置替换双层 Tag 中的外层 Tag

背景信息

在需要配置替换双层 Tag 中的外层 Tag 的 AC6605 设备上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type trunk**，配置接口的类型为 Trunk 类型。

步骤 4 执行命令 **port trunk allow-pass vlan** *vlan-id* ，配置接口加入 **map-vlan**。

步骤 5 执行命令 **qinq vlan-translation enable**，使能接口 VLAN 转换功能。

步骤 6 执行命令 **port vlan-mapping vlan** *vlan-id1* **inner-vlan** *vlan-id2* [**to** *vlan-id3*] **map-vlan** *vlan-id4* [**remark-8021p** *8021p-value*]，配置替换双层 Tag 中的外层 Tag。

说明

配置 VLAN Mapping 功能的接口类型必须为 Trunk 或 Hybrid，接口必须以 Tagged 的方式加入映射后的 **map-vlan**。

----结束

检查配置结果

操作步骤

- 使用命令 **display vlan** *vlan-id* 查看接口是否加入映射后的本地 VLAN。
- 使用命令 **display current-configuration** 查看接口的双层 Tag 的 VLAN Mapping 配置。

  在配置成功时，执行上面的命令，应能得到如下的结果：

  - 接口已加入映射后的本地 VLAN。
  - 接口的双层 Tag 的 VLAN Mapping 配置正确。

----结束

3.4.5 配置举例

介绍 VLAN Mapping 的各种组网举例。

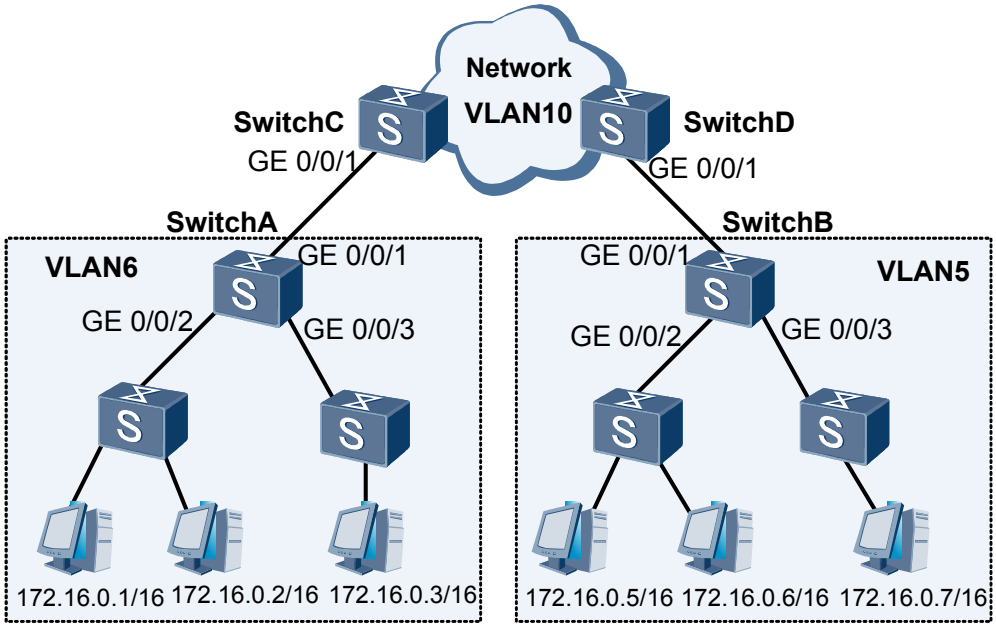
配置单层 Tag 的 VLAN Mapping 示例

组网需求

在如图 3-25 所示的网络中，VLAN6 内的用户需要通过网络中的 VLAN10 与 VLAN5 内的用户通信。

版权所有 © 华为技术有限公司

图 3-25 配置 VLAN Mapping 示例组网图



配置思路

采用如下的思路配置 VLAN Mapping：

1. 在 SwitchA、SwitchB、SwitchC、SwitchD 上创建各自所属的 VLAN。
2. 配置 SwitchA、SwitchB、SwitchC、SwitchD 接口加入各自创建的 VLAN。
3. 在 SwitchA 的接口 GigabitEthernet0/0/1 上配置 VLAN Mapping。
4. 在 SwitchB 的接口 GigabitEthernet0/0/1 上配置 VLAN Mapping。

数据准备

为完成此配置例，需准备如下的数据：

- 在 SwitchA 上需要创建的 VLAN6。
- 在 SwitchB 上需要创建的 VLAN5。
- 在 SwitchC、SwitchD 上需要创建的 VLAN10。

操作步骤

步骤 1 配置 VLAN

在 SwitchA 创建 VLAN6。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 6
```

在 SwitchB 创建 VLAN5。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 5
```


华为专有和保密信息
版权所有 © 华为技术有限公司

在 SwitchC 创建 VLAN10。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 10
```

在 SwitchD 创建 VLAN10。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan 10
```

步骤 2 配置接口加入 VLAN

在 SwitchA 上配置接口 GigabitEthernet0/0/2、GigabitEthernet0/0/3 加入 VLAN6。

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 6
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 6
[SwitchA-GigabitEthernet0/0/3] quit
```

在 SwitchA 上配置接口 GigabitEthernet0/0/1 加入 VLAN6。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 6
[SwitchA-GigabitEthernet0/0/1] quit
```

在 SwitchB 上配置接口 GigabitEthernet0/0/2、GigabitEthernet0/0/3 加入 VLAN5。

```
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 5
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] port link-type trunk
[SwitchB-GigabitEthernet0/0/3] port trunk allow-pass vlan 5
[SwitchB-GigabitEthernet0/0/3] quit
```

在 SwitchB 上配置接口 GigabitEthernet0/0/1 加入 VLAN5。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 5
[SwitchB-GigabitEthernet0/0/1] quit
```

在 SwitchC 上配置接口 GigabitEthernet0/0/1 加入 VLAN10。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
```

在 SwitchD 上配置接口 GigabitEthernet0/0/1 加入 VLAN10。

```
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] port link-type trunk
[SwitchD-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchD-GigabitEthernet0/0/1] quit
```

步骤 3 配置 VLAN Mapping

在 SwitchA 的接口 GigabitEthernet0/0/1 上配置 VLAN Mapping。

```
[SwitchA-GigabitEthernet0/0/1] qinq vlan-translation enable
```


版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/1] port vlan-mapping vlan 10 map-vlan 6
```

在 SwitchB 的接口 GigabitEthernet0/0/1 上配置 VLAN Mapping。

```
[SwitchB-GigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchB-GigabitEthernet0/0/1] port vlan-mapping vlan 10 map-vlan 5
```

步骤 4 验证配置结果

从 VLAN6 内用户的任意一台主机 ping VLAN5 内用户的任意一台主机，或从 VLAN5 内用户的任意一台主机 pingVLAN6 内用户的任意一台主机，可以 ping 通则表示配置成功。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 6
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port link-type trunk
 port trunk allow-pass vlan 6
 port vlan-mapping vlan 10 map-vlan 6
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 6
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 6
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 5
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port link-type trunk
 port trunk allow-pass vlan 5
 port vlan-mapping vlan 10 map-vlan 5
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 5
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 10
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchD 的配置文件

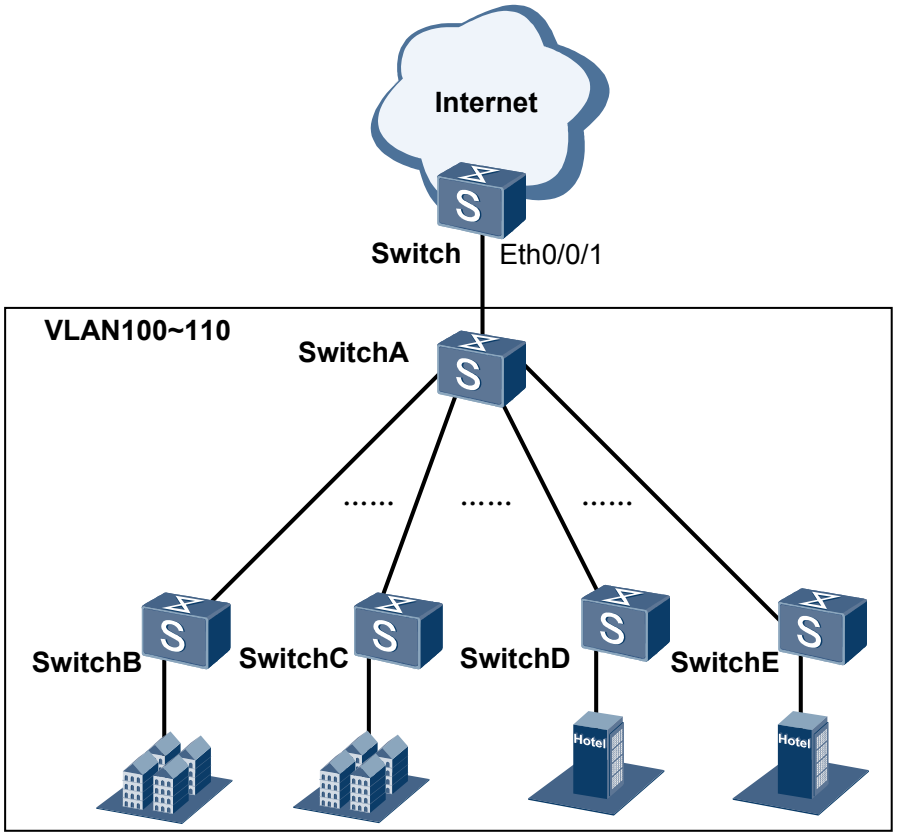
```
#
 sysname SwitchD
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

配置单层 Tag 的 VLAN Mapping 示例（N：1）

组网需求

在如图 3-26 所示的网络中，VLAN100 ～ 110 的用户通过运营商的汇聚交换机 Switch 与网络相连。

图 3-26 配置 VLAN Mapping 示例组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 VLAN Mapping：

1. 在 Switch 上创建映射前和映射后的 VLAN。
2. 在 Switch 上配置接口 GE0/0/1 以 Tagged 方式加入映射前和映射后的 VLAN。
3. 在 Switch 上配置接口 GE0/0/1 的 VLAN Mapping 功能。

数据准备

为完成此配置例，需准备如下的数据：

- 在 Switch 上创建映射前的 VLAN100 ～ 110。
- 在 Switch 上创建映射后的 VLAN10。

操作步骤

步骤 1 配置 Switch

创建 VLAN。

```
<Quidway> system-view
[Quidway] vlan batch 10 100 to 110
```

配置接口加入 VLAN。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 10 100 to 110
```

配置 VLAN Mapping 功能。

```
[Quidway-GigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-GigabitEthernet0/0/1] port vlan-mapping vlan 100 to 110 map-vlan 10
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 验证配置结果

VLAN100 ～ 110 的用户可以通过 Switch 正常访问网络。

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Quidway
#
vlan batch 10 100 to 110
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 10 100 to 110
 port vlan-mapping vlan 100 to 110 map-vlan 10
#
return
```

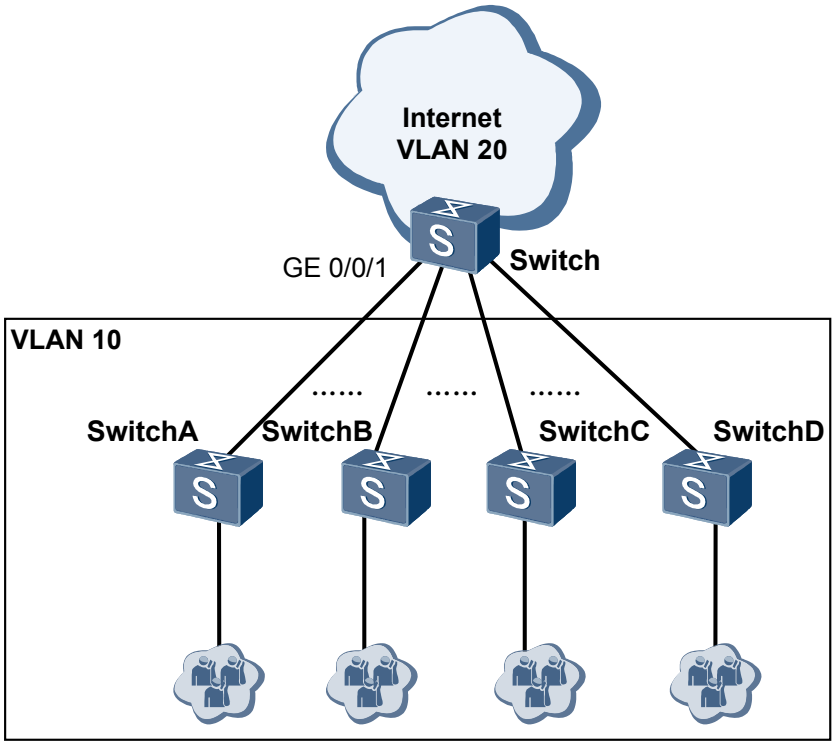
配置全局 VLAN Mapping 示例

版权所有 © 华为技术有限公司

组网需求

在如图 3-27 所示的网络中，VLAN10 的用户通过 Switch 与网络相连。

图 3-27 配置 VLAN Mapping 示例组网图



配置思路

采用如下的思路配置全局 VLAN Mapping：

1. 在 Switch 上创建映射前 VLAN 和映射后 VLAN。
2. 在 Switch 上配置接口 GE0/0/1 以 Tagged 方式加入映射后 VLAN。
3. 在 Switch 上配置接口 GE0/0/1 的 VLAN 转换功能。
4. Switch 的其他下行接口配置与 GE0/0/1 类似，此处不再赘述。
5. 在 Switch 上配置全局 VLAN Mapping 功能。

数据准备

为完成此配置举例，需准备如下的数据：

- 映射前 VLAN10。
- 映射后 VLAN20。

操作步骤

步骤 1 配置 Switch

创建 VLAN。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

配置接口加入 VLAN。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 10 20
```

#配置接口 VLAN 转换功能。

```
[Quidway-GigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-GigabitEthernet0/0/1] quit
```

配置 VLAN Mapping 功能。

```
[Quidway] vlan 10
[Quidway-vlan10] vlan-mapping map-vlan 20 remark-8021p 5
[Quidway-vlan10] quit
```

步骤 2 验证配置结果

VLAN10 的用户可以通过 Switch 正常访问网络。

----结束

配置文件

- Switch 的配置文件

```
#
sysname Quidway
#
vlan batch 10 20
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 20
 qinq vlan-translation enable
#
vlan-mapping map-vlan 20 remark-8021p 5
#
return
```

3.5 QinQ 配置

介绍 QinQ 的基本知识、配置方法和配置实例。

3.5.1 QinQ 概念

简要介绍 QinQ 的基本概念。

QinQ（802.1Q-in-802.1Q）协议是基于 IEEE 802.1Q 技术的一种二层隧道协议。由于在公网中传递的帧有两层 802.1Q Tag（一个公网 Tag，一个私网 Tag），所以称之为 QinQ 协议。

QinQ 的核心思想是将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，报文带着两层 Tag 穿越网络运营商的骨干网络，从而为用户提供一种较为简单的二层 VPN 隧道。

3.5.2 AC6605 支持的 QinQ 特性

介绍 QinQ 特性在 AC6605 中的支持情况。

版权所有 © 华为技术有限公司

灵活 QinQ 功能

AC6605 支持灵活 QinQ 功能，该功能是对 QinQ 的功能进行了扩展，使得接口可以灵活地根据帧的私网 VLAN ID 给它加上不同公网 VLAN ID 的外层 Tag，以达到区分不同用户的目的。

AC6605 不仅支持接口+VLAN 方式的灵活 QinQ 功能，还支持基于流的灵活 QinQ 功能。

基于流的灵活 QinQ 相关命令介绍请参考《AC6605 无线接入控制器 命令参考》中的 QoS 命令。

QinQ 外层协议的灵活配置

由于不同的厂商在实现 QinQ 功能时，公网外层 Tag 采用了不同的协议类型，为了能实现 AC6605 与其它厂商设备对接，AC6605 支持 QinQ 外层协议的灵活配置。

3.5.3 配置基于接口的 QinQ

介绍接口类型、外层 Tag 协议类型和基于接口 QinQ 的配置过程与步骤。

建立配置任务

应用环境

为了使私网与公网有效分离，并最大限度地节省 VLAN 资源。在 AC6605 提供的 QinQ 接口上，配置二层 802.1Q Tag。私网 Tag 用于内部网络（如企业网），公网 Tag 用于外部网络（如运营商的网络），从而最多可以提供 4094×4094 个 VLAN，并满足不同私网用户之间相同 VLAN 可以透明传输。

前置任务

无

数据准备

在配置基于接口的 QinQ 之前，需要准备以下数据。

序号	数据
1	QinQ 接口的编号
2	（可选）外层 VLAN Tag 的协议类型
3	外层 VLAN Tag 的 VLAN 编号

配置接口类型

背景信息

请在需要配置基于接口的 QinQ 的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type dot1q-tunnel**，配置接口类型为 dot1q-tunnel。

缺省情况下，接口的类型为 Hybrid。

当接口类型为 dot1q-tunnel 时，该接口不支持二层组播功能。

----结束

指定外层 VLAN Tag 的 VLAN ID

背景信息

请在需要配置基于接口的 QinQ 的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN。

步骤 3 执行命令 **quit**，退出 VLAN 视图。

步骤 4 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 5 执行命令 **port default vlan** *vlan-id*，配置外层 VLAN Tag 的 VLAN 编号（即接口的缺省 VLAN）。

----结束

检查配置结果

操作步骤

- 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口的 QinQ 配置。

----结束

3.5.4 配置灵活 QinQ

介绍接口类型、叠加后外层 VLAN 和灵活 QinQ 的配置过程与步骤。

建立配置任务

应用环境

为了让用户跨越运营商网络进行通信，需要添加外层 VLAN Tag。

版权所有 © 华为技术有限公司

前置任务

无

数据准备

在配置灵活 QinQ 之前，需要准备以下数据。

序号	数据
1	配置灵活 QinQ 功能的接口的编号
2	内层 VLAN Tag 的 VLAN 编号
3	外层 VLAN Tag 的 VLAN 编号

配置接口类型

背景信息

请在需要配置灵活 QinQ 的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type hybrid**，配置接口类型为 Hybrid。

缺省情况下，接口的类型为 Hybrid。

----结束

配置接口加入 VLAN

背景信息

请在需要配置灵活 QinQ 的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port hybrid untagged vlan** *vlan-id*，配置接口以 Untagged 方式加入叠加后的 VLAN。

叠加后的外层 VLAN 必须是设备上已经存在的 VLAN，叠加前的 VLAN 可以不创建。

----结束

版权所有 © 华为技术有限公司

配置灵活 QinQ

背景信息

端口学习 MAC 地址时，学习的是 QinQ 报文外层 VLAN 的 MAC 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **qinq vlan-translation enable**，使能接口 VLAN 转换功能。

步骤 4 执行命令 **port vlan-stacking vlan** *vlan-id1* [**to** *vlan-id2*] **stack-vlan** *vlan-id3* [**remark-8021p** *8021p-value*]，配置灵活 QinQ。其中：

- *vlan-id1* [**to** *vlan-id2*]表示配置待添加 VLAN Tag 的用户 VLAN 编号。
- **stack-vlan** *vlan-id3* 表示添加外层 VLAN Tag 的 VLAN 编号。
- [**remark-8021p** *8021p-value*]表示叠加后外层 VLAN 的内部优先级。
  缺省情况下，外层 VLAN 优先级与内层 VLAN 优先级保持一致。

----结束

检查配置结果

操作步骤

- 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口的灵活 QinQ 配置。

----结束

3.5.5 配置 VLANIF 接口支持 QinQ Stacking 功能

当用户需要从本端设备远程登录到远端设备上进行远端管理时，可在远端设备上的管理 VLAN 对应的 VLANIF 接口上部署 QinQ Stacking 功能实现。

建立配置任务

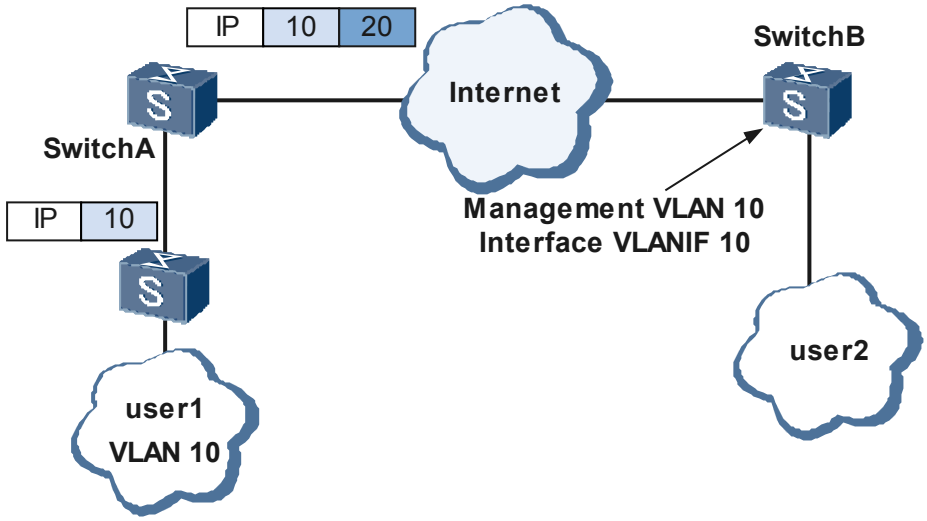
在进行 VLANIF 接口支持 QinQ Stacking 功能配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 3-28 所示，SwitchA 与远端设备 SwitchB 通过第三方网络互连。SwitchB 已经部署管理 VLAN，SwitchA 下挂的用户所属 VLAN ID 与管理 VLAN ID 一样。而运营商提供的 VLAN ID 与管理 VLAN ID（用户所属的 VLAN ID）不相同。

版权所有 © 华为技术有限公司

图 3-28 VLANIF 接口支持 QinQ Stacking 功能组网图



当用户需要从 SwitchA 远程登录到远端设备 SwitchB 上进行远端管理 VLAN 业务时，可在远端设备 SwitchB 上通过在管理 VLAN 对应的 VLANIF 接口上部署 VLAN Stacking 功能实现远程管理。

- 当 SwitchA 用户发送报文到 SwitchB 时：

  通过 SwitchA 的用户侧接口上部署 QinQ 功能，使上送到运营商网络的用户报文带有两层 VLAN Tag，外层 Tag 与运营商提供的 VLAN Tag 相同，以实现用户报文能够透传运营商网络到达远端 SwitchB。

  当部署了 QinQ Stacking 功能的 SwitchB 接收到带有两层 VLAN Tag 的用户报文时，与 VLANIF 接口上配置的两层 VLAN Tag 进行比较。当外层 VLAN Tag 一样时，将剥掉外层 VLAN Tag，将报文上送给 IP 层处理。
- 当 SwitchB 用户发送报文到 SwitchA 时：

  当部署了 QinQ Stacking 功能的 VLANIF 接口收到数据帧时，给数据帧打上一层 QinQ Stacking 功能配置的 VLAN Tag。新增的外层 VLAN Tag 与运营商提供的 VLAN Tag 保持一致。从而使带有两层 VLAN Tag 的报文透传运营商网络到达本端 SwitchA。本端 SwitchA 将外层 VLAN Tag 剥掉，报文最终到达 SwitchA 用户。

前置任务

在配置 VLANIF 接口支持 QinQ Stacking 功能之前，需要完成以下任务：

- 创建 VLAN
- 配置管理 VLAN

数据准备

在配置 VLANIF 接口支持 QinQ Stacking 功能之前，需准备以下数据。

序号	数据
1	VLAN 编号

版权所有 © 华为技术有限公司

配置 VLANIF 接口支持 QinQ Stacking 功能

在 VLANIF 接口上配置 QinQ Stacking 功能后，可实现 VLANIF 接口的 QinQ Stacking 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口。

创建 VLANIF 接口时，相关联的管理 VLAN 必须已经存在。

步骤 3 执行命令 **qinq stacking vlan** *vlan-id*，配置 QinQ Stacking 功能。

说明

- 在 VLANIF 接口上配置 QinQ Stacking 功能时，VLANIF 接口对应的 VLAN 必须是管理 VLAN。其他类型的 VLAN，创建 VLANIF 接口后均不支持配置 QinQ Stacking 功能。
- 执行本命令后，若需要修改新增外层 VLAN Tag，必须先执行命令 **undo qinq stacking vlan** 取消 QinQ Stacking 功能后再重新配置。
- 本命令与 **icmp host-unreachable send** 命令互斥，需要执行 **undo icmp host-unreachable send** 命令后才可以配置。

----结束

检查配置结果

VLANIF 接口上支持 QinQ Stacking 功能成功配置后，可实现用户从本端设备远程登录到远端设备上进行远端管理。

前提条件

已经完成 VLANIF 接口上支持 QinQ Stacking 功能的所有配置。

操作步骤

步骤 1 执行命令 **display vlan** [*vlan-id* [**verbose**]]，查看管理 VLAN 配置是否正确。

步骤 2 在 VLANIF 接口下执行命令 **display this**，查看 QinQ Stacking 配置是否正确。

----结束

3.5.6 配置外层 VLAN Tag 的协议类型

介绍配置接口类型、外层 Tag 的协议类型的过程与步骤。

建立配置任务

应用环境

为了实现与不同厂商的设备互通，接口的 QinQ 外层 VLAN Tag 协议类型应配置为和该接口相连的设备能够识别的协议类型。

版权所有 © 华为技术有限公司

前置任务

无

数据准备

在配置外层 VLAN Tag 的协议类型之前，需要准备以下数据。

序号	数据
1	接口的编号
2	外层 VLAN Tag 的协议类型

配置接口类型

背景信息

请在需要配置外层 VLAN Tag 协议类型的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type** { **hybrid** | **trunk** | **access** }，配置接口类型。

缺省情况下，接口的类型为 Hybrid。

----结束

配置外层 VLAN Tag 的协议类型

背景信息

请在需要配置外层 VLAN Tag 协议类型的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **qinq protocol** *protocol-id*，配置外层 VLAN Tag 的协议类型。

qinq protocol 命令不能在 QinQ 类型接口下配置。

qinq protocol 在入方向只会对报文起到识别作用,在出方向可以为报文打上 TPID 或者修改 TPID。

缺省情况下，外层 VLAN Tag 的协议类型为 0x8100。

版权所有 © 华为技术有限公司

说明

- 为了实现与不同厂商的设备互通，接口的 QinQ 外层 VLAN Tag 协议类型应配置为和该接口相连的设备能够识别的协议类型。
- 使用 **qinq protocol** 命令配置的协议类型不能与一些特定的协议类型编号相同，否则会导致接口不能正确区分相应类型的协议报文。如：协议类型不能配置为 0x0806（ARP 协议对应的协议号）。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口外层 VLAN Tag 的协议类型配置。

----结束

3.5.7 配置举例

介绍 QinQ 的各种组网举例。

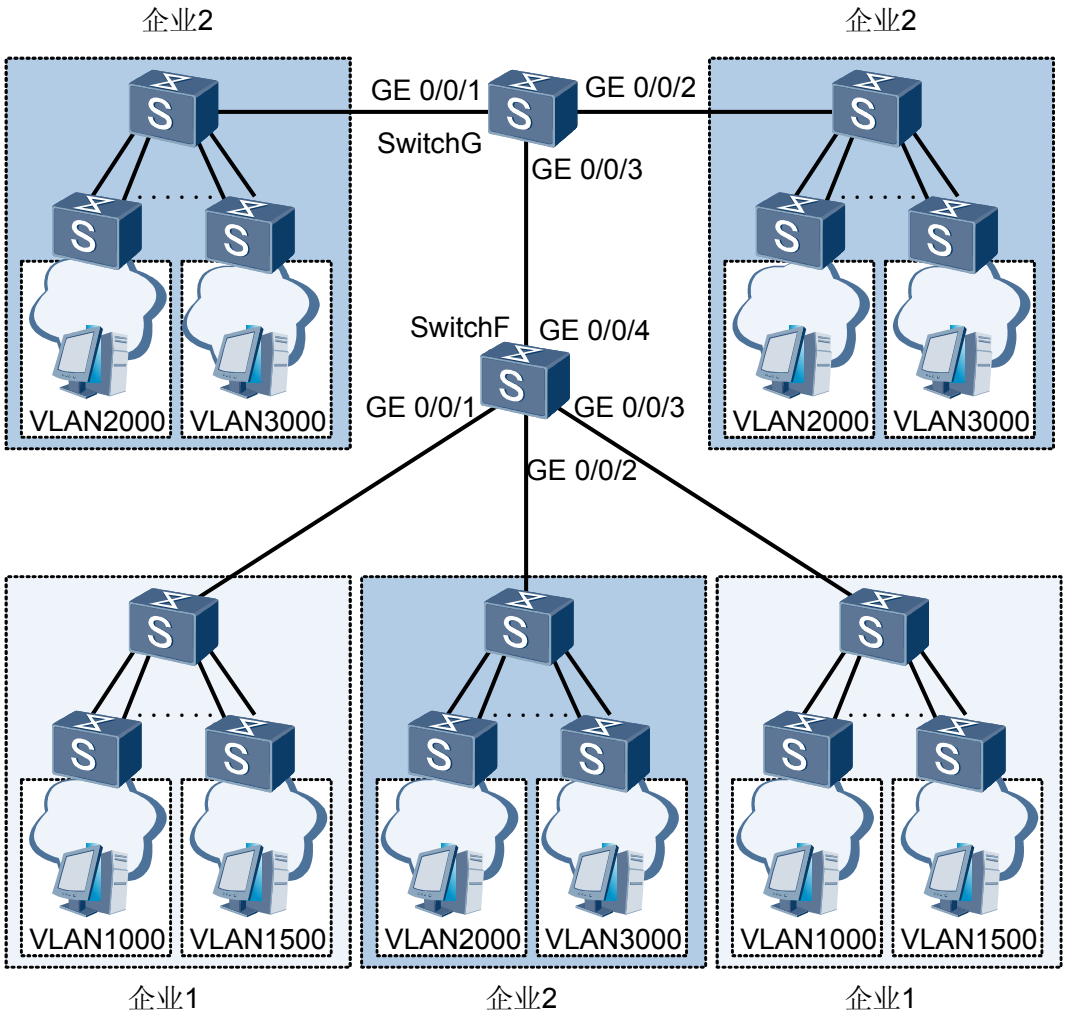
配置基于接口的 QinQ 示例

组网需求

如图 3-29 所示，网络中有两个大企业，企业 1 有两个办公地，企业 2 有三个办公地，这两个企业的各办公地的企业网都分别和运营商网络中的 SwitchG 或 SwitchF 相连。企业 1 的网络中使用 VLAN1000 ～ VLAN1500，企业 2 的网络中使用 VLAN2000 ～ VLAN3000。要求企业内部各办公地相同 VLAN 内用户可以通过运营商的网络互相通信，但两个企业之间互相隔离。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-29 配置基于接口的 QinQ 组网图



配置思路

采用如下的思路配置 QinQ：

1. 在 SwitchF 上创建 VLAN10 和 VLAN20，在 SwitchG 上创建 VLAN20。
2. 在 SwitchF 上配置接口 GE0/0/1、GE0/0/2、GE0/0/3 的类型为 QinQ。
3. 在 SwitchG 上配置接口 GE0/0/1、GE0/0/2 的类型为 QinQ。
4. 配置 SwitchF 的接口 GE0/0/4 和 SwitchG 的接口 GE0/0/3 以 Tag 方式加入 VLAN20。

数据准备

为完成此配置例，需准备如下的数据：

- 在运营商网络中企业 1 被划分在 VLAN10 中。
- 在运营商网络中企业 2 被划分在 VLAN20 中。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 VLAN

在 SwitchF 上创建 VLAN10 和 VLAN20。

```
<Quidway> system-view
[Quidway] sysname SwitchF
[SwitchF] vlan batch 10 20
```

在 SwitchG 上创建 VLAN20。

```
<Quidway> system-view
[Quidway] sysname SwitchG
[SwitchG] vlan 20
```

步骤 2 配置接口类型为 QinQ

在 SwitchF 上配置接口 GE0/0/1、GE0/0/2、GE0/0/3 类型为 QinQ，GE0/0/1、GE0/0/3 的外层 Tag 为 VLAN10，GE0/0/2 的外层 Tag 为 VLAN20。

```
[SwitchF] interface gigabitethernet 0/0/1
[SwitchF-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[SwitchF-GigabitEthernet0/0/1] port default vlan 10
[SwitchF-GigabitEthernet0/0/1] quit
[SwitchF] interface gigabitethernet 0/0/2
[SwitchF-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[SwitchF-GigabitEthernet0/0/2] port default vlan 20
[SwitchF-GigabitEthernet0/0/2] quit
[SwitchF] interface gigabitethernet 0/0/3
[SwitchF-GigabitEthernet0/0/3] port link-type dot1q-tunnel
[SwitchF-GigabitEthernet0/0/3] port default vlan 10
[SwitchF-GigabitEthernet0/0/3] quit
```

在 SwitchG 上配置接口 GE0/0/1、GE0/0/2 类型为 QinQ 接口，GE0/0/1、GE0/0/2 的外层 Tag 为 VLAN20。

```
[SwitchG] interface gigabitethernet 0/0/1
[SwitchG-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[SwitchG-GigabitEthernet0/0/1] port default vlan 20
[SwitchG-GigabitEthernet0/0/1] quit
[SwitchG] interface gigabitethernet 0/0/2
[SwitchG-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[SwitchG-GigabitEthernet0/0/2] port default vlan 20
[SwitchG-GigabitEthernet0/0/2] quit
```

步骤 3 配置其它接口

在 SwitchF 上配置接口 GE0/0/4 加入 VLAN20。

```
[SwitchF] interface gigabitethernet 0/0/4
[SwitchF-GigabitEthernet0/0/4] port link-type trunk
[SwitchF-GigabitEthernet0/0/4] port trunk allow-pass vlan 20
[SwitchF-GigabitEthernet0/0/4] quit
```

在 SwitchG 上配置接口 GE0/0/3 加入 VLAN20。

```
[SwitchG] interface gigabitethernet 0/0/3
[SwitchG-GigabitEthernet0/0/3] port link-type trunk
[SwitchG-GigabitEthernet0/0/3] port trunk allow-pass vlan 20
[SwitchG-GigabitEthernet0/0/3] quit
```

步骤 4 验证配置结果

从企业 1 任意办公地内任意 VLAN 的一台主机 ping 企业 1 其它工作地同一 VLAN 内的主机，如果可以 ping 通则表示企业 1 内部可以互相通信。

版权所有 © 华为技术有限公司

从企业 2 任意办公地内任意 VLAN 的一台主机 ping 企业 2 其它工作地同一 VLAN 内的主机，如果可以 ping 通则表示企业 2 内部可以互相通信。

从企业 1 任意办公地内的任意一台主机 ping 企业 2 内的主机，如果不能 ping 通则表示企业 1 和企业 2 是互相隔离的。

----结束

配置文件

以下仅给出 Switch 的配置文件。

- SwitchF 的配置文件

```
#
 sysname SwitchF
#
 vlan batch 10 20
#
interface GigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 20
#
interface GigabitEthernet0/0/3
 port link-type dot1q-tunnel
 port default vlan 10
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

- SwitchG 的配置文件

```
#
 sysname SwitchG
#
 vlan batch 20
#
interface GigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 20
#
interface GigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

配置灵活 QinQ 示例

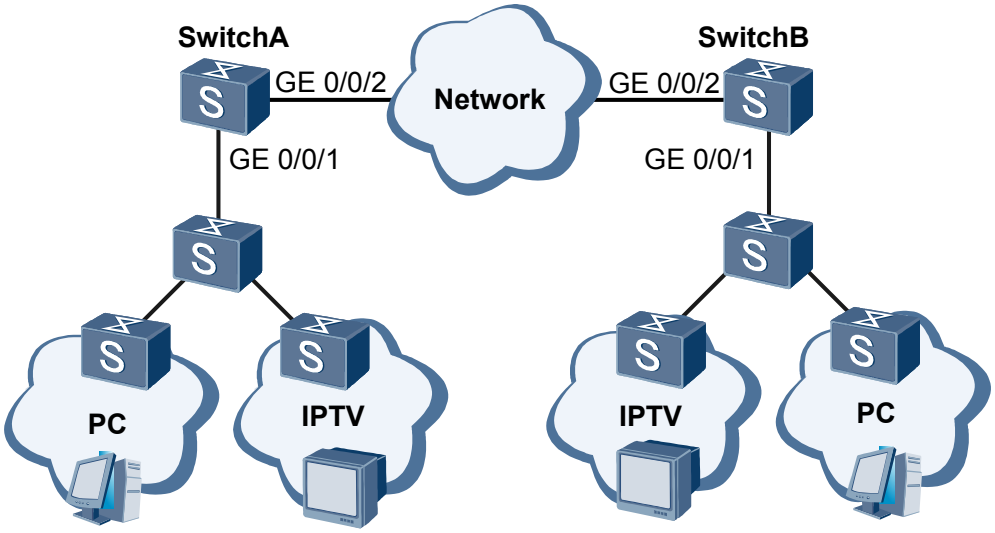
组网需求

如图 3-30 所示，PC 上网用户和 IPTV 用户通过 SwitchA 和 SwitchB 接入运营商网络，通过网络互相通信。

版权所有 © 华为技术有限公司

要求 PC 上网用户和 IPTV 用户分别以 VLAN2 和 VLAN3 通过网络。

图 3-30 配置灵活 QinQ 组网图



配置思路

采用如下的思路配置灵活 QinQ：

1. 在 SwitchA 和 SwitchB 上创建相关 VLAN。
2. 在 SwitchA 和 SwitchB 上配置接口类型并加入 VLAN。
3. 在 SwitchA 和 SwitchB 的接口上配置灵活 QinQ 功能。

数据准备

为完成此配置例，需准备如下的数据：

- PC 上网用户被划分在 VLAN100 ～ VLAN200 中。
- IPTV 用户被划分在 VLAN300 ～ VLAN400 中。
- 在公网中 PC 上网用户被划分到 VLAN2 中传输。
- 在公网中 IPTV 用户被划分到 VLAN3 中传输。

操作步骤

步骤 1 创建 VLAN

在 SwitchA 上创建 VLAN2、VLAN3，即叠加后的外层 VLAN。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 2 3
```

在 SwitchB 上创建 VLAN2、VLAN3，即叠加后的外层 VLAN。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 2 3
```

步骤 2 在接口上配置灵活 QinQ

配置 SwitchA 的接口 GE0/0/1。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SwitchA-GigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchA-GigabitEthernet0/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2
[SwitchA-GigabitEthernet0/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB 的接口 GE0/0/1。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SwitchB-GigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchB-GigabitEthernet0/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2
[SwitchB-GigabitEthernet0/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 3 配置其它接口

在 SwitchA 上配置接口 GE0/0/2 加入 VLAN2、VLAN3。

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SwitchA-GigabitEthernet0/0/2] quit
```

在 SwitchB 上配置接口 GE0/0/2 加入 VLAN2、VLAN3。

```
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SwitchB-GigabitEthernet0/0/2] quit
```

步骤 4 验证配置结果

查看 SwitchA 上各接口的配置信息。

```
<SwitchA> display current-configuration interface gigabitethernet 0/0/1
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
return
<SwitchA> display current-configuration interface gigabitethernet 0/0/2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

查看 SwitchB 上各接口的配置信息。

```
<SwitchB> display current-configuration interface gigabitethernet 0/0/1
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
```


版权所有 © 华为技术有限公司

```
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
return
<SwitchB> display current-configuration interface gigabitethernet 0/0/2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

如果 SwitchA、SwitchB 上配置正确，则：

- PC 上网用户可以通过运营商网络互相通信。
- IPTV 用户可以通过运营商网络互相通信。

----结束

配置文件

以下仅给出 Switch 的配置文件。

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2 to 3
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2 to 3
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

配置灵活 QinQ 示例-VLAN Mapping 接入

组网需求

如图 3-31 所示，家庭网关连接的用户业务有 PC 上网业务、IPTV 业务、VoIP 业务。

版权所有 © 华为技术有限公司

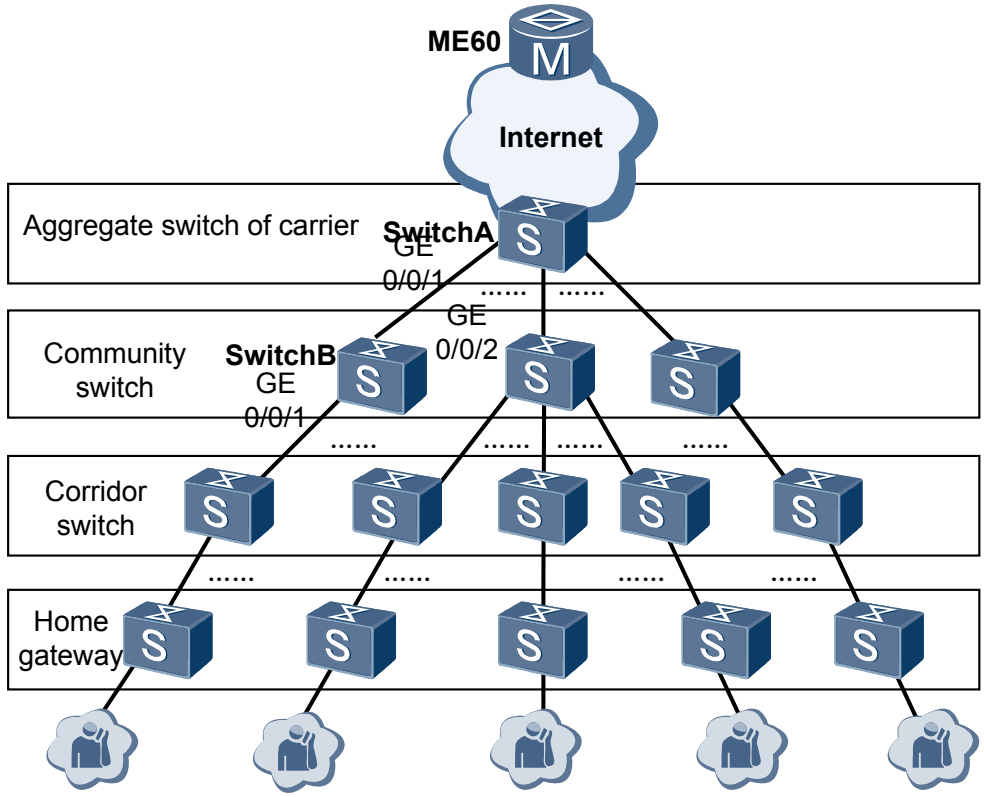
楼道交换机分配各种业务的 VLAN 为：

- PC 上网业务独立的 VLAN：VLAN1000 ～ VLAN1100
- IPTV 业务共享的 VLAN：VLAN1101
- VoIP 业务共享的 VLAN：VLAN1102
- 家庭网关共享的 VLAN：VLAN1103

每个小区交换机下行与 50 个楼道交换机相连，对楼道交换机上送的 PC 上网业务 VLAN 分别映射为 VLAN101、VLAN102、VLAN103、……VLAN150。

运营商的汇聚交换机下行与 50 个小区交换机相连，对小区交换机上送的报文添加外层 VLAN，分别为：VLAN21、VLAN22、VLAN23、……VLAN70。

图 3-31 配置灵活 QinQ 组网图



配置思路

采用如下的思路配置灵活 QinQ 以及 VLAN Mapping：

1. 在 SwitchA 和 SwitchB 上创建相关 VLAN。
2. 在 SwitchB 上配置 VLAN Mapping 功能，并将接口加入 VLAN。
3. 在 SwitchA 上配置灵活 QinQ 功能，并将接口加入 VLAN。
4. SwitchA 和 SwitchB 的其他下行接口配置与 GE0/0/1 类似，此处不再赘述。
5. SwitchA 的其他下行小区交换机配置与 SwitchB 类似，此处不再赘述。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- 在 SwitchB 上配置接口 GE0/0/1 以 Tagged 方式加入 VLAN1000 ～ VLAN1100、VLAN1101、VLAN1102、VLAN1103、VLAN101。
- 在 SwitchB 上配置接口 GE0/0/2 以 Tagged 方式加入 VLAN101 ～ VLAN150、VLAN1101、VLAN1102、VLAN1103。
- 在 SwitchA 上配置接口 GE0/0/1 以 Tagged 方式加入 VLAN1101、VLAN1102、VLAN1103。
- 在 SwitchA 上配置接口 GE0/0/1 以 Untagged 方式加入 VLAN21。
- 在 SwitchB 接口 GE0/0/1 上配置 VLAN Mapping 功能。
- 在 SwitchA 接口 GE0/0/1 上配置灵活 QinQ 功能。

操作步骤

步骤 1 配置 SwitchA

创建 VLAN

```
<Quidway> system-view
[Quidway] vlan batch 21 to 70 1101 to 1103
```

配置接口加入 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 21
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 1101 to 1103
[Quidway-GigabitEthernet0/0/1] quit
```

配置接口灵活 QinQ 功能

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-GigabitEthernet0/0/1] port vlan-stacking vlan 101 to 150 stack-vlan 21
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 配置 SwitchB

创建 VLAN

```
<Quidway> system-view
[Quidway] vlan batch 101 to 150 1000 to 1103
```

配置接口加入 VLAN

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 101 1000 to 1103
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid tagged vlan 101 to 150 1101 to 1103
[Quidway-GigabitEthernet0/0/2] quit
```

配置接口 VLAN Mapping 功能

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-GigabitEthernet0/0/1] port vlan-mapping vlan 1000 to 1100 map-vlan 101
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 3 检查配置结果

版权所有 © 华为技术有限公司

PC 上网业务、IPTV 业务、VoIP 业务都可以正常使用。

----结束

配置文件

SwitchA 配置文件。

```
#
 sysname Quidway
#
 vlan batch 21 to 70 1101 to 1103
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 1101 to 1103
 port hybrid untagged vlan 21
 port vlan-stacking vlan 101 to 150 stack-vlan 21
#
return
```

SwitchB 配置文件。

```
#
 sysname Quidway
#
 vlan batch 101 to 150 1000 to 1103
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 101 1000 to 1103
 port vlan-mapping vlan 1000 to 1100 map-vlan 101
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 101 to 150 1101 to 1103
#
return
```

配置 VLANIF 接口支持 QinQ Stacking 示例

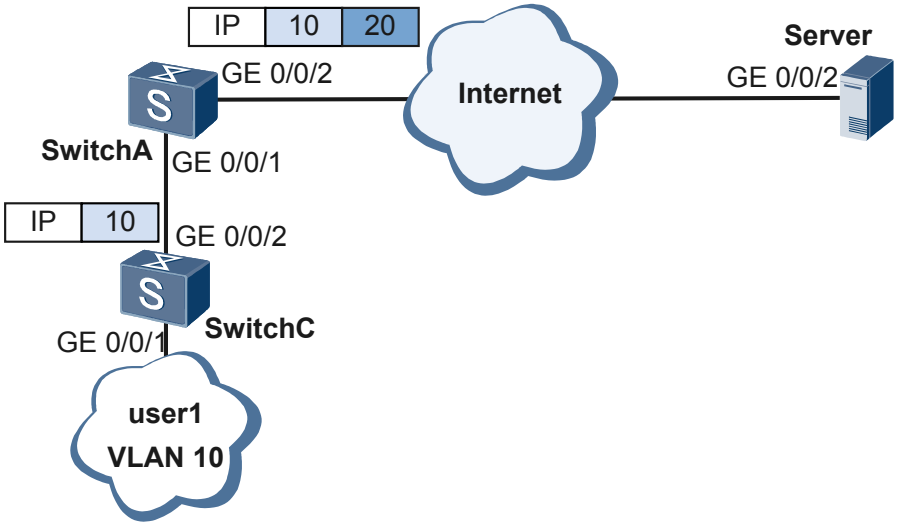
该组网的特点是远端设备 Server 已经部署管理 VLAN，本端设备 SwitchA 下挂的用户所属 VLAN ID 与管理 VLAN ID 一样。而运营商提供的 VLAN ID 与管理 VLAN ID（用户所属的 VLAN ID）不相同。当用户需要从 SwitchA 上远程登录到 Server 上进行远端管理 VLAN 业务时，可通过本示例实现。

组网需求

如图 3-32 所示，SwitchA 与远端设备 Server 通过第三方网络互连。Server 已经部署管理 VLAN，SwitchA 下挂的用户所属 VLAN ID 与管理 VLAN ID 一样。而运营商提供的 VLAN ID 与管理 VLAN ID（用户所属的 VLAN ID）不相同。

版权所有 © 华为技术有限公司

图 3-32 VLANIF 接口支持 QinQ Stacking 功能组网图



当用户需要从 SwitchA 远程登录到远端设备 Server 上进行远端管理业务时，可在远端设备 Server 上通过在管理 VLAN 对应的 VLANIF 接口上部署 QinQ Stacking 功能实现远程管理。

说明

在 VLANIF 接口上配置 QinQ Stacking 功能时，VLANIF 接口对应的 VLAN 必须是管理 VLAN。其他类型的 VLAN，创建 VLANIF 接口后均不支持配置 QinQ Stacking 功能。

配置思路

采用如下的思路配置 VLANIF 接口支持 QinQ Stacking：

1. 在 SwitchA 上配置 QinQ 功能。
2. 在 Server 上进行如下配置：
   a. 创建 VLAN10，并配置为管理 VLAN。
   b. 在对应的管理 VLAN 下，配置 VLANIF 接口。
   c. 在 VLANIF 接口下，配置 QinQ Stacking 功能。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 为用户数据报文所打的外层 Tag 值。
- Server 上管理 VLAN ID。

操作步骤

步骤 1 配置 SwitchC

允许接口 GE0/0/1 和 GE0/0/2 通过 VLAN10 报文。

```
<Quidway> system-view
[Quidway] sysname SwitchC
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[SwitchC] vlan batch 10
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port hybrid tagged vlan 10
[SwitchC-GigabitEthernet0/0/2] quit
```

步骤 2 配置 SwitchA

配置 QinQ 功能，使 SwitchA 发送到 Server 的报文带有两层 Tag。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 20
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port vlan-stacking vlan 10 stack-vlan 20
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port hybrid tagged vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤 3 配置 Server

允许接口 GE0/0/2 通过 VLAN20 报文。

```
<Quidway> system-view
[Quidway] sysname Server
[Server] vlan batch 10 20
[Server] interface gigabitethernet 0/0/2
[Server-GigabitEthernet0/0/2] port hybrid tagged vlan 20
[Server-GigabitEthernet0/0/2] quit
```

配置 QinQ Stacking 功能。

```
[Server] vlan 10
[Server-vlan10] management-vlan
[Server-vlan10] quit
[Server] interface vlanif 10
[Server-Vlanif10] undo icmp host-unreachable send
[Server-Vlanif10] qinq stacking vlan 20
[Server-Vlanif10] ip address 10.10.10.1 24
[Server-Vlanif10] quit
[Server] interface gigabitethernet 0/0/2
[Server-GigabitEthernet0/0/2] port hybrid tagged vlan 10 20
```

步骤 4 检查配置结果

从 SwitchA 可以远程登录到 Server 上，实现远程管理 VLAN 业务。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 20
#
interface GigabitEthernet 0/0/1
 port hybrid untagged vlan 20
 port vlan-stacking vlan 10 stack-vlan 20
#
interface GigabitEthernet 0/0/2
 port hybrid tagged vlan 20
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10
#
interface GigabitEthernet 0/0/1
 port hybrid tagged vlan 10
#
interface GigabitEthernet 0/0/2
 port hybrid tagged vlan 10
#
return
```

- Server 的配置文件

```
#
 sysname Server
#
 vlan batch 10 20
#
vlan 10
 management-vlan
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
 undo icmp host-unreachable send
 qinq stacking vlan 20
#
interface GigabitEthernet 0/0/2
 port hybrid tagged vlan 10 20
#
return
```

3.6 GVRP 配置

介绍了 GVRP 的基本知识、GVRP 配置方法和配置实例。

3.6.1 GVRP 概述

简要介绍 GVRP 和 GARP 的基本概念。

GVRP 简介

GARP VLAN 注册协议 GVRP（GARP VLAN Registration Protocol）是通用属性注册协议 GARP（Generic Attribute Registration Protocol）的一种应用，下面先介绍一下 GARP 的相关内容。

GARP 简介

GARP 提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息（如 VLAN、组播地址等）。

GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用实体称为 GARP 应用，GVRP 就是 GARP 的一种应用。当 GARP 应用实体存在于设备的某个接口上时，该接口对应于一个 GARP 应用实体。

- GARP 消息和定时器

版权所有 © 华为技术有限公司

- GARP 消息

  GARP 成员之间的信息交换借助于消息的传递来完成，主要有三类消息起作用，分别为 Join 消息、Leave 消息和 LeaveAll 消息。

  - 当一个 GARP 应用实体希望其它设备注册自己的属性信息时，它将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GARP 应用实体进行注册时，它也会向外发送 Join 消息。
  - 当一个 GARP 应用实体希望其它设备注销自己的属性信息时，它将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性后，它也会向外发送 Leave 消息。
  - 每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GARP 应用实体将对外发送 LeaveAll 消息，LeaveAll 消息用来注销所有的属性，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。

  Join 消息、Leave 消息与 LeaveAll 消息配合确保信息的重新注册或注销。

  通过消息交互，所有待注册的属性信息可以传播到同一局域网配置了 GARP 的所有设备上。

- GARP 定时器

  GARP 消息发送的时间间隔是通过定时器来实现的，GARP 定义了四种定时器，用于控制 GARP 消息的发送周期：

  - Hold 定时器：当 GARP 应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条 Join 消息对外发送，而是启动 Hold 定时器，当该定时器超时后，GARP 应用实体将此时段内收到的所有注册信息放在同一个 Join 消息中向外发送，从而节省带宽资源。
  - Join 定时器：GARP 应用实体可以通过将每个 Join 消息向外发送两次来保证消息的可靠传输，在第一次发送的 Join 消息没有得到回复的时候，GARP 应用实体会第二次发送 Join 消息。两次 Join 消息发送之间的时间间隔用 Join 定时器来控制。
  - Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 消息，则注销该属性信息。
  - LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

  说明

  - GARP 定时器的值将应用于所有在同一局域网内运行的 GARP 应用（如 GVRP）。
  - Hold 定时器、Join 定时器和 Leave 定时器的值可以在每个接口单独进行设置；而 LeaveAll 定时器只需在设备的全局进行设置即可，设置完成后，该值将在设备的所有接口上生效。
  - 在全网有多台设备的情况下，各个设备的 LeaveAll 定时器的取值可能不相同，但各设备都将以全网最小的 LeaveAll 定时器为准发送 LeaveAll 消息。因为每次发送 LeaveAll 消息时，当其它设备接收到之后都会清零 LeaveAll 定时器，因此即使全网存在很多不同的 LeaveAll 定时器，也只有最小的那个 LeaveAll 定时器起作用。

- GARP 运行过程

  通过 GARP 机制，一个 GARP 成员上的配置信息会迅速传播到整个局域网。GARP 成员可以是终端工作站或网桥。GARP 成员通过声明或回收声明来通知其它的 GARP 成员注册或注销自己的属性信息，并根据其它 GARP 成员的声明或回收声明注册或注销对方的属性信息。当接口接收到一个属性声明时，该接口将注册该属性，如果接口接收到回收属性的声明，该接口将注销该属性。

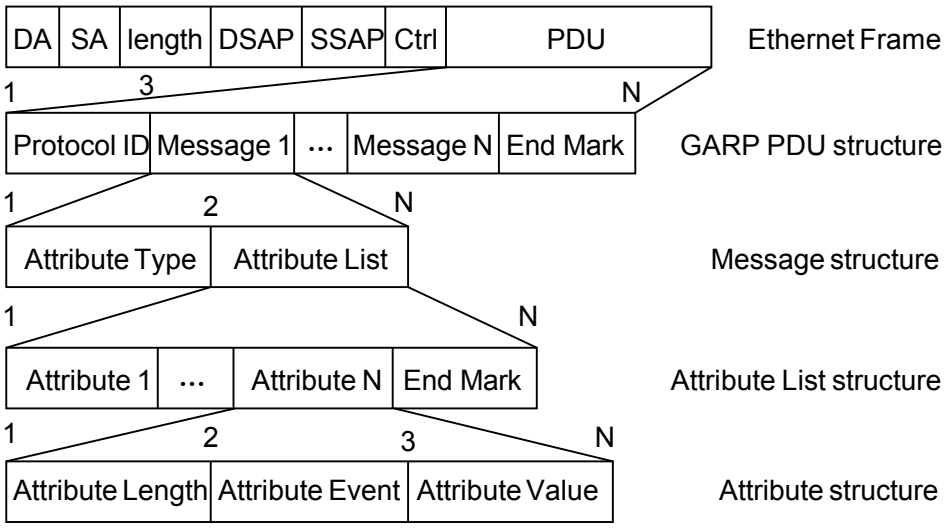
版权所有 © 华为技术有限公司

GARP 应用实体的协议数据报文以特定的组播 MAC 地址为目的 MAC。设备在接收到 GARP 应用实体的报文后，会根据其目的 MAC 地址加以区分并交给不同的 GARP 应用（如 GVRP）去处理。

- GARP 的报文格式

  GARP 的报文格式如图 3-33 所示。

图 3-33 GARP 报文格式



各个字段的说明如下表所示。

字段	含义	取值
Protocol ID	协议 ID。	取值为 1。
Message	消息，每个 Message 由 Attribute Type、Attribute List 构成。	-
Attribute Type	属性类型，由具体的 GARP 的应用定义。	对于 GVRP，属性类型为 0x01，表示属性取值为 VLAN ID。
Attribute List	属性列表，由多个属性构成。	-
Attribute	属性，每个属性由 Attribute Length、Attribute Event、Attribute Value 构成。	-
Attribute Length	属性长度。	取值 2 ～ 255，单位为字节。

华为专有和保密信息
版权所有 © 华为技术有限公司

字段	含义	取值
Attribute Event	属性描述的事件。	● 0：LeaveAll Event ● 1：JoinEmpty Event ● 2：JoinIn Event ● 3：LeaveEmpty Event ● 4：LeaveIn Event ● 5：Empty Event
Attribute Value	属性取值。	GVRP 的属性取值为 VLAN ID，但 LeaveAll 属性的 Attribute Value 值无效。
End Mark	结束标志、GARP 的 PDU 的结尾标志。	以 0x00 取值表示。

3.6.2 AC6605 支持的 GVRP 特性

介绍 GVRP 特性在 AC6605 中的支持情况。

GVRP 是 GARP 的一种应用。它基于 GARP 的工作机制，维护设备中的 VLAN 动态注册信息，并传播该信息到其它的设备中。

设备启动 GVRP 特性后，能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个接口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以便使同一局域网内所有设备的 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

GVRP 的接口注册模式有三种：

- Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动创建的那部分。
- Forbidden 模式：禁止该接口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何的 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN1。

说明

AC6605 最多支持 4094 个动态 VLAN。

GVRP 功能只能运行在 MSTP 的 CIST 实例上，并且在 CIST 实例上被 MSTP 阻塞的接口不能收发 GVRP 报文。

3.6.3 配置 GVRP 功能

介绍配置 GVRP 功能的过程与步骤。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

在某些复杂的二层网络中，配置 GVRP 功能可以使接口动态加入或退出 VLAN 以简化配置。

前置任务

在配置 GVRP 功能之前，需完成以下任务：

- 接口已加入所有 VLAN。
- 确认已经配置了接口上送 BPDU 报文到 CPU 处理的功能。

数据准备

在配置 GVRP 功能之前，需准备以下数据。

序号	数据
1	（可选）GVRP 接口的注册模式
2	（可选）GARP 定时器时长

使能 GVRP 功能

背景信息

请在需要使能 GVRP 功能的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **gvrp**，使能全局 GVRP 功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **port link-type trunk**，配置接口为 Trunk 类型。

步骤 5 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置接口加入 VLAN。

步骤 6 执行命令 **gvrp**，使能接口 GVRP 功能。

缺省情况下，全局和接口的 GVRP 功能都处于关闭状态。

说明

- 在开启接口 GVRP 功能之前，必须先开启全局 GVRP 功能。
- 开启接口 GVRP 功能必须在 Trunk 接口操作。

----结束

版权所有 © 华为技术有限公司

（可选）配置 GVRP 接口注册模式

背景信息

GVRP 的接口注册模式有三种：

- Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动创建的那部分。
- Forbidden 模式：禁止该接口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何的 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN1。

说明

配置 GVRP 接口注册模式之前，需要先使能接口的 GVRP 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **gvrp registration** { **fixed** | **forbidden** | **normal** }，配置 GVRP 接口注册模式。

缺省情况下，GVRP 接口注册模式为 **normal**。

----结束

（可选）配置 GARP 定时器功能

背景信息

每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其他 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

在全网有多台设备的情况下，各个设备的 LeaveAll 定时器的取值可能不相同，但每台设备都将以全网最小的 LeaveAll 定时器为准发送 LeaveAll 消息。因为每次 LeaveAll 定时器超时后发送 LeaveAll 消息，其它的设备接收到之后都会清零 LeaveAll 定时器，因此即使全网存在很多不同的 LeaveAll 定时器，也只有最小的那个 LeaveAll 定时器起作用。

使用命令 **garp timer** 设置接口的 GARP 定时器时，需要注意以下几点：

- **undo garp timer** 命令用来恢复接口的 GARP 定时器的值为缺省值。如果缺省值不满足取值范围的要求，则 **undo garp timer** 命令无效。
- 各个定时器的取值范围会由于其他定时器取值的改变而改变。如果用户想要设置的定时器的值不在当前可以设置的取值范围内，可以通过改变相关定时器的取值实现。
- 如果用户想恢复各定时器的值为缺省值，可以先恢复 **Hold** 定时器的值为缺省值，然后再依次恢复 **Join**、**Leave**、**LeaveAll** 定时器的值为缺省值。

版权所有 © 华为技术有限公司

说明

在实际组网中，建议用户将 GVRP 定时器配置为以下的推荐值：

- GARP Hold 定时器：100 厘秒（1 秒钟）
- GARP Join 定时器：600 厘秒（6 秒钟）
- GARP Leave 定时器：3000 厘秒（30 秒钟）
- GARP LeaveAll 定时器：12000 厘秒（2 分钟）

当动态 VLAN 数增加时，定时器的时间也需要相应的增加。

请在需要配置 GARP 定时器的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **garp timer leaveall** *timer-value*，配置 GARP 的 LeaveAll 定时器的值。

缺省情况下，LeaveAll 定时器的值为 1000 厘秒，即 10 秒。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **garp timer** { **hold** | **join** | **leave** } *timer-value*，配置接口 **Hold** 定时器、**Join** 定时器、**Leave** 定时器的值。

缺省情况下，**Hold** 定时器的值为 10 厘秒，**Join** 定时器的值为 20 厘秒，**Leave** 定时器的值为 60 厘秒。

----结束

检查配置结果

操作步骤

- 使用命令 **display gvrp status** 查看全局 GVRP 的开启或关闭状态信息。
- 使用命令 **display gvrp statistics** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]查看接口的 GVRP 统计信息。
- 使用命令 **display garp timer** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]查看 GARP 定时器的值。

----结束

3.6.4 维护

介绍清除 GARP 统计信息的方法。

清除 GARP 统计信息

版权所有 © 华为技术有限公司

背景信息

注意

清除 GARP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在用户视图下使用命令 **reset garp statistics** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]清除接口的 GARP 统计信息。

----结束

3.6.5 配置举例

介绍了 GVRP 的典型组网配置。

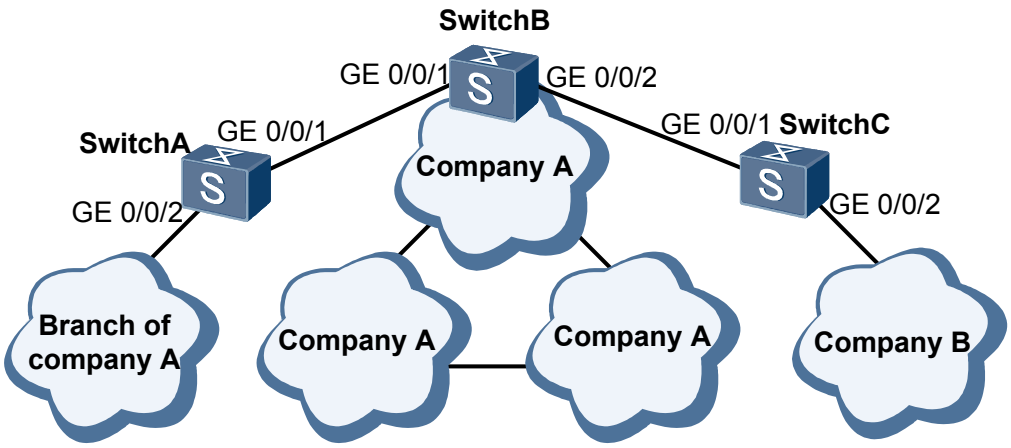
配置 GVRP 示例

组网需求

如图 3-34 所示，公司 A 的分公司与总部通过 SwitchA 和 SwitchB 互通，公司 A 的所有交换机配置 GVRP 功能并配置接口注册模式为 Normal，以简化配置。

公司 B 通过 SwitchB 和 SwitchC 与公司 A 互通，公司 B 的所有交换机配置 GVRP 功能并将与公司 A 相连的接口的注册模式配置为 Fixed，以控制只允许公司 B 配置的 VLAN 通过。

图 3-34 配置 GVRP 的组网图



配置思路

采用如下的思路配置 GVRP：

版权所有 © 华为技术有限公司

1. 全局使能 GVRP 功能。
2. 配置接口类型为 Trunk 类型。
3. 使能接口的 GVRP 功能。
4. 配置接口注册模式。

数据准备

为完成此配置例，需准备如下的数据：

- 在 SwitchA、SwitchB 和 SwitchC 上配置接口允许所有 VLAN 通过。
- 在 SwitchA 和 SwitchB 上配置接口的注册模式为 Normal。
- 在 SwitchC 上配置接口 GE0/0/1 的注册模式为 Fixed，配置接口 GE0/0/2 的注册模式为 Normal。
- 在 SwitchC 上创建属于公司 B 的 VLAN101 ～ VLAN200。

操作步骤

步骤 1 配置交换机 SwitchA

全局使能 GVRP 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] gvrp
```

配置接口为 Trunk 类型，并允许所有 VLAN 通过。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan all
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan all
[SwitchA-GigabitEthernet0/0/2] quit
```

使能接口的 GVRP 功能，并配置接口注册模式。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] gvrp
[SwitchA-GigabitEthernet0/0/1] gvrp registration normal
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] gvrp
[SwitchA-GigabitEthernet0/0/2] gvrp registration normal
[SwitchA-GigabitEthernet0/0/2] bpdu enable
[SwitchA-GigabitEthernet0/0/2] quit
```

SwitchB 配置与 SwitchA 配置类似，这里不再赘述。

步骤 2 配置交换机 SwitchC

创建 VLAN101 ～ VLAN200。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 101 to 200
```

全局使能 GVRP 功能。

```
[SwitchC] gvrp
```


版权所有 © 华为技术有限公司

配置接口为 Trunk 类型，并允许所有 VLAN 通过。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan all
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan all
[SwitchC-GigabitEthernet0/0/2] quit
```

使能接口的 GVRP 功能，并配置接口注册模式。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] gvrp
[SwitchC-GigabitEthernet0/0/1] gvrp registration fixed
[SwitchC-GigabitEthernet0/0/1] bpdu enable
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] gvrp
[SwitchC-GigabitEthernet0/0/2] gvrp registration normal
[SwitchC-GigabitEthernet0/0/2] bpdu enable
[SwitchC-GigabitEthernet0/0/2] quit
```

步骤 3 验证配置结果

配置完成后，公司 A 的分公司用户可以与总部互通，公司 A 属于 VLAN101 ～ VLAN200 的用户可以与公司 B 用户互通。

在 SwitchA 上使用命令 **display gvrp status**，查看全局 GVRP 的使能情况，结果如下：

```
<SwitchA> display gvrp status
 GVRP is enabled
```

在 SwitchA 上使用命令 **display gvrp statistics**，查看接口的 GVRP 统计信息，其中包括：GVRP 状态、GVRP 注册失败次数、上一个 GVRP 数据单元源 MAC 地址和接口 GVRP 注册类型，结果如下：

```
<SwitchA> display gvrp statistics
 GVRP statistics on port GigabitEthernet0/0/1
 GVRP status                     : Enabled
 GVRP registrations failed       : 0
 GVRP last PDU origin            : 0000-0000-0000
 GVRP registration type          : Normal
```

SwitchB 和 SwitchC 的查看方法与 SwitchA 类似，这里不再赘述。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 gvrp
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 gvrp
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 101 to 200
#
 gvrp
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
 gvrp registration fixed
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

3.7 MAC 表配置

介绍了 MAC 表的基本知识、配置方法和配置实例。

3.7.1 MAC 表概述

简要介绍 MAC 表的基本概念、生成方式、表项分类和基于 MAC 表的报文转发。

MAC 表的定义

AC6605 内存有一张 MAC 地址表，简称 MAC 表。MAC 表用于存放 AC6605 所学习到的其它设备的 MAC 地址、VLAN 编号和出接口（即发送该数据的接口）。在转发数据时，AC6605 根据数据帧中的目的 MAC 地址和 VLAN 编号查询 MAC 表，快速定位出接口，从而减少广播。

MAC 表的生成方式

- 自动生成 MAC 地址表项:一般情况下，MAC 地址表是设备通过源 MAC 地址学习过程而自动建立的。为适应网络的变化，MAC 地址表需要不断更新。MAC 地址表

版权所有 © 华为技术有限公司

中自动生成的表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称作老化时间。如果在到达生存周期前纪录被刷新，则该表项的老化时间重新计算。

- 手工配置 MAC 地址表项:设备通过源 MAC 地址学习自动建立 MAC 地址表时，无法区分合法用户和黑客用户的报文，带来了安全隐患。如果黑客用户将攻击报文的源 MAC 地址伪装成合法用户的 MAC 地址，并从设备的其它接口进入，设备就会学习到错误的 MAC 地址表项，于是就会将本应转发给合法用户的报文转发给黑客用户。为了提高接口安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止假冒身份的非法用户骗取数据。手工配置的 MAC 地址表项优先级高于自动生成的表项。

MAC 表的分类

MAC 地址表项分为动态表项、静态表项和黑洞表项。

- 动态表项：由接口自己通过源 MAC 地址学习获得，但需保证源 MAC 地址学习功能处于打开状态。
- 静态表项：由用户手工配置，静态 MAC 地址表项优先级高于动态表项。
- 黑洞表项：由用户手工配置，用于丢弃含有特定源 MAC 地址或目的 MAC 地址的数据帧。黑洞 MAC 地址表项优先级高于动态表项。

基于 MAC 表的报文转发

设备在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

- 单播方式：当 MAC 地址表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文从该表项中的转发出接口发送。
- 广播方式：当设备收到的报文为广播报文、组播报文或 MAC 地址表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外的所有接口转发。

3.7.2 AC6605 支持的 MAC 表特性

本章节介绍了 MAC 表特性在 AC6605 中的支持情况以及配置逻辑，理解配置逻辑后，您可以更快速准确地完成配置任务。

1. 用户可对 AC6605 的 MAC 表项进行配置，来提高设备的安全性，控制 MAC 表的规模。
   - 配置静态 MAC 表项：将一些固定的上行设备或信任用户的 MAC 地址配置为静态 MAC 表项，可以保证其安全通信。
   - 配置黑洞 MAC 表项：可以防止黑客通过 MAC 地址攻击网络。
   - 配置动态 MAC 表项老化时间：合理配置动态 MAC 表项的老化时间，可以防止 MAC 地址表项爆炸式增长。
2. 为了满足安全性要求和一些特殊场合的应用，还支持如下扩展功能的配置：
   - 配置禁止 MAC 地址学习功能:适用于网络环境固定的场景或已经明确了转发路径的场景。可以限制非信任用户接入，防止 MAC 地址攻击，提高网络安全性。
   - 限制 MAC 地址学习数量：在安全性比较差的网络中，可用于防止变换 MAC 地址攻击。
   - 配置接口安全：在安全性要求较高的网络中，在接口上配置接口安全功能，可阻止其他非信任的主机通过本接口和交换机通信，增强设备安全性。

版权所有 © 华为技术有限公司

- MAC 地址防漂移：对于固定的上行设备或服务器，可提高接口的优先级，防止伪造 MAC 地址攻击。
- MAC 地址漂移检测功能：配置 MAC 地址漂移检测功能可减少网络环路对本设备的影响。
- 配置丢弃全零 MAC 地址报文：当网络中的一些主机或设备发生故障时，会向 AC6605 发送源 MAC 或目的 MAC 地址为全零的报文，配置该功能可丢弃这些全零报文并上报告警，管理员可根据告警信息来定位故障设备。
- 配置 MAC 刷新 ARP 功能：配置 MAC 刷新 ARP 功能后，如果 MAC 表项的出接口变化，会及时更新 ARP 表项。
- 配置端口桥功能：配置端口桥功能后，接口将处理同源同宿报文，适用于 AC6605 下挂无二层转发能力的设备或 AC6605 作为数据中心的接入设备的网络场景。

禁止 MAC 地址学习

开启 MAC 地址学习功能时，收到来自周边设备的以太网帧，解析出源 MAC 地址，结合接收该以太网帧的接口，在 MAC 地址表项中添加新表项。以后 AC6605 接收到去往该目的 MAC 地址的以太网帧时，直接查询 MAC 地址表项就可以得到正确的发送接口，可以避免广播。

关闭 MAC 地址学习功能后，设备将不会再从该接口学习新的 MAC 地址。

限制 MAC 地址学习数量

AC6605 支持基于接口、VLAN 的 MAC 地址学习限制功能。当学习到的 MAC 表项达到限制数目时不再学习 MAC 地址，还可以配置告警功能来提醒网络管理员，防止黑客通过 MAC 地址攻击用户设备或网络。

接口安全

接口安全功能是将交换机接口学习到的 MAC 地址变为安全动态 MAC 地址或 Sticky MAC 地址，可以阻止其他非信任的 MAC 主机通过本接口和交换机通信，增强设备安全性。

安全动态 MAC 与 Sticky MAC 区别如下：

- 安全动态 MAC：使能接口安全功能后学习到的 MAC 地址。安全动态 MAC 地址不会被老化，但可以通过配置老化时间使其变为可以老化，设备重启后安全动态 MAC 地址会丢失，需要重新学习。
- Sticky MAC：使能接口 Sticky MAC 功能后学习到的 MAC 地址。Sticky MAC 地址不会被老化，保存配置后重启设备，Sticky MAC 地址不会丢失，无需重新学习。

MAC 地址防漂移

网络中的产生环路或非法用户进行网络攻击都会造成 MAC 地址发生漂移，导致 MAC 地址不稳定。配置接口 MAC 地址学习优先级可以保证在正确的接口学习到 MAC 地址，当不同接口学到相同的 MAC 地址表项时，高优先级接口学到的 MAC 地址表项可以覆盖低优先级接口学到的 MAC 地址表项。还可以根据现网需求来配置是否允许相同优先级的接口发生 MAC 地址表项覆盖。

版权所有 © 华为技术有限公司

MAC 地址漂移检测

配置 MAC 地址漂移检测功能可以检测 MAC 地址是否发生漂移，若出现 MAC 地址漂移则执行处理动作，例如阻断端口，尽量减小环路引起的 MAC 地址震荡对设备的影响。用户也可以配置系统检测到 MAC 地址漂移时只给网管发送告警。

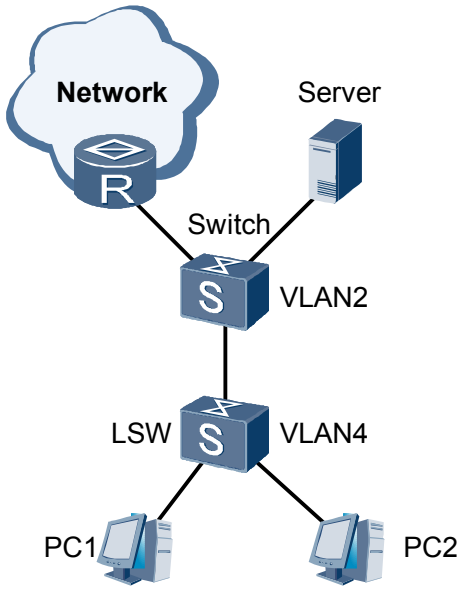
3.7.3 配置静态 MAC 表项

配置静态 MAC 地址，使携带特定目的 MAC 地址的报文由指定接口转发，可以防止设备不受伪造 MAC 地址攻击。

应用环境

Switch 的接口连接固定的上行设备或比较重要的服务器，比如图 3-35 中的 Server，为了防止伪造 MAC 地址攻击 Server，窃取 Server 上的重要信息，保证用户与 Server 正常通信，可将 Server 的 MAC 地址配置为静态 MAC，使携带特定目的 MAC 地址的报文由指定接口转发。

图 3-35 配置静态 MAC 表项组网图



前置任务

无

数据准备

在配置静态 MAC 表之前，需要准备以下数据。

序号	数据
1	目的 MAC 地址、出接口号、目的设备出接口所属的 VLAN 编号

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id1*，添加静态 MAC 表项。

说明

静态 MAC 地址表项的优先级高于动态 MAC 地址表项。

----结束

检查配置结果

使用命令 **display mac-address static** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]查看静态 MAC 表项信息。

3.7.4 配置黑洞 MAC 表项

配置黑洞 MAC 表项，丢弃目的 MAC 或源 MAC 地址为特定值的报文。

应用环境

为了防止无用的 MAC 地址表项占用 MAC 表，也为了防止黑客通过 MAC 地址攻击用户设备或网络，可将非信任用户的 MAC 地址配置为黑洞 MAC，丢弃目的 MAC 或源 MAC 地址为这些非信任 MAC 地址的报文。

前置任务

无

数据准备

在配置黑洞 MAC 表之前，需要准备以下数据。

序号	数据
1	目的 MAC 或源 MAC 地址、目的设备出接口所属的 VLAN 编号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-address blackhole** *mac-address* [**vlan** *vlan-id*]，添加黑洞 MAC 表项。

----结束

版权所有 © 华为技术有限公司

检查配置结果

使用命令 **display mac-address blackhole** [**vlan** *vlan-id*] [**verbose**]查看黑洞 MAC 表项信息。

3.7.5 配置动态 MAC 表项的老化时间

动态 MAC 表项不需要手工创建,表项可老化。可配置动态 MAC 表项的老化时间，防止 MAC 地址表项爆炸式增长。

应用环境

动态 MAC 表项由 AC6605 通过源 MAC 地址学习过程而自动建立，不需要手工创建。动态 MAC 表项并非永远有效，系统为 MAC 地址表项启动一个老化定时器，如果 MAC 地址表项在两倍表项老化时间内没有更新，则该表项将被删除。如果得到更新，则该表项的老化时间重新计算。老化时间越短，则 AC6605 对周边的网络变化越敏感。

随着网络拓扑的不断变化，AC6605 将会学习到越来越多的 MAC 地址。为了避免 MAC 地址表项爆炸式增长，需要合理配置动态 MAC 表项的老化时间，及时删除 MAC 地址表中的废弃 MAC 地址表项。

前置任务

无

数据准备

在配置动态 MAC 表之前，需要准备以下数据。

序号	数据
1	动态 MAC 表项的老化时间

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-address aging-time** *aging-time*，配置动态 MAC 表项的老化时间。

缺省情况下，动态 MAC 表项的老化时间为 300 秒。

----结束

检查配置结果

- 使用命令 **display mac-address aging-time**，查看动态 MAC 表项的老化时间是否配置正确。

3.7.6 配置禁止 MAC 地址学习功能

在固定网络中，配置关闭固定接口的 MAC 地址学习功能，其他服务器或终端将无法通过该接口通信，可以提高设备的安全性。

版权所有 © 华为技术有限公司

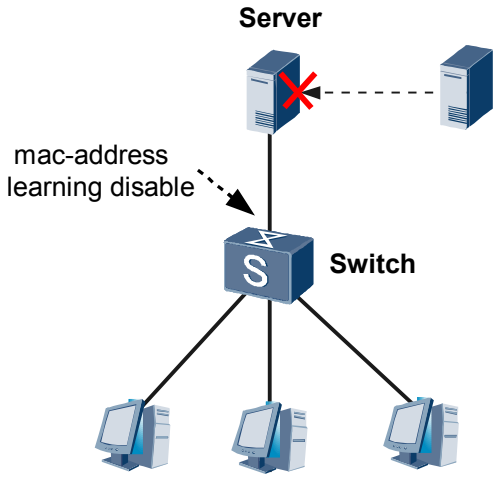
建立配置任务

在进行配置禁止 MAC 地址学习功能前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 3-36 所示，Switch 上某固定接口与服务器相连，网络管理员为了提高设备的安全性，可以指定该接口只允许某些 MAC 地址的报文通过。可在该接口上配置该服务器的静态 MAC 地址，且关闭该接口的 MAC 地址学习功能，指定动作为丢弃。这样，其他服务器或终端将无法通过该接口通信，增强网络的稳定性和安全性。

图 3-36 禁止 MAC 地址学习功能应用组网图



前置任务

无

数据准备

在配禁止 MAC 地址学习功能之前，需要准备以下数据。

序号	数据
1	接口类型和接口编号
2	VLAN 编号

配置基于接口禁止 MAC 地址学习

配置关闭该接口的 MAC 地址学习功能，可提高接口连接设备的安全性。

华为专有和保密信息
版权所有 © 华为技术有限公司

背景信息

开启 MAC 地址学习功能时，收到来自周边设备的以太网帧，解析出源 MAC 地址，结合接收该以太网帧的接口，在 MAC 地址表项中添加新表项。以后设备接收到去往该目的 MAC地址的以太网帧时，则直接查询 MAC 地址表项就可以得到正确的发送接口，可以避免广播。关闭 MAC 地址学习功能后，设备将不会再从该接口学习新的 MAC 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **mac-address learning disable** [**action** { **discard** | **forward** }]，在接口上禁止 MAC 地址学习功能。

缺省情况下，接口的 MAC 地址学习功能是使能的。

关闭 MAC 地址学习功能的缺省动作为 **forward**，即对报文按照 MAC 地址表项进行转发，如果没有对应的 MAC 地址表项，则广播该报文。当配置动作为 **discard** 时，会对报文的源 MAC 地址进行匹配，当接口和 MAC 地址与 MAC 地址表项匹配时，对该报文进行转发；当接口和 MAC 地址与 MAC 地址表项不匹配时，丢弃该报文。

说明

配置关闭 MAC 地址学习功能后，若动作为 **forward**，只能做到控制学习的 MAC 地址表项数量，无法做到阻止某些设备或终端访问网络。

----结束

配置基于 VLAN 禁止 MAC 地址学习

配置基于 VLAN 禁止 MAC 地址学习，可提高 VLAN 内用户的安全性，防止 MAC 地址攻击。

背景信息

在 VLAN 上禁止 MAC 地址学习功能后，如果再收到报文，会对报文的源 MAC 地址进行匹配，当与 MAC 地址表项匹配时，则对该报文进行转发。当与 MAC 地址表项不匹配时，则广播该报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-address learning disable**，在 VLAN 上禁止 MAC 地址学习功能。

缺省情况下，VLAN 的 MAC 地址学习功能是使能的。

----结束

版权所有 © 华为技术有限公司

检查配置结果

配置禁止 MAC 地址学习功能后，可以查看接口的配置信息是否正确，还可查看 VLAN 的 MAC 地址学习功能的状态。

操作步骤

- 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口配置信息。
- 使用命令 **display vlan** 查看 VLAN 配置信息。

----结束

3.7.7 配置限制 MAC 地址学习数量

介绍限制 MAC 地址学习数量的配置过程与步骤，可以基于接口和 VLAN 来对 MAC 地址学习数量进行限制。

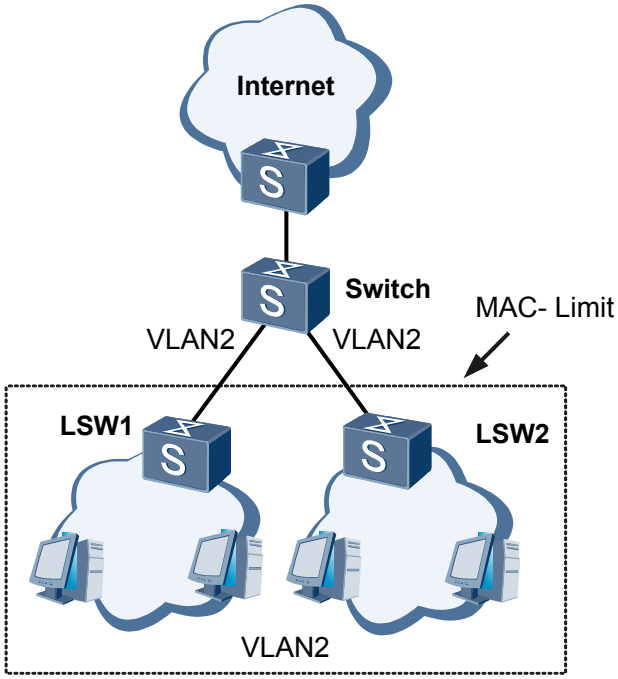
建立配置任务

在进行限制 MAC 地址学习数量配置前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 3-37 所示，在一些安全性比较差的网络中，如小区用户、缺乏安全管理的企业内部网中，容易受到黑客的 MAC 地址攻击。由于 MAC 表的容量是有限的，当黑客伪造大量源 MAC 地址不同的报文并发送给 Switch 后，Switch 的 MAC 表就可能被填满。当 Switch 的 MAC 表被填满后，即使它再收到正常的报文，也无法学习到报文中的源 MAC 地址。配置限制 MAC 地址学习数量，当超过限制数量时不再学习 MAC 地址，可以配置发送告警动作，防止 MAC 地址攻击，提高网络安全性。

图 3-37 限制 MAC 地址学习数量功能应用组网图



版权所有 © 华为技术有限公司

前置任务

在配置 MAC 地址学习限制之前，需完成以下任务：

- 清除接口或 VLAN 上已经学习到的 MAC 地址。

数据准备

在配置 MAC 地址学习限制之前，需要准备以下数据。

序号	数据
1	基于接口和 VLAN 的 MAC 地址学习限制数量

配置基于接口限制 MAC 地址学习数量

配置基于接口限制 MAC 地址学习数量后，当超过限制数量时不再学习 MAC 地址，可以配置发送告警动作，防止 MAC 地址攻击，提高网络安全性。

背景信息

MAC 地址表项数目达到限制后，源 MAC 为新 MAC 地址的报文继续被转发，但是 MAC 地址表项不记录。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **mac-limit maximum** *max-num*，限制接口的 MAC 地址学习数量。

缺省情况下，不限制 MAC 地址学习数量。

步骤 4 执行命令 **mac-limit alarm** { **disable** | **enable** }，配置当 MAC 地址数量达到限制后是否进行告警。

缺省情况下，对超过 MAC 地址学习数量限制的报文进行告警。

----结束

配置基于 VLAN 限制 MAC 地址学习数量

配置基于 VLAN 限制 MAC 地址学习数量后，当超过限制数量时不再学习 MAC 地址，可以配置发送告警动作，防止 MAC 地址攻击，提高网络安全性。

背景信息

MAC 地址表项数目达到限制后，源 MAC 为新 MAC 地址的报文继续被转发，但是 MAC 地址表项不记录。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-limit maximum** *max-num*，限制 VLAN 上的 MAC 地址学习数量。

缺省情况下，不限制 MAC 地址学习数量。

步骤 4 执行命令 **mac-limit alarm** { **disable** | **enable** }，配置当 MAC 地址数量达到限制后是否进行告警。

缺省情况下，对超过 MAC 地址学习数量限制的报文进行告警。

----结束

检查配置结果

配置 MAC 地址学习数量限制后，可以查看 MAC 地址学习限制的配置是否正确。

操作步骤

步骤 1 使用命令 **display mac-limit** [*interface-type interface-number* | **vlan** *vlan-id*]，查看 MAC 地址学习数量限制信息。

----结束

3.7.8 配置接口安全

介绍接口安全的配置过程与步骤。

建立配置任务

接口安全功能是将交换机接口学习到的 MAC 地址变为安全动态 MAC 地址或 Sticky MAC 地址，可以阻止其他非信任的 MAC 主机通过本接口和交换机通信，增强设备安全性。

应用环境

在对接入用户的安全性要求较高的网络中，可以配置接口安全功能，将接口学习到的 MAC 地址转换为安全动态 MAC 或 Sticky MAC，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，只允许这些 MAC 地址和交换机通信。这样可以阻止其他非信任的 MAC 主机通过本接口和交换机通信，提高设备与网络的安全性。

前置任务

- 关闭基于接口的 MAC 地址学习限制功能。
- 关闭配置 MUX VLAN 功能。
- 关闭 MAC 认证功能。
- 关闭 802.1x 认证功能。
- 关闭 DHCP Snooping 的 MAC 安全功能。

版权所有 © 华为技术有限公司

数据准备

在配置接口安全功能之前，需要准备以下数据。

序号	数据
1	配置安全动态 MAC 的接口类型和接口编号、接口 MAC 地址学习数量、接口安全保护动作、安全动态 MAC 表项的老化时间
2	配置 Sticky MAC 的接口类型和接口编号、接口 MAC 地址学习数量、接口安全保护动作

配置安全动态 MAC 功能

配置该功能后，接口会将学习到的 MAC 地址转换为安全动态 MAC 地址。当接口学习的安全动态 MAC 数量达到上限后，不再学习新的 MAC 地址，只允许这些 MAC 和交换机通信。可根据现网的组网需要来设置对应的保护动作参数。

背景信息

缺省情况下，安全动态 MAC 表项不会被老化，但可以通过在接口上配置安全动态 MAC 老化时间使其变为可以老化，设备重启后安全动态 MAC 地址会丢失，需要重新学习。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port-security enable**，使能接口安全功能。

缺省情况下，AC6605 的接口未使能接口安全功能。

说明

必须使能接口安全功能后，才可以配置安全动态 MAC 的学习限制数量、接口安全保护动作和安全动态 MAC 的老化时间。

步骤 4 （可选）执行命令 **port-security max-mac-num** *max-number*，配置接口安全动态 MAC 学习限制数量。

使能接口安全功能后，缺省情况下，接口学习的 MAC 地址限制数量为 1。

步骤 5 （可选）执行命令 **port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置接口安全保护动作。

缺省情况下，接口安全保护动作为 **restrict**。

接口安全保护动作有以下三种：

- **protect**：当学习到的 MAC 地址数达到接口限制数时，接口丢弃源地址在 MAC 表以外的报文。
- **restrict**：当学习到的 MAC 地址数超过接口限制数时，接口丢弃源地址在 MAC 表以外的报文，并同时发出告警。

版权所有 © 华为技术有限公司

- **shutdown**：当学习到的 MAC 地址数超过接口限制数时，接口执行 Shutdown 操作，同时发出告警。

步骤 6 （可选）执行命令 **port-security aging-time** *time* [**type** { **absolute** | **inactivity** }]，配置接口学习到的安全动态 MAC 地址的老化时间。

缺省情况下，接口学习的安全动态 MAC 地址不老化。

----结束

配置 Sticky MAC 功能

配置该功能后，接口会将学习到的 MAC 地址转换为 Sticky MAC。当接口学习的 Sticky MAC 数量达到上限后，不再学习新的 MAC 地址，只允许这些 MAC 和交换机通信，可根据现网的组网需要来设置对应的保护动作参数。

背景信息

Sticky MAC 不会被老化，设备重启后 Sticky MAC 也不会丢失，无需重新学习。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port-security enable**，使能接口安全功能。

缺省情况下，AC6605 的接口未使能接口安全功能。

步骤 4 执行命令 **port-security mac-address sticky**，使能接口 Sticky MAC 功能。

缺省情况下，接口未使能 Sticky MAC 功能。

步骤 5 （可选）执行命令 **port-security max-mac-num** *max-number*，配置接口 Sticky MAC 学习限制数量。

使能接口 Sticky MAC 功能后，缺省情况下，接口学习的 MAC 地址限制数量为 1。

步骤 6 （可选）执行命令 **port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置接口安全保护动作。

缺省情况下，接口安全保护动作为 **restrict**。

接口安全保护动作有以下三种：

- **protect**：当学习到的 MAC 地址数达到接口限制数时，接口丢弃源地址在 MAC 表以外的报文。
- **restrict**：当学习到的 MAC 地址数超过接口限制数时，接口丢弃源地址在 MAC 表以外的报文，同时发出告警。
- **shutdown**：当学习到的 MAC 地址数超过接口限制数时，接口执行 Shutdown 操作，同时发出告警。

步骤 7 （可选）执行命令 **port-security mac-address sticky** *mac-address* **vlan** *vlan-id*，手动配置一条 **sticky-mac** 表项。

----结束

版权所有 © 华为技术有限公司

检查配置结果

配置接口安全功能后，可以查看配置信息是否正确，还可查看安全动态 MAC 地址表项和 Sticky MAC 表项信息。

操作步骤

- 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口配置信息。
- 使用命令 **display mac-address security** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]查看安全动态 MAC 表项。
- 使用命令 **display mac-address sticky** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]查看 Sticky MAC 表项。

----结束

3.7.9 配置 MAC 地址防漂移

介绍接口 MAC 地址防漂移的配置过程与步骤。

建立配置任务

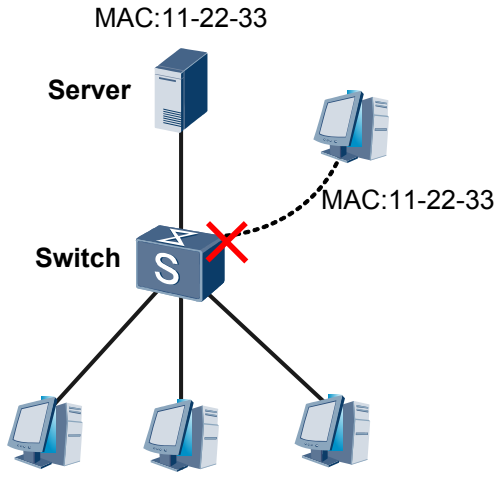
在配置 MAC 防漂移前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

MAC 防漂移功能主要应用于以下场景中：

如图 3-38 所示，为防止非法用户伪造服务器 MAC 地址入侵 AC6605，可以提高服务器侧接口的 MAC 地址学习优先级。配置接口 MAC 地址学习优先级可以保证在正确的接口学习到 MAC 地址，当不同接口学到相同的 MAC 地址表项时，高优先级接口学到的 MAC 地址表项可以覆盖低优先级接口学到的 MAC 地址表项，可以保证 AC6605 不会从其他接口学习到伪造服务器的 MAC 地址。这样用户可以访问正确的服务器，正常使用网络资源。

图 3-38 MAC 防漂移应用组网图



版权所有 © 华为技术有限公司

前置任务

无

数据准备

在配置 MAC 地址防漂移之前，需要准备以下数据。

序号	数据
1	（可选）接口学习 MAC 地址的优先级

配置接口 MAC 地址学习优先级

接口配置不同的 MAC 地址学习优先级后，如果不同接口学到相同的 MAC 地址表项，那么高优先级接口学到的 MAC 地址表项可以覆盖低优先级接口学到的 MAC 地址表项，防止 MAC 地址发生漂移。

背景信息

在 AC6605 上配置某接口学习 MAC 地址的优先级来防漂移，如果 AC6605 接口连接的网络设备（例如：服务器）下电后，AC6605 另外的接口学习到与该网络设备同样的 MAC 地址，当网络设备再次上电后还可以学习到正确的 MAC 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **mac-learning priority** *priority-id*，配置接口学习 MAC 地址的优先级。

缺省情况下，接口学习 MAC 地址的优先级为 0，数值越大优先级越高。

----结束

配置不允许相同优先级接口 MAC 漂移

配置不允许相同优先级的接口发生 MAC 地址表项覆盖，也可以防止 MAC 漂移，提高网络的安全性。

背景信息

在 AC6605 上配置不允许相同优先级的接口发生 MAC 地址漂移，如果 AC6605 接口连接的网络设备（例如：服务器）下电后，AC6605 另外的接口学习到与该网络设备同样的 MAC 地址，当网络设备再次上电后不能学习到正确的 MAC 地址。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **undo mac-learning priority** *priority-id* **allow-flapping**，配置不允许相同优先级的接口发生 MAC 地址漂移。

缺省情况下，允许相同优先级的接口发生 MAC 地址漂移。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display current-configuration** 查看接口 MAC 地址学习优先级的配置。

----结束

3.7.10 配置 MAC 地址漂移检测功能

介绍 MAC 地址漂移检测功能的配置方法。

建立配置任务

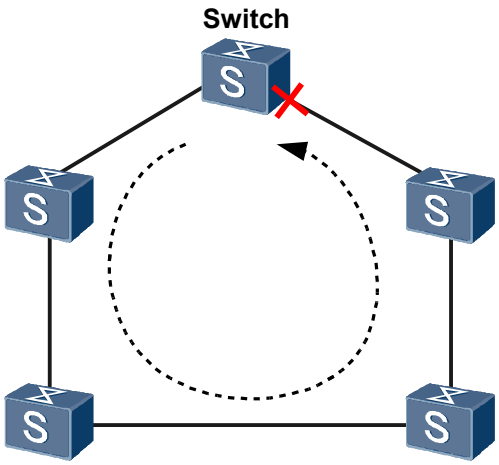
在进行 MAC 地址漂移检测配置前了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 3-39 所示网络中的产生环路会造成 MAC 地址发生漂移，导致 MAC 地址不稳定。配置 MAC 地址漂移检测功能可以检测指定 VLAN 下的所有 MAC 地址是否发生漂移。

配置 MAC 地址漂移检测功能后，系统将检测该 VLAN 内所有 MAC 地址是否发生移动，判断是否出现 MAC 地址漂移。若出现 MAC 地址漂移则执行处理动作，例如阻断端口，从而破除环路，尽量减小环路引起的 MAC 地址震荡、广播风暴等对设备的影响。用户也可以配置系统检测到 MAC 地址漂移时只给网管发送告警。

图 3-39 MAC 漂移检测应用组网图



版权所有 © 华为技术有限公司

前置任务

无

数据准备

在配置 MAC 地址漂移检测功能之前，需要准备以下数据：

序号	数据
1	MAC 地址漂移检测的 VLAN 编号
2	接口的阻断时间
3	指定接口永久阻断的重试次数

配置 MAC 地址漂移检测

配置 MAC 地址漂移检测功能可以检测指定 VLAN 下的所有的 MAC 地址是否发生漂移。当 MAC 地址发生漂移时，可根据需求配置阻断接口或 MAC 地址、或者上报告警。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **loop-detect eth-loop** { [**block-mac**] **block-time** *block-time* **retry-times** *retry-times* | **alarm-only** }，配置 MAC 地址漂移检测功能。

当系统检测到 VLAN 内有 MAC 地址发生漂移时，可以进行以下处理动作：

- 接口阻断或 MAC 地址阻断。当检测到 MAC 地址发生漂移则执行接口阻断或 MAC 地址阻断动作。当指定 **block-mac** 参数时，将不阻断整个接口，而是按照发生漂移的 MAC 地址进行流量阻断。
- 发送告警。当检测到 MAC 地址发生漂移时只给网管发送告警。

----结束

（可选）解除接口阻断或 MAC 地址阻断

当系统检测到某 VLAN 内有 MAC 地址发生漂移且发生漂移的接口或 MAC 地址被永久阻断时，只能通过配置解除指定 VLAN 下的接口阻断或 MAC 地址阻断来恢复到正常状态。

背景信息

配置 MAC 地址漂移检测后，系统将检测该 VLAN 内所有 MAC 地址是否发生漂移，若出现 MAC 地址漂移则执行阻断动作，阻断时间到达后放开并重新进行检测。若 20 秒内没有再次检测到 MAC 地址漂移，则接口阻塞被完全解除，重新开始一轮检测；若在 20

版权所有 © 华为技术有限公司

秒内再次检测到 MAC 地址漂移，则再次开始阻塞，如此反复，直到达到设定的重试次数，若依然能够检测到 MAC 地址漂移，则永久阻断该接口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **reset loop-detect eth-loop vlan** *vlan-id* { **all** | **interface** *interface-type interface-number* | **mac-address** *mac-address* }，配置解除指定 VLAN 下的接口阻断或 MAC 地址阻断。

执行 **reset loop-detect eth-loop** 命令解除指定 VLAN 下的接口阻断或 MAC 地址阻断前，可以先执行 **display loop-detect eth-loop** 命令查看 MAC 地址漂移检测信息，根据检测信息进行相应的解除阻断配置。

----结束

检查配置结果

配置 MAC 地址漂移检测功能后，可查看各 VLAN 下检测 MAC 地址漂移的配置信息、永久阻断的接口信息和 MAC 地址信息。

操作步骤

步骤 1 使用命令 **display loop-detect eth-loop** [**vlan** *vlan-id*]来查看指定 VLAN 下 MAC 地址漂移的检测信息。

----结束

3.7.11 配置丢弃全零 MAC 地址报文功能

配置该功能后，AC6605 会丢弃源 MAC 或目的 MAC 为全 0 的 MAC 地址报文。

应用环境

网络中的一些主机或设备发生故障时，会向 AC6605 发送源 MAC 或目的 MAC 地址为全 0 的报文。可配置 AC6605 丢弃这些报文，还可以配置在收到这些报文时上报告警，管理员可根据告警信息来定位故障设备。

前置任务

- 已搭建好配置环境。

数据准备

无

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **drop illegal-mac enable**，配置 AC6605 丢弃全 0 非法 MAC 地址报文。

缺省情况下，AC6605 没有配置丢弃全 0 非法 MAC 地址报文的功能。

版权所有 © 华为技术有限公司

步骤 3 （可选）执行命令 **drop illegal-mac alarm**，配置 AC6605 收到全 0 非法 MAC 地址报文时生成一条告警。

缺省情况下，AC6605 收到全 0 非法 MAC 地址报文时不生成告警。

说明

配置 **drop illegal-mac alarm** 命令后只能告警一次。如果需要继续告警，必须重新配置该命令。

----结束

检查配置结果

使用 **display current-configuration** 命令查看 AC6605 是否配置丢弃全 0 非法 MAC 地址报文的功能。

3.7.12 配置 MAC 刷新 ARP 功能

配置 MAC 刷新 ARP 功能后，如果 MAC 表项的出接口变化，会及时更新 ARP 表项。

应用环境

网络中每台在网设备都有一个 IP 地址，用于该主机与其他设备的通信。在以太网中，主机或交换设备或路由设备是根据 MAC 地址来发送、接收以太网数据帧。ARP 用于提供 IP 地址到 MAC 地址的映射。当不同网段间通信时，需要使用 ARP 表项来将 IP 地址映射到正确的 MAC 地址及相应的出接口上。

如果用户更换某主机位置，使主机连接到设备的另一个接口上，该主机的 MAC 地址将在另一个接口上被学习到，其对应的 MAC 表项的出接口将会变化，但是 ARP 表项在到达老化时间后才会更新表项中的出接口。在到达老化时间之前，设备将使用错误的 ARP 表项来进行通信。配置 MAC 刷新 ARP 功能后，如果 MAC 表项的出接口变化时，会即时更新 ARP 表项。

前置任务

无

数据准备

无

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-address update arp**，配置 MAC 刷新 ARP 功能。

缺省情况下，没有配置 MAC 刷新 ARP 功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

- 该命令只对动态 ARP 表项生效，不会更新静态 ARP 表项。
- 使用 **arp anti-attack entry-check enable** 命令配置 ARP 防地址欺骗功能后，MAC 刷新 ARP 功能不生效。
- 使能了 MAC 刷新 ARP 功能后，只有 MAC 表项的出接口发生变化，才会更新对应的 ARP 表项。

----结束

检查配置结果

使用命令 **display current-configuration** 查看 MAC 刷新 ARP 功能是否配置成功。

3.7.13 配置端口桥功能

配置端口桥功能后，接口将处理同源同宿报文。

应用环境

同源同宿报文即源 MAC 地址和目的 MAC 地址均在设备的同一端口上学习到的报文。缺省情况下，交换机不转发同源同宿报文，当端口收到这种报文时，交换机判断为非法报文并直接丢弃该报文。配置端口桥功能后，当端口收到同源同宿报文时，若设备上的 MAC 地址表中存在与该报文的目的 MAC 地址对应的表项，则将报文从本端口转发出去。

端口桥功能主要应用于以下场景：

- 交换机下挂有不具备二层转发能力的设备，当这些无二层转发能力的设备连接的用户有互通需求时，会直接将报文上送到交换机，由交换机完成转发功能。此时需要使能端口桥功能，使端口转发同源同宿报文。
- 在数据中心做接入交换机且下挂服务器，一台服务器中启用多个虚拟机，并且虚拟机之间需要进行数据交换。为了提高数据交换速度与服务器性能，可以使能端口桥功能，由交换机来进行数据交换。

数据准备

序号	数据
1	接口类型和接口编号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port bridge enable**，配置端口桥功能。

缺省情况下，没有配置端口桥功能。

----结束

版权所有 © 华为技术有限公司

检查配置结果

使用命令 **display current-configuration** 查看端口桥功能是否配置成功。

3.7.14 配置举例

介绍 MAC 表的各种组网举例。

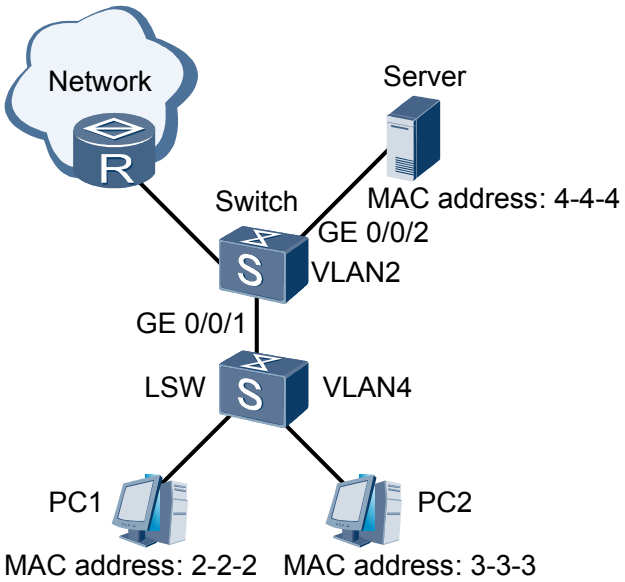
配置 MAC 表示例

组网需求

如图 3-40 所示，用户主机 PC1 的 MAC 地址为 0002-0002-0002，用户主机 PC2 的 MAC 地址为 0003-0003-0003，通过 LSW 连接 Switch。连接 Switch 的接口为 GigabitEthernet0/0/1，该接口所属 VLAN 为 VLAN2。Server 服务器的 MAC 地址为 0004-0004-0004，连接 Switch 的接口为 GigabitEthernet0/0/2，该接口所属 VLAN 为 VLAN2。

- 为防止 MAC 地址攻击，在 Switch 的 MAC 表中为该用户主机添加一条静态表项。Switch 通过出接口 GigabitEthernet0/0/1 发送报文时将 VLAN 更改为 LSW 所属的 VLAN4，同时配置 Switch 的动态 MAC 表项老化时间为 500s。
- 为防止假冒 Server 的 MAC 地址窃取重要用户信息，在 Switch 上配置静态 MAC 地址转发功能。

图 3-40 配置 MAC 表组网图



配置思路

采用如下的思路配置 MAC 表：

1. 创建 VLAN，并将接口加入到 VLAN 中。

版权所有 © 华为技术有限公司

2. 添加静态 MAC 表。
3. 配置动态 MAC 表的老化时间。

数据准备

为完成此配置例，需准备如下的数据：

- PC1 的 MAC 地址为 0002-0002-0002。
- PC2 的 MAC 地址为 0003-0003-0003。
- Server 的 MAC 地址为 0004-0004-0004。
- Switch 所属 VLAN 为 VLAN2。
- 与 LSW 相连的 Switch 的接口为 GigabitEthernet0/0/1。
- 与 Server 相连的 Switch 的接口为 GigabitEthernet0/0/2。
- 通过出接口发送报文时需要更改的 VLAN 为 VLAN4。
- Switch 的动态 MAC 表项老化时间为 500s。

操作步骤

步骤 1 添加静态 MAC 地址表项

创建 VLAN2，将接口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 加入 VLAN2，并配置接口 GigabitEthernet0/0/1 的 VLAN Mapping 功能。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[Quidway-GigabitEthernet0/0/1] port vlan-mapping vlan 4 map-vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 2
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

配置静态 MAC 地址表项。

```
[Quidway] mac-address static 2-2-2 gigabitethernet 0/0/1 vlan 2
[Quidway] mac-address static 3-3-3 gigabitethernet 0/0/1 vlan 2
[Quidway] mac-address static 4-4-4 gigabitethernet 0/0/2 vlan 2
```

步骤 2 配置动态表项老化时间

```
[Quidway] mac-address aging-time 500
```

步骤 3 验证配置结果

在任意视图下执行 **display mac-address** 命令，查看静态 MAC 表是否添加成功。

```
[Quidway] display mac-address static vlan 2
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI                 Learned-From        Type
-------------------------------------------------------------------------------
0002-0002-0002       2/-                      GE0/0/1             static
0003-0003-0003       2/-                      GE0/0/1             static
0004-0004-0004       2/-                      GE0/0/2             static
-------------------------------------------------------------------------------
Total items displayed  = 3
```


版权所有 © 华为技术有限公司

在任意视图下执行 **display mac-address aging-time** 命令，查看动态表项老化时间是否配置成功。

```
[Quidway] display mac-address aging-time
  Aging time: 500 seconds
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2
#
 mac-address aging-time 500
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
 port vlan-mapping vlan 4 map-vlan 2
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
 mac-address static 0002-0002-0002 GigabitEthernet0/0/1 vlan 2
 mac-address static 0003-0003-0003 GigabitEthernet0/0/1 vlan 2
 mac-address static 0004-0004-0004 GigabitEthernet0/0/2 vlan 2
#
return
```

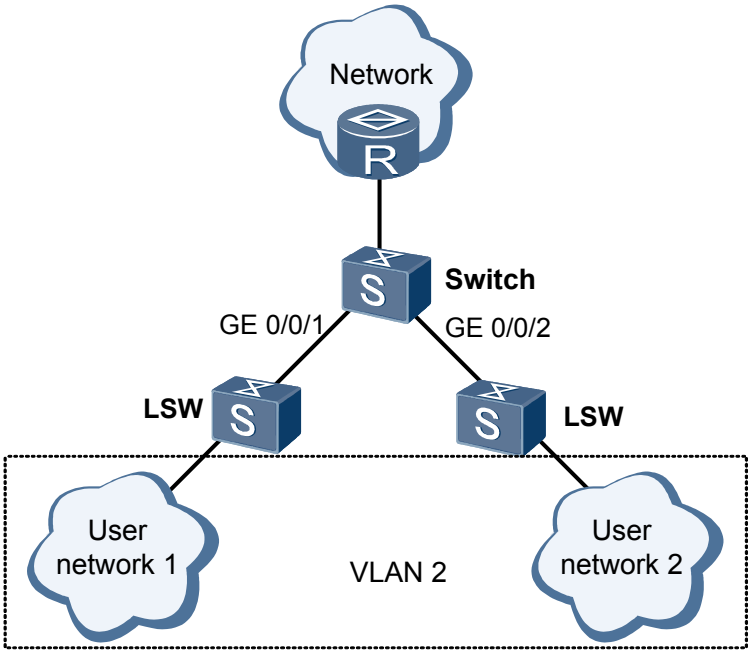
配置基于 VLAN 的 MAC 地址学习限制示例

组网需求

如图 3-41 所示，用户网络 1 通过 LSW 与 Switch 相连，连接 Switch 的接口为 GigabitEthernet0/0/1。用户网络 2 通过 LSW 与 Switch 相连，连接 Switch 的接口为 GigabitEthernet0/0/2。GigabitEthernet0/0/1、GigabitEthernet0/0/2 属于 VLAN2。为防止 MAC 地址攻击，控制接入用户数量，对 VLAN2 进行 MAC 地址学习的限制。

版权所有 © 华为技术有限公司

图 3-41 配置基于 VLAN 的 MAC 地址学习限制组网图



配置思路

采用如下的思路配置基于 VLAN 的 MAC 地址学习限制：

1. 创建 VLAN，并将接口加入到 VLAN 中。
2. 配置 VLAN 的 MAC 地址学习限制。

数据准备

为完成此配置例，需准备如下的数据：

- 接口所属 VLAN 为 VLAN2。
- 用户接口为 GigabitEthernet0/0/1、GigabitEthernet0/0/2。
- 最大 MAC 地址学习数量为 100。

操作步骤

步骤 1 配置 MAC 地址学习限制

将 GigabitEthernet0/0/1、GigabitEthernet0/0/2 加入 VLAN2。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 2
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

在 VLAN2 上配置 MAC 地址学习限制规则：最多可以学习 100 个 MAC 地址，超过最大 MAC 地址学习数量的报文继续转发但不加入 MAC 地址表，并进行告警提示。

```
[Quidway] vlan 2
[Quidway-vlan2] mac-limit maximum 100  alarm enable
[Quidway-vlan2] quit
```

步骤 2 验证配置结果

在任意视图下执行 **display mac-limit** 命令，查看 MAC 地址学习限制规则是否配置成功。

```
<Quidway> display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 1

PORT                VLAN/VSI/SI      SLOT Maximum Rate(ms) Action  Alarm
------------------------------------------------------------------------------
-                   2                -    100     -        forward enable
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2
#
vlan 2
 mac-limit maximum 100
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
return
```

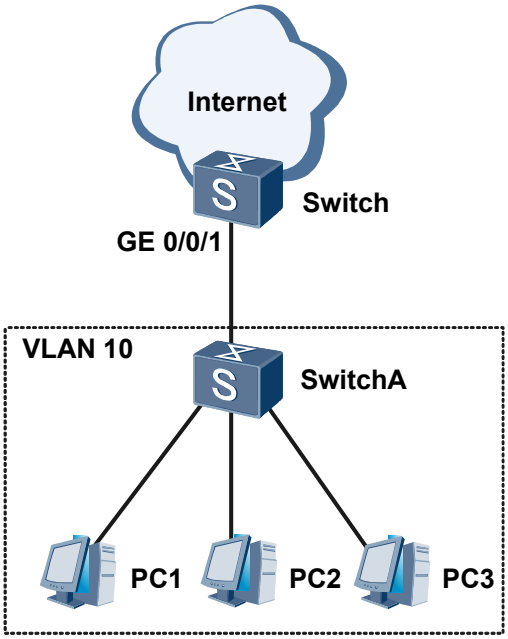
配置接口安全示例

组网需求

如图 3-42 所示，公司为了提高信息安全，将 Switch 连接员工 PC 侧的接口使能了接口安全功能，并且设置了接口学习 MAC 地址数的上限为信任的设备总数，这样其他外来人员使用自己带来的 PC 无法访问公司的网络。

版权所有 © 华为技术有限公司

图 3-42 配置接口安全示例组网图



配置思路

采用如下的思路配置接口安全：

1. 创建 VLAN，并配置接口的链路类型为 Trunk。
2. 使能接口安全功能。
3. 使能接口 Sticky MAC 功能。
4. 配置接口安全功能的保护动作。
5. 配置接口 MAC 地址学习限制数。

数据准备

为完成此配置例，需准备如下的数据：

- 接口允许通过的 VLAN 编号。
- Switch 连接 PC 的接口类型和编号。
- 接口安全功能的保护动作。
- 接口 MAC 地址学习限制数。

操作步骤

步骤 1 创建 VLAN，并配置接口的链路类型

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```


华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 2 配置接口安全功能

使能接口安全功能。

```
[Quidway-GigabitEthernet0/0/1] port-security enable
```

使能接口 Sticky MAC 功能。

```
[Quidway-GigabitEthernet0/0/1] port-security mac-address sticky
```

配置接口安全功能的保护动作。

```
[Quidway-GigabitEthernet0/0/1] port-security protect-action protect
```

配置接口 MAC 地址学习限制数。

```
[Quidway-GigabitEthernet0/0/1] port-security max-mac-num 4
```

其他接口如需使能接口安全功能，请重复上述配置。

步骤 3 验证配置结果

将 PC1 换成其他设备，无法访问公司网络。

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 port-security enable
 port-security protect-action protect
 port-security mac-address sticky
 port-security max-mac-num 4
#
return
```

配置 MAC 防漂移示例

该示例可用于提高公司服务器或重要用户的安全性，防止被非法用户攻击。

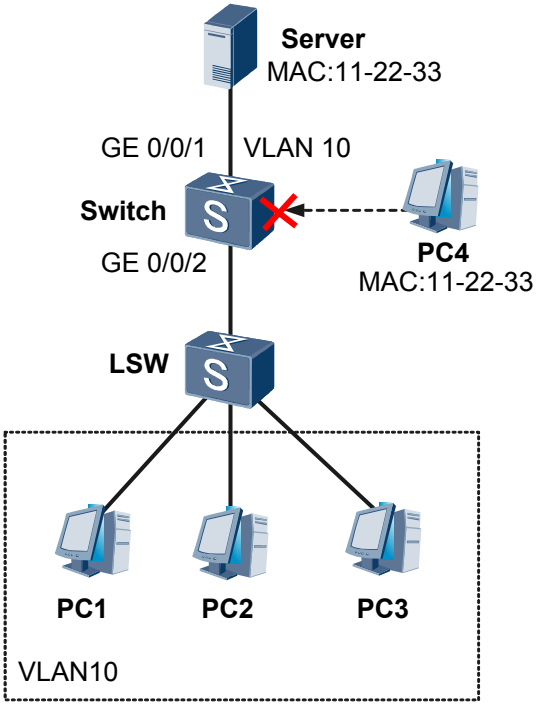
组网需求

某企业网络中，员工用户需要访问企业的服务器。由于在企业网中很难控制接入用户的行为，如果某些非法用户从其他接口假冒服务器的 MAC 地址发送报文，则服务器的 MAC 地址将在其他接口学习到，不仅会导致用户与服务器不能正常通信，还会导致一些重要用户信息被窃取。

如图 3-43 所示，为了提高服务器安全性，防止被非法用户攻击，可配置 MAC 防漂移功能。

版权所有 © 华为技术有限公司

图 3-43 配置 MAC 防漂移组网图



配置思路

采用如下的思路配置 MAC 防漂移：

1. 创建 VLAN,并将接口加入到 VLAN 中。
2. 在服务器连接的接口上配置 MAC 防漂移功能。

数据准备

为完成此配置例，需准备如下的数据：

- 接口所属 VLAN 为 VLAN10。
- 服务器侧接口：GigabitEthernet 0/0/1
- 用户侧接口：GigabitEthernet 0/0/2
- 连接服务器接口的 MAC 地址学习优先级为 2。

操作步骤

步骤 1 创建 VLAN,并将接口加入到 VLAN 中。

将 GigabitEthernet0/0/1、GigabitEthernet0/0/2 加入 VLAN10。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet0/0/2] quit
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
```

步骤 2 # 在 GigabitEthernet0/0/1 上配置 MAC 地址学习的优先级为 2。

```
[Quidway-GigabitEthernet0/0/1] mac-learning priority 2
```

步骤 3 验证配置结果

在任意视图下执行 **display current-configuration** 命令，查看接口 MAC 地址学习的优先级配置是否正确。

```
<Quidway> display current-configuration
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mac-learning priority 2
#
return
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mac-learning priority 2
#
interface GigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 10
#
return
```

3.8 STP/RSTP 配置

STP（Spanning Tree Protocol，生成树协议）将环形网络修剪成为一个无环的树型网络，避免报文在环形网络中的增生和无限循环；RSTP（Rapid Spanning Tree Protocol，快速生成树协议）在 STP 基础上实现了快速收敛，并增加了边缘端口的概念及保护功能。

3.8.1 STP/RSTP 简介

STP 是数据链路层的管理协议，通过阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的；RSTP 基于 STP 协议，对原有的 STP 协议进行了更加细致的修改和补充，实现了网络拓扑快速收敛。

STP/RSTP 概述

STP/RSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，解决交换网络中的环路问题。

版权所有 © 华为技术有限公司

STP/RSTP 概述

在一个复杂的网络环境中，难免会出现环路。并且，由于冗余备份的需要，网络设计者都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样，偶然或必然中都会导致环路产生。

环路会产生广播风暴，最终导致整个网络资源被耗尽，网络瘫痪不可用。环路还会引起MAC 地址表震荡导致 MAC 地址表项被破坏。

为了破除环路，可以采用数据链路层协议 STP，运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

但是，STP 拓扑收敛速度慢，IEEE 于 2001 年发布的 802.1W 标准定义了 RSTP，RSTP 在 STP 基础上进行了改进，实现了网络拓扑快速收敛。

STP/RSTP 相关概念

- 根桥

  树形网络结构必须有树根，于是 STP/RSTP 引入了根桥（Root Bridge）概念。

  对于一个 STP/RSTP 网络，根桥有且只有一个，它是整个网络的逻辑中心，但不一定是物理中心。但是根据网络拓扑的变化，根桥可能改变。

- ID

  ID 分为：桥 ID 即 BID（Bridge ID）和端口 ID 即 PID（Port ID）。

  - BID：桥 ID

    IEEE 802.1D 标准中规定 BID 是由 2 字节的桥优先级（Bridge Priority）与桥 MAC 地址构成，即 BID（8 字节）= 网桥优先级（2 字节）+ 网桥 MAC（6 字节）。

    在 STP 网络中，桥 ID 最小的设备会被选举为根桥。在华为公司的设备上，桥优先级支持手工配置，取值范围是 0 ～ 61440，缺省情况下，桥优先级是 32768。

  - PID：端口 ID

    PID 由两部分构成的，即 PID（16 位） = 端口优先级（4 位）+ 端口号（12 位）。

    PID 只在某些情况下对选择指定端口有作用，即在选择指定端口时，两个端口的根路径开销和发送交换设备 BID 都相同的情况下，比较端口的 PID，PID 小者为指定端口。如**图 3-44** 所示，设备 S2 的端口 A 和端口 B 的根路径开销和发送交换设备 BID 都相同，所以进行 PID 的比较，端口 A 的 PID 小，则该端口为所在网段的指定端口。在华为公司的设备上，端口优先级支持手工配置，取值范围是 0 ～ 240，步长为 16，即取值为 0、16、32 等，缺省情况下，端口优先级是 128。

- 路径开销

  路径开销是一个端口量，是 STP/RSTP 协议用于选择链路的参考值。STP/RSTP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树形网络结构。

  在一个 STP/RSTP 网络中，某端口到根桥累计的路径开销就是所经过的各个桥上的各端口的路径开销累加而成，这个值叫做根路径开销。

- 端口角色

  - STP 端口

版权所有 © 华为技术有限公司

- 根端口

  所谓根端口就是去往根桥路径最近的端口，根端口负责向根桥方向转发数据，根端口的选择标准是依据根路径开销判定。在一台设备上所有使能 STP 的端口中，根路径开销最小者，就是根端口。在一个运行 STP/RSTP 协议的设备上根端口有且只有一个，而且根桥上没有根端口。

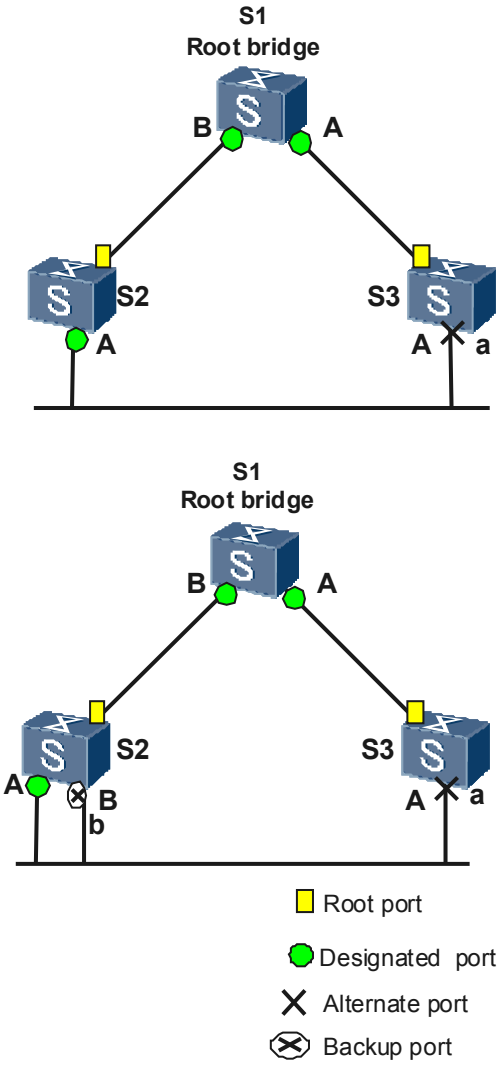
- 指定端口

  对一台交换设备而言，它的指定端口是向下游交换设备转发 BPDU 报文的端口。根桥的所有端口都是指定端口。在环网的每一网段都会选举出一个指定端口，在一个网段上拥有指定端口的交换设备被称作该网段的指定桥。

- RSTP 端口

RSTP 在 STP 基础上新增加了 2 种端口角色：Alternate 端口和 Backup 端口。通过端口角色的增补，简化了生成树协议的理解及部署。

图 3-44 端口角色示意图



如图 3-44 所示，RSTP 的端口角色共有 4 种：根端口、指定端口、Alternate 端口和 Backup 端口。

版权所有 © 华为技术有限公司

根端口和指定端口的作用同 STP 协议中定义，Alternate 端口和 Backup 端口的描述如下：

- 从配置 BPDU 报文发送角度来看：
  - Alternate 端口是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。
  - Backup 端口是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。
- 从用户流量角度来看：
  - Alternate 端口作为根端口的备份端口，提供了从指定桥到根的另一条可切换路径。
  - Backup 端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。

- 端口状态
  - STP 端口状态

    运行 STP 协议的设备上端口状态如**表 3-11** 所示。

表 3-11 STP 端口状态

端口状态	目的	说明
Forwarding	端口既转发用户流量也转发 BPDU 报文。	只有根端口或指定端口才能进入 Forwarding 状态。
Learning	设备会根据收到的用户流量构建 MAC 地址表，但不转发用户流量。	过渡状态，增加 Learning 状态防止临时环路。
Listening	确定端口角色，将选举出根桥、根端口和指定端口。	过渡状态。
Blocking	端口仅仅接收并处理 BPDU，不转发用户流量。	阻塞端口的最终状态。
Disabled	端口不仅不转发 BPDU 报文，也不转发用户流量。	端口状态为 Down。

  - RSTP 端口状态

    RSTP 在 STP 基础上进行了端口状态的改进，如**表 3-12** 所示。

表 3-12 RSTP 端口状态

端口状态	说明
Forwarding	在这种状态下，端口既转发用户流量又接收/发送 BPDU 报文。

华为专有和保密信息
版权所有 © 华为技术有限公司

端口状态	说明
Learning	这是一种过渡状态。在 Learning 下，交换设备会根据收到的用户流量，构建 MAC 地址表，但不转发用户流量，所以叫做学习状态。 Learning 状态的端口接收/发送 BPDU 报文，不转发用户流量。
Discarding	Discarding 状态的端口只接收 BPDU 报文。

注意

华为公司数据通信设备缺省情况处于 MSTP 模式，当从 MSTP 模式切换到 STP 模式，运行 STP 协议的设备上端口支持的端口状态仍然保持和 MSTP 支持的端口状态一样（MSTP 端口状态与 RSTP 端口状态相同），支持的状态仅包括 Forwarding、Learning 和 Discarding，如**表 3-12** 所示。

- 三种定时器
  - Hello Timer

    通过设置 Hello Timer 定时器时间的大小控制 BPDU 发送间隔。
  - Forward Delay Timer

    通过设置 Forward Delay Timer 定时器时间的大小控制端口在 Listening 和 Learing 状态的持续时间。
  - Max Age

    通过设置 Max Age 定时器时间的大小控制存储 BPDU 的超时时间，超时认为根桥连接失败。

三种生成树协议的比较

对于 STP/RSTP/MSTP 三种生成树协议，特点与场景比较如**表 3-13** 所示。

表 3-13 STP/RSTP/MSTP 特点与场景比较

生成树协议	特点	应用场景	注意事项
STP	形成一棵无环路的树：解决广播风暴并实现冗余备份。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。	**说明** ● 若当前交换设备既支持 STP 又支持 RSTP，建议选择使用 RSTP。 ● 若当前交换设备既支持 STP/RSTP 又支持 MSTP，建议选择使用 MSTP，详见 **MSTP 配置**。
RSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。		

版权所有 © 华为技术有限公司

生成树协议	特点	应用场景	注意事项
MSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。 ● 多颗生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。	

AC6605 支持的 STP/RSTP 特性

配置 STP/RSTP 时，您将接触到基本功能、拓扑收敛、保护功能以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

STP/RSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。STP/RSTP 的基本配置思路如下：

1. 在环形网络中，选举其中的一个交换设备作为根桥（Root bridge）。用户可以通过配置交换设备的优先级人为影响根桥的选择。
2. 计算出其他交换设备到根桥的最短路径，为每个非根交换设备选举一个根端口。用户可以通过配置交换设备到根桥的路径开销人为影响根端口的选择。
3. 通过端口的根路径开销、发送交换设备的 BID 及端口 ID 为每个连接选举出一个指定端口。在端口的根路径开销及发送交换设备的 BID 都相同的情况下，用户可以通过配置交换设备的端口优先级人为影响指定端口的选择。

为了满足特殊场合的应用和扩展功能，STP/RSTP 还支持如下功能：

- RSTP 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。
- RSTP 提供如表 3-14 所示的各种保护功能。
- 为了实现与其他制造商设备的互通，需要在华为公司运行 STP/RSTP 的设备上配置合适的参数，以确保通信畅通。

表 3-14 RSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。

版权所有 © 华为技术有限公司

保护功能	场景	配置影响
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的 BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

3.8.2 配置 STP/RSTP 基本功能

对于一个存在环路的以太网，通过给网络中的交换设备配置 STP/RSTP 基本功能，STP/RSTP 协议阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。

通过给交换设备配置 STP/RSTP 的工作模式后，启动 STP/RSTP，STP/RSTP 便开始进行生成树计算，将网络修剪成树状，破除环路。但是，若网络规划者需要人为干预生成树计算的结果，可以采取以下方式：

- 配置交换设备的优先级数值：数值越小，交换设备的优先级越高，成为根桥的可能性越大；数值越大，交换设备的优先级越低，成为根桥的可能性越小。
- 配置端口路径开销数值：在同一种计算方法下，数值越小，端口到根桥的路径开销越小，成为根端口的可能性就越大；数值越大，端口到根桥的路径开销越大，成为根端口的可能性越小。
- 配置端口的优先级数值：数值越小，端口成为指定端口的可能性就越大；数值越大，端口成为指定端口的可能性越小。

版权所有 © 华为技术有限公司

建立配置任务

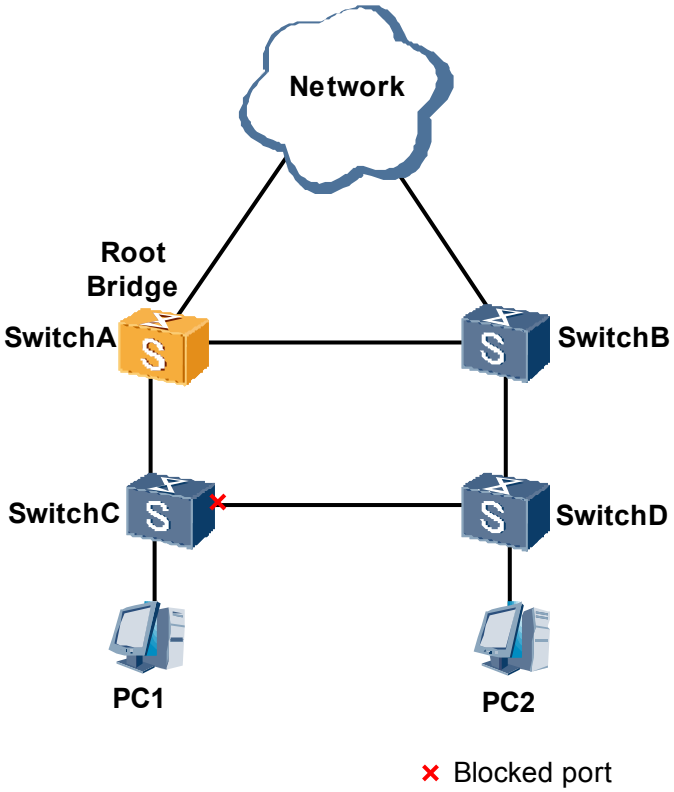
在配置 STP/RSTP 基本功能前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。网络规划者规划好网络后，可在网络中部署 STP/RSTP 协议预防环路。当网络中存在环路，STP/RSTP 通过阻塞某个端口以达到破除环路的目的。

如图 3-45 所示，SwitchA、SwitchB、SwitchC 和 SwitchD 构成环形网络，通过在环形网络中运行 STP/RSTP 以破除环路。

图 3-45 环形网络示意图



说明

若当前设备既支持 STP 又支持 RSTP，建议选择使用 RSTP。

前置任务

在配置 STP/RSTP 基本功能之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up

版权所有 © 华为技术有限公司

数据准备

在配置 STP/RSTP 基本功能之前，需要准备以下数据。

序号	数据
1	（可选）当前交换设备的优先级数值
2	（可选）端口优先级数值
3	（可选）端口的路径开销值

配置 STP/RSTP 工作模式

在配置 STP/RSTP 基本功能前需要选择 STP/RSTP 工作模式，RSTP 兼容 STP。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp mode** { **stp** | **rstp** }，配置交换设备的 STP/RSTP 工作模式。

缺省情况下，设备的工作模式为 MSTP。

----结束

（可选）配置交换设备优先级

交换设备优先级值越小，则交换设备在环网中的优先级越高，成为根桥的可能性越大。

背景信息

在一个运行 STP/RSTP 的网络中，有且仅有一个根桥，它是整棵生成树的逻辑中心。在进行根桥的选择时，一般会希望选择性能高、网络层次高的交换设备作为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此需要配置优先级以保证该设备成为根桥。

对于网络中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

注意

如果当前交换机已配置为根交换机或者备份根交换机，就不能再配置优先级。如果要配置交换机的优先级，必须先去使能根交换机或者备份根交换机功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp priority** *priority*，配置交换设备在系统中的优先级。

缺省情况下，交换设备的优先级取值是 32768。

版权所有 © 华为技术有限公司

说明

- 如果为当前设备配置系统优先级目的是配置当前设备为根桥设备，则可以直接选择执行命令stp root primary，配置后该设备优先级数值自动为 0。
- 执行命令 stp root secondary 可以配置当前交换设备为备份根桥设备，配置后该设备优先级数值自动为 4096。

  同一台交换设备不能既作为根桥又作为备用根桥。

----结束

（可选）配置端口路径开销

端口路径开销会影响根端口的选择，在一台设备所有使能 STP/RSTP 的端口中，到根桥的路径开销最小者，就是根端口。

背景信息

路径开销是一个端口量，是 STP/RSTP 协议用于选择链路的参考值。

端口路径开销值取值范围由路径开销计算方法决定，当确定路径开销计算方法后，如果端口所处链路的速率值越大，则建议将该端口的路径开销值在指定范围内设置越小。

以华为的私有计算方法为例，不同速率的端口路径开销的缺省值不同，具体参见表 3-15。

表 3-15 端口所对应的链路速率与端口路径开销值对应表

链路速率	推荐值	推荐取值范围	值域
10Mbit/s	2000	200-20000	1-200000
100Mbit/s	200	20-2000	1-200000
1Gbit/s	20	2-200	1-200000
10Gbit/s	2	2-20	1-200000
10Gbit/s 以上	1	1-2	1-200000

存在环路的网络环境中，对于链路速率值相对较小的端口，建议将其路径开销值配置相对较大，以使其在生成树算法中被选举成为阻塞端口，阻塞其所在链路。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }，配置端口路径开销计算方法。

缺省情况下，路径开销值的计算方法为 IEEE 802.1t 标准方法。

同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 4 执行命令 **stp cost** *cost*，设置当前端口的路径开销值。

- 使用华为的私有计算方法时参数 *cost* 取值范围是 1 ～ 200000。
- 使用 IEEE 802.1D 标准方法时取值范围是 1 ～ 65535。
- 使用 IEEE 802.1t 标准方法时取值范围是 1 ～ 200000000。

----结束

（可选）配置端口优先级

交换设备的端口优先级值越小，则在生成树算法中进行指定端口选举时，该端口被指定为指定端口的机率越大；否则，该端口在生成树算法中被阻塞的机率越大。

背景信息

在参与 STP/RSTP 生成树计算时，对于处在环路中的交换设备端口，其优先级的高低会影响到是否被选举为指定端口，详见 **STP/RSTP 概述**。

在根路径开销及发送交换设备的 BID 相同的情况下，如果希望将环路中的某交换设备的端口阻塞从而破除环路，则可将其端口优先级值设置比缺省值大，使得在选举过程中成为被阻塞的端口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 执行命令 **stp port priority** *priority*，配置端口的优先级。

缺省情况下，交换设备端口的优先级取值是 128。

----结束

启用 STP/RSTP

使能 STP/RSTP 功能后，生成树算法才开始计算。

背景信息

在环形网络中一旦启用 STP/RSTP，STP/RSTP 便立即开始进行生成树计算。而且，诸如交换设备的优先级、端口优先级等参数都会影响到生成树的计算，在计算过程中这些参数的变动可能会导致网络震荡。为了保证生成树计算过程快速而且稳定，必须在交换设备及其端口进行必要的基本配置以后才能启用 STP/RSTP。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp enable**，使能交换设备的 STP/RSTP 功能。

缺省情况下，AC6605 的 STP/RSTP 功能处于禁用状态。

----结束

版权所有 © 华为技术有限公司

检查配置结果

STP/RSTP 基本功能配置成功后，可查看生成树算法计算的结果是否符合要求，如：端口角色、端口状态等。

前提条件

已经完成 STP/RSTP 基本功能的配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.8.3 配置 STP/RSTP 影响拓扑收敛的参数

基于 STP 没有对拓扑是否已经收敛制定反馈机制，RSTP 在 STP 基础上实现了快速收敛。

STP 不能实现快速收敛，但是诸如网络直径、Hello Time 定时器、Max Age 定时器、Forward Delay 定时器等参数会影响其收敛速度。RSTP 在 STP 基础上进行改进之后，实现快速收敛。对于 STP/RSTP 影响拓扑收敛的参数，除了上述系统参数外，还有端口的链路类型、端口是否支持快速迁移机制、BPDU 的最大发送数目等端口参数。

对于运行 STP/RSTP 的设备，配置参数情况详见**表 3-16**。

表 3-16 影响 STP/RSTP 拓扑收敛的参数

参数类型	参数含义	涉及命令	说明
系统参数	网络直径和定时器（Hello Time、Forward Delay 和 Max Age）以及 Hello Time 定时器与倍数参数形成的超时时间	● stp bridge-diameter *diameter* ● stp timer hello *hello-time* ● stp timer forward-delay *forward-delay* ● stp timer max-age *max-age* ● stp timer-factor *factor*	建议直接通过配置网络直径控制定时器时间的大小，交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。然后通过 stp timer-factor *factor* 配置超时时间。

华为专有和保密信息
版权所有 © 华为技术有限公司

参数类型	参数含义	涉及命令	说明
端口参数	端口的链路类型	● stp point-to-point { **auto** | **force-false** | **force-true** }	点对点链路帮助实现快速收敛。 ● 如果当前端口工作在全双工模式，则当前端口相连的链路是点对点链路。 ● 如果当前端口工作在半双工模式，可强制链路类型为点对点链路。 ● 其他情况选择端口自动识别是否与点对点链路相连。
	端口迁移到RSTP 模式	● stp mcheck	在运行 RSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。 当端口无法自动迁回 RSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 RSTP 模式。
	端口在每个 Hello Time 时间内 BPDU 的最大发送数目	● stp transmit-limit *packet-number*	适当的配置端口在每个 Hello time 时间内 BPDU 的最大发送数目，可以限制端口发送 BPDU 的速度，防止网络拓扑震荡时 RSTP 占用过多的带宽资源。
	边缘端口的设置	● stp edged-port **enable** ● error-down auto-recovery **cause** *cause-item* **interval** *interval-value*	与终端相连的端口不用参与 STP/RSTP 计算，将该端口配置成边缘端口，该端口便不再参与计算。 在设备上配置 BPDU 保护功能后，边缘端口收到 BPDU 报文会被 Shutdown，可以实现端口在一定的延迟时间后自动恢复为 Up 状态。

建立配置任务

在进行 STP/RSTP 影响快速收敛的参数配置前，请认真了解各项配置的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

华为专有和保密信息
版权所有 © 华为技术有限公司

应用环境

在运行 RSTP 的网络环境中，快速收敛机制的实现需要配置一些影响快速收敛的参数，配置合适的参数后才能实现最佳快速收敛效果。

说明

因为本配置任务中所包含的命令缺省情况下也能完成 RSTP 的快速收敛，所以本配置任务所包含的所有配置过程，以及配置过程中包含的所有配置步骤都是可选的，可根据实际需要选择配置其中的部分内容。

前置任务

在配置 STP/RSTP 影响拓扑收敛的参数前，需完成以下任务：

- 配置 STP/RSTP 基本功能

数据准备

在配置 STP/RSTP 影响拓扑收敛的参数之前，需要准备以下数据。

序号	数据
1	网络直径
2	Hello Time 时间、Forward Delay 时间、Max Age 时间、超时时间（3 x hello time x time factor）
3	端口的链路类型
4	端口是否使用普通的快速迁移机制
5	端口是否需要迁移回 RSTP 模式
6	BPDU 的最大发送数目值
7	端口是否需要设置为边缘端口
8	如果端口为边缘端口，是否需要配置其在 Shutdown 后自动恢复功能
9	端口是否需要清除生成树的统计信息
10	如果端口为边缘端口，是否需要配置端口为 BPDU filter 端口

配置系统参数

影响 STP/RSTP 拓扑收敛的系统参数有网络直径、Hello Time 定时器、未收到上游的 BPDU 就重新开始生成树计算的超时时间（3 x hello time x time factor）等，配置合适的系统参数，实现最快的拓扑收敛。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp bridge-diameter** *diameter*，配置网络直径。

缺省情况下，网络直径为 7。

版权所有 © 华为技术有限公司

- 快速生成树是在整个交换网络应用单生成树实例，不能解决由于网络规模增大带来的性能降低问题，网络直径不要超过 7。
- 建议通过执行命令 **stp bridge-diameter** *diameter* 配置网络直径去配置 Forward Delay 时间、Hello Time 时间以及 Max Age 时间，因为交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。

步骤 3 执行命令 **stp timer-factor** *factor*，配置未收到上游的 BPDU 就重新开始生成树计算的超时时间。

缺省情况下，交换设备未收到上游的 BPDU 就重新开始生成树计算的超时时间是 Hello Timer 的 9 倍。

步骤 4 （可选）若需要对 Forward Delay 时间、Hello Time 时间以及 Max Age 时间直接进行配置，则分别进行如下操作：

- 执行命令 **stp timer forward-delay** *forward-delay*，配置交换设备的 Forward Delay 时间。

  缺省情况下，交换设备的 Forward Delay 时间是 1500 厘秒。
- 执行命令 **stp timer hello** *hello-time*，配置交换设备的 Hello Time 时间。

  缺省情况下，交换设备的 Hello Time 时间是 200 厘秒。
- 执行命令 **stp timer max-age** *max-age*，配置交换设备的 Max Age 时间。

  缺省情况下，交换设备的 Max Age 时间是 2000 厘秒。

说明

根交换设备的 Hello Time、Forward Delay 以及 Max Age 三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡。

- 2 × (Forward Delay − 1.0 second) >= Max Age
- Max Age >= 2 × (Hello Time + 1.0 second)

----结束

配置端口参数

影响 RSTP 拓扑快速收敛的端口参数主要有自动识别端口的链路类型是否为点到点链路、BPDU 的最大发送数目等。配置合适的端口参数，实现 RSTP 最快的拓扑收敛。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp point-to-point** { **auto** | **force-false** | **force-true** }，配置指定端口的链路类型。

缺省情况下，指定端口自动识别是否与点对点链路相连，点对点链路支持快速收敛。

- 如果当前以太网端口工作在全双工模式，则当前端口相连的链路是点到点链路，选择参数 **force-true** 实现快速收敛。
- 如果当前以太网端口工作在半双工模式，可通过执行命令 **stp point-to-point force-true** 强制链路类型为点对点链路，实现快速收敛。

步骤 4 执行命令 **stp mcheck**，执行 MCheck 操作。

版权所有 © 华为技术有限公司

在运行 RSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 RSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 RSTP 模式：

- 运行 STP 的交换设备被关机或移走
- 运行 STP 的交换设备切换为 RSTP 模式

说明

在系统视图下执行命令 **stp mcheck**，所有端口都将执行 MCheck 操作。

步骤 5 执行命令 **stp transmit-limit** *packet-number*，配置端口在每个 Hello Time 时间内 BPDU 的最大发送数目。

缺省情况下，端口在每个 Hello Time 时间内 BPDU 的最大发送数目为 147。

步骤 6 （可选）执行命令 **stp edged-port enable**，将端口配置成边缘端口。

若设备与终端相连，则相连的端口为边缘端口，可执行本操作将该端口配置成边缘端口。

缺省情况下，端口为非边缘端口。

步骤 7 执行命令 **quit**，退回到系统视图。

步骤 8 （可选）执行命令 **error-down auto-recovery cause** *cause-item* **interval** *interval-value*，使能处于 error-down 状态的边缘端口状态自动恢复为 Up 的功能，同时设置接口状态自动恢复为 Up 的延迟时间。

此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

----结束

后续处理

当生成树的拓扑结构发生改变时，和它建立映射关系的 VLAN 的转发路径也将发生变化。此时，交换设备的 ARP 表中与这些 VLAN 相关的表项也需要更新。根据对 ARP 表项的处理方式不同，STP/RSTP 的收敛方式分为 fast 和 normal 两种：

- fast：ARP 表将需要更新的表项直接删除。
- normal：ARP 表中需要更新的表项快速老化。

  交换设备将 ARP 表中这些表项的剩余存活时间置为 0，对这些表项进行老化处理。如果配置的 ARP 老化探测次数大于零，则 ARP 对这些表项进行老化探测。

  这两种方式对 MAC 表项的处理方式相同，都是直接删除。

在系统视图下执行命令 **stp converge** { **fast** | **normal** }，可配置端口的收敛方式。

缺省情况下，端口的 STP/RSTP 收敛方式为 normal。

说明

建议选择 normal 收敛方式。若选择 fast 方式，频繁的 ARP 表项删除可能会导致主控板和接口板 CPU 占用率高达 100%，报文处理超时导致网络震荡。

检查配置结果

在配置 STP/RSTP 影响拓扑收敛的参数后，可以查看配置是否生效。

版权所有 © 华为技术有限公司

前提条件

已经完成影响拓扑收敛的参数配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.8.4 配置 RSTP 保护功能

华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

建立配置任务

在进行 RSTP 保护功能配置前，请认真了解各项配置的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

RSTP 提供如表 3-17 所示的各种保护功能。

表 3-17 RSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

华为专有和保密信息
版权所有 © 华为技术有限公司

保护功能	场景	配置影响
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

前置任务

在配置 RSTP 保护功能之前，需要完成以下任务：

- 配置 RSTP 基本功能

  说明

  在配置 BPDU 保护功能前，需要在交换设备上配置边缘端口。

数据准备

在配置 RSTP 保护功能之前，需要准备以下数据。

序号	数据
1	启动 Root 保护功能的端口号
2	启动环路保护功能的端口号

配置交换设备的 BPDU 保护功能

交换设备上启动 BPDU 保护功能后，如果边缘端口收到 BPDU，交换设备将关闭这些端口，同时通知网管系统。

背景信息

边缘端口直接和用户终端相连，正常情况下，边缘端口不会收到 BPDU 报文。如果攻击者伪造 BPDU 恶意攻击交换设备，当边缘端口接收到 BPDU 报文时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。通过使能 BPDU 保护可以防止伪造 BPDU 恶意攻击。

版权所有 © 华为技术有限公司

说明

请在有边缘端口的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp bpdu-protection**，配置交换设备边缘端口的 BPDU 保护功能。

缺省情况下，交换设备的 BPDU 保护功能处于禁用状态。

----结束

后续处理

如果用户希望被 Shutdown 的边缘端口可自动恢复，可通过配置使能端口自动恢复功能，并设置延迟时间，即在系统视图下执行命令 **error-down auto-recovery cause** *cause-item* **interval** *interval-value*，使能接口管理状态自动恢复为 Up 的功能，并设置接口自动恢复为 Up 的延时时间使被关闭的端口经过延时时间后能够自动恢复。对于参数 **interval** *interval-value*，取值范围是 30 ～ 86400，单位是秒，配置时需要注意两点：

- 取值越小表示接口的管理状态自动恢复为 Up 的延迟时间越短，接口 Up/Down 状态震荡频率越高。
- 取值越大表示接口的管理状态自动恢复为 Up 的延迟时间越长，接口流量中断时间越长。

配置交换设备的 TC 保护功能

启用 TC 保护功能后，在单位时间内，交换设备处理 TC 类型 BPDU 报文的次数可配置，以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护交换设备的目的。

背景信息

如果攻击者伪造拓扑变化 BPDU 报文恶意攻击交换设备，交换设备短时间内会收到很多拓扑变化 BPDU 报文，频繁的删除操作会给设备造成很大的负担，也给网络的稳定带来很大隐患。

启用 TC 保护功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp tc-protection**，使能交换设备对 TC 类型 BPDU 报文的保护功能。

缺省情况下，交换设备的 TC 保护功能处于使能状态。

步骤 3 执行命令 **stp tc-protection threshold** *threshold*，配置交换设备在收到 TC 类型 BPDU 报文后，单位时间内，处理 TC 类型 BPDU 报文并立即刷新转发表项的阈值。

版权所有 © 华为技术有限公司

说明

单位时间的取值与 RSTP 的 Hello Time 一致，可以通过执行命令 stp timer hello *hello-time* 进行配置。

----结束

配置端口的 Root 保护功能

在交换设备上配置 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

背景信息

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换设备有可能会收到优先级更高的 BPDU 报文，使得合法根交换设备失去根交换设备的地位，引起网络拓扑结构的错误变动。这种不合法的拓扑变化，可能会导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。为了防止这种情况发生，可在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

说明

Root 保护是指定端口上的特性。当端口的角色是指定端口时，配置的 Root 保护功能才生效。若在其他类型的端口上配置 Root 保护功能，Root 保护功能不会生效。

请在根交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 执行命令 **stp root-protection**，配置交换设备的 Root 保护功能。

缺省情况下，端口的 Root 保护功能处于关闭状态。

----结束

配置端口的环路保护功能

环路保护功能会抑制由于链路拥塞等原因产生的环路。

背景信息

在运行 RSTP 协议的网络中，根端口和其他阻塞端口状态是依靠不断接收来自上游交换设备的 BPDU 维持。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换设备的 BPDU 时，交换设备会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。为了防止以上情况发生，可部署环路保护功能。

在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 BPDU，端口状态才恢复正常为 Forwarding 状态。

说明

由于 Alternate 端口是根端口的备份端口，如果交换设备上有 Alternate 端口，需要在根端口和 Alternate 端口上同时配置环路保护。

版权所有 © 华为技术有限公司

在交换设备的根端口和 Alternate 端口上进行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入根端口或 Alternate 端口的接口视图。

步骤 3 执行命令 **stp loop-protection**，配置交换设备根端口或 Alternate 端口的环路保护功能。

缺省情况下，端口的环路保护功能处于关闭状态。

----结束

检查配置结果

完成 RSTP 保护功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 RSTP 保护功能的所有配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息，包括是否启用交换设备的 BPDU 保护功能、其他保护类型等信息。

----结束

3.8.5 配置 STP/RSTP 支持和其他制造商设备互通的参数

为了实现与其他制造商设备的互通，需要在华为公司运行 STP/RSTP 的设备上配置相应的参数，以确保通信畅通。

建立配置任务

配置 STP/RSTP 支持和其他制造商设备互通的参数前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在运行 STP/RSTP 的网络中，因为协议格式不一致等原因会导致设备无法正常互通，在这种情况下，需要配置 STP/RSTP 支持和其他制造商设备互通的参数来实现互通。

前置任务

在配置 STP/RSTP 支持和其他制造商设备互通的参数前，需完成以下任务：

- 配置 STP/RSTP 基本功能

数据准备

在配置 STP/RSTP 支持和其他制造商设备互通的参数之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	收发 BPDU 报文的格式

配置端口 Proposal/Agreement 机制的迁移方式

为了实现华为公司的数据通信与其他制造商设备互通，需要根据其他制造商设备的 P/A 机制选择端口的快速迁移方式。

背景信息

Proposal/Agreement 机制，目前交换设备的端口支持以下两种方式：

- 增强方式：当前接口在计算同步标志位时计算根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口。
  - 上游设备继续发送 Agreement 报文，下游设备接收到后，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。
- 普通方式：当前接口在计算同步标志位时忽略根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。

华为数据通信设备和其他制造商的设备进行互通时，需要根据其他制造商设备的 Proposal/Agreement 机制，选择接口使用增强的快速迁移机制还是普通的快速迁移机制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 执行命令 **stp no-agreement-check**，配置端口使用普通的快速迁移方式。

缺省情况下，端口使用增强的快速迁移机制。

----结束

检查配置结果

在配置 STP/RSTP 支持和其他制造商设备互通的参数后，通过检查配置结果可以查看是否生效。

前提条件

配置 STP/RSTP 支持和其他制造商设备互通的参数已经完成。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息。

----结束

3.8.6 维护 STP/RSTP

STP/RSTP 相关维护命令，包括清除 STP/RSTP 的统计数据。

清除 STP/RSTP 统计信息

通过 **reset** 命令可以将 STP/RSTP 统计计数置 0，便于重新统计。

背景信息

注意

清除 STP/RSTP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 STP/RSTP 的统计信息后，请在用户视图下执行以下命令。

操作步骤

步骤 1 执行命令 **reset stp** [**interface** *interface-type interface-number*] **statistics**，清除生成树的统计信息。

----结束

3.8.7 配置举例

配置举例结合组网需求、配置思路和数据准备来了解实际网络中 STP/RSTP 的应用场景，并提供配置文件。

配置 STP 功能示例

通过本示例，了解 STP 的基本功能，帮助您配置 STP 基本功能。

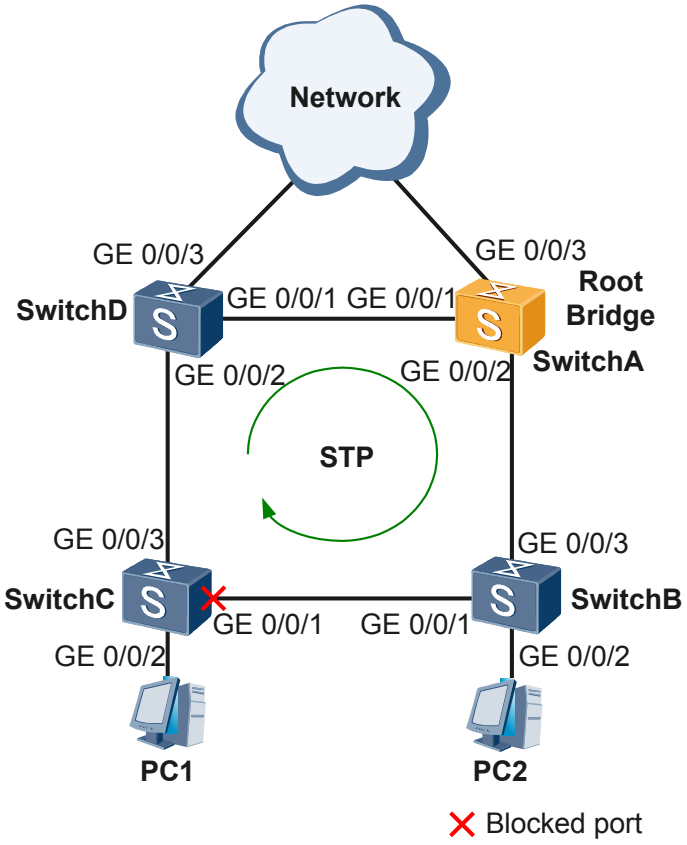
组网需求

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可以在网络中部署 STP 协议预防环路。当网络中存在环路，STP 通过阻塞某个端口以达到破除环路的目的。如图 3-46 所示，当前网络中存在环路，SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 STP，通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

版权所有 © 华为技术有限公司

图 3-46 配置 STP 功能组网图



配置思路

采用以下思路配置 STP 功能：

1. 在处于环形网络中的交换设备上配置 STP 基本功能，包括：
   a. 配置环网中的设备生成树协议工作在 STP 模式。
   b. 配置根桥和备份根桥设备。
   c. 配置端口的路径开销值，实现将该端口阻塞。
   d. 使能 STP，实现破除环路。

   说明

   与 PC 机相连的端口不用参与 STP 计算，建议将其去使能 STP。

数据准备

为完成此配置举例，需要准备如下的数据：

- 各 GE 端口号，如图 3-46 所示
- 根桥是 SwitchA，备份根桥是 SwitchD
- 阻塞口的路径开销值是 20000

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 STP 基本功能

1. 配置环网中的设备生成树协议工作在 STP 模式

   # 配置 SwitchA 的 STP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchA
   [SwitchA] stp mode stp
   ```

   # 配置交换设备 SwitchB 的 STP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchB
   [SwitchB] stp mode stp
   ```

   # 配置交换设备 SwitchC 的 STP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchC
   [SwitchC] stp mode stp
   ```

   # 配置交换设备 SwitchD 的 STP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchD
   [SwitchD] stp mode stp
   ```

2. 配置根桥和备份根桥设备

   # 配置 SwitchA 为根桥。

   ```
   [SwitchA] stp root primary
   ```

   # 配置 SwitchD 为备份根桥。

   ```
   [SwitchD] stp root secondary
   ```

3. 配置端口的路径开销值，实现将该端口阻塞

   说明

   - 端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为私有计算方法为例，配置将被阻塞端口的路径开销值为 20000。
   - 同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

   # 配置 SwitchC 端口 GE0/0/1 端口路径开销值为 20000。

   ```
   [SwitchC] interface gigabitethernet 0/0/1
   [SwitchC-GigabitEthernet0/0/1] stp cost 20000
   [SwitchC-GigabitEthernet0/0/1] quit
   ```

4. 使能 STP，实现破除环路

   - 将与 PC 机相连的端口去使能 STP

     # 配置 SwitchB 端口 GE0/0/2 的 STP 去使能。

     ```
     [SwitchB] interface gigabitethernet 0/0/2
     [SwitchB-GigabitEthernet0/0/2] stp disable
     [SwitchB-GigabitEthernet0/0/2] quit
     ```

     # 配置 SwitchC 端口 GE0/0/2 的 STP 去使能。

     ```
     [SwitchC] interface gigabitethernet 0/0/2
     [SwitchC-GigabitEthernet0/0/2] stp disable
     [SwitchC-GigabitEthernet0/0/2] quit
     ```

   - 设备全局使能 STP

     # 设备 SwitchA 全局使能 STP。

     ```
     [SwitchA] stp enable
     ```

     # 设备 SwitchB 全局使能 STP。

     ```
     [SwitchB] stp enable
     ```


版权所有 © 华为技术有限公司

设备 SwitchC 全局使能 STP。

```
[SwitchC] stp enable
```

设备 SwitchD 全局使能 STP。

```
[SwitchD] stp enable
```

- 除与终端设备相连的端口外，其他端口使能 BPDU 功能

设备 SwitchA 端口 GE0/0/1 和 GE0/0/2 使能 BPDU。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] bpdu enable
[SwitchA-GigabitEthernet0/0/2] quit
```

设备 SwitchB 端口 GE0/0/1 和 GE0/0/3 使能 BPDU。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] bpdu enable
[SwitchB-GigabitEthernet0/0/3] quit
```

设备 SwitchC 端口 GE0/0/1 和 GE0/0/3 使能 BPDU。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] bpdu enable
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/3
[SwitchC-GigabitEthernet0/0/3] bpdu enable
[SwitchC-GigabitEthernet0/0/3] quit
```

设备 SwitchD 端口 GE0/0/1 和 GE0/0/2 使能 BPDU。

```
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] bpdu enable
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] bpdu enable
[SwitchD-GigabitEthernet0/0/2] quit
```

步骤 2 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

在 SwitchA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[SwitchA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1            DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2            DESI  FORWARDING      NONE
```

将 SwitchA 配置为根桥后，与 SwitchB、SwitchD 相连的端口 GE0/0/2 和 GE0/0/1 在生成树计算中被选举为指定端口。

在 SwitchB 上执行 **display stp interface gigabitethernet 0/0/1 brief** 命令，查看端口 GE0/0/1 状态，结果如下：

```
[SwitchB] display stp interface gigabitethernet 0/0/1 brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1            DESI  FORWARDING      NONE
```

端口 GE0/0/1 在生成树选举中成为指定端口，处于 Forwarding 状态。

在 SwitchC 上执行 **display stp brief** 命令，查看端口状态，结果如下：

```
[SwitchC] display stp brief
 MSTID  Port                        Role  STP State     Protection
```


版权所有 © 华为技术有限公司

```
0    GigabitEthernet0/0/1            ALTE  DISCARDING    NONE
0    GigabitEthernet0/0/3            ROOT  FORWARDING    NONE
```

端口 GE0/0/3 在生成树选举中成为根端口，处于 **FORWARDING** 状态。

端口 GE0/0/1 在生成树选举中成为 Alternate 端口，处于 **DISCARDING** 状态。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 stp mode stp
 stp instance 0 root primary
 stp enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 stp mode stp
 stp enable
#
interface GigabitEthernet0/0/2
 stp disable
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 stp mode stp
 stp enable
#
interface GigabitEthernet0/0/1
 stp instance 0 cost 20000
#
interface GigabitEthernet0/0/2
 stp disable
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 stp mode stp
 stp instance 0 root secondary
 stp enable
#
return
```

配置 RSTP 功能示例

通过本示例，了解 RSTP 的基本功能，帮助您配置 RSTP 基本功能。

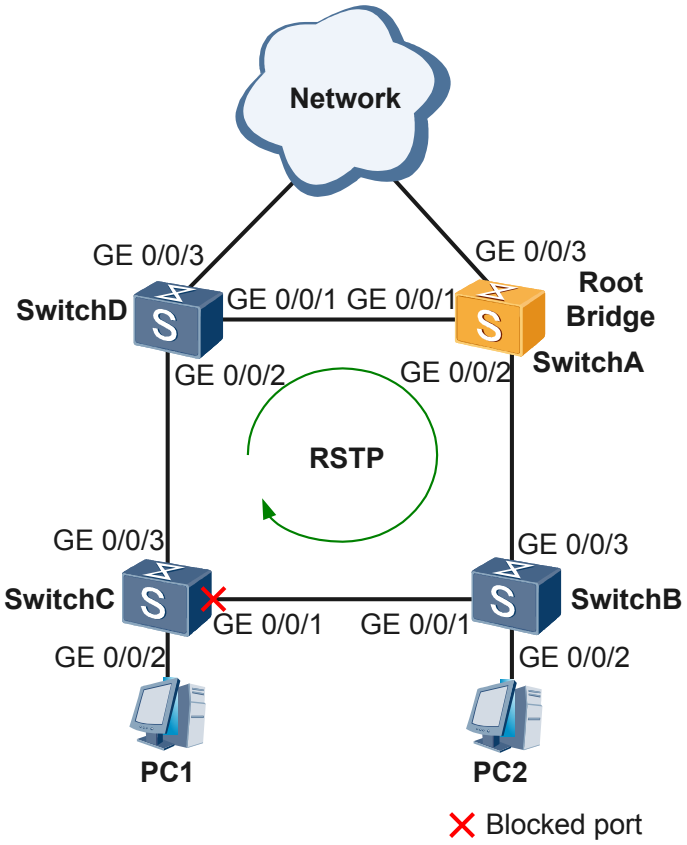
版权所有 © 华为技术有限公司

组网需求

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可以在网络中部署 RSTP 协议预防环路。当网络中存在环路，RSTP 通过阻塞某个端口以达到破除环路的目的。如图 3-47 所示，当前网络中存在环路，SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 RSTP，通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

图 3-47 配置 RSTP 功能组网图



配置思路

采用以下思路配置 RSTP 功能：

1. 在处于环形网络中的交换设备上配置 RSTP 基本功能，包括：
   a. 配置环网中的设备生成树协议工作在 RSTP 模式。
   b. 配置根桥和备份根桥设备。
   c. 配置端口的路径开销值，实现将该端口阻塞。
   d. 使能 RSTP，实现破除环路。

版权所有 © 华为技术有限公司

说明

与 PC 机相连的端口不用参与 RSTP 计算，建议将其去使能 RSTP。

2. 配置保护功能，实现对设备或链路的保护。例如：在根桥设备的指定端口配置根保护功能。

数据准备

为完成此配置举例，需要准备如下的数据：

- 各 GE 端口号，如图 3-47 所示
- 根桥是 SwitchA，备份根桥是 SwitchD
- 阻塞口的路径开销值是 20000

操作步骤

步骤 1 配置 RSTP 基本功能

1. 配置环网中的设备生成树协议工作在 RSTP 模式

   # 配置 SwitchA 的 RSTP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchA
   [Switch] stp mode rstp
   ```

   # 配置交换设备 SwitchB 的 RSTP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchB
   [SwitchB] stp mode rstp
   ```

   # 配置交换设备 SwitchC 的 RSTP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchC
   [SwitchC] stp mode rstp
   ```

   # 配置交换设备 SwitchD 的 RSTP 工作模式。

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchD
   [SwitchD] stp mode rstp
   ```

2. 配置根桥和备份根桥设备

   # 配置 SwitchA 为根桥。

   ```
   [SwitchA] stp root primary
   ```

   # 配置 SwitchD 为备份根桥。

   ```
   [SwitchD] stp root secondary
   ```

3. 配置端口的路径开销值，实现将该端口阻塞

   说明

   - 端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为私有计算方法为例，配置将被阻塞端口的路径开销值为 20000。
   - 同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

   # 配置 SwitchC 端口 GE0/0/1 端口路径开销值为 20000。

   ```
   [SwitchC] interface gigabitethernet 0/0/1
   [SwitchC-GigabitEthernet0/0/1] stp cost 20000
   [SwitchC-GigabitEthernet0/0/1] quit
   ```

4. 使能 RSTP，实现破除环路

   - 将与 PC 机相连的端口去使能 RSTP

版权所有 © 华为技术有限公司

配置 SwitchB 端口 GE0/0/2 的 RSTP 去使能。

```
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] stp disable
[SwitchB-GigabitEthernet0/0/2] quit
```

配置 SwitchC 端口 GE0/0/2 的 RSTP 去使能。

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] stp disable
[SwitchC-GigabitEthernet0/0/2] quit
```

- 设备全局使能 RSTP

  # 设备 SwitchA 全局使能 RSTP。

  ```
  [SwitchA] stp enable
  ```

  # 设备 SwitchB 全局使能 RSTP。

  ```
  [SwitchB] stp enable
  ```

  # 设备 SwitchC 全局使能 RSTP。

  ```
  [SwitchC] stp enable
  ```

  # 设备 SwitchD 全局使能 RSTP。

  ```
  [SwitchD] stp enable
  ```

- 除与终端设备相连的端口外，其他端口使能 BPDU 功能

  # 设备 SwitchA 端口 GE0/0/1 和 GE0/0/2 使能 BPDU。

  ```
  [SwitchA] interface gigabitethernet 0/0/1
  [SwitchA-GigabitEthernet0/0/1] bpdu enable
  [SwitchA-GigabitEthernet0/0/1] quit
  [SwitchA] interface gigabitethernet 0/0/2
  [SwitchA-GigabitEthernet0/0/2] bpdu enable
  [SwitchA-GigabitEthernet0/0/2] quit
  ```

  # 设备 SwitchB 端口 GE0/0/1 和 GE0/0/3 使能 BPDU。

  ```
  [SwitchB] interface gigabitethernet 0/0/1
  [SwitchB-GigabitEthernet0/0/1] bpdu enable
  [SwitchB-GigabitEthernet0/0/1] quit
  [SwitchB] interface gigabitethernet 0/0/3
  [SwitchB-GigabitEthernet0/0/3] bpdu enable
  [SwitchB-GigabitEthernet0/0/3] quit
  ```

  # 设备 SwitchC 端口 GE0/0/1 和 GE0/0/3 使能 BPDU。

  ```
  [SwitchC] interface gigabitethernet 0/0/1
  [SwitchC-GigabitEthernet0/0/1] bpdu enable
  [SwitchC-GigabitEthernet0/0/1] quit
  [SwitchC] interface gigabitethernet 0/0/3
  [SwitchC-GigabitEthernet0/0/3] bpdu enable
  [SwitchC-GigabitEthernet0/0/3] quit
  ```

  # 设备 SwitchD 端口 GE0/0/1 和 GE0/0/2 使能 BPDU。

  ```
  [SwitchD] interface gigabitethernet 0/0/1
  [SwitchD-GigabitEthernet0/0/1] bpdu enable
  [SwitchD-GigabitEthernet0/0/1] quit
  [SwitchD] interface gigabitethernet 0/0/2
  [SwitchD-GigabitEthernet0/0/2] bpdu enable
  [SwitchD-GigabitEthernet0/0/2] quit
  ```

步骤 2 配置保护功能，如在根桥设备的指定端口配置根保护功能

在 SwitchA 端口 GE0/0/1 上配置根保护功能。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp root-protection
[SwitchA-GigabitEthernet0/0/1] quit
```

在 SwitchA 端口 GE0/0/2 上配置根保护功能。

版权所有 © 华为技术有限公司

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp root-protection
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤 3 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

在 SwitchA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[SwitchA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1            DESI  FORWARDING      ROOT
   0    GigabitEthernet0/0/2            DESI  FORWARDING      ROOT
```

将 SwitchA 配置为根桥后，与 SwitchB、SwitchD 相连的端口 GE0/0/2 和 GE0/0/1 在生成树计算中被选举为指定端口，并在指定端口上配置根保护功能。

在 SwitchB 上执行 **display stp interface gigabitethernet 0/0/1 brief** 命令，查看端口 GE0/0/1 状态，结果如下：

```
[SwitchB] display stp interface gigabitethernet 0/0/1 brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1            DESI  FORWARDING      NONE
```

端口 GE0/0/1 在生成树选举中成为指定端口，处于 Forwarding 状态。

在 SwitchC 上执行 **display stp brief** 命令，查看端口状态，结果如下：

```
[SwitchC] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1            ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/3            ROOT  FORWARDING      NONE
```

端口 GE0/0/3 在生成树选举中成为根端口，处于 **FORWARDING** 状态。

端口 GE0/0/1 在生成树选举中成为 Alternate 端口，处于 **DISCARDING** 状态。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 stp mode rstp
 stp instance 0 root primary
 stp enable
#
interface GigabitEthernet0/0/1
 stp root-protection
#
interface GigabitEthernet0/0/2
 stp root-protection
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 stp mode rstp
 stp enable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/2
 stp disable
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 stp mode rstp
 stp enable
#
interface GigabitEthernet0/0/1
 stp instance 0 cost 20000
#
interface GigabitEthernet0/0/2
 stp disable
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 stp mode rstp
 stp instance 0 root secondary
 stp enable
#
return
```

3.9 MSTP 配置

MSTP（Multiple Spanning Tree Protocol，多生成树协议）将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

3.9.1 MSTP 简介

MSTP 通过设置 VLAN 映射表把 VLAN 和生成树实例联系起来，通过多生成树实例实现业务流量的负载均衡。

MSTP 概述

MSTP 功能兼容 STP 和 RSTP 功能，同时弥补 STP 和 RSTP 的缺陷。MSTP 既可以快速收敛，又能为冗余链路提供更好的负载分担。

MSTP 背景

STP 和 RSTP 是用于局域网中预防和消除环路的协议，运行 STP/RSTP 协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

STP 和 RSTP 存在同一个缺陷：由于局域网内所有的 VLAN 共享一棵生成树，因此无法在 VLAN 间实现数据流量的负载均衡，链路被阻塞后将不承载任何流量，造成带宽浪费，还有可能造成部分 VLAN 的报文无法转发。

版权所有 © 华为技术有限公司

为了弥补 STP 和 RSTP 的缺陷，IEEE 于 2002 年发布的 802.1S 标准定义了 MSTP。MSTP 兼容 STP 和 RSTP，既可以快速收敛，又提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

STP/RSTP/MSTP 三种生成树协议的特点与应用场景比较如表 3-18 所示。

表 3-18 三种生成树协议的比较

生成树协议	特点	应用场景	注意事项
STP	形成一棵无环路的树：解决广播风暴并实现冗余备份。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。	**说明** ● 若当前交换设备只支持 STP，建议选择使用 STP，详见 **STP/RSTP 配置**。 ● 若当前交换设备既支持 STP 又支持 RSTP，建议使用 RSTP，详见 **STP/RSTP 配置**。 ● 若当前交换设备既支持 STP/RSTP 又支持 MSTP，建议选择使用 MSTP。
RSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。		
MSTP	● 形成一棵或多棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。 ● 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。	

MSTP 概述

在一个复杂的网络环境中，难免会出现环路；并且，由于冗余备份的需要，网络设计者都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样，偶然或必然中都会存在环路。

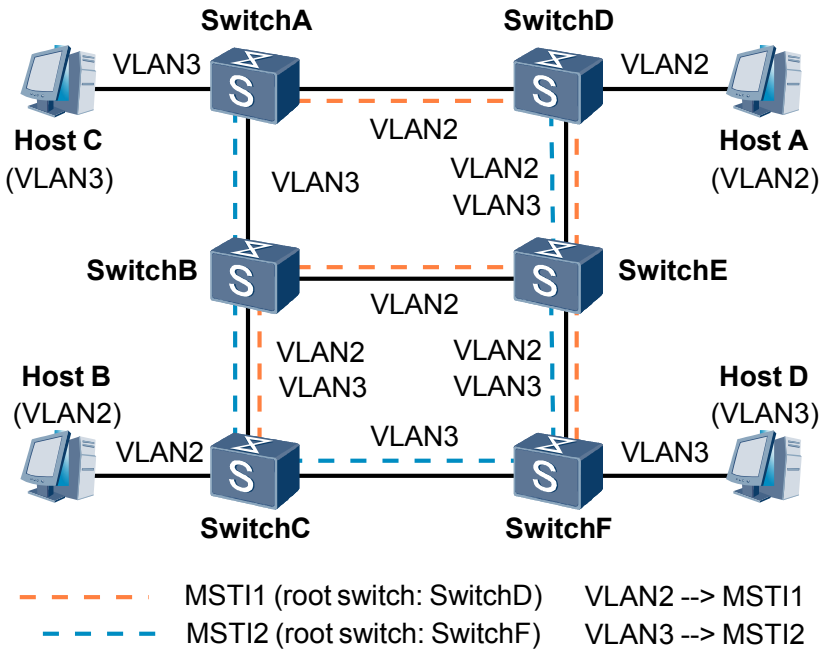
环路会产生广播风暴，最终导致整个网络资源被耗尽，网络瘫痪不可用。环路还会引起 MAC 地址表震荡导致 MAC 地址表项被破坏。

MSTP 兼容 STP 和 RSTP，通过多实例能实现对业务流量和用户流量的隔离，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

现将 MSTP 应用于图 3-48 中的局域网，应用后生成 MSTI 如图 3-48 所示。

版权所有 © 华为技术有限公司

图 3-48 MST 域内的多棵生成树示意图



- MSTI1 以 SwitchD 为根交换设备，转发 VLAN2 的报文。
- MSTI2 以 SwitchF 为根交换设备，转发 VLAN3 的报文。

这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负载分担。

MSTP 基本概念

- MST 域（MST Region）

  MST 域是多生成树域（Multiple Spanning Tree Region），由交换网络中的多台交换设备以及它们之间的网段所构成。这些设备具有下列特点：

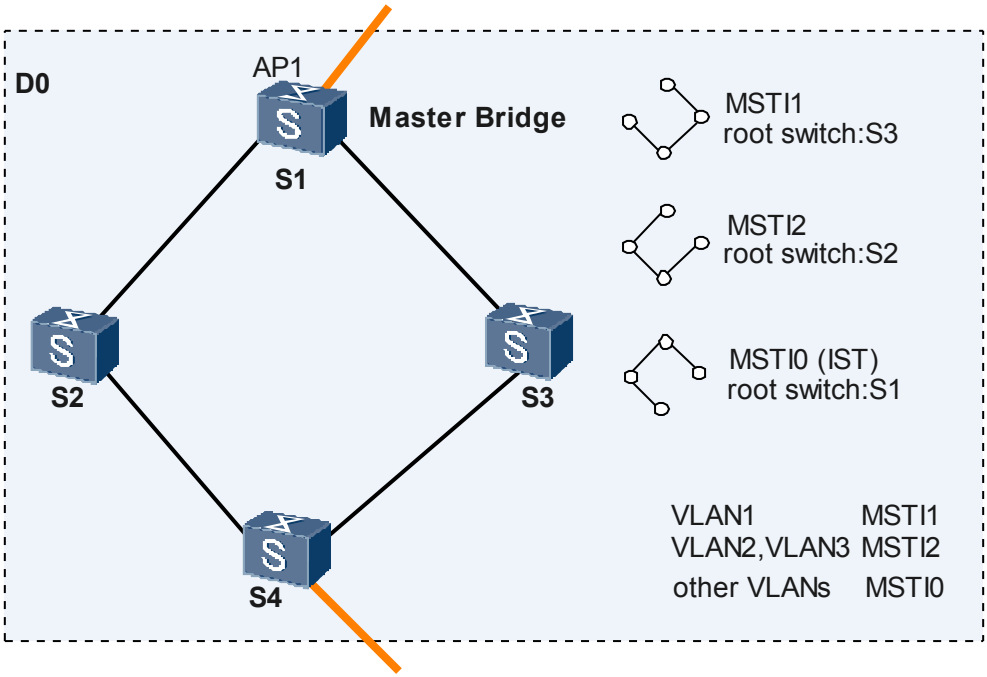
  - 都启动了 MSTP。
  - 具有相同的域名。
  - 具有相同的 VLAN 到生成树实例映射配置。
  - 具有相同的 MSTP 修订级别配置。

  一个局域网可以存在多个 MST 域，各 MST 域之间在物理上直接或间接相连。用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

  如图 3-49 所示的 MST Region D0 中由交换设备 S1、S2、S3 和 S4 构成，域中有 3 个 MSTI。

版权所有 © 华为技术有限公司

图 3-49 MST Region 的基本概念示意图



- VLAN 映射表

  VLAN 映射表是 MST 域的属性，它描述了 VLAN 和 MSTI 之间的映射关系。

  如图 3-49 所示，MST 域 D0 的 VLAN 映射表是：

  - VLAN1 映射到 MSTI1
  - VLAN2 和 VLAN3 映射到 MSTI2
  - 其余 VLAN 映射到 MSTI0

- 域根

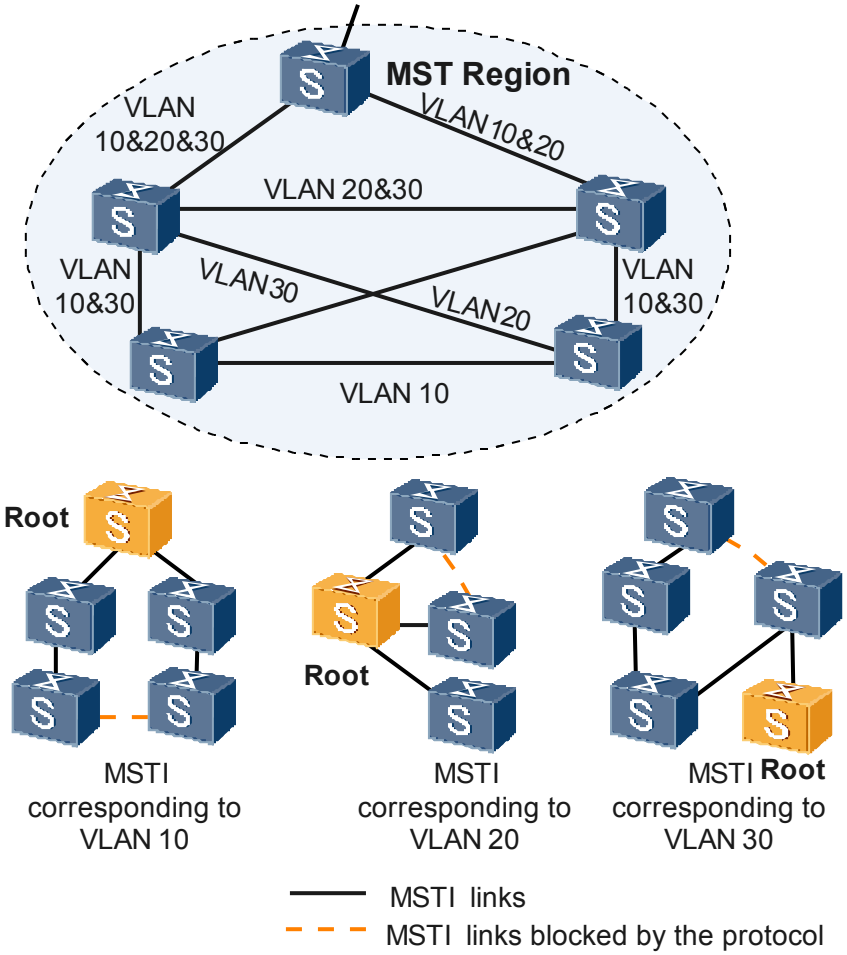
  域根（Regional Root）分为 IST（Internal Spanning Tree）域根和 MSTI 域根。

  IST 域根如图 3-51 所示，在 B0、C0 和 D0 中，IST 生成树中距离总根（CIST Root）最近的交换设备是 IST 域根。

  一个 MST 域内可以生成多棵生成树，每棵生成树都称为一个 MSTI。MSTI 域根是每个多生成树实例的树根。如图 3-50 所示，域中不同的 MSTI 有各自的域根。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-50 MSTI 的基本概念示意图

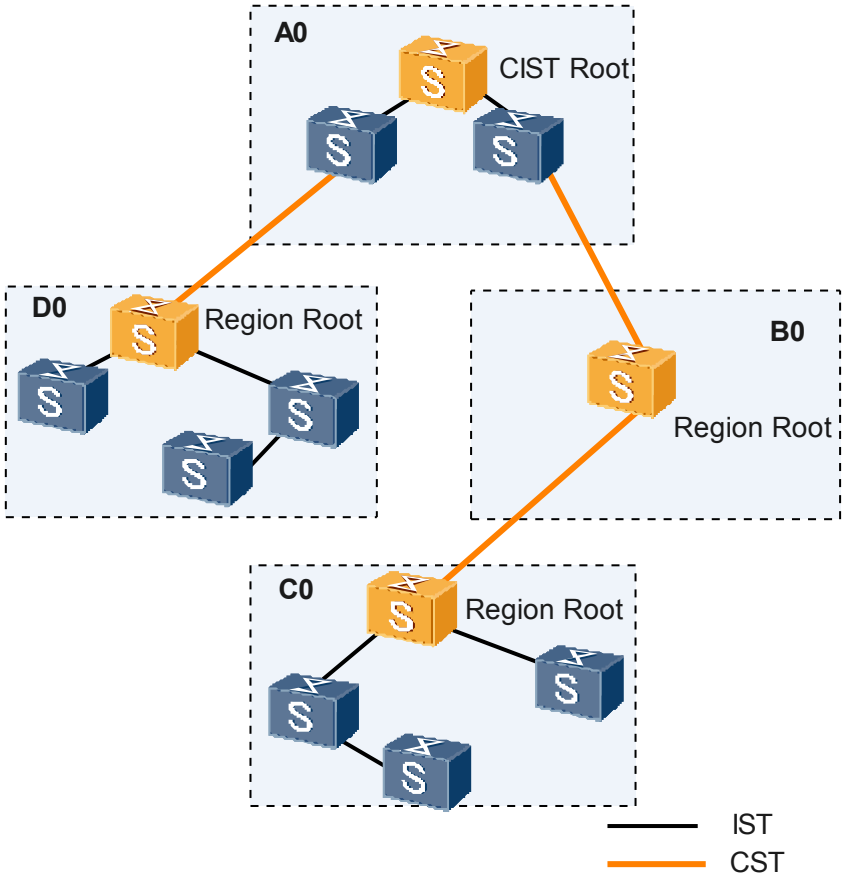


MSTI 之间彼此独立，MSTI 可以与一个或者多个 VLAN 对应。但一个 VLAN 只能与一个 MSTI 对应。

- 总根

版权所有 © 华为技术有限公司

图 3-51 MSTP 网络基本概念示意图



如图 3-51 所示，总根是 CIST（Common and Internal Spanning Tree）的根桥。总根是区域 A0 中的某台设备。

- CST

  公共生成树 CST（Common Spanning Tree）是连接交换网络内所有 MST 域的一棵生成树。

  如果把每个 MST 域看作是一个节点，CST 就是这些节点通过 STP 或 RSTP 协议计算生成的一棵生成树。

  如图 3-51 所示，较粗的线条连接各个域构成 CST。

- IST

  内部生成树 IST（Internal Spanning Tree）是各 MST 域内的一棵生成树。

  IST 是一个特殊的 MSTI，MSTI 的 ID 为 0，通常称为 MSTI0。

  IST 是 CIST 在 MST 域中的一个片段。

  如图 3-51 所示，较细的线条在域中连接该域的所有交换设备构成 IST。

- CIST

  公共和内部生成树 CIST 是通过 STP 或 RSTP 协议计算生成的，连接一个交换网络内所有交换设备的单生成树。

  如图 3-51 所示，所有 MST 域的 IST 加上 CST 就构成一棵完整的生成树，即 CIST。

- SST

版权所有 © 华为技术有限公司

构成单生成树 SST（Single Spanning Tree）有两种情况：

- 运行 STP 或 RSTP 的交换设备只能属于一个生成树。
- MST 域中只有一个交换设备，这个交换设备构成单生成树。

如图 3-51 所示，B0 中的交换设备就是一棵单生成树。

- 端口角色

MSTP 在 RSTP 的基础上新增了 2 种端口，MSTP 的端口角色共有 7 种：根端口、指定端口、Alternate 端口、Backup 端口、边缘端口、Master 端口和域边缘端口。

根端口、指定端口、Alternate 端口、Backup 端口和边缘端口的作用同 RSTP 协议中定义，MSTP 中定义的所有端口角色如表 3-19 所示。

说明

除边缘端口外，其他端口角色都参与 MSTP 的计算过程。

同一端口在不同的生成树实例中可以担任不同的角色。

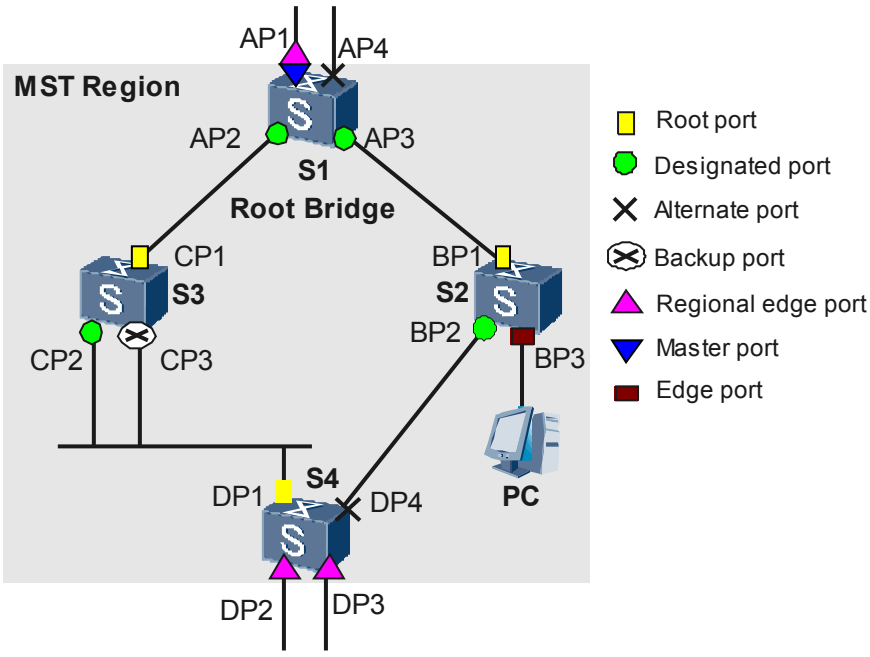
表 3-19 端口角色

端口角色	说明
根端口	在非根桥上，离根桥最近的端口是本交换设备的根端口。根交换设备没有根端口。 根端口负责向树根方向转发数据。 如图 3-52 所示，S1 为根桥，CP1 为 S3 的根端口，BP1 为 S2 的根端口，DP1 为 S4 的根端口。
指定端口	对一台交换设备而言，它的指定端口是向下游交换设备转发 BPDU 报文的端口。 如图 3-52 所示，AP2 和 AP3 为 S1 的指定端口，BP2 为 S2 的指定端口，CP2 为 S3 的指定端口。
Alternate 端口	● 从配置 BPDU 报文发送角度来看，Alternate 端口就是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。 ● 从用户流量角度来看，Alternate 端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口。 如图 3-52 所示，BP2 和 AP4 为 Alternate 端口。
Backup 端口	● 从配置 BPDU 报文发送角度来看，Backup 端口就是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。 ● 从用户流量角度来看，Backup 端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。 如图 3-52 所示，CP3 为 Backup 端口。
Master 端口	Master 端口是 MST 域和总根相连的所有路径中最短路径上的端口。 Master 端口是域中的报文去往总根的必经之路。 Master 端口是特殊域边缘端口，Master 端口在 IST/CIST 上的角色是 Root Port，在其它各实例上的角色都是 Master 端口。 如图 3-52 所示，交换设备 S1、S2、S3、S4 和它们之间的链路构成一个 MST 域，S1 交换设备的端口 AP1 在域内的所有端口中到总根的路径开销最小，所以 AP1 为 Master 端口。

华为专有和保密信息
版权所有 © 华为技术有限公司

端口角色	说明
域边缘端口	域边缘端口是指位于 MST 域的边缘并连接其它 MST 域或 SST 的端口。 进行 MSTP 计算时，域边缘端口在 MSTI 上的角色和 CIST 实例的角色保持一致。即如果边缘端口在 CIST 实例上的角色是 Master 端口（连接域到总根的端口），则它在域内所有 MSTI 上的角色也是 Master 端口。 如图 3-52 所示，MST 域内的 AP1、DP2 和 DP3 都和其它域直接相连，它们都是本 MST 域的边缘端口。 如图 3-52，AP1 是域边缘端口，它在 CIST 上的角色是 Master 端口，则 AP1 在 MST 域内所有生成树实例上的角色都是 Master 端口。
边缘端口	如果指定端口位于整个域的边缘，不再与任何交换设备连接，这种端口叫做边缘端口。 边缘端口一般与用户终端设备直接连接。 如图 3-52 所示，BP3 为边缘端口。

图 3-52 端口角色示意图



- 端口状态

  MSTP 定义的端口状态与 RSTP 协议中定义相同，如表 3-20 所示。

版权所有 © 华为技术有限公司

表 3-20 端口状态

端口状态	说明
Forwarding	在这种状态下，端口既转发用户流量又接收/发送 BPDU 报文。
Learning	这是一种过渡状态。在 Learning 下，交换设备会根据收到的用户流量，构建 MAC 地址表，但不转发用户流量，所以叫做学习状态。 Learning 状态的端口接收/发送 BPDU 报文，不转发用户流量。
Discarding	Discarding 状态的端口只接收 BPDU 报文。

端口状态和端口角色是没有必然联系的，**表 3-21** 显示了各种端口角色能够具有的端口状态。

表 3-21 端口角色

端口状态	根端口/Master 端口	指定端口	域边缘端口	Alternate 端口	Backup 端口
Forwarding	Yes	Yes	Yes	No	No
Learning	Yes	Yes	Yes	No	No
Discarding	Yes	Yes	Yes	Yes	Yes

Yes：表示端口支持的状态。

No：表示端口不支持的状态。

AC6605 支持的 MSTP 特性

配置 MSTP 时，您将接触到基本功能、拓扑收敛、保护功能、多进程以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

MSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。同时，MSTP 引入多实例，通过将不同 VLAN 映射到不同实例中，实现不同 VLAN 的流量负载分担。MSTP 的基本配置思路如下：

1. 在环形网络中，划分域，在域中配置不同的实例。
2. 为各个实例选出其中的一个交换设备作为根桥（Root bridge）。
3. 在各个实例中，计算出其他交换设备到根桥的最短路径，为每个非根交换设备选举一个根端口。
4. 在各个实例中，通过端口 ID 为每个连接选举出一个指定端口。

版权所有 © 华为技术有限公司

根据不同的组网情况，可能还会涉及到 Backup 端口、Master 端口等端口角色的确认，详见 **MSTP 端口描述**。

为了满足特殊场合的应用和扩展功能，MSTP 还支持如下功能：

- MSTP 通过 Proposal/Agreement 机制等实现快速收敛。
- MSTP 提供如**表 3-22** 所示的保护功能。
- 在 MSTP 和 STP/RSTP 混合应用场景中，MSTP 多进程实现如**图 3-53** 所示接入层各个接入环的相互生成树计算独立。
- 为了实现与其他制造商设备的互通，需要在华为公司运行 MSTP 的设备上配置合适的参数，以确保通信畅通。

表 3-22 MSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的 BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

版权所有 © 华为技术有限公司

保护功能	场景	配置影响
共享链路保护	在交换设备双归属接入网络的组网中，当多个进程的共享链路故障时，可能会引起环路。	当共享链路故障时，通过共享链路保护功能，使本设备的工作模式强制转换为RSTP，配合使用根保护功能，可以避免网络环路。

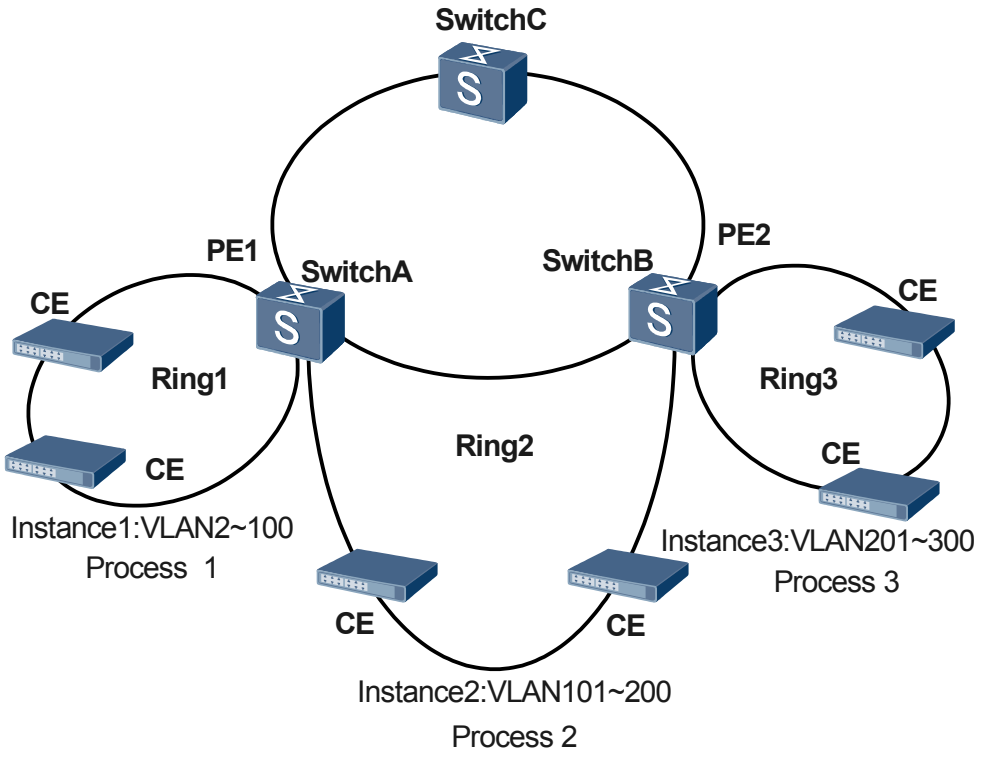
MSTP 多进程

- 背景信息

  在二层单接环和二层双接环混合组网环境下，交换设备同时承载二三层业务。为了实现不同的环完成不同的业务，可在该组网上部署 MSTP 多进程，实现不同环上的生成树协议进行独立计算，互不影响。

  如图 3-53 所示，SwitchA、SwitchB 和 SwitchC 之间通过二层链路相连，并且同时启动 MSTP 协议。环上的 CE 设备只支持 STP/RSTP 协议并且存在多个接入环，不同的接入环在 SwitchA 和 SwitchB 上通过不同的端口接入。

  图 3-53 MSTP 多进程的典型组网



如图 3-53 所示网络中，存在多个二层接入环 Ring1、Ring2 和 Ring3，因此需要在这些环路上启用生成树协议来防止环路。SwitchA 和 SwitchB 同时连接了多个接入环，各个环之间互相独立，不需要互通，这样在启动生成树时就不能将所有的接入环路计算成一个大生成树，需要各个接入环上的生成树协议进行独立计算，互不影响。

对于 MSTP 协议标准来说，本身可以支持生成树多实例，只是要求所有设备支持 MSTP 且所有设备的 MSTP 域配置必须一致。而组网图中与交换设备相连的 CE 设

版权所有 © 华为技术有限公司

备只支持 STP/RSTP 协议。根据 MSTP 协议标准，交换设备收到来自 CE 的 STP/RSTP 报文后，则认为彼此不属于同一个域。如果按照标准的 MSTP 协议，交换设备和CE 环只会计算出一个生成树，不能实现各个接入环的相互独立。

在这种情况下，可以使用 MSTP 多进程的功能。在 SwitchA 和 SwitchB 上运行多个 MSTP 进程，每个 MSTP 进程功能相同，也支持生成多实例，每个 MSTP 进程对应一个接入环。

使用 MSTP 多进程功能后，每个 MSTP 进程可以管理设备上的部分端口，即设备的二层端口资源被多个 MSTP 进程分割管理，每个 MSTP 进程上都运行标准的 MSTP。

说明

如果 CE 设备支持 MSTP 协议，也可以配置 MSTP 多进程。

正常启动后，设备默认存在 ID 为 0 的 MSTP 进程，系统视图和接口视图中的 MSTP 相关配置都属于此进程。

- 共享链路

  如图 3-53 所示，SwitchA 和 SwitchB 之间的链路是二层链路，并运行 MSTP 协议。SwitchA 和 SwitchB 之间的共享链路和接入 CE 链路的不同在于：共享链路上的端口需要参与多个接入环和多个 MSTP 进程的计算，这样 SwitchA 和 SwitchB 之间的 MSTP 协议报文就需要能区分是来自哪个进程的 MSTP 协议报文。

  此外，共享链路上的同一个端口同时参与多个 MSTP 进程的计算，多个 MSTP 进程中都会计算出端口状态，这样端口就可能同时存在多个状态，从而无法决定采用哪个生成树的状态。

  对于上述情况，共享链路上的端口虽然参与多个 MSTP 进程的状态计算，但是只具有 MSTP 进程 0 的状态，不会影响其他 MSTP 进程。

说明

AC6605 不支持 PVST 协议，无法处理 PVST 报文。但可以使用**二层协议透传功能**对收到的 PVST 报文透传。

3.9.2 配置 MSTP 基本功能

在 STP/RSTP 基本功能实现基础上，MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立，实现用户流量与业务流量的分离，达到网络负载均衡的目的。

通过给交换设备配置 MSTP 的工作模式、配置域并激活后，启动 MSTP，MSTP 便开始进行生成树计算，将网络修剪成树状，破除环路。但是，若网络规划者需要人为干预生成树计算的结果，可以采取以下方式：

- 配置交换设备在指定生成树实例中的优先级数值：数值越小，交换设备在该生成树实例中的优先级越高，成为根桥的可能性越大；数值越大，交换设备在该生成树实例中的优先级越低，成为根桥的可能性越小。
- 配置端口在指定生成树实例中的路径开销数值：在同一种计算方法下，数值越小，端口在该生成树实例中到根桥的路径开销越小，成为根端口的可能性就越大；数值越大，端口在该生成树实例中到根桥的路径开销越大，成为根端口的可能性越小。
- 配置端口在指定生成树实例中的优先级数值：数值越小，端口在该生成树实例中成为指定端口的可能性就越大；数值越大，端口在该生成树实例中成为指定端口的可能性越小。

版权所有 © 华为技术有限公司

建立配置任务

配置 MSTP 基本功能前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

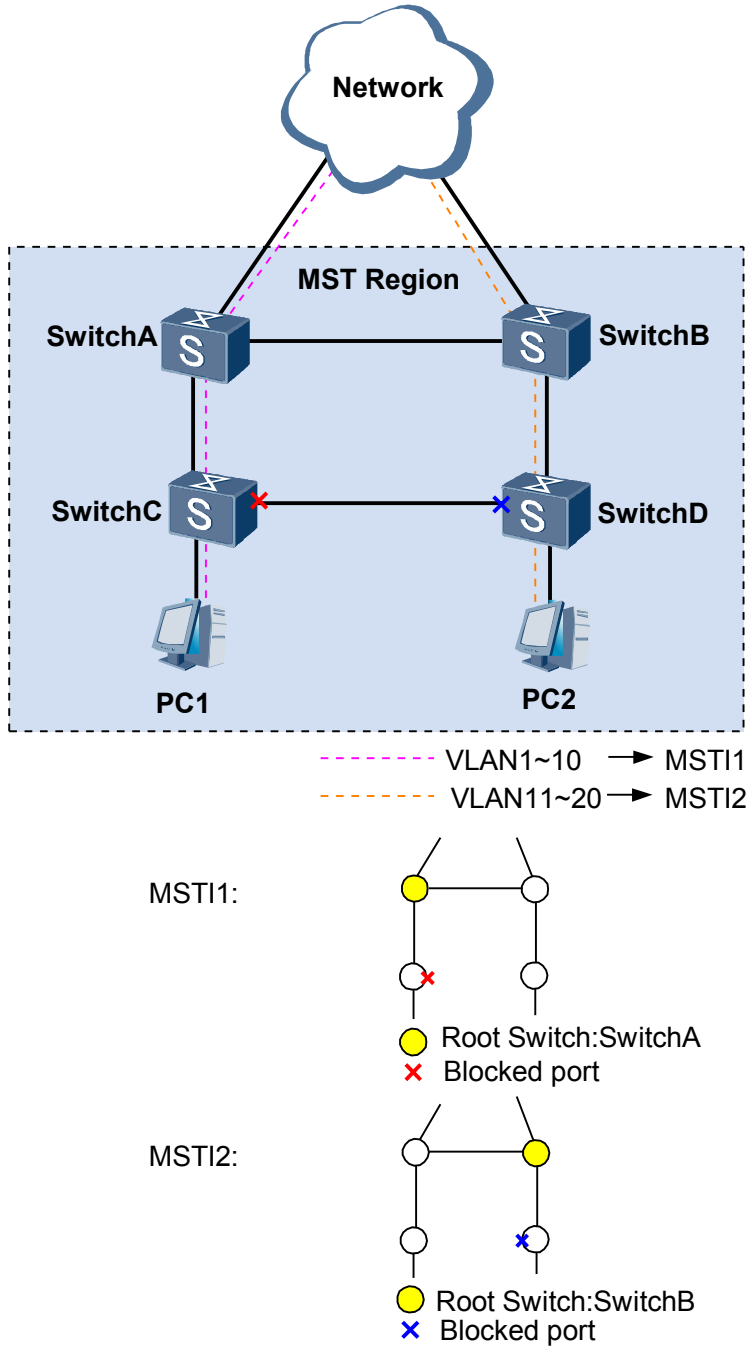
在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可在网络中部署 MSTP 协议预防环路。当网络中存在环路，MSTP 通过阻塞某个或某些端口以达到破除环路的目的，同时通过配置多实例实现多个 VLAN 的流量负载分担。

如图 3-54 所示，SwitchA、SwitchB、SwitchC 和 SwitchD 都支持 MSTP。现通过配置实例 MSTI1 和 MSTI2，然后设置各实例的根桥设备和阻塞口，完成对 VlAN1 ～ 10 和 VLAN11 ～ 20 流量的负载分担。

版权所有 © 华为技术有限公司

图 3-54 配置 MSTP 的基本功能组网图



说明

如果当前设备支持 MSTP，建议使用 MSTP。

前置任务

在配置 MSTP 基本功能前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up

版权所有 © 华为技术有限公司

- 配置端口的 VLAN 特性

数据准备

在配置 MSTP 基本功能之前，需要准备以下数据。

序号	数据
1	MSTP 工作模式
2	交换设备所属 MST 域的域名、多生成树实例和 VLAN 的映射关系、MST 域的 MSTP 修订级别
3	（可选）生成树实例 ID
4	（可选）交换设备在指定多生成树实例中的优先级
5	（可选）端口在指定多生成树实例中的优先级
6	（可选）端口在指定生成树实例中的路径开销

配置 MSTP 工作模式

在配置 MSTP 基本功能前需要选择 MSTP 工作模式，MSTP 兼容 STP/RSTP。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp mode mstp**，配置交换设备的 MSTP 工作模式。

缺省情况下，交换设备的工作模式为 MSTP。

因为 STP 和 MSTP 不能互相识别报文，而 MSTP 和 RSTP 可以互相识别报文，所以若工作在 MSTP 工作模式下，交换设备会设置所有和运行 STP 的交换设备直接相连的端口工作在 STP 模式下，其他端口工作在 MSTP 模式下，实现运行不同生成树协议的设备之间的互通。

----结束

配置 MST 域并激活

通过 MSTP 把一个交换网络划分成多个 MST 域。在完成配置 MST 域名、配置多生成树实例与 VLAN 的映射关系和配置 MST 域的 MSTP 修订级别后激活 MST 域完成对 MST 域的配置。

背景信息

MST 域即多生成树域，是由交换网络中的多台交换设备以及它们之间的网段所构成。这些交换设备启动 MSTP 后，具有相同域名、相同 VLAN 到生成树映射配置和相同 MSTP 修订级别配置，并且物理上直接相连。一个交换网络可以存在多个 MST 域，用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

版权所有 © 华为技术有限公司

注意

只要两台交换设备的以下配置相同，这两台交换设备就属于同一个 MST 域。

- MST 域的域名。
- 多生成树实例和 VLAN 的映射关系。
- MST 域的修订级别。

请在需要加入 MST 域的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行命令 **region-name** *name*，配置 MST 域的域名。

缺省情况下，MST 域的域名等于交换设备主控板上管理网口的 MAC 地址。

步骤 4 选择执行以下两个步骤中的其中一个，配置多生成树实例与 VLAN 的映射关系。

- 执行命令 **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10>，配置多生成树实例和 VLAN 的映射关系。
- 执行命令 **vlan-mapping modulo** *modulo*，配置多生成树实例和 VLAN 按照缺省算法自动分配映射关系。

缺省情况下，MST 域内所有的 VLAN 都映射到生成树实例 0。

说明

- 命令 **vlan-mapping modulo** *modulo* 实现的自动分配机制很难刚好满足实际的多生成树实例与 VLAN 的映射关系，建议使用命令 **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10>配置多生成树实例和 VLAN 的映射关系。
- **vlan-mapping modulo** *modulo* 是指 VLAN ID 减 1 后除以 modulo 值的余数再加 1，即(VLAN ID-1)%modulo+1。通过此算法来分配到对应的实例中，即余数加 1 为几就将此 VLAN 分配到实例几中。

步骤 5 （可选）执行命令 **revision-level** *level*，配置 MST 域的 MSTP 修订级别。

缺省情况下，MSTP 域的 MSTP 修订级别为 0。

当设备所在域的 MSTP 修订级别不为 0 ，则需要执行本操作。

说明

由于 MST 域相关参数（特别是 VLAN 映射表）的变化会引起 MSTP 重新计算生成树，从而引起网络拓扑振荡。因此，在完成配置 MST 域名、配置多生成树实例与 VLAN 的映射关系和配置 MST 域的 MSTP 修订级别后，建议在 MST 域视图下执行命令 check region-configuration 确定未生效的域参数配置是否正确。在确认域参数无误后，执行命令 active region-configuration 激活新的 MST 域配置。

步骤 6 执行命令 **active region-configuration**，激活 MST 域的配置，使域名、VLAN 映射表和 MSTP 修订级别生效。

如果不执行本操作，以上配置的域名、VLAN 映射表和 MSTP 修订级别无法生效。

版权所有 © 华为技术有限公司

如果在启动 MSTP 特性后又修改了交换设备的 MST 域相关参数，可以通过执行命令 active region-configuration 激活 MST 域，使修改后的参数生效。

----结束

（可选）配置交换设备在指定生成树实例中的优先级

交换设备在指定生成树实例中的优先级值越小，则交换设备的优先级越高，成为该生成树实例根桥的可能性越大。

背景信息

在一个生成树实例中，有且仅有一个根桥，它是该生成树实例的逻辑中心。在进行根桥的选择时，一般会希望选择性能高、网络层次高的交换设备作为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此需要配置优先级以保证该设备成为根桥。

对于生成树实例中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

注意

如果当前交换机已配置为根交换机或者备份根交换机，就不能再配置优先级。如果要配置交换机的优先级，必须先去使能根交换机或者备份根交换机功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp** [**instance** *instance-id*] **priority** *priority*，配置交换设备在指定生成树实例中的优先级。

缺省情况下，交换设备的优先级取值是 32768。

如果不指定 **instance**，则配置交换设备在实例 0 中的优先级。

说明

- 如果为当前设备配置系统优先级目的是配置当前设备为根桥设备，则可以直接选择执行命令 stp [instance *instance-id*] root primary，配置后该设备优先级数值自动为 0。
- 执行命令 stp [instance *instance-id*] root secondary 可以配置当前交换设备为备份根桥设备，配置后该设备优先级数值自动为 4096。

  同一台交换设备不能既作为根桥又作为备用根桥。

----结束

（可选）配置端口在指定生成树实例中的路径开销

端口路径开销会影响指定生成树实例中根端口的选择，在该实例中，某台设备所有端口到达根桥路径开销最小者，就是根端口。

背景信息

路径开销是一个端口量，是 MSTP 协议用于选择链路的参考值。

版权所有 © 华为技术有限公司

端口的路径开销是生成树计算的重要依据，在不同生成树实例中为同一端口配置不同的路径开销值，可以使不同 VLAN 的流量沿不同的物理链路转发，实现按 VLAN 的负载分担功能。

存在环路的网络环境中，对于链路速率值相对较小的端口，建议将其路径开销值配置相对较大，以使其在生成树算法中被选举成为阻塞端口，阻塞其所在链路。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }，配置端口路径开销计算方法。

缺省情况下，路径开销缺省值的计算方法为 IEEE 802.1t 标准方法。

同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 4 执行命令 **stp instance** *instance-id* **cost** *cost*，设置当前端口在指定生成树实例中的路径开销值。

- 使用华为的私有计算方法时参数 *cost* 取值范围是 1 ～ 200000。
- 使用 IEEE 802.1D 标准方法时取值范围是 1 ～ 65535。
- 使用 IEEE 802.1t 标准方法时取值范围是 1 ～ 200000000。

----结束

（可选）配置端口在指定生成树实例中的优先级

交换设备的端口优先级值越小，被指定为指定端口的机率越大；端口优先级值越大，则该端口被阻塞的机率越大。

背景信息

在参与 MSTP 生成树计算时，对于处在生成树实例中的交换设备端口，其优先级的高低会影响到是否被选举为指定端口。

在根路径开销及发送交换设备的 BID 相同的情况下，如果希望将生成树实例中的某交换设备的端口阻塞从而破除环路，则可将其端口优先级值设置比缺省值大，使得在选举过程中成为被阻塞的端口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 执行命令 **stp instance** *instance-id* **port priority** *priority*，配置端口在指定生成树实例中的优先级。

缺省情况下，端口的优先级数值为 128。

优先级数值的取值范围是 0 ～ 240，步长为 16，即取值为 0、16、32 等。

----结束

版权所有 © 华为技术有限公司

启用 MSTP

当交换设备配置 MSTP 基本功能后，交换设备 MSTP 使能，MSTP 功能才能生效。

背景信息

在环形网络中一旦启用 MSTP，MSTP 便立即开始进行生成树计算。而且，诸如交换设备的优先级、端口优先级等参数都会影响到生成树的计算，在计算过程中这些参数的变动可能会导致网络震荡。为了保证生成树计算过程快速而且稳定，必须在对交换设备及其端口进行必要的基本配置以后才能启用 MSTP。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp enable**，使能交换设备的 MSTP 功能。

缺省情况下，AC6605 的 MSTP 功能处于禁用状态。

----结束

检查配置结果

完成 MSTP 基本功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 基本功能的配置。

操作步骤

- 使用命令 **display stp** [**instance** *instance-id*][**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。
- 执行命令 **display stp region-configuration**，查看已经生效的 MST 域的配置信息。
- 执行命令 **display stp region-configuration** [**digest**]，查看已经生效的 MST 域配置的摘要。

----结束

3.9.3 配置 MSTP 多进程

MSTP 设备将端口绑定在进程中，设备将以进程为单位进行 MSTP 计算，不在此进程内的端口将不参与此进程的 MSTP 计算。

建立配置任务

配置 MSTP 多进程前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

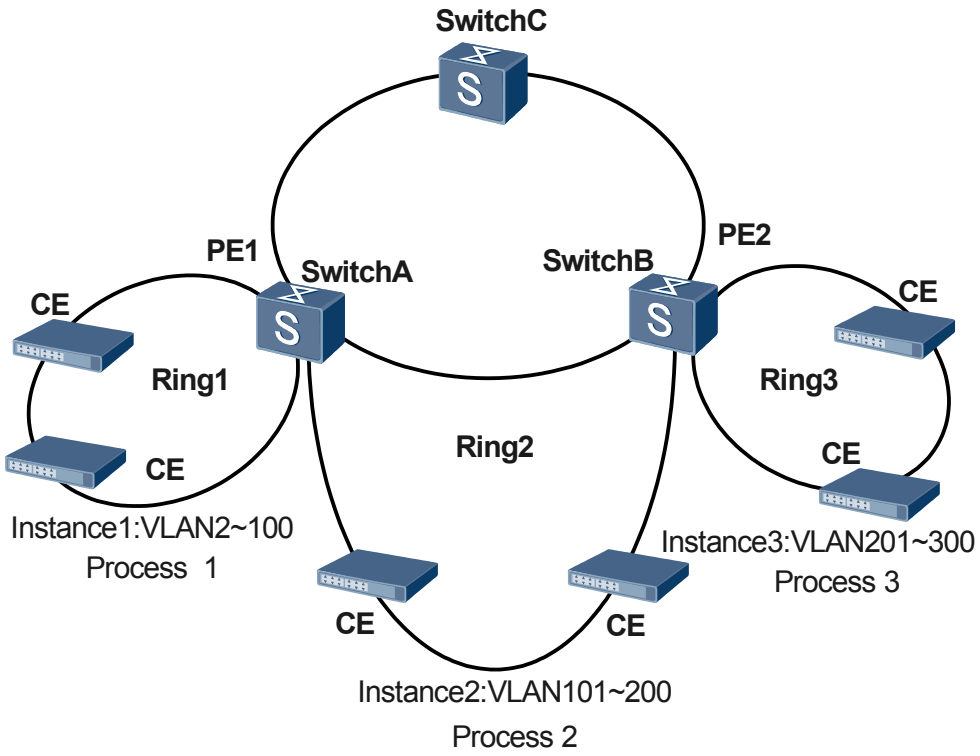
版权所有 © 华为技术有限公司

应用环境

在二层单接环和二层双接环混合组网环境下，交换设备同时承载二三层业务。为了实现不同的环完成不同的业务，可在该组网上部署 MSTP 多进程，实现不同环上的生成树协议进行独立计算，互不影响。

如图 3-55 所示，SwitchA、SwitchB 和 SwitchC 之间通过二层链路相连，并且同时启动 MSTP 协议。环上的 CE 设备只支持 STP/RSTP 协议并且存在多个接入环，不同的接入环在 SwitchA 和 SwitchB 上通过不同的端口接入。

图 3-55 MSTP 多进程的典型组网



前置任务

在配置 MSTP 多进程之前，需要完成以下任务：

- 配置 MSTP 基本功能

数据准备

在配置 MSTP 多进程之前，需要准备以下数据。

序号	数据
1	MSTP 进程的 ID
2	设备在指定多生成树实例中的优先级

华为专有和保密信息
版权所有 © 华为技术有限公司

创建 MSTP 进程

进程的 ID 是识别 MSTP 多进程的唯一标识。MSTP 设备将端口绑定在进程中，设备将以进程为单位进行 MSTP 协议计算，不在此进程内的端口将不参与此进程的协议计算。

背景信息

请在与接入环相连接的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp process** *process-id*，创建一个指定 ID 的 MSTP 进程并进入该 MSTP 进程视图。

步骤 3 执行命令 **stp mode mstp**，配置 MSTP 进程的工作模式。

缺省情况下，当前 MSTP 进程的工作模式为 MSTP。

说明

- 正常启动后，设备默认存在 ID 为 0 的 MSTP 进程，系统视图和接口视图中的 MSTP 相关配置都属于此进程，此进程的默认工作模式为 MSTP。
- 如果要把一个接口加入到 ID 非 0 的 MSTP 进程中，请分别使用 stp process 命令和 stp binding process 命令。

----结束

配置端口加入 MSTP 进程－接入链路

使能 MSTP 功能的设备与接入环相连的链路叫做接入链路。通过将端口加入 MSTP 进程中，以参与 MSTP 协议计算。

背景信息

请在与接入环相连接的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

此命令中指定的接口必须是设备与接入环相连接的二层接口。

步骤 3 执行命令 **stp binding process** *process-id*，把当前接口加入指定 ID 的 MSTP 进程中。

----结束

配置端口加入 MSTP 进程－共享链路

多个接入环共用的链路叫做共享链路。共享链路上的端口需要参与多个接入环和多个 MSTP 进程的计算。通过将端口加入 MSTP 进程中，以参与 MSTP 协议计算。

背景信息

请在与接入环相连接的设备上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

此命令中指定的接口不是设备与接入环相连接的接口，而是配置了 MSTP 多进程的设备之间的共享链路上的接口。

步骤 3 执行命令 **stp binding process** *process-id* [**to** *process-id*] **link-share**，配置共享链路上的端口参与多个 MSTP 进程的状态计算。

说明

对于存在 link-share 链路的进程，必须全局 stp enable。对于以 link-share 方式加入进程的端口，端口下必须 stp enable。

----结束

配置 MSTP 多进程的优先级和根保护

配置 MSTP 多进程的优先级和根保护可以对接入环的链路进行保护。

背景信息

为了防止共享链路故障而导致接入环之间形成环路，建议配置 MSTP 多进程的优先级和根保护。

具体配置方法是需要在次高优先级设备的接入端口配置根保护。

- MSTP 进程优先级的配置方法，请参见**配置交换设备在指定生成树实例中的优先级**中的内容。
- 根保护的配置方法，请参见**配置端口的 Root 保护功能**中的内容。

说明

下游设备的 STP 优先级必须低于 UPE 设备的优先级。

配置 MSTP 多进程的 TC 通告功能

配置 MSTP 多进程的 TC 通告功能后，当前 MSTP 进程在收到 TC 报文后，能够及时通告给其他指定 MSTP 进程中的实例，以便使其及时刷新 MAC 表项和 ARP 表项，从而保证用户业务不中断。

背景信息

请在与接入环相连接的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp process** *process-id*，进入已创建的 MSTP 进程视图。

步骤 3 执行命令 **stp tc-notify process 0**，使能当前 MSTP 进程的 TC 通告功能。

版权所有 © 华为技术有限公司

执行命令 **stp tc-notify process 0** 后，当前 MSTP 进程在收到 TC 报文后，能够及时通告给 MSTP 进程 0 中的实例，以便使其及时刷新 MAC 表项和 ARP 表项，从而保证用户业务不中断。

----结束

检查配置结果

完成 MSTP 多进程相关命令配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 多进程功能的所有配置。

操作步骤

步骤 1 执行命令 **display stp** [**process** *process-id*] [**instance** *instance-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.9.4 配置 MSTP 影响拓扑收敛的参数

MSTP 兼容实现了 RSTP 的快速收敛机制。在以下影响 MSTP 拓扑收敛的参数中选择合适的参数，配置后实现最快的拓扑收敛速度。

建立配置任务

配置 MSTP 影响拓扑收敛的参数前，请认真了解各项配置的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在运行 MSTP 的网络环境中，快速收敛机制的实现需要配置影响快速收敛的参数，配置合适的参数后才能实现最佳快速收敛效果。

说明

因为本配置任务中所包含的命令缺省情况下也能完成 MSTP 的快速收敛，所以本配置任务所包含的所有配置过程，以及配置过程中包含的所有配置步骤都是可选的，可根据实际需要选择配置其中的部分内容。

前置任务

在配置 MSTP 影响拓扑收敛的参数之前，需要完成以下任务：

- 配置 MSTP 基本功能

数据准备

在配置影响拓扑收敛的参数之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	网络直径
2	Hello Time 时间、Forward Delay 时间、Max Age 时间、超时时间（3 x hello time x time factor）
3	MST 域的最大跳数
4	端口的链路类型
5	端口是否使用普通的快速迁移机制
6	端口是否需要迁移回 RSTP 模式
7	BPDU 的最大发送数目值
8	端口是否需要设置为边缘端口
9	如果端口为边缘端口，是否需要配置其在 Shutdown 后自动恢复功能
10	端口是否需要清除生成树的统计信息
11	如果端口为边缘端口，是否需要配置端口为 BPDU filter 端口

配置系统参数

影响 MSTP 拓扑收敛的系统参数有网络直径、Hello Time 定时器与倍数参数形成的超时时间（3 x hello time x time factor）等，配置合适的系统参数，实现最快的拓扑收敛。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **stp process** *process-id*，进入 MSTP 进程视图。

说明

本步骤仅需要在 ID 非 0 的 MSTP 进程中配置系统参数时执行。当在 ID 为 0 的进程中配置时，可跳过本步，直接进入下一步。

步骤 3 执行命令 **stp bridge-diameter** *diameter*，配置网络直径。

缺省情况下，网络直径为 7。

- 快速生成树是在整个交换网络应用单生成树实例，不能解决由于网络规模增大带来的性能降低问题，网络直径不要超过 7。
- 建议通过执行命令 **stp bridge-diameter** *diameter* 配置网络直径去配置 Forward Delay 时间、Hello Time 时间以及 Max Age 时间，因为交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。

步骤 4 执行命令 **stp timer-factor** *factor*，配置未收到上游的 BPDU 就重新开始生成树计算的超时时间。

缺省情况下，交换设备未收到上游的 BPDU 就重新开始生成树计算的超时时间是 Hello Timer 的 9 倍。

版权所有 © 华为技术有限公司

步骤 5 （可选）若需要对 Forward Delay 时间、Hello Time 时间以及 Max Age 时间直接进行配置，则分别进行如下操作：

- 执行命令 **stp timer forward-delay** *forward-delay*，配置交换设备的 Forward Delay 时间。

  缺省情况下，交换设备的 Forward Delay 时间是 1500 厘秒。

- 执行命令 **stp timer hello** *hello-time*，配置交换设备的 Hello Time 时间。

  缺省情况下，交换设备的 Hello Time 时间是 200 厘秒。

- 执行命令 **stp timer max-age** *max-age*，配置交换设备的 Max Age 时间。

  缺省情况下，交换设备的 Max Age 时间是 2000 厘秒。

说明

根交换设备的 Hello Time、Forward Delay 以及 Max Age 三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡。

- 2 × (Forward Delay − 1.0 second) >= Max Age
- Max Age >= 2 × (Hello Time + 1.0 second)

步骤 6 执行命令 **stp max-hops** *hop*，配置 MST 域的最大跳数。

缺省情况下，MST 域的最大跳数为 20。

步骤 7 执行命令 **stp mcheck**，执行 MCheck 操作。

在运行 MSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 MSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 MSTP 模式：

- 运行 STP 的交换设备被关机或移走
- 运行 STP 的交换设备切换为 MSTP 模式

说明

在系统视图下执行命令 **stp mcheck**，所有端口都将执行 MCheck 操作。

----结束

配置端口参数

影响 MSTP 拓扑收敛的端口参数有端口的链路类型、BPDU 的最大发送数目等。配置合适的端口参数，实现最快的拓扑收敛。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp point-to-point** { **auto** | **force-false** | **force-true** }，配置指定端口的链路类型。

缺省情况下，指定端口自动识别是否与点对点链路相连，点对点链路支持快速收敛。

- 如果当前以太网端口工作在全双工模式，则当前端口相连的链路是点到点链路，选择参数 **force-true** 实现快速收敛。

版权所有 © 华为技术有限公司

- 如果当前以太网端口工作在半双工模式，可通过执行命令 **stp point-to-point force-true** 强制链路类型为点对点链路，实现快速收敛。

步骤 4 执行命令 **stp mcheck**，执行 MCheck 操作。

在运行 MSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 MSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 MSTP 模式：

- 运行 STP 的交换设备被关机或移走
- 运行 STP 的交换设备切换为 MSTP 模式

步骤 5 执行命令 **stp transmit-limit** *packet-number*，配置端口在每个 Hello Time 时间内 BPDU 的最大发送数目。

缺省情况下，端口在每个 Hello Time 时间内 BPDU 的最大发送数目为 147。

步骤 6 （可选）执行命令 **stp edged-port enable**，将端口配置成边缘端口。

若设备与终端相连，则相连的端口为边缘端口，可执行本操作将该端口配置成边缘端口。

缺省情况下，端口为非边缘端口。

步骤 7 执行命令 **quit**，退回到系统视图。

步骤 8 （可选）执行命令 **error-down auto-recovery cause** *cause-item* **interval** *interval-value*，使能处于 error-down 状态的边缘端口状态自动恢复为 Up 的功能，同时设置接口状态自动恢复为 Up 的延迟时间。

此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

----结束

后续处理

当生成树的拓扑结构发生改变时，和它建立映射关系的 VLAN 的转发路径也将发生变化。此时，交换设备的 ARP 表中与这些 VLAN 相关的表项也需要更新。根据对 ARP 表项的处理方式不同，MSTP 的收敛方式分为 fast 和 normal 两种：

- fast：ARP 表将需要更新的表项直接删除。
- normal：ARP 表中需要更新的表项快速老化。

  交换设备将 ARP 表中这些表项的剩余存活时间置为 0，对这些表项进行老化处理。如果配置的 ARP 老化探测次数大于零，则 ARP 对这些表项进行老化探测。

  这两种方式对 MAC 表项的处理方式相同，都是直接删除。

在系统视图下执行命令 **stp converge** { **fast** | **normal** }，可配置端口的收敛方式。

缺省情况下，端口的 MSTP 收敛方式为 normal。

说明

建议选择 normal 收敛方式。若选择 fast 方式，频繁的 ARP 表项删除可能会导致主控板和接口板 CPU 占用率高达 100%，报文处理超时导致网络震荡。

版权所有 © 华为技术有限公司

检查配置结果

完成影响 MSTP 拓扑快速收敛的参数配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成对设备影响 MSTP 拓扑快速收敛的所有参数配置。

操作步骤

- 执行命令 **display stp** [**instance** *instance-id*] [**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.9.5 配置 MSTP 保护功能

华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

建立配置任务

配置 MSTP 保护功能前，请认真了解此特性的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

MSTP 提供如表 3-23 所示的各种保护功能。

表 3-23 MSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

版权所有 © 华为技术有限公司

保护功能	场景	配置影响
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。
共享链路保护	在交换设备双归属接入网络的组网中，当多个进程的共享链路故障时，可能会引起环路。	当共享链路故障时，通过共享链路保护功能，使本设备的工作模式强制转换为 RSTP，配合使用根保护功能，可以避免网络环路。

说明

- 正常启动后，设备默认存在 ID 为 0 的 MSTP 进程，系统视图和接口视图中的 MSTP 相关配置都属于此进程。
- 关于 MSTP 多进程的配置，请参见**配置 MSTP 多进程**。

前置任务

在配置交换设备的 MSTP 保护功能之前，需要完成以下任务：

- 配置 MSTP 基本功能

  说明

  在配置 BPDU 保护功能前，需要在交换设备上配置边缘端口。

数据准备

在配置交换设备的 MSTP 保护功能之前，需要准备以下数据。

序号	数据
1	启动 Root 保护功能的端口号
2	启动环路保护功能的端口号

版权所有 © 华为技术有限公司

配置交换设备的 BPDU 保护功能

交换设备上启动 BPDU 保护功能后，如果边缘端口收到 BPDU，交换设备将关闭这些端口，同时通知网管系统。

背景信息

边缘端口直接和用户终端相连，正常情况下，边缘端口不会收到 BPDU 报文。如果攻击者伪造 BPDU 恶意攻击交换设备，当边缘端口接收到 BPDU 报文时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。通过使能 BPDU 保护可以防止伪造 BPDU 恶意攻击。

说明

请在有边缘端口的交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **stp process** *process-id*，进入 MSTP 进程视图。

说明

本步骤仅需要在 ID 非 0 的 MSTP 进程中配置交换设备的 BPDU 保护功能时执行。当在 ID 为 0 的进程中配置时，可跳过本步，直接进入下一步。

步骤 3 执行命令 **stp bpdu-protection**，配置交换设备的 BPDU 保护功能。

缺省情况下，交换设备的 BPDU 保护功能处于禁用状态。

----结束

配置交换设备的 TC 保护功能

启用 TC 保护功能后，在单位时间内，MSTP 进程处理 TC 类型 BPDU 报文的次数可配置，以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护交换设备的目的。

背景信息

如果攻击者伪造拓扑变化 BPDU 报文恶意攻击交换设备，交换设备短时间内会收到很多拓扑变化 BPDU 报文，频繁的删除操作会给设备造成很大的负担，也给网络的稳定带来很大隐患。

启用 TC 保护功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **stp process** *process-id*，进入 MSTP 进程视图。

版权所有 © 华为技术有限公司

说明

本步骤仅需要在 ID 非 0 的 MSTP 进程中配置交换设备的 TC 保护功能时执行。当在 ID 为 0 的进程中配置时，可跳过本步，直接进入下一步。

步骤 3 执行命令 **stp tc-protection**，使能 MSTP 进程对 TC 类型 BPDU 报文的保护功能。

缺省情况下，交换设备的 TC 保护功能处于使能状态。

步骤 4 执行命令 **stp tc-protection threshold** *threshold*，配置 MSTP 进程在收到 TC 类型 BPDU 报文后，单位时间内，处理 TC 类型 BPDU 报文并立即刷新转发表项的阈值。

说明

单位时间的取值与 MSTP 的 Hello Time 一致，可以通过执行命令 stp timer hello *hello-time* 进行配置。

----结束

配置端口的 Root 保护功能

在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

背景信息

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换设备有可能会收到优先级更高的 BPDU 报文，使得合法根交换设备失去根交换设备的地位，引起网络拓扑结构的错误变动。这种不合法的拓扑变化，可能会导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。为了防止这种情况发生，可在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

说明

Root 保护是指定端口上的特性。当端口在所有实例中都是指定端口时，配置的 Root 保护功能才能起到保护根交换设备的目的。若在其他类型的端口上配置 Root 保护功能，Root 保护功能不会生效。

在 MST 域中的根交换设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3（可选）执行命令 **stp binding process** *process-id*，将端口绑定到进程。

说明

本步骤仅在需要把接口绑定到 ID 非 0 进程时配置。当接口属于 ID 为 0 的进程，可跳过本步，直接进入下一步。

步骤 4 执行命令 **stp root-protection**，配置交换设备的 Root 保护功能。

缺省情况下，端口的 Root 保护功能处于关闭状态。

----结束

配置端口的环路保护功能

环路保护功能会抑制由于链路拥塞等原因产生的环路。

版权所有 © 华为技术有限公司

背景信息

在运行 MSTP 协议的网络中，根端口和其他阻塞端口状态是依靠不断接收来自上游交换设备的 BPDU 维持。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换设备的 BPDU 时，交换设备会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。为了防止以上情况发生，可部署环路保护功能。

在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 BPDU，端口状态才恢复正常为 Forwarding 状态。

说明

由于 Alternate 端口是根端口的备份端口，如果交换设备上有 Alternate 端口，需要在根端口和 Alternate 端口上同时配置环路保护。

在 MST 域中交换设备的根端口和 Alternate 端口上进行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp binding process** *process-id*，将端口绑定到进程。

说明

本步骤仅在需要把接口绑定到 ID 非 0 进程时配置。当接口属于 ID 为 0 的进程，可跳过本步，直接进入下一步。

步骤 4 执行命令 **stp loop-protection**，配置交换设备根端口的环路保护功能。

缺省情况下，端口的环路保护功能处于关闭状态。

----结束

配置交换设备的共享链路保护功能

交换设备的共享链路保护功能是指故障发生时将工作模式切换为 RSTP，同时配合根保护避免形成环路。

背景信息

共享链路保护功能用在交换设备双归属接入网络的场景中。

当共享链路故障时，通过共享链路保护功能，使本设备的工作模式强制转换为 RSTP，配合使用根保护功能，可以避免网络环路。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp process** *process-id*，进入 MSTP 进程视图。

步骤 3 执行命令 **stp link-share-protection**，使能共享链路保护功能。

----结束

版权所有 © 华为技术有限公司

检查配置结果

完成 MSTP 保护功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 保护功能的所有配置。

操作步骤

- 执行命令 **display stp** [**instance** *instance-id*] [**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.9.6 配置 MSTP 支持和其他制造商设备互通的参数

为了实现与其他制造商设备的互通，需要在华为公司运行 MSTP 的设备上配置一些参数，以确保通信畅通。这些参数包括收发 BPDU 报文的协议格式、MSTP 报文的协议格式和使能摘要监听功能。

建立配置任务

配置 MSTP 支持和其他制造商设备互通的参数前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在运行 MSTP 的网络中，因为协议格式不一致、BPDU 报文密钥不一致等原因会导致设备无法正常互通，在这种情况下，需要配置 MSTP 支持和其他制造商设备互通的参数来实现互通。

前置任务

在配置 MSTP 支持和其他制造商设备互通的参数之前，需要完成以下任务：

- 配置 MSTP 基本功能

数据准备

在配置 MSTP 支持和其他制造商设备互通的参数之前，需要准备以下数据。

序号	数据
1	收发 BPDU 报文的协议格式
2	收发 MSTP 协议报文的格式

配置端口 Proposal/Agreement 机制的迁移方式

为了实现华为公司的数据通信与其他制造商设备互通，需要根据其他制造商设备的 P/A 机制选择端口的快速迁移方式。

版权所有 © 华为技术有限公司

背景信息

Proposal/Agreement 机制，目前交换设备的端口支持以下两种方式：

- 增强方式：当前接口在计算同步标志位时计算根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口。
  - 上游设备继续发送 Agreement 报文，下游设备接收到后，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。
- 普通方式：当前接口在计算同步标志位时忽略根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。

华为数据通信设备和其他制造商的设备进行互通时，需要根据其他制造商设备的 Proposal/Agreement 机制，选择接口使用增强的快速迁移机制还是普通的快速迁移机制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp binding process** *process-id*，将端口绑定到进程。

说明

本步骤仅在需要把接口绑定到 ID 非 0 进程时配置。当接口属于 ID 为 0 的进程，可跳过本步，直接进入下一步。

步骤 4 执行命令 **stp no-agreement-check**，配置端口使用普通的快速迁移方式。

缺省情况下，端口使用增强的快速迁移机制。

----结束

配置端口收发 MSTP 协议的报文格式

MSTP 协议报文收发模式包括协议格式自适应、标准 IEEE 802.1s 报文和私有协议报文三种模式，默认情况下为自适应模式。

背景信息

MSTP 协议报文存在两种格式，一种为 dot1s，即 IEEE802.1s 规定的报文格式，另一种为 legacy，是一种私有报文格式。配置 MSTP 协议报文格式自适应的功能，即根据收到的 MSTP 协议报文格式自动切换接口支持的 MSTP 协议报文格式，使报文格式与对端匹配。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 MST 域中的交换设备上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp binding process** *process-id*，将端口绑定到进程。

说明

本步骤仅在需要把接口绑定到 ID 非 0 进程时配置。当接口属于 ID 为 0 的进程，可跳过本步，直接进入下一步。

步骤 4 执行命令 **stp compliance** { **auto** | **dot1s** | **legacy** }，配置端口协议报文格式。

缺省情况下，MSTP 报文收发格式为 auto 模式。

说明

如果直连的接口上一端配置 dot1s，而另一端配置 legacy，是不能协商成功的。

----结束

使能摘要监听功能

当华为设备与其他制造商的设备互连时，在域名、修订级别、VLAN mapping 表全都一致的情况下，由于双方 BPDU 报文密钥不一致，会导致两台设备不能正常互通，在这种情况下，需要在交换设备上使能摘要监听功能。

背景信息

在 MST 域中的交换设备上进行以下配置，实现华为设备的 BPDU 报文密钥与其他制造商设备的 BPDU 报文密钥一致。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入以太接口视图。

步骤 3 （可选）执行命令 **stp binding process** *process-id*，将端口绑定到进程。

说明

本步骤仅在需要把接口绑定到 ID 非 0 进程时配置。当接口属于 ID 为 0 的进程，可跳过本步，直接进入下一步。

步骤 4 执行命令 **stp config-digest-snoop**，使能端口上配置摘要监听的功能。

----结束

检查配置结果

完成 MSTP 支持和其他制造商设备互通的配置参数后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 支持和其他制造商设备互通的所有参数配置。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **display stp** [**instance** *instance-id*] [**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。

----结束

3.9.7 维护 MSTP

MSTP 相关维护命令，包括清除 MSTP 的统计数据。

清除 MSTP 统计信息

通过 reset 命令可以将 MSTP 统计计数置 0，便于重新统计。

背景信息

注意

清除 MSTP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 MSTP 的统计信息后，请在用户视图下执行以下命令。

操作步骤

步骤 1 执行命令 **reset stp** [**interface** *interface-type interface-number*] **statistics**，清除生成树的统计信息。

----结束

3.9.8 配置举例

介绍了 MSTP 的典型组网配置。

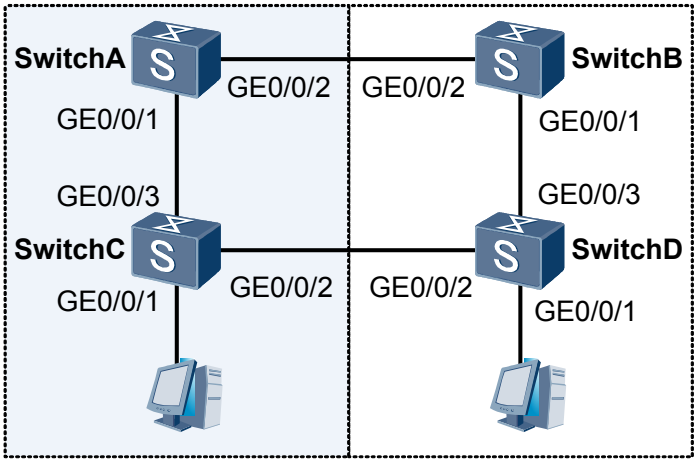
配置 MSTP 的基本功能示例

组网需求

交换机 SwitchA、SwitchB、SwitchC 和 SwitchD 都支持 MSTP，本例中的交换机都使用二层接口运行 MSTP。

版权所有 © 华为技术有限公司

图 3-56 配置 MSTP 的基本功能组网图



配置思路

采用如下的思路配置 MSTP 的基本功能：

1. 将 SwitchA 和 SwitchC 配置到一个域内，域名为 RG1，创建实例 1。
2. 将 SwitchB 和 SwitchD 配置到另外一个域，域名为 RG2，创建实例 1。
3. 配置交换机 SwitchA 为 CIST 总根。
4. 在域 RG1 内，交换机 SwitchA 为 CIST 域根，SwitchA 为实例 1 的域根。在 SwitchA 的 GE0/0/2 和 GE0/0/1 上应用根保护功能。
5. 在域 RG2 内，交换机 SwitchB 为 CIST 域根，SwitchD 为实例 1 的域根。
6. SwitchC 和 SwitchD 的 GE0/0/1 与 PC 机相连，设置为边缘端口，同时在 SwitchC 和 SwitchD 上应用 BPDU 保护功能。
7. 在 SwitchA、SwitchB、SwitchC 和 SwitchD 使用华为私有计算方法计算路径开销。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 和 SwitchC 的域名为 RG1
- SwitchB 和 SwitchD 的域名为 RG2
- 各 GigabitEthernet 端口号如图 3-56 所示
- VLAN 号是 1 ～ 20

操作步骤

步骤 1 配置交换机 SwitchA

配置 SwitchA 的 MST 域。

```
<SwitchA> system-view
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name RG1
[SwitchA-mst-region] instance 1 vlan 1 to 10
```


华为专有和保密信息
版权所有 © 华为技术有限公司

激活域配置。

```
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

配置 SwitchA 在实例 0 中的优先级为 0，保证 SwitchA 作为 CIST 的总根。

```
[SwitchA] stp instance 0 priority 0
```

配置 SwitchA 在实例 1 中的优先级为 0，保证 SwitchA 作为实例 1 的域根。

```
[SwitchA] stp instance 1 priority 0
```

配置端口路径开销的计算方法为华为私有计算方法。

```
[SwitchA] stp pathcost-standard legacy
```

创建 VLAN 2 到 20。

```
[SwitchA] vlan batch 2 to 20
```

将 GE0/0/2 加入 VLAN。

```
[SwitchA] interface interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchA-GigabitEthernet0/0/2] bpdu enable
[SwitchA-GigabitEthernet0/0/2] quit
```

将 GE0/0/1 加入 VLAN。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] quit
```

在 GE0/0/1 上启动根保护。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp root-protection
[SwitchA-GigabitEthernet0/0/1] quit
```

在 GE0/0/2 上启动根保护。

```
[SwitchA] interface interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp root-protection
[SwitchA-GigabitEthernet0/0/2] quit
```

启动 MSTP。

```
[SwitchA] stp enable
```

步骤 2 配置交换机 SwitchB

配置 SwitchB 的 MST 域。

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name RG2
[SwitchB-mst-region] instance 1 vlan 1 to 10
```

激活域配置。

```
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

配置 SwitchB 在实例 0 中的优先级为 4096，保证 SwitchB 作为 CIST 的域根。

```
[SwitchB] stp instance 0 priority 4096
```


版权所有 © 华为技术有限公司

配置端口路径的开销计算方法为华为私有计算方法。

```
[SwitchB] stp pathcost-standard legacy
```

创建 VLAN 2 到 20。

```
[SwitchB] vlan batch 2 to 20
```

将 GE0/0/1 加入 VLAN。

```
[SwitchB] interface interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] quit
```

将 GE0/0/2 加入 VLAN。

```
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchB-GigabitEthernet0/0/2] bpdu enable
[SwitchB-GigabitEthernet0/0/2] quit
```

启动 MSTP。

```
[SwitchB] stp enable
```

步骤 3 配置 SwitchC

配置 SwitchC 的 MST 域。

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name RG1
[SwitchC-mst-region] instance 1 vlan 1 to 10
```

激活域配置。

```
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

配置端口路径开销的计算方法为华为私有计算方法。

```
[SwitchC] stp pathcost-standard legacy
```

启动 BPDU 保护功能

```
[SwitchC] stp bpdu-protection
```

创建 VLAN 2 到 20。

```
[SwitchC] vlan batch 2 to 20
```

将 GE0/0/2 加入 VLAN。

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchC-GigabitEthernet0/0/2] bpdu enable
[SwitchC-GigabitEthernet0/0/2] quit
```

将 Eth0/0/3 加入 VLAN。

```
[SwitchC] interface gigabitethernet 0/0/3
[SwitchC-GigabitEthernet0/0/3] port link-type trunk
[SwitchC-GigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[SwitchC-GigabitEthernet0/0/3] bpdu enable
[SwitchC-GigabitEthernet0/0/3] quit
```

将 GE0/0/1 配置成边缘端口。

版权所有 © 华为技术有限公司

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] stp edged-port enable
[SwitchC-GigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchC-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchC-GigabitEthernet0/0/1] quit
```

启动 MSTP。

```
[SwitchC] stp enable
```

步骤 4 配置 SwitchD

配置 SwitchD 的 MST 域。

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name RG2
[SwitchD-mst-region] instance 1 vlan 1 to 10
```

激活域配置。

```
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

配置 SwitchD 在实例 1 中的优先级为 0，保证 SwitchD 作为实例 1 的域根。

```
[SwitchD] stp instance 1 priority 0
```

配置端口路径开销的计算方法为华为私有计算方法。

```
[SwitchD] stp pathcost-standard legacy
```

启动 BPDU 保护功能。

```
[SwitchD] stp bpdu-protection
```

创建 VLAN 2 到 20。

```
[SwitchD] vlan batch 2 to 20
```

将 GE0/0/2 加入 VLAN。

```
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] port link-type trunk
[SwitchD-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchD-GigabitEthernet0/0/2] bpdu enable
[SwitchD-GigabitEthernet0/0/2] quit
```

将 GE0/0/3 加入 VLAN。

```
[SwitchD] interface gigabitethernet 0/0/3
[SwitchD-GigabitEthernet0/0/3] port link-type trunk
[SwitchD-GigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[SwitchD-GigabitEthernet0/0/3] bpdu enable
[SwitchD-GigabitEthernet0/0/3] quit
```

将 GE0/0/1 配置成边缘端口。

```
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] stp edged-port enable
[SwitchD-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-GigabitEthernet0/0/1] quit
```

启动 MSTP。

```
[SwitchD] stp enable
```

步骤 5 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

版权所有 © 华为技术有限公司

在 SwitchA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
<SwitchA> display stp brief
 MSTID     Port                Role  STP State     Protection
   0       GigabitEthernet0/0/1        DESI  FORWARDING      ROOT
   0       GigabitEthernet0/0/2        DESI  FORWARDING      ROOT
   1       GigabitEthernet0/0/1        DESI  FORWARDING      ROOT
   1       GigabitEthernet0/0/2        DESI  FORWARDING      ROOT
```

由于交换机 SwitchA 在 CIST 内优先级最高，所以 SwitchA 被选择为 CIST 总根，同时它也是 RG1 的域根。SwitchA 的 GE0/0/2 和 GE0/0/1 在 CIST 上都是指定端口。

交换机 SwitchA 实例 1 上的优先级在域 RG1 内最高，所以 SwitchA 被选择为实例 1 的域根。GE0/0/2 和 GE0/0/1 在实例 1 上都被计算为指定端口。

在 SwitchC 上执行 **display stp interface brief** 命令，结果如下：

```
<SwitchC> display stp interface gigabitethernet 0/0/3 brief
 MSTID     Port                Role  STP State     Protection
   0       GigabitEthernet0/0/3          ROOT  FORWARDING      NONE
   1       GigabitEthernet0/0/3          ROOT  FORWARDING      NONE
<SwitchC> display stp interface gigabitethernet 0/0/2 brief
 MSTID     Port                Role  STP State     Protection
   1       GigabitEthernet0/0/2          DESI  FORWARDING      NONE
   0       GigabitEthernet0/0/2          DESI  FORWARDING      NONE
```

SwitchC 的 GE0/0/3 在 CIST 和实例 1 中为根端口。SwitchC 的另一个 GE0/0/2，在 CIST 和实例 1 中都是指定端口。

在交换机 SwitchB 上执行 **display stp brief** 命令，结果如下：

```
<SwitchB> display stp brief
 MSTID     Port                Role  STP State     Protection
   0       GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0       GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   1       GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   1       GigabitEthernet0/0/2        MAST  FORWARDING      NONE
```

交换机 SwitchB 在 CIST 上的优先级低于 SwitchA，GE0/0/2 在 CIST 被计算为根端口。同时因为 SwitchA 和 SwitchB 不属于同一个域，所以 GE0/0/2 在实例 1 上被计算为 Master 端口。在实例 1 中，SwitchB 的优先级低于 SwitchD，所以 GE0/0/1 被计算为根端口。SwitchB 在 CIST 中的优先级高于 SwitchD，GE0/0/1 在 CIST 被计算为指定端口。

在 SwitchD 上执行 **display stp interface brief** 命令，结果如下：

```
<SwitchD> display stp interface gigabitethernet 0/0/3 brief
 MSTID     Port                Role  STP State     Protection
   0       GigabitEthernet0/0/3          ROOT  FORWARDING      NONE
   1       GigabitEthernet0/0/3          DESI  FORWARDING      NONE
<SwitchD> display stp interface gigabitethernet 0/0/2 brief
 MSTID     Port                Role  STP State     Protection
   0       GigabitEthernet0/0/2          ALTE  DISCARDING      NONE
   1       GigabitEthernet0/0/2          ALTE  DISCARDING      NONE
```

因为 SwitchD 的 GE0/0/2 在 CIST 上为 Alternate 端口，又因为 SwitchD 与 SwitchC 不在同一个域，所以 GE0/0/2 在实例 1 中的也被选择为 Alternate 端口。

GE0/0/3 在 CIST 为根端口，因为 SwitchD 在实例 1 中的优先级比 SwitchB 高，所以 GE0/0/3 在实例 1 上被作为指定端口。

----结束

版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2 to 20
#
 stp instance 0 priority 0
 stp instance 1 priority 0
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
 region-name RG1
 instance 1 vlan 1 to 10
 active region-configuration
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
 stp root-protection
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
 stp root-protection
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2 to 20
#
 stp instance 0 priority 4096
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
 region-name RG2
 instance 1 vlan 1 to 10
 active region-configuration
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 2 to 20
#
 stp bpdu-protection
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
 region-name RG1
 instance 1 vlan 1 to 10
 active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
```


版权所有 © 华为技术有限公司

```
 port hybrid untagged vlan 20
 stp edged-port enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 2 to 20
#
 stp instance 1 priority 0
 stp bpdu-protection
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
 region-name RG2
 instance 1 vlan 1 to 10
 active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 stp edged-port enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 1 to 20
#
return
```

配置 MSTP 多进程下单接环和多接环接入示例

通过本示例，可以了解通过 MSTP 多进程实现不同的二层环完成不同的业务。

组网需求

在二层单接环和二层双接环混合组网环境下，交换设备同时承载二三层业务。为了实现不同的环完成不同的业务，可在该组网上部署 MSTP 多进程，实现不同环上的生成树协议进行独立计算，互不影响。

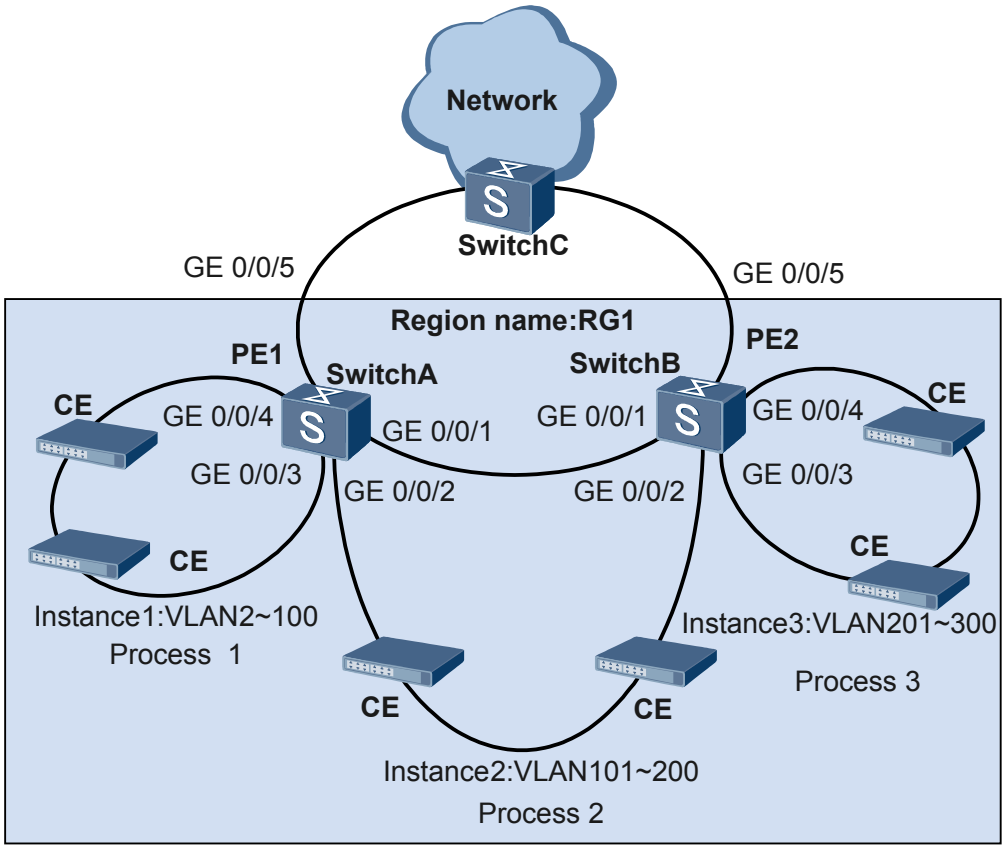
如图 3-57 所示，二层单接环和二层双接环混合组网环境下，交换设备 SwitchA 和 SwitchB 同时承载二三层业务。在该组网下，接入双接环的两台交换设备 SwitchA 和 SwitchB 下均存在单接环。

说明

在 MSTP 多进程的环中，建议端口阻塞不要配置在与根保护端口直连的链路上。

版权所有 © 华为技术有限公司

图 3-57 MSTP 多进程下单接环和多接环接入组网



配置思路

采用如下的思路配置 MSTP 多进程：

1. 配置 MSTP 基本功能，将设备加入到域，并创建实例，实现对流量的负载分担。

   说明

   - 每个环只能配置一个域。
   - 一个 CE 设备只能加入一个环。
2. 创建 MSTP 多进程，实现对端口的分割管理，包括：
   a. 在设备上创建多进程并将端口加入到相应的进程。
   b. 配置共享链路。
3. 配置其他功能，实现对设备或链路的保护，包括：
   - 配置优先级和根保护。
   - 配置共享链路保护功能。
4. 配置设备的二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

华为专有和保密信息
版权所有 © 华为技术有限公司

- MSTP 的域名 RG1，实例 1、实例 2 和实例 3
- VLAN 编号 2 ～ 300
- MSTP 进程的 ID

操作步骤

步骤 1 配置 MSTP 基本功能，将设备加入到域，并创建实例

1. 在设备上配置域和实例

   # 在 SwitchA 上配置域和实例。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name RG1
[SwitchA-mst-region] instance 1 vlan 2 to 100
[SwitchA-mst-region] instance 2 vlan 101 to 200
[SwitchA-mst-region] instance 3 vlan 201 to 300
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

   # 在 SwitchB 上配置域和实例。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name RG1
[SwitchB-mst-region] instance 1 vlan 2 to 100
[SwitchB-mst-region] instance 2 vlan 101 to 200
[SwitchB-mst-region] instance 3 vlan 201 to 300
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

2. 启动 MSTP

   # 配置 SwitchA。

```
[SwitchA] stp enable
```

   # 配置 SwitchB。

```
[SwitchB] stp enable
```

步骤 2 创建 MSTP 多进程

1. 在设备上创建多进程并将端口加入到相应的进程

   #在 SwitchA 上创建进程 1 和进程 2。

```
[SwitchA] stp process 1
[SwitchA-mst-process-1] quit
[SwitchA] stp process 2
[SwitchA-mst-process-2] quit
```

   #在 SwitchB 上创建进程 2 和进程 3。

```
[SwitchB] stp process 2
[SwitchB-mst-process-2] quit
[SwitchB] stp process 3
[SwitchB-mst-process-3] quit
```

   #将 SwitchA 的端口 GE0/0/3 和 GE0/0/4 加入到进程 1，端口 GE0/0/2 加入到进程 2。

```
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] stp enable
[SwitchA-GigabitEthernet0/0/4] bpdu enable
[SwitchA-GigabitEthernet0/0/4] stp binding process 1
[SwitchA-GigabitEthernet0/0/4] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] stp enable
[SwitchA-GigabitEthernet0/0/3] bpdu enable
[SwitchA-GigabitEthernet0/0/3] stp binding process 1
```


版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp enable
[SwitchA-GigabitEthernet0/0/2] bpdu enable
[SwitchA-GigabitEthernet0/0/2] stp binding process 2
[SwitchA-GigabitEthernet0/0/2] quit
```

将 SwitchB 的端口 GE0/0/3 和 GE0/0/4 加入到进程 3，端口 GE0/0/2 加入到进程 2。

```
[SwitchB] interface gigabitethernet 0/0/4
[SwitchB-GigabitEthernet0/0/4] stp enable
[SwitchB-GigabitEthernet0/0/4] bpdu enable
[SwitchB-GigabitEthernet0/0/4] stp binding process 3
[SwitchB-GigabitEthernet0/0/4] quit
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] stp enable
[SwitchB-GigabitEthernet0/0/3] bpdu enable
[SwitchB-GigabitEthernet0/0/3] stp binding process 3
[SwitchB-GigabitEthernet0/0/3] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] stp enable
[SwitchB-GigabitEthernet0/0/2] bpdu enable
[SwitchB-GigabitEthernet0/0/2] stp binding process 2
[SwitchB-GigabitEthernet0/0/2] quit
```

2. 配置共享链路

配置 SwitchA。

```
[SwitchA] interface gigabitethernet0/0/1
[SwitchA-GigabitEthernet0/0/1] stp enable
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] stp binding process 2 link-share
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB。

```
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] stp enable
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] stp binding process 2 link-share
[SwitchB-GigabitEthernet0/0/1] quit
```

3. 启动进程的 MSTP 功能

配置 SwitchA。

```
[SwitchA] stp process 1
[SwitchA-stp-process-1] stp enable
[SwitchA-stp-process-1] quit
[SwitchA] stp process 2
[SwitchA-stp-process-2] stp enable
[SwitchA-stp-process-2] quit
```

配置 SwitchB。

```
[SwitchB] stp process 3
[SwitchB-stp-process-3] stp enable
[SwitchB-stp-process-3] quit
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp enable
[SwitchB-stp-process-2] quit
```

步骤 3 配置其他功能

- 配置优先级和根保护

配置 SwitchA。

```
[SwitchA] stp process 1
[SwitchA-stp-process-1] stp instance 0 root primary
[SwitchA-stp-process-1] stp instance 1 root primary
[SwitchA-stp-process-1] quit
[SwitchA] stp process 2
```


版权所有 © 华为技术有限公司

```
[SwitchA-stp-process-2] stp instance 0 root primary
[SwitchA-stp-process-2] stp instance 2 root primary
[SwitchA-stp-process-2] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp root-protection
[SwitchA-GigabitEthernet0/0/2] quit
```

配置 SwitchB。

```
[SwitchB] stp process 3
[SwitchB-stp-process-3] stp instance 0 root primary
[SwitchB-stp-process-3] stp instance 3 root primary
[SwitchB-stp-process-3] quit
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp instance 0 root secondary
[SwitchB-stp-process-2] stp instance 2 root secondary
[SwitchB-stp-process-2] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] stp root-protection
[SwitchB-GigabitEthernet0/0/2] quit
```

说明

- 每个环中都要确保下游 CE 设备的 MSTP 优先级低于交换设备。
- 在双接环接入时，建议 SwitchA 和 SwitchB 分别作为不同实例的主备根。

- 配置 MSTP 多进程的共享链路保护功能

  # 配置 SwitchA。

```
[SwitchA] stp process 2
[SwitchA-stp-process-2] stp link-share-protection
[SwitchA-stp-process-2] quit
```

  # 配置 SwitchB。

```
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp link-share-protection
[SwitchB-stp-process-2] quit
```

步骤 4 创建 VLAN，并将接口加入到 VLAN 中

在 SwitchA 上创建 VLAN2 ～ VLAN200，并将端口 GE0/0/3 和端口 GE0/0/4 加入到 VLAN2 ～ 100 中，将端口 GE0/0/1 和端口 GE0/0/2 加入到 VLAN101 ～ 200 中。

```
[SwitchA] vlan batch 2 to 200
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type  trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 100
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type  trunk
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 2 to 100
[SwitchA-GigabitEthernet0/0/4] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type  trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 to 200
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type  trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 101 to 200
[SwitchA-GigabitEthernet0/0/2] quit
```

在 SwitchB 上创建 VLAN101 ～ VLAN300，并将端口 GE0/0/3 和端口 GE0/0/4 加入到 VLAN201 ～ VLAN300 中，将端口 GE0/0/1 和端口 GE0/0/2 加入到 VLAN101 ～ 200 中。

```
[SwitchB] vlan batch 101 to 300
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] port link-type  trunk
[SwitchB-GigabitEthernet0/0/3] port trunk allow-pass vlan 201 to 300
```


版权所有 © 华为技术有限公司

```
[SwitchB-GigabitEthernet0/0/3] quit
[SwitchB] interface gigabitethernet 0/0/4
[SwitchB-GigabitEthernet0/0/4] port link-type  trunk
[SwitchB-GigabitEthernet0/0/4] port trunk allow-pass vlan 201 to 300
[SwitchB-GigabitEthernet0/0/4] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type  trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 to 200
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type  trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 101 to 200
[SwitchB-GigabitEthernet0/0/2] quit
```

步骤 5 检查配置结果

- 在 SwitchA 上执行 **display stp interface brief** 命令，可以看到：

  # 端口 GE0/0/4 在 MSTP 进程 1 的 CIST 和实例 1 中为指定端口。

```
[SwitchA] display stp process 1 interface giabitgigabitethernet 0/0/4 brief
 MSTID      Port                        Role  STP State       Protection
   0    GigabitEthernet0/0/4            DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/4            DESI  FORWARDING      NONE
```

  # 端口 GE0/0/2 在 MSTP 进程 2 的 CIST 和实例 2 中为指定端口。

```
[SwitchA] display stp process 2 interface giabitgigabitethernet 0/0/2 brief
 MSTID      Port                        Role  STP State       Protection
   0    GigabitEthernet0/0/2            DESI  FORWARDING      ROOT
   2    GigabitEthernet0/0/2            DESI  FORWARDING      ROOT
```

- 在 SwitchB 上执行 **display stp interface brief** 命令，可以看到：

  # 端口 GE0/0/4 在 MSTP 进程 3 的 CIST 和实例 3 中为指定端口。

```
[SwitchB] display stp process 3 interface giabitgigabitethernet 0/0/4 brief
 MSTID      Port                        Role  STP State       Protection
   0    GigabitEthernet0/0/4            DESI  FORWARDING      NONE
   3    GigabitEthernet0/0/4            DESI  FORWARDING      NONE
```

  # 端口 GE0/0/2 在 MSTP 进程 2 的 CIST 和实例 2 中为指定端口。

```
[SwitchB] display stp process 2 interface giabitgigabitethernet 0/0/2 brief
 MSTID      Port                        Role  STP State       Protection
   0    GigabitEthernet0/0/2            DESI  FORWARDING      ROOT
   2    GigabitEthernet0/0/2            DESI  FORWARDING      ROOT
```

----结束

配置文件

以下只给出 MSTP 相关的配置文件。

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2 to 300
#
 stp enable
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 100
  instance 2 vlan 101 to 200
  instance 3 vlan 201 to 300
  active region-configuration
#
stp process 1
 stp instance 0 root primary
```


版权所有 © 华为技术有限公司

```
 stp instance 1 root primary
 stp enable
stp process 2
 stp instance 0 root primary
 stp instance 2 root primary
 stp link-share-protection
 stp enable
#
interface GigabitEthernet0/0/1
 port link-type  trunk
 port trunk allow-pass vlan 101 to 200
 stp binding process 2 link-share
#
interface GigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 101 to 200
 stp binding process 2
 stp root-protection
#
interface GigabitEthernet0/0/3
 port link-type  trunk
 port trunk allow-pass vlan 2 to 100
 stp binding process 1
#
interface GigabitEthernet0/0/4
 port link-type  trunk
 port trunk allow-pass vlan 2 to 100
 stp binding process 1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2 to 300
#
 stp enable
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 100
  instance 2 vlan 101 to 200
  instance 3 vlan 201 to 300
  active region-configuration
#
stp process 2
 stp instance 0 root secondary
 stp instance 2 root secondary
 stp link-share-protection
 stp enable
stp process 3
 stp instance 0 root primary
 stp instance 3 root primary
 stp enable
#
interface GigabitEthernet0/0/1
 port link-type  trunk
 port trunk allow-pass vlan 101 to 200
 stp binding process 2 link-share
#
interface GigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 101 to 200
 stp binding process 2
 stp root-protection
#
interface GigabitEthernet0/0/3
 port link-type  trunk
 port trunk allow-pass vlan 201 to 300
```


版权所有 © 华为技术有限公司

```
 stp binding process 3
#
interface GigabitEthernet0/0/4
 port link-type  trunk
 port trunk allow-pass vlan 201 to 300
 stp binding process 3
#
return
```

3.10 SEP 配置

SEP（Smart GigabitEthernet Protection）作为以太网保护协议，通过选择性地阻塞网络中冗余链路，阻止网络形成逻辑环路，达到消除环路的目的。

3.10.1 SEP 简介

智能以太保护协议 SEP 是一个专用于以太网链路层的环网协议，收敛速度快，支持任意拓扑且支持拓扑查看。

SEP 概述

SEP 支持开放环、封闭环、单环及多环拓扑，并满足各种拓扑的冗余保护。

SEP 概述

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。

为了解决环路问题，华为公司的数据通信设备支持如表 3-24 所示环路网协议。

表 3-24 环网协议

环网协议	优点	缺点	场景
STP/ RSTP/ MSTP	STP、RSTP、MSTP 是以太网络二层破环技术的标准协议，应用成熟、场景广泛，且支持与其他制造商设备互通。	收敛时间在秒级，不能满足一些实时业务的要求，且收敛时间受网络拓扑影响。	适用于收敛时间要求不高的二层网络。
RRPP	RRPP 是华为公司私有协议，收敛速度快，收敛时间小于 50 毫秒，且支持不同业务流量负载均衡。	● 不支持与其他制造商设备互通。 ● 对网络拓扑有严格的要求，需要人为划分逻辑拓扑分出主环子环，不利于复杂网络的部署。	适用于收敛时间要求高的单环、相切环、相交环。

版权所有 © 华为技术有限公司

环网协议	优点	缺点	场景
SEP	● SEP 是华为公司私有协议，收敛速度快，收敛时间小于 50 毫秒，且支持与其他制造商设备互通。 ● SEP 支持各种类型的复杂组网。如，支持与 STP、RSTP、MSTP、RRPP 协议混合组网，支持任意拓扑且支持拓扑查看。 通过查看拓扑可快速找出阻塞端口。当有故障产生，可快速定位故障出现的位置，从而提高了可维护性。 ● 支持多种阻塞端口选择策略，从而灵活地实现了流量负载分担。	● 部署 SEP 协议的网络上的设备必须都是华为公司数据通信设备。 ● 部署 SEP 协议的网络，网络收敛后必定选出一个阻塞端口阻塞数据流量通过，即使是直连链路。	适用于收敛时间要求高的二层网络。

SEP 定义

SEP 是一种专用于以太网链路层的环网协议，以 SEP 段为基本单位。所谓 SEP 段，就是由一组配置了相同的 SEP 段 ID 和控制 VLAN 且互连的二层交换设备群体构成。

每台二层交换设备上只能有两个端口加入同一个 SEP 段。在 SEP 段中，为了防止出现环路，可以启动环路保护机制，选择性地阻塞端口，消除以太网冗余链路。当环网发生链路故障时，运行 SEP 协议的设备可以迅速地放开阻塞端口，进行链路倒换，恢复环网上各节点间链路通信。

如图 3-58 所示是一个典型的 SEP 应用。CE1 通过交换机组成的环形网络接入 NPE，并在 NPE 上部署了 VRRP 备份组。最初，NPE1 是主用状态，NPE2 是备用状态。当 NPE1 与 LSW5 之间的链路或节点设备发生故障时，以 LSW1 与 LSW5 之间的链路发生故障为例，半环上有没有部署 SEP 将影响流量是否正常转发。

- 未部署 SEP

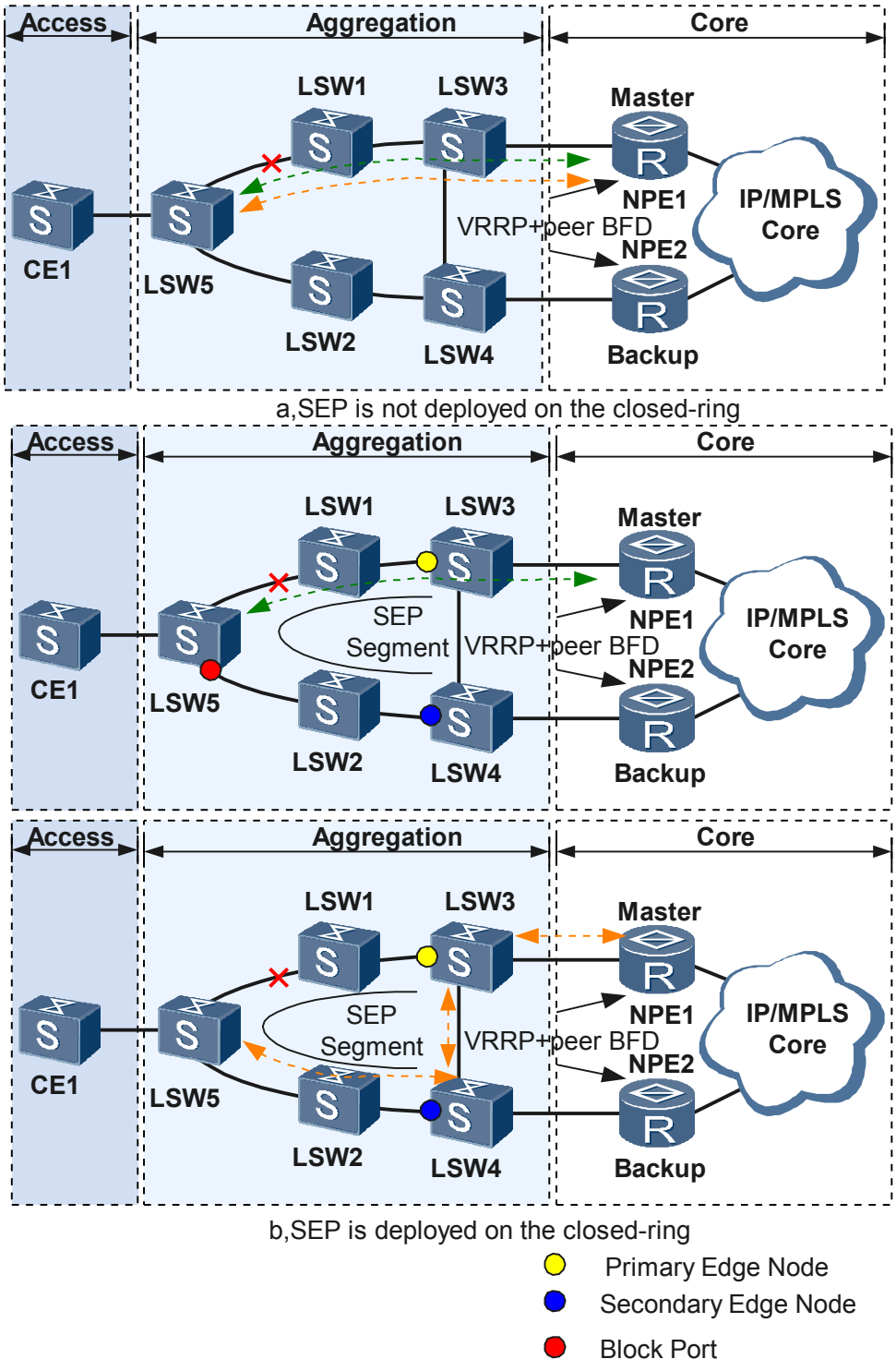
  CE1 上送的流量仍然按原路径转发，流量中断。

- 部署 SEP

  通过 SEP 协议环路保护机制，LSW5 上的阻塞端口放开并进入转发状态，同时发送 LSA（Link Status Advertisement）报文通知 SEP 段上的其他节点设备刷新各自的 LSA 数据库。CE1 上送的流量切换到备用链路 LSW5->LSW2->LSW4->LSW3->NPE1，保证了流量正常传输。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-58 SEP 典型应用示意图

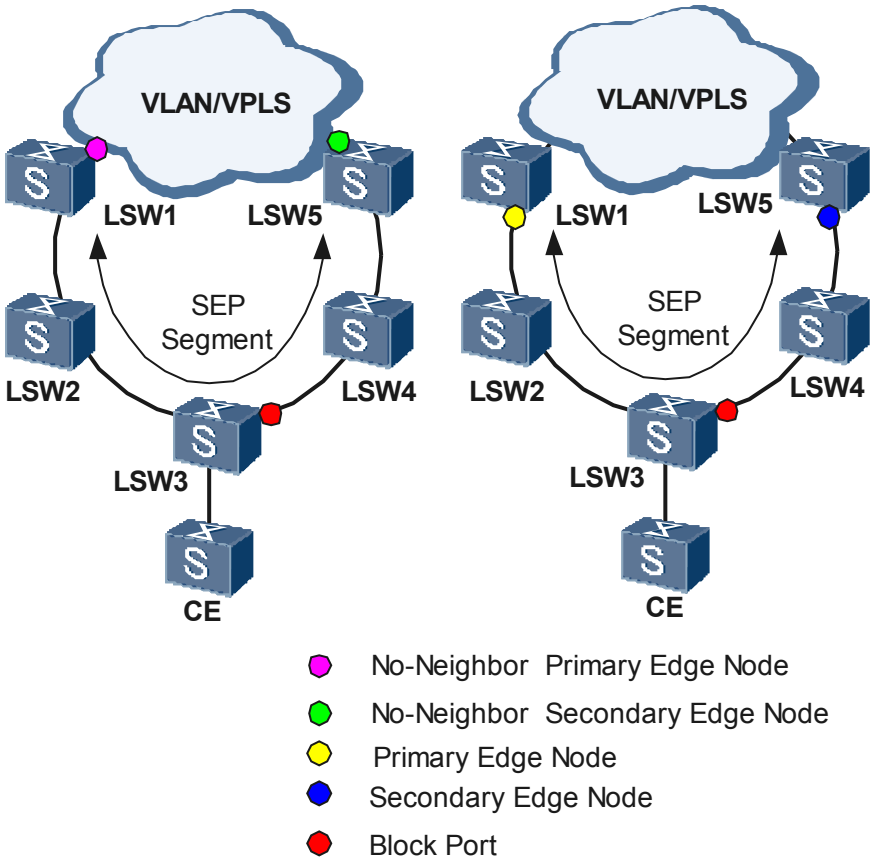


SEP 相关术语

结合图 3-58 和图 3-59 介绍 SEP 的基本概念。

版权所有 © 华为技术有限公司

图 3-59 SEP 组网图



- SEP 段

  SEP 以 SEP 段为基本单位。所谓 SEP 段，就是由一组配置了相同的 SEP 段 ID 和控制 VLAN 且互连的二层交换设备群体构成。

  一个 SEP 段物理上对应一个环形或者线性连接的以太网拓扑。每个 SEP 段具有控制 VLAN、边缘端口和普通端口等要素。

- 控制 VLAN

  在 SEP 段中，控制 VLAN 只用来传递 SEP 协议报文。

  每个 SEP 段必须配置控制 VLAN。当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN。

  不同 SEP 段可以使用相同 ID 的控制 VLAN。

  与控制 VLAN 相对，数据 VLAN 用来传递数据报文。

- 节点

  加入 SEP 段的二层交换设备称之为节点。每个节点不能多于两个端口加入同一个 SEP 段。

- 端口角色

  SEP 协议中规定，端口的角色主要有普通端口和边缘端口两大类。

  如表 3-25 所示，边缘端口可以分为主边缘端口、副边缘端口、无邻居主边缘端口和无邻居副边缘端口。

版权所有 © 华为技术有限公司

说明

正常情况下，边缘端口和无邻居边缘端口不会同时出现在同一个 SEP 段中。

表 3-25 端口角色

端口角色	子端口角色	说明	场景
普通端口（Common Port）	-	在 SEP 段中，除边缘端口以外所有的端口都是普通端口。 普通端口负责监测自己直连的启动 SEP 协议的链路状态，并把链路状态的变化消息及时通知邻居端口。邻居端口不断向 SEP 段中其他端口扩散消息，最后到达主边缘端口。然后由主边缘端口决策如何处理上报的链路状态变化消息。	-
边缘端口（Edge Port）	主边缘端口（Primary Edge Port）	一个 SEP 段中只有一个主边缘端口，由用户配置并选举决定。 主边缘端口的职责是发起阻塞端口抢占、终结报文、以及向其他网络发送拓扑变化消息。	开放环组网 封闭环组网 多环组网 SEP+RRPP 混合组网
	副边缘端口（Secondary Edge Port）	一个 SEP 段中只有一个副边缘端口，由用户配置并选举决定。 副边缘端口的职责是终结报文、以及向其他网络发送拓扑变化消息。	
	无邻居主边缘端口（No-Neighbor Primary Edge Port）	如图 3-59 所示，处于 SEP 段最边缘的端口是无邻居边缘端口，由用户配置决定。 无邻居主边缘端口的职责是发起阻塞端口抢占、终结报文、以及向其他网络发送拓扑变化消息。 无邻居主边缘端口一般用于与其他制造商设备互通或与不支持 SEP 协议的设备互通。	SEP +MSTP 混合组网
	无邻居副边缘端口（No-Neighbor Secondary Edge Port）	无邻居副边缘端口的职责是终结报文、以及向其他网络发送拓扑变化消息。 无邻居副边缘端口一般用于与其他制造商设备互通或与不支持 SEP 协议的设备互通。	

- 阻塞端口

  在 SEP 段中，为了防止形成环路而被阻塞的端口称为阻塞端口。

  在 SEP 段中，不指定端口为特定阻塞端口，SEP 段中的每个端口均有可能成为阻塞端口。在 SEP 段完好的情况下，一个 SEP 段中只有一个阻塞端口。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 启动 SEP 协议的端口状态

  SEP 段中，启动 SEP 协议的端口状态分为两种，如表 3-26 所示。

  表 3-26 端口状态表

端口状态	说明
Forwarding	在 Forwarding 状态下，端口既转发用户流量又接收、发送 SEP 协议报文。
Discarding	在 Discarding 状态下，端口只接收、发送 SEP 协议报文。

  端口状态和端口角色没有必然的联系。不同角色的端口均支持 Forwarding 和 Discarding 两种状态。

SEP 破除环路基本原理

1. 成功创建 SEP 段后，将环网上设备的端口加入 SEP 段，并为端口配置端口角色。
2. 端口加入 SEP 段后，开始启动邻居协商机制。最后完成邻居协商的链路两端的其中一个端口将成为阻塞端口。
3. 阻塞端口发送 LSA 报文，通知 SEP 段上其他节点设备更新各自的 LSA 数据库。

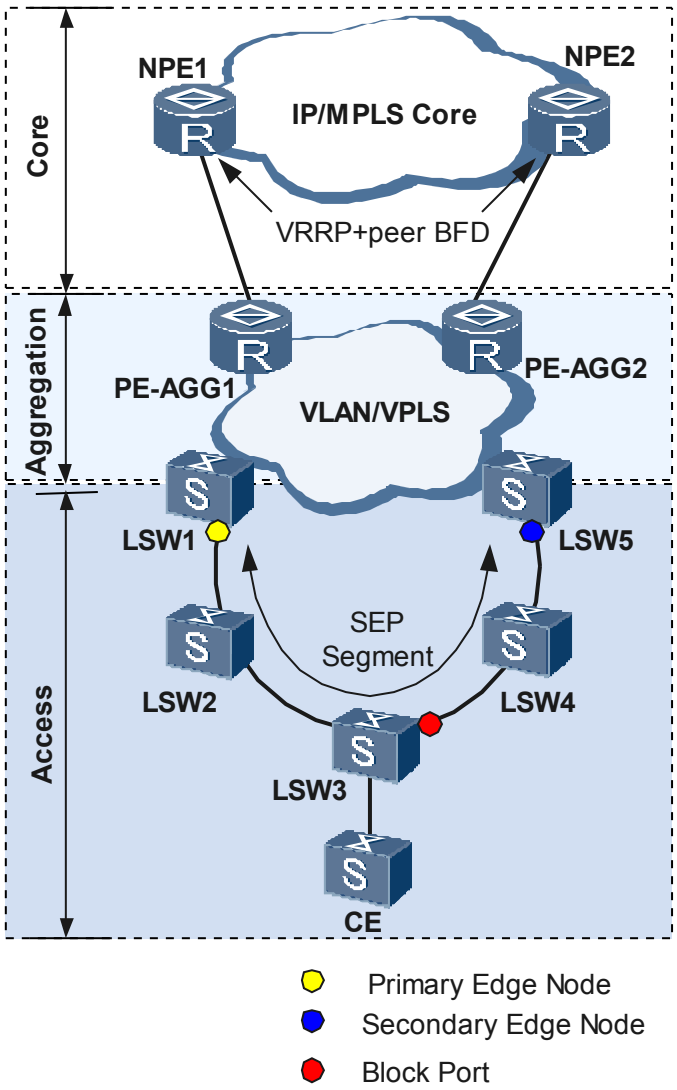
   阻塞端口不允许数据报文通过，但是允许 SEP 协议报文通过。
4. SEP 段上的其他节点设备更新 LSA 数据库后明确转发路径，成功破除环路。

SEP 支持的典型组网

- 开放环组网

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-60 SEP 开放环组网图



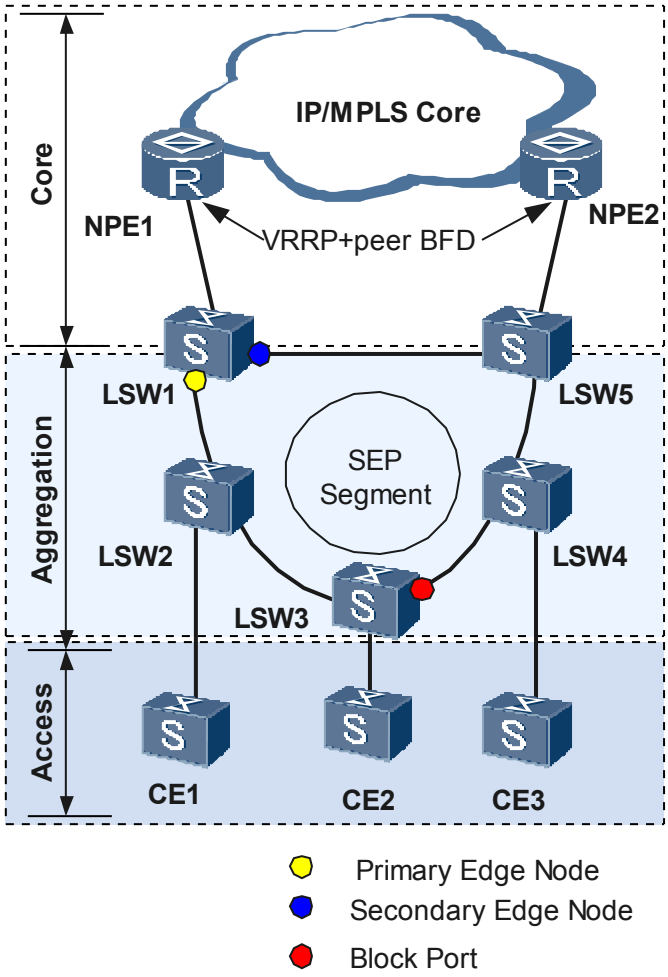
如图 3-60 所示，组网分为接入层、汇聚层和核心层。LSW1 ～ LSW5 组成了双归链路接入上级二层网络组网，LSW1 与 LSW5 之间非直连，这种组网方式称之为开放环接入。此组网位于接入层，完成单播业务及组播业务的二层透传功能。通过在接入层运行 SEP 协议，实现接入环的冗余保护倒换。

开放环组网的特点是环上的两个边缘端口部署在两个边缘设备上。

- 封闭环组网

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-61 SEP 封闭环组网图



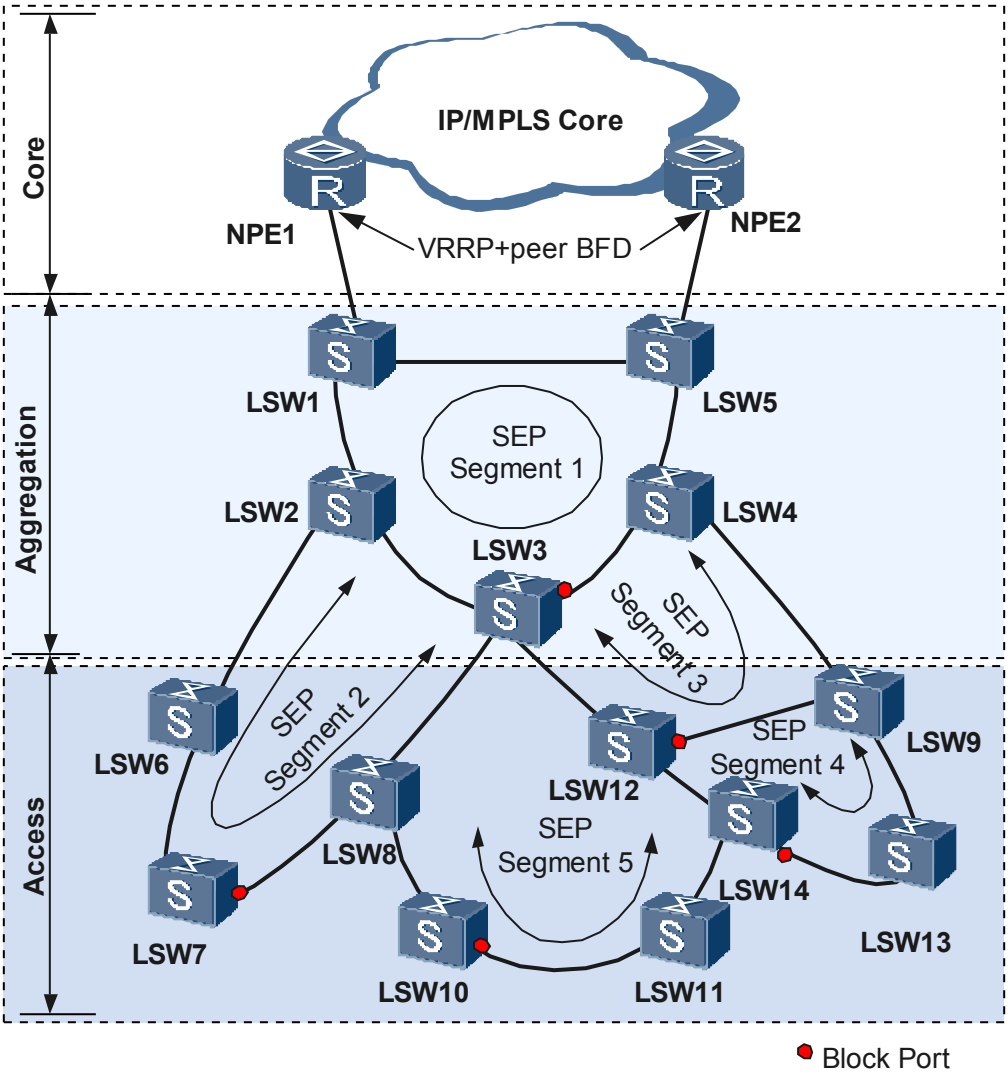
如图 3-61 所示，LSW1 ～ LSW5 组成了双归链路接入上级二层网络组网，位于上级二层网络的两台边缘设备 LSW1 和 LSW5 之间是直连的方式，这种组网方式称之为封闭环接入。此组网位于汇聚层，完成单播及组播业务的汇聚。通过在汇聚层运行 SEP 协议，实现汇聚层的冗余保护倒换。

封闭环组网的特点是环上的两个边缘端口部署在同一个边缘设备上。

- 多环组网

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-62 SEP 多环组网图



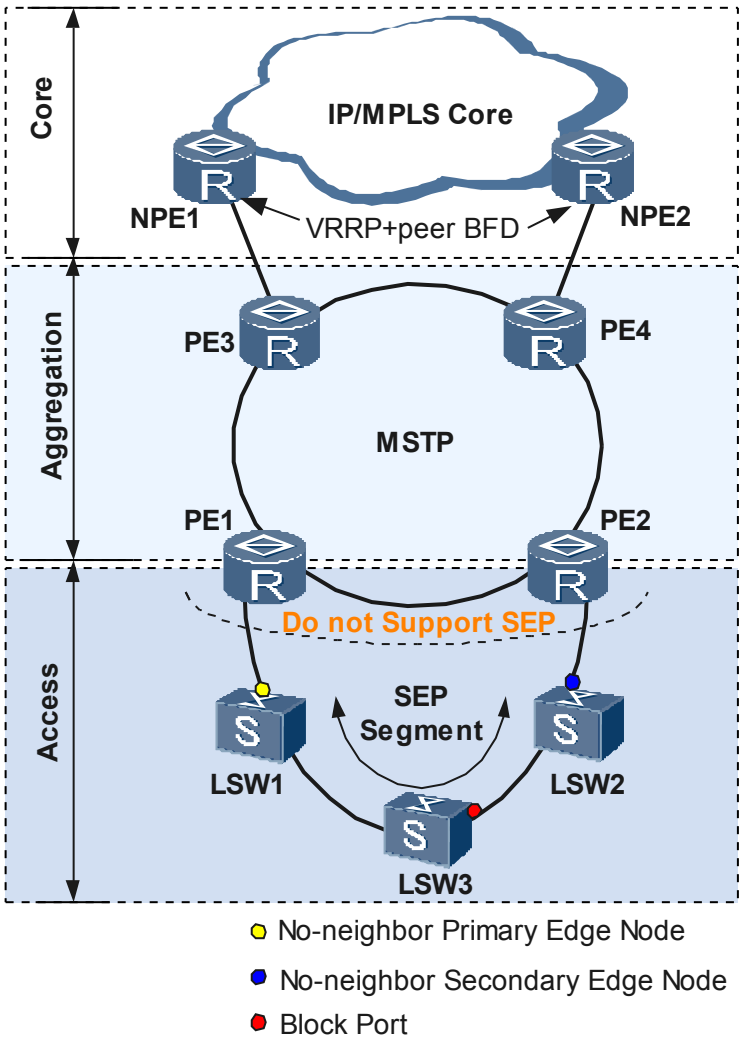
如图 3-62 所示，LSW1 ～ LSW14 的组网方式称为多环接入，LSW1 ～ LSW5 位于汇聚层，LSW6 ～ LSW14 位于接入层。网络中接入层与汇聚层均透传二层业务。通过在接入层与汇聚层运行 SEP 协议，实现接入层与汇聚层的冗余保护倒换。如果接入层拓扑发生变化，SEP 段内会发送 FLUSH-FDB 报文通知本 SEP 段内其他节点进行 MAC 转发表和 ARP 表刷新。SEP 段上的边缘设备会发送 TC 报文，通知上级网络，本 SEP 段的拓扑发生变化。

多环组网在配置上和单环的差别在于需要配置环间的拓扑变化通告。

- 混合组网
  - SEP+MSTP 混合组网

版权所有 © 华为技术有限公司

图 3-63 SEP+MSTP 混合环组网图



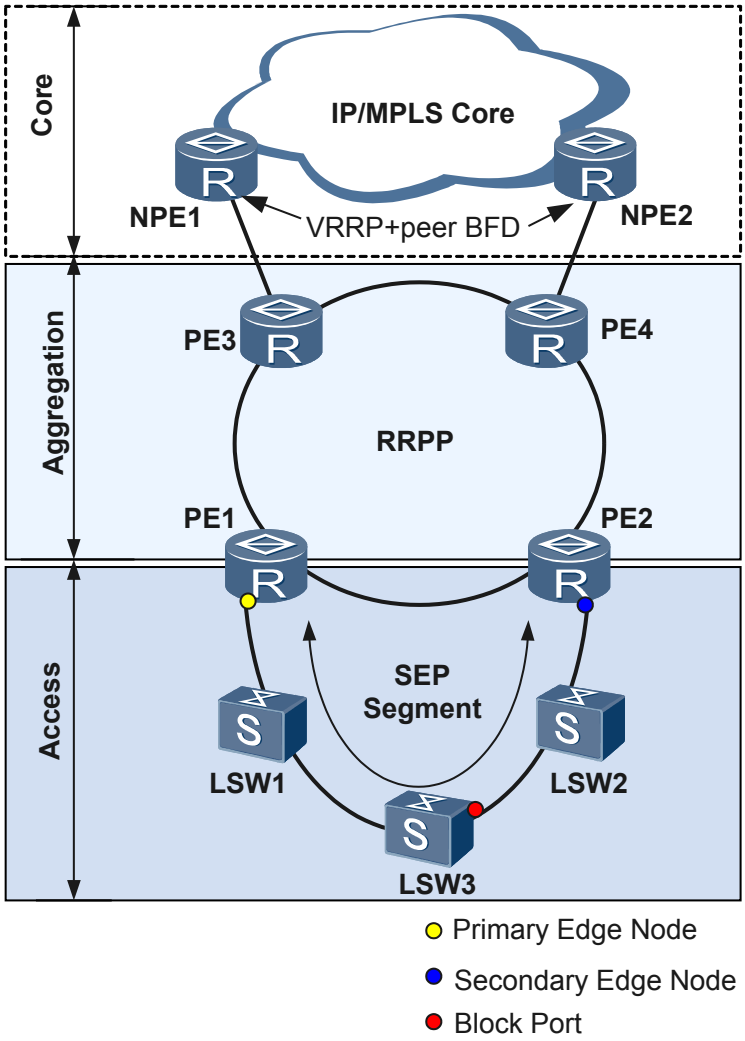
如图 3-63 所示，LSW1 ～ LSW3 组成 SEP 段接入 MSTP 环，这种组网方式称为 SEP+MSTP 混合组网。LSW1 ～ LSW3 位于接入层，完成单播或组播业务的二层透传功能。通过在接入层运行 SEP 协议，实现接入环的冗余保护倒换。如果接入层拓扑发生变化，SEP 段内会发送 FLUSH-FDB 报文通知本 SEP 段内其他节点进行 MAC 转发表和 ARP 表刷新。SEP 段上的边缘设备 LSW1 和 LSW2 会发送 TC 报文，通知汇聚层，SEP 段的拓扑发生变化。

SEP+MSTP 混合环组网的特点是需要在运行 SEP 协议的网络中的边缘设备上部署无邻居边缘端口，并部署 SEP 向 STP 拓扑变化通告。

- SEP+RRPP 混合组网

版权所有 © 华为技术有限公司

图 3-64 SEP+RRPP 混合环组网图



如图 3-64 所示，PE1、PE2 和 LSW1 ～ LSW3 组成 SEP 段接入 RRPP 环，这种组网方式称为 SEP+RRPP 混合组网。PE1、PE2 和 LSW1 ～ LSW3 位于接入层，完成单播或组播业务的二层透传功能。通过在接入层运行 SEP 协议，实现接入环的冗余保护倒换。如果接入层拓扑发生变化，SEP 段内会发送 FLUSH-FDB 报文通知本 SEP 段内其他节点进行 MAC 转发表和 ARP 表刷新。SEP 段上的边缘设备 PE1 和 PE2 会发送 TC 通告，通知汇聚层，SEP 段的拓扑发生变化。

混合环组网的特点是需要在运行 SEP 协议的网络中的边缘设备上部署 SEP 向 RRPP 拓扑变化通告。

说明

以上各种类型拓扑，SEP 的配置基本相同，区别在于主边缘端口、无邻居主边缘端口、副边缘端口、无邻居副边缘端口的选择和配置，具体描述请参见表 3-25。

AC6605 支持的 SEP 特性

本章节从 SEP 的配置逻辑角度介绍 AC6605 支持的 SEP 特性。理解 SEP 的配置逻辑后，您可以更快速、准确地完成配置任务。

SEP 的配置逻辑是：

版权所有 © 华为技术有限公司

1. SEP 基本功能配置成功后，SEP 协议开始计算，最后完成邻居协商的链路两端的其中一个端口将成为阻塞端口，消除以太网冗余链路。

   说明

   如果网管通过 Telnet 方式登录 SEP 半环的节点设备进行配置，在配置半环时，为了保证网络管理通畅，必须保证：

   - 由于节点设备是二层设备，所以配置 IP 地址需要用到 VLANIF，要求 VLANIF 所对应的 VLAN 必须映射到 SEP 的保护实例中。
   - 必须从半环的一端开始配置 SEP 基本功能，依次进行配置，直到另外一端。

2. 通过 SEP 协议计算出的阻塞端口有时并不是用户所期望的阻塞点，通过灵活指定阻塞端口，可满足用户需求。
3. 为了实现负载分担，有效利用带宽，可在运行 SEP 协议的网络上部署保护实例，将保护实例与 VLAN 映射，从而实现负载分担。
4. 运行 SEP 协议的网络经常需要和部署其他特性的网络综合运用。为了保证网络的可靠性，当网络中有拓扑发生变化时，无论是运行 SEP 协议的网络还是部署其他特性的网络均需要感知网络拓扑变化，并采取保护措施保证数据可靠传输。因此需要在运行 SEP 协议的网络上部署网络拓扑变化通告功能。

灵活指定阻塞端口

正常情况下，阻塞端口是最后完成邻居协商的链路两端的其中一个端口，通过协商选出的阻塞端口有时并不是用户所需求的阻塞点。为了满足用户的需求，用户可灵活指定阻塞端口，指定阻塞端口后并不立即生效。只有抢占机制生效后，阻塞端口才会从当前的阻塞点抢占到用户指定的阻塞点。

- 端口阻塞方式

  用户可通过配置端口阻塞方式来指定阻塞端口在网络中的位置。SEP 支持阻塞端口方式如表 3-27 所示。

表 3-27 端口阻塞方式表

端口阻塞方式	说明
指定优先级最高的端口为阻塞端口	适用于网络规模较大的网络中。 故障恢复后，SEP 段上优先级最高的端口将成为阻塞端口。但是需要人为预先设置 SEP 段上的端口优先级。
指定 SEP 段中间位置的端口为阻塞端口	适用于网络中流量需要对称分布的场景中。 故障恢复后，位于 SEP 段上中间位置的端口将成为阻塞端口。
根据用户配置的跳数指定阻塞端口	适用于网络规模较小的网络中。 故障恢复后，根据用户配置的跳数阻塞指定端口。但是网络规划者需要熟悉整个 SEP 段的拓扑，并了解阻塞端口距离主边缘端口的跳数。
根据设备名+端口名指定阻塞端口	适用于网络规模较小的网络中。 故障恢复后，根据设备名+端口名阻塞指定端口。但是网络规划者需要熟悉整个 SEP 上的设备名称和接口名称，并保证设备名称是唯一的。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 抢占功能

  用户指定端口的阻塞方式后，阻塞端口是否从当前阻塞点迁移到用户指定的阻塞点，可以通过抢占和不抢占两种模式决定。如表 3-28 所示。

表 3-28 抢占功能模式

抢占功能模式		优点	缺点
不抢占模式		无需用户配置，缺省情况下，SEP 处于不抢占模式。 不抢占模式下阻塞端口不会造成 SEP 段上的链路短暂中断。	阻塞端口是最后完成邻居协商的链路两端的其中一个端口。
抢占模式	延时抢占	无需人为干涉，每一次故障恢复，系统都能够自动完成每一次抢占，并保证当前阻塞点迁移到用户指定的阻塞点。	● 需要人为预先通过命令指定延时抢占，且抢占延时时间没有缺省值，用户必须通过命令配置抢占延时时间。 ● 延时抢占配置成功后，需要人为预先模拟一次故障，才能保证阻塞端口是用户指定的端口。
	手工抢占	可以人为控制当前阻塞点是否迁移到用户指定的阻塞点。	● 需要人为预先通过命令指定手工抢占。 ● 故障恢复后，当抢占动作完成，手工抢占不再起作用。 为了保证下一次故障恢复后，当前阻塞点能够迁移到用户指定的阻塞点，需要再进行一次手工抢占配置。这增加了用户的维护量。

说明

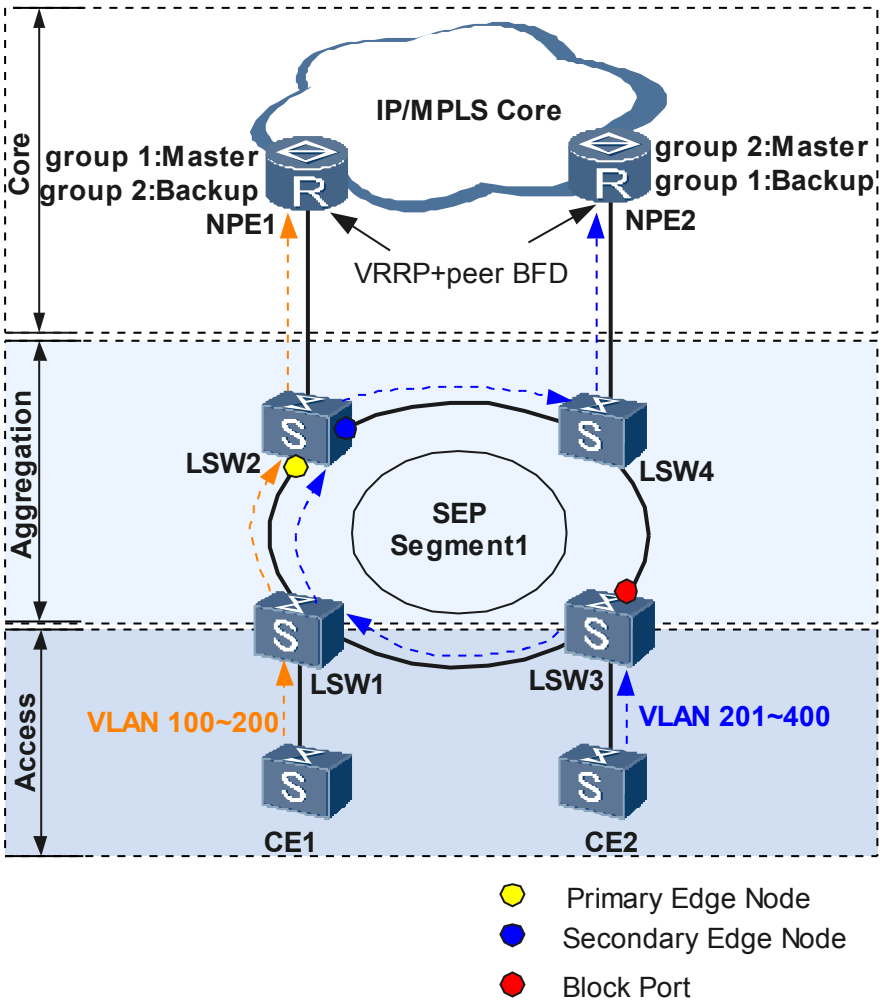
抢占模式下阻塞端口会触发 SEP 段中短暂的链路中断。

SEP 多实例

如图 3-65 所示，在普通的 SEP 组网图中，一个物理环上只能配置一个 SEP 段，也只能指定一个阻塞点。当 SEP 段处于完整状态时，阻塞端口会阻止所有的用户数据通过。这样，所有用户数据在 SEP 段上只能通过一条路径传输，阻塞端口另一侧的链路空闲，造成带宽浪费。

版权所有 © 华为技术有限公司

图 3-65 SEP 组网图



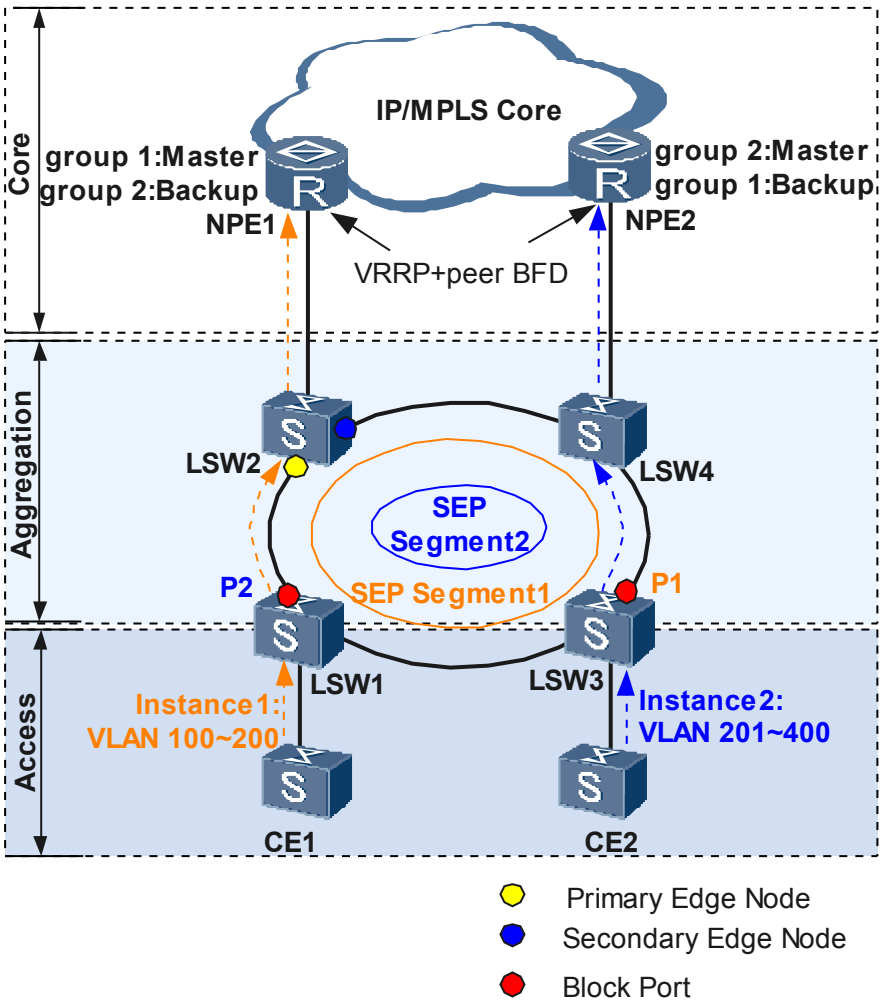
SEP 多实例允许在一个物理环路上配置两个逻辑环路，即两个 SEP 段。每一个 SEP 段上所有设备、端口角色、控制 VLAN 等都必须遵循基本的 SEP 原则。相应的，一个物理环路上有两个阻塞端口，各个阻塞端口分别检测物理环路的完整性，并相应的阻塞或放开，彼此互不影响。

一个物理环路上可以包含一个或两个 SEP 段，每个 SEP 段上均需要配置一个保护实例，每个保护实例代表一个 VLAN 范围。不同的 SEP 段计算出的拓扑仅对该 SEP 段有效，不影响其他 SEP 段。

通过给每个 SEP 段配置不同的保护实例，各阻塞端口只对本 SEP 段所保护的 VLAN 有效。属于不同 VLAN 的数量流量就可以通过不同的路径传输，从而实现流量的负载分担和链路备份。

版权所有 © 华为技术有限公司

图 3-66 SEP 多实例组网图



如图 3-66 所示，LSW1 ～ LSW4 组成的 SEP 多实例环上有两个 SEP 段。P1 是 ID 为 1 的 SEP 段的阻塞端口，P2 是 ID 为 2 的 SEP 段的阻塞端口。

- SEP 段 1 上配置保护实例 1，保护对应的 VLAN100 ～ VLAN200 数据，其传输路径是 LSW1->LSW2->NPE1。P2 作为 SEP 段 2 的阻塞端口，阻塞仅对 VLAN201 ～ VLAN400 数据有效，不会影响 VLAN100 ～ VLAN200 数据通过。
- SEP 段 2 上配置保护实例 2，保护对应的 VLAN201 ～ VLAN400 数据，其传输路径是 LSW3->LSW4->NPE2。P1 作为 SEP 段 1 的阻塞端口，阻塞仅对 VLAN100 ～ VLAN200 数据有效，不会影响 VLAN201 ～ VLAN400 数据通过。

当节点或链路故障时，各 SEP 段独立计算拓扑变化，更新各自节点上的 LSA 数据库。

网络拓扑变化通告

在启用 SEP 协议的拓扑中，表 3-29 标识了 SEP 拓扑发生变化。

版权所有 © 华为技术有限公司

表 3-29 SEP 拓扑变化

SEP 拓扑变化	说明
端口故障	在 SEP 段完整的情况下，有端口故障产生。 端口故障包括链路故障和端口邻居状态故障。
故障恢复且抢占生效	SEP 段中存在故障，当最后一处故障恢复，同时进行了阻塞端口抢占。

网络拓扑变化通告如**表 3-30** 所示。

表 3-30 网络拓扑变化通告

网络拓扑变化通告	场景	说明	解决方案
下级网络向上级发送拓扑变化通告	运行 SEP 协议网络与运行其他特性的网络混合组网，且运行其他特性的网络位于上级网络。 这里的其他特性包括：SEP、STP、RRPP、SmartLink。	● 如果人为更改了下级运行 SEP 协议网络中指定的阻塞端口，此 SEP 段中的拓扑发生变化。由于上级网络将感知不到此 SEP 段的拓扑发生变化，将导致流量中断。 ● 如果下级运行 SEP 协议网络中有端口发生故障导致拓扑变化，此时由于上级网络感知不到下级网络拓扑发生变化，将导致流量中断。	SEP 拓扑变化通告
	用户通过 SmartLink 接入运行 SEP 协议网络。	SmartLink 链路切换时会发送 SmartLink Flush 报文通知远端设备。 如果 SEP 段上的设备不能识别 SmartLink Flush 报文，即无法感知下游网络拓扑发送变化，将导致流量中断。	使能 SEP 段上的设备处理 SmartLink Flush 报文功能
上级网络向下级发送拓扑变化通告	运行 SEP 协议的网络与支持部署 CFM 功能的网络混合组网，且部署 CFM 功能的网络位于上级网络。	当上级网络发生故障导致拓扑变化时，由于下级运行 SEP 协议的网络不能感知上级网络的拓扑变化，将导致流量中断。	SEP 与 CFM 联动功能

3.10.2 配置 SEP 基本功能

当环网上没有故障链路时，SEP 能够消除以太网冗余环路；当环网发生链路故障时，SEP 能够迅速恢复环网上各节点间通信通路。

版权所有 © 华为技术有限公司

建立配置任务

在进行 SEP 基本功能配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

为了进行链路备份，提高网络可靠性，用户通常会使用冗余链路接入上层网络，但是使用冗余链路会在网络中产生环路。环路会造成报文在环路内不断的循环转发，最终导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为了阻塞冗余环路，并实现当环网上发生链路故障时，阻塞的冗余链路能够迅速恢复通信，可在环网上部署 SEP 协议。

前置任务

在配置 SEP 基本功能之前，需完成以下任务：

- 在物理上搭建环形拓扑的组网环境。
- 设备正确上电，且工作正常。

数据准备

在配置 SEP 基本功能之前，需准备以下数据。

序号	数据
1	SEP 段 ID
2	SEP 段控制 VLAN 的 ID
3	加入 SEP 段端口的端口角色

创建 SEP 段

SEP 协议以 SEP 段为基本单位。所谓 SEP 段，就是由一组配置了相同的 SEP 段 ID 和控制 VLAN 且互连的二层交换设备群体构成。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，创建 SEP 段并进入 Sep-segment 视图。

若需要删除已经创建的 SEP 段，请确认此 SEP 段中没有接口。如果指定 SEP 段中已经存在接口，请在加入 SEP 段的接口视图下执行命令 **undo sep segment** *segment-id*，将接口从指定 SEP 段中退出，否则不允许删除。

----结束

版权所有 © 华为技术有限公司

配置控制 VLAN

在 SEP 段中，控制 VLAN 只用来转发 SEP 协议报文，不用来转发用户业务报文，从而提高了 SEP 协议的安全性。每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN。

背景信息

说明

在无邻居场景下，不在 SEP 段中的设备不能加入 SEP 段的控制 VLAN，否则会导致网络成环。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **control-vlan** *vlan-id*，配置 SEP 段的控制 VLAN，用于转发 SEP 协议报文。

由参数 *vlan-id* 指定的控制 VLAN 必须是未被创建的，未被 RRPP 协议使用且未被 port trunk、default、mapping、stacking 等方式使用过的 VLAN。

- 不同 SEP 段可以使用相同 ID 的控制 VLAN。
- 如果 SEP 段中已经加入接口，那么将不能直接删除控制 VLAN。若需要删除已配置的控制 VLAN，必须在接口视图下执行命令 **undo sep segment** *segment-id* 将接口退出 SEP 段，然后再执行命令 **undo control-vlan** 删除控制 VLAN。
- 如果 SEP 段中没有接口加入，可以多次配置控制 VLAN，以最后一次配置为准。
- 控制 VLAN 成功创建后，配置文件会自动显示创建普通 VLAN 的命令。

  每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN。
  - 如果接口类型是 Trunk 类型，则配置文件中，加入 SEP 段的接口下会自动显示命令 **port trunk allow-pass vlan**。
  - 如果接口类型是 Hybrid 类型，则配置文件中，加入 SEP 段的接口下会自动显示命令 **port hybrid tagged vlan**。

----结束

创建保护实例

只有先成功创建 SEP 段的保护实例，才能成功将端口加入 SEP 段。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **protected-instance** { **all** | { *instance-id1* [**to** *instance-id2*] &<1-10> } }，创建 SEP 段的保护实例。

缺省情况下，SEP 段上没有配置保护实例。

----结束

版权所有 © 华为技术有限公司

将二层端口加入 SEP 段并配置端口角色

为了保证 SEP 协议报文的正常转发，必须将二层端口加入 SEP 段并为加入 SEP 段的端口设置不同的端口角色。

背景信息

端口加入 SEP 段后，如果符合参与主边缘端口选举要求，则主动将自己的端口角色设置为主边缘端口，并开始周期发送主边缘选举报文，不需要等待邻居协商成功。

主边缘选举报文中携带端口角色（主边缘端口、副边缘端口、普通端口）、端口的桥 MAC 地址、端口 ID、拓扑数据库状态是否完整等信息。

端口角色的设置如表 3-31 所示。

表 3-31 端口角色

端口角色	子端口角色	说明	场景
普通端口（Common Port）	-	在 SEP 段中，除边缘端口以外所有的端口都是普通端口。 普通端口负责监测自己直连的启动 SEP 协议的链路状态，并把链路状态的变化消息及时通知邻居端口。邻居端口不断向 SEP 段中其他端口扩散消息，最后到达主边缘端口。然后由主边缘端口决策如何处理上报的链路状态变化消息。	-
边缘端口（Edge Port）	主边缘端口（Primary Edge Port）	一个 SEP 段中只有一个主边缘端口，由用户配置并选举决定。 主边缘端口的职责是发起阻塞端口抢占、终结报文、以及向其他网络发送拓扑变化消息。	开放环组网 封闭环组网 多环组网 SEP+RRPP 混合组网
	副边缘端口（Secondary Edge Port）	一个 SEP 段中只有一个副边缘端口，由用户配置并选举决定。 副边缘端口的职责是终结报文、以及向其他网络发送拓扑变化消息。	
	无邻居主边缘端口（No-Neighbor Primary Edge Port）	如图 3-59 所示，处于 SEP 段最边缘的端口是无邻居边缘端口，由用户配置决定。 无邻居主边缘端口的职责是发起阻塞端口抢占、终结报文、以及向其他网络发送拓扑变化消息。 无邻居主边缘端口一般用于与其他制造商设备互通或与不支持 SEP 协议的设备互通。	SEP+MSTP 混合组网

版权所有 © 华为技术有限公司

端口角色	子端口角色	说明	场景
	无邻居副边缘端口（No-Neighbor Secondary Edge Port）	无邻居副边缘端口的职责是终结报文、以及向其他网络发送拓扑变化消息。 无邻居副边缘端口一般用于与其他制造商设备互通或与不支持 SEP 协议的设备互通。	

说明

正常情况下，边缘端口和无邻居边缘端口不会同时出现在同一个 SEP 段中。

除了无邻居边缘端口以外，所有在端口加入 SEP 段之前，必须已经去使能 STP。

在将端口加入 SEP 段之前，必须先创建 SEP 段的保护实例。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **interface** *interface-type interface-number*，进入需要加入 SEP 段的以太网接口视图。

步骤 3 执行命令 **stp disable**，去使能二层端口的 STP 功能。

步骤 4 执行命令 **sep segment** *segment-id* [**edge** [**no-neighbor**] { **primary** | **secondary** }]，将二层端口加入指定 SEP 段，并为加入 SEP 段的二层端口设置不同的端口角色。

说明

在 AC6605 上同一接口允许加入两个 SEP 段。

----结束

检查配置结果

SEP 基本功能成功配置后，您可以查看到加入指定 SEP 段的端口名、端口角色、邻居端口状态、本地端口转发状态等信息。

前提条件

已经成功完成 SEP 基本功能所有配置。

操作步骤

- 执行命令 **display sep interface** [*interface-type interface-number* | **segment** *segment-id*] [**verbose**]，查看本设备上加入 SEP 的端口信息。
- 执行命令 **display sep topology** [**segment** *segment-id*] [**verbose**]，查看 SEP 段的拓扑状态信息。

----结束

版权所有 © 华为技术有限公司

3.10.3 灵活指定阻塞端口

缺省情况下，阻塞端口是最后完成邻居协商的链路两端的其中一个端口，此端口有时并不是用户所需求的阻塞点。为了满足用户的需求，用户可灵活指定阻塞端口。

建立配置任务

在进行灵活指定阻塞端口配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

正常情况下，阻塞端口是最后完成邻居协商的链路两端的其中一个端口，通过协商选出的阻塞端口有时并不是用户所需求的阻塞点。为了满足用户的需求，用户可灵活指定阻塞端口，指定阻塞端口后并不立即生效。只有抢占机制生效后，阻塞端口才会从当前的阻塞点抢占到用户指定的阻塞点。

前置任务

在灵活指定阻塞端口之前，需完成以下任务：

- 已经成功完成**配置 SEP 基本功能**。

数据准备

在灵活指定阻塞端口之前，需准备以下数据。

序号	数据
1	端口的阻塞方式
2	SEP 抢占模式

配置端口的阻塞方式

在 SEP 段中，不指定端口为特定阻塞端口，SEP 段中的每个端口均有可能成为阻塞端口，用户可配置端口的阻塞方式指定阻塞端口。

背景信息

在 SEP 段中，为了防止形成环路而被阻塞的端口称为阻塞端口。

用户可通过配置端口阻塞方式来指定阻塞端口在网络中的位置。SEP 支持阻塞端口方式如**表 3-32** 所示。

版权所有 © 华为技术有限公司

表 3-32 端口阻塞方式表

端口阻塞方式	说明
指定优先级最高的端口为阻塞端口	适用于网络规模较大的网络中。 故障恢复后，SEP 段上优先级最高的端口将成为阻塞端口。但是需要人为预先设置 SEP 段上的端口优先级。
指定 SEP 段中间位置的端口为阻塞端口	适用于网络中流量需要对称分布的场景中。 故障恢复后，位于 SEP 段上中间位置的端口将成为阻塞端口。
根据用户配置的跳数指定阻塞端口	适用于网络规模较小的网络中。 故障恢复后，根据用户配置的跳数阻塞指定端口。但是网络规划者需要熟悉整个 SEP 段的拓扑，并了解阻塞端口距离主边缘端口的跳数。
根据设备名+端口名指定阻塞端口	适用于网络规模较小的网络中。 故障恢复后，根据设备名+端口名阻塞指定端口。但是网络规划者需要熟悉整个 SEP 上的设备名称和接口名称，并保证设备名称是唯一的。

请在主边缘端口或无邻居主边缘端口位于的设备上执行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **block port** { **optimal** | **middle** | **hop** *hop-id* | **sysname** *sysname* **interface** *interface-type interface-number* }，配置端口的阻塞方式。

缺省情况下，系统会自动协商出一个阻塞端口。协商的原则是从最后建立起来或故障恢复的那条链路的两个端口中协商出一个阻塞端口。

- **optimal**，指定优先级高的端口是阻塞端口。
- **middle**，指定 SEP 网络中间位置的端口是阻塞端口。
- **hop**，根据跳数指定阻塞端口。

  hop-id 取值是 1 时，表示阻塞的端口是主边缘端口。主边缘端口的邻居端口 hop-id 为 2，hop-id 沿着主边缘端口的下游邻居方向依次增加。
- **sysname+interface**，根据设备名+端口名指定阻塞端口。

如何选择端口阻塞方式，请见上表。

----结束

后续处理

如果端口阻塞方式选择指定优先级高的端口是阻塞端口，请在需要阻塞的接口视图下执行命令 **sep segment** *segment-id* **priority** *priority*，将需要阻塞的端口优先级调高，保证故障恢复时，阻塞端口成功迁移到用户指定的端口。

版权所有 © 华为技术有限公司

缺省情况下，加入 SEP 段中的端口优先级是 64。端口优先级的取值范围是 1 ～ 128，取值越大，优先级越高。

配置抢占模式

SEP 抢占模式分为延时抢占和手工抢占。

背景信息

用户指定端口的阻塞方式后，阻塞端口是否从当前阻塞点迁移到用户指定的阻塞点，可以通过抢占和不抢占两种模式决定。如表 3-33 所示。

表 3-33 抢占功能模式

抢占功能模式		优点	缺点
不抢占模式		无需用户配置，缺省情况下，SEP 处于不抢占模式。 不抢占模式下阻塞端口不会造成 SEP 段上的链路短暂中断。	阻塞端口是最后完成邻居协商的链路两端的其中一个端口。
抢占模式	延时抢占	无需人为干涉，每一次故障恢复，系统都能够自动完成每一次抢占，并保证当前阻塞点迁移到用户指定的阻塞点。	● 需要人为预先通过命令指定延时抢占，且抢占延时时间没有缺省值，用户必须通过命令配置抢占延时时间。 ● 延时抢占配置成功后，需要人为预先模拟一次故障，才能保证阻塞端口是用户指定的端口。
	手工抢占	可以人为控制当前阻塞点是否迁移到用户指定的阻塞点。	● 需要人为预先通过命令指定手工抢占。 ● 故障恢复后，当抢占动作完成，手工抢占不再起作用。 为了保证下一次故障恢复后，当前阻塞点能够迁移到用户指定的阻塞点，需要再进行一次手工抢占配置。这增加了用户的维护量。

触发抢占必须满足以下条件：

- SEP 段拓扑必须是完整。
- SEP 段中已经成功选举出主边缘端口或无邻居主边缘端口。
- 主边缘端口或无邻居主边缘端口位于的设备上，已经灵活指定阻塞端口。

请在主边缘端口或无邻居主边缘端口位于的设备上执行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **preempt** { **manual** | **delay** *seconds* }，在主边缘端口上配置 SEP 的抢占模式。

缺省情况下，主边缘端口上没有配置抢占模式，即为不抢占模式。

----结束

检查配置结果

灵活指定阻塞端口成功配置后，您可以查看到指定的阻塞端口。

前提条件

已经成功完成灵活指定阻塞端口所有配置。

操作步骤

- 执行命令 **display sep topology** [**segment** *segment-id*] [**verbose**]，查看 SEP 段的拓扑状态信息。

----结束

3.10.4 配置 SEP 多实例

SEP 多实例允许在一个物理环路上配置两个 SEP 段，通过给每个 SEP 段创建不同的保护实例，及将 VLAN 映射到指定保护实例，从而实现业务流量的负载分担和链路备份。

建立配置任务

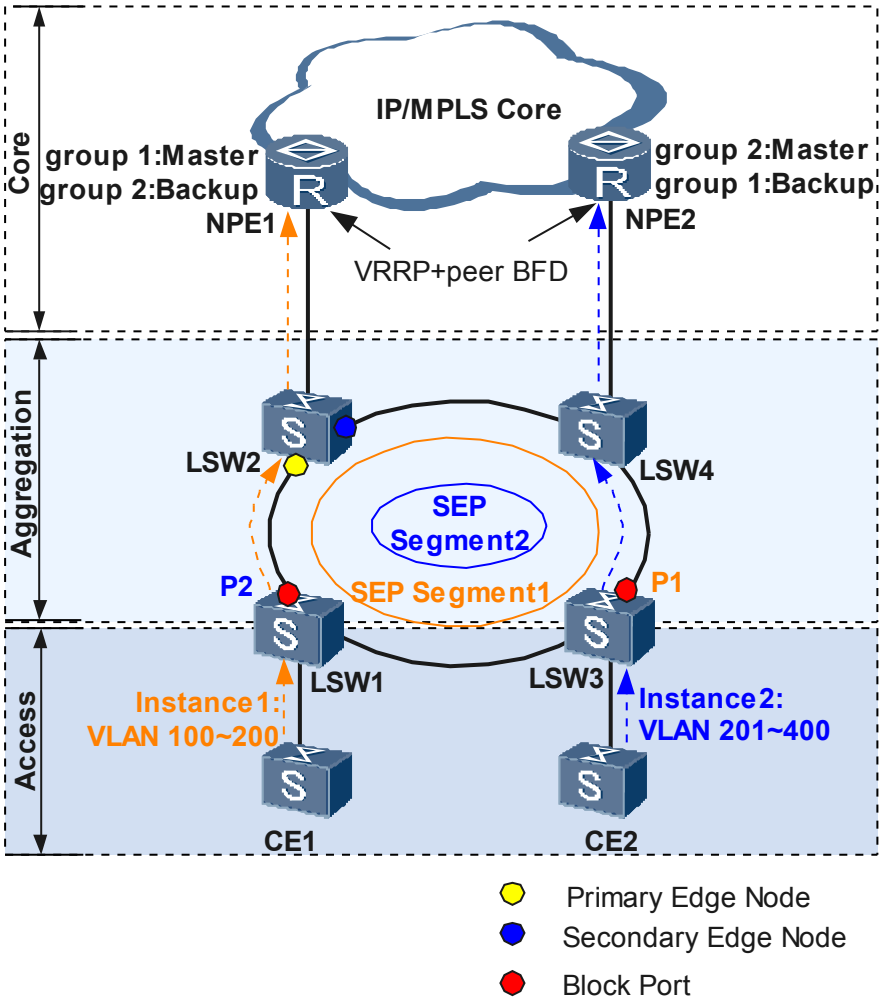
在进行 SEP 多实例配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在普通的 SEP 组网图中，一个物理环上只能配置一个 SEP 段，也只能指定一个阻塞点。当 SEP 段处于完整状态时，阻塞端口会阻止所有的用户数据通过。这样，所有用户数据在 SEP 段上只能通过一条路径传输，阻塞端口另一侧的链路空闲，造成带宽浪费。

版权所有 © 华为技术有限公司

图 3-67 SEP 多实例组网图



为了解决带宽浪费，同时实现负载分担和链路备份，如图 3-67 所示，可在 SEP 段上部署多实例，不同的实例与不同的 VLAN 映射。这样属于不同 VLAN 的数量流量就可以通过不同的路径传输，从而实现流量的负载分担和链路备份，也解决了带宽浪费问题。

说明

- 目前，SEP 多实例只允许在一个物理环路上配置两个逻辑环路，即两个 SEP 段。

前置任务

在配置 SEP 多实例之前，需完成以下任务：

- 已经成功**配置 SEP 基本功能**。
- 已经成功**灵活指定阻塞端口**。

数据准备

在配置 SEP 多实例之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	SEP 段的保护实例 ID
2	与 SEP 段映射的 VLAN ID

配置并激活保护实例与 VLAN 的映射关系

一个物理环路上可以包含一个或两个 SEP 段，为了保证用户流量可靠传输，每个 SEP 段上均需要配置一个保护实例，通过将保护实例和指定 VLAN 映射，可实现负载分担和链路备份。

背景信息

保护实例与 VLAN 的映射关系成功配置后，只有激活此配置，保护实例与 VLAN 的映射关系才能生效，从而实现负载分担和链路备份。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行命令 **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>，配置保护实例与 VLAN 的映射关系。

参数 *instance-id* 必须与 **protected-instance** 中指定的 *instance-id* 一致。

步骤 4 执行命令 **active region-configuration**，激活保护实例与 VLAN 的映射关系的配置。

保护实例与 VLAN 的映射关系生效后，SEP 段上端口的转发状态变化或拓扑变化只影响对应的 VLAN，而不影响其他 VLAN，从而保证用户数据可靠传输。

----结束

检查配置结果

SEP 多实例成功配置后，您可以查看到不同的 SEP 段上对应的不同阻塞端口。

前提条件

已经成功完成 SEP 多实例所有配置。

操作步骤

- 执行命令 **display sep topology** [**segment** *segment-id*] [**verbose**]，查看 SEP 段的拓扑状态信息。

----结束

版权所有 © 华为技术有限公司

3.10.5 配置网络拓扑变化通告

网络拓扑变化通告部署在连接上、下级网络的设备上，用于上、下级网络拓扑变化时发送拓扑变化通告通知对方网络，以便对方网络中的所有设备及时清除 MAC 地址表项和 ARP 表项，重新学习对方网络拓扑变化后的 MAC 地址，从而保证用户流量不中断。

建立配置任务

在进行网络拓扑变化通告配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

目前，AC6605 支持如表 3-34 所示两种网络拓扑变化通告，用户可根据实际需要选择部署网络拓扑变化通告。

表 3-34 网络拓扑变化通告

网络拓扑变化通告	场景	说明	解决方案
下级网络向上级发送拓扑变化通告	运行 SEP 协议网络与运行其他特性的网络混合组网，且运行其他特性的网络位于上级网络。 这里的其他特性包括：SEP、STP、RRPP、SmartLink。	● 如果人为更改了下级运行 SEP 协议网络中指定的阻塞端口，此 SEP 段中的拓扑发生变化。由于上级网络将感知不到此 SEP 段的拓扑发生变化，将导致流量中断。 ● 如果下级运行 SEP 协议网络中有端口发生故障导致拓扑变化，此时由于上级网络感知不到下级网络拓扑发生变化，将导致流量中断。	SEP 拓扑变化通告
	用户通过 SmartLink 接入运行 SEP 协议网络。	SmartLink 链路切换时会发送 SmartLink Flush 报文通知远端设备。 如果 SEP 段上的设备不能识别 SmartLink Flush 报文，即无法感知下游网络拓扑发送变化，将导致流量中断。	使能 SEP 段上的设备处理 SmartLink Flush 报文功能
上级网络向下级发送拓扑变化通告	运行 SEP 协议的网络与支持部署 CFM 功能的网络混合组网，且部署 CFM 功能的网络位于上级网络。	当上级网络发生故障导致拓扑变化时，由于下级运行 SEP 协议的网络不能感知上级网络的拓扑变化，将导致流量中断。	SEP 与 CFM 联动功能

前置任务

在配置网络拓扑变化通告之前，需完成以下任务：

华为专有和保密信息
版权所有 © 华为技术有限公司

- 已经成功**配置 SEP 基本功能**。
- 已经成功**灵活指定阻塞端口**。

数据准备

在配置网络拓扑变化通告之前，需准备以下数据。

序号	数据
1	SEP 段 ID
2	网络拓扑变化通告方式
3	MD 和 MA 的名称、MEP 的 ID、MEP 所在接口的名称、MEP 的类型，使能以太网 CFM 功能的接口、与以太网 CFM 功能联动的接口

配置下级网络拓扑变化通告-SEP 拓扑变化通告

SEP 协议运行在接入层，为了便于上级网络及时感知接入层网络拓扑是否发生变化，需要在连接上、下层网络的设备上部署 SEP 拓扑变化通告。

背景信息

当指定 SEP 段的拓扑发生变化，而没有及时通知到上级网络，那么上级网络的 MAC 地址表中仍然保留下游网络拓扑变化前的 MAC 地址表项，这样就会导致用户流量中断。为了保证用户流量正常通信，需要部署下级网络向上级网络发送拓扑变化通告，用户可根据实际网络选择本 SEP 段的拓扑变化通知的指定对象。

说明

目前，SEP 拓扑变化通告的对象包括：其他 SEP 段、运行 STP 协议的网络、运行 RRPP 协议的网络和部署 SmartLink 特性的网络。

当上级网络收到下游网络拓扑变化的消息后，会在本网络内发送 TC 报文，通知本网络内的所有设备清除 MAC 地址，重新学习下游网络拓扑变化后的 MAC 地址，从而保证用户流量不中断。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **tc-notify** { **segment** { *segment-id1* [**to** *segment-id2*] } &<1－10> | **stp** | **rrpp** | **smart-link send-packet vlan** *vlan-id* }，配置 SEP 拓扑变化通告。

缺省情况下，本 SEP 段不发送网络拓扑变化通告。

----结束

后续处理

如果 SEP 段上存在多级环（3 级或 3 级以上），当多条链路发送拓扑变化通告，将导致上级网络接收到多个相同的拓扑变化通告，使得上级网络处理有效报文的效率降低，此

版权所有 © 华为技术有限公司

时需要抑制拓扑变化通告。抑制拓扑变化通告可避免上级网络同时处理多条相同的拓扑变化通告报文，使得上级网络在保护时间内仅处理 3 条不同源的拓扑变化通告报文，同时还可以避免 SEP段上的设备受到 TC（Topology Change）攻击。

在 Sep-segment 视图下，执行命令 **tc-protection interval** *interval-value*，配置 SEP 拓扑变化保护时间间隔，抑制拓扑变化通告。

缺省情况下，SEP 拓扑变化保护时间间隔是 2 秒，2 秒钟内只处理 3 个不同源的拓扑变化通告报文，且处理不同源的拓扑变化通告报文个数是固定的，不随配置的保护时间变化。

如果设备收到的是同源的拓扑变化通告报文，那么设备在任何时间内只处理一条拓扑变化通告报文。即，同源的拓扑变化通告报文处理不受配置的保护时间影响。

说明

- 当存在多级环（3 级或 3 级以上）时必须配置此命令，否则采用缺省值。
- 配置较长的时间间隔，可以使 SEP 协议运行更稳定，但是会导致环路收敛性能降低。

配置下级网络拓扑变化通告-使能 SEP 段上设备处理 SmartLink Flush 报文功能

当用户通过 SmartLink 接入 SEP 网络，SmartLink 的主备链路切换时会发送 SmartLink Flush 报文通知远端设备。此时，SEP 段上连接用户的设备必须拥有处理 SmartLink Flush 报文的能力。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **sep segment** *segment-id*，进入已经成功创建的 Sep-segment 视图。

步骤 3 执行命令 **deal smart-link-flush**，使能 SEP 段上设备处理 SmartLink Flush 报文功能。

当 SEP 段上的设备收到 SmartLink Flush 报文后会在 SEP 段上进行 FLUSH-FDB（Forwarding Database）扩散，通告 SEP 段上其他设备网络拓扑发生变化。

缺省情况下，SEP 段上设备未使能处理 SmartLink Flush 报文功能。

----结束

配置上级网络拓扑变化通告-SEP 与 CFM 联动功能

SEP 协议运行在接入层或汇聚层，为了便于运行 SEP 协议的网络及时感知上级网络拓扑是否发生变化，需要在连接上、下层网络的设备上部署 SEP 和 CFM 联动功能。

背景信息

当 CFM 检测到上层网络产生故障时，边缘设备通过 CFM 协议报文将故障消息通知 OAM 管理模块，触发边缘设备上绑定 CFM 的端口 SEP 状态变为 Down。

当边缘设备上绑定 CFM 的端口 SEP 状态变为 Down 后，边缘设备的对端设备（位于 SEP 段上）上的端口需要发出 FLUSH-FDB 报文通知 SEP 段上其他节点拓扑发生变化。SEP 段上的设备接收到 FLUSH-FDB 报文后，SEP 段上的阻塞端口需要放开进入转发状态，并发送 FLUSH-FDB 报文，触发刷新 SEP 段上的节点 MAC 地址转发表和 ARP 表，从而实现下级网络感知上级网络故障，保证业务可靠传输。

版权所有 © 华为技术有限公司

说明

802.1ag（Connectivity Fault Management，简称 CFM）定义了基于以太网承载网络的连接检测的 OAM（Operations Administration and Maintenance）功能，包括 CC/LB/LT，适用于大规模组网的端到端场景，是网络级的 OAM。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **oam-mgr**，进入 OAM 管理视图。

步骤 3 执行命令 **oam-bind ingress cfm md** *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*，配置 SEP 与 CFM 联动功能。

- **md** *md-name*：指定一个维护域。与 *ma-name* 组合最长为 44 个字符。
- **ma** *ma-name*：指定一个维护联合(maintenance association)。与 *md-name* 组合最长为 44 个字符。
- **interface** 必须已经成功加入 SEP 段。

----结束

检查配置结果

网络拓扑变化通告成功配置后，您可以查看到网络拓扑通告指定对象。

前提条件

已经成功完成网络拓扑变化通告所有配置。

操作步骤

- 执行命令 **display sep interface verbose**，查看下级网络拓扑变化通告的配置信息。
- 在 OAM 管理视图下执行命令 **display this**，查看上级网络拓扑变化通告的配置信息。

----结束

3.10.6 维护 SEP

SEP 相关维护命令包括清除 SEP 的统计信息等。

清除 SEP 的统计信息

通过 **reset** 命令可以将 SEP 统计计数置 0，便于重新统计。

背景信息

注意

清除 SEP 的统计信息后，以前的信息将无法恢复，请务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 请在用户视图下执行命令 **reset sep interface** *interface-type interface-number* **statistics**，清除 SEP 统计信息。

----结束

调试 SEP

在 SEP 出现运行故障时，请在用户视图下执行 **debugging** 命令进行调试，查看调试信息，并定位故障的原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行命令 **undo debugging all** 关闭调试开关。

操作步骤

步骤 1 在用户视图下执行命令 **debugging sep** { **all** | **common** | **error** | **machine** | **message** | **pdu** [[**epa** | **lsa** | **nbr** | **preempt**] [**transmit** | **receive**]] } [**segment** *segment-id* | **interface** *interface-type interface-number*]

----结束

3.10.7 配置举例

配置举例结合组网需求、配置思路和数据准备例举了 SEP 的典型应用场景，并提供配置文件。

配置 SEP 封闭环示例

该组网的特点是多台二层交换设备组成双归链路接入上级网络，位于上级网络的两台边缘设备之间是直连的方式。此组网位于汇聚层，完成单播业务及组播业务的二层透传功能。通过在汇聚层运行 SEP 协议，实现冗余保护倒换。

组网需求

为了进行链路备份，提高网络可靠性，用户通常会使用冗余链路接入上层网络，但是使用冗余链路会在网络中产生环路。环路会造成报文在环路内不断的循环转发，最终导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为了阻塞冗余环路，并实现当环网上发生链路故障时，阻塞的冗余链路能够迅速恢复通信，可在环网上部署 SEP 协议。

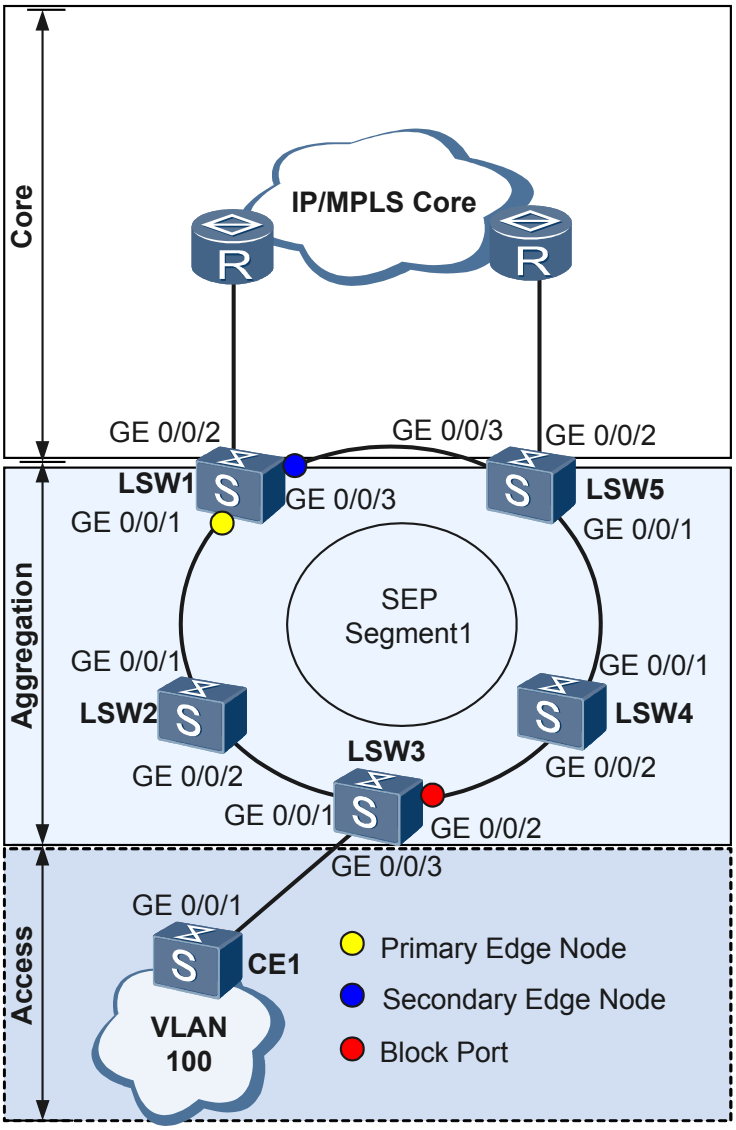
如图 3-68 所示，多台二层交换设备 LSW1 ～ LSW5 形成环形网络接入核心层网络。此种情况下：

在汇聚层运行 SEP 协议。

版权所有 © 华为技术有限公司

- 当环网上没有故障链路时，SEP 能够消除以太网冗余环路。
- 当环网上发生链路故障时，SEP 能够迅速恢复环网上各节点间通信通路。

图 3-68 SEP 封闭环组网图



配置思路

采用如下的思路配置 SEP 封闭环：

1. 配置 SEP 基本功能：
   a. 在 LSW1 ～ LSW5 上配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN。
   b. 将环网上所有设备加入 SEP 段并配置 LSW1 上接口 GE0/0/1 和 GE0/0/3 加入 SEP 段的端口角色。

版权所有 © 华为技术有限公司

c. 在端口角色为主边缘端口的设备上配置灵活指定阻塞端口的方式是依据端口优先级，优先阻塞优先级高的端口。

d. 配置加入 SEP 段的端口优先级。

配置 LSW3 上的端口 GE0/0/2 优先级最高，SEP 段上其他的端口均采用缺省优先级，确保阻塞优先级最高的端口。

e. 在端口角色为主边缘端口的设备上配置 SEP 抢占模式是延时抢占。

2. 配置 CE1、LSW1 ～ LSW5 二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- SEP 段 ID
- SEP 段控制 VLAN ID
- 加入 SEP 段的端口角色
- SEP 的抢占模式
- 端口的阻塞方式
- 加入 SEP 段的端口优先级

操作步骤

步骤 1 配置 SEP 基本功能

1. 配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 控制 VLAN

配置 LSW1。

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

配置 LSW2。

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

配置 LSW3。

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

配置 LSW4。

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
```

配置 LSW5。

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
```


版权所有 © 华为技术有限公司

```
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```

说明

- 控制 VLAN 的 ID 必须是没有被创建或使用的，但是在配置文件会自动显示创建普通 VLAN 的命令。
- 每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN，加入 SEP 段的接口下会自动显示命令 **port hybrid tagged vlan**。

2. 将环网上的设备加入 Segment1，并配置端口角色

说明

缺省情况下，二层端口上 STP 处于使能状态。再将端口加入 SEP 段之前，请先去使能 STP。

配置 LSW1 的接口 GE0/0/1 端口角色为主边缘端口、接口 GE0/0/3 端口角色为副边缘端口。

```
[LSW1] interface gigabitethernet 0/0/1
[LSW1-GigabitEthernet0/0/1] stp disable
[LSW1-GigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-GigabitEthernet0/0/1] quit
[LSW1] interface gigabitethernet 0/0/3
[LSW1-GigabitEthernet0/0/3] stp disable
[LSW1-GigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet0/0/3] quit
```

配置 LSW2。

```
[LSW2] interface gigabitethernet 0/0/1
[LSW2-GigabitEthernet0/0/1] stp disable
[LSW2-GigabitEthernet0/0/1] sep segment 1
[LSW2-GigabitEthernet0/0/1] quit
[LSW2] interface gigabitethernet 0/0/2
[LSW2-GigabitEthernet0/0/2] stp disable
[LSW2-GigabitEthernet0/0/2] sep segment 1
[LSW2-GigabitEthernet0/0/2] quit
```

配置 LSW3。

```
[LSW3] interface gigabitethernet 0/0/1
[LSW3-GigabitEthernet0/0/1] stp disable
[LSW3-GigabitEthernet0/0/1] sep segment 1
[LSW3-GigabitEthernet0/0/1] quit
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] stp disable
[LSW3-GigabitEthernet0/0/2] sep segment 1
[LSW3-GigabitEthernet0/0/2] quit
```

配置 LSW4。

```
[LSW4] interface gigabitethernet 0/0/1
[LSW4-GigabitEthernet0/0/1] stp disable
[LSW4-GigabitEthernet0/0/1] sep segment 1
[LSW4-GigabitEthernet0/0/1] quit
[LSW4] interface gigabitethernet 0/0/2
[LSW4-GigabitEthernet0/0/2] stp disable
[LSW4-GigabitEthernet0/0/2] sep segment 1
[LSW4-GigabitEthernet0/0/2] quit
```

配置 LSW5。

```
[LSW5] interface gigabitethernet 0/0/1
[LSW5-GigabitEthernet0/0/1] stp disable
[LSW5-GigabitEthernet0/0/1] sep segment 1
[LSW5-GigabitEthernet0/0/1] quit
[LSW5] interface gigabitethernet 0/0/3
[LSW5-GigabitEthernet0/0/3] stp disable
[LSW5-GigabitEthernet0/0/3] sep segment 1
[LSW5-GigabitEthernet0/0/3] quit
```

3. 配置灵活指定阻塞端口

版权所有 © 华为技术有限公司

在主边缘端口位于的设备 LSW1 上配置阻塞端口的方式为依据端口优先级，优先阻塞优先级高的端口。

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port optimal
```

4. 配置 LSW3 上的端口 GE0/0/2 优先级

```
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] sep segment 1 priority 128
[LSW3-GigabitEthernet0/0/2] quit
```

5. 配置抢占模式

在主边缘端口位于的设备 LSW1 上配置抢占模式为延时抢占。

```
[LSW1-sep-segment1] preempt delay 30
[LSW1-sep-segment1] quit
```

说明

- 延时抢占时间没有缺省值，用户必须通过本命令配置延时抢占时间。
- 当最后一个端口故障恢复后，边缘端口将不再收到故障通告报文。主边缘端口在 3 秒内没有收到故障通告报文，立即启动延时定时器。延时定时器超时后，SEP 段中的节点设备执行阻塞端口抢占。

  所以，在此配置示例中，需要先人为制造端口故障，再恢复端口故障，延时抢占才能成功执行。例如:

  在 LSW2 设备上对端口 GE0/0/2 执行 **shutdown** 命令，模拟端口故障。然后再在端口 GE0/0/2 执行 **undo shutdown** 命令，端口故障恢复。

步骤 2 配置 CE 和 LSW1 ～ LSW5 的二层转发功能

具体配置过程略。请参考本配置举例中的配置文件。

步骤 3 验证配置结果

- 对 LSW3 上的接口 GE0/0/1 执行命令 **shutdown** 模拟端口故障，在 LSW3 上执行命令 display sep interface 查看接口 GE0/0/2 能否从阻塞状态放开进入转发状态。

```
<LSW3> display sep interface gigabitethernet 0/0/2
SEP segment 1
-------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
-------------------------------------------------------------
GE0/0/2             common        up                  forwarding
```

----结束

配置文件

- LSW1 的配置文件

```
#
 sysname LSW1
#
 vlan batch 10 100 200
#
sep segment 1
 control-vlan 10
 block port optimal
 preempt delay 30
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 edge primary
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
```


版权所有 © 华为技术有限公司

```
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1 edge secondary
#
return
```

- LSW2 的配置文件

```
#
 sysname LSW2
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- LSW3 的配置文件

```
#
 sysname LSW3
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
 sep segment 1 priority 128
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- LSW4 的配置文件

```
#
 sysname LSW4
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- LSW5 的配置文件

```
#
 sysname LSW5
#
 vlan batch 10 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

配置 SEP 多环示例

该组网的特点是接入层和汇聚层均由多台二层交换设备构成环形网络，通过在接入层和汇聚层运行 SEP 协议，实现接入层和汇聚层冗余保护倒换。

组网需求

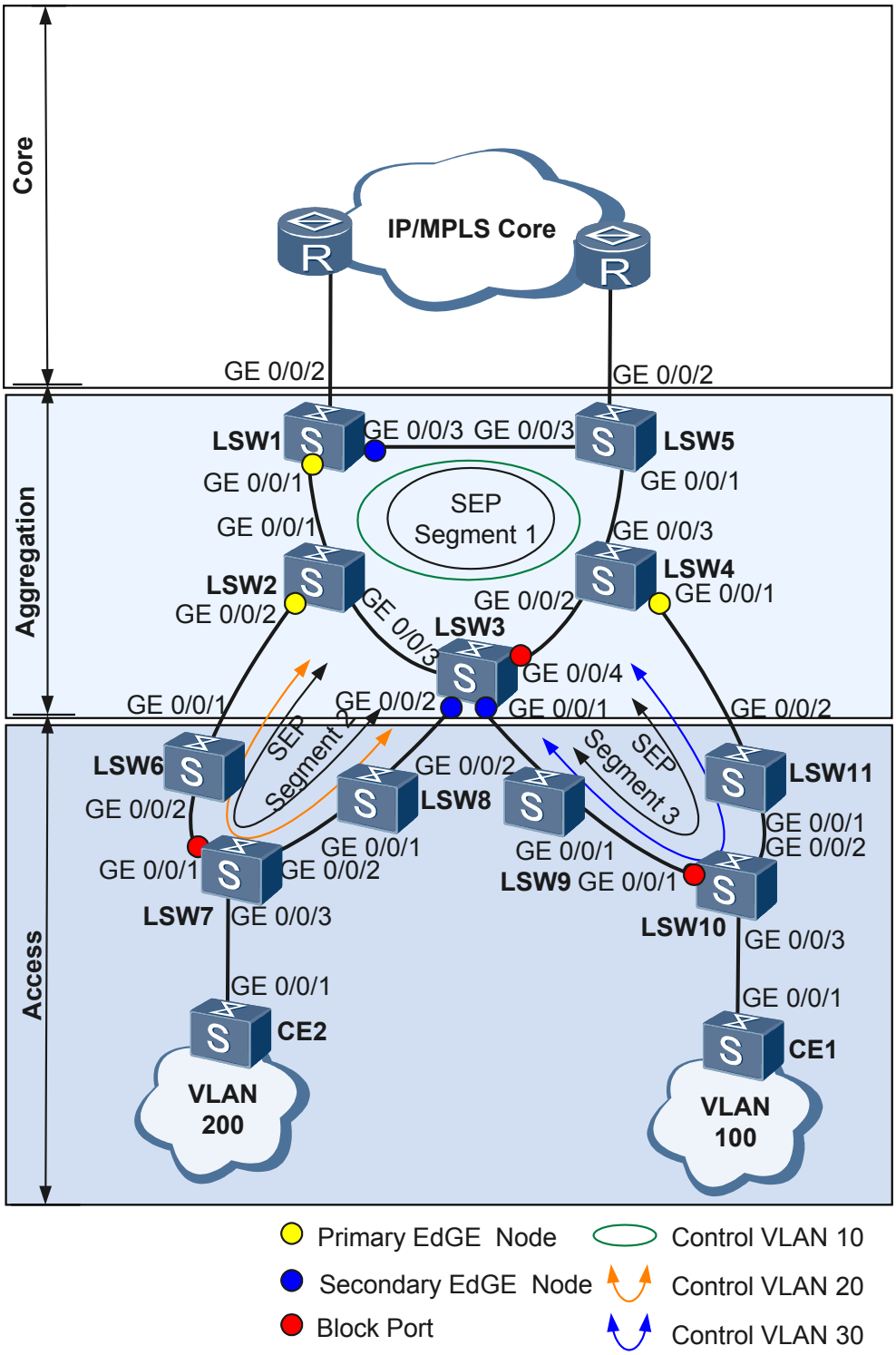
为了进行链路备份，提高网络可靠性，用户通常会使用冗余链路接入上层网络，但是使用冗余链路会在网络中产生环路。环路会造成报文在环路内不断的循环转发，最终导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为了阻塞冗余环路，并实现当环网上发生链路故障时，阻塞的冗余链路能够迅速恢复通信，可在环网上部署 SEP 协议。

如图 3-69 所示，接入层和汇聚层由多台二层交换设备构成环形网络接入核心层网络。此种情况下：

版权所有 © 华为技术有限公司

- 在接入层、汇聚层运行 SEP 协议。当环网上没有故障链路时，SEP 能够消除以太网冗余环路。当环网上发生链路故障时，SEP 能够迅速恢复环网上各节点间通信通路。

图 3-69 SEP 多环组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 SEP 多环：

1. 配置 SEP 基本功能：
   a. 配置 Segment ID 分别为 1、2、3 的 SEP 段，VLAN ID 分别为 10、20 和 30 的控制 VLAN。
      - 在 LSW1 ～ LSW5 上配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN。
      - 在 LSW2、LSW6 ～ LSW8 和 LSW3 上配置 Segment ID 为 2 的 SEP 段和 VLAN ID 为 20 的控制 VLAN。
      - 在 LSW3、LSW9 ～ LSW11 和 LSW4 上配置 Segment ID 为 3 的 SEP 段和 VLAN ID 为 30 的控制 VLAN。
   b. 将环网上的设备加入 SEP 段，并配置 SEP 段边缘设备上加入 SEP 段中的端口角色。
      - 将 LSW1 ～ LSW5 构成环网的接口加入 Segment ID 为 1 的 SEP 段，并配置 LSW1 上接口 GE0/0/1 和 GE0/0/3 加入 SEP 段的端口角色。
      - 将 LSW2 上接口 GE0/0/2，LSW6 ～ LSW8 上两个接口及 LSW3 上的接口 GE0/0/2 加入 Segment ID 为 2 的 SEP 段，并分别配置 LSW2 和 LSW3 上接口 GE0/0/2 加入 SEP 段的端口角色。
      - 将 LSW3 上接口 GE0/0/1，LSW9 ～ LSW11 上两个接口及 LSW4 上的接口 GE0/0/1 加入 Segment ID 为 3 的 SEP 段，并分别配置 LSW3 和 LSW4 上接口 GE0/0/1 加入 SEP 段的端口角色。
   c. 在端口角色为主边缘端口的设备上配置灵活指定阻塞端口。
      - Segment1 采用的阻塞端口方式是依据端口优先级，优先阻塞优先级高的端口。
      - Segment2 采用的阻塞端口方式是依据设备名+接口名。
      - Segment3 采用的阻塞端口方式是依据用户配置的跳数指定阻塞端口。
   d. 在端口角色为主边缘端口的设备上配置 SEP 抢占模式。

      Segment1 采用的抢占模式是延时抢占；Segment2 和 Segment3 采用的抢占模式是手工抢占。
   e. 在 SEP 段之间相交的设备 LSW2、LSW3 和 LSW4 上配置 SEP 拓扑变化通告。
2. 配置 CE1、CE2、LSW1 ～ LSW11 二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- SEP 段 ID
- SEP 段控制 VLAN ID
- 加入 SEP 段的端口角色
- SEP 的抢占模式
- 端口的阻塞方式
- 加入 SEP 段的端口优先级

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 SEP 基本功能

1. 配置 Segment ID 分别为 1、2、3 的 SEP 段，并按图 3-69 所示，配置 VLAN ID 为 10、20、30 的控制 VLAN

配置 LSW1。

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

配置 LSW2。

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
[LSW2] sep segment 2
[LSW2-sep-segment2] control-vlan 20
[LSW2-sep-segment2] protected-instance all
[LSW2-sep-segment2] quit
```

配置 LSW3。

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
[LSW3] sep segment 2
[LSW3-sep-segment2] control-vlan 20
[LSW3-sep-segment2] protected-instance all
[LSW3-sep-segment2] quit
[LSW3] sep segment 3
[LSW3-sep-segment3] control-vlan 30
[LSW3-sep-segment3] protected-instance all
[LSW3-sep-segment3] quit
```

配置 LSW4。

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
[LSW4] sep segment 3
[LSW4-sep-segment3] control-vlan 30
[LSW4-sep-segment3] protected-instance all
[LSW4-sep-segment3] quit
```

配置 LSW5。

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```

配置 LSW6 ～ LSW11。

LSW6 ～ LSW11 的配置与 LSW1 ～ LSW5 的配置类似，主要区别在于不同 SEP 段配置的控制 VLAN 不同。

具体配置过程略。请参见本示例的配置文件。

版权所有 © 华为技术有限公司

说明

- 控制 VLAN 的 ID 必须是没有被创建或使用的，但是在配置文件会自动显示创建普通 VLAN 的命令。
- 每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN，加入 SEP 段的接口下会自动显示命令 **port hybrid tagged vlan**。

2. 按图 3-69 所示，将环网上的设备加入指定 SEP 段，并设置端口角色

说明

缺省情况下，二层端口上 STP 处于使能状态。再将端口加入 SEP 段之前，请先去使能 STP。

配置 LSW1 的接口 GE0/0/1 端口角色为主边缘端口、接口 GE0/0/3 端口角色为副边缘端口。

```
[LSW1] interface gigabitethernet 0/0/1
[LSW1-GigabitEthernet0/0/1] stp disable
[LSW1-GigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-GigabitEthernet0/0/1] quit
[LSW1] interface gigabitethernet 0/0/3
[LSW1-GigabitEthernet0/0/3] stp disable
[LSW1-GigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet0/0/3] quit
```

配置 LSW2。

```
[LSW2] interface gigabitethernet 0/0/1
[LSW2-GigabitEthernet0/0/1] stp disable
[LSW2-GigabitEthernet0/0/1] sep segment 1
[LSW2-GigabitEthernet0/0/1] quit
[LSW2] interface gigabitethernet 0/0/3
[LSW2-GigabitEthernet0/0/3] stp disable
[LSW2-GigabitEthernet0/0/3] sep segment 1
[LSW2-GigabitEthernet0/0/3] quit
[LSW2] interface gigabitethernet 0/0/2
[LSW2-GigabitEthernet0/0/2] stp disable
[LSW2-GigabitEthernet0/0/2] sep segment 2 edge primary
[LSW2-GigabitEthernet0/0/2] quit
```

配置 LSW3。

```
[LSW3] interface gigabitethernet 0/0/3
[LSW3-GigabitEthernet0/0/3] stp disable
[LSW3-GigabitEthernet0/0/3] sep segment 1
[LSW3-GigabitEthernet0/0/3] quit
[LSW3] interface gigabitethernet 0/0/4
[LSW3-GigabitEthernet0/0/4] stp disable
[LSW3-GigabitEthernet0/0/4] sep segment 1
[LSW3-GigabitEthernet0/0/4] quit
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] stp disable
[LSW3-GigabitEthernet0/0/2] sep segment 2 edge secondary
[LSW3-GigabitEthernet0/0/2] quit
[LSW3] interface gigabitethernet 0/0/1
[LSW3-GigabitEthernet0/0/1] stp disable
[LSW3-GigabitEthernet0/0/1] sep segment 3 edge secondary
[LSW3-GigabitEthernet0/0/1] quit
```

配置 LSW4。

```
[LSW4] interface gigabitethernet 0/0/2
[LSW4-GigabitEthernet0/0/2] stp disable
[LSW4-GigabitEthernet0/0/2] sep segment 1
[LSW4-GigabitEthernet0/0/2] quit
[LSW4] interface gigabitethernet 0/0/3
[LSW4-GigabitEthernet0/0/3] stp disable
[LSW4-GigabitEthernet0/0/3] sep segment 1
[LSW4-GigabitEthernet0/0/3] quit
[LSW4] interface gigabitethernet 0/0/1
[LSW4-GigabitEthernet0/0/1] stp disable
[LSW4-GigabitEthernet0/0/1] sep segment 3 edge primary
[LSW4-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

配置 LSW5。

```
[LSW5] interface gigabitethernet 0/0/1
[LSW5-GigabitEthernet0/0/1] stp disable
[LSW5-GigabitEthernet0/0/1] sep segment 1
[LSW5-GigabitEthernet0/0/1] quit
[LSW5] interface gigabitethernet 0/0/3
[LSW5-GigabitEthernet0/0/3] stp disable
[LSW5-GigabitEthernet0/0/3] sep segment 1
[LSW5-GigabitEthernet0/0/3] quit
```

配置 LSW6 ～ LSW11。

LSW6 ～ LSW11 的配置与 LSW1 ～ LSW5 的配置类似，主要区别在于 LSW6 ～ LSW11 上加入 SEP 段的端口不需要指定端口角色。

具体配置过程略。请参见本示例的配置文件。

3. 配置灵活指定阻塞端口

在 Segment1 中主边缘端口位于的设备 LSW1 上配置阻塞端口的方式为依据端口优先级，优先阻塞优先级高的端口。

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port optimal
[LSW1-sep-segment1] quit
```

配置 LSW3 上的端口 GE0/0/4 优先级为 128，优先阻塞优先级高的端口。

```
[LSW3] interface gigabitethernet 0/0/4
[LSW3-GigabitEthernet0/0/4] sep segment 1 priority 128
[LSW3-GigabitEthernet0/0/4] quit
```

Segment1 中的其他端口均采用默认优先级。

在 Segment2 中主边缘端口位于的设备 LSW2 上配置阻塞端口的方式为依据设备名+接口名。

用户在配置前，可通过命令 **display sep topology** 查看当前环的拓扑信息，获取到拓扑中所有端口信息，然后指定设备名和端口名。

```
[LSW2] sep segment 2
[LSW2-sep-segment2] block port sysname LSW7 interface gigabitethernet 0/0/1
[LSW2-sep-segment2] quit
```

在 Segment3 中主边缘端口位于的设备 LSW4 上配置阻塞端口的方式为依据用户配置的跳数指定阻塞端口。

```
[LSW4] sep segment 3
[LSW4-sep-segment3] block port hop 5
[LSW4-sep-segment3] quit
```

说明

SEP 约定，主边缘端口的跳数为 1，主边缘端口的邻居端口的跳数为 2。跳数是沿着主边缘端口的下游邻居方向依次增加。

4. 配置抢占模式

在 Segment1 中主边缘端口位于的设备 LSW1 上配置抢占模式为延时抢占。

```
[LSW1] sep segment 1
[LSW1-sep-segment1] preempt delay 30
```


版权所有 © 华为技术有限公司

说明

- 延时抢占时间没有缺省值，用户必须通过本命令配置延时抢占时间。
- 当最后一个端口故障恢复后，边缘端口将不再收到故障通告报文。主边缘端口在 3 秒内没有收到故障通告报文，立即启动延时定时器。延时定时器超时后，SEP 段中的节点设备执行阻塞端口抢占。

  所以，在此配置示例中，需要先人为制造端口故障，再恢复端口故障，延时抢占才能成功执行。例如:

  在 LSW2 设备上对端口 GE0/0/2 执行 **shutdown** 命令，模拟端口故障。然后再在端口 GE0/0/2 执行 **undo shutdown** 命令，端口故障恢复。

在 Segment2 中主边缘端口位于的设备 LSW2 上配置抢占模式为手工抢占。

```
[LSW2] sep segment 2
[LSW2-sep-segment2] preempt manual
```

在 Segment3 中主边缘端口位于的设备 LSW4 上配置抢占模式为手工抢占。

```
[LSW4] sep segment 3
[LSW4-sep-segment3] preempt manual
```

5. 配置 SEP 拓扑变化通告

   # 在 Segment2 中配置 Segment2 的拓扑变化通告给 Segment1。

   # 配置 LSW2。

```
[LSW2] sep segment 2
[LSW2-sep-segment2] tc-notify segment 1
[LSW2-sep-segment2] quit
```

   # 配置 LSW3。

```
[LSW3] sep segment 2
[LSW3-sep-segment2] tc-notify segment 1
[LSW3-sep-segment2] quit
```

   # 在 Segment3 中配置 Segment3 的拓扑变化通告给 Segment1。

   # 配置 LSW3。

```
[LSW3] sep segment 3
[LSW3-sep-segment3] tc-notify segment 1
[LSW3-sep-segment3] quit
```

   # 配置 LSW4。

```
[LSW4] sep segment 3
[LSW4-sep-segment3] tc-notify segment 1
[LSW4-sep-segment3] quit
```

   说明

   SEP 拓扑通告用于下级网络向上级网络通告，部署于 SEP 段之间相交的设备上。

步骤 2 配置 CE 和 LSW1 ～ LSW11 的二层转发功能

具体配置过程略。请参考本配置举例中的配置文件。

步骤 3 验证配置结果

上述配置成功后，执行以下操作，验证配置结果。以 LSW1 为例。

- 对 LSW2 上的接口 GE0/0/1 执行命令 **shutdown** 模拟端口故障，在 LSW3 上执行命令 display sep interface 查看接口 GE0/0/4 能否从阻塞状态放开进入转发状态。

```
<LSW3> display sep interface gigabitethernet 0/0/4
SEP segment 1
------------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------------
GE0/0/4             common        up                  forwarding
```

----结束

版权所有 © 华为技术有限公司

配置文件

- LSW1 的配置文件

```
#
 sysname LSW1
#
 vlan batch 10 100 200 300
#
sep segment 1
 control-vlan 10
 block port optimal
 preempt delay 30
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1 edge primary
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid tagged vlan 100 200
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200 300
 stp disable
 sep segment 1 edge secondary
#
return
```

- LSW2 的配置文件

```
#
 sysname LSW2
#
 vlan batch 10 20 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 20
 block port sysname LSW7 interface GigabitEthernet0/0/1
 tc-notify segment 1
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2 edge primary
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```

- LSW3 的配置文件

```
#
 sysname LSW3
#
 vlan batch 10 20 30 100 200
#
```


版权所有 © 华为技术有限公司

```
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 20
 tc-notify segment 1
 protected-instance 0 to 48
sep segment 3
 control-vlan 30
 tc-notify segment 1
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3 edge secondary
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2 edge secondary
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/4
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
 sep segment 1 priority 128
#
return
```

- LSW4 的配置文件

```
#
 sysname LSW4
#
 vlan batch 10 30 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 30
 protected-instance 0 to 48
sep segment 3
 control-vlan 30
 block port hop 5
 tc-notify segment 1
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3 edge primary
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```


版权所有 © 华为技术有限公司

- LSW5 的配置文件

```
#
 sysname LSW5
#
 vlan batch 10 100 200 300
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid tagged vlan 100 200
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200 300
 stp disable
 sep segment 1
#
return
```

- LSW6 的配置文件

```
#
 sysname LSW6
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
return
```

- LSW7 的配置文件

```
#
 sysname LSW7
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 200
#
return
```

- LSW8 的配置文件

```
#
 sysname LSW8
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
return
```

- LSW9 的配置文件

```
#
 sysname LSW9
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
return
```

- LSW10 的配置文件

```
#
 sysname LSW10
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- LSW11 的配置文件

```
#
 sysname LSW11
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 vlan batch 200
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
#
return
```

配置 SEP 混合环示例

本示例中的组网特点是接入层与汇聚层相交的两台设备不支持 SEP 协议，通过在接入层部署 SEP 协议实现冗余保护倒换，并在 SEP 段的边缘设备上部署网络拓扑变化通告，实现上级网络及时了解下级网络的拓扑变化。

组网需求

为了进行链路备份，提高网络可靠性，用户通常会使用冗余链路接入上层网络，但是使用冗余链路会在网络中产生环路。环路会造成报文在环路内不断的循环转发，最终导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为了阻塞冗余环路，并实现当环网上发生链路故障时，阻塞的冗余链路能够迅速恢复通信，可在环网上部署 SEP 协议。

版权所有 © 华为技术有限公司

说明

本示例汇聚层以运行 MSTP 协议为例。

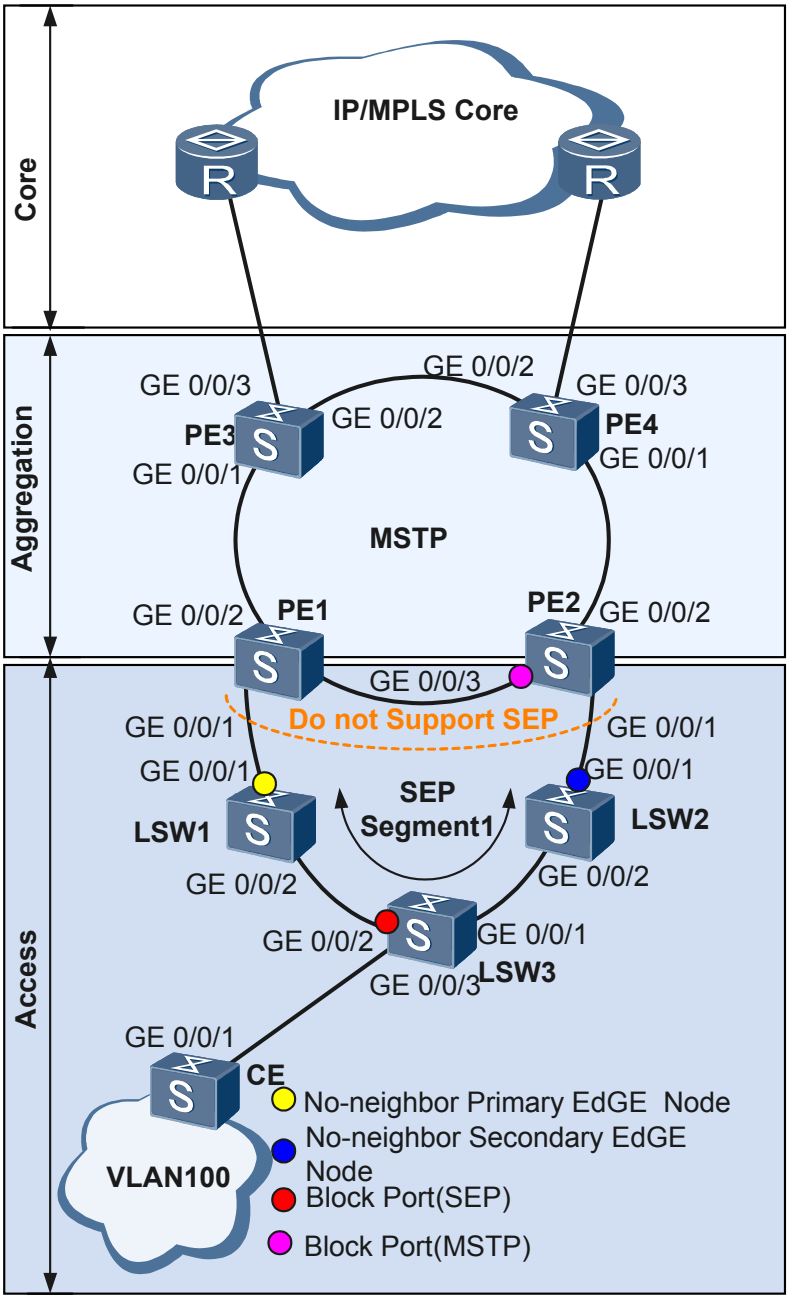
如图 3-70 所示，接入层由多台二层交换设备组成、汇聚层由多台三层设备组成环形网络接入核心层。汇聚层已经部署 MSTP 协议以消除冗余链路，此种情况下，在接入层运行 SEP 协议。

- 当环网上没有故障链路时，SEP 能够消除以太网冗余环路。
- 当环网上发生链路故障时，SEP 能够迅速恢复本环网上各节点间通信通路。
- 在 SEP 段的边缘设备上部署网络拓扑变化通告，实现上级网络及时了解下级网络的拓扑变化。

  当上级网络收到下游网络拓扑变化的消息后，会在本网络内发送 TC 报文，通知本网络内的所有设备清除 MAC 地址，重新学习下游网络拓扑变化后的 MAC 地址，从而保证用户流量不中断。

版权所有 © 华为技术有限公司

图 3-70 SEP 混合环组网图



配置思路

采用如下的思路配置 SEP 混合环：

1. 配置 SEP 基本功能：
   a. 在 LSW1 ～ LSW3 上配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN。
   b. 将设备 LSW1 ～ LSW3 加入 SEP 段，并配置 SEP 段边缘设备 LSW1 和 LSW2 上加入 SEP 段中的端口角色。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

由于 PE1 和 PE2 设备不支持 SEP 协议，故在 LSW1 和 LSW2 设备上选择的端口角色必须是无邻居边缘端口。

c. 在端口角色为无邻居主边缘端口的设备上配置灵活指定阻塞端口方式为阻塞 SEP 段中间位置的端口。

d. 配置 SEP 抢占模式为手工抢占。

e. 配置 SEP 拓扑变化通告，将 SEP 段拓扑变化通知上级使用 STP 协议的网络。

2. 配置 MSTP 基本功能：

a. 将 PE1 ～ PE4 配置到一个域内，域名为 RG1。

b. 在 PE1 ～ PE4 创建 VLAN，并将 STP 环上接口加入 VLAN。

c. 配置 PE3 为根桥、PE4 为备份根桥。

3. 配置 CE1、LSW1 ～ LSW3 二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- SEP 段 ID
- SEP 段控制 VLAN ID
- 加入 SEP 段的端口角色
- SEP 的抢占模式
- 端口的阻塞方式
- STP 域名、实例、优先级

操作步骤

步骤 1 配置 SEP 基本功能

1. 配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN

配置 LSW1。

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

配置 LSW2。

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

配置 LSW3。

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```


版权所有 © 华为技术有限公司

说明

- 控制 VLAN 的 ID 必须是没有被创建或使用的，但是在配置文件会自动显示创建普通 VLAN 的命令。
- 每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN，加入 SEP 段的接口下会自动显示命令 **port hybrid tagged vlan**。

2. 将 LSW1 ～ LSW3 加入 Segmengt 1，并设置端口角色

   # 配置 LSW1。

```
[LSW1] interface gigabitethernet 0/0/1
[LSW1-GigabitEthernet0/0/1] sep segment 1 edge no-neighbor primary
[LSW1-GigabitEthernet0/0/1] quit
[LSW1] interface gigabitethernet 0/0/2
[LSW1-GigabitEthernet0/0/2] stp disable
[LSW1-GigabitEthernet0/0/2] sep segment 1
[LSW1-GigabitEthernet0/0/2] quit
```

   # 配置 LSW2。

```
[LSW2] interface gigabitethernet 0/0/1
[LSW2-GigabitEthernet0/0/1] sep segment 1 edge no-neighbor secondary
[LSW2-GigabitEthernet0/0/1] quit
[LSW2] interface gigabitethernet 0/0/2
[LSW2-GigabitEthernet0/0/2] stp disable
[LSW2-GigabitEthernet0/0/2] sep segment 1
[LSW2-GigabitEthernet0/0/2] quit
```

   # 配置 LSW3。

```
[LSW3] interface gigabitethernet 0/0/1
[LSW3-GigabitEthernet0/0/1] stp disable
[LSW3-GigabitEthernet0/0/1] sep segment 1
[LSW3-GigabitEthernet0/0/1] quit
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] stp disable
[LSW3-GigabitEthernet0/0/2] sep segment 1
[LSW3-GigabitEthernet0/0/2] quit
```

3. 配置灵活指定阻塞端口

   # 在 Segment1 中无邻居主边缘端口位于的设备 LSW1 上配置阻塞端口的方式为依据处于 SEP 段中间位置的端口为阻塞端口。

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port middle
```

4. 配置抢占模式

   # 在 Segment1 中主边缘端口位于的设备 LSW1 上配置抢占模式为手工抢占。

```
[LSW1-sep-segment1] preempt maunal
```

5. 配置 SEP 拓扑变化通告

   # 在 Segment1 中配置 Segment1 的拓扑变化通告给 STP 协议。

   # 配置 LSW1。

```
[LSW1-sep-segment1] tc-notify stp
[LSW1-sep-segment1] quit
```

   # 配置 LSW2。

```
[LSW2] sep segment 1
[LSW2-sep-segment1] tc-notify stp
[LSW2-sep-segment1] quit
```

上述配置成功后，执行以下操作，验证配置结果。以 LSW1 为例。

- 在 LSW1 上执行命令 display sep topology，查看 SEP 段的拓扑信息。

  从拓扑显示信息中可以看出设备 LSW3 上的端口 GE0/0/2 的端口转发状态为 **discarding**，其余端口的转发状态均为 **forwarding**

版权所有 © 华为技术有限公司

```
<LSW1> display sep topology
SEP segment 1
--------------------------------------------------------------------
System Name      Port Name          Port Role       Port Status
--------------------------------------------------------------------
LSW1             GE0/0/1            *primary        forwarding
LSW1             GE0/0/2            common          forwarding
LSW3             GE0/0/1            common          forwarding
LSW3             GE0/0/2            common          discarding
LSW2             GE0/0/1            common          forwarding
LSW2             GE0/0/2            *secondary      forwarding
```

步骤 2 配置 MSTP 基本功能

1. 配置 MST 域。

   # 配置 PE1。

   ```
   <Quidway> system-view
   [Quidway] sysname PE1
   [PE1] stp region-configuration
   [PE1-mst-region] region-name RG1
   [PE1-mst-region] active region-configuration
   [PE1-mst-region] quit
   ```

   # 配置 PE2。

   ```
   <Quidway> system-view
   [Quidway] sysname PE2
   [PE2] stp region-configuration
   [PE2-mst-region] region-name RG1
   [PE2-mst-region] active region-configuration
   [PE2-mst-region] quit
   ```

   # 配置 PE3。

   ```
   <Quidway> system-view
   [Quidway] sysname PE3
   [PE3] stp region-configuration
   [PE3-mst-region] region-name RG1
   [PE3-mst-region] active region-configuration
   [PE3-mst-region] quit
   ```

   # 配置 PE4。

   ```
   <Quidway> system-view
   [Quidway] sysname PE4
   [PE4] stp region-configuration
   [PE4-mst-region] region-name RG1
   [PE4-mst-region] active region-configuration
   [PE4-mst-region] quit
   ```

2. 创建 VLAN，并将环上接口加入 VLAN。

   # 在 PE1 上创建 VLAN100，并将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN100 中。

   ```
   [PE1] vlan 100
   [PE1-vlan100] quit
   [PE1] interface gigabitethernet 0/0/1
   [PE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100
   [PE1-GigabitEthernet0/0/1] quit
   [PE1] interface gigabitethernet 0/0/2
   [PE1-GigabitEthernet0/0/2] port hybrid tagged vlan 100
   [PE1-GigabitEthernet0/0/2] quit
   [PE1] interface gigabitethernet 0/0/3
   [PE1-GigabitEthernet0/0/3] port hybrid tagged vlan 100
   [PE1-GigabitEthernet0/0/3] quit
   ```

   # 分别在 PE2、PE3 和 PE4 上创建 VLAN100，并分别将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN100 中。

   PE2、PE3、PE4 与 PE1 的配置相同，具体配置过程略。请参见本示例的配置文件。

版权所有 © 华为技术有限公司

3. 启动 MSTP。

   # 配置 PE1。

   ```
   [PE1] stp enable
   ```

   # 配置 PE2。

   ```
   [PE2] stp enable
   ```

   # 配置 PE3。

   ```
   [PE3] stp enable
   ```

   # 配置 PE4。

   ```
   [PE4] stp enable
   ```

4. 配置 PE3 为根桥、PE4 为备份根桥。

   # 配置 PE3 在 MSTI0 中的优先级为 0，保证 PE3 作为根桥。

   ```
   [PE3] stp instance 0 priority 0
   [PE3] stp root primary
   ```

   # 配置 PE4 在 MSTI0 中的优先级为 4096，保证 PE4 作为备份根桥。

   ```
   [PE4] stp instance 0 priority 4096
   [PE4] stp root secondary
   ```

上述配置完成后，在 PE2 上执行命令 **display stp brief**，查看端口 GE0/0/3 是否为阻塞端口。

```
<PE4> display stp brief
MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/3        ALTE  DISCARDING      NONE
```

步骤 3 配置 CE 和 LSW1 ～ LSW3 的二层转发功能

具体配置过程略。请参考本示例中的配置文件。

步骤 4 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 LSW1 为例。

- 对 LSW2 上的接口 GE0/0/1 执行命令 **shutdown** 模拟端口故障，在 LSW3 上执行命令 display sep interface 查看接口 GE0/0/2 能否从阻塞状态放开进入转发状态。

  ```
  <LSW3> display sep interface gigabitethernet 0/0/2
  SEP segment 1
  ------------------------------------------------------------------
  Interface           Port Role     Neighbor Status     Port Status
  ------------------------------------------------------------------
  GE0/0/2             common        up                  forwarding
  ```

----结束

配置文件

- LSW1 的配置文件

  ```
  #
   sysname LSW1
  #
   vlan batch 10 100
  #
  sep segment 1
   control-vlan 10
   block port middle
   tc-notify stp
   protected-instance 0 to 48
  ```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 no-neighbor edge primary
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- LSW2 的配置文件

```
#
 sysname LSW2
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 tc-notify stp
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 no-neighbor edge secondary
#
return
```

- LSW3 的配置文件

```
#
 sysname LSW3
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan vlan 100
#
return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 100
#
 stp enable
#
```


版权所有 © 华为技术有限公司

```
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 100
#
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- PE3 的配置文件

```
#
 sysname PE3
#
 vlan batch 100 200
#
 stp instance 0 root primary
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
return
```

- PE4 的配置文件

```
#
 sysname PE4
#
 vlan batch 100 200
```


版权所有 © 华为技术有限公司

```
#
 stp instance 0 root secondary
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

配置 SEP+RRPP 混合环组网示例（下级网络拓扑变化通告）

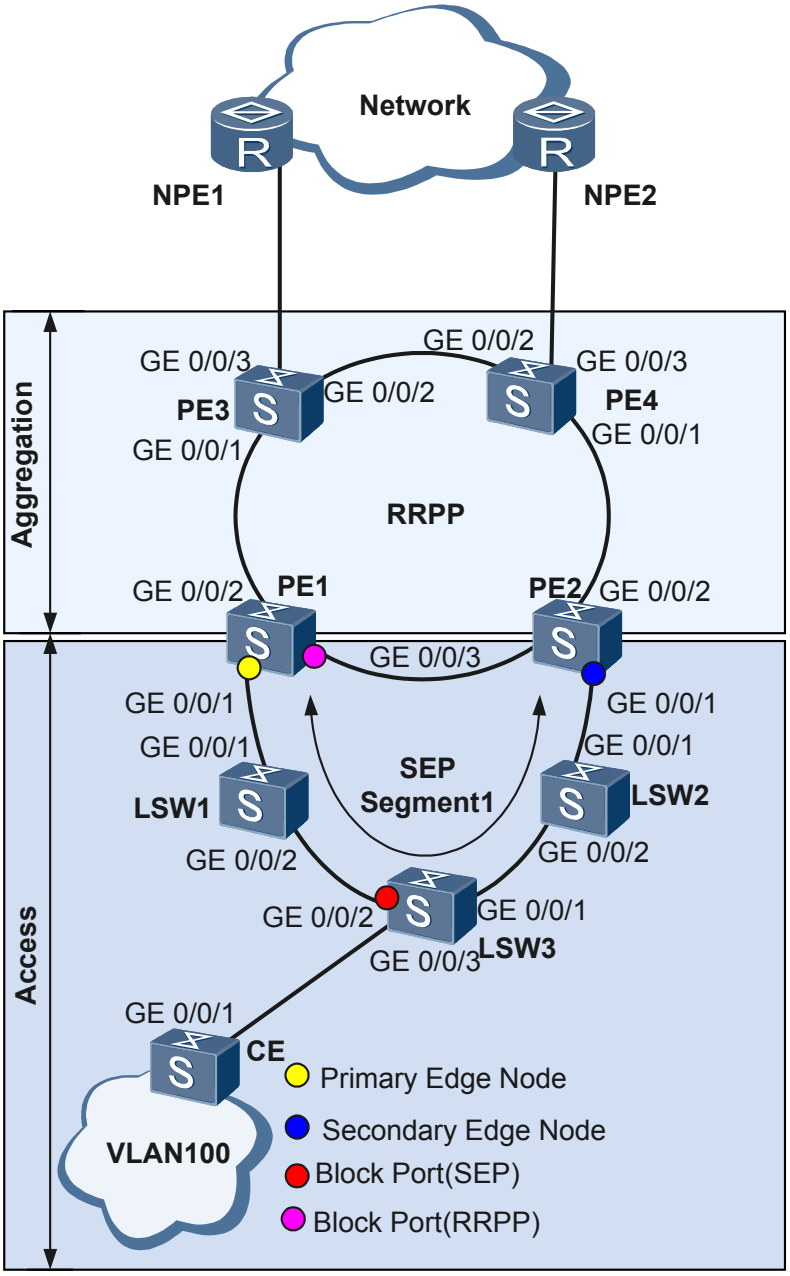
本示例中的组网特点是通过在接入层部署 SEP 协议实现冗余保护倒换，并在 SEP 段的边缘设备上部署网络拓扑变化通告，实现上级网络及时了解下级网络的拓扑变化。

组网需求

为了进行链路备份，提高网络可靠性，用户通常会使用冗余链路接入上层网络，但是使用冗余链路会在网络中产生环路。环路会造成报文在环路内不断的循环转发，最终导致广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为了阻塞冗余环路，并实现当环网上发生链路故障时，阻塞的冗余链路能够迅速恢复通信，可在环网上部署 SEP 协议。

版权所有 © 华为技术有限公司

图 3-71 SEP+RRPP 混合组网图



如图 3-71 所示，接入层、汇聚层由多台二层交换设备组成环形网络接入核心层，汇聚层已经部署 RRPP 协议以消除冗余链路，此种情况下，在接入层运行 SEP 协议：

- 当环网上没有故障链路时，SEP 能够消除以太网冗余环路。
- 当环网上发生链路故障时，SEP 能够迅速恢复本环网上各节点间通信通路。
- 在 SEP 段的边缘设备上部署网络拓扑变化通告，实现上级网络及时了解下级网络的拓扑变化。

  当上级网络收到下游网络拓扑变化的消息后，会在本网络内发送 TC 报文，通知本网络内的所有设备清除 MAC 地址，重新学习下游网络拓扑变化后的 MAC 地址，从而保证用户流量不中断。

华为专有和保密信息
版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 SEP+RRPP 混合环：

1. 配置 SEP 基本功能：
   a. 在 PE1、PE2 和 LSW1 ～ LSW3 上配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN。
   b. 将设备 PE1、PE2 和 LSW1 ～ LSW3 加入 SEP 段，并配置 SEP 段边缘设备 PE1 和 PE2 上加入 SEP 段中的端口角色。
   c. 在端口角色为主边缘端口的设备上配置端口阻塞方式，灵活指定阻塞端口。
   d. 配置 SEP 抢占模式，确保故障恢复时用户指定的阻塞端口生效。
   e. 配置 SEP 拓扑变化通告，将 SEP 段拓扑变化通知上级使用 RRPP 协议的网络。
2. 配置 RRPP 基本功能。
   a. 将 PE1 ～ PE4 配置到一个域内，域 ID 为 1。在 PE1 ～ PE4 上创建控制 VLAN，ID 为 5，配置保护 VLAN。
   b. 配置 PE1 为主环的主节点，PE2 ～ PE4 为主环的传输节点，并配置主环节点的主端口和副端口。
   c. 在 PE1 ～ PE4 创建 VLAN，并将 RRPP 环上接口加入 VLAN。
3. 配置 CE、LSW1 ～ LSW3、PE1 ～ PE4 的二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- SEP 段 ID、控制 VLAN ID、加入 SEP 段的端口角色、端口阻塞方式、SEP 抢占模式。
- RRPP 域 ID、环 ID、控制 VLAN ID。

操作步骤

步骤 1 配置 SEP 基本功能

1. 配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN

   # 配置 PE1。

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1] sep segment 1
[PE1-sep-segment1] control-vlan 10
[PE1-sep-segment1] protected-instance all
[PE1-sep-segment1] quit
```

   # 配置 PE2。

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] sep segment 1
[PE2-sep-segment1] control-vlan 10
[PE2-sep-segment1] protected-instance all
[PE2-sep-segment1] quit
```

   # 配置 LSW1。

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
```


版权所有 © 华为技术有限公司

```
[LSW1-sep-segment1] quit
```

配置 LSW2。

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

配置 LSW3。

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

2. 将 PE1、PE2 和 LSW1 ～ LSW3 加入 Segmengt 1，并设置端口角色

说明

缺省情况下，二层端口上 STP 处于使能状态。在将端口加入 SEP 段之前，请先去使能 STP。

配置 PE1。

```
[PE1] interface gigabitethernet 0/0/1
[PE1-GigabitEthernet0/0/1] stp disable
[PE1-GigabitEthernet0/0/1] sep segment 1 edge primary
[PE1-GigabitEthernet0/0/1] quit
```

配置 LSW1。

```
[LSW1] interface gigabitethernet 0/0/1
[LSW1-GigabitEthernet0/0/1] stp disable
[LSW1-GigabitEthernet0/0/1] sep segment 1
[LSW1-GigabitEthernet0/0/1] quit
[LSW1] interface gigabitethernet 0/0/2
[LSW1-GigabitEthernet0/0/2] stp disable
[LSW1-GigabitEthernet0/0/2] sep segment 1
[LSW1-GigabitEthernet0/0/2] quit
```

配置 LSW2。

```
[LSW2] interface gigabitethernet 0/0/1
[LSW2-GigabitEthernet0/0/1] stp disable
[LSW2-GigabitEthernet0/0/1] sep segment 1
[LSW2-GigabitEthernet0/0/1] quit
[LSW2] interface gigabitethernet 0/0/2
[LSW2-GigabitEthernet0/0/2] stp disable
[LSW2-GigabitEthernet0/0/2] sep segment 1
[LSW2-GigabitEthernet0/0/2] quit
```

配置 LSW3。

```
[LSW3] interface gigabitethernet 0/0/1
[LSW3-GigabitEthernet0/0/1] stp disable
[LSW3-GigabitEthernet0/0/1] sep segment 1
[LSW3-GigabitEthernet0/0/1] quit
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] stp disable
[LSW3-GigabitEthernet0/0/2] sep segment 1
[LSW3-GigabitEthernet0/0/2] quit
```

配置 PE2。

```
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] stp disable
[PE2-GigabitEthernet0/0/1] sep segment 1 edge secondary
[PE2-GigabitEthernet0/0/1] quit
```

上述配置成功后，在 PE1 上执行命令 **display sep topology**，查看 SEP 段的拓扑信息，可以看到阻塞端口是最后完成邻居协商的链路两端的其中一个端口。

```
[PE1] display sep topology
```


版权所有 © 华为技术有限公司

```
SEP segment 1
--------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------
PE1                  GE0/0/1          primary         forwarding
LSW1                 GE0/0/1          common          forwarding
LSW1                 GE0/0/2          common          forwarding
LSW3                 GE0/0/2          common          forwarding
LSW3                 GE0/0/1          common          forwarding
LSW2                 GE0/0/2          common          forwarding
LSW2                 GE0/0/1          common          forwarding
PE2                  GE0/0/1          secondary       discarding
```

3. 灵活指定阻塞端口

   # 在 Segment1 中主边缘端口位于的设备 PE1 上配置阻塞端口的方式为依据处于 SEP 段中间位置的端口为阻塞端口。

```
[PE1] sep segment 1
[PE1-sep-segment1] block port middle
```

4. 配置抢占模式

   # 在 Segment1 中主边缘端口位于的设备 PE1 上配置抢占模式为手工抢占。

```
[PE1-sep-segment1] preempt maunal
```

5. 配置 SEP 拓扑变化通告

   # 在 Segment1 中配置 Segment1 的拓扑变化通告给 RRPP 协议。

   # 配置 PE1。

```
[PE1-sep-segment1] tc-notify rrpp
[PE1-sep-segment1] quit
```

   # 配置 PE2。

```
[PE2] sep segment 1
[PE2-sep-segment1] tc-notify rrpp
[PE2-sep-segment1] quit
```

上述配置成功后，执行以下操作，验证配置结果。以 PE1 为例。

- 在 PE1 上执行命令 **display sep topology**，查看 SEP 段的拓扑信息。

  从拓扑显示信息中可以看出设备 LSW3 上的端口 GE0/0/2 的端口转发状态为 **discarding**，其余端口的转发状态均为 **forwarding**

```
[PE1] display sep topology
SEP segment 1
--------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------
PE1                  GE0/0/1          primary         forwarding
LSW1                 GE0/0/1          common          forwarding
LSW1                 GE0/0/2          common          forwarding
LSW3                 GE0/0/2          common          discarding
LSW3                 GE0/0/1          common          forwarding
LSW2                 GE0/0/2          common          forwarding
LSW2                 GE0/0/1          common          forwarding
PE2                  GE0/0/1          secondary       forwarding
```

- 在 PE1 上执行命令 **display sep interface verbose**，查看本设备上加入 SEP 段的接口详细信息。

```
[PE1] display sep interface verbose
SEP segment 1
Control-vlan             :10
Preempt Delay Timer      :0
TC-Notify Propagate to :rrpp
--------------------------------------------------------------
Interface              :GE0/0/1
Port Role              :Config = primary / Active =  primary
Port Priority          :64
```


版权所有 © 华为技术有限公司

```
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :LSW1 - GE0/0/1 (00e0-0829-7c00.0000)
NBR TLV             rx :2124             tx :2126
LSP INFO TLV        rx :2939             tx :135
LSP ACK TLV         rx :113              tx :768
PREEMPT REQ TLV     rx :0                tx :3
PREEMPT ACK TLV     rx :3                tx :0
TC Notify           rx :5                tx :3
EPA                 rx :363              tx :397
```

步骤 2 配置 RRPP 基本功能

1. 将 PE1 ～ PE4 配置到一个域内，域 ID 为 1。在 PE1 ～ PE4 上创建控制 VLAN，ID 为 100，配置保护 VLAN。

   # 配置 PE1。

   ```
   <Quidway> system-view
   [Quidway] sysname PE1
   [PE1] stp region-configuration
   [PE1-mst-region] instance 1 vlan 5 6 100
   [PE1-mst-region] active region-configuration
   [PE1-mst-region] quit
   [PE1] rrpp domain 1
   [PE1-rrpp-domain-region1] control-vlan 5
   [PE1-rrpp-domain-region1] protected-vlan reference-instance 1
   ```

   # 配置 PE2。

   ```
   <Quidway> system-view
   [Quidway] sysname PE2
   [PE2] stp region-configuration
   [PE2-mst-region] instance 1 vlan 5 6 100
   [PE2-mst-region] active region-configuration
   [PE2-mst-region] quit
   [PE2] rrpp domain 1
   [PE2-rrpp-domain-region1] control-vlan 5
   [PE2-rrpp-domain-region1] protected-vlan reference-instance 1
   ```

   # 配置 PE3。

   ```
   <Quidway> system-view
   [Quidway] sysname PE3
   [PE3] stp region-configuration
   [PE3-mst-region] instance 1 vlan 5 6 100
   [PE3-mst-region] active region-configuration
   [PE3-mst-region] quit
   [PE3] rrpp domain 1
   [PE3-rrpp-domain-region1] control-vlan 5
   [PE3-rrpp-domain-region1] protected-vlan reference-instance 1
   ```

   # 配置 PE4。

   ```
   <Quidway> system-view
   [Quidway] sysname PE4
   [PE4] stp region-configuration
   [PE4-mst-region] instance 1 vlan 5 6 100
   [PE4-mst-region] active region-configuration
   [PE4-mst-region] quit
   [PE4] rrpp domain 1
   [PE4-rrpp-domain-region1] control-vlan 5
   [PE4-rrpp-domain-region1] protected-vlan reference-instance 1
   ```

2. 创建 VLAN，并将环上接口加入 VLAN。

   # 在 PE1 上创建 VLAN100，并将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN100 中。

   ```
   [PE1] vlan 100
   [PE1-vlan100] quit
   [PE1] interface gigabitethernet 0/0/1
   [PE1-GigabitEthernet0/0/1] stp disable
   [PE1-GigabitEthernet0/0/1] port link-type trunk
   ```


版权所有 © 华为技术有限公司

```
[PE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[PE1-GigabitEthernet0/0/1] quit
[PE1] interface gigabitethernet 0/0/2
[PE1-GigabitEthernet0/0/2] stp disable
[PE1-GigabitEthernet0/0/2] port link-type trunk
[PE1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[PE1-GigabitEthernet0/0/2] quit
[PE1] interface gigabitethernet 0/0/3
[PE1-GigabitEthernet0/0/3] stp disable
[PE1-GigabitEthernet0/0/3] port link-type trunk
[PE1-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[PE1-GigabitEthernet0/0/3] quit
```

在 PE2 上创建 VLAN100，并将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN100 中。

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] stp disable
[PE2-GigabitEthernet0/0/1] port link-type trunk
[PE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[PE2-GigabitEthernet0/0/1] quit
[PE2] interface gigabitethernet 0/0/2
[PE2-GigabitEthernet0/0/2] stp disable
[PE2-GigabitEthernet0/0/2] port link-type trunk
[PE2-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[PE2-GigabitEthernet0/0/2] quit
[PE2] interface gigabitethernet 0/0/3
[PE2-GigabitEthernet0/0/3] stp disable
[PE2-GigabitEthernet0/0/3] port link-type trunk
[PE2-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[PE2-GigabitEthernet0/0/3] quit
```

在 PE3 上创建 VLAN100，并将接口 GE0/0/1 和 GE0/0/2 加入 VLAN100 中。

```
[PE3] vlan 100
[PE3-vlan100] quit
[PE3] interface gigabitethernet 0/0/1
[PE3-GigabitEthernet0/0/1] stp disable
[PE3-GigabitEthernet0/0/1] port link-type trunk
[PE3-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[PE3-GigabitEthernet0/0/1] quit
[PE3] interface gigabitethernet 0/0/2
[PE3-GigabitEthernet0/0/2] stp disable
[PE3-GigabitEthernet0/0/2] port link-type trunk
[PE3-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[PE3-GigabitEthernet0/0/2] quit
```

在 PE4 上创建 VLAN100，并将接口 GE0/0/1 和 GE0/0/2 加入 VLAN100 中。

```
[PE4] vlan 100
[PE4-vlan100] quit
[PE4] interface gigabitethernet 0/0/1
[PE4-GigabitEthernet0/0/1] stp disable
[PE4-GigabitEthernet0/0/1] port link-type trunk
[PE4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[PE4-GigabitEthernet0/0/1] quit
[PE4] interface gigabitethernet 0/0/2
[PE4-GigabitEthernet0/0/2] stp disable
[PE4-GigabitEthernet0/0/2] port link-type trunk
[PE4-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[PE4-GigabitEthernet0/0/2] quit
```

3. 配置 PE1 为主环的主节点，PE2 ～ PE4 为主环的传输节点，并配置主环节点的主端口和副端口。

   # 配置 PE1。

```
[PE1] rrpp domain 1
[PE1-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitGigabitEthernet0/0/2
secondary-port gigabitGigabitEthernet0/0/3 level 0
[PE1-rrpp-domain-region1] ring 1 enable
```


版权所有 © 华为技术有限公司

配置 PE2。

```
[PE2] rrpp domain 1
[PE2-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitGigabitEthernet0/0/2
secondary-port gigabitGigabitEthernet0/0/3 level 0
[PE2-rrpp-domain-region1] ring 1 enable
```

配置 PE3。

```
[PE3] rrpp domain 1
[PE3-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitGigabitEthernet0/0/1
secondary-port gigabitGigabitEthernet0/0/2 level 0
[PE3-rrpp-domain-region1] ring 1 enable
```

配置 PE4。

```
[PE4] rrpp domain 1
[PE4-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitGigabitEthernet0/0/1
secondary-port gigabitGigabitEthernet0/0/2 level 0
[PE4-rrpp-domain-region1] ring 1 enable
```

4. 启动 RRPP。

配置 PE1。

```
[PE1] rrpp enable
```

配置 PE2。

```
[PE2] rrpp enable
```

配置 PE3。

```
[PE3] rrpp enable
```

配置 PE4。

```
[PE4] rrpp enable
```

上述配置完成后，在设备上执行命令 **display rrpp brief** 或者 **display rrpp verbose domain**，以 PE1 为例。

```
[PE1] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      M     GigabitEthernet0/0/2     GigabitEthernet0/0/3    Yes
```

可以看到 PE1 上使能了 RRPP 协议。在域 1 的控制 VLAN 为 VLAN5，保护 VLAN 为 Instance1，PE1 为环 1 的主节点，主端口为 GE0/0/2，副端口为 GE0/0/3。

```
[PE1] display rrpp verbose domain 1
Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                          Is Active: Yes
Primary port   : GigabitEthernet0/0/2            Port status: UP
Secondary port : GigabitEthernet0/0/3            Port status: BLOCKED
```


版权所有 © 华为技术有限公司

可以看到域 1 的控制 VLAN 为 VLAN5，保护 VLAN 为 Instance1。PE1 在域 1 中是主节点，节点状态是 Complete，主端口为 GE0/0/2，副端口为 GE0/0/3。

步骤 3 配置 CE、LSW1 ～ LSW3、PE1 ～ PE4 的二层转发功能

具体配置过程略。请参考本示例中的配置文件。

步骤 4 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 LSW1 为例。

- 对 LSW2 上的接口 GE0/0/1 执行命令 **shutdown** 模拟端口故障，在 LSW3 上执行命令 **display sep interface** 查看接口 GE0/0/2 能否从阻塞状态放开进入转发状态。

```
[LSW3] display sep interface gigabitethernet 0/0/2
SEP segment 1
------------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------------
GE0/0/2             common        up                  forwarding
```

----结束

配置文件

- LSW1 的配置文件

```
#
 sysname LSW1
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
return
```

- LSW2 的配置文件

```
#
 sysname LSW2
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
return
```

- LSW3 的配置文件

```
#
 sysname LSW3
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 5 to 6 100
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 5 to 6 100
  active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port GigabitEthernet
0/0/3 level 0
 ring 1 enable
#
sep segment 1
 control-vlan 10
 block port middle
 tc-notify rrpp
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 stp disable
 sep segment 1 edge primary
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100
 stp disable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100
 stp disable
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 5 to 6 100
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 5 to 6 100
  active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/2 secondary-port GigabitEthernet
0/0/3 level 0
 ring 1 enable
#
sep segment 1
 control-vlan 10
 tc-notify rrpp
 protected-instance 0 to 48
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 stp disable
 sep segment 1 edge secondary
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100
 stp disable
#
return
```

- PE3 的配置文件

```
#
 sysname PE3
#
 vlan batch 5 to 6 100 200
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 5 to 6 100
  active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet
0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 100
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 200
 stp disable
#
interface GigabitEthernet0/0/3
 port default vlan 200
 port trunk allow-pass vlan 5 to 6 100
#
return
```

- PE4 的配置文件

```
#
 sysname PE4
#
 vlan batch 5 to 6 100 200
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 5 to 6 100
  active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet
0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 200
 stp disable
#
interface GigabitEthernet0/0/3
 port default vlan 200
 port trunk allow-pass vlan 5 to 6 100
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

配置 SEP 多实例示例

本示例中的组网特点是封闭环路上存在两个 SEP 段，不同的 SEP 段处理不同的 VLAN 业务，实现流量负载负担，并提供链路备份。

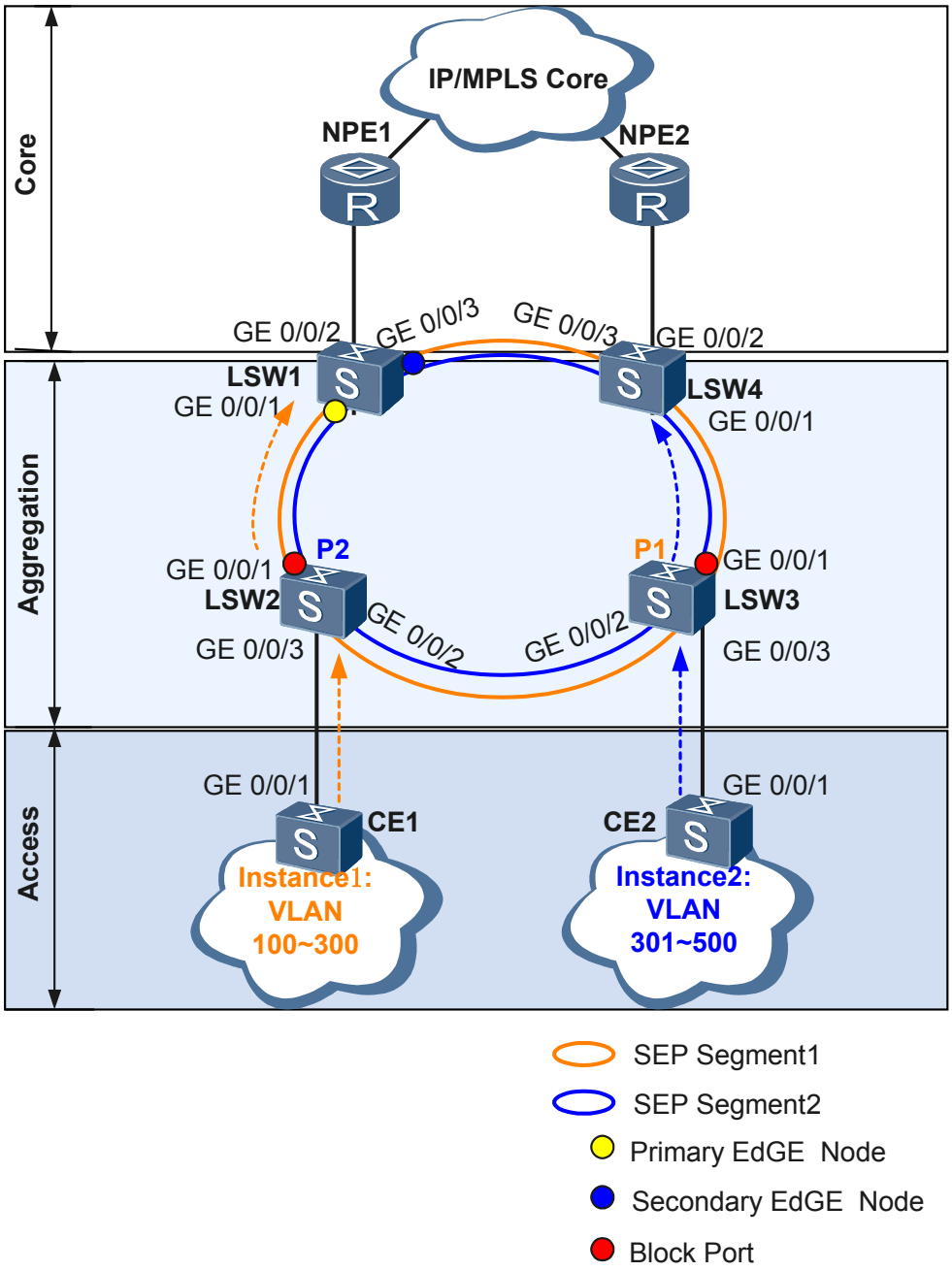
版权所有 © 华为技术有限公司

组网需求

在普通的 SEP 组网图中，一个物理环上只能配置一个 SEP 段，也只能指定一个阻塞点。当 SEP 段处于完整状态时，阻塞端口会阻止所有的用户数据通过。这样，所有用户数据在 SEP 段上只能通过一条路径传输，阻塞端口侧的链路空闲，造成带宽浪费。

为了解决带宽浪费问题，并实现负载分担，华为公司实现了 SEP 多实例。

图 3-72 SEP 多实例封闭环组网图



如图 3-72 所示，多台二层交换设备 LSW1 ～ LSW4 形成环形网络接入核心层网络。此种情况下：

华为专有和保密信息
版权所有 © 华为技术有限公司

- 在汇聚层运行 SEP 协议。
  - 当环网上没有故障链路时，SEP 能够消除以太网冗余环路。
  - 当环网上发生链路故障时，SEP 能够迅速恢复环网上各节点间通信通路。
- 在 LSW1 ～ LSW4 上配置 SEP 多实例，通过两个 SEP 段解决带宽浪费问题，实现负载分担并提供链路备份。

配置思路

采用如下的思路配置 SEP 多实例封闭环：

1. 配置 SEP 基本功能：
   a. 在 LSW1 ～ LSW4 上创建两个 SEP 段和一个控制 VLAN。
      不同 SEP 段可以使用相同 ID 的控制 VLAN。
   b. 配置 SEP 保护实例，并将实例与用户 VLAN 映射，确保端口的转发状态变化或拓扑变化只影响对应的 VLAN，而不影响其他 VLAN，保证用户数据可靠传输。
   c. 将环网上所有设备加入 SEP 段,并配置 LSW1 上接口 GE0/0/1 是主边缘端口、GE0/0/3 是副边缘端口。
   d. 在端口角色为主边缘端口的设备上配置端口阻塞方式，灵活指定阻塞端口。
   e. 配置 SEP 抢占模式，确保故障恢复时用户指定的阻塞端口生效。
2. 配置 CE1、CE2、LSW1 ～ LSW4 二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- SEP 段 ID
- 控制 VLAN ID
- 加入 SEP 段的端口角色
- 端口阻塞方式
- SEP 抢占模式
- SEP 保护实例 ID

操作步骤

步骤 1 创建 SEP 段和控制 VLAN

- 配置 Segment ID 为 1 的 SEP 段和 VLAN ID 为 10 的控制 VLAN

  # 配置 LSW1。

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] quit
```

  # 配置 LSW2。

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] quit
```

  # 配置 LSW3。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] quit
```

配置 LSW4。

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] quit
```

- 配置 Segment ID 为 2 的 SEP 段和 VLAN ID 为 10 的控制 VLAN

配置 LSW1。

```
[LSW1] sep segment 2
[LSW1-sep-segment2] control-vlan 10
[LSW1-sep-segment2] quit
```

配置 LSW2。

```
[LSW2] sep segment2
[LSW2-sep-segment2] control-vlan 10
[LSW2-sep-segment2] quit
```

配置 LSW3。

```
[LSW3] sep segment 2
[LSW3-sep-segment2] control-vlan 10
[LSW3-sep-segment2] quit
```

配置 LSW4。

```
[LSW4] sep segment 2
[LSW4-sep-segment2] control-vlan 10
[LSW4-sep-segment2] quit
```

说明

- 控制 VLAN 的 ID 必须是没有被创建或使用的。
- 控制 VLAN 成功创建后，配置文件会自动显示创建普通 VLAN 的命令。

  每个 SEP 段必须配置控制 VLAN，当接口加入已经配置控制 VLAN 的 SEP 段后，接口将自动加入控制 VLAN。

步骤 2 配置 SEP 段保护实例，并将实例与用户 VLAN 映射。

配置 LSW1。

```
[LSW1] vlan batch 100 to 500
[LSW1] sep segment 1
[LSW1-sep-segment1] protected-instance 1
[LSW1-sep-segment1] quit
[LSW1] sep segment 2
[LSW1-sep-segment2] protected-instance 2
[LSW1-sep-segment2] quit
[LSW1] stp region-configuration
[LSW1-mst-region] instance 1 vlan 100 to 300
[LSW1-mst-region] instance 2 vlan 301 to 500
[LSW1-mst-region] active region-configuration
[LSW1-mst-region] quit
```

LSW2 ～ LSW4 配置略。LSW2 ～ LSW4 配置与 LSW1 配置类似，具体配置请参见本示例配置文件。

步骤 3 将环网上的设备加入 SEP 段，并配置端口角色

说明

缺省情况下，二层端口上 STP 处于使能状态。在将端口加入 SEP 段之前，请先去使能 STP。

配置 LSW1 的端口 GE0/0/1 端口角色为主边缘端口，GE0/0/3 端口角色为副边缘端口。

```
[LSW1] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[LSW1-GigabitEthernet0/0/1] stp disable
[LSW1-GigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-GigabitEthernet0/0/1] sep segment 2 edge primary
[LSW1-GigabitEthernet0/0/1] quit
[LSW1] interface gigabitethernet 0/0/3
[LSW1-GigabitEthernet0/0/3] stp disable
[LSW1-GigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet0/0/3] sep segment 2 edge secondary
[LSW1-GigabitEthernet0/0/3] quit
```

配置 LSW2。

```
[LSW2] interface gigabitethernet 0/0/1
[LSW2-GigabitEthernet0/0/1] stp disable
[LSW2-GigabitEthernet0/0/1] sep segment 1
[LSW2-GigabitEthernet0/0/1] sep segment 2
[LSW2-GigabitEthernet0/0/1] quit
[LSW2] interface gigabitethernet 0/0/2
[LSW2-GigabitEthernet0/0/2] stp disable
[LSW2-GigabitEthernet0/0/2] sep segment 1
[LSW2-GigabitEthernet0/0/2] sep segment 2
[LSW2-GigabitEthernet0/0/2] quit
```

配置 LSW3。

```
[LSW3] interface gigabitethernet 0/0/1
[LSW3-GigabitEthernet0/0/1] stp disable
[LSW3-GigabitEthernet0/0/1] sep segment 1
[LSW3-GigabitEthernet0/0/1] sep segment 2
[LSW3-GigabitEthernet0/0/1] quit
[LSW3] interface gigabitethernet 0/0/2
[LSW3-GigabitEthernet0/0/2] stp disable
[LSW3-GigabitEthernet0/0/2] sep segment 1
[LSW3-GigabitEthernet0/0/2] sep segment 2
[LSW3-GigabitEthernet0/0/2] quit
```

配置 LSW4。

```
[LSW4] interface gigabitethernet 0/0/1
[LSW4-GigabitEthernet0/0/1] stp disable
[LSW4-GigabitEthernet0/0/1] sep segment 1
[LSW4-GigabitEthernet0/0/1] sep segment 2
[LSW4-GigabitEthernet0/0/1] quit
[LSW4] interface gigabitethernet 0/0/3
[LSW4-GigabitEthernet0/0/3] stp disable
[LSW4-GigabitEthernet0/0/3] sep segment 1
[LSW4-GigabitEthernet0/0/3] sep segment 2
[LSW4-GigabitEthernet0/0/3] quit
```

上述配置成功后，在 LSW1 上执行命令 **display sep topology**，查看 SEP 段的拓扑信息，可以看到阻塞端口是最后完成邻居协商的链路两端的其中一个端口。

```
[LSW1] display sep topology
SEP segment 1
--------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------------
LSW1                 GE0/0/1          primary         forwarding
LSW2                 GE0/0/1          common          forwarding
LSW2                 GE0/0/2          common          forwarding
LSW3                 GE0/0/2          common          forwarding
LSW3                 GE0/0/1          common          forwarding
LSW4                 GE0/0/1          common          forwarding
LSW4                 GE0/0/3          common          forwarding
LSW1                 GE0/0/3          secondary       discarding

SEP segment 2
--------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------------
LSW1                 GE0/0/1          primary         forwarding
```


版权所有 © 华为技术有限公司

```
LSW2                GE0/0/1         common          forwarding
LSW2                GE0/0/2         common          forwarding
LSW3                GE0/0/2         common          forwarding
LSW3                GE0/0/1         common          forwarding
LSW4                GE0/0/1         common          forwarding
LSW4                GE0/0/3         common          forwarding
LSW1                GE0/0/3         secondary       discarding
```

步骤 4 灵活指定阻塞端口

在主边缘端口所在的设备 LSW1 上配置阻塞端口的方式是系统名+端口名，抢占模式是延时抢占。

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port sysname LSW3 interface gigabitethernet 0/0/1
[LSW1-sep-segment1] preempt delay 15
[LSW1-sep-segment1] quit
[LSW1] sep segment 2
[LSW1-sep-segment2] block port sysname LSW2 interface gigabitethernet 0/0/1
[LSW1-sep-segment2] preempt delay 15
[LSW1-sep-segment2] quit
```

上述配置成功后，查看 SEP 拓扑，以 LSW1 显示为例。

在 LSW1 上执行命令 **display sep topology**，查看 SEP 段的拓扑信息。

```
[LSW1] display sep topology
SEP segment 1
--------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------
LSW1                 GE0/0/1          primary         forwarding
LSW2                 GE0/0/1          common          forwarding
LSW2                 GE0/0/2          common          forwarding
LSW3                 GE0/0/2          common          forwarding
LSW3                 GE0/0/1          common          discarding
LSW4                 GE0/0/1          common          forwarding
LSW4                 GE0/0/3          common          forwarding
LSW1                 GE0/0/3          secondary       forwarding

SEP segment 2
--------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
--------------------------------------------------------------
LSW1                 GE0/0/1          primary         forwarding
LSW2                 GE0/0/1          common          discarding
LSW2                 GE0/0/2          common          forwarding
LSW3                 GE0/0/2          common          forwarding
LSW3                 GE0/0/1          common          forwarding
LSW4                 GE0/0/1          common          forwarding
LSW4                 GE0/0/3          common          forwarding
LSW1                 GE0/0/3          secondary       forwarding
```

从拓扑显示信息中可以看出：

- 在 Segment 1 中，LSW3 上的端口 GE0/0/1 的转发状态为 **discarding**，其余端口的转发状态均为 **forwarding**。
- 在 Segment 2 中，LSW2 上的端口 GE0/0/1 的转发状态为 **discarding**，其余端口的转发状态均为 **forwarding**。

步骤 5 配置 CE1、CE2、LSW1 ～ LSW4 的二层转发功能

具体配置过程略。请参考本配置举例中的配置文件。

步骤 6 验证配置结果

模拟故障产生情况下，查看阻塞端口是否能够从阻塞状态放开进入转发状态。

将 LSW2 上的端口 GE0/0/1 **shutdown** 模拟端口故障。

版权所有 © 华为技术有限公司

在 LSW3 上执行命令 **display sep interface**，查看在 Segment 1 中端口 GE0/0/1 能否从阻塞状态放开进入转发状态。

```
[LSW3] display sep interface gigabitethernet 0/0/1
SEP segment 1
------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------
GE0/0/1             common        up                  forwarding
SEP segment 2
------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------
GE0/0/1             common        up                  forwarding
```

从上述表项可以发现 GE0/0/1 的状态可以成功从阻塞状态进入转发状态，Segment 1 中转发路径变化并没有影响 Segment 2 的转发路径。

----结束

配置文件

- LSW1 的配置文件

```
#
 sysname LSW1
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 block port sysname LSW3 interface GigabitEthernet0/0/1
 preempt delay 15
 protected-instance 1
sep segment 2
 control-vlan 10
 block port sysname LSW2 interface GigabitEthernet0/0/1
 preempt delay 15
 protected-instance 2
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1 edge primary
 sep segment 2 edge primary
#
interface GigabitEthernet0/0/3
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1 edge secondary
 sep segment 2 edge secondary
#
return
```

- LSW2 的配置文件

```
#
 sysname LSW2
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
```


版权所有 © 华为技术有限公司

```
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface GigabitEthernet0/0/2
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface GigabitEthernet0/0/3
 port hybrid  tagged vlan 100 to 300
#
return
```

- LSW3 的配置文件

```
#
 sysname LSW3
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface GigabitEthernet0/0/2
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface GigabitEthernet0/0/3
 port hybrid  tagged vlan 301 to 500
#
return
```

- LSW4 的配置文件

```
#
 sysname LSW4
#
 vlan batch 10 60 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
```


版权所有 © 华为技术有限公司

```
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface GigabitEthernet0/0/3
 port hybrid  tagged vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100 to 300
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 100 to 300
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 vlan batch 301 to 500
#
interface GigabitEthernet0/0/1
 port hybrid  tagged vlan 301 to 500
#
return
```

3.11 二层协议透明传输配置

介绍了二层协议透明传输的基本知识、配置方法和配置实例。

3.11.1 二层协议透明传输概述

简要介绍二层协议透明传输的基本概念。

二层协议透明传输的产生背景

在实际网络环境中，用户网络之间的某些二层协议，如 MSTP，HGMP，LACP 等，需要穿越骨干网络完成二层协议的计算功能。

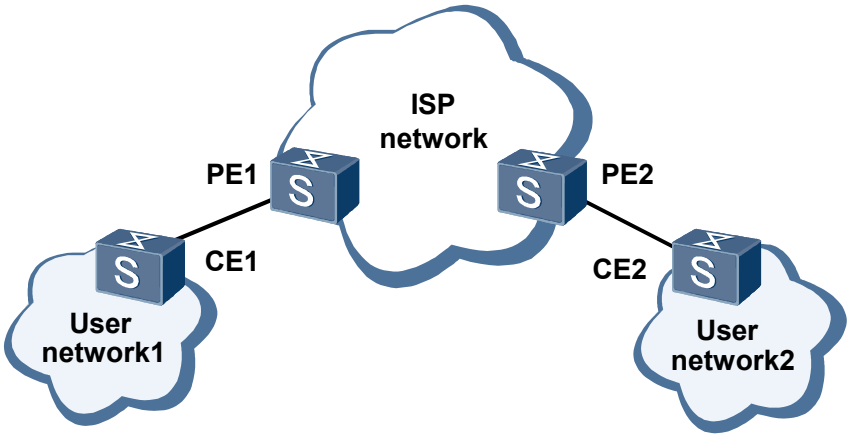
如图 3-73 所示。用户网络 1 和用户网络 2 共同运行某些二层协议，例如 MSTP 协议，这样就要求用户网络 1 的二层协议报文能够穿过骨干网络到达用户网络 2，完成生成树计算。通常二层协议报文的目的 MAC 都是一样的，例如 MSTP 协议，其协议报文是 BPDU 报文，目的 MAC 均是 0180-C200-0000。因此，当用户网络的二层协议报文到达

版权所有 © 华为技术有限公司

骨干网络的 PE 设备时，PE 不能识别该二层协议报文是来自用户网络还是来自骨干网自身，都会把收到的二层协议报文发送给 CPU 进行处理，完成生成树计算。

这样用户网络 1 的设备就和 PE1 完成了生成树计算功能，而不是和用户网络 2 的设备完成生成树计算。用户网络 1 的二层协议报文无法穿越骨干网络到达用户网络 2 中。

图 3-73 二层协议在 ISP 网络透明传输



为了解决上述的问题，此时可以使用二层协议透明传输功能。

二层协议报文需要在骨干网络中透明传输，其传输过程中必须达到以下要求：

- 同一个用户网络的所有 Site 都能收到其他 Site 的二层协议报文。
- 用户网络的二层协议报文不能被骨干网设备的 CPU 处理。
- 不同客户网络中的二层协议报文必须隔离，不能互相影响。

二层协议透明传输的基本原理是：

- 在骨干网的用户接入侧替换原始二层协议报文的组播目的 MAC 地址为特定的组播 MAC 地址。
- 修改 MAC 后的报文在骨干网中根据配置的透明传输方式决定是否对报文进行封装外层 VLAN Tag。
- 当该二层协议报文到达出节点时，通过匹配设备上配置的特殊组播目的 MAC 和二层协议的映射关系，将报文的组播目的 MAC 还原成该二层协议标准的组播目的 MAC 地址，并根据配置的透明传输方式决定是否剥除外层 VLAN Tag，然后转发到用户侧。

3.11.2 AC6605 支持的二层协议透明传输特性

介绍二层协议透明传输特性在 AC6605 中的支持情况。

按照应用场景的不同，AC6605 支持如下几种方式的二层协议透明传输：

- 基于接口的二层协议透明传输。

版权所有 © 华为技术有限公司

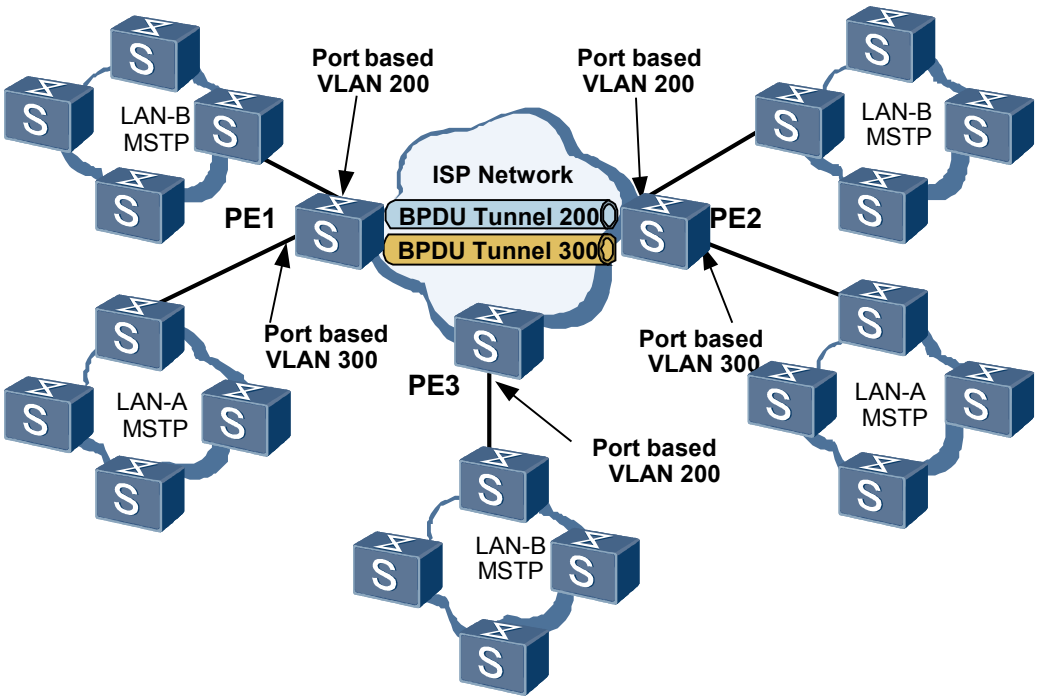
- 基于 VLAN 的二层协议透明传输。
- 基于 QinQ 的二层协议透明传输。

目前 AC6605 支持透明传输的二层协议报文有：

- STP（Spanning Tree Protocol）
- LACP（Link Aggregation Control Protocol）
- EOAM3ah（GigabitEthernet Operation, Administration, and Maintenance 802.3ah）
- LLDP（Link Layer Discovery Protocol）
- GVRP（Generic VLAN Registration Protocol）
- GMRP（Generic Multicast Registration Protocol）
- HGMP（HUAWEI Group Management Protocol）
- VTP（Vlan Trunking Protocol）
- UDLD（Unidirectional Link Detection）
- PAGP（Port Aggregation Protocol）
- CDP（Cisco Discovery Protocol）
- PVST+（Per VLAN Spanning Tree Plus）
- SSTP（Shared Spanning Tree Protocol）
- DTP（Dynamic Trunking Protocol）
- 用户自定义的协议

基于接口的二层协议透明传输

图 3-74 基于接口的二层协议透明传输



版权所有 © 华为技术有限公司

如图 3-74 所示，PE 设备的每个接口只连接了一个用户网络，但是所有的用户网络不属于同一个 LAN。这时用户网络发送到 PE 的二层协议报文（BPDU）也不带有 Tag，而 PE 设备需要区分该二层协议报文来自哪一个用户LAN。LAN-A 的二层协议报文必须被转发到其他 LAN-A 的用户网络中，而不能被转发到 LAN-B 的用户网络中，并且还要避免该二层协议报文被运营商网络设备处理。

针对这种场景，设备有以下处理方式：

- 替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址。

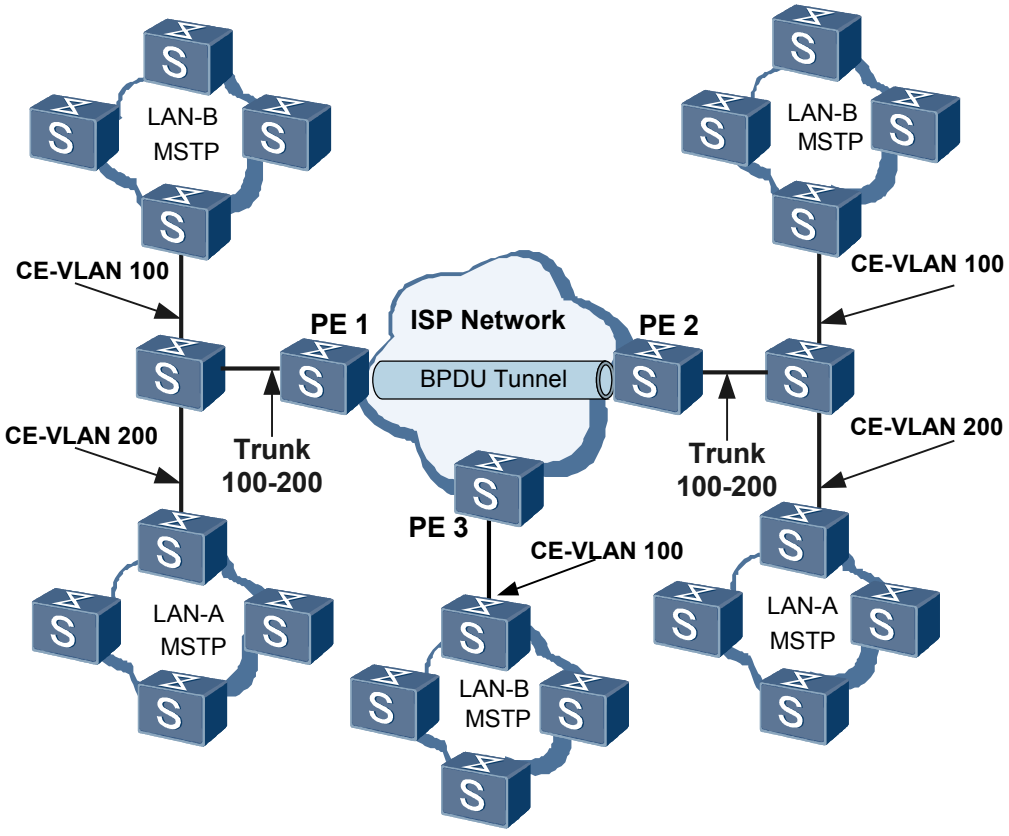
  说明

  这种方式适用于所有类型的二层协议透明传输。

  1. 骨干网设备收到用户网络的二层协议报文并识别出该报文属于哪种二层协议的报文（如 STP 协议的 BPDU 报文），根据接口的缺省 VLAN，给该报文打上对应的 VLAN ID。
  2. 骨干网设备根据配置的特殊组播目的 MAC 和二层协议的映射关系，将该二层协议报文的标准组播目的 MAC 地址修改为指定的组播目的 MAC 地址。
  3. 修改 MAC 后的二层报文在骨干网内部的节点上按照普通的二层报文转发，用户网络的二层协议报文正常地穿越骨干网络。
  4. 用户网络的二层协议报文到达骨干网设备的出节点设备时，再次根据设备上配置的特殊组播目的 MAC 和二层协议的映射关系，将该报文的组播目的 MAC 地址还原成二层协议的标准组播 MAC 地址，然后再转发到用户侧。

基于 VLAN 的二层协议透明传输

图 3-75 基于 VLAN 的二层协议透明传输



版权所有 © 华为技术有限公司

在多数情况下，PE 都是作为汇聚设备存在，如图 3-75 所示，PE1 的汇聚接口上同时收到来自 LAN-A、LAN-B 的报文。为了区分这两个不同的用户网络，CE 发送到 PE 的二层协议报文就必须携带 VLAN ID，其中，LAN-A 的 VLAN ID 为 200，LAN-B 的 VLAN ID 为 100。

目前，例如 STP/RSTP/MSTP 等，一些二层协议的协议报文是要求不带 VLAN 封装的，当骨干网设备收到这些带 VLAN 封装的二层协议报文时，骨干网设备会认为是非法报文，直接将该报文丢弃。此时可以在骨干网设备上配置基于 VLAN 的二层协议透明传输，二层协议报文会直接通过二层隧道，穿越骨干网络。

与基于接口的二层协议透明传输类似，针对这种场景，设备有以下处理方式：

- 替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址。

  说明

  这种方式适用于所有类型的二层协议透明传输。

  1. 配置用户网络设备发送到骨干网的二层协议报文带有指定的 VLAN ID。
  2. 配置骨干网设备能够识别带有 VLAN ID 的二层协议报文，并允许这些 VLAN ID 通过。
  3. 骨干网设备根据配置的特殊组播目的 MAC 和二层协议的映射关系，将该二层协议报文的标准组播目的 MAC 地址修改为指定的组播目的 MAC 地址。
  4. 修改 MAC 后的二层报文在骨干网内部的节点上按照普通的二层报文转发，用户网络的二层协议报文正常地穿越骨干网络。
  5. 用户网络的二层协议报文到达骨干网设备的出节点设备时，再次根据设备上配置的特殊组播目的 MAC 和二层协议的映射关系，将该报文的组播目的 MAC 地址还原成二层协议的标准组播 MAC 地址，然后再转发到用户侧。

基于 QinQ 的二层协议透明传输

- QinQ 概述

  QinQ 协议是基于 IEEE 802.1Q 技术的一种二层隧道协议。QinQ 技术是一项扩展 VLAN 空间的技术，通过在 802.1Q 标签报文的基础上再增加一层 802.1Q 的标签头来达到扩展 VLAN 空间的功能，从而实现私网 VLAN 在公网透明传输，进而达到多种应用的效果。由于在骨干网中传递的报文有两层 802.1Q Tag 头（一层公网 Tag，一层私网 Tag），即 802.1Q-in-802.1Q，所以称之为 QinQ 协议。

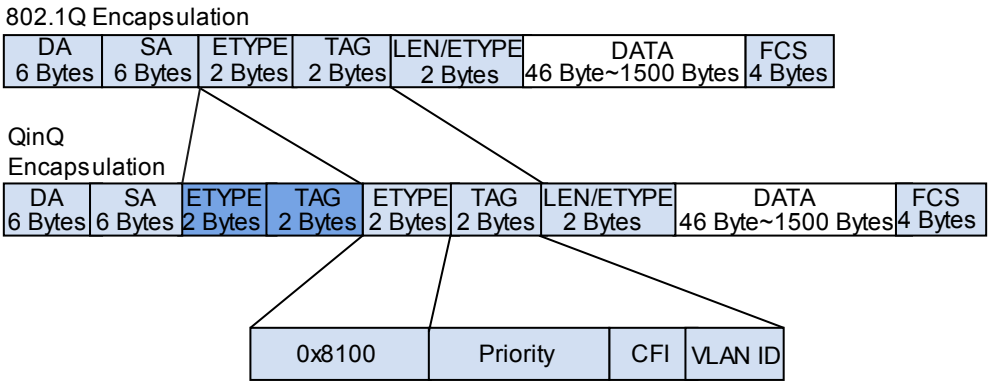
  QinQ 的报文格式如图 3-76 所示。与 802.1Q 的报文相比，QinQ 的报文在源地址（SA）后面又增加了一层标签，称为外层标签或者公网 Tag，用来携带公网的 VLAN ID。内层标签通常被称作私网 Tag，用来携带私网的 VLAN ID。

  说明

  在二层接口上配置的 QinQ 功能，也称为 VLAN Stacking。

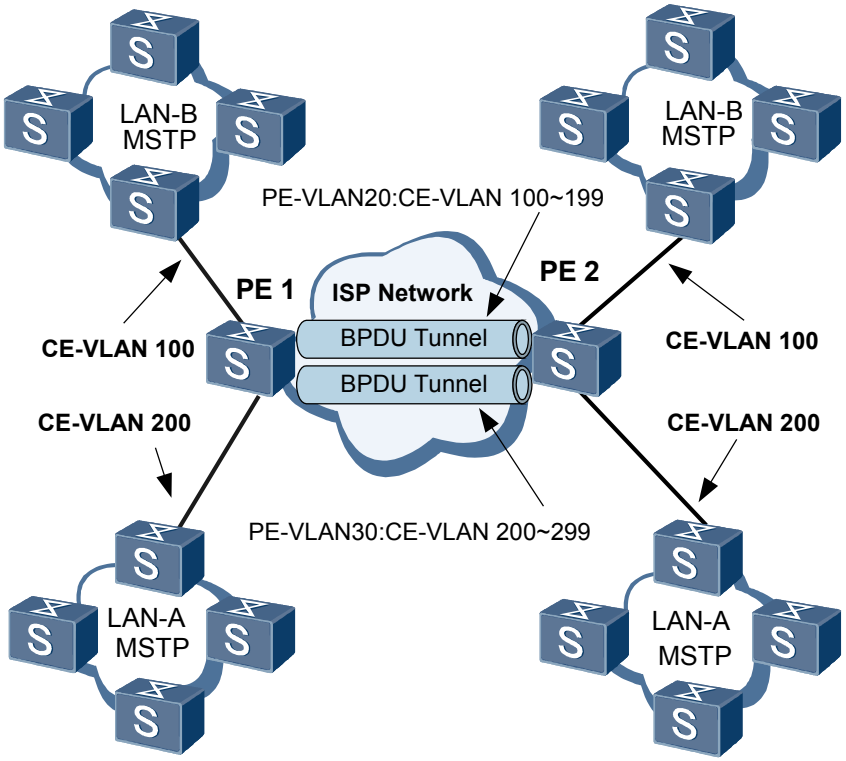
版权所有 © 华为技术有限公司

图 3-76 802.1Q 封装与 QinQ 封装



- 基于 QinQ 的二层协议透明传输

图 3-77 基于 QinQ 的二层协议透明传输。



当接入大量用户网络时，如果仍采用上述的基于 VLAN 的方式透明传输二层协议报文，那么就需要使用大量的运营商 VLAN ID，造成 VLAN ID 资源的紧张。此时，可以在骨干网络内部使用 QinQ 方式来转发用户的二层协议报文。

如图 3-77 所示，PE 的汇聚接口上配置基于 QinQ 的二层协议透明传输功能，根据用户网络来分配不同的外层 Tag。

1. 配置用户网络设备发送到骨干网的二层协议报文带有指定的 VLAN ID。
2. 在骨干网入节点设备的接口上，使能二层协议透明传输和 QinQ 功能。

版权所有 © 华为技术有限公司

3. 骨干网设备根据用户 VLAN ID，为二层协议报文分配不同的外层 Tag，即公网中的 VLAN ID。
4. 骨干网设备根据不同的外层 Tag，选择不同的二层隧道，二层协议报文在层骨干网内部的节点上按照普通的二层报文转发。
5. 在骨干网出节点设备的接口上，同样使能二层协议透明传输和 QinQ 功能。
6. 骨干网出节点设备去掉外层 Tag，并根据内层用户 VLAN ID，把二层协议报文转发到相应的用户网络中。

如图 3-77 所示，PE 收到 VLAN 为 100 ～ 199 的二层协议报文，为该报文打上外层 VLAN20，然后在骨干网络中传输；PE 收到 VLAN 为 200 ～ 299 的二层协议报文，为该报文打上外层 VLAN30，然后在骨干网络中传输。这样既能实现不同用户网络的二层协议报文在骨干网络中的透明传输，又可以节约运营商的 VLAN。

3.11.3 配置基于接口的二层协议透明传输

当骨干网设备上每个接口只有一个用户网络接入，且用户网络发送的二层协议报文不需要携带 VLAN Tag 时，为了实现该二层协议报文在骨干网络中的透明传输，可以配置基于接口的二层协议透明传输功能。

建立配置任务

应用环境

如果骨干网设备的每个接口只有一个用户网络接入，且该用户网络发送的二层协议报文不需携带 VLAN Tag，为了实现该用户网络的二层协议报文在骨干网络的透明传输，此时可以配置基于接口的二层协议透明传输。用户网络的二层协议报文在骨干网络中沿着不同的二层隧道穿越骨干网络到达目的用户网络中，实现正常的协议计算功能。

前置任务

在配置基于接口的二层协议透明传输功能之前，需完成以下任务：

- 所有接口都正确连接。
- 配置基于二层接口的 VLAN。
- 使用 **bpdu enable** 命令配置接口上送 BPDU 报文功能。

数据准备

在配置基于接口的二层协议透明传输功能之前，需要准备以下数据。

序号	数据
1	用户自定义协议名称
2	组播 MAC 地址和协议 MAC 地址
3	PE 的用户侧接口名称和缺省的 VLAN ID 值

（可选）自定义二层透明传输协议的特征信息

版权所有 © 华为技术有限公司

背景信息

当用户网络中特定组播目的 MAC 地址的协议报文（非标准二层协议报文），需要在骨干网络中进行透明传输时，可以在 PE 上定义二层透明传输协议的特征信息。

请在 PE 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **l2protocol-tunnel user-defined-protocol** *protocol-name* **protocol-mac** *protocol-mac* [**encape-type** { { **gigabitethernetii** | **snap** } **protocol-type** *protocol-type* | **llc dsap** *dsap-value* **ssap** *ssap-value* }] **group-mac** { *group-mac* | **default-group-mac** }，自定义二层透明传输协议的特征信息。包括协议的名称、以太封装类型、报文的目的 MAC 地址、报文被替换后的组播 MAC 地址等。

配置用户自定义的二层透明传输协议的特征信息时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：

- BPDU 报文：0180-C200-0000 ～ 0180-C200-002F。
- Smart Link 协议报文：010F-E200-0004。
- 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。
- 本设备上已经使用过的普通组播 MAC 地址。

----结束

指定二层协议透明传输的方式

背景信息

配置透明传输方式时包括修改骨干网设备可以识别的缺省二层协议组播 MAC 地址为其他的组播 MAC 地址和替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址。

在 PE 上根据二层协议的类型和需要透明传输的方式，选择如下配置步骤之一。

操作步骤

- 替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **l2protocol-tunnel** *protocol-type* **group-mac** *group-mac*，把二层协议报文的组播目的 MAC 地址替换成为一个指定的组播 MAC 地址。

版权所有 © 华为技术有限公司

说明

这种方式适用于所有类型的二层协议透明传输。

配置二层协议透明传输功能时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：

- BPDU 报文：0180-C200-0000 ~ 0180-C200-002F。
- Smart Link 协议报文：010F-E200-0004。
- 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。
- 本设备上已经使用过的普通组播 MAC 地址。

----结束

使能接口的二层协议透明传输功能

背景信息

请在 PE 上根据需要透明传输的协议类型，进行以下配置。

操作步骤

步骤 1 执行命令 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 PE 的用户侧接口视图。

步骤 3 执行命令 **port hybrid pvid vlan** *vlan-id*，配置接口的缺省 VLAN。

步骤 4 执行命令 **port hybrid untagged vlan** *vlan-id*，配置接口以 untagged 方式允许缺省 VLAN 通过。

步骤 5 执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，配置接口以 tagged 方式允许 VLAN 通过。

说明

接口允许通过 VLAN 的范围必须包含用户二层协议报文中的 VLAN ID。

步骤 6 执行命令 **l2protocol-tunnel** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* } **enable**，使能接口的二层协议透明传输功能。

说明

- 配置接口允许通过的 VLAN，请参见《AC6605 配置指南-以太网》中的 VLAN 配置。
- 如果需要使用 **l2protocol-tunnel** 命令，在接口上使能用户自定义协议的透明传输功能，请先使用 **l2protocol-tunnel user-defined-protocol** 命令，定义用户的二层透明传输协议的特征信息。此外，除 STP 协议报文在全局有默认的 group-mac 外，在接口下对其他协议报文使能透明传输功能时，全局都必须先配置 group-mac，具体请参见 **l2protocol-tunnel group-mac** 命令。
- 不能把 **l2protocol-tunnel** 命令和 **l2protocol-tunnel vlan** 命令在同一个接口下配置相同协议类型，否则会提示配置冲突。

----结束

检查配置结果

背景信息

已完成基于接口的二层协议透明传输功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display l2protocol-tunnel group-mac** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* }查看所有的二层协议或者指定的二层协议的透明传输信息。

----结束

3.11.4 配置基于 VLAN 的二层协议透明传输

当骨干网设备上每个接口有多个用户网络接入，且用户网络发送的二层协议报文需要携带 VLAN Tag 时，为了实现该二层协议报文在骨干网络中的透明传输，可以配置基于 VLAN 的二层协议透明传输功能。

建立配置任务

应用环境

如果骨干网设备的每个接口有多个用户网络接入，且该用户网络发送的二层协议报文需携带 VLAN Tag，为了实现该用户网络的二层协议报文在骨干网络的透明传输，此时可以配置基于 VLAN 的二层协议透明传输。用户网络的二层协议报文在骨干网络中沿着不同的二层隧道穿越骨干网络到达目的用户网络中，实现正常的协议计算功能。

前置任务

在配置基于 VLAN 的二层协议透明传输功能之前，需完成以下任务：

- 所有接口都正确连接。
- 使用 **bpdu enable** 命令配置接口上送 BPDU 报文功能。

数据准备

在配置基于 VLAN 的二层协议透明传输功能之前，需要准备以下数据。

序号	数据
1	用户自定义协议名称
2	组播 MAC 地址和协议 MAC 地址
3	PE 的用户侧接口名称和允许通过的 VLAN 范围

（可选）自定义二层透明传输协议的特征信息

背景信息

当用户网络中特定组播目的 MAC 地址的协议报文（非标准二层协议报文），需要在骨干网络中进行透明传输时，可以在 PE 上定义二层透明传输协议的特征信息。

请在 PE 上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **l2protocol-tunnel user-defined-protocol** *protocol-name* **protocol-mac** *protocol-mac* [**encape-type** { { **gigabitethernetii** | **snap** } **protocol-type** *protocol-type* | **llc dsap** *dsap-value* **ssap** *ssap-value* }] **group-mac** { *group-mac* | **default-group-mac** }，自定义二层透明传输协议的特征信息。包括协议的名称、以太封装类型、报文的目的 MAC 地址、报文被替换后的组播 MAC 地址等。

配置用户自定义的二层透明传输协议的特征信息时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：

- BPDU 报文：0180-C200-0000 ～ 0180-C200-002F。
- Smart Link 协议报文：010F-E200-0004。
- 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。
- 本设备上已经使用过的普通组播 MAC 地址。

----结束

配置二层协议透明传输的方式

背景信息

配置透明传输方式时包括修改骨干网设备可以识别的缺省二层协议组播 MAC 地址为其他的组播 MAC 地址和替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址。

在 PE 上根据二层协议的类型和需要透明传输的方式，选择如下配置步骤之一。

操作步骤

- 替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **l2protocol-tunnel** *protocol-type* **group-mac** *group-mac*，把二层协议报文的组播目的 MAC 地址替换成为一个指定的组播 MAC 地址。

     说明

     这种方式适用于所有类型的二层协议透明传输。

     配置二层协议透明传输功能时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：

     - BPDU 报文：0180-C200-0000 ~ 0180-C200-002F。
     - Smart Link 协议报文：010F-E200-0004。
     - 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。
     - 本设备上已经使用过的普通组播 MAC 地址。

----结束

使能接口基于 VLAN 的二层协议透明传输功能

版权所有 © 华为技术有限公司

背景信息

请在 PE 上根据需要透明传输的协议类型，进行以下配置。

操作步骤

步骤 1 执行命令 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 PE 的用户侧接口视图。

步骤 3 执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，配置接口以 tagged 方式允许 VLAN 通过。

说明

接口允许通过 VLAN 的范围必须包含用户二层协议报文中的 VLAN ID。

步骤 4 执行命令 **l2protocol-tunnel** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* } { **vlan** *low-id* [**to** *high-id*] } &<1-10>，使能接口基于 VLAN 的二层协议透明传输功能。

说明

- 配置接口 tagged 报文，请参见《AC6605 配置指南-以太网》中的 VLAN 配置。
- 如果需要使用 **l2protocol-tunnel vlan** 命令，在接口上使能用户自定义协议的透明传输功能，请先使用 **l2protocol-tunnel user-defined-protocol** 命令，定义用户的二层透明传输协议的特征信息。此外，除 STP 协议报文在全局有默认的 group-mac 外，在接口下对其他协议报文使能透明传输功能时，全局都必须先配置 group-mac，具体请参见 **l2protocol-tunnel group-mac** 命令。
- 不能把 **l2protocol-tunnel vlan** 命令和 **l2protocol-tunnel** 命令在同一个接口下配置相同协议类型，否则会提示配置冲突。

----结束

检查配置结果

背景信息

已完成二层协议透明传输功能的所有配置。

操作步骤

- 使用命令 **display l2protocol-tunnel group-mac** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* }查看所有的二层协议或者指定的二层协议的透明传输信息。

----结束

3.11.5 配置基于 QinQ 的二层协议透明传输

当骨干网设备上每个接口有多个用户网络接入，且用户网络发送的报文需要携带 VLAN Tag 时，为了实现不用用户网络的协议报文在骨干网络中的透明传输，同时为了节省运营商的 VLAN ID，可以配置基于 QinQ 的二层协议透明传输功能。

建立配置任务

应用环境

如果骨干网设备的每个接口有多个用户网络接入，且用户网络发送的二层协议报文需要携带 VLAN Tag，为了实现不同用户网络的二层协议报文在骨干网络的透明传输，同时

版权所有 © 华为技术有限公司

为了节省运营商的 VLAN ID，可以配置基于 QinQ 的二层协议透明传输。这样，骨干网络根据二层协议报文的外层 VLAN ID为用户分配不同的隧道，属于不同 VLAN 的二层协议报文经过不同的隧道穿越骨干网络。

前置任务

在配置基于 QinQ 的二层协议透明传输功能之前，需完成以下任务：

- 所有接口都正确连接。
- 使用 **bpdu enable** 命令配置接口上送 BPDU 报文功能。

数据准备

在配置基于 QinQ 的二层协议透明传输功能之前，需要准备以下数据。

序号	数据
1	用户自定义协议名称
2	组播 MAC 地址和协议 MAC 地址
3	PE 的用户侧接口名称、缺省 VLAN ID 和允许通过的 VLAN 范围
4	二层协议报文的外层 VLAN ID

（可选）自定义二层透明传输协议的特征信息

背景信息

当用户网络中特定组播目的 MAC 地址的协议报文（非标准二层协议报文），需要在骨干网络中进行透明传输时，可以在 PE 上定义二层透明传输协议的特征信息。

请在 PE 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **l2protocol-tunnel user-defined-protocol** *protocol-name* **protocol-mac** *protocol-mac* [**encape-type** { { **gigabitethernetii** | **snap** } **protocol-type** *protocol-type* | **llc dsap** *dsap-value* **ssap** *ssap-value* }] **group-mac** { *group-mac* | **default-group-mac** }，自定义二层透明传输协议的特征信息。包括协议的名称、以太封装类型、报文的目的 MAC 地址、报文被替换后的组播 MAC 地址等。

配置用户自定义的二层透明传输协议的特征信息时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：

- BPDU 报文：0180-C200-0000 ～ 0180-C200-002F。
- Smart Link 协议报文：010F-E200-0004。
- 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。

版权所有 © 华为技术有限公司

- 本设备上已经使用过的普通组播 MAC 地址。

----结束

配置二层协议透明传输的方式

背景信息

配置透明传输方式时包括修改骨干网设备可以识别的缺省二层协议组播 MAC 地址为其他的组播 MAC 地址和替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址。

在 PE 上根据二层协议的类型和需要透明传输的方式，选择如下配置步骤之一。

操作步骤

- 替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **l2protocol-tunnel** *protocol-type* **group-mac** *group-mac*，把二层协议报文的组播目的 MAC 地址替换成为一个指定的组播 MAC 地址。

     说明

     配置二层协议透明传输功能时，下面的组播 MAC 地址不能作为二层协议报文被替换后的组播 MAC 地址：
     - BPDU 报文：0180-C200-0000 ~ 0180-C200-002F。
     - Smart Link 协议报文：010F-E200-0004。
     - 特殊的组播 MAC 地址：0100-0CCC-CCCC 和 0100-0CCC-CCCD。
     - 本设备上已经使用过的普通组播 MAC 地址。

----结束

使能接口基于 QinQ 的二层协议透明传输功能

背景信息

请在 PE 上根据需要透明传输的协议类型，进行以下配置。

操作步骤

步骤 1 执行命令 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 PE 的用户侧接口视图。

步骤 3 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，配置接口以 untagged 方式允许 VLAN 通过。

步骤 4 执行命令 **qinq vlan-translation enable**，使能接口 VLAN 转换功能。

步骤 5 执行命令 **port vlan-stacking vlan** *vlan-id1* [**to** *vlan-id2*] **stack-vlan** *vlan-id3*，为用户的二层协议报文打上外层 VLAN Tag。

步骤 6 执行命令 **l2protocol-tunnel** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* } { **vlan** *low-id* [**to** *high-id*] } &<1-10>，使能接口基于 VLAN 的二层协议透明传输功能。

版权所有 © 华为技术有限公司

说明

- 步骤 5 指定的外层 VLAN 需要包含在步骤 6 配置的 VLAN 中。
- 配置接口 untagged 报文，请参见《AC6605 配置指南-以太网》中的 VLAN 配置。
- 如果需要使用 **l2protocol-tunnel vlan** 命令，在接口上使能用户自定义协议的透明传输功能，请先使用 **l2protocol-tunnel user-defined-protocol** 命令，定义用户的二层透明传输协议的特征信息。此外，除 STP 协议报文在全局有默认的 group-mac 外，在接口下对其他协议报文使能透明传输功能时，全局都必须先配置 group-mac，具体请参见 **l2protocol-tunnel group-mac** 命令。
- 不能把 **l2protocol-tunnel vlan** 命令和 **l2protocol-tunnel** 命令在同一个接口下配置相同协议类型，否则会提示配置冲突。

----结束

检查配置结果

背景信息

已完成二层协议透明传输功能的所有配置。

操作步骤

- 使用命令 **display l2protocol-tunnel group-mac** { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* }查看所有的二层协议或者指定的二层协议的透明传输信息。

----结束

3.11.6 维护二层协议透明传输

调试二层协议透明传输。

调试二层协议透明传输

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现二层协议透明传输运行故障时，请在用户视图下执行下面的 **debugging** 命令对二层协议透明传输功能进行调试，查看调试信息，定位故障并分析故障的原因。

操作步骤

- 在用户视图下执行 **debugging l2protocol-tunnel** [**msg** | **error** | **event**]命令打开二层协议透明传输的调试信息开关。

----结束

版权所有 © 华为技术有限公司

3.11.7 配置举例

以基于端口、基于 VLAN、基于 QINQ 的二层协议透明传输场景为例，介绍了二层协议透明传输的配置实现过程。

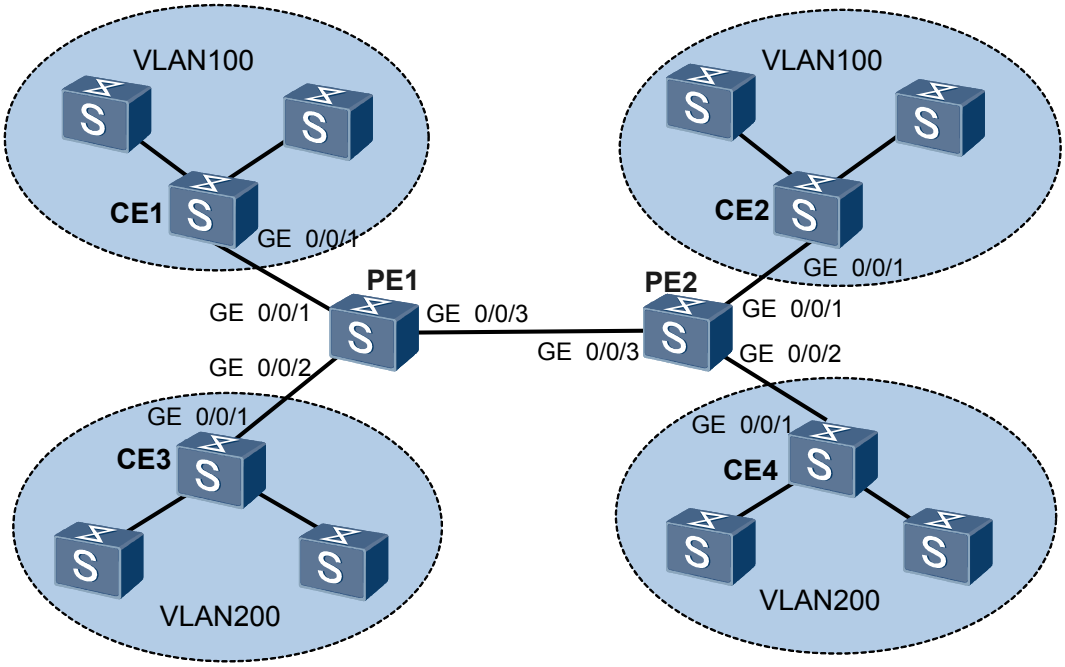
配置基于接口的二层协议透明传输示例

组网需求

如图 3-78 所示，CE 设备通过 PE 设备相连，CE 网络之间运行 STP 协议，因此 CE 的 STP 协议报文需要穿越 PE 之间的骨干网络。PE 的每个接口，只有 1 台 CE 接入，PE 接收到 CE 的 STP 协议报文。此时可以配置基于接口的二层协议透明传输。

本例采用替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址的方法，配置骨干网络透明传输 CE 发送来的 STP 协议报文。默认的 STP 协议报文的目的 MAC 地址为 0180-C200-0000。

图 3-78 配置基于接口的二层协议透明传输组网图



配置思路

采用如下思路基于接口的二层协议透明传输的基本功能：

1. 配置 CE 的 STP 功能。
2. 把 PE 的 CE 侧接口加入到指定的 VLAN 中。
3. 配置 PE 基于接口的二层协议透明传输功能。
4. 配置 PE 的 PSN 侧接口允许 VLAN100 和 VLAN200 的报文通过。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- PE 的 CE 侧接口所属的 VLAN ID 值。
- PE 的 PSN 侧接口允许通过的 VLAN 范围。

操作步骤

步骤 1 使能 CE 设备和 PE 设备的生成树计算功能

配置 CE1。

```
<Quidway> system-view
[Quidway] sysname CE1
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] stp enable
[CE1] interface gigabitethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[CE1-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[CE1-GigabitEthernet0/0/1] bpdu enable
```

配置 CE2。

```
<Quidway> system-view
[Quidway] sysname CE2
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] stp enable
[CE2] interface gigabitethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[CE2-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[CE2-GigabitEthernet0/0/1] bpdu enable
```

配置 CE3。

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] stp enable
[CE3] interface gigabitethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port hybrid pvid vlan 200
[CE3-GigabitEthernet0/0/1] port hybrid untagged vlan 200
[CE3-GigabitEthernet0/0/1] bpdu enable
```

配置 CE4。

```
<Quidway> system-view
[Quidway] sysname CE4
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] stp enable
[CE4] interface gigabitethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port hybrid pvid vlan 200
[CE4-GigabitEthernet0/0/1] port hybrid untagged vlan 200
[CE4-GigabitEthernet0/0/1] bpdu enable
```

配置 PE1。

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1]
```

配置 PE2。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2]
```

步骤 2 将 PE1 和 PE2 的接口 GE0/0/1 加入到 VLAN100 中，将 PE1 和 PE2 的接口 GE0/0/2 加入到 VLAN200 中，PE 设备使能二层协议透明传输功能

配置 PE1。

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] interface gigabitethernet 0/0/1
[PE1-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[PE1-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[PE1-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
[PE1-GigabitEthernet0/0/1] bpdu enable
[PE1-GigabitEthernet0/0/1] quit
[PE1] vlan 200
[PE1-vlan200] quit
[PE1] interface gigabitethernet 0/0/2
[PE1-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[PE1-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[PE1-GigabitEthernet0/0/2] l2protocol-tunnel stp enable
[PE1-GigabitEthernet0/0/2] bpdu enable
[PE1-GigabitEthernet0/0/2] quit
```

配置 PE2。

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[PE2-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[PE2-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
[PE2-GigabitEthernet0/0/1] bpdu enable
[PE2-GigabitEthernet0/0/1] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] interface gigabitethernet 0/0/2
[PE2-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[PE2-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[PE2-GigabitEthernet0/0/2] l2protocol-tunnel stp enable
[PE2-GigabitEthernet0/0/2] bpdu enable
[PE2-GigabitEthernet0/0/2] quit
```

步骤 3 配置 PE 替换接收到 CE 的 STP 协议报文的 MAC 地址

配置 PE1

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

配置 PE2

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

步骤 4 配置 PE 的 PSN 侧接口 GE0/0/3 允许 VLAN100 和 VLAN200 的报文通过

配置 PE1。

```
[PE1] interface gigabitethernet 0/0/3
[PE1-GigabitEthernet0/0/3] port hybrid tagged vlan 100 200
[PE1-GigabitEthernet0/0/3] quit
```

配置 PE2。

```
[PE2] interface gigabitethernet 0/0/3
[PE2-GigabitEthernet0/0/3] port hybrid tagged vlan 100 200
[PE2-GigabitEthernet0/0/3] quit
```


版权所有 © 华为技术有限公司

步骤 5 检查配置结果

配置完成后，在 PE 上使用 **display l2protocol-tunnel group-mac** 命令可以查看透明传输的二层协议名称、协议类型、协议报文的组播目的 MAC 地址、Group MAC 地址以及报文的优先级。

以 PE1 的显示为例。

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

配置完成后，在 CE1 和 CE2 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE1 和 CE2 之间完成了生成树计算功能。CE1 上的 GE0/0/1 为根（Root）端口，CE2 上的 GE0/0/1 为指定（Designated）端口。

```
<CE1> display stp
-------[CIST Global Info] [Mode MSTP] -------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :6
TC count per hello  :6
STP Converge Mode   :Normal
Share region-configuration :enabled
Time since last TC received :0 days 2h:24m:36s
----[Port1(GigabitEthernet0/0/1)] [FORWARDING] ----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :6
          TCN: 0, Config: 0, RST: 0, MST: 6
 BPDU Received       :4351
          TCN: 0, Config: 0, RST: 0, MST: 4351
<CE2> display stp
-------[CIST Global Info] [Mode MSTP] -------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :3
TC count per hello  :3
STP Converge Mode   :Normal
Share region-configuration :enabled
Time since last TC received :0 days 2h:26m:42s
----[Port1(GigabitEthernet0/0/1)] [FORWARDING] ----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
```


版权所有 © 华为技术有限公司

```
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :4534
          TCN: 0, Config: 0, RST: 0, MST: 4534
 BPDU Received       :6
          TCN: 0, Config: 0, RST: 0, MST: 6
```

在 CE3 和 CE4 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE3 和 CE4 之间完成了生成树计算功能。CE3 上的 GE0/0/1 为根（Root）端口，CE4 上的 GE0/0/1 为指定（Designated）端口。

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-0967-58a0
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-0952-f13e / 199999
CIST RegRoot/IRPC   :32768.000b-0967-58a0 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :enabled
Time since last TC received :0 days 10h:54m:37s
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-0952-f13e / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :114
          TCN: 0, Config: 0, RST: 0, MST: 114
 BPDU Received       :885
          TCN: 0, Config: 0, RST: 0, MST: 885
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-0952-f13e
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-0952-f13e / 0
CIST RegRoot/IRPC   :32768.000b-0952-f13e / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Share region-configuration :enabled
Time since last TC received :0 days 8h:59m:18s
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
```


版权所有 © 华为技术有限公司

```
Port Role           :Designated Port
Port Priority       :128
Port Cost(Dot1T )   :Config=auto / Active=200000000
Desg. Bridge/Port   :32768.000b-0952-f13e / 128.82
Port Edged          :Config=disabled / Active=disabled
Point-to-point      :Config=auto / Active=true
Transit Limit       :147 packets/hello-time
Protection Type     :None
Port Stp Mode       :MSTP
Port Protocol Type  :Config=auto / Active= dot1s
BPDU Encapsulation  :Config=stp / Active=stp
PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
TC or TCN send      :0
TC or TCN received  :0
BPDU Sent           :1834
         TCN: 0, Config: 0, RST: 0, MST: 1834
BPDU Received       :1
         TCN: 0, Config: 0, RST: 0, MST: 1
```

----结束

配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- CE3 的配置文件

```
#
 sysname CE3
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```

- CE4 的配置文件

```
#
 sysname CE4
#
```


版权所有 © 华为技术有限公司

```
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 l2protocol-tunnel stp enable
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
 l2protocol-tunnel stp enable
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100 200
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 l2protocol-tunnel stp enable
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
 l2protocol-tunnel stp enable
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 100 200
#
return
```

配置基于 VLAN 的二层协议透明传输示例

组网需求

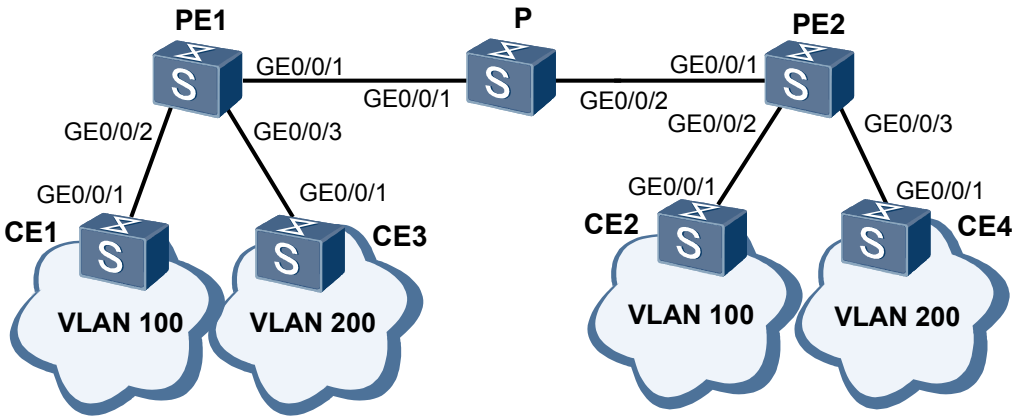
如图 3-79 所示，CE 设备和 PE 设备相连，CE 网络之间运行 STP 协议，CE 的 STP 协议报文需要穿越 PE 之间的骨干网络。PE 的每个接口是汇聚接口，PE 接收到 CE 的 STP 协议报文携带 Tag 以区分不同的用户。此时可以配置基于 VLAN 的二层协议透明传输，使得：

版权所有 © 华为技术有限公司

- VLAN100 中的设备可以共同完成生成树计算。
- VLAN200 中的设备可以共同完成生成树计算。

本例采用替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址的配置方法。默认的 STP 协议报文的目的 MAC 地址为 0180-C200-0000。

图 3-79 配置基于 VLAN 的二层协议透明传输组网图



配置思路

采用如下的思路配置基于 VLAN 的二层协议透明传输的基本功能：

1. 使能 CE 设备的 STP 功能。
2. 配置 CE 发送到 PE 的 STP 协议报文带有指定的 Tag 值。
3. 配置 PE 基于 VLAN 的二层协议透明传输功能。
4. 配置 PE 的 PSN 侧接口允许 VLAN100 和 VLAN200 的报文通过。
5. 配置 P 的普通二层转发功能。允许 PE 之间的报文能被在骨干网中传输。

数据准备

为完成此配置例，需准备如下的数据：

- CE 发送到 PE 的 STP 协议报文的 Tag 值。
- PE 和 CE 各个接口所属的 VLAN ID 值。

操作步骤

步骤 1 使能 CE 和 PE 设备的生成树计算功能。

配置 CE1

```
[CE1] stp enable
```

配置 CE2

```
[CE2] stp enable
```

配置 CE3

版权所有 © 华为技术有限公司

```
[CE3] stp enable
```

配置 CE4

```
[CE4] stp enable
```

步骤 2 配置 CE1 与 CE2 发送到 PE 的 STP 协议报文带 Tag100。配置 CE3 与 CE4 发送到 PE 的 STP 协议报文带 Tag200。

配置 CE1

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface gigabitethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE1-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE1-GigabitEthernet0/0/1] bpdu enable
```

配置 CE2

```
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] interface gigabitethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE2-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE2-GigabitEthernet0/0/1] bpdu enable
```

配置 CE3

```
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] interface gigabitethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE3-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE3-GigabitEthernet0/0/1] bpdu enable
```

配置 CE4

```
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] interface gigabitethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE4-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE4-GigabitEthernet0/0/1] bpdu enable
```

步骤 3 配置 PE 的接口，使得 CE 的 STP 协议报文可以透明传输到 P。

配置 PE1

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
[PE1] interface gigabitethernet 0/0/1
[PE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[PE1-GigabitEthernet0/0/1] quit
[PE1] interface gigabitethernet 0/0/2
[PE1-GigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE1-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE1-GigabitEthernet0/0/2] bpdu enable
[PE1-GigabitEthernet0/0/2] quit
[PE1] interface gigabitethernet 0/0/3
[PE1-GigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE1-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE1-GigabitEthernet0/0/3] bpdu enable
[PE1-GigabitEthernet0/0/3] quit
```

配置 PE2

```
[PE2] vlan 100
```


版权所有 © 华为技术有限公司

```
[PE2-vlan100] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[PE2-GigabitEthernet0/0/1] quit
[PE2] interface gigabitethernet 0/0/2
[PE2-GigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE2-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE2-GigabitEthernet0/0/2] bpdu enable
[PE2-GigabitEthernet0/0/2] quit
[PE2] interface gigabitethernet 0/0/3
[PE2-GigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE2-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE2-GigabitEthernet0/0/3] bpdu enable
[PE2-GigabitEthernet0/0/3] quit
```

步骤 4 配置 PE 替换接收到 CE 的 STP 协议报文的 MAC 地址。

配置 PE1

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

配置 PE2

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

步骤 5 配置 P 的普通二层转发功能，并允许来自 PE 的 VLAN100 和 VLAN200 的报文通过。

```
[P] vlan 100
[P-vlan100] quit
[P] vlan 200
[P-vlan200] quit
[P] interface gigabitethernet 0/0/1
[P-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[P-GigabitEthernet0/0/1] quit
[P] interface gigabitethernet 0/0/2
[P-GigabitEthernet0/0/2] port hybrid tagged vlan 100 200
[P-GigabitEthernet0/0/2] quit
```

步骤 6 检查配置结果

配置完成后，在 PE 上使用 **display l2protocol-tunnel group-mac** 命令可以查看透明传输的二层协议名称、协议类型、协议报文的组播目的 MAC 地址、Group MAC 地址以及报文的优先级。

以 PE1 的显示为例。

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

配置完成后，在 CE1 和 CE2 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE1 和 CE2 之间完成了生成树计算功能。CE1 上的 Eth0/0/1 为根（Root）端口，CE2 上的 Eth0/0/1 为指定（Designated）端口。

```
<CE1> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09f0-1b91
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 199999
CIST RegRoot/IRPC   :32768.000b-09f0-1b91 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
```


版权所有 © 华为技术有限公司

```
Time since last TC received :0 days 3h:53m:43s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :237
          TCN: 0, Config: 0, RST: 0, MST: 237
 BPDU Received       :9607
          TCN: 0, Config: 0, RST: 0, MST: 9607
<CE2> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09d4-b66c
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 0
CIST RegRoot/IRPC   :32768.000b-09d4-b66c / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :1
TC count per hello  :1
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:29m:6s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7095
          TCN: 0, Config: 0, RST: 0, MST: 7095
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

在 CE3 和 CE4 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE3 和 CE4 之间完成了生成树计算功能。CE3 上的 Eth0/0/1 为根（Root）端口，CE4 上的 Eth0/0/1 为指定（Designated）端口。

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
```


版权所有 © 华为技术有限公司

```
Time since last TC received :0 days 3h:57m:0s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :238
          TCN: 0, Config: 0, RST: 0, MST: 238
 BPDU Received       :9745
          TCN: 0, Config: 0, RST: 0, MST: 9745
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:33m:17s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7171
          TCN: 0, Config: 0, RST: 0, MST: 7171
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

----结束

配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
```


版权所有 © 华为技术有限公司

```
 stp bpdu vlan 100
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- CE3 的配置文件

```
#
 sysname CE3
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- CE4 的配置文件

```
#
 sysname CE4
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
Return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

- P 的配置文件

```
#
```


版权所有 © 华为技术有限公司

```
 sysname P
#
 vlan batch 100 200
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

配置基于 VLAN 的二层协议透明传输示例

组网需求

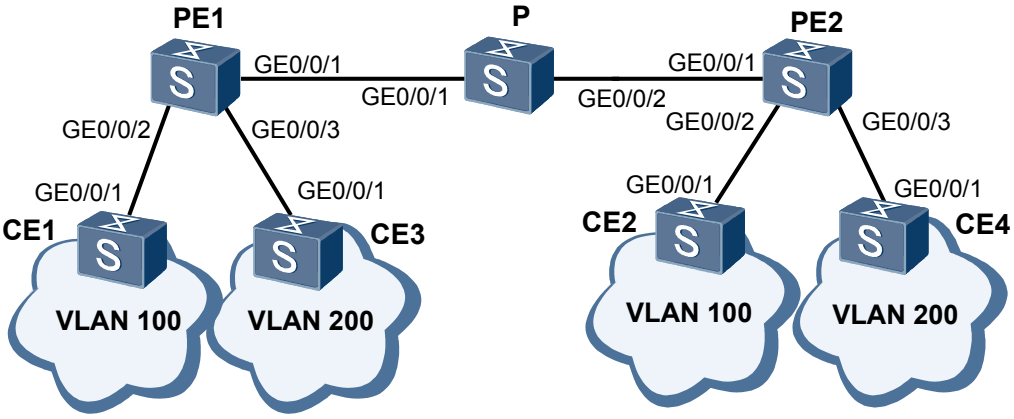
如图 3-80 所示，CE 设备和 PE 设备相连，CE 网络之间运行 STP 协议，CE 的 STP 协议报文需要穿越 PE 之间的骨干网络。PE 的每个接口是汇聚接口，PE 接收到 CE 的 STP 协议报文携带 Tag 以区分不同的用户。此时可以配置基于 VLAN 的二层协议透明传输，使得：

- VLAN100 中的设备可以共同完成生成树计算。
- VLAN200 中的设备可以共同完成生成树计算。

本例采用替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址的配置方法。默认的 STP 协议报文的目的 MAC 地址为 0180-C200-0000。

版权所有 © 华为技术有限公司

图 3-80 配置基于 VLAN 的二层协议透明传输组网图



配置思路

采用如下的思路配置基于 VLAN 的二层协议透明传输的基本功能：

1. 使能 CE 设备的 STP 功能。
2. 配置 CE 发送到 PE 的 STP 协议报文带有指定的 Tag 值。
3. 配置 PE 基于 VLAN 的二层协议透明传输功能。
4. 配置 PE 的 PSN 侧接口允许 VLAN100 和 VLAN200 的报文通过。
5. 配置 P 的普通二层转发功能。允许 PE 之间的报文能被在骨干网中传输。

数据准备

为完成此配置例，需准备如下的数据：

- CE 发送到 PE 的 STP 协议报文的 Tag 值。
- PE 和 CE 各个接口所属的 VLAN ID 值。

操作步骤

步骤 1 使能 CE 和 PE 设备的生成树计算功能。

配置 CE1

```
[CE1] stp enable
```

配置 CE2

```
[CE2] stp enable
```

配置 CE3

```
[CE3] stp enable
```

配置 CE4

```
[CE4] stp enable
```

步骤 2 配置 CE1 与 CE2 发送到 PE 的 STP 协议报文带 Tag100。配置 CE3 与 CE4 发送到 PE 的 STP 协议报文带 Tag200。

配置 CE1

版权所有 © 华为技术有限公司

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface gigabitethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE1-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE1-GigabitEthernet0/0/1] bpdu enable
```

配置 CE2

```
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] interface gigabitethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE2-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE2-GigabitEthernet0/0/1] bpdu enable
```

配置 CE3

```
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] interface gigabitethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE3-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE3-GigabitEthernet0/0/1] bpdu enable
```

配置 CE4

```
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] interface gigabitethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE4-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE4-GigabitEthernet0/0/1] bpdu enable
```

步骤 3 配置 PE 的接口，使得 CE 的 STP 协议报文可以透明传输到 P。

配置 PE1

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
[PE1] interface gigabitethernet 0/0/1
[PE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[PE1-GigabitEthernet0/0/1] quit
[PE1] interface gigabitethernet 0/0/2
[PE1-GigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE1-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE1-GigabitEthernet0/0/2] bpdu enable
[PE1-GigabitEthernet0/0/2] quit
[PE1] interface gigabitethernet 0/0/3
[PE1-GigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE1-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE1-GigabitEthernet0/0/3] bpdu enable
[PE1-GigabitEthernet0/0/3] quit
```

配置 PE2

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[PE2-GigabitEthernet0/0/1] quit
[PE2] interface gigabitethernet 0/0/2
[PE2-GigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE2-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE2-GigabitEthernet0/0/2] bpdu enable
[PE2-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

```
[PE2] interface gigabitethernet 0/0/3
[PE2-GigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE2-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE2-GigabitEthernet0/0/3] bpdu enable
[PE2-GigabitEthernet0/0/3] quit
```

步骤 4 配置 PE 替换接收到 CE 的 STP 协议报文的 MAC 地址。

配置 PE1

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

配置 PE2

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

步骤 5 配置 P 的普通二层转发功能，并允许来自 PE 的 VLAN100 和 VLAN200 的报文通过。

```
[P] vlan 100
[P-vlan100] quit
[P] vlan 200
[P-vlan200] quit
[P] interface gigabitethernet 0/0/1
[P-GigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[P-GigabitEthernet0/0/1] quit
[P] interface gigabitethernet 0/0/2
[P-GigabitEthernet0/0/2] port hybrid tagged vlan 100 200
[P-GigabitEthernet0/0/2] quit
```

步骤 6 检查配置结果

配置完成后，在 PE 上使用 **display l2protocol-tunnel group-mac** 命令可以查看透明传输的二层协议名称、协议类型、协议报文的组播目的 MAC 地址、Group MAC 地址以及报文的优先级。

以 PE1 的显示为例。

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

配置完成后，在 CE1 和 CE2 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE1 和 CE2 之间完成了生成树计算功能。CE1 上的 GE0/0/1 为根（Root）端口，CE2 上的 GE0/0/1 为指定（Designated）端口。

```
<CE1> display stp
-------[CIST Global Info][Mode MSTP]--------
CIST Bridge         :32768.000b-09f0-1b91
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 199999
CIST RegRoot/IRPC   :32768.000b-09f0-1b91 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:53m:43s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
```


版权所有 © 华为技术有限公司

```
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :237
          TCN: 0, Config: 0, RST: 0, MST: 237
 BPDU Received       :9607
          TCN: 0, Config: 0, RST: 0, MST: 9607
<CE2> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09d4-b66c
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 0
CIST RegRoot/IRPC   :32768.000b-09d4-b66c / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :1
TC count per hello  :1
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:29m:6s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7095
          TCN: 0, Config: 0, RST: 0, MST: 7095
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

在 CE3 和 CE4 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE3 和 CE4 之间完成了生成树计算功能。CE3 上的 GE0/0/1 为根（Root）端口，CE4 上的 GE0/0/1 为指定（Designated）端口。

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:57m:0s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
```


版权所有 © 华为技术有限公司

```
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :238
          TCN: 0, Config: 0, RST: 0, MST: 238
 BPDU Received       :9745
          TCN: 0, Config: 0, RST: 0, MST: 9745
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:33m:17s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7171
          TCN: 0, Config: 0, RST: 0, MST: 7171
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

----结束

配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 vlan batch 100
#
stp enable
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- CE3 的配置文件

```
#
 sysname CE3
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- CE4 的配置文件

```
#
 sysname CE4
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
Return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

- P 的配置文件

```
#
 sysname P
#
 vlan batch 100 200
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
return
```


版权所有 © 华为技术有限公司

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

配置基于 QinQ 的二层协议透明传输示例

组网需求

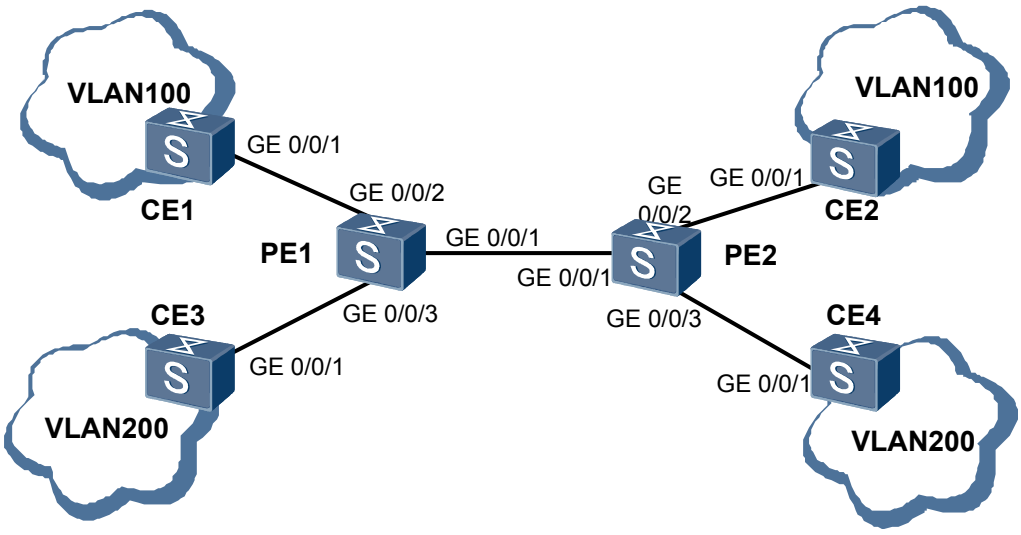
如图 3-81 所示，CE 设备通过 PE 设备相连。CE 网络之间运行 STP 协议，CE1 和 CE2 发送到 PE 的 STP 协议报文带有 Tag100；CE3 和 CE4 发送到 PE 的 STP 协议报文带有 Tag200。在 PE 上配置二层协议透明传输功能，使得：

- VLAN100 中的设备可以共同完成生成树计算。
- VLAN200 中的设备可以共同完成生成树计算。

同时，为了节省公网 VLAN ID，在 PE 上配置 VLAN Stacking。使得 CE 发送到 PE 带有 Tag100 和 Tag200 的 STP 协议报文，都被打上外层 Tag 10 在骨干网络中传输。此时，骨干网络中传输的 STP 协议报文带有两层 Tag。

本例采用替换来自用户网络的原始二层协议报文的组播 MAC 地址为指定组播 MAC 地址的配置方法。默认的 STP 协议报文的目的 MAC 地址为 0180-C200-0000。

图 3-81 基于 QinQ 的二层协议透明传输组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置基于 QinQ 的二层协议透明传输的基本功能：

1. 使能 CE 设备的 STP 功能。
2. 配置 CE 发送到 PE 的 STP 协议报文带有指定的 Tag 值。
3. 配置 PE 基于 VLAN 的二层协议透明传输功能。
4. 配置 PE 的 QinQ（VLAN Stacking）功能。使得 CE 发出的带有不同 Tag 值的 STP 协议报文都被打上外层 Tag10 在骨干网络中传输。

数据准备

为完成此配置例，需准备如下的数据：

- CE 发送到 PE 的 STP 协议报文的内层 Tag 值。
- PE 为收到的 STP 协议报文打上的新 Tag 值。
- PE 和 CE 各个接口所属的 VLAN ID 值。

操作步骤

步骤 1 使能 CE 设备和 PE 设备的生成树计算功能

配置 CE1。

```
[CE1] stp enable
```

配置 CE2。

```
[CE2] stp enable
```

配置 CE3。

```
[CE3] stp enable
```

配置 CE4。

```
[CE4] stp enable
```

步骤 2 配置 CE1 与 CE2 发送到 PE 的 STP 协议报文带 Tag100。配置 CE3 与 CE4 发送到 PE 的 STP 协议报文带 Tag200

配置 CE1。

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface gigabitethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE1-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE1-GigabitEthernet0/0/1] bpdu enable
[CE1-GigabitEthernet0/0/1] quit
```

配置 CE2。

```
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] interface gigabitethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE2-GigabitEthernet0/0/1] stp bpdu vlan 100
[CE2-GigabitEthernet0/0/1] bpdu enable
```


版权所有 © 华为技术有限公司

```
[CE2-GigabitEthernet0/0/1] quit
```

配置 CE3。

```
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] interface gigabitethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE3-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE3-GigabitEthernet0/0/1] bpdu enable
[CE3-GigabitEthernet0/0/1] quit
```

配置 CE4。

```
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] interface gigabitethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE4-GigabitEthernet0/0/1] stp bpdu vlan 200
[CE4-GigabitEthernet0/0/1] bpdu enable
[CE4-GigabitEthernet0/0/1] quit
```

步骤 3 配置 PE 的 QinQ 透明传输功能。使来自 CE 的 VLAN100 和 VLAN200 的报文被打上外层 Tag10 在 PSN 网络中传输。

配置 PE1。

```
[PE1] vlan 10
[PE1-Vlan10] quit
[PE1] interface gigabitethernet 0/0/1
[PE1-GigabitEthernet0/0/1] port hybrid tagged vlan 10
[PE1-GigabitEthernet0/0/1] quit
[PE1] interface gigabitethernet 0/0/2
[PE1-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[PE1-GigabitEthernet0/0/2] qinq vlan-translation enable
[PE1-GigabitEthernet0/0/2] port vlan-stacking vlan 100 stack-vlan 10
[PE1-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 10
[PE1-GigabitEthernet0/0/2] bpdu enable
[PE1-GigabitEthernet0/0/2] quit
[PE1] interface gigabitethernet 0/0/3
[PE1-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[PE1-GigabitEthernet0/0/3] qinq vlan-translation enable
[PE1-GigabitEthernet0/0/3] port vlan-stacking vlan 200 stack-vlan 10
[PE1-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 10
[PE1-GigabitEthernet0/0/3] bpdu enable
[PE1-GigabitEthernet0/0/3] quit
```

配置 PE2。

```
[PE2] vlan 10
[PE2-Vlan10] quit
[PE2] interface gigabitethernet 0/0/1
[PE2-GigabitEthernet0/0/1] port hybrid tagged vlan 10
[PE2-GigabitEthernet0/0/1] quit
[PE2] interface gigabitethernet 0/0/2
[PE2-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[PE2-GigabitEthernet0/0/2] qinq vlan-translation enable
[PE2-GigabitEthernet0/0/2] port vlan-stacking vlan 100 stack-vlan 10
[PE2-GigabitEthernet0/0/2] l2protocol-tunnel stp vlan 10
[PE2-GigabitEthernet0/0/2] bpdu enable
[PE2-GigabitEthernet0/0/2] quit
[PE2] interface gigabitethernet 0/0/3
[PE2-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[PE2-GigabitEthernet0/0/3] qinq vlan-translation enable
[PE2-GigabitEthernet0/0/3] port vlan-stacking vlan 200 stack-vlan 10
[PE2-GigabitEthernet0/0/3] l2protocol-tunnel stp vlan 10
[PE2-GigabitEthernet0/0/3] bpdu enable
[PE2-GigabitEthernet0/0/3] quit
```


版权所有 © 华为技术有限公司

步骤 4 配置 PE 替换接收到 CE 的 STP 协议报文的 MAC 地址。

配置 PE1

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

配置 PE2

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

步骤 5 检查配置结果

配置完成后，在 PE 上使用 **display l2protocol-tunnel group-mac** 命令可以查看透明传输的二层协议名称、协议类型、协议报文的组播目的 MAC 地址、Group MAC 地址以及报文的优先级。

以 PE1 的显示为例。

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

配置完成后，在 CE1 和 CE2 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE1 和 CE2 之间完成了生成树计算功能。CE1 上的 Eth0/0/1 为根（Root）端口，CE2 上的 Eth0/0/1 为指定（Designated）端口。

```
<CE1> display stp
-------[CIST Global Info][Mode MSTP]--------
CIST Bridge         :32768.000b-09f0-1b91
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 199999
CIST RegRoot/IRPC   :32768.000b-09f0-1b91 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:53m:43s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :237
          TCN: 0, Config: 0, RST: 0, MST: 237
 BPDU Received       :9607
          TCN: 0, Config: 0, RST: 0, MST: 9607
<CE2> display stp
-------[CIST Global Info][Mode MSTP]--------
CIST Bridge         :32768.000b-09d4-b66c
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 0
CIST RegRoot/IRPC   :32768.000b-09d4-b66c / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
```


版权所有 © 华为技术有限公司

```
TC or TCN received  :1
TC count per hello  :1
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:29m:6s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7095
          TCN: 0, Config: 0, RST: 0, MST: 7095
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

在 CE3 和 CE4 设备上执行 **display stp** 命令可以检查 MSTP 的根。CE3 和 CE4 之间完成了生成树计算功能。CE4 上的 Eth0/0/1 为根（Root）端口，CE4 上的 Eth0/0/1 为指定（Designated）端口。

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:57m:0s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :238
          TCN: 0, Config: 0, RST: 0, MST: 238
 BPDU Received       :9745
          TCN: 0, Config: 0, RST: 0, MST: 9745
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
```


版权所有 © 华为技术有限公司

```
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:33m:17s
----[Port17(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7171
          TCN: 0, Config: 0, RST: 0, MST: 7171
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

在 PE 设备上执行 **display vlan** 命令可以查看 QinQ 的信息。

以 PE1 的显示为例。

```
<PE1> display vlan 10 verbose
* : Management-VLAN
----------------------
VLAN ID      : 10
VLAN Type    : Common
Description  : VLAN 0010
Status       : Enable
Broadcast    : Enable
MAC Learning : Enable
Statistics   : Disable
Property     : Default
VLAN State   : Up
-----------------
Tagged        Port: GigabitEthernet0/0/1
-----------------
QinQ-stack    Port: GigabitEthernet0/0/2        GigabitEthernet0/0/3
```

----结束

配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
```


版权所有 © 华为技术有限公司

```
 vlan batch 100
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- CE3 的配置文件

```
#
 sysname CE3
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- CE4 的配置文件

```
#
 sysname CE4
#
 vlan batch 200
#
stp enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 vlan batch 10
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface GigabitEthernet0/0/2
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 100 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
interface GigabitEthernet0/0/3
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 200 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 vlan batch 10
#
```


版权所有 © 华为技术有限公司

```
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface GigabitEthernet0/0/2
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 100 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
interface GigabitEthernet0/0/3
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 200 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
return
```

3.12 Loopback Detection 配置

介绍 Loopback Detection 的基本知识、配置方法和配置实例。

3.12.1 Loopback Detection 概述

简要介绍 Loopback Detection 的基本概念。

网络中的环路会导致设备对广播、组播以及未知单播等报文进行重复发送，造成网络资源的浪费甚至导致网络瘫痪。为了能够及时发现二层网络中的环路，以避免对整个网络造成严重影响，需要提供一种检测功能，使网络中出现环路时能及时通知用户检查网络连接和配置情况，并能够将出问题的接口受控。

Loopback Detection（环回检测）功能可以检测设备的接口是否发生环回，它通过从接口定时发送检测报文，并检测该报文是否能够从发出去的接口送回来。当设备发现接口存在环回情况，可以及时通过发送告警信息到网管系统，使管理人员及时发现并解决网络问题，避免长时间断网现象。此外，设备还可以进行接口受控，根据需求选择配置阻塞接口、禁止接口 MAC 学习、关闭接口三种处理方式，能迅速将环回对网络的影响降低至最小。

3.12.2 配置 Loopback Detection 功能

介绍 Loopback Detection 功能的配置方法。

建立配置任务

在进行 Loopback Detection 功能配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

Loopback Detection 功能适用于以下两种场景：

在网络部署的过程中，经常出现接口 TX-RX 自环的问题，比如光纤插错、本接口被高压击坏等情况都可能导致接口 TX-RX 自环。如**图 3-82** 所示，Switch 的接口发生自环，从而导致从接口发出的报文又环回到本接口，导致流量异常、网络的 MAC 漂移等问题。

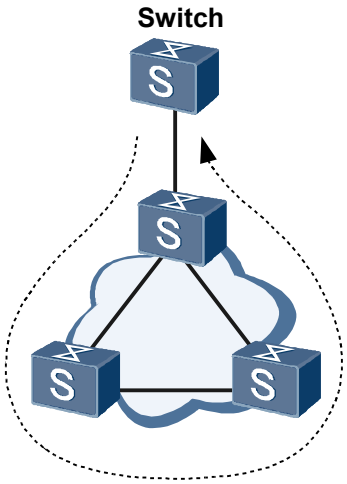
版权所有 © 华为技术有限公司

图 3-82 Loopback Detection 应用组网图



如图 3-83 所示，Switch 连接的外部网络中发生环路，使从接口发出的报文经过外部网络后被环回至本接口。

图 3-83 Loopback Detection 应用组网图



在以上的两种情况下，可以在 Switch 的接口上配置 Loopback Detection 功能，检测接口是否存在环回。当设备检测到某接口存在环回，则设备进行一系列的处理动作，例如堵塞该接口。那么只有存在环回的接口下的用户不能正常通信，而 Switch 连接的其他用户不会受到影响。在后续检测中，设备检测到该接口下的环回消失，则取消对接口的受控，使接口下的用户恢复通信。

说明

- Loopback Detection 仅为单节点环路检测技术，不具备网络级的破除环路功能。
- Loopback Detection 功能需要发送大量报文来进行环路检测，这将会耗费一定的 CPU 资源，请在不需要环路检测时及时关闭此功能。

前置任务

在配置 Loopback Detection 功能之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

版权所有 © 华为技术有限公司

数据准备

在配置 Loopback Detection 功能之前，需要准备以下数据：

序号	数据
1	以太网接口的编号
2	环路检测的 VLAN 编号
3	（可选）环路检测后的处理方式
4	（可选）接口的恢复时间
5	（可选）检测报文的发送周期

使能接口 Loopback Detection 功能

使能接口 Loopback Detection 功能后，接口才会发送环回检测报文来进行接口环回检测。

背景信息

可以通过如下两种方式使能接口 Loopback Detection 功能。

- 在系统视图下使能所有接口 Loopback Detection 功能。
- 在接口视图下使能单个接口 Loopback Detection 功能。

操作步骤

- 在系统视图下使能所有接口 Loopback Detection 功能。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **loopback-detect enable**，使能所有接口的 Loopback Detection 功能。
     缺省情况下，接口的 Loopback Detection 功能为关闭状态。

     窍门

     当设备大部分接口都需要配置 Loopback Detection 功能时，使用这种配置方式可以简化配置步骤。
- 在接口视图下使能单个接口的 Loopback Detection 功能。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **loopback-detect enable**，使能该接口的 Loopback Detection 功能。

  缺省情况下，接口的 Loopback Detection 功能为关闭状态。

  说明

  Eth-Trunk 逻辑端口和成员端口都不支持配置 Loopback Detection 功能。

----结束

配置对指定 VLAN 的 Loopback Detection 功能

配置对指定一个或多个指定 VLAN 进行环回检测。

版权所有 © 华为技术有限公司

背景信息

接口开启 Loopback Detection 功能后，系统默认发送的为 Untag 检测报文，即不对任何指定 VLAN 进行环回检测。当接口是以 Tagged 方式加入 VLAN，接口发出去 Untag 检测报文在链路上会被丢弃，接口将收不到环回回来的报文，因此需要配置对指定的 VLAN 进行环回检测。

配置对指定 VLAN 的 Loopback Detection 功能，接口会定时发送 1 份 Untagged 检测报文和多份带指定 VLAN Tag 的检测报文，一个接口最多可发送 8 份带指定 VLAN Tag 的检测报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **loopback-detect packet vlan** *vlan-id*，配置对指定的 VLAN 进行环回检测。

缺省情况下，没有配置指定 VLAN 报文进行环回检测。最多可配置对 8 个 VLAN 进行环回检测。

说明

配置该功能之前，必须满足以下条件:

- 指定的 VLAN 必须先创建。
- 接口以 Tagged 方式加入该 VLAN。

----结束

（可选）配置 Loopback Detection 处理动作

如果发现接口有环回，设备会将该接口设置为处于环回检测工作状态，可配置发送告警、阻塞接口、禁止接口 MAC 学习、关闭接口四种处理动作。

背景信息

开启 Loopback Detection 功能后，接口会周期性地检测是否收到环回报文。用户可以配置检测到有环回报文时的处理方式，尽量减轻环路对本设备和整个网络的影响。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 **loopback-detect action** { **block** | **nolearn** | **shutdown** | **trap** }，配置接口的 Loopback Detection 处理动作。

缺省情况下，接口处理动作为 **block**。

当系统发现接口存在环回时，可对该接口进行以下 4 种处理动作：

- **block**：堵塞接口。当检测到环回时，将该接口与其他接口隔离，进入该接口的数据报文将无法转发到其他接口。

版权所有 © 华为技术有限公司

- **nolearn**：禁止接口 MAC 地址学习。当检测到环回时，该接口将不再进行 MAC 地址学习。
- **shutdown**：关闭接口。当检测到环回时，将关闭该接口。
- **trap**：接口只上报告警。当检测到环回时，接口只上报告警信息，无其他动作。

----结束

（可选）配置环回消失后接口恢复时间

背景信息

请在需要配置 Loopback Detection 的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入端口视图。

步骤 3 执行命令 **loopback-detect recovery-time** *recovery-time*，设置环回消失后接口的恢复时间。

缺省情况下，环回消失后接口将在 3 个报文发送周期内自动恢复。

说明

- 建议恢复时间至少是报文发送时间的 3 倍；如果发送周期配置的非常小，恢复时间建议至少比发送周期大 10 秒。
- 被 **shutdown** 的接口不能自动恢复，只能通过 **undo shutdown** 命令手动恢复。

----结束

（可选）配置接口 Loopback Detection 报文发送周期

背景信息

由于网络时刻处于变化中，因此环回检测是一个持续的过程，接口以一定的时间间隔发送环回检测报文，这个时间间隔即 Loopback Detection 报文发送周期。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **loopback-detect packet-interval** *packet-interval-time*，设置接口 Loopback Detection 报文的发送周期。

缺省情况下，Loopback Detection 报文的发送周期为 5 秒。

----结束

检查配置结果

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display loopback-detect** 来查看环回检测的配置信息和接口状态。

----结束

3.12.3 配置举例

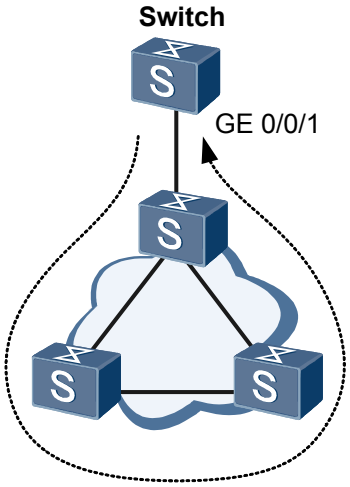
介绍 Loopback Detection 的组网举例。

配置 Loopback Detection 示例

组网需求

如图 3-84 所示，若接口 GE0/0/1 所连接的网络存在环路，导致广播风暴，则可能会影响到 Switch 以及整个网络的通信。在 Switch 上配置 Loopback Detection 功能，检测设备的接口是否有环回存在，从而判断接口所连接的外部网络是否存在环路。

图 3-84 Loopback Detection 应用组网图



配置思路

采用如下思路配置 Loopback Detection 功能：

1. 使能接口的 Loopback Detection 功能。
2. 配置接口对指定 VLAN 报文进行环回检测
3. 配置 Loopback Detection 功能的相关参数。

数据准备

为完成此配置例，需准备如下的数据：

- 配置 Loopback Detection 的接口 GE0/0/1

版权所有 © 华为技术有限公司

- Loopback Detection 报文的发送周期 10 秒
- 指定 VLAN100 进行环回检测
- 接口恢复时间 30 秒

操作步骤

步骤 1 使能接口 Loopback Detection 功能

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] loopback-detect enable
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 配置接口对指定 VLAN 报文进行环回检测

```
[Quidway] vlan 100
[Quidway-vlan100] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 100
[Quidway-GigabitEthernet0/0/1] loopback-detect packet vlan 100
```

步骤 3 配置 Loopback Detection 功能的相关参数

配置接口 Loopback Detection 处理方式

```
[Quidway-GigabitEthernet0/0/1] loopback-detect action block
```

#配置环路消失后接口的恢复时间

```
[Quidway-GigabitEthernet0/0/1] loopback-detect recovery-time 30
[Quidway-GigabitEthernet0/0/1] quit
```

配置接口 Loopback Detection 报文的发送周期

```
[Quidway] loopback-detect packet-interval 10
```

步骤 4 检查配置结果

配置完成后，当接口 GigabitEthernet0/0/1 发生环路时会自动阻塞接口，环路消失后，经过 30 秒，阻塞接口恢复为正常状态。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
 vlan batch 100
#
 loopback-detect packet-interval 10
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 100
 loopback-detect enable
 loopback-detect recovery-time 30
 loopback-detect packet vlan 100
#
return
```


版权所有 © 华为技术有限公司

4 IP 业务配置

关于本章

本文档针对 AC6605 的 IP 业务，介绍了从 IP 地址配置、DNS、IPv6 DNS、ARP、DHCP、IP 性能、IPv6 基础配置、IPv6 over IPv4 隧道配置的各种基础知识和协议配置。阅读本文档可了解 IP 业务特性的基本概念和配置过程。

4.1 IP 地址配置
通过为网络设备配置 IP 地址，可以实现网络设备之间数据的通信。

4.2 ARP 配置
ARP 协议用于将 IP 地址映射到 MAC 地址，实现以太网数据帧的传送。

4.3 DHCP 配置
DHCP 技术适用于各种网络，配置 DHCP 保证了网络中 IP 地址的合理分配，提高整个网络 IP 地址的使用率。

4.4 DHCPv6 配置
目前，AC6605 在 IPv6 网络中仅支持应用为 DHCP 中继功能，本章介绍 DHCPv6 中继的配置方法。

4.5 IP 性能配置
介绍 IP 性能的基本概念，并提供配置过程和配置实例。

4.6 DHCP 策略 VLAN 配置
介绍 DHCP 策略 VLAN 的基本概念、工作方式和配置过程，并提供配置举例。

4.7 DNS 配置
通过配置 DNS（Domain Name System）实现网络设备通过域名进行通信。

4.8 IPv6 基础配置
介绍了 IPv6 的基本概念和特性及相关配置过程。

4.9 IPv6 DNS 配置
通过配置 IPv6 DNS（Domain Name System）实现网络设备通过域名进行通信。

4.10 IPv6 over IPv4 隧道配置
IPv6 over IPv4 隧道技术的出现解决了 IPv4 网路向 IPv6 网络过渡的问题。

版权所有 © 华为技术有限公司

4.1 IP 地址配置

通过为网络设备配置 IP 地址，可以实现网络设备之间数据的通信。

4.1.1 IP 地址概述

IP 是 TCP/IP 协议栈中最为核心的协议，TCP、UDP、ICMP、IGMP 报文的数据都以 IP 数据报格式进行传输。不同网络的设备使用网络层地址—IP 地址进行通信。

在 IP 网络中通信，每个主机都需要拥有一个 IP 地址。

IP 地址是在 Internet 上使用的 32 比特地址，由网络号和主机号两部分组成。

IP 地址的网络号字段用来标识一个网络，主机号字段用来标识网络中的具体某台网络设备。对于这些设备而言，无论实际所处的物理位置如何，只要它们的网络号相同，它们就处在同一个网络中。

4.1.2 AC6605 支持的 IP 地址特性

可以通过静态手工配置、动态 DHCP 方式获得 IP 地址。

AC6605 支持几种 IP 地址的配置方法：

- 静态手工配置接口的 IP 地址
- DHCP 服务器方式获取接口的 IP 地址

AC6605 支持同一设备网段地址的空间重叠，以节约地址空间。

- 在同一设备不同接口上可以配置网段重叠但不能完全相同的 IP 地址。例如，设备上某接口配置了地址 20.1.1.1/16 后，另一接口若配置 20.1.1.2/24，此时会有提示信息，但配置仍然成功；若另一接口配置 20.1.1.2/16，系统会提示地址冲突，配置失败。
- 同一接口的主从 IP 地址之间可以配置网段重叠的 IP 地址。例如，在接口上配置了主 IP 地址 20.1.1.1/24 后，若配置从 IP 地址 20.1.1.2/16 sub，此时会有提示信息，但配置仍然成功。
- 同一设备不同接口的主从 IP 地址之间可以配置网段重叠但不能完全相同的 IP 地址。例如，设备上某接口配置了地址 20.1.1.1/16 后，另一接口若配置 20.1.1.2/24 sub，此时会有提示信息，但配置仍然成功。

为节约 IP 地址空间，AC6605 支持将接口的 IP 地址掩码长度配置为 31 位。配置了 31 位掩码后，同一个网段下将只有两个 IP 地址，即网段地址和该网段广播地址，均被解释为主机地址。

4.1.3 配置接口的 IP 地址

为网络设备配置 IP 地址，使该设备可以与网络上其他设备进行通信。

建立配置任务

介绍配置接口 IP 地址的应用环境、前置任务、数据准备和配置过程。

版权所有 © 华为技术有限公司

应用环境

为了使接口运行 IP 业务，需要为接口配置 IP 地址。交换机的每个接口可以配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。

一般情况下，一个接口只需配置一个主 IP 地址，但在有些特殊情况下需要配置从 IP 地址。比如，一台交换机通过一个接口连接了一个物理网络，但该物理网络的计算机分别属于 2 个不同的 C 类网络，为了使交换机与物理网络中的所有计算机通信，就需要在该接口上配置一个主 IP 地址和一个从 IP 地址。

前置任务

在配置接口的 IP 地址之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up

数据准备

在配置接口的 IP 地址之前，需准备以下数据。

序号	数据
1	接口的编号
2	接口的主 IP 地址和子网掩码
3	（可选）接口的从 IP 地址和子网掩码

配置接口的主 IP 地址

接口上的主 IP 地址只能为一个。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置主 IP 地址。

一个接口只能有一个主 IP 地址，当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。

----结束

（可选）配置接口的从 IP 地址

当接口需要和几个网络号不同的网络进行通信时，需要为该接口配置从 IP 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } **sub**，配置从 IP 地址。

每个接口最多可配置 8 个从 IP 地址。

----结束

检查配置结果

可以查看接口 IP 地址的配置信息。

前提条件

已经完成接口 IP 地址的所有配置。

操作步骤

- 使用 **display ip interface** [**brief**] [*interface-type* [*interface-number*]]命令查看接口的 IP 配置信息。
- 使用 **display interface** [*interface-type* [*interface-number*]]命令查看接口的信息。

----结束

4.1.4 配置举例

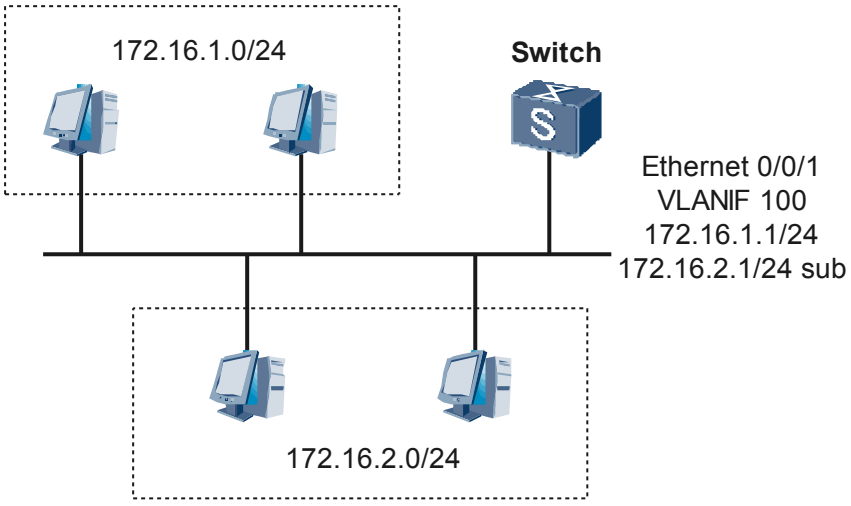
举例说明 IP 地址的配置。

配置 VLANIF 接口的主从 IP 地址示例

组网需求

如图 4-1 所示，为 Switch 设备的以太网接口 GigabitEthernet 0/0/1 连接一个局域网，该局域网中的计算机分别属于 2 个不同的网段 172.16.1.0/24 和 172.16.2.0/24，要求通过 Switch 能分别访问这两个网络，并且网段 172.16.1.0/24 内的主机和 172.16.2.0/24 内的主机不能互通。

图 4-1 配置 IP 地址示例



版权所有 © 华为技术有限公司

配置思路

配置主从 IP 地址的思路如下：

1. 分析接口所连接的网段地址。
2. 配置接口的主从 IP 地址。

数据准备

为完成此配置举例，需要准备如下的数据：

- VLANIF 接口的主 IP 地址和子网掩码。
- VLANIF 接口的从 IP 地址和子网掩码。

操作步骤

步骤 1 配置 Switch 的 GigabitEthernet 0/0/1 接口所属 VLANIF 100 接口的 IP 地址。

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-Vlan100] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 172.16.1.1 24
[Quidway-Vlanif100] ip address 172.16.2.1 24 sub
```

步骤 2 验证配置结果。

从 Switch 上 Ping 网段 172.16.1.0 内的主机，可通。

```
<Quidway> ping 172.16.1.2
PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=128 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

从 Switch 上 Ping 网段 172.16.2.0 内的主机，可通。

```
<Quidway> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

----结束

版权所有 © 华为技术有限公司

配置文件

Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan 100
#
interface Vlanif100
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

4.2 ARP 配置

ARP 协议用于将 IP 地址映射到 MAC 地址，实现以太网数据帧的传送。

4.2.1 ARP 概述

ARP 协议是任何以太网设备都必须支持的协议。实现三层 IP 地址与二层 MAC 地址之间的动态映射。

局域网中每台主机或交换机都可配置一个 32 位的 IP 地址，这个地址用于该主机的所有通信中。IP 地址的分配是独立于机器的硬件地址的。

而在以太网中，主机或交换机是根据 48 位的 MAC（Medium Access Control）地址来发送、接收以太网数据帧的，这个 MAC 地址又称为物理地址或硬件地址，是制造设备时分配到以太网接口中的。因而，在实际的网络互联中，需要一种地址解析的机制来为这两种不同的地址形式提供映射。

ARP（Address Resolution Protocol）用于将一个 IP 地址映射到正确的 MAC 地址。

4.2.2 AC6605 支持的 ARP 特性

介绍 ARP 特性在 AC6605 中的支持情况。

AC6605 支持动态 ARP、静态 ARP、Proxy ARP 和二层拓扑探测功能。

ARP

ARP 可以分为动态和静态两种：

- 通常将用户手工配置的 IP 地址到 MAC 地址的映射，称之为静态 ARP。
- 如果 ARP 映射表由 ARP 协议动态维护，则称之为动态 ARP。

Proxy ARP

AC6605 支持的 Proxy ARP 包括三种：

- 路由式 Proxy ARP

  路由式 Proxy ARP 就是使那些在同一网段却不在同一物理网络上的计算机或交换机能够相互通信的一种功能。

版权所有 © 华为技术有限公司

在实际应用中，如果连接交换机的当前主机上没有配置缺省网关地址（即不知道如何到达本网络的中介系统），此时将无法进行数据转发。

路由式 Proxy ARP 可以解决这个问题，主机发送一个 ARP 请求（请求目的主机的 MAC 地址），使能 Proxy ARP 功能的交换机收到这样的请求后，会使用自己的 MAC 地址作为该 ARP 请求的回应，以此来欺骗主机进行数据转发。

使能 Proxy ARP 功能的交换机还可隐藏物理网络的细节，使得处于不同物理网络但网段相同的 GigabitEthernet A 和 GigabitEthernet B 的内部主机之间可以正常的相互通信。

- VLAN 内 Proxy ARP

  如果两个用户属于相同的 VLAN，但 VLAN 内配置了用户隔离。用户间要互通，需要在关联了 VLAN 的接口上启动 VLAN 内 Proxy ARP 功能。

  若交换机的接口使能了 VLAN 内 Proxy ARP 功能，接口在接收到目的地址不是自己的 ARP 请求报文后，交换机并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果满足代理条件，则将交换机的 MAC 地址发送给 ARP 请求方。

  VLAN 内 Proxy ARP 主要用于配置了用户隔离的 VLAN 内的用户间互通。

- VLAN 间 Proxy ARP

  如果两个用户属于不同的 VLAN，用户间要进行三层互通，需要在关联了 VLAN 的接口上启动 VLAN 间 Proxy ARP 功能。

  若交换机的接口使能了 VLAN 间 Proxy ARP 功能，接口在接收到目的地址不是自己的 ARP 请求报文后，交换机并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果满足代理条件，则将交换机的 MAC 地址发送给 ARP 请求方。

  VLAN 间 Proxy ARP 主要用于：

  - 处于不同 VLAN 的用户进行三层通信。
  - 可在 Super VLAN 对应的 VLANIF 接口上启动 VLAN 间 Proxy ARP 功能，实现 Sub VLAN 间用户互通。

4.2.3 配置静态 ARP

静态 ARP 是指 IP 地址和 MAC 地址之间有固定的映射关系。静态 ARP 需要网络管理员手动配置。

建立配置任务

介绍配置静态 ARP 的应用环境、前置任务、数据准备和配置过程。

应用环境

配置静态 ARP 可用在以下情况。

- 为了将目的 IP 地址不在本网段的报文，穿过本网段的某个网关，使得到该 IP 地址的报文能通过该网关进行转发。
- 当用户需要过滤掉一些目的 IP 地址为非法的报文时，将这些非法的 IP 地址绑定到某个不存在的 MAC 地址。

前置任务

在配置 ARP 之前，需完成以下任务：

版权所有 © 华为技术有限公司

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up
- 配置接口的网络层协议

数据准备

在配置 ARP 之前，需准备以下数据。

序号	数据
1	静态 ARP 表项的 IP 地址和 MAC 地址
2	静态 ARP 表项的所在的 VPN 实例名和 VLAN ID

配置普通静态 ARP 表项

当需要实现普通接口互通时，配置静态 ARP 表项。

背景信息

在设备上同时配置静态 ARP 和 VRRP 时，不能将 VLANIF 接口下所配置的 VRRP 备份组的虚拟 IP 地址作为该静态 ARP 表项中的 IP 地址，否则会生成错误的主机路由，影响正常转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp static** *ip-address mac-address*，配置普通静态 ARP 表项。

说明

静态 ARP 表项在交换机正常工作时一直有效。

----结束

配置 VLAN 内的静态 ARP 表项

如果两个用户属于相同的 VLAN，但 VLAN 内配置了用户隔离。用户间要互通，需要在关联了 VLAN 的接口上启动 VLAN 内的静态 ARP 功能。

背景信息

在设备上同时配置静态 ARP 和 VRRP 时，不能将 VLANIF 接口下所配置的 VRRP 备份组的虚拟 IP 地址作为该静态 ARP 表项中的 IP 地址，否则会生成错误的主机路由，影响正常转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令，配置 VLAN 内的静态 ARP 表项。

版权所有 © 华为技术有限公司

配置 VLAN 内的静态 ARP 表项时，请根据实际情况执行以下配置：

- 执行命令 **arp static** *ip-address mac-address* [**vid** *vlan-id* **interface** *interface-type interface-number*]。

  配置静态 ARP 表项时如果只配置 IP 地址和 MAC 地址，不指定 VLAN ID 和 ARP 报文的出接口，系统会自动选择出接口；如果指定了 VLAN ID 和 ARP 报文的出接口，系统会按照配置的出接口转发报文。

  如果 VLAN 对应的接口绑定了 VPN，设备会对这条静态 ARP 表项进行自动关联，把相应的 VPN 关联到该表项中。该条命令适用于“基于端口划分的 VLAN”。

说明

静态 ARP 表项在交换机正常工作时一直有效。

----结束

配置 VPN 实例内的静态 ARP 表项

当需要实现 VPN 实例内的设备通过二层互相访问时，可以配置 VPN 实例内的静态 ARP。

背景信息

在设备上同时配置静态 ARP 和 VRRP 时，不能将 VLANIF 接口下所配置的 VRRP 备份组的虚拟 IP 地址作为该静态 ARP 表项中的 IP 地址，否则会生成错误的主机路由，影响正常转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name*，配置 VPN 实例内的静态 ARP 表项。

说明

静态 ARP 表项在交换机正常工作时一直有效。

----结束

检查配置结果

可以查看静态 ARP 的配置信息。

前提条件

已经完成 ARP 功能的所有配置。

操作步骤

- 使用 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令基于 VPN 实例查看 ARP 映射表。
- 使用 **display arp statistics** { **all** }命令查看 ARP 表项的统计信息。

----结束

版权所有 © 华为技术有限公司

4.2.4 优化动态 ARP

动态 ARP 是指系统自动进行 IP 地址到以太网 MAC 地址的解析。

建立配置任务

介绍优化动态 ARP 的应用环境、前置任务、数据准备和配置过程。

应用环境

建立动态 ARP 是主机和交换机本身就具有的功能。不需要使用命令启动此功能，但可以调整动态 ARP 动作的一些参数。

前置任务

无

数据准备

优化动态 ARP 之前，需准备以下数据。

序号	数据
1	动态 ARP 表项的老化探测次数
2	动态 ARP 表项的老化超时时间

调整动态 ARP 的老化参数

当设备需要频繁更新 ARP 表项时，可以将 ARP 表项的老化超时时间调整小、将 ARP 表项的老化探测次调整大、将 ARP 表项的老化探测时间间隔调整小。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **arp detect-times** *detect-times*，设置动态 ARP 表项的老化探测次数。

步骤 4 执行命令 **arp expire-time** *expire-time*，设置动态 ARP 表项的老化超时时间。

缺省情况下，动态 ARP 表项的老化探测次数为 3，老化超时时间为 1200 秒，即 20 分钟。

步骤 5 执行命令 **arp detect-mode unicast**，设置接口以单播方式发送 ARP 老化探测报文。

缺省情况下，接口以广播方式发送 ARP 老化探测报文。

----结束

版权所有 © 华为技术有限公司

使能 ARP 抑制功能

系统在同一时间内接收到大量源 IP 地址相同的 ARP 报文时，需要对 ARP 表项进行重复更新。为了维护系统性能，可以启动 ARP 抑制功能，系统将对 ARP 报文只应答，不更新。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp-suppress enable**，使能当前设备上的 ARP 抑制功能。

----结束

使能二层拓扑探测功能

使能二层拓扑探测功能后，当二层接口状态由 Down 变为 Up 时，系统更新所有该二层口所属 VLAN 对应的 ARP 表项。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **l2-topology detect enable**，使能二层拓扑探测功能。

缺省情况下，系统不使能二层拓扑探测功能。

----结束

检查配置结果

可以查看动态 ARP 的配置信息。

前提条件

已经完成 ARP 功能的所有配置。

操作步骤

- 使用 **display arp interface** *interface-type interface-number* 命令基于接口查看 ARP 映射表。
- 使用 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令基于 VPN 实例查看 ARP 映射表。
- 使用 **display arp statistics** { **all** }命令查看 ARP 表项的统计信息。

----结束

4.2.5 配置路由式 Proxy ARP

代理 ARP 的功能就是使 IP 地址属于同一网段却不属于同一物理网络的设备能够相互通信。

版权所有 © 华为技术有限公司

建立配置任务

介绍配置路由式 Proxy ARP 的应用环境、前置任务、数据准备和配置过程。

应用环境

一个企业的 2 个物理网络，属于同一 IP 网络的不同子网，中间使用交换机分隔。为了使这两个物理网络实现互通，需要在交换机与物理网络连接的接口上启动 Proxy ARP 功能。

各子网中的主机 IP 地址的网络号应一致，主机上不需要配置缺省网关。

前置任务

在配置路由式 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up

数据准备

在配置路由式 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动路由式 Proxy ARP 的接口编号
2	启动路由式 Proxy ARP 的接口 IP 地址

配置接口的 IP 地址

在启动路由式 Proxy ARP 的接口上配置的 IP 地址应该与该接口所连接的局域网中主机的 IP 地址处于同一网段。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

AC6605 仅支持在 VLANIF 接口上使能路由式 Proxy ARP。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口 IP 地址。

在启动路由式 Proxy ARP 的接口上配置的 IP 地址应该与该接口所连接的局域网中主机的 IP 地址处于同一网段。

----结束

配置路由式 Proxy ARP 功能

实现同一 IP 网络内不同子网的互通，需配置路由式 Proxy ARP 功能。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **arp-proxy enable**，使能接口的路由式 Proxy ARP 功能。

缺省情况下，关闭接口的路由式 Proxy ARP 功能。

在交换机上使能路由式 Proxy ARP 后，主机应该减小 ARP 老化时间，使无效的 ARP 项尽快失效，减少发给交换机不能转发的报文。

----结束

检查配置结果

可以查看路由式 Proxy ARP 的配置信息。

前提条件

已经完成路由式 Proxy ARP 功能的所有配置。

操作步骤

- 使用 **display arp interface** *interface-type interface-number* 命令基于接口查看 ARP 映射表。
- 使用 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令基于 VPN 实例查看 ARP 映射表。
- 使用 **display arp statistics** 命令查看 ARP 表项的统计信息。

----结束

4.2.6 配置 VLAN 内 Proxy ARP

实现了同一 VLAN 内，被隔离主机之间的互通。

建立配置任务

介绍配置 VLAN 内 Proxy ARP 的应用环境、前置任务、数据准备和配置过程。

应用环境

如果两个用户属于相同的 VLAN，但 VLAN 内配置了用户隔离。用户间要互通，需要在关联了 VLAN 的接口上启动 VLAN 内 Proxy ARP 功能。

前置任务

在配置 VLAN 内 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置 VLAN
- 配置 VLAN 内用户隔离

版权所有 © 华为技术有限公司

数据准备

在配置 VLAN 内 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动 VLAN 内 Proxy ARP 的接口编号
2	启动 VLAN 内 Proxy ARP 的接口 IP 地址
3	启动 VLAN 内 Proxy ARP 的接口关联的 VLAN ID

配置接口的 IP 地址

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

AC6605 仅支持在 VLANIF 接口上使能 VLAN 内 Proxy ARP。

步骤 3 执行 **ip address** *ip-address* { *mask* | *mask-length* }命令，配置接口的 IP 地址。

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

----结束

使能 VLAN 内 Proxy ARP

需要在关联了 VLAN 的接口上启动 VLAN 内 Proxy ARP 功能，实现相同 VLAN 内被隔离的用户间互通。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行 **arp-proxy inner-sub-vlan-proxy enable** 命令，使能 VLAN 内 Proxy ARP。

----结束

检查配置结果

可以查看 VLAN 内 Proxy ARP 的配置信息。

前提条件

已经完成 VLAN 内 Proxy ARP 功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 在任意视图下执行 **display arp interface** *interface-type interface-number* 命令，基于接口了解 ARP 的运行情况。
- 使用 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令基于 VPN 实例查看 ARP 映射表。
- 使用 **display arp statistics** 命令查看 ARP 表项的统计信息。

----结束

4.2.7 配置 VLAN 间 Proxy ARP

实现了不同 VLAN 内，主机之间的互通。

建立配置任务

介绍配置 VLAN 间 Proxy ARP 的应用环境、前置任务、数据准备和配置过程。

应用环境

如果两个用户属于不同的 VLAN，用户间要互通，需要在关联了 VLAN 的子接口上启动 VLAN 间 Proxy ARP 功能。

各 VLAN 中的主机的 IP 地址应在同一网段。

前置任务

在配置 VLAN 间 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置 VLAN 聚合

数据准备

在配置 VLAN 间 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动 VLAN 间 Proxy ARP 的接口编号
2	启动 VLAN 间 Proxy ARP 的接口 IP 地址
3	启动 VLAN 间 Proxy ARP 的接口关联的 VLAN ID

配置接口的 IP 地址

在接口上配置的 IP 地址应该与该接口所关联的所有 VLAN 中的用户 IP 地址在同一网段。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

AC6605 仅支持在 VLANIF 接口上使能 VLAN 间 Proxy ARP。

步骤 3 执行 **ip address** *ip-address* { *mask* | *mask-length* }命令，配置接口的 IP 地址。

在接口上配置的 IP 地址应该与该接口所关联的所有 VLAN 中的用户 IP 地址在同一网段。

----结束

使能 VLAN 间 Proxy ARP

需要在 VLANIF 接口上启动 VLAN 间 Proxy ARP 功能，实现属于不同 VLAN 的用户间的互通。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行 **arp-proxy inter-sub-vlan-proxy enable** 命令，使能 VLAN 间 Proxy ARP。

----结束

检查配置结果

可以查看 VLAN 间 Proxy ARP 的配置信息。

前提条件

已经完成 VLAN 间 Proxy ARP 功能的所有配置。

操作步骤

- 在任意视图下执行 **display arp interface** *interface-type interface-number* 命令，基于接口了解 ARP 的运行情况。
- 使用 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令基于 VPN 实例查看 ARP 映射表。
- 使用 **display arp statistics** 命令查看 ARP 表项的统计信息。

----结束

4.2.8 维护 ARP

维护 ARP 包括清除 ARP 统计信息、监控 ARP 运行状况。

清除 ARP 表项

介绍了使用 reset 命令清除 ARP 表项。

版权所有 © 华为技术有限公司

背景信息

注意

- 清除 ARP 表项后，将取消 IP 地址和 MAC 地址的映射关系，可能导致无法访问某些节点。清除前请务必仔细确认。
- 清除静态 ARP 表项后，静态 ARP 表项将无法恢复，清除前请务必仔细确认。

操作步骤

步骤 1 在确认需要清除 ARP 映射表中的 ARP 项后，请在用户视图下执行 **reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }命令。

----结束

监控 ARP 运行状况

介绍了使用 display 命令监控 ARP 运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 ARP 的运行情况。

操作步骤

- 在任意视图下执行 **display arp interface** *interface-type interface-number* 命令，基于接口了解 ARP 的运行情况。
- 在任意视图下执行 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**]命令，基于 VPN 实例了解 ARP 的运行情况。

----结束

调试 ARP

介绍了使用 debugging 命令调试 ARP。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。尤其当 CPU 占用率接近 100%时，打开 arp 模块的 debug 开关可能导致单板复位，请慎用。

在 ARP 运行出现故障时，请在用户视图下执行下面的 **debugging** 命令对 ARP 进行调试，查看调试信息，定位故障并分析故障原因。

版权所有 © 华为技术有限公司

打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南-系统管理》中信息中心的内容。有关 **debugging** 命令的解释请参见《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 在用户视图下执行 **debugging arp packet** [**interface** *interface-type interface-number*] 命令，调试 ARP。
- 在用户视图下执行 **debugging arp-proxy** [**inner-sub-vlan-proxy** | **inter-sub-vlan-proxy**] [**interface** *interface-type interface-number*]命令，调试 Proxy ARP。
- 在用户视图下执行 **debugging arp process** [**interface** *interface-type interface-number*] 命令，调试 ARP 报文的处理过程。

----结束

4.2.9 配置举例

举例说明静态 ARP、路由式 ARP、VLAN 内 Proxy ARP、VLAN 间 Proxy ARP、ARP 二层拓扑探测的配置。

配置 ARP 示例

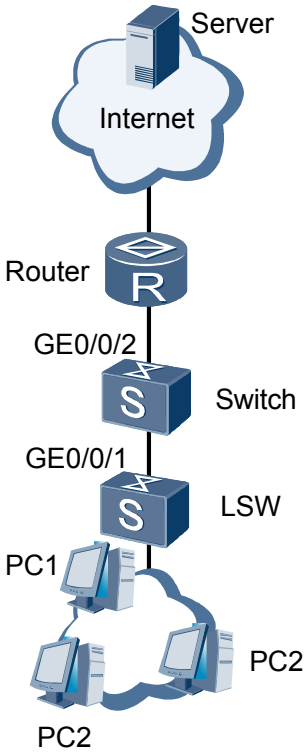
组网需求

如图 4-2 所示，Switch 的接口 GE0/0/1 通过 LAN Switch（即 LSW）连接主机，接口 GE0/0/2 通过路由器 Router 连接 Server。要求：

- GE0/0/1 属于 VLAN2，GE0/0/2 属于 VLAN3。
- 为了适应网络的快速变化，保证报文的正确转发，在 Switch 的接口 VLANIF2 上配置动态 ARP 的参数。
- 为了保证 Server 的安全性，防止非法 ARP 报文的侵入，在 Switch 的接口 GE0/0/2 上增加一个静态 ARP 表项，Router 的 IP 地址为 10.2.2.3，对应的 MAC 地址为 00e0-fc01-0000。

版权所有 © 华为技术有限公司

图 4-2 配置 ARP 组网图



配置思路

ARP 的配置思路如下：

1. 创建 VLAN，并将接口加入到 VLAN 中。
2. 配置用户侧 VLANIF 接口的动态 ARP 的参数。
3. 配置静态 ARP 表项。

数据准备

为完成此配置示例，需准备如下的数据：

- 接口 GE0/0/1 属于 VLAN2，接口 GE0/0/2 属于 VLAN3。
- 接口 VLANIF2 的 IP 地址为 2.2.2.2，子网掩码为 255.255.255.0。ARP 表项老化时间为 60 秒，老化探测次数为 2 次。
- 接口 VLANIF3 的 IP 地址为 10.2.2.2，子网掩码为 255.255.255.0。
- Router 与 Switch 对接的接口 IP 地址为 10.2.2.3，子网掩码为 255.255.255.0，对应的 MAC 地址为 00e0-fc01-0000。

操作步骤

步骤 1 创建 VLAN，并将接口加入到 VLAN 中。

创建 VLAN2 和 VLAN3。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] vlan batch 2 3
```

将接口 GE0/0/1 加入 VLAN2 中，接口 GE0/0/2 加入 VLAN3 中。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid tagged vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid tagged vlan 3
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置 VLANIF 接口的动态 ARP 的参数。

创建接口 VLANIF2。

```
[Quidway] interface vlanif 2
```

配置接口 VLANIF2 的 IP 地址。

```
[Quidway-Vlanif2] ip address 2.2.2.2 255.255.255.0
```

配置 ARP 表项老化时间为 60 秒。

```
[Quidway-Vlanif2] arp expire-time 60
```

配置 ARP 表项老化探测次数为 2 次。

```
[Quidway-Vlanif2] arp detect-times 2
[Quidway-Vlanif2] quit
```

创建接口 VLANIF3。

```
[Quidway] interface vlanif 3
```

配置接口 VLANIF3 的 IP 地址。

```
[Quidway-Vlanif3] ip address 10.2.2.2 255.255.255.0
[Quidway-Vlanif3] quit
```

步骤 3 配置静态 ARP 表项。

配置一条静态 ARP 表项：IP 地址为 10.2.2.3，对应的 MAC 地址为 00e0-fc01-0000，VLAN 编号为 3，出接口为 GE0/0/2。

```
[Quidway] arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface gigabitethernet 0/0/2
[Quidway] quit
```

步骤 4 检查配置结果。

执行命令 **display current-configuration**，查看表项老化时间、老化探测次数和 ARP 映射表信息。

```
<Quidway> display current-configuration | include arp
 arp expire-time 60
 arp detect-times 2
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface GigabitEthernet0/0/2
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
```


版权所有 © 华为技术有限公司

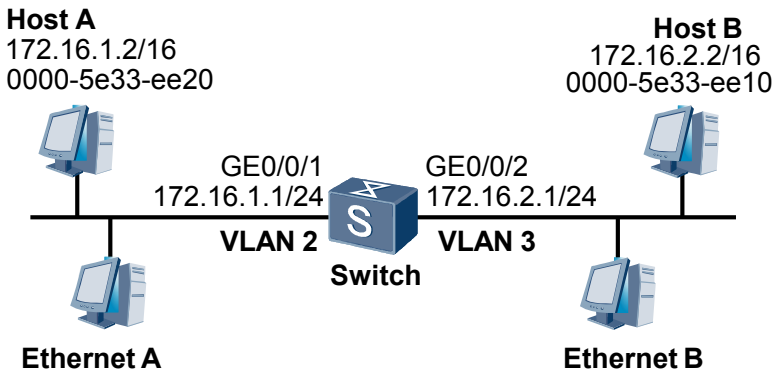
```
vlan batch 2 to 3
#
interface Vlanif2
 ip address 2.2.2.2 255.255.255.0
 arp expire-time 60
 arp detect-times 2
#
interface Vlanif3
 ip address 10.2.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 2
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 3
#
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface GigabitEthernet0/0/2
#
return
```

配置路由式 Proxy ARP 示例

组网需求

如图 4-3 所示，Switch 的两个以太网接口 GE0/0/1 和 GE0/0/2 分别连接一个局域网，两个局域网的网段均为 172.16.0.0/16。两台计算机 HostA 和 HostB 没有配置默认网关，要求在 Switch 上配置路由式 Proxy ARP，使分处在两个局域网的主机能互通。

图 4-3 配置路由式 Proxy ARP 组网图



配置思路

路由式 Proxy ARP 的配置思路如下：

1. 配置接口的 IP 地址
2. 在接口使能路由式 Proxy ARP 功能

数据准备

为完成此配置举例，需要准备如下数据：

- 相关接口的 IP 地址

版权所有 © 华为技术有限公司

- 主机的 IP 地址

操作步骤

步骤 1 创建 VLAN2，并将 GE0/0/1 加入到 VLAN 中。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 2
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 创建并配置接口 VLANIF2。

```
[Quidway]  interface vlanif 2
[Quidway-Vlanif2] ip address 172.16.1.1 255.255.255.0
```

步骤 3 在 VLANIF2 上使能路由式 Proxy ARP 功能。

```
[Quidway-Vlanif2] arp-proxy enable
[Quidway-Vlanif2] quit
```

步骤 4 创建 VLAN3，并将 GE0/0/2 加入到 VLAN 中。

```
[Quidway] vlan 3
[Quidway-vlan3] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 3
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 5 创建并配置接口 VLANIF3。

```
[Quidway] interface vlanif 3
[Quidway-Vlanif3] ip address 172.16.2.1 255.255.255.0
```

步骤 6 在 VLANIF3 上使能路由式 Proxy ARP 功能。

```
[Quidway-Vlanif3] arp-proxy enable
[Quidway-Vlanif3] quit
```

步骤 7 配置主机

配置主机 HostA 的 IP 地址为 172.16.1.2/16。

配置主机 HostB 的 IP 地址为 172.16.2.2/16。

步骤 8 验证配置结果

主机 HostA 上 ping 主机 HostB，可以通。

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
interface Vlanif2
 ip address 172.16.1.1 255.255.255.0
 arp-proxy enable
#
interface Vlanif3
```


版权所有 © 华为技术有限公司

```
 ip address 172.16.2.1 255.255.255.0
 arp-proxy enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 3
#
return
```

配置 VLAN 内 Proxy ARP 示例

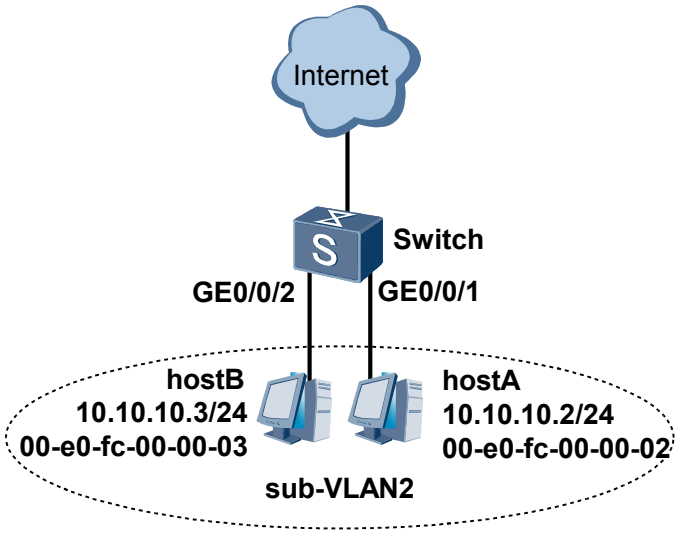
组网需求

如图 4-4 所示，Switch 的接口 GE0/0/2 和 GE0/0/1 属于同一个 sub-VLAN2。该 sub-VLAN 属于 super-VLAN3。要求：

- 属于同一 VLAN2 的两台主机 hostA 和 hostB 之间二层隔离。
- hostA 和 hostB 之间通过 VLAN 内 Proxy ARP 实现三层互通。

Super-VLAN 的 VLANIF 接口的 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0。

图 4-4 配置 VLAN 内 Proxy ARP 组网图



配置思路

VLAN 内 Proxy ARP 的配置思路如下：

1. 创建和配置 Super-VLAN 和 Sub-VLAN。
2. 将接口加入到从 Sub-VLAN 中。
3. 创建 Super-VLAN 的 VLANIF 接口并配置其 IP 地址。
4. 在 Super-VLAN 的 VLANIF 接口使能 VLAN 内 Proxy ARP 功能。

版权所有 © 华为技术有限公司

数据准备

为完成此配置示例，需准备如下的数据：

- Super-VLAN 和 Sub-VLAN 的 VLANID。
- 接口 GE0/0/2 和 GE0/0/1 属于 Sub-VLAN2。
- Super-VLAN 的接口 VLANIF3 的 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0。

操作步骤

步骤 1 配置 Super-VLAN 和 Sub-VLAN。

配置 Sub-VLAN2。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-Vlanif2] quit
```

使能 GE0/0/1 和 GE0/0/2 端口隔离功能。

```
[Quidway] port-isolate mode l2
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port-isolate enable
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port-isolate enable
[Quidway-GigabitEthernet0/0/2] quit
```

将 GE0/0/1 和 GE0/0/2 加入到 Sub-VLAN2 中。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

配置 Super-VLAN3，并将 Sub-VLAN2 增加到 Super-VLAN 中。

```
[Quidway] vlan 3
[Quidway-vlan3] aggregate-vlan
[Quidway-vlan3] access-vlan 2
[Quidway-vlan3] quit
```

步骤 2 创建和配置接口 VLANIF3。

创建接口 VLANIF3。

```
[Quidway] interface vlanif 3
```

配置接口 VLANIF3 的 IP 地址。

```
[Quidway-Vlanif3] ip address 10.10.10.1 24
```

步骤 3 在接口 VLANIF3 启动 VLAN 内 Proxy ARP。

```
[Quidway-Vlanif3] arp-proxy inner-sub-vlan-proxy enable
[Quidway-Vlanif3] quit
```

步骤 4 检查配置结果。

执行命令 **display current-configuration**，查看 Super-VLAN、Sub-VLAN 以及 VLANIF 接口的相关配置。查询结果请见下面给出的配置文件。

执行命令 **display arp**，查看所有 ARP 表项。

```
<Quidway> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
```


版权所有 © 华为技术有限公司

```
                                          VLAN
--------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif3
10.10.10.2      00e0-fc00-0002  19        D-0         GE0/0/1
                                          2
10.10.10.3      00e0-fc00-0003  19        D-0         GE0/0/2
                                          2
--------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0    Interface:1
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
vlan 3
 aggregate-vlan
 access-vlan 2
#
interface Vlanif3
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inner-sub-vlan-proxy enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
 port-isolate enable group 1
#
return
```

配置 VLAN 间 Proxy ARP 示例

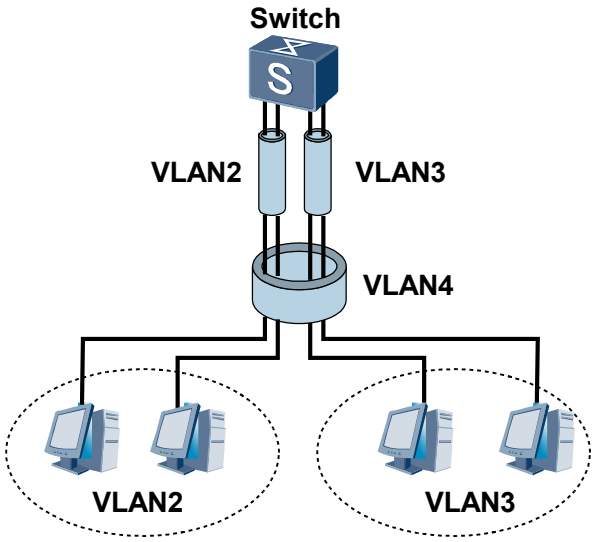
组网需求

如图 4-5 所示，VLAN2 和 VLAN3 组成 Super-VLAN4。要求：

- 作为 Sub-VLAN 的 VLAN2 和 VLAN3 内的主机之间不能互相 Ping 通。
- 配置 VLAN 间 Proxy ARP 后，VLAN2 和 VLAN3 内的主机之间可以互相 Ping 通。

版权所有 © 华为技术有限公司

图 4-5 配置 VLAN 间 Proxy ARP 组网图



配置思路

VLAN 间 Proxy ARP 的配置思路如下：

1. 配置 Super-VLAN 和 Sub-VLAN。
2. 将接口加入到从 Sub-VLAN 中。
3. 创建 Super-VLAN 的 VLANIF 接口并配置其 IP 地址。
4. 启动 VLAN 间 Proxy ARP。

数据准备

为完成此配置示例，需准备如下的数据：

- Super-VLAN 和 Sub-VLAN 的 VLANID。
- 接口 GE0/0/2 和 GE0/0/1 属于 Sub-VLAN2。
- 接口 GE0/0/4 和 GE0/0/3 属于 Sub-VLAN3。
- Super-VLAN 的接口 VLANIF4 的 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0。

操作步骤

步骤 1 配置 Super-VLAN 和 Sub-VLAN。

配置 Sub-VLAN2。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

将 GE0/0/1 和 GE0/0/2 加入到 Sub-VLAN2 中。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

配置 Sub-VLAN3。

```
<Quidway> system-view
[Quidway] vlan 3
[Quidway-vlan3] quit
```

将 GE0/0/3 和 GE0/0/4 加入到 Sub-VLAN3 中。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] port default vlan 3
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type access
[Quidway-GigabitEthernet0/0/4] port default vlan 3
[Quidway-GigabitEthernet0/0/4] quit
```

配置 Super-VLAN4，并将 Sub-VLAN2 增加到 Super-VLAN 中。

```
[Quidway] vlan 4
[Quidway-vlan4] aggregate-vlan
[Quidway-vlan4] access-vlan 2
[Quidway-vlan4] access-vlan 3
[Quidway-vlan4] quit
```

步骤 2 创建和配置接口 VLANIF4。

创建接口 VLANIF4。

```
[Quidway] interface vlanif 4
```

配置接口 VLANIF4 的 IP 地址。

```
[Quidway-Vlanif4] ip address 10.10.10.1 24
```

步骤 3 在接口 VLANIF4 启动 VLAN 间 Proxy ARP。

```
[Quidway-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
[Quidway-Vlanif4] quit
```

步骤 4 检查配置结果。

执行命令 **display current-configuration**，查看 Super-VLAN、Sub-VLAN 以及 VLANIF 接口的相关配置。查询结果请见下面给出的配置文件。

执行命令 **display arp**，查看所有 ARP 表项。

```
<Quidway> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN
------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif4
10.10.10.2      00e0-fc00-0002  19        D-0         GE0/0/1
                                          2/-
10.10.10.3      00e0-fc00-0003  19        D-0         GE0/0/2
                                          2/-
10.10.10.4      00e0-fc00-0004  19        D-0         GE0/0/3
                                          3/-
10.10.10.5      00e0-fc00-0005  19        D-0         GE0/0/4
                                          3/-
------------------------------------------------------------------------------
Total:5         Dynamic:4       Static:0    Interface:1
```

----结束

版权所有 © 华为技术有限公司

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
 #
interface Vlanif4
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 3
#
return
```

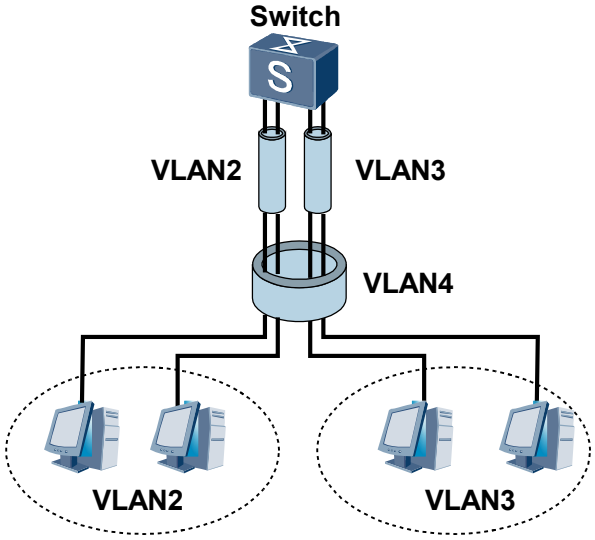
配置 VLAN 间 Proxy ARP 示例

组网需求

如图 4-6 所示，VLAN2 和 VLAN3 组成 Super-VLAN4。要求：

- 作为 Sub-VLAN 的 VLAN2 和 VLAN3 内的主机之间不能互相 Ping 通。
- 配置 VLAN 间 Proxy ARP 后，VLAN2 和 VLAN3 内的主机之间可以互相 Ping 通。

图 4-6 配置 VLAN 间 Proxy ARP 组网图



版权所有 © 华为技术有限公司

配置思路

VLAN 间 Proxy ARP 的配置思路如下：

1. 配置 Super-VLAN 和 Sub-VLAN。
2. 将接口加入到从 Sub-VLAN 中。
3. 创建 Super-VLAN 的 VLANIF 接口并配置其 IP 地址。
4. 启动 VLAN 间 Proxy ARP。

数据准备

为完成此配置示例，需准备如下的数据：

- Super-VLAN 和 Sub-VLAN 的 VLANID。
- 接口 GE0/0/2 和 GE0/0/1 属于 sub-VLAN2。
- 接口 GE0/0/4 和 GE0/0/3 属于 sub-VLAN3。
- Super-VLAN 的接口 VLANIF4 的 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0。

操作步骤

步骤 1 配置 Super-VLAN 和 Sub-VLAN。

配置 Sub-VLAN2。

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

将 GE0/0/1 和 GE0/0/2 加入到 Sub-VLAN2 中。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 2
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

配置 Sub-VLAN3。

```
<Quidway> system-view
[Quidway] vlan 3
[Quidway-vlan3] quit
```

将 GE0/0/3 和 GE0/0/4 加入到 Sub-VLAN3 中。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] port default vlan 3
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type access
[Quidway-GigabitEthernet0/0/4] port default vlan 3
[Quidway-GigabitEthernet0/0/4] quit
```

配置 Super-VLAN4，并将 Sub-VLAN2 增加到 Super-VLAN 中。

```
[Quidway] vlan 4
[Quidway-vlan4] aggregate-vlan
[Quidway-vlan4] access-vlan 2
```


版权所有 © 华为技术有限公司

```
[Quidway-vlan4] access-vlan 3
[Quidway-vlan4] quit
```

步骤 2 创建和配置接口 VLANIF4。

创建接口 VLANIF4。

```
[Quidway] interface vlanif 4
```

配置接口 VLANIF4 的 IP 地址。

```
[Quidway-Vlanif4] ip address 10.10.10.1 24
```

步骤 3 在接口 VLANIF4 启动 VLAN 间 Proxy ARP。

```
[Quidway-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
[Quidway-Vlanif4] quit
```

步骤 4 检查配置结果。

执行命令 **display current-configuration**，查看 Super-VLAN、Sub-VLAN 以及 VLANIF 接口的相关配置。查询结果请见下面给出的配置文件。

执行命令 **display arp**，查看所有 ARP 表项。

```
<Quidway> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif4
10.10.10.2      00e0-fc00-0002  19        D-0         GE0/0/1
                                          2
10.10.10.3      00e0-fc00-0003  19        D-0         GE0/0/2
                                          2
10.10.10.4      00e0-fc00-0004  19        D-0         GE0/0/3
                                          3
10.10.10.5      00e0-fc00-0005  19        D-0         GE0/0/4
                                          3
------------------------------------------------------------------------------
Total:5         Dynamic:4       Static:0    Interface:1
```

----结束

配置文件

以下仅给出 Switch 的配置文件。

```
#
 sysname Quidway
#
 vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
 #
interface Vlanif4
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
```


版权所有 © 华为技术有限公司

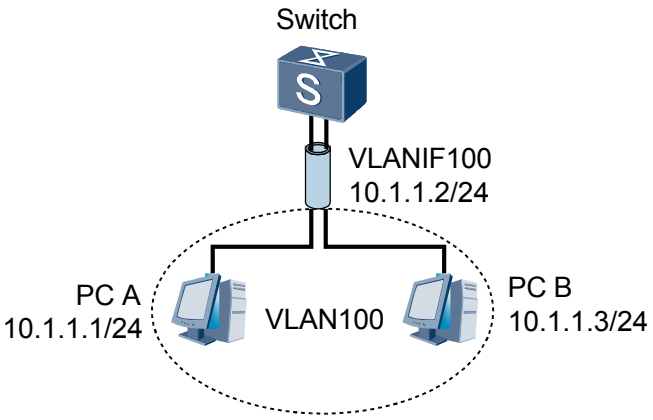
```
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 3
#
return
```

配置 ARP 二层拓扑探测示例

组网需求

如图 4-7 所示，两个 GE 接口以 default 方式加入 VLAN100，两个 GE 口所连主机的 IP 地址如图所示。

图 4-7 配置 ARP 二层拓扑探测示例



配置思路

采用如下的思路配置二层拓扑探测：

1. 配置两个 GE 接口以 default 方式加入 VLAN 100。
2. 使能二层拓扑探测功能，查看 ARP 表项的变化。

数据准备

完成此配置，需准备如下的数据：

- 要加入 VLAN 的接口类型和接口编号
- VLANIF 接口和 PC 的 IP 地址

操作步骤

步骤 1 创建 VLAN100，并配置 Switch 的两个 GE 接口以 default 方式加入 VLAN。

创建 VLAN100，配置 VLANIF 接口的 IP 地址。

```
<Quidway> system-view
[Quidway] vlan 100
```


版权所有 © 华为技术有限公司

```
[Quidway-vlan100] quit
[Quidway] interface vlanif 100
[Quidway-vlanif100] ip address 10.1.1.2 24
[Quidway-vlanif100] quit
```

配置 GE 接口以 default 方式加入 VLAN100。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 100
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 100
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 使能二层拓扑探测功能。

```
[Quidway] l2-topology detect enable
```

步骤 3 重启接口 GE0/0/1，并查看 ARP 表项及老化时间的变化。

查看 Switch 的 ARP 表项，可以看到 Switch 已经学习到了 PC 的 MAC 地址。

```
[Quidway] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M)  TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900             I -           Vlanif100
10.1.1.1        00e0-c01a-4901  20         D-0           GE0/0/1
10.1.1.3        00e0-de24-bf04  20         D-0           GE0/0/2
------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0    Interface:1
```

依次 **shutdown**、**undo shutdown** 接口 GE0/0/1，并查看 ARP 表项的老化时间。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] shutdown
[Quidway-GigabitEthernet0/0/1] undo shutdown
[Quidway-GigabitEthernet0/0/1] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900             I -           Vlanif100
10.1.1.3        00e0-de24-bf04  0          D-0           GE0/0/2
------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

说明

由输出信息可以看到，GE0/0/1 被 shutdown 之后，从 GE0/0/1 学习到的 ARP 表项被删除。GE0/0/1 被 undo shutdown，接口状态重新变为 Up 后，从 GE0/0/2 学习到的 ARP 表项的老化时间变为 0。当老化时间变为 0 时，设备会发送 ARP 探测报文，更新 ARP 表项。

```
[Quidway-GigabitEthernet0/0/1] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900             I -           Vlanif100
10.1.1.3        00e0-de24-bf04  20         D-0           GE0/0/2
------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

说明

表项更新后，老化时间重新变为默认值 20（分钟）。

----结束

版权所有 © 华为技术有限公司

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
L2-topolgy detect enable
#
 vlan 100
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 100
#
return
```

4.3 DHCP 配置

DHCP 技术适用于各种网络，配置 DHCP 保证了网络中 IP 地址的合理分配，提高整个网络 IP 地址的使用率。

4.3.1 DHCP 概述

DHCP 是一种终端自动配置协议，客户端通过 DHCP 协议可获取一个合法的动态 IP 地址。

概述

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。

DHCP 协议以服务器/客户端（Server/Client）模式工作，DHCP 客户端向 DHCP 服务器动态地请求配置信息，DHCP 服务器可以很方便地为客户端动态发送配置信息。

早期的 DHCP 协议只适用于 DHCP 客户端和服务器处于同一个子网内的情况，不可以跨网段工作，这样就需要为每一个子网配置一个 DHCP 服务器，浪费资源。DHCP 中继的引入解决了这一问题。

定义

DHCP 服务器

DHCP Server 即 DHCP 服务器，负责客户端 IP 地址的分配。客户端向服务器发送配置申请报文（包括 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回携带相应配置信息的报文，请求报文和回应报文都采用 UDP 进行封装。

DHCP 中继

版权所有 © 华为技术有限公司

DHCP Relay 即 DHCP 中继，它是为解决服务器和客户端不在同一个网段而提出来的，它提供了对 DHCP 广播报文的透明传输功能，能够把 DHCP 客户端的广播报文透明地传送到其它网段的 DHCP 服务器上，同样能够把 DHCP 服务器端的广播报文透明地传送到其它网段的 DHCP客户端。

4.3.2 AC6605 支持的 DHCP 特性

AC6605 支持 DHCP 服务器和 DHCP 中继的功能。

AC6605 支持的 DHCP 特性主要应用场景如**表 4-1** 所示。

表 4-1 DHCP 主要应用场景

AC6605 支持的特性	场景
基于全局地址池的 DHCP 服务器	客户端和 DHCP 服务器处于相同网段或不同网段
基于接口地址池的 DHCP 服务器	客户端和 DHCP 服务器处于相同网段
DHCP 中继	客户端和 DHCP 服务器处于不同网段

AC6605 作为 DHCP 服务器

AC6605 支持作为 DHCP 服务器为上线用户分配 IP 地址。客户端向服务器发送配置申请报文（包括 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回携带相应配置信息的报文，请求报文和回应报文都采用 UDP 进行封装。

当 AC6605 作为 DHCP 服务器时，支持两种分配地址模式：通过 DHCP 全局地址池向客户端分配 IP 地址和通过 DHCP 接口地址池向客户端分配 IP 地址。

- DHCP 全局地址池模式：当接口收到 DHCP 客户端发来的 DHCP 报文时，将从本地 DHCP 服务器的全局地址池中分配地址。具体配置请参见 **4.3.3 配置基于全局地址池的 DHCP 服务器**。
- DHCP 接口地址池模式：当接口收到 DHCP 客户端发来的 DHCP 报文时，将会优先从本地 DHCP 服务器的接口地址池中分配地址；如果接口地址池中没有可供分配的地址，则会从包含该接口地址池网段的全局地址池中进行分配。具体配置请参见 **4.3.4 配置基于 VLANIF 接口地址池的 DHCP 服务器**。

说明

AC6605 还支持 DHCP Snooping 功能，DHCP Snooping 的配置方法，请参见《AC6605 无线接入控制器 配置指南-安全》。

AC6605 作为 DHCP 中继

AC6605 实现了 DHCP 中继功能，能够在处于不同子网间的 DHCP 客户端和服务器之间承担中继服务，将 DHCP 协议报文中继到跨网段的目的 DHCP 服务器（或客户端），于是许多网络上的 DHCP 客户端可以使用同一个 DHCP 服务器。这样，既节省开销又便于集中管理。

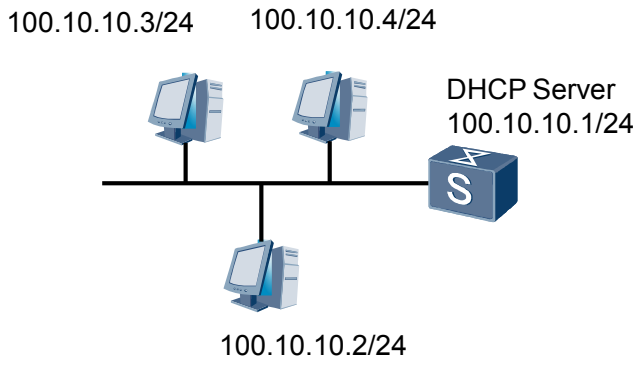
设备作为 DHCP 中继使能了 DHCP 服务后，接口收到 DHCP 客户端发来的 DHCP 报文时，DHCP 中继将报文转发给外部 DHCP 服务器，由外部服务器分配地址。中继模式的具体配置请参见 **4.3.5 配置 DHCP 中继**。

版权所有 © 华为技术有限公司

应用

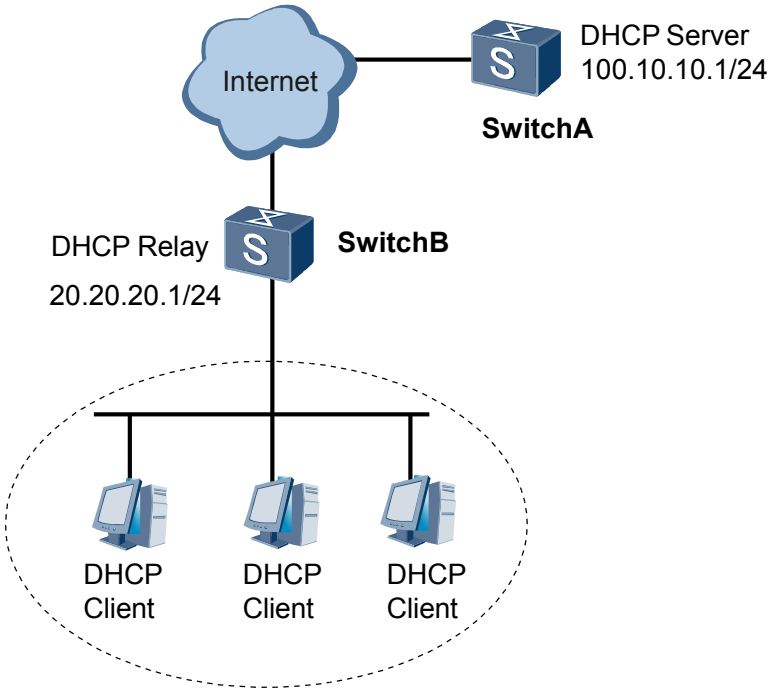
AC6605 作为 DHCP 服务器，当客户端和 DHCP 服务器处于相同网段时，DHCP 服务器可采用 DHCP 全局地址池或 DHCP 接口地址池任一种模式为客户端分配 IP 地址。

图 4-8 客户端和 DHCP 服务器处于同一网段组网图



AC6605 分别作为 DHCP 服务器和 DHCP 中继，当客户端和 DHCP 服务器处于不同网段时，DHCP 服务器只能采用 DHCP 全局地址池模式为客户端分配 IP 地址。

图 4-9 客户端和 DHCP 服务器处于不同网段组网图



4.3.3 配置基于全局地址池的 DHCP 服务器

配置基于全局地址池的 DHCP 服务器，服务器从该地址池中选择一个空闲的 IP 地址分配给客户端。

版权所有 © 华为技术有限公司

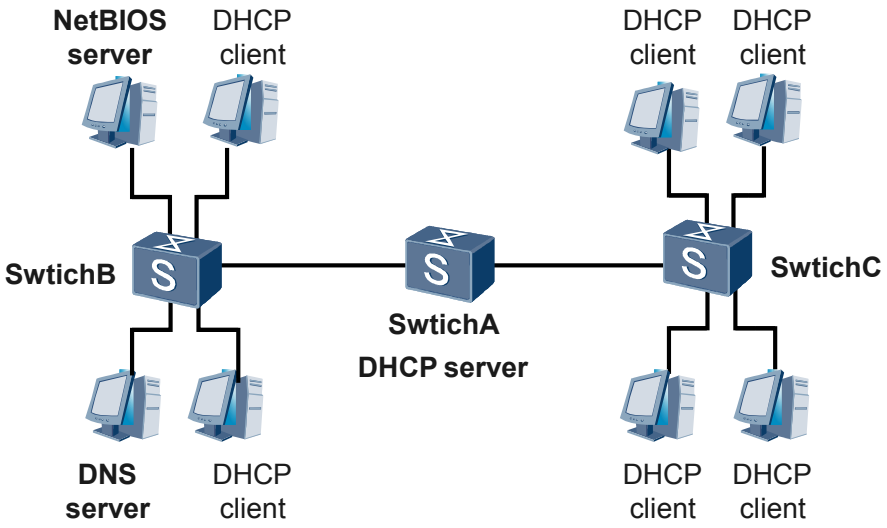
建立配置任务

在配置全局地址池的 DHCP 服务器前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在企业网网络中，如果网络中的计算机不能与分配 IP 地址的服务器直接相连，而要穿过其它网络设备。在这种情况下，为了让计算机能动态获取 IP 地址，通常要配置 AC6605 为基于全局地址池的 DHCP 服务器。如图 4-10 所示。

图 4-10 基于全局地址池的 IP 地址分配组网图



AC6605 应用于全局地址池的 DHCP 服务器时，通常与 DHCP 中继协同工作。

前置任务

在配置基于全局地址池的 DHCP 服务器之前，需完成以下任务：

- 保证 DHCP 客户端的和 AC6605 之间链路正常，能够通信
- 配置 DNS 服务器（根据实际需要，可选择配置）
- 配置 NetBIOS 服务器（根据实际需要，可选择配置）
- 配置 AC6605 到 DNS 服务器和 NetBIOS 服务器的路由（如果没有配置这两种服务器，则无需配置路由）
- 配置 DHCP 自定义选项（根据实际需要，可选择配置）

数据准备

在配置基于全局地址池的 DHCP 服务器之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	地址池的名字、IP 地址范围、租期、（可选）地址池中不参与自动分配的 IP 地址的范围、（可选）需要静态绑定的 IP 地址和 MAC 地址表项
2	DHCP 客户端的出口网关
3	（可选）DNS 服务器的 IP 地址以及 DHCP 客户端的域名
4	（可选）NetBIOS 服务器的 IP 地址以及 DHCP 客户端的 NetBIOS 节点类型
5	（可选）DHCP 自定义选项的编码以及对应的 ASCII 字符串、十六进制数字或 IP 地址

配置接口工作在全局地址池模式

当 DHCP 服务器的接口收到 DHCP 客户端发来的 DHCP 报文时，配置从本地 DHCP 服务器的全局地址池中分配 IP 地址。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ip address** *ip address* { *mask* | *mask-length*}，配置此 VLANIF 接口的 IP 地址。

配置了接口的 IP 地址后，此接口下的用户上线时，如果 DHCP 客户端和 AC6605 之间没有中继设备，AC6605 会选择和此 IP 地址在同一个网段的地址池来分配地址。

如果接口未配置 IP 地址，或者没有和接口地址在相同网段的地址池，用户无法上线。

如果 DHCP 客户端和 AC6605 之间还存在中继设备，AC6605 需解析收到的中继报文中的网关地址，如果网关地址匹配不到相应的地址池，则用户上线失败。

步骤 5 执行命令 **dhcp select global**，使能接口的 DHCP 服务功能，指定 DHCP 服务器从全局地址池分配地址。

----结束

配置 DHCP 全局地址池的地址分配方式

根据 DHCP 客户端的实际需要，可以选择采用静态地址绑定方式或动态地址分配方式，但不能同时对一个 DHCP 全局地址池的一个 IP 地址配置这两种方式。

背景信息

AC6605 上最多可以创建 128 个地址池，包括全局地址池和接口地址池，二者没有单独限制；动态地址分配需要指定用于分配的地址范围，而静态地址绑定则可以看作是只包

版权所有 © 华为技术有限公司

含一个地址的特殊的 DHCP 地址池。配置全局地址池的相关属性，包括地址范围、地址租期、不参与自动分配的 IP 地址以及静态绑定的 IP 地址。

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入全局地址池视图。

缺省情况下，AC6605 上没有创建任何全局地址池。

步骤 3 执行命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置地址池下的 IP 地址范围。

配置地址池网段时，同一地址池中只能配置一个地址段，通过掩码设定地址范围的大小，不能超出网关地址网段的范围。

步骤 4 执行命令 **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }，配置 IP 地址租期。

缺省情况下，IP 地址的租期为 1 天。

对于不同的地址池，DHCP 服务器可以指定不同的地址租用期限，但同一地址池中的地址都具有相同的期限。

步骤 5 （可选）执行命令 **excluded-ip-address** *start-ip-address* [*end-ip-address*]，配置地址池中不参与自动分配的 IP 地址。

有些地址分配给其他的服务，如分配给 DNS 服务器就不能再分配给客户端使用。可以执行 **excluded-ip-address** 命令配置地址池中不参与自动分配的 IP 地址。多次执行该命令，可以配置多个不参与自动分配的 IP 地址段。

步骤 6 （可选）执行命令 **static-bind ip-address** *ip-address* **mac-address** *mac-address*，将地址池中的 IP 地址与 MAC 地址绑定。

当一个用户需要固定的 IP 地址时，可以将地址池中没有在使用的 IP 地址与用户的 MAC 地址绑定。

步骤 7 执行命令 **gateway-list** *ip-address* &<1-8>，配置 DHCP 全局地址池的出口网关。

说明

为了对流量进行负载分担和提高网络的可靠性，可以配置多个出口网关。每个地址池最多可以配置 8 个网关地址，网关地址不能是子网广播地址。

配置 DHCP 服务器上 IP 地址池的出口网关时，此网关的 IP 地址和相邻 DHCP 中继的网关 IP 地址必须完全一致。

----结束

（可选）配置 DHCP 全局地址池的 DNS 服务

每个客户端都有各自的一个域名，为了使 DHCP 客户端之间成功通过域名访问，避免 DNS 服务器在域名解析时造成 IP 地址冲突，DHCP 服务器在为客户端分配 IP 地址的同时指定客户端使用的域名后缀。

背景信息

在 DHCP 服务器上，使用 **domain-name** 命令可以在每个全局地址池上指定客户端使用的域名后缀。在给客户端分配 IP 地址的同时，也将域名后缀发送给客户端。在客户端

版权所有 © 华为技术有限公司

进行域名解析时，用户只需要输入域名的部分字段，客户端会自动将输入的域名加上域名后缀进行解析。

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **domain-name** *domain-name*，配置分配给 DHCP 客户端的 DNS 域名后缀。

在 DHCP 服务器上，可以为每个地址池分别指定客户端使用的 DNS 域名后缀。配置了 DNS 域名后缀，也即指定了 DHCP 客户端可用的 DNS 域名服务器。

步骤 4 执行命令 **dns-list** *ip-address* &<1-8>，配置 DHCP 客户端使用的 DNS 服务器的 IP 地址。

为了对流量进行负载分担和提高网络的可靠性，可配置多个 DNS 服务器。每个地址池最多可以配置 8 个 DNS 服务器地址。

----结束

（可选）配置 DHCP 全局地址池的 NetBIOS 服务

对于使用 Windows Microsoft 操作系统的客户端，由 NetBIOS 服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

说明

NetBIOS：Network Basic Input Output System，网络基本输入/输出系统的简称。

DHCP 客户端使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种。

- b 类节点（b-node）：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。
- m 类节点（m-node）：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **nbns-list** *ip-address* &<1-8>，配置 DHCP 客户端的 NetBIOS 服务器地址。

版权所有 © 华为技术有限公司

每个地址池最多可以配置 8 个 NetBIOS 服务器地址。

步骤 4 执行命令 **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }，配置 DHCP 客户端的 NetBIOS 节点类型。

缺省情况下，不指定客户端的 NetBIOS 节点类型。

----结束

（可选）配置 DHCP 全局地址池自定义选项

随着 DHCP 的不断发展，新的可选配置项会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将新选项添加到 DHCP 服务器的属性列表中。

背景信息

如果用户在 DHCP 服务器端配置了 Option，DHCP 客户端在申请 IP 地址的时候，会通过服务器端回应的 DHCP 报文获得 Option 字段中的配置信息。

说明

常用的功能，如客户端的 DNS 服务、NetBIOS 服务、租期等，可以通过 Option 命令进行配置，但是以相关命令的配置为优先。如果相关命令没有配置，而配置了对应的 Option 选项，那么会取用 Option 命令配置的值。

相关命令如下：

- DNS 服务：**domain-name**、**dns-list**
- NetBIOS 服务：**nbns-list**、**netbios-type**
- 租期：**lease**

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* &<1-10> | **ip-address** *ip-address* &<1-8> }，配置 DHCP 自定义选项。

option 命令用于将指定选项内容通过服务器端回应的 DHCP 报文携带给客户端。使用该命令前，需要明确选项功能。DHCP 的知名选项，请参考 RFC2132。

----结束

（可选）配置防止 IP 地址重复分配功能

为防止 IP 地址重复分配导致地址冲突，AC6605 应用为 DHCP 服务器时为客户端分配地址前，需要先对该地址进行探测。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

地址探测是通过 **dhcp server ping** 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果在最长等待 Ping 响应的时间内没有得到应答，则继续发送 Ping 报文，直到发

版权所有 © 华为技术有限公司

送 Ping 包数量达到最大值，如果仍然没有收到应答，则认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址是唯一的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server ping packet** *number*，配置 AC6605 发送 Ping 包的最大数量。

缺省情况下，AC6605 发送 Ping 包的最大数量为 2。

步骤 3 执行命令 **dhcp server ping timeout** *milliseconds*，配置 AC6605 发送 Ping 包的最长等待响应时间。

缺省情况下，AC6605 等待 Ping 响应的最长时间为 500 毫秒。

----结束

（可选）配置 DHCP 数据保存功能

将当前的 DHCP 用户信息保存到 AC6605 的存储设备上，当 AC6605 发生故障时可以从存储设备中及时恢复数据。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

AC6605 作为 DHCP 服务器时，用户可以启用 DHCP 数据保存功能，定时将地址信息保存到存储设备中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server database enable**，使能 DHCP 地址池分配的 IP 地址信息保存到 Flash 的功能。

执行本命令后，系统将生成 lease.txt 和 conflict.txt 两个文件，存放在 Flash 的 DHCP 文件夹中，分别保存正常的地址租借信息和地址冲突信息。

步骤 3 执行命令 **dhcp server database write-delay** *interval*，配置数据保存时间间隔。

缺省情况下，未使能 DHCP 数据保存到 Flash 的功能。如果使能此功能，缺省情况下，每隔 7200 秒保存一次当前的 DHCP 数据，并覆盖之前的数据文件。

步骤 4 执行命令 **dhcp server database recover**，使能 DHCP 数据恢复功能。

使能 DHCP 数据恢复功能后，系统重启时将从 Flash 的文件中恢复 DHCP 数据。

----结束

检查配置结果

查看基于全局地址池的 DHCP 服务器的配置信息。

版权所有 © 华为技术有限公司

前提条件

已经完成基于全局地址池的 DHCP 服务器的所有配置。

操作步骤

- 使用命令 **display dhcp server statistics** 查看 DHCP 服务器的统计信息。
- 使用命令 **display ip pool name** *ip-pool-name* [*low-ip-address high-ip-address* | **all** | **expired** | **conflict** | **used**]查看已经配置的全局地址池信息。

----结束

任务示例

执行命令 **display dhcp server statistics** 查看 DHCP 服务器的统计信息。

```
<Quidway> display dhcp server statistics
Server Statistics:

 Client Request:             6
  Dhcp Discover:             1
  Dhcp Request:              4
  Dhcp Decline:              0
  Dhcp Release:              1
  Dhcp Inform:               0
 Server Reply:               4
  Dhcp Offer:                1
  Dhcp Ack:                  3
  Dhcp Nak:                  0
 Bad Messages:               0
```

执行命令 **display ip pool name** *ip-pool-name* 查看名称为“huawei”的 IP 地址池信息。

```
<Quidway> display ip pool name huawei
Pool-Name      : huawei
  Pool-No        : 2
  Lease          : 3 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-Server0    : 10.10.10.5
  DNS-Server1    : 10.10.10.6
  NBNS-Server0   : 20.20.20.5
  Netbios-type   : -
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.10.10.10
  Mask           : 255.255.255.0
  Vpn instance   : --
  ------------------------------------------------------------------------------
           Start              End  Total   Used   Idle(Expired)   Conflict Disable
  ------------------------------------------------------------------------------
       10.10.10.1     10.10.10.254    253      0    253          0        0
  ------------------------------------------------------------------------------
```

4.3.4 配置基于 VLANIF 接口地址池的 DHCP 服务器

配置基于 VLANIF 接口地址池的 DHCP 服务器，从这个接口上线的用户都从该地址池中分配地址。

建立配置任务

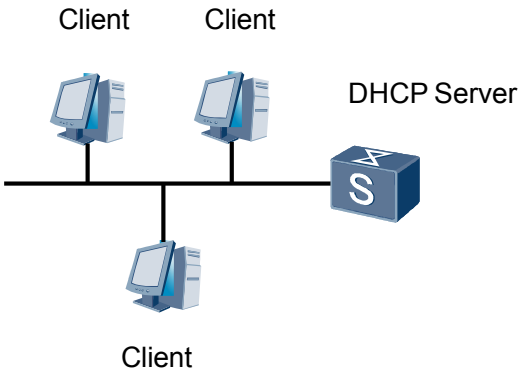
在配置接口地址池的 DHCP 服务器前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

如果网络中的计算机与分配 IP 地址的服务器处于同一网段。在这种情况下，为了让计算机能动态获取 IP 地址，通常要配置 AC6605 为基于接口地址池的 DHCP 服务器。如图 4-11 所示。

图 4-11 基于接口地址池的 IP 地址分配组网图



接口地址池优先于全局地址池分配地址。即如果接口上配置接口地址池，即使全局地址池已存在，客户端优先从接口地址池中获取地址。AC6605 的接口地址池只能在 VLANIF 接口上配置。

前置任务

在配置基于 VLANIF 接口地址池的 DHCP 服务器之前，需完成以下任务：

- 保证 DHCP 客户端的和 AC6605 之间链路正常，能够通信
- 配置 DNS 服务器（根据实际需要，可选择配置）
- 配置 NetBIOS 服务器（根据实际需要，可选择配置）
- 配置 AC6605 到 DNS 服务器和 NetBIOS 服务器的路由（如果没有配置这两种服务器，则无需配置路由）

数据准备

在配置基于 VLANIF 接口地址池的 DHCP 服务器之前，需准备以下数据。

序号	数据
1	使能地址池功能的 VLANIF 接口编号、IP 地址范围、租期、（可选）地址池中不参与自动分配的 IP 地址的范围、（可选）需要静态绑定的 IP 地址和 MAC 地址表项
2	（可选）DHCP 客户端的出口网关
3	（可选）DNS 服务器的 IP 地址以及 DHCP 客户端的域名
4	（可选）NetBIOS 服务器的 IP 地址以及 DHCP 客户端的 NetBIOS 节点类型

版权所有 © 华为技术有限公司

序号	数据
5	（可选）DHCP 自定义选项的编码以及对应的 ASCII 字符串、十六进制数字或 IP 地址

配置接口地址池的地址分配方式

根据客户端的实际需要，可以选择采用静态地址绑定方式或动态地址分配方式，但不能同时对一个 DHCP 全局地址池配置这两种方式。

背景信息

接口地址池优先于全局地址池分配地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

步骤 5 执行命令 **dhcp select interface**，配置设备采用接口地址池的 DHCP 服务器模式。

接口地址池的地址范围就是接口的 IP 地址所在的网段，且只在此接口下有效。

步骤 6 执行命令 **dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }，配置 IP 地址租期。

缺省情况下，IP 地址的租期为 1 天。

步骤 7 （可选）执行命令 **dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*]，配置地址池中不参与自动分配的 IP 地址。

有些地址分配给其他的服务，如分配给 DNS 服务器就不能再分配给客户端使用。可以执行该命令配置地址池中不参与自动分配的 IP 地址。多次执行该命令，可以配置多个不参与自动分配的 IP 地址段。

步骤 8 （可选）执行命令 **dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address*，将地址池中的 IP 地址与 MAC 地址绑定。

当一个用户需要固定的 IP 地址时，可以将地址池中没有在使用的 IP 地址与用户的 MAC 地址绑定。

----结束

（可选）配置 VLANIF 接口地址池的 DNS 服务

每个客户端都有各自的一个域名，为了使 DHCP 客户端之间成功通过域名访问，避免 DNS 服务器在域名解析时造成 IP 地址冲突，DHCP 服务器在为客户端分配 IP 地址的同时指定客户端使用的域名后缀。

版权所有 © 华为技术有限公司

背景信息

在 DHCP 服务器上，使用 **dhcp server domain-name** 命令可以在每个接口地址池上指定客户端使用的域名后缀。在给客户端分配 IP 地址的同时，也将域名后缀发送给客户端。在客户端进行域名解析时，用户只需要输入域名的部分字段，客户端会自动将输入的域名加上域名后缀进行解析。

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **dhcp server domain-name** *domain-name*，配置 DHCP 客户端可用的 DNS 域名后缀。

步骤 4 执行命令 **dhcp server dns-list** *ip-address* &<1-8>，为 DHCP 客户端指定 DNS 服务器的 IP 地址。

为了对流量进行负载分担和提高网络的可靠性，可配置多个 DNS 服务器。每个地址池最多可以配置 8 个 DNS 服务器地址。

----结束

（可选）配置 VLANIF 接口地址池的 NetBIOS 服务

对于使用 Windows Microsoft 操作系统的客户端，由 NetBIOS 服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

DHCP 客户端使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种。

- b 类节点（b-node）：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。
- m 类节点（m-node）：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **dhcp server nbns-list** *ip-address* &<1-8>，为 DHCP 客户端指定 NetBIOS 服务器的 IP 地址。

版权所有 © 华为技术有限公司

每个地址池最多可以配置 8 个 NetBIOS 服务器地址。

步骤 4 执行命令 **dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }，为 DHCP 客户端指定 NetBIOS 节点类型。

缺省情况下，不指定客户端的 NetBIOS 节点类型。

----结束

（可选）配置 VLANIF 接口地址池的 DHCP 自定义选项

随着 DHCP 的不断发展，新的可选配置项会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将新选项添加到 DHCP 服务器的属性列表中。

背景信息

如果用户在 DHCP 服务器端配置了 Option，DHCP 客户端在申请 IP 地址的时候，会通过服务器端回应的 DHCP 报文获得 Option 字段中的配置信息。

说明

常用的功能，如客户端的 DNS 服务、NetBIOS 服务、租期等，可以通过 Option 命令进行配置，但是以相关命令的配置为优先。如果相关命令没有配置，而配置了对应的 Option 选项，那么会取用 Option 命令配置的值。

相关命令如下：

- DNS 服务：**dhcp server domain-name**、**dhcp server dns-list**
- NetBIOS 服务：**dhcp server nbns-list**、**dhcp server netbios-type**
- 租期：**dhcp server lease**

请在作为 DHCP 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **dhcp server option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* &<1-10> | **ip-address** *ip-address* &<1-8> }，配置 DHCP 自定义选项。

dhcp server option 命令用于将指定选项内容通过服务器端回应的 DHCP 报文携带给客户端。使用该命令前，需要明确选项功能。DHCP 的知名选项，请参考 RFC2132。

----结束

（可选）配置防止 IP 地址重复分配功能

为防止 IP 地址重复分配导致地址冲突，AC6605 应用为 DHCP 服务器时为客户端分配地址前，需要先对该地址进行探测。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

地址探测是通过 **dhcp server ping** 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果在最长等待 Ping 响应的时间内没有得到应答，则继续发送 Ping 报文，直到发

版权所有 © 华为技术有限公司

送 Ping 包数量达到最大值，如果仍然没有收到应答，则认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址是唯一的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server ping packet** *number*，配置 AC6605 发送 Ping 包的最大数量。

缺省情况下，AC6605 发送 Ping 包的最大数量为 2。

步骤 3 执行命令 **dhcp server ping timeout** *milliseconds*，配置 AC6605 发送 Ping 包的最长等待响应时间。

缺省情况下，AC6605 等待 Ping 响应的最长时间为 500 毫秒。

----结束

（可选）配置 DHCP 数据保存功能

将当前的 DHCP 用户信息保存到 AC6605 的存储设备上，当 AC6605 发生故障时可以从存储设备中及时恢复数据。

背景信息

请在作为 DHCP 服务器的设备上进行以下配置。

AC6605 作为 DHCP 服务器时，用户可以启用 DHCP 数据保存功能，定时将地址信息保存到存储设备中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server database enable**，使能 DHCP 地址池分配的 IP 地址信息保存到 Flash 的功能。

执行本命令后，系统将生成 lease.txt 和 conflict.txt 两个文件，存放在 Flash 的 DHCP 文件夹中，分别保存正常的地址租借信息和地址冲突信息。

步骤 3 执行命令 **dhcp server database write-delay** *interval*，配置数据保存时间间隔。

缺省情况下，未使能 DHCP 数据保存到 Flash 的功能。如果使能此功能，缺省情况下，每隔 7200 秒保存一次当前的 DHCP 数据，并覆盖之前的数据文件。

步骤 4 执行命令 **dhcp server database recover**，使能 DHCP 数据恢复功能。

使能 DHCP 数据恢复功能后，系统重启时将从 Flash 的文件中恢复 DHCP 数据。

----结束

检查配置结果

查看基于 VLANIF 接口地址池的 DHCP 服务器的配置信息。

版权所有 © 华为技术有限公司

前提条件

已经完成基于 VLANIF 接口地址池的 DHCP 服务器的所有配置。

操作步骤

- 使用命令 **display dhcp server statistics** 查看 DHCP 服务器的统计信息。
- 使用命令 **display ip pool interface** *interface-name* [*start-ip-address high-ip-address* | **all** | **expired** | **conflict** | **used**]查看已经配置的接口地址池信息。

----结束

任务示例

执行命令 **display dhcp server statistics** 查看 DHCP 服务器的统计信息。

```
<Quidway> display dhcp server statistics
Server Statistics:

 Client Request:            6
  Dhcp Discover:            1
  Dhcp Request:             4
  Dhcp Decline:             0
  Dhcp Release:             1
  Dhcp Inform:              0
 Server Reply:              4
  Dhcp Offer:               1
  Dhcp Ack:                 3
  Dhcp Nak:                 0
 Bad Messages:              0
```

执行命令 **display ip pool interface** *ip-pool-name* 查看“VLANIF10”的接口地址池信息。

```
<Quidway> display ip pool interface vlanif10
Pool-name      : vlanif10
  Pool-No        : 2
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Interface       Status           : Unlocked
  Gateway-0      : 192.168.10.2
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
        Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
   192.168.10.1  192.168.10.254   253     0   253        0         0         0
 ------------------------------------------------------------------------------
```

4.3.5 配置 DHCP 中继

局域网内的客户端可以通过 DHCP 中继与其他子网的 DHCP 服务器通信，最终取得合法的 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

建立配置任务

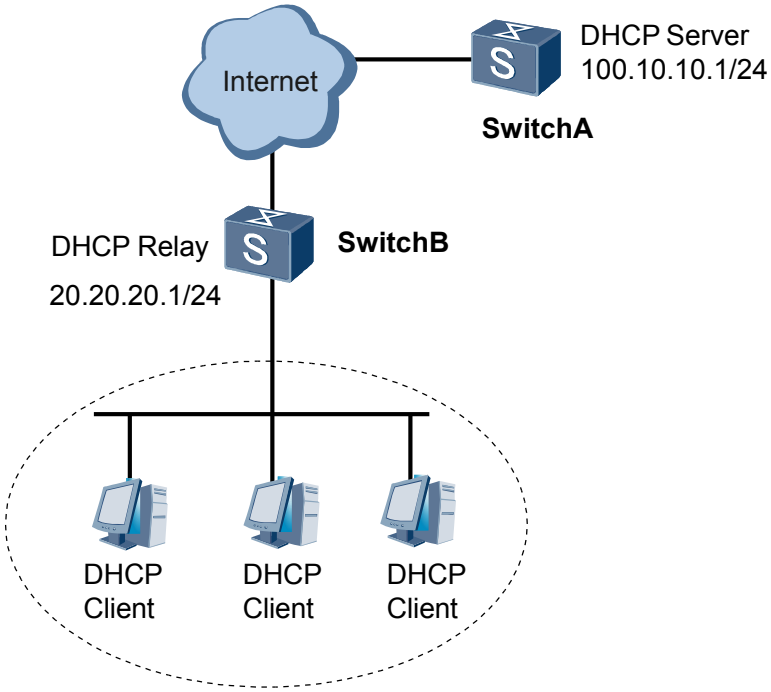
在配置 DHCP 中继前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

如果本地网络没有配置 DHCP 服务器，可以在 AC6605 上启动 DHCP 中继功能，从客户端来的 DHCP 请求可通过 DHCP 中继传到 DHCP 服务器，如图 4-12 所示。此时，为了保证客户端正常获取 IP 地址，该服务器必须是基于全局地址池的 DHCP 服务器，即服务器与 DHCP 中继相连的接口不允许再配置接口地址池。

图 4-12 DHCP 中继应用组网图



前置任务

在配置 DHCP 中继之前，需完成以下任务：

- 配置 DHCP 服务器
- 配置 AC6605 到 DHCP 服务器的路由

数据准备

在配置 DHCP 中继之前，需准备以下数据。

序号	数据
1	DHCP 服务器组的组名
2	DHCP 服务器组中的 DHCP 服务器 IP 地址
3	启动 DHCP 中继功能的接口编号及接口的 IP 地址

版权所有 © 华为技术有限公司

配置接口工作在 DHCP 中继模式

当客户端与 DHCP 服务器不在同一网段时，通过在 DHCP 中继设备转发客户端到 DHCP 服务器的请求。

背景信息

说明

DHCP 服务器和 DHCP 客户端之间的 DHCP 报文中继次数不能超过 16 次，否则 DHCP 报文将被丢弃。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能系统 DHCP 功能。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

说明

配置服务器上 IP 地址池的出口网关时，网关的 IP 地址和 DHCP 中继的网关 IP 地址必须完全一致。

步骤 5 执行命令 **dhcp select relay**，启动 VLANIF 接口的 DHCP 中继功能。

----结束

后续处理

AC6605 应用为 DHCP 中继时，从客户端来的 DHCP 请求报文可以通过 DHCP 中继传到 DHCP 服务器。使能 VLANIF 接口的中继功能后，还需要在接口下配置 DHCP 服务器的 IP 地址。AC6605 支持以下两种方法配置 DHCP 服务器的 IP 地址：

- **配置 DHCP 中继转发的目的服务器组**并**配置接口绑定 DHCP 服务器组**。
- 直接在 VLANIF 接口视图下执行命令 **dhcp relay server-ip** *ip-address*，配置 DHCP 中继所代理的 DHCP 服务器地址。

配置 DHCP 中继转发的目的服务器组

在通常情况下，一台 DHCP 中继会同时代理多台 DHCP 服务器，建立 DHCP 服务器组来统一管理该 DHCP 中继代理的 DHCP 服务器，从而在指定的 DHCP 服务器组中为通过 DHCP 中继接入的用户分配 IP 地址。

背景信息

请在作为 DHCP 中继的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server group** *group-name*，创建 DHCP 服务器组并进入 DHCP 服务器组视图。

版权所有 © 华为技术有限公司

全局最多可以配置 32 个 DHCP 服务器组。

步骤 3 执行命令 **dhcp-server** *ip-address* [*ip-address-index*]，向 DHCP 服务器组中添加 DHCP 服务器。

每个 DHCP 服务器组下最多可以配置 20 个 DHCP 服务器。不指定索引时，系统将自动分配一个空闲的索引。

步骤 4 （可选）执行命令 **vpn-instance** *vpn-instance-name*，将 DHCP 服务器组绑定 VPN 实例。

----结束

配置接口绑定 DHCP 服务器组

一个 DHCP 服务器组可以对应多个 VLANIF 接口。一个 VLANIF 接口下只能指定一个 DHCP 服务器组，即一个 VLANIF 接口下的 DHCP request 报文最多可以中继转发到一个 DHCP 服务器组。

背景信息

请在作为 DHCP 中继的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **dhcp relay server-select** *group-name*，指定 VLANIF 接口对应的 DHCP 服务器组。

也可执行 **dhcp relay server-ip** 命令添加 VLANIF 接口对应的服务器。

----结束

（可选）配置 DHCP 中继请求 DHCP 服务器释放客户端的 IP 地址

在某些情况下，比如强制某用户下线等，可能需要通过服务器手工释放客户端申请到的 IP 地址。

背景信息

如果 DHCP 服务器没有收到释放客户端的 IP 地址的请求，则客户端的 IP 地址租约到期后会继续重新申请 IP 地址；通过配置 DHCP 中继后，中继会主动向 DHCP 服务器发送 Release 报文，DHCP 服务器收到该报文后，将会释放指定 IP 地址的租约。

请在作为 DHCP 中继的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **dhcp relay release** *client-ip-address mac-address* [*server-ip-address*]，向 DHCP 服务器申请释放 DHCP 客户端已经获取到的 IP 地址。

版权所有 © 华为技术有限公司

- 在系统视图下，配置通过 AC6605 释放客户端的 IP 地址时：
  - 如果不指定 DHCP 服务器，则向所有配置为中继模式的接口所对应的 DHCP 服务器组中的 DHCP 服务器发送释放申请。
  - 如果指定了 DHCP 服务器的 IP 地址，则只向指定 DHCP 服务器发送释放申请。
- 在 VLANIF 接口视图下，配置通过 AC6605 释放客户端的 IP 地址时：
  - 如果不指定 DHCP 服务器，则向该接口所对应的 DHCP 服务器组中的所有 DHCP 服务器发送释放申请。
  - 如果指定了 DHCP 服务器的 IP 地址，则只向指定 DHCP 服务器发送释放申请。

----结束

检查配置结果

DHCP 中继配置成功后，通过命令查看 DHCP 中继的配置信息。

前提条件

已经完成 DHCP 中继功能的所有配置。

操作步骤

- 使用 **display dhcp relay** { **all** | **interface** *interface-type interface-number* }命令查看 VLANIF 接口配置的中继 DHCP 服务器组和服务器组对应的服务器。
- 使用 **display dhcp relay statistics** 命令查看 DHCP 中继统计信息。
- 使用 **display dhcp server group** *group-name* 命令查看 DHCP 服务器组的配置信息。

----结束

任务示例

执行命令 **display dhcp relay interface** *interface-type interface-number* 查看指定接口 VLANIF100 配置的 DHCP 服务器组及其包含的 DHCP 服务器信息。

```
<Quidway> display dhcp relay interface vlanif 100
DHCP relay agent running information of interface Vlanif100 :
 Server IP address [01] : 10.2.2.3
 Gateway address in use : 10.2.2.2
```

执行命令 **display dhcp relay statistics** 查看 DHCP 中继统计信息。

```
<Quidway> display dhcp relay statistics
The statistics of DHCP RELAY:
    DHCP packets received from clients    : 0
        DHCP DISCOVER packets received    : 0
        DHCP REQUEST packets received     : 0
        DHCP RELEASE packets received     : 0
        DHCP INFORM packets received      : 0
        DHCP DECLINE packets received     : 0
    DHCP packets sent to clients          : 0
        Unicast packets sent to clients   : 0
        Broadcast packets sent to clients : 0
    DHCP packets received from servers    : 0
        DHCP OFFER packets received       : 0
        DHCP ACK packets received         : 0
        DHCP NAK packets received         : 0
    DHCP packets sent to servers          : 0
    DHCP Bad packets received             : 0
```


版权所有 © 华为技术有限公司

执行命令 **display dhcp server group** *group-name* 查看 DHCP 服务器组 group1 的配置信息。

```
<Quidway> display dhcp server group group1
Group-name          : group1
    (0)  Server-IP    : 100.10.10.1
    (1)  Server-IP    : 100.10.10.2
    Gateway           : --
    VPN instance      : --
```

4.3.6 维护 DHCP

完成 DHCP 配置后，介绍如何清除 DHCP 统计信息以及如何监控 DHCP 运行状况。

清除 DHCP 的统计信息

在日常维护工作中，用户可以使用 reset 命令清除指定 DHCP Server 组的统计信息。

背景信息

注意

清除 DHCP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除 DHCP 服务器的统计信息后，请在用户视图下执行 **reset dhcp server statistics** 命令。
- 在确认需要清除 DHCP 中继的统计信息后，请在用户视图下执行 **reset dhcp relay statistics** 命令。

----结束

监控 DHCP 运行状况

在日常维护工作中，用户可以在任意视图下选择执行以下命令，了解 DHCP 的运行情况。

操作步骤

- 使用 **display dhcp relay** { **all** | **interface** *interface-type interface-number* }命令查看 VLANIF 接口配置的中继 DHCP 服务器组和服务器组对应的服务器。
- 使用 **display dhcp relay statistics** 命令查看 DHCP Relay 统计信息。
- 使用 **display dhcp server group** [*group-name*]命令查看 DHCP 服务器组成员的配置信息。

----结束

4.3.7 配置举例

DHCP 的配置举例包括组网需求、组网图、配置注意事项、配置思路和配置步骤。通过配置举例可以了解在各种网络中 DHCP 的应用实例。

版权所有 © 华为技术有限公司

同网段内配置基于全局地址池的 DHCP 服务器示例

客户端和 DHCP 服务器在同一网段，配置基于全局地址池的 DHCP 服务器给客户端分配 IP 地址的过程。

组网需求

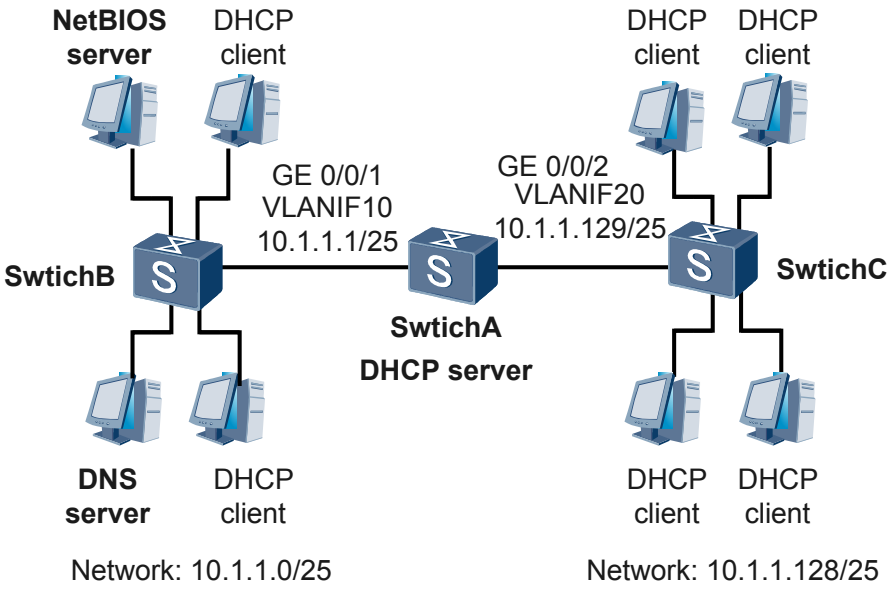
某公司有两个处于同一网络内的办公室，为了节省网络资源，两个办公室内的 PC 机由一台交换机作为服务器统一分配 IP 地址。

如图 4-13 所示，SwitchA 应用为 DHCP 服务器，SwitchB 和 SwitchC 为用户接入交换机。可在 SwitchA 上配置基于全局的地址池和接口的地址池，下面以全局地址池为例配置 SwitchA 为同一网段中的客户端动态分配 IP 地址。地址池网段 10.1.1.0/24 分为两个网段：10.1.1.0/25 和 10.1.1.128/25。DHCP 服务器两个 VLANIF 接口的 IP 地址分别为 10.1.1.1/25 和 10.1.1.129/25。

网段 10.1.1.0/25 内的 PC 机数量比较少且较位置固定，地址租用期限配置为 10 天，DNS 地址为 10.1.1.2，无 NetBIOS 地址，出口网关地址为 10.1.1.126。

网段 10.1.1.128/25 内的 PC 机数量较多但经常外借，地址租用期限配置为 2 天，DNS 地址为 10.1.1.2，NetBIOS 地址为 10.1.1.4，出口网关地址为 10.1.1.254。

图 4-13 配置基于全局地址池的 DHCP 服务器组网图



配置思路

DHCP 服务器的配置思路如下：

1. 启动公司网络内 SwitchA 的 DHCP 服务器功能。
2. 在 Switch 上创建地址池并配置地址池的相关属性，如地址池范围、出口网关、NetBIOS 地址、地址租用期限等，准备提供给客户端。

版权所有 © 华为技术有限公司

3. 配置 VLANIF 接口下本地 DHCP 服务器的地址分配方式，DHCP 服务器从全局地址池中给客户端分配 IP 地址。

数据准备

要完成此配置举例，需要准备以下数据：

SwitchA 上全局地址池编号及范围

说明

以下配置均在 SwitchA 上进行。

操作步骤

步骤 1 启动 DHCP 服务。

```
<Quidway> system-view
[Quidway] dhcp enable
```

步骤 2 创建地址池并配置相关属性。

配置 IP 地址池 1 的属性（地址池范围、DNS 地址、出口网关和地址池租期）。

```
[Quidway] ip pool 1
[Quidway-ip-pool-1] network 10.1.1.0 mask 255.255.255.128
[Quidway-ip-pool-1] dns-list 10.1.1.2
[Quidway-ip-pool-1] gateway-list 10.1.1.126
[Quidway-ip-pool-1] excluded-ip-address 10.1.1.2
[Quidway-ip-pool-1] excluded-ip-address 10.1.1.4
[Quidway-ip-pool-1] lease day 10
[Quidway-ip-pool-1] quit
```

配置 IP 地址池 2 的属性（地址池范围、DNS 地址、出口网关、NetBOIS 地址和地址池租期）

```
[Quidway] ip pool 2
[Quidway-ip-pool-2] network 10.1.1.128 mask 255.255.255.128
[Quidway-ip-pool-2] dns-list 10.1.1.2
[Quidway-ip-pool-2] nbns-list 10.1.1.4
[Quidway-ip-pool-2] gateway-list 10.1.1.254
[Quidway-ip-pool-2] lease day 2
[Quidway-ip-pool-2] quit
```

步骤 3 配置 VLANIF 接口下地址分配方式。

配置接口 GE 0/0/1 和 GE 0/0/2 分别加入相应的 VLAN。

```
[Quidway] vlan batch 10 20
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 20
[Quidway-GigabitEthernet0/0/2] quit
```

配置 VLANIF10 接口下的客户端从全局地址池中获取 IP 地址。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 255.255.255.128
[Quidway-Vlanif10] dhcp select global
[Quidway-Vlanif10] quit
```

配置 VLANIF20 接口下的客户端从全局地址池中获取 IP 地址。

版权所有 © 华为技术有限公司

```
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 10.1.1.129 255.255.255.128
[Quidway-Vlanif20] dhcp select global
[Quidway-Vlanif20] quit
```

步骤 4 验证配置结果。

在 Switch 上使用 **display ip pool** 命令用来查看 IP 地址池配置情况。

```
[Quidway] display ip pool
  ------------------------------------------------------------------------
  Pool-Name      : 2
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.254
  Mask           : 255.255.255.128
  Vpn instance   : --

  ------------------------------------------------------------------------
  Pool-Name      : 1
  Pool-No        : 2
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.126
  Mask           : 255.255.255.128
  Vpn instance   : --


   IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

配置文件

SwitchA 的配置文件

```
#
 sysname Quidway
#
 vlan batch 10 20
#
dhcp enable
#
 ip pool 1
 ip pool 2
#
ip pool 1
 gateway-list 10.1.1.126
 network 10.1.1.0 mask 255.255.255.128
 excluded-ip-address 10.1.1.2
 excluded-ip-address 10.1.1.4
 dns-list 10.1.1.2
 lease day 10 hour 0 minute 0
#
ip pool 2
 gateway-list 10.1.1.254
 network 10.1.1.128 mask 255.255.255.128
 dns-list 10.1.1.2
 nbns-list 10.1.1.4
 lease day 5 hour 0 minute 0
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.128
 dhcp select global
#
interface Vlanif20
```


版权所有 © 华为技术有限公司

```
 ip address 10.1.1.129 255.255.255.128
 dhcp select global
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

同网段内配置基于接口地址池的 DHCP 服务器示例

配置基于接口地址池的 DHCP 服务器解决在同一网络内的客户端从服务器获取 IP 地址的过程。

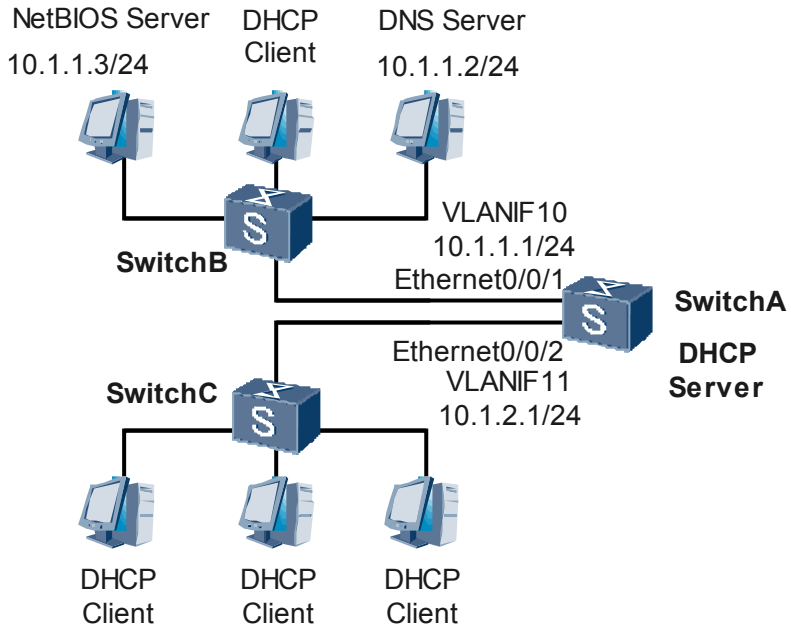
组网需求

某学校有两个处于不同网络的机房，要求用一台交换机设备分别为两个机房的 PC 机分配 IP 地址。

为了解决上述问题，可部署一台交换机连接两个机房的接入交换机，通过两个接口地址池为机房内的 PC 机分配 IP 地址。

如图 4-14 所示，SwitchA 应用为 DHCP Server，SwitchB 和 SwitchC 是用户接入交换机。要求在 SwitchA 上的 GE0/0/1 接口和 GE0/0/2 接口配置基于 VLANIF 接口地址池的 DHCP 服务器，为两个机房内的 PC 机分配 IP 地址。

图 4-14 配置基于 VLANIF 接口地址池的 DHCP 服务器组网图



配置思路

基于 VLANIF 接口地址池的 DHCP 服务器的配置思路如下：

版权所有 © 华为技术有限公司

1. 启动 SwitchA 的 DHCP 服务器功能。
2. 创建 VLANIF 接口，并配置 VLANIF 接口的 IP 地址，以确定接口地址池的 IP 地址网段。
3. 使能 VLANIF 接口地址池，DHCP 服务器从接口地址池中给机房内的 PC 机分配 IP 地址。
4. 配置地址池相关属性，包括 DNS 服务器地址、NetBOIS 服务器地址、地址租期等，准备提供给客户端。

数据准备

要完成此配置举例，需要准备以下数据：

- 接口的 IP 地址
- DNS 服务器地址、NetBOIS 服务器地址
- 地址池中地址租用期限

操作步骤

步骤 1 启动 DHCP 服务。

```
<Quidway> system-view
[Quidway] dhcp enable
```

步骤 2 配置接口加入 VLAN。

配置 GE 0/0/1 接口加入 VLAN10。

```
[Quidway] vlan batch 10 to 11
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
```

配置 GE 0/0/2 加接口入 VLAN11。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 11
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 11
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 3 配置 VLANIF 接口 IP 地址。

配置 VLANIF10 接口地址。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
[Quidway-Vlanif10] quit
```

配置 VLANIF11 接口地址。

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] ip address 10.1.2.1 24
[Quidway-Vlanif11] quit
```

步骤 4 使能 VLANIF 接口地址池。

配置 VLANIF10 接口下的客户端从接口地址池中获取 IP 地址。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp select interface
[Quidway-Vlanif10] quit
```

配置 VLANIF11 接口下的客户端从接口地址池中获取 IP 地址。

版权所有 © 华为技术有限公司

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] dhcp select interface
[Quidway-Vlanif11] quit
```

步骤 5 配置接口地址池的 DNS 服务和 NetBOIS 服务。

配置 VLANIF10 接口地址池下的 DNS 服务和 NetBOIS 服务。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp server domain-name huawei.com
[Quidway-Vlanif10] dhcp server dns-list 10.1.1.2
[Quidway-Vlanif10] dhcp server nbns-list 10.1.1.3
[Quidway-Vlanif10] dhcp server excluded-ip-address 10.1.1.2
[Quidway-Vlanif10] dhcp server excluded-ip-address 10.1.1.3
[Quidway-Vlanif10] dhcp server netbios-type b-node
```

步骤 6 配置接口地址池中地址租用期限。

配置 VLANIF10 接口地址租用期限为 30 天。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp server lease day 30
[Quidway-Vlanif10] quit
```

配置 VLANIF11 接口地址租用期限为 20 天。

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] dhcp server lease day 20
[Quidway-Vlanif11] quit
```

步骤 7 验证配置结果。

在 SwitchA 上使用 **display ip pool interface** 命令用来查看接口地址池配置情况。

```
[Quidway] display ip pool interface vlanif10
  Pool-Name      : vlanif10
  Pool-No        : 0
  Lease          : 30 Days 0 Hours 0 Minutes
  Domain-name    : huawei.com
  DNS-Server0    : 10.1.1.2
  NBNS-Server0   : 10.1.1.3
  Netbios-type   : b-node
  Position       : Interface       Status          : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
        Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
    10.1.1.1       10.1.1.254   253     0   251       0         0         2
 ------------------------------------------------------------------------------
[Quidway] display ip pool interface vlanif11
  Pool-Name      : vlanif11
  Pool-No        : 1
  Lease          : 20 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-Server0    : -
  NBNS-Server0   : -
  Netbios-type   : -
  Position       : Interface       Status          : Unlocked
  Gateway-0      : 10.1.2.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
        Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
     10.1.2.1     10.1.2.254   253     0   253       0         0         0
 ------------------------------------------------------------------------------
```

----结束

版权所有 © 华为技术有限公司

配置文件

SwitchA 的配置文件

```
#
 sysname Quidway
#
 vlan batch 10 to 11
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server excluded-ip-address 10.1.1.2 10.1.1.3
 dhcp server dns-list 10.1.1.2
 dhcp server netbios-type b-node
 dhcp server nbns-list 10.1.1.3
 dhcp server lease day 30 hour 0 minute 0
 dhcp server domain-name huawei.com
#
interface Vlanif11
 ip address 10.1.2.1 255.255.255.0
 dhcp select interface
 dhcp server lease day 20 hour 0 minute 0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
return
```

不同网段内配置 DHCP 服务器和 DHCP 中继示例

介绍 DHCP 服务器和客户端不在同一子网中时，DHCP 服务器和 DHCP 中继的配置过程。

组网需求

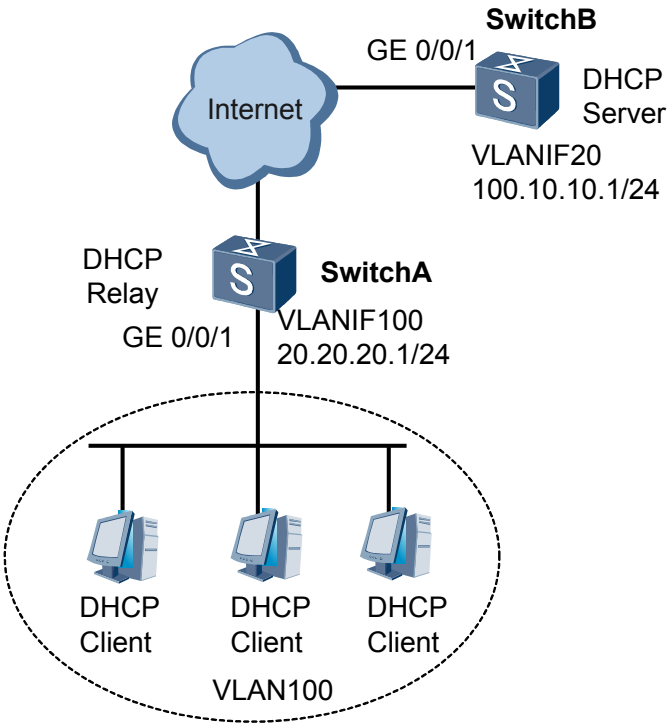
某公司拥有多个办公地点且位于不同的商务楼宇中，在同一楼宇内办公地点的主机在相同的局域网内，要求在同一楼宇内的主机由公司统一的服务器分配 IP 地址，公司服务器在位于不同于办公点的网络内。

如图 4-15，DHCP 客户端所在的网段为 20.20.20.0/24，而 DHCP 服务器所在的网段为 100.10.10.0/24。需要通过带 DHCP 中继功能的 Switch 中继 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。

由于公司服务器和办公点的主机处于不同网段，基于接口的地址池无法给不同网段的主机分配 IP 地址，应当配置一个 20.20.20.0/24 网段的全局地址池，并且 DHCP 服务器到 20.20.20.0/24 网段路由可达。

版权所有 © 华为技术有限公司

图 4-15 配置 DHCP 中继组网图



配置思路

SwitchA 为 DHCP 中继的配置思路如下：

1. 在 SwitchA 上创建 DHCP 服务器组并为服务器组添加 DHCP 服务器 SwitchB，使 SwitchB 成为公司分配 IP 地址给其它主机的服务器。
2. 在接口 VLANIF100 下使能 DHCP 中继功能，使之成为 DHCP 中继服务器。
3. 为接口 VLANIF100 绑定创建的 DHCP 服务器组，指定中继指向的公司的主服务器。

SwitchB 为 DHCP 服务器的配置思路如下：

1. 配置 DHCP 服务器到中继的接口 GE 0/0/1 的路由，使公司服务器到中继的路由可达。
2. 使能公司服务器的 DHCP 功能，配置 DHCP 服务器的接口 GE 0/0/1 下的各楼宇内的主机从服务器全局地址池中获取 IP 地址。
3. 在公司 DHCP 服务器上创建全局地址池，为公司内的主机分配 IP 地址。

数据准备

完成此配置举例，需要准备以下数据：

- DHCP 服务器组的组名
- DHCP 服务器组中的 DHCP 服务器的接口编号及接口 IP 地址
- 启动 DHCP 中继功能的接口编号及接口的 IP 地址

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 DHCP 服务器组并为服务器组添加 DHCP 服务器。

创建 DHCP 服务器组。

```
<Quidway> system-view
[Quidway] dhcp server group dhcpgroup1
```

为 DHCP 服务器组添加 DHCP 服务器。

```
[Quidway-dhcp-server-group-dhcpgroup1] dhcp-server 100.10.10.1
[Quidway-dhcp-server-group-dhcpgroup1] quit
```

步骤 2 在 VLANIF 接口下使能 DHCP 中继功能。

创建 VLAN 并将 GE 0/0/1 接口加入到 VLAN 中。

```
[Quidway] vlan 100
[Quidway-Vlan100] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Quidway-GigabitEthernet0/0/1] quit
```

使能全局 DHCP 功能，并使能 VLANIF 接口下 DHCP 中继功能。

```
[Quidway] dhcp enable
[Quidway] interface vlanif 100
[Quidway-Vlanif100] dhcp select relay
[Quidway-Vlanif100] quit
```

步骤 3 为 VLANIF 接口绑定指定的 DHCP 服务器组。

为 VLANIF 接口配置 IP 地址。

```
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 20.20.20.1 24
```

为 VLANIF 接口指定 DHCP 服务器。

```
[Quidway-Vlanif100] dhcp relay server-select dhcpgroup1
[Quidway-Vlanif100] quit
```

步骤 4 配置 DHCP 服务器。

创建 VLAN 并将 GE 0/0/1 接口加入到 VLAN 中。

```
[Quidway] vlan 20
[Quidway-Vlan20] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[Quidway-GigabitEthernet0/0/1] quit
```

启动 DHCP 服务，配置接口 VLANIF20 下的客户端从全局地址池中获取 IP 地址。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 100.10.10.1 24
[Quidway-Vlanif20] dhcp select global
[Quidway-Vlanif20] quit
```

在 DHCP 服务器上配置一个 20.20.20.0/24 网段的 IP 地址池，并且添加到 SwitchA 的静态路由，保证 DHCP 服务器到 20.20.20.0/24 网段路由可达。

版权所有 © 华为技术有限公司

```
[Quidway] ip pool 1
[Quidway-ip-pool-1] network 20.20.20.0 mask 24
[Quidway-ip-pool-1] quit
```

将 IP 地址池网段添加到 DHCP 中继的静态路由，保证 DHCP 服务器到 20.20.20.0/24 网段路由可达。（略）

步骤 5 验证配置结果。

在 SwitchA 上使用 **display dhcp relay** 命令用来查看接口的 DHCP 中继配置情况。

```
[Quidway] display dhcp relay interface vlanif100
 DHCP relay agent running information of interface Vlanif100 :
 Server group name      : dhcpgroup1
 Gateway address in use : 100.10.10.1
```

在 SwitchB 上使用 **display ip pool** 命令用来查看 IP 地址池配置情况。

```
[Quidway] display ip pool
  ------------------------------------------------------------------------
  Pool-Name      : 1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : -
  Mask           : 255.255.255.0
  Vpn instance   : --
 IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

配置文件

SwitchA 的配置文件

```
#
 sysname Quidway
#
 vlan 100
#
 dhcp enable
#
dhcp server group dhcpgroup1
 dhcp-server 100.10.10.1
#
interface Vlanif100
 ip address 20.20.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select dhcpgroup1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

SwitchB 的配置文件

```
#
 sysname Quidway
#
 vlan batch 20
#
dhcp enable
 #
ip pool 1
 network 20.20.20.0 mask 255.255.255.0
 #
```


版权所有 © 华为技术有限公司

```
interface Vlanif20
 ip address 100.10.10.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

4.4 DHCPv6 配置

目前，AC6605 在 IPv6 网络中仅支持应用为 DHCP 中继功能，本章介绍 DHCPv6 中继的配置方法。

4.4.1 DHCPv6 概述

DHCPv6（Dynamic Host Configuration Protocol for IPv6）是针对 IPv6 编址方案设计的、为主机分配 IPv6 地址和其他网络配置参数的协议。

DHCPv6 分配地址的优点

与其他 IPv6 地址分配方式（手工配置、通过路由器公告消息中的网络前缀无状态自动配置等）相比，DHCPv6 具有以下优点：

- 更好地控制地址的分配。通过 DHCPv6 不仅可以记录为主机分配的地址，还可以为特定主机分配特定的地址，以便于网络管理。
- 除了 IPv6 地址外，还可以为主机提供 DNS 服务器、域名等网络配置参数。

DHCPv6 基本概念

- 组播地址

  在 DHCPv6 协议中，客户端不用配置 DHCPv6 服务器的 IP 地址，而是发送目的地址为组播地址的 Solicit 报文来定位 DHCPv6 服务器。

  DHCPv6 用到的组播地址有两个：

  - FF02::1:2（All_DHCP_Relay_Agents_and_Servers）：所有 DHCP 服务器和中继代理的组播地址。这个地址是链路范围的，用于客户端和相邻的服务器及中继代理之间通信。所有 DHCP 服务器和中继代理都是该组的成员。
  - FF05::1:3（All_DHCP_Servers）：所有 DHCP 服务器多播地址。这个地址是站点范围的，用于中继代理和服务器之间的通信，站点内的所有 DHCP 服务器都是此组的成员。

- UDP 端口号

  DHCPv6 报文承载在 UDPv6 上，客户端监听的端口号是 546，服务器、中继代理监听的 UDP 端口号是 547。

- DUID

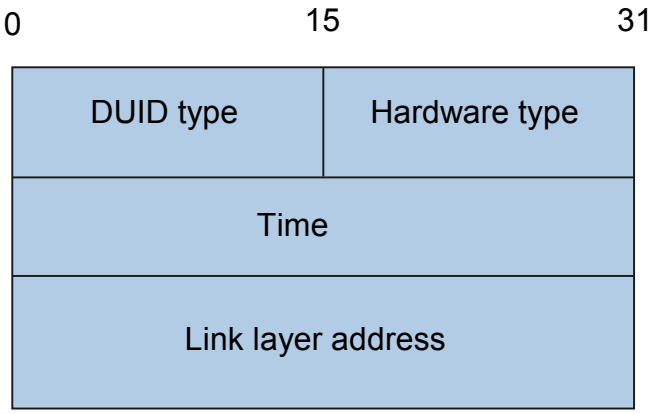
  DUID（DHCP Unique Identifier）是唯一标识一台 DHCPv6 设备（包括客户端、中继和服务器）的标识符，用于 DHCPv6 设备之间的相互验证。

  AC6605 采用 DUID-LLT（DUID Based on Link-layer Address and Time），即使用基于硬件类型、链路层地址和生成时间的 DUID 作为 DHCPv6 设备的标识。

  DUID-LLT 格式如图 4-16 所示：

版权所有 © 华为技术有限公司

图 4-16 DUID-LLT 格式



- DUID type：DUID 类型。DUID-LLT 类型取值为 0x0001。
- Hardware type：硬件类型。设备支持的硬件类型为以太网，取值为 0x0006。
- Time：生成 DUID 的系统时间。在生成 DUID 前，系统时间必须配置好，或有其他可用的时钟源。
- Link layer address：链路层地址。链路层地址来自设备的任何一个接口，该接口有一个唯一的链路层地址。取值为 MAC 地址。

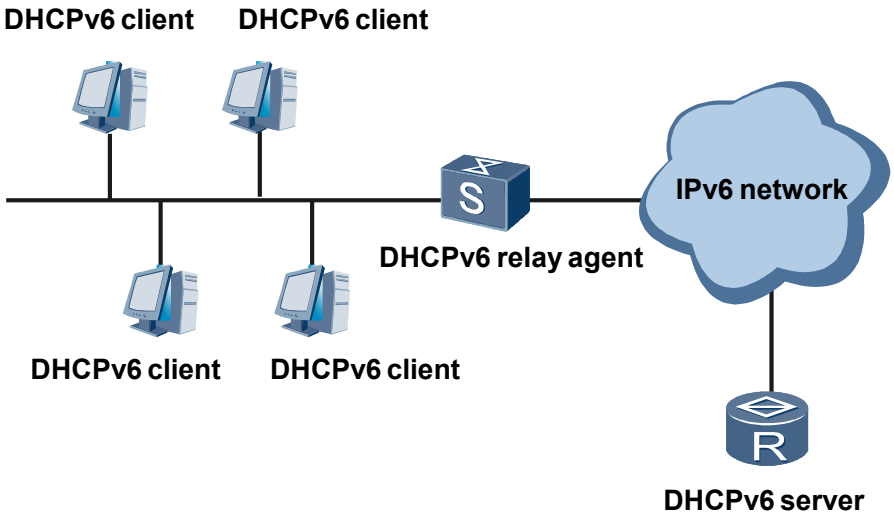
4.4.2 AC6605 支持的 DHCPv6 特性

目前，AC6605 仅支持 DHCPv6 中继功能，不能作为 DHCPv6 服务器或客户端。

DHCPv6 典型组网

DHCPv6 的典型组网如图 4-17 所示。DHCPv6 客户端通过链路范围的组播地址与 DHCPv6 服务器通信，以获取 IPv6 地址和其他网络配置参数。如果服务器和客户端不在同一个链路范围内，则需要通过 DHCPv6 中继来转发报文，这样可以避免在每个链路范围内都部署 DHCPv6 服务器，既节省了成本，又便于进行集中管理。

图 4-17 DHCPv6 典型组网图



版权所有 © 华为技术有限公司

说明

目前，AC6605 仅支持 DHCPv6 中继功能，不能作为 DHCPv6 服务器或客户端。

AC6605 支持的 DHCPv6 中继功能

- 支持转发来自 DHCPv6 客户端的报文

  如果 AC6605 为第一跳 DHCPv6 中继代理设备，那么它收到的 DHCP 报文直接来自 DHCPv6 客户端，AC6605 将解析、封装、转发直接来自于客户端的 DHCPv6 报文。

- 支持转发来自 DHCPv6 中继代理的报文

  如果 AC6605 不是第一跳 DHCPv6 中继代理，那么它收到的 DHCP 报文来自其他的 DHCPv6 中继代理，AC6605 将解析、封装、转发来自于其他中继代理的 DHCPv6 报文。

- 支持转发来自 DHCPv6 服务器的报文

  如果 AC6605 为最后一跳 DHCPv6 中继代理，那么它收到的 DHCP 报文直接来自 DHCPv6 服务器，AC6605 将解析、封装、转发直接来自于服务器的 DHCPv6 报文。

- 支持 Remote-ID 选项

  AC6605 支持在转发的 relay-forward 报文中插入或强制插入 Remote-ID 选项。

- 支持对转发的 DHCPv6 报文限速

  为了防止大量来自客户端或中继代理的报文对本设备形成冲击，AC6605 还支持对转发的 DHCPv6 报文进行限速。当丢弃的报文数超过一定阈值时，发出告警信息。

- 支持对转发的 DHCPv6 报文进行统计

  AC6605 应用了 DHCPv6 中继功能，系统会对经过中继的 DHCPv6 报文进行统计。

4.4.3 配置 DHCPv6 中继

当 DHCPv6 客户端和 DHCPv6 服务器不在同一个链路时，在客户端和服务器之间需要架设 DHCPv6 Relay 设备，通过中继代理功能传递客户端和服务器交互的 DHCPv6 报文。

建立配置任务

介绍配置 DHCPv6 中继的应用环境、前置任务和数据准备。

应用环境

当 DHCPv6 客户端向 DHCPv6 服务器申请 IP 地址，而客户端和服务器不在同一个链路时，在客户端和服务器之间需要架设中继设备，通过中继代理功能传递客户端和服务器交互的 DHCPv6 报文。

前置任务

在配置 DHCPv6 中继功能之前，需完成以下任务：

- 配置 DHCPv6 服务器
- 配置 AC6605 到 DHCPv6 服务器的路由

版权所有 © 华为技术有限公司

数据准备

在配置 DHCPv6 中继功能之前，需准备以下数据。

序号	数据
1	使能 DHCPv6 中继功能的接口类型和接口编号，接口类型为 VLANIF 接口
2	使能 Remote-ID 功能的接口类型和接口编号，接口类型为 GigabitEthernet、GE
3	（可选）DHCPv6 报文限速阈值、报文限速丢弃告警阈值

使能 DHCPv6 中继功能

在 AC6605 上使能 VLANIF 接口的 DHCPv6 中继代理功能时，可以同时配置 DHCPv6 服务器或下一跳中继代理的 IPv6 地址，并可以指定中继报文的出接口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **ipv6**，使能 IPv6 报文转发功能。

步骤 4 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 5 执行命令 **ipv6 enable**，使能 IPv6 报文转发功能。

步骤 6 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }，配置接口的 IPv6 地址。

步骤 7 执行命令 **dhcpv6 relay destination** *ipv6-address* [**interface** *interface-type interface-number*]，使能 VLANIF 接口的 DHCPv6 中继代理功能，并设置 DHCPv6 服务器或下一跳中继代理的 IPv6 地址，同时可以指定中继报文的出接口。

缺省情况下，VLANIF 接口未使能 DHCPv6 中继代理功能。

- 如果配置的 IPv6 地址是全局地址或者站点地址则不需要指定出接口，报文通过查找路由将中继报文发往配置的 IPv6 地址。
- 如果配置的 IPv6 地址是本地地址或组播地址，则需要指定服务器或下一跳中继所在的出接口。

AC6605 全局支持使能 DHCPv6 中继代理功能的接口数目最大为 8 个，每个接口下最多可以配置 8 个目的地址。

----结束

（可选）配置 Remote-ID

Remote-ID 选项通过携带客户端的一些信息来唯一标识客户端。

背景信息

服务器可以根据 Remote-ID 选项内容，进行地址分配、参数配置、前缀代理的决策。Remote-ID 选项内容由厂商自定义，通常可以携带以下信息：拨号连接中呼叫者的电话

版权所有 © 华为技术有限公司

号码、用户名、点对点连接中对端 IP 地址、接入的端口信息等。目前 Remote-ID 最大字节数是 247Bytes。

AC6605 应用为 DHCPv6 中继时，对 Remote-ID 的处理如下：

- AC6605 收到直接来自客户端的报文，在构造 Relay-forward 报文时，根据配置添加 Remote-ID 选项。
- AC6605 收到服务器的 Relay-reply 报文中如果包含 Remote-ID 选项，将选项从报文中剔除，然后转发给客户端或其他中继代理。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcpv6 remote-id format** { **default** | **user-defined** *text* }，配置 DHCPv6 报文中 Remote-ID 选项的格式。

缺省情况下，DHCPv6 报文中 Remote-ID 使用 default 格式。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

接口类型可以是 GigabitEthernet 接口、GE 接口。

步骤 4 执行命令 **dhcpv6 remote-id insert enable**，使能在 DHCPv6 中继报文中插入 Remote-ID 选项的功能。或者执行命令 **dhcpv6 remote-id rebuild enable**，使能在 DHCPv6 中继报文中强制插入 Remote-ID 的功能。

- 配置 **dhcpv6 remote-id insert enable** 命令后， 如果原来的 DHCPv6 报文中没有 Remote-ID 选项，则插入 Remote-ID 选项；如果原来的 DHCPv6 报文中有 Remote-ID 选项，则不处理。
- 配置 **dhcpv6 remote-id rebuild enable** 命令后， 如果原来的 DHCPv6 报文中没有 Remote-ID 选项，则插入 Remote-ID 选项；如果原来的 DHCPv6 报文中有 Remote-ID 选项，则删除报文中原有的 Remote-ID，插入新的 Remote-ID 选项。

这两条命令之间是覆盖关系，即如果在同一视图下同时配置了这两条命令，后配置的命令生效。

----结束

（可选）配置 DHCPv6 报文限速功能

为了防止大量来自客户端或中继代理的报文对本设备形成冲击，AC6605 还支持对转发的 DHCPv6 报文进行限速。

背景信息

使能 DHCPv6 报文限速功能后，DHCPv6 报文超过速率限制值时会被丢弃，当丢弃的报文数超过一定阈值时，AC6605 支持日志功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **dhcpv6 packet-rate** *packet-rate*，使能 DHCPv6 报文限速功能，并配置速率抑制值。

版权所有 © 华为技术有限公司

缺省情况下，AC6605 没有使能 DHCPv6 报文限速功能。

步骤 4 执行命令 **dhcpv6 packet-rate drop-alarm enable**，使能 DHCPv6 报文限速丢弃日志功能。

使能了 DHCPv6 报文限速丢弃日志功能后，如果每秒经过 AC6605 的 DHCPv6 报文数超过配置的速率限制值，则被丢弃处理。缺省情况下，当丢弃的报文数超过 100 个包时，发出日志信息。

步骤 5 执行命令 **dhcpv6 packet-rate drop-alarm threshold** *threshold*，配置 DHCPv6 报文限速丢弃日志的阈值。

----结束

检查配置结果

查看 DHCPv6 中继的配置信息。

前提条件

已经完成 DHCPv6 中继功能的所有配置。

操作步骤

- 使用命令 **display dhcpv6 relay** [**interface** *interface-type interface-number*] 查看 DHCPv6 中继代理功能的接口配置信息。

  目前接口类型只支持 VLANIF 接口。
- 使用命令 **display dhcpv6 relay statistics** [**interface** *interface-type interface-number*] 查看 DHCPv6 中继代理的报文统计信息。

  目前接口类型只支持 VLANIF 接口。

----结束

4.4.4 维护 DHCPv6

清除 DHCPv6 中继的统计信息和监控 DHCPv6 中继运行状况。

清除 DHCPv6 中继统计信息

AC6605 应用了 DHCPv6 中继功能时，系统会对经过中继的 DHCPv6 报文进行统计。当需要清除当前的统计计数时，可以在用户视图或系统视图下执行命令清除 DHCPv6 中继代理的报文统计信息。

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **reset dhcpv6 relay statistics** [**interface** *interface-type interface-number*] 命令清除 DHCPv6 中继代理的报文统计信息。

  接口类型为 VLANIF 接口。不指定接口时清除所有 DHCPv6 报文统计信息，指定接口时清除被指定接口的报文统计信息。

----结束

监控 DHCPv6 中继运行状况

使用 display 命令监控 DHCPv6 中继运行状况。

操作步骤

- 使用命令 **display dhcpv6 relay** [**interface** *interface-type interface-number*] 查看 DHCPv6 中继代理功能的接口配置信息。
- 使用命令 **display dhcpv6 relay statistics** [**interface** *interface-type interface-number*] 查看 DHCPv6 中继代理的报文统计信息。

----结束

4.4.5 配置举例

举例说明 DHCPv6 中继的配置过程。

配置 DHCPv6 中继示例

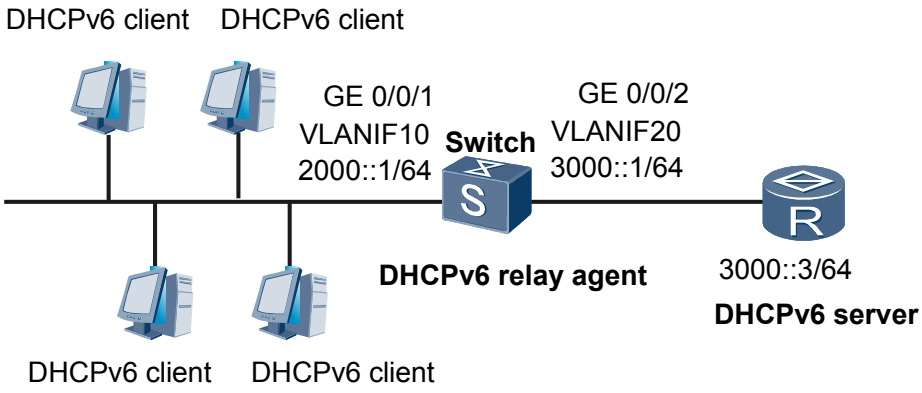
本举例介绍 DHCPv6 中继的配置过程。

组网需求

如图 4-18 所示，DHCPv6 客户端所在网络地址为 2000::/64，DHCPv6 服务器的地址为 3000::3/64。客户端和服务器不在同一个链路，需要通过 DHCPv6 中继转发报文。

要求将 Switch 作为 DHCPv6 中继，为客户端和服务器转发报文。Switch 同时作为 2000::/64 网络的网关设备，通过 RA 消息中的 M 标志位和 O 标志位指定该网络中的主机通过 DHCPv6 获取 IPv6 地址和其他网络配置参数。

图 4-18 DHCPv6 中继组网图



版权所有 © 华为技术有限公司

配置思路

DHCPv6 中继的配置思路如下：

1. 启动 DHCP 服务。
2. 创建 VLANIF 接口，并配置 VLANIF 接口的 IPv6 地址。
3. 使能 DHCPv6 中继功能，并配置 DHCPv6 服务器地址。
4. 配置 Switch 为网关。

数据准备

要完成此配置举例，需要准备以下数据：

- 接口的 IPv6 地址
- DHCPv6 服务器地址

操作步骤

步骤 1 启动 DHCP 服务。

```
<Quidway> system-view
[Quidway] dhcp enable
```

步骤 2 配置接口加入 VLAN。

配置 GigabitEthernet0/0/1 接口加入 VLAN10。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
```

配置 GigabitEthernet0/0/2 加接口入 VLAN20。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 20
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 3 配置 VLANIF 接口的 IPv6 地址。

使能 IPv6 报文转发功能。

```
[Quidway] ipv6
```

配置 VLANIF10 接口的 IPv6 地址。

```
[Quidway] vlan batch 10 20
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ipv6 enable
[Quidway-Vlanif10] ipv6 address 2000::1 64
[Quidway-Vlanif10] quit
```

配置 VLANIF20 接口的 IPv6 地址。

```
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ipv6 enable
[Quidway-Vlanif20] ipv6 address 3000::1 64
[Quidway-Vlanif20] quit
```


版权所有 © 华为技术有限公司

步骤 4 使能 DHCPv6 中继功能。

使能 VLANIF10 接口的 DHCPv6 中继功能，并配置 DHCPv6 服务器地址。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcpv6 relay destination 3000::3
```

步骤 5 配置 Switch 作为网关。

配置发布 RA 消息，并配置 M 和 O 标志位。

```
[Quidway-Vlanif10] undo ipv6 nd ra halt
[Quidway-Vlanif10] ipv6 nd autoconfig managed-address-flag
[Quidway-Vlanif10] ipv6 nd autoconfig other-flag
[Quidway-Vlanif10] quit
```

步骤 6 验证配置结果。

在 Switch 上使用 **display dhcpv6 relay** 命令用来查看 DHCPv6 中继配置情况。

```
[Quidway] display dhcpv6 relay
 Interface    Mode    Destination
------------------------------------------------------------------
Vlanif10     Relay   3000::3
------------------------------------------------------------------
```

在 Switch 上使用 **display dhcpv6 relay statistics** 命令用来查看 DHCPv6 中继转发报文的统计信息。

```
[Quidway] display dhcpv6 relay statistics
MessageType              Recieve          Send             Error
 Solicit                  0                0                0
 Advertise                0                0                0
 Request                  0                0                0
 Confirm                  0                0                0
 Renew                    0                0                0
 Rebind                   0                0                0
 Reply                    0                0                0
 Release                  0                0                0
 Decline                  0                0                0
 Reconfigure              0                0                0
 Information-request      0                0                0
 Relay-forward            0                0                0
 Relay-reply              0                0                0
 UnknownType              0                0                0
```

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
 vlan batch 10 20
#
 ipv6
#
dhcp enable
#
interface Vlanif10
 ipv6 enable
 ipv6 address 2000::1/64
 undo ipv6 nd ra halt
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 dhcpv6 relay destination 3000::3
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif20
 ipv6 enable
 ipv6 address 3000::1/64
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

4.5 IP 性能配置

介绍 IP 性能的基本概念，并提供配置过程和配置实例。

4.5.1 IP 性能概述

在一些特定的网络环境里，需要调整 IP 的参数，以便网络性能达到最佳。这里主要介绍 AC6605 支持的 IP 性能参数。

4.5.2 AC6605 支持的 IP 性能

ICMP

- ICMP 主机不可达报文

  如果 AC6605 在转发报文时发现报文同时满足以下条件：

  - 报文的目的地址没有对应的路由。
  - 该报文也不是到本机的报文。

  那么 AC6605 将丢弃该报文，同时向源地址返回一个 ICMP 主机不可达报文，以通知源主机停止发送到该目的地的报文。

- ICMP 报文开关的作用

  在正常情况下，以上报文能够确保业务报文的正确发送。但是，当网络流量较大时，如果以上的现象出现较多，则 AC6605 会因此发送大量的 ICMP 报文，增大网络的流量负担。尤其是当遇到恶意攻击时，容易产生恶性循环，从而加剧网络的拥塞。

  解决上述问题的办法是在 ICMP 报文的出接口增加控制开关，用来打开或关闭 ICMP 主机不可达报文的发送开关。如果关闭这个开关，则 AC6605 不会发送该报文，从而起到减小网络流量负担、防止遭到恶意攻击的作用。

4.5.3 配置 IP 性能优化

介绍 IP 性能优化的配置，以在特性的网络环境里，通过设置 IP 的一系列参数以达到最佳效果。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

在一些特定的网络环境里，需要微调 IP 的参数，以便达到最佳的效果。优化 IP 性能涉及到设置一系列的参数。

前置任务

在配置 IP 性能优化之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 配置接口的 IP 地址。
- 配置 ACL。

数据准备

在配置 IP 性能优化之前，需准备以下数据。

序号	数据
1	接口的编号
2	需要进行源地址校验的接口编号
3	需要转发广播报文的接口编号以及用于指定广播报文的 ACL 编号
4	需要配置 ICMP 主机不可达功能的接口编号
5	SYN-Wait 定时器、FIN-Wait 定时器、Socket 收发缓冲区的大小

配置 IP 源地址校验功能

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 5 执行命令 **ip verify source-address**，配置 IP 源地址校验功能。

缺省情况下，接口不对接收的报文进行源地址合法性检查。

----结束

版权所有 © 华为技术有限公司

配置 ICMP 属性

背景信息

缺省情况下，系统 ICMP 重定向报文发送功能和系统 ICMP 主机不可达报文发送功能是打开的。

注意

- 如果关闭 ICMP 主机不可达报文发送功能，则 AC6605 在任何情况下都不会再发出 ICMP 主机不可达报文。

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **icmp host-unreachable send**，打开系统 ICMP 主机不可达报文发送功能。

----结束

配置 TCP 属性

背景信息

可以配置的 TCP 属性包括：

- SYN-Wait 定时器：当发送 SYN 报文时，TCP 启动 SYN-Wait 定时器，若 SYN-Wait 超时前未收到回应报文，则 TCP 连接将被终止。SYN-Wait 定时器的取值范围是 2 秒～ 600 秒，缺省值是 75 秒。
- FIN-Wait 定时器：当 TCP 的连接状态由 FIN_WAIT_1 变为 FIN_WAIT_2 时启动 FIN-Wait 定时器，若 FIN-Wait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。FIN-Wait 定时器的取值范围是 76 秒～ 3600 秒，缺省值是 675 秒。
- 面向连接 Socket 的接收和发送缓冲区的大小 *window-size*：取值范围是 1k 字节～ 32k 字节，缺省值是 8k 字节。

在系统视图下多次配置 TCP 的各个属性，只有最后一次配置生效。

请在 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp timer syn-timeout** *interval*，配置 TCP 连接建立 SYN-Wait 定时器时间。

步骤 3 执行命令 **tcp timer fin-timeout** *interval*，配置 TCP 的 FIN-WAIT（FIN_WAIT_2）定时器时间。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **tcp window** *window-size*，配置 TCP 的 Socket 接收和发送缓冲区的大小。

----结束

检查配置结果

前提条件

已经完成 IP 性能优化的所有配置。

操作步骤

- 使用 **display tcp status** [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]]命令查看 TCP 连接状态。
- 使用 **display tcp statistics** 命令查看 TCP 流量统计信息。
- 使用 **display udp statistics** 命令查看 UDP 流量统计信息。
- 使用 **display ip statistics** 命令查看 IP 流量统计信息。
- 使用 **display ip socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **sock-type** *socket-type*]命令查看已创建的 IPv4 Socket 信息。
- 使用 **display icmp statistics** 命令查看 ICMP 流量统计信息。
- 使用 **display rawlink statistics** 命令查看 RawLink 统计信息。
- 使用 **display fib** [*slot-id*]命令查看接口板的 FIB 表。
- 使用 **display fib** [*slot-id*] [**vpn-instance** *vpn-instance-name*] [**verbose**]命令查看转发信息表的信息。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **acl** *acl-number* [**verbose**]命令查看 FIB 信息，把通过了指定访问控制列表过滤规则的 FIB 表项按照一定格式显示出来。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* 命令查看出接口为指定接口的 FIB 表项。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **ip-prefix** *prefix-name* [**verbose**]命令查看 IP 报文中前缀列表为指定前缀列表的 FIB 表项。
- 使用 **display fib** [*slot-id*][**vpn-instance** *vpn-instance-name*] *destination-address1* [*destination-mask1*] [**longer**] [**verbose**]命令查看与目的地址在输入的掩码范围内的 IP 地址匹配的所有目的地址 FIB 表项。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **next-hop** *ip-address* 命令查看下一跳 IP 地址为指定的下一跳的 IP 地址的 FIB 表项。
- 使用 **display fib** [*slot-id*] [**vpn-instance** *vpn-instance-name*] **statistics** 查看 FIB 表项的总数目。

----结束

4.5.4 维护 IP 性能

介绍如何清除 IP 性能统计信息、监控 IP 性能运行状况以及如何调试 IP 性能。

版权所有 © 华为技术有限公司

清除 IP 性能统计信息

背景信息



注意

清除 IP/TCP/UDP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除 IP 统计信息后，请在用户视图下执行 **reset ip statistics** [**interface** *interface-type interface-number*]命令。
- 在确认需要清除 Socket Monitor 中的信息后，请在用户视图下执行 **reset ip socket monitor** [**task-id** *task-id* **socket-id** *socket-id*]命令。
- 在确认需要清除 TCP 统计信息后，请在用户视图下执行 **reset tcp statistics** 命令。
- 在确认需要清除 UDP 统计信息后，请在用户视图下执行 **reset udp statistics** 命令。
- 在确认需要清除 RawLink 统计信息后，请在用户视图下执行 **reset rawlink statistics** 命令。

----结束

监控 IP 性能运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 IP 性能的运行情况。

操作步骤

- 使用 **display tcp status** [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]]命令查看 TCP 连接状态。
- 使用 **display tcp statistics** 命令查看 TCP 流量统计信息。
- 使用 **display udp statistics** 命令查看 UDP 流量统计信息。
- 使用 **display ip statistics** 命令查看 IP 流量统计信息。
- 使用 **display ip socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **sock-type** *socket-type*]命令查看已创建的 IPv4 Socket 信息。
- 使用 **display icmp statistics** 命令查看 ICMP 流量统计信息。
- 使用 **display rawlink statistics** 命令查看 RawLink 统计信息。
- 使用 **display fib** [*slot-id*]命令查看接口板的 FIB 表。
- 使用 **display fib** [*slot-id*] [**vpn-instance** *vpn-instance-name*] [**verbose**]命令查看转发信息表的信息。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **acl** *acl-number* [**verbose**]命令查看 FIB 信息，把通过了指定访问控制列表过滤规则的 FIB 表项按照一定格式显示出来。

版权所有 © 华为技术有限公司

- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* 命令查看出接口为指定接口的 FIB 表项。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **ip-prefix** *prefix-name* [**verbose**]命令查看 IP 报文中前缀列表为指定前缀列表的 FIB 表项。
- 使用 **display fib** [*slot-id*][**vpn-instance** *vpn-instance-name*] *destination-address1* [*destination-mask1*] [**longer**] [**verbose**]命令查看与目的地址在输入的掩码范围内的 IP 地址匹配的所有目的地址 FIB 表项。
- 使用 **display fib** [**vpn-instance** *vpn-instance-name*] **next-hop** *ip-address* 命令查看下一跳 IP 地址为指定的下一跳的 IP 地址的 FIB 表项。
- 使用 **display fib** [*slot-id*] [**vpn-instance** *vpn-instance-name*] **statistics** 查看 FIB 表项的总数目。

----结束

调试 IP 性能

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 IP/TCP/UDP/RAWIP/RAWLINK 运行故障时，请在用户视图下执行下面的 **debugging** 命令对 IP/TCP/UDP/RAWIP/RAWLINK 进行调试，查看调试信息，定位故障并分析故障原因。

有关 **debugging** 命令的解释请参见《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 在用户视图下执行 **debugging ip packet** [**error**] [**acl** *acl-number*] [**verbose**]命令，调试 IP 报文。
- 在用户视图下执行 **debugging ip icmp** [**verbose**]命令，调试 ICMP。
- 在用户视图下执行 **debugging udp packet** [**src-ip** *src-address*] [**src-port** *src-port*] [**dest-ip** *dest-address*] [**dest-port** *dest-port*]命令或 **debugging udp packet** [**task-id** *task-id*] [**socket-id** *socket-id*]命令，调试 UDP 报文。
- 在用户视图下执行 **debugging tcp packet** [**src-ip** *src-address*] [**src-port** *src-port*] [**dest-ip** *dest-address*] [**dest-port** *dest-port*] [**flag** *flag-number*]命令或 **debugging tcp packet** [**task-id** *task-id*] [**socket-id** *socket-id*] [**flag** *flag-number*]命令，调试 UDP 报文。
- 在用户视图下执行 **debugging tcp event** [**local-ip** *local-address*] [**local-port** *local-port*] [**remote-ip** *remote-address*] [**remote-port** *remote-port*]命令或 **debugging tcp event** [**task-id** *task-id*] [**socket-id** *socket-id*]命令，调试 TCP 事件。
- 在用户视图下执行 **debugging tcp md5** [**src-ip** *src-address*] [**src-port** *src-port*] [**dest-ip** *dest-address*] [**dest-port** *dest-port*]命令或 **debugging tcp md5** [**task-id** *task-id*] [**socket-id** *socket-id*]命令，调试 TCP MD5 认证。

版权所有 © 华为技术有限公司

- 在用户视图下执行 **debugging rawip packet** [**src-ip** *src-address*] [**dest-ip** *dest-address*] [**protocol** *protocol-number*] [**verbose** *verbose-number*]命令或 **debugging rawip packet** [**task-id** *task-id*] [**socket-id** *socket-id*] [**verbose** *verbose-number*]命令，调试 RAWIP 报文。
- 在用户视图下执行 **debugging rawlink packet** [**src-mac** *src-mac*] [**dest-mac** *dest-mac*] [**verbose** *verbose-number*]命令或 **debugging rawlink packet** [**task-id** *task-id*] [**socket-id** *socket-id*] [**verbose** *verbose-number*]命令，调试 RAWLINK 报文。

----结束

4.5.5 配置举例

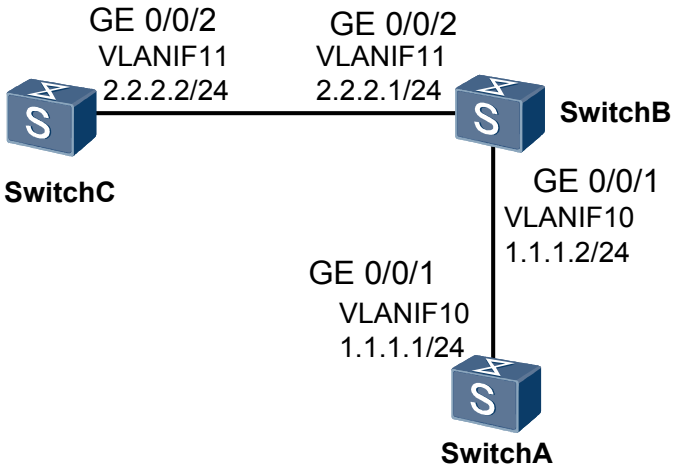
介绍 IP 性能优化的配置实例。

配置 ICMP 属性主机不可达报文示例

组网需求

如图 4-19 所示，为测试主机不可达报文的发送，需要 SwitchA、SwitchB、SwitchC 三台设备，并且这三台设备通过各自的 GigabitEthernet 口相连。

图 4-19 配置 ICMP 属性主机不可达报文组网图



配置思路

配置发送 ICMP 主机不可达报文的思路如下：

1. 在各 Switch 上的相应接口上配置 IP 地址。
2. 配置到达非直连设备的静态路由。
3. 在系统视图下使能发送 ICMP 主机不可达报文的功能。
4. 在接口视图下使能发送 ICMP 主机不可达报文的功能。

版权所有 © 华为技术有限公司

说明

缺省情况下，系统视图和接口视图下的 ICMP 主机不可达报文功能处于使能状态。如果没有修改过，则不需要配置这一步。

数据准备

完成此配置，需准备如下的数据：

- 到达非直连设备的静态路由
- 接口的 IP 地址

操作步骤

步骤 1 配置 SwitchA

配置接口 VLANIF10 的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-Vlan10] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 1.1.1.1 24
[SwitchA-Vlanif10] quit
```

在 SwitchA 上配置静态路由。

```
[SwitchA] ip route-static 2.2.2.0 24 1.1.1.2
```

步骤 2 配置 SwitchB

在 SwitchB 上配置接口 VLANIF10 的 IP 地址，并使能主机不可达的报文发送功能。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] icmp host-unreachable send
[SwitchB] vlan 10
[SwitchB-Vlan10] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 1.1.1.2 24
[SwitchB-Vlanif10] quit
[SwitchB] vlan 11
[SwitchB-Vlan11] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port hybrid tagged vlan 11
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 11
[SwitchB-Vlanif11] ip address 2.2.2.1 24
[SwitchB-Vlanif11] icmp host-unreachable send
[SwitchB-Vlanif11] quit
```

步骤 3 配置 SwitchC

在 SwitchC 上配置接口 VLANIF11 的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 11
[SwitchC-Vlan11] quit
```


版权所有 © 华为技术有限公司

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port hybrid tagged vlan 11
[SwitchC-GigabitEthernet0/0/2] quit
[SwitchC] interface vlanif 11
[SwitchC-Vlanif11] ip address 2.2.2.2 24
[SwitchC-Vlanif11] quit
```

步骤 4 验证配置结果。

打开 SwitchA 的 ICMP 报文调试开关。

```
<SwitchA> debugging ip icmp
<SwitchA> terminal monitor
<SwitchA> terminal debugging
```

在 SwitchA 上运行 **ping 2.2.2.3**，可以从通过测试仪器抓取的 SwitchA 接收到的数据包中看到 SwitchB 发送的主机不可达报文。

```
[SwitchA] ping 2.2.2.3
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan 10
#
interface vlanif 10
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10 to 11
#
interface vlanif 10
 ip address 1.1.1.2 255.255.255.0
#
interface vlanif 11
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan 11
#
interface vlanif 11
 ip address 2.2.2.2 255.255.255.0
```


版权所有 © 华为技术有限公司

```
 #
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
return
```

4.6 DHCP 策略 VLAN 配置

介绍 DHCP 策略 VLAN 的基本概念、工作方式和配置过程，并提供配置举例。

4.6.1 DHCP 策略 VLAN 概述

在配置了策略 VLAN 的 AC6605 上，各接口所连接主机所属的 VLAN 是通过该主机的 IP 地址来匹配的。当一个新加入网络的主机连接到某一接口时，由于没有合法的 IP 地址，所以它无法加入到对应的 VLAN 中。

引入 DHCP 策略 VLAN 功能，是为了使新加入网络的主机能够通过 DHCP 服务器获得合法的 IP 地址，然后根据其 IP 地址划入对应的 VLAN。

4.6.2 AC6605 支持的 DHCP 策略 VLAN 特性

AC6605 支持三种 DHCP 策略 VLAN 的配置方法：

- 配置基于 MAC 地址的 DHCP 策略 VLAN
- 配置基于接口的 DHCP 策略 VLAN
- 配置普通 DHCP 策略 VLAN

4.6.3 配置基于 MAC 地址的 DHCP 策略 VLAN

介绍如何配置基于 MAC 地址的 DHCP 策略 VLAN

建立配置任务

应用环境

多台用户主机通过 AC6605 的某个接口加入到网络中,为了使这些主机能够通过 DHCP 服务器申请到 IP 地址并加入到相应的 VLAN，需要为 AC6605 配置基于 MAC 地址的 DHCP 策略 VLAN。

前置任务

在配置基于 MAC 地址的 DHCP 策略 VLAN 之前，需完成以下任务：

- 配置 AC6605 上连接新加入主机接口的缺省 VLAN。

数据准备

在配置基于 MAC 地址的 DHCP 策略 VLAN 之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	新加入主机的 MAC 地址
2	DHCP 服务器所在 VLAN 的 VLAN ID

配置过程

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入与主机相连的接口视图。

步骤 3 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置该接口所属的 VLAN，这些 VLAN 的帧以 Untagged 方式通过接口，到达用户主机。

步骤 4 执行命令 **vlan** *vlan-id*，进入 DHCP 服务器所在 VLAN 的视图。

步骤 5 执行命令 **dhcp policy-vlan mac-address** *mac-address1* [**to** *mac-address2*] [**priority** *priority*]，配置基于 MAC 地址的 DHCP 策略 VLAN。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看系统当前 VLAN 视图的运行配置	**display this**

在配置了基于 MAC 地址的 DHCP 策略 VLAN 的 VLAN 视图下执行 **display this** 命令，可以看到基于 MAC 地址的 DHCP 策略 VLAN 配置成功。

```
[Quidway-vlan2] display this
#
vlan 2
 dhcp policy-vlan mac-address 0002-0002-0002 priority 2
#
```

4.6.4 配置基于接口的 DHCP 策略 VLAN

介绍如何配置基于接口的 DHCP 策略 VLAN

版权所有 © 华为技术有限公司

建立配置任务

应用环境

多台用户主机分别通过 AC6605 的不同接口加入到网络中，为了使这些新加入网络的主机能顺利申请到 IP 地址，需要为 AC6605 配置基于接口的 DHCP 策略 VLAN。

前置任务

在配置基于接口的 DHCP 策略 VLAN 之前，需完成以下任务：

- 配置 AC6605 上连接新加入主机接口的缺省 VLAN。
- 配置 AC6605 上连接新加入主机接口的链路类型为 Hybrid。

数据准备

在配置基于接口的 DHCP 策略 VLAN 之前，需准备以下数据。

序号	数据
1	AC6605 设备上与新加入主机相连的接口的编号
2	DHCP 服务器所在 VLAN 的 VLAN ID

配置过程

背景信息

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入与新加入设备相连的接口视图。

步骤 3 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置该接口所属的 VLAN，这些 VLAN 的帧以 Untagged 方式通过接口，到达用户主机。

步骤 4 执行命令 **vlan** *vlan-id*，进入 DHCP 服务器所在 VLAN 的视图。

步骤 5 执行命令 **dhcp policy-vlan port** *interface-type interface-number1* [**to** *interface-number2*] [**priority** *priority*]，配置基于接口的 DHCP 策略 VLAN。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

版权所有 © 华为技术有限公司

操作	命令
查看系统当前 VLAN 视图的运行配置	**display this**

在配置了基于接口 DHCP 策略 VLAN 的 VLAN 视图下执行 **display this** 命令，可以看到基于接口的 DHCP 策略 VLAN 配置成功。

```
[Quidway-vlan2] display this
#
vlan 2
 dhcp policy-vlan port GigabitEthernet 0/0/2 priority 2
#
```

4.6.5 配置普通 DHCP 策略 VLAN

介绍如何配置普通 DHCP 策略 VLAN

建立配置任务

应用环境

为了使没有匹配基于 MAC 地址和基于接口的 DHCP 策略规则的新加入网络的主机能顺利申请到合法的 IP 地址，需要为 AC6605 配置普通 DHCP 策略 VLAN。

前置任务

在配置普通 DHCP 策略 VLAN 之前，需完成以下任务：

- 配置 AC6605 上连接新加入主机接口的缺省 VLAN。

数据准备

在配置普通 DHCP 策略 VLAN 之前，需准备以下数据。

序号	数据
1	DHCP 服务器所在 VLAN 的 VLAN ID

配置过程

背景信息

请在 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入与新加入设备相连的接口视图。

步骤 3 执行命令 **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置该接口所属的 VLAN，这些 VLAN 的帧以 Untagged 方式通过接口，到达用户主机。

步骤 4 执行命令 **vlan** *vlan-id*，进入 DHCP 服务器所在 VLAN 的视图。

步骤 5 执行命令 **dhcp policy-vlan generic** [**priority** *priority*]，配置普通 DHCP 策略 VLAN。

----结束

检查配置结果

完成上述配置后，请执行下面的命令检查配置结果。

操作	命令
查看系统当前 VLAN 视图的运行配置	**display this**

在配置了普通 DHCP 策略 VLAN 的 VLAN 视图下执行 **display this** 命令，可以看到普通的 DHCP 策略 VLAN 配置成功。

```
[Quidway-vlan2] display this
#
vlan 2
 dhcp policy-vlan generic priority 2
#
```

4.6.6 维护

查看 DHCP 策略 VLAN 的配置情况。

监控运行状况

在日常维护工作中，可以在相应的 VLAN 视图下执行以下命令，了解 DHCP 策略 VLAN 的配置状况。

操作	命令
查看 DHCP 策略 VLAN 的配置信息	**display this**

4.6.7 配置举例

举例说明 DHCP 策略 VLAN 的配置。

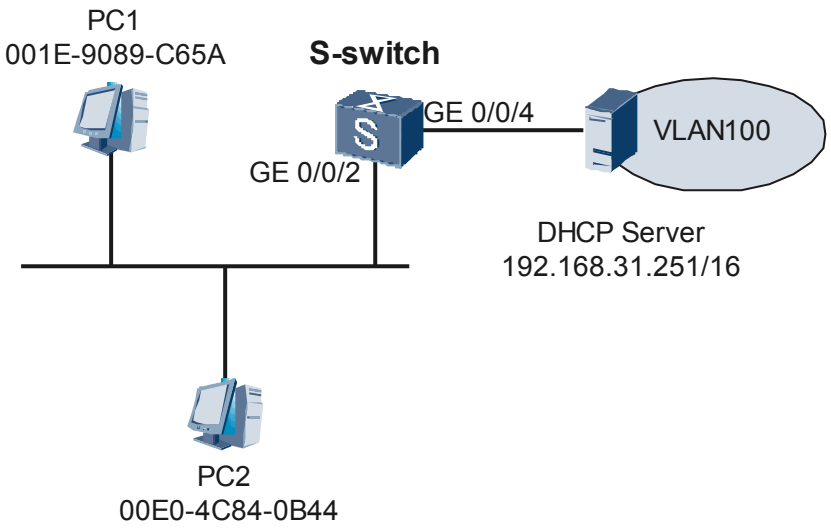
版权所有 © 华为技术有限公司

配置基于 MAC 地址的 DHCP 策略 VLAN 示例

组网需求

如图 4-20 所示，AC6605 的以太网口 GE0/0/2 连接两台新加入网络的 PC 机，接口 GE0/0/4 连接一台 DHCP 服务器，该服务器加入到 VLAN100 中。PC1 和 PC2 的 MAC 地址分别为 001E-9089-C65A 和 00E0-4C84-0B44。

图 4-20 配置基于 MAC 地址的 DHCP 策略 VLAN 组网图



配置思路

配置基于 MAC 地址的 DHCP 策略 VLAN 的思路如下：

1. 全局使能 DHCP 功能。
2. 明确 DHCP 服务器位于哪个 VLAN。
3. 配置基于 MAC 地址的 DHCP 策略 VLAN。

数据准备

为完成此配置举例，需准备如下的数据：

- 新加入主机的 MAC 地址
- AC6605 接口的缺省 VLAN

配置步骤

1. 配置 AC6605

   # 全局使能 DHCP 功能，配置 AC6605 的接口 GE0/0/2 和 GE0/0/4 的类型为 Hybrid，并且 VLAN100 的帧以 Untagged 方式通过该接口。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 2
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 2 to 100
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port hybrid pvid vlan 100
[Quidway-GigabitEthernet0/0/4] port hybrid untagged vlan 100
Quidway-GigabitEthernet0/0/4] quit
```

配置基于 MAC 地址的 DHCP 策略 VLAN。

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] dhcp policy-vlan mac-address 001E-9089-C65A priority 5
[Quidway-vlan100] dhcp policy-vlan mac-address 00E0-4C84-0B44 priority 5
[Quidway-vlan100] quit
```

2. 验证配置结果

当 PC1 和 PC2 成功上线获得 IP 地址后，分别从 PC1 和 PC2 上 ping DHCP 服务器，可以 ping 通。

```
C:\>ping 192.168.31.251

Pinging 192.168.31.251 with 32 bytes of data:

Reply from 192.168.31.251: bytes=32 time=126ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.31.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 126ms, Average = 33ms
```

配置文件

AC6605 的配置文件

```
#
dhcp enable
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2 to 100
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
vlan 100
 dhcp policy-vlan mac-address 001e-9089-c65a priority 5
 dhcp policy-vlan mac-address 00e0-4c84-0b44 priority 5
#
return
```

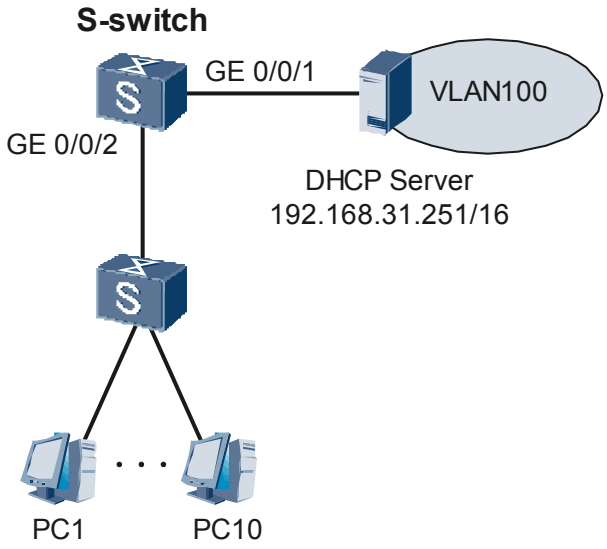
配置基于接口的 DHCP 策略 VLAN 示例

组网需求

如图 4-21 所示，AC6605 的接口 GE0/0/2 连接一台接入交换机，接口 GE0/0/1 连接 DHCP 服务器，该服务器加入到 VLAN100 中。接入交换机连接了 10 台用户主机。

版权所有 © 华为技术有限公司

图 4-21 配置基于接口的 DHCP 策略 VLAN 组网图



配置思路

配置基于接口的 DHCP 策略 VLAN 的思路如下：

1. 全局使能 DHCP 功能。
2. 明确 DHCP 服务器位于哪个 VLAN。
3. 配置基于接口的 DHCP 策略 VLAN。

数据准备

为完成此配置举例，需准备如下的数据：

- AC6605 连接下游接入交换机的接口编号。
- AC6605 接口的缺省 VLAN

配置步骤

1. 配置 AC6605

   # 全局使能 DHCP 功能，配置 AC6605 的接口 GE0/0/1 和 GE0/0/2 的链路类型为 Hybrid，并且 VLAN100 的帧以 Untagged 方式通过该接口。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10 to 100
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 20 to 100
[Quidway-GigabitEthernet0/0/2] quit
```

2. # 配置基于接口的 DHCP 策略 VLAN。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] dhcp policy-vlan port gigabitethernet 0/0/2 priority 5
```

配置文件

AC6605 的配置文件

```
#
dhcp enable
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10 to 100
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20 to 100
#
vlan 100
 dhcp policy-vlan port GigabitEthernet 0/0/2 priority 5
#
return
```

4.7 DNS 配置

通过配置 DNS（Domain Name System）实现网络设备通过域名进行通信。

4.7.1 DNS 概述

为网络上的设备配置域名后，通过域名解析服务器建立域名与 IP 地址的对应关系。用户可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

TCP/IP 不仅提供了 IP 地址来确定设备，而且还专门设计了一种字符串形式的主机命名机制，这就是所谓的域名系统 DNS（Domain Name System）。此系统使用一种有层次的命名方式，为网上的设备指定一个有意义的名字，并且在网络上设置域名解析服务器，建立域名与 IP 地址的对应关系。这样一来用户就可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

4.7.2 AC6605 支持的 DNS 特性

域名解析分为动态 DNS 解析和静态 DNS 解析。

域名解析分为动态 DNS 解析和静态 DNS 解析，二者可以相辅相成，在解析域名时，可以首先采用静态解析的方法，如果静态解析不成功，再采用动态解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可以提高域名解析效率。

AC6605 支持以上两种解析方法。

4.7.3 配置 DNS

通过配置 DNS，建立域名与 IP 地址的对应关系，实现设备使用域名与其他设备通信。

建立配置任务

介绍配置 DNS 的应用环境、前置任务、数据准备和配置过程。

版权所有 © 华为技术有限公司

应用环境

登录到交换机的本地用户如果使用域名与其他设备通信就需要配置 DNS。DNS 表项就是域名与 IP 地址的映射。

如果用户使用域名访问其他设备的次数很少，或者没有可用的 DNS 服务器时，需要配置静态 DNS。配置静态 DNS 需要网络管理员知道域名与 IP 地址的对应关系，且在域名与 IP 地址的对应关系变化时，需要手动修改 DNS 表项。

如果用户需要使用域名访问很多的设备，且有可用的 DNS 服务器，此时可配置动态 DNS。动态 DNS 需要有 DNS 服务器的支持。

前置任务

在配置 DNS 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up
- 配置本交换机与 DNS 服务器之间的路由
- 配置 DNS 服务器

数据准备

在配置 DNS 之前，需准备以下数据。

序号	数据
1	静态 DNS 表项的域名和对应的 IP 地址
2	DNS 服务器的 IP 地址
3	动态 DNS 的域名或域名的列表

配置静态 DNS 表项

可以通过手动建立域名和 IP 地址之间的对应关系表，将一些常用的域名放入表中。当客户端需要域名所对应的 IP 地址时，即到静态域名解析表中去查找指定的域名，获得所对应的 IP 地址，提高域名解析的效率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip host** *host-name ip-address*，配置主机名和对应 IP 地址。

每个主机名只能对应一个 IP 地址，当对同一主机名进行多次配置时，最后配置的 IP 地址有效。如果有多个主机名需要解析，则需要重复步骤 2。

最多可以配置 50 个静态 DNS 表项。

----结束

版权所有 © 华为技术有限公司

配置动态 DNS 服务

动态域名解析需要专用的域名解析服务器，该服务器运行域名解析服务器程序，提供域名和 IP 地址的对应关系，负责接收客户端提出的域名解析请求。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能动态域名解析功能。

步骤 3 执行命令 **dns server** *ip-address*，增加域名服务器。

步骤 4 （可选）执行命令 **dns server source-ip** *source-ip-address*，指定本端交换机的 IP 地址。

指定本端交换机的 IP 地址，以指定的 IP 地址与 DNS 服务器端通信，从而保证通信的安全。

步骤 5 执行命令 **dns domain** *domain-name*，增加域名后缀。

----结束

后续处理

系统最多支持 6 个域名服务器、1 个指定的源地址、10 个域名后缀。如果要配置多个域名服务器，则需重复步骤 3。如果要配置多个域名后缀，则需重复步骤 5。

检查配置结果

可以查看 DNS 的配置信息。

前提条件

已经完成 DNS 功能的所有配置。

操作步骤

- 使用 **display ip host** 命令查看静态 DNS 表。
- 使用 **display dns server** 命令查看域名服务器的配置信息。
- 使用 **display dns domain** 命令查看域名后缀的配置信息。
- 使用 **display dns dynamic-host** 命令查看动态 DNS 表项信息。

----结束

任务示例

执行 **display ip host** 命令，可以查看静态 DNS 表项，包括主机名和 IP 地址的映射信息。

```
<Quidway> display ip host
Host          Age       Flags          Address
hw            0         static         10.1.1.1
gww           0         static         192.168.1.1
```

执行 **display dns server** 命令，可以查看所有域名服务器的 IP 地址。

```
<Quidway> display dns server
IPv4 Dns Servers :
Domain-server        IpAddress
```


版权所有 © 华为技术有限公司

```
    1               172.16.1.1
    2               172.16.1.2

IPv6 Dns Servers :
No configured servers.
```

执行 **display dns domain** 命令，可以查看域名后缀列表。

```
<Quidway> display dns domain
No                  Domain-name
1                   com
2                   net
```

执行 **display dns dynamic-host** 命令，可以查看域名缓存区内的动态 DNS 表项信息。

```
<Quidway> display dns dynamic-host
No  Domain-name         IpAddress       TTL    Alias
1   www.huawei.com      91.1.1.1        3521
2   www.huawei.com.cn   87.1.1.1        3000
```

4.7.4 维护 DNS

维护 DNS 包括清除 DNS 表项、监控 DNS 运行状况。

清除 DNS 表项

介绍了使用 reset 命令清除 DNS 表项。

背景信息



注意

清除 DNS 表项后，将无法恢复，清除之前务必仔细确认。

操作步骤

步骤 1 在确认需要清除动态域名缓存区信息后，请在用户视图下执行 **reset dns dynamic-host** 命令。

----结束

监控 DNS 运行状况

介绍了使用 display 监控 DNS 运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 DNS 的运行情况。

操作步骤

- 在任意视图下执行 **display ip host** 命令，查看静态 DNS 表。
- 在任意视图下执行 **display dns server** 命令，查看域名服务器的配置信息。

版权所有 © 华为技术有限公司

- 在任意视图下执行 **display dns domain** 命令，查看域名后缀的配置信息。
- 在任意视图下执行 **display dns dynamic-host** 命令，查看动态域名缓存区信息。

----结束

调试 DNS

介绍了使用 debugging 命令调试 DNS。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 DNS 运行故障时，请在用户视图下执行下面的 **debugging** 命令对 DNS 进行调试，查看调试信息，定位故障并分析故障原因。

打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南-系统管理》中信息中心的内容。有关 **debugging** 命令的解释请参见《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

步骤 1 在用户视图下执行 **debugging dns** 命令，调试动态 DNS。

----结束

4.7.5 配置举例

举例说明 DNS 的配置。

配置 DNS 示例

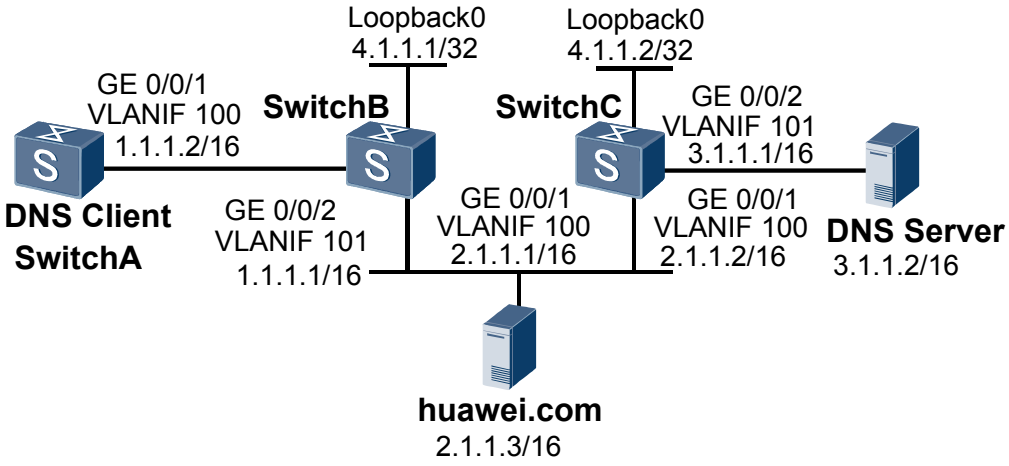
组网需求

如图 4-22 所示，设备 SwitchA 作为 DNS Client 端和 DNS Server 配合，使得设备 SwitchA 通过域名（huawei.com）能够访问 IP 地址为 2.1.1.3/16 的主机，配置域名后缀 com 和 net。

在 SwitchA 上配置 SwitchB 和 SwitchC 的静态 DNS 表项，使得 SwitchA 能够使用域名（SwitchB 和 SwitchC）对设备进行管理。

版权所有 © 华为技术有限公司

图 4-22 配置 DNS 组网图



配置思路

DNS 的配置思路如下：

1. 配置静态 DNS 表项
2. 使能 DNS 域名解析功能
3. 配置 DNS 服务器的 IP 地址
4. 配置域名后缀

数据准备

为完成此配置举例，需要准备如下数据：

- 设备 SwitchB 和 SwitchC 的域名名称
- DNS 服务器的 IP 地址
- 域名后缀

操作步骤

步骤 1 配置设备 SwitchA

配置静态 DNS 表项。

```
<SwitchA> system-view
[SwitchA] ip host SwitchB 4.1.1.1
[SwitchA] ip host SwitchC 4.1.1.2
```

使能 DNS 域名解析功能。

```
[SwitchA] dns resolve
```

配置 DNS Server 的 IP 地址。

```
[SwitchA] dns server 3.1.1.2
```

配置域名后缀 net。

```
[SwitchA] dns domain net
```


版权所有 © 华为技术有限公司

配置域名后缀 com。

```
[SwitchA] dns domain com
[SwitchA] quit
```

说明

若要完成对域名的解析，还需要配置 SwitchA 至 DNS Server 的路由。路由的配置方法请参看《AC6605 无线接入控制器 配置指南-IP 路由》。

步骤 2 验证配置结果

在设备 SwitchA 上执行 **ping huawei.com** 命令，可以 ping 通，且对应的目的地址为 2.1.1.3。

```
<SwitchA> ping huawei.com
Trying DNS server (3.1.1.2)
  PING huawei.com (2.1.1.3): 56  data bytes, press CTRL_C to break
    Reply from 2.1.1.3: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2.1.1.3: bytes=56 Sequence=2 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=3 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=4 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=5 ttl=126 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

在 SwitchA 用 **display ip host** 命令可以查看到静态 DNS 表项中主机名和 IP 地址的对应关系。

```
<SwitchA> display ip host
Host                 Age        Flags  Address
SwitchB              0          static 4.1.1.1
SwitchC              0          static 4.1.1.2
```

在 SwitchA 用 **display dns dynamic-host** 命令可以查看到动态缓存区中的动态 DNS 表项信息。

```
<SwitchA> display dns dynamic-host
No  Domain-name          IpAddress            TTL      Alias
1   huawei.com           2.1.1.3              3579
```

说明

显示信息中的 TTL 表示该表项存在的时间，单位是秒。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
 ip host SwitchB 4.1.1.1
 ip host SwitchC 4.1.1.2
#
 dns resolve
 dns server 3.1.1.2
 dns domain net
 dns domain com
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ip address 1.1.1.2 255.255.0.0
#
rip 1
 network 1.0.0.0
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 101
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface LoopBack0
 ip address 4.1.1.1 255.255.255.255
#
interface vlanif100
 ip address 2.1.1.1 255.255.0.0
#
interface vlanif101
 ip address 1.1.1.1 255.255.0.0
#
rip 1
 network 2.0.0.0
 network 1.0.0.0
 network 4.0.0.0
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 100 101
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface LoopBack0
 ip address 4.1.1.2 255.255.255.255
#
interface vlanif100
 ip address 2.1.1.2 255.255.0.0
#
interface vlanif101
 ip address 3.1.1.1 255.255.0.0
#
rip 1
 network 2.0.0.0
 network 3.0.0.0
network 4.0.0.0
```


版权所有 © 华为技术有限公司

```
#
return
```

4.8 IPv6 基础配置

介绍了 IPv6 的基本概念和特性及相关配置过程。

4.8.1 IPv6 概述

介绍 IPv6 的基本概念。

IPv6 基本概念

IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation），它是 Internet 工程任务组（IETF）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别就是 IP 地址的长度从 32 位升为 128 位。

IPv6 地址介绍

IPv6 的 128 位 IP 地址有以下两种表示形式。

- X:X:X:X:X:X:X:X

  在这种形式中，128 位的 IP 地址被分为 8 组，每组的 16 位用 4 个十六进制字符（0 ～ 9，A ～ F）来表示，组和组之间用冒号（:）隔开。其中每个“X”代表一组十六进制数值。
- X:X:X:X:X:X:d.d.d.d

  分为如下两种类型

  - IPv4 兼容 IPv6 地址
  - IPv4 映射 IPv6 地址

  其中 IPv4 兼容 IPv6 地址用于配置 IPv6 over IPv4 隧道。

  在这种形式中，“X”代表高阶的六组数字，用十六进制数来表示每组的 16 比特。“d”代表低阶的四组数字，用十进制数表示每组的 8 比特。后边的部分（d.d.d.d）其实就是一个标准的 IPv4 地址。

一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID。
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID。

4.8.2 AC6605 支持的 IPv6 特性

AC6605 支持 IPv6 协议族以及 TCP6 协议族。

AC6605 支持的 IPv6 特性

AC6605 支持在 VLANIF 接口、Loopback 接口和 Tunnel 接口配置 IPv6 地址。

每个接口最多可配置 20 个 IPv6 地址，包括链路本地地址和全球单播地址。

链路本地地址用于邻居发现协议和无状态自动配置进程中链路本地节点之间的通信。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。

版权所有 © 华为技术有限公司

链路本地地址可以通过自动生成或手动配置两种方式获得：使能系统自动配置链路本地地址的命令后，系统将为接口自动生成一个链路本地地址；手动配置的链路本地地址必须是一个有效的链路本地地址（FE80::/10）。

因为链路本地地址只能用于链路本地节点之间的通信，通常用于满足协议的通信需求，与用户间的通信没有直接关系，所以推荐使用链路本地地址的自动生成方式。

全球单播地址等同于 IPv4 公网地址，用于公网上的数据转发，是用户通信所必需的地址。

EUI-64 地址与全球单播地址作用相同，区别是前者只需指定网络位，其主机位由接口的 MAC 地址转化而来，而后者需要指定整个 128bit 的完整地址。

IPv6 邻居发现

IPv6 邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议代替了 IPv4 中的 ARP 协议（Address Resolution Protocol）、ICMP 重定向消息（Redirect）、和 ICMP 设备发现消息（Router Discovery），并提供了其他功能。

IPv6 的 FIB 特性

为了连接不同的网络拓扑需要运行不同的路由协议，这样就产生了 RIB（Routing Information base）。RIB 是创建 FIB 的基础，AC6605 会根据路由管理策略，从 RIB 中提取出最小转发信息并放入 FIB。用户还可通过路由管理向 FIB 中增加静态路由。

FIB（Forwarding Information Base）中包含了 AC6605 在转发报文时所必需的一组最小信息。一个 FIB 条目中一般包括目的地址、前缀长度、传输端口、下一跳地址、标明路由特征的标志以及时间戳。AC6605 使用 FIB 的各项来转发报文。

FIB 的操作包括两个单独的部分，用于控制平面的是 FibAgent，用于转发平面的是 FibContainer。控制平面（FibAgent）负责跟 RM 模块交互，将 FIB 下载到转发引擎，对于分布式系统，还需要将 FIB 下载到 I/O 板。

FIB 包含的元素有：

- Destination address：报文发送的目的网络地址或主机地址。
- Prefix length：目的地址前缀长度，可确定目的地址是否对应网络或主机。
- Nexthop：为了将报文发送到目的地址所要经过的紧邻的下一跳地址。
- Flag(s)：标明路由特征。
- Interface：报文的出接口。
- Timestamp：FIB 项生成的时间。

4.8.3 配置接口的 IPv6 地址

手工为网络设备配置 IPv6 地址，使该设备可以与网络上其他设备进行通信。

建立配置任务

介绍配置接口的 IPv6 地址的应用环境、前置任务、数据准备和配置过程。

应用环境

在交换机与 IPv6 设备通信时，需要为接口配置 IPv6 地址。

版权所有 © 华为技术有限公司

EUI-64 地址与全球单播地址作用相同，区别是前者只需指定网络位，其主机位由接口的 MAC 地址转化而来，而后者需要指定整个 128bit 的完整地址。需要注意的是，EUI-64 地址指定的网络位前缀长度（prefix-length）不能大于 64。

EUI-64 地址和全球单播地址可以同时配置，也可以任选其一，都可以完成正常通信；但是同一接口下配置的多个地址不能属于同一网段。

前置任务

在配置接口的 IPv6 地址之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up

数据准备

在配置接口的 IPv6 地址之前，需准备以下数据。

序号	数据
1	接口的编号
2	手动配置的链路本地地址
3	全球单播地址和前缀长度

启动 IPv6 报文转发功能

在接口视图下使能了 IPv6 功能，才能在接口下进行其他 IPv6 相关的配置。如果希望接口可以转发 IPv6 报文，还必须在系统视图下使能 IPv6 功能。

背景信息

如果要使能接口对 IPv6 报文进行转发的功能，必须同时使能系统视图下和接口视图下的 IPv6 功能。因为：

- 在系统视图下执行命令 **ipv6**，只是使能了交换机对 IPv6 报文的转发功能，并没有使能接口的 IPv6 功能，也不能进行 IPv6 的相关配置。
- 在接口视图下执行命令 **ipv6 enable**，只是使能了接口的 IPv6 功能，接口的 IPv6 协议状态仍是 Down，交换机不能对 IPv6 报文进行转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6**，使能交换机 IPv6 报文转发能力

缺省情况下，交换机不使能对 IPv6 报文的转发能力。

如果要对 IPv6 报文进行转发，必须先在系统视图下使能交换机的 IPv6 报文转发能力。否则即使在接口上使能了 IPv6 功能，接口的 IPv6 协议仍处于 Down 状态，交换机无法转发 IPv6 的报文。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **interface** *interface-type interface-number*，进入需要使能 IPv6 功能的 VLANIF 接口视图。

步骤 4 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

如果要在接口视图下进行 IPv6 的相关配置，必须先在接口视图下使能 IPv6 功能。

缺省情况下，接口下不使能 IPv6 功能。

----结束

配置接口的链路本地 IPv6 地址

链路本地地址用于邻居发现协议和无状态自动配置进程中链路本地上节点之间的通信。链路本地地址只在本地链路有效。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 请根据不同情况进行以下配置。

- 如果配置接口的自动链路本地地址，请执行命令 **ipv6 address auto link-local**。
- 如果手动配置接口的链路本地地址，请执行命令 **ipv6 address** *ipv6-address* **link-local**。

如果不使用命令配置接口的链路本地地址，当**配置接口的全球单播 IPv6 地址**后，会自动生成一个链路本地地址。

----结束

配置接口的全球单播 IPv6 地址

全球单播地址等同于 IPv4 公网地址，可用于路由前缀可以聚合的链路，降低路由表项的数量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } 或 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**，配置接口的全球单播地址。

----结束

检查配置结果

前提条件

已经完成 IPv6 地址的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令查看接口 IPv6 信息。
- 使用 **display ipv6 statistics** 命令查看 IPv6 报文统计信息。

----结束

4.8.4 配置 IPv6 邻居发现

IPv6 邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议代替了 IPv4 中的 ARP 协议（Address Resolution Protocol）、ICMP 设备发现消息（Router Discovery）和 ICMP 重定向消息（Redirect）。新增了邻居可达性检测功能。

建立配置任务

介绍配置 IPv6 邻居发现的应用环境、前置任务、数据准备和配置过程。

应用环境

大部分的 ND 配置是基于接口来实现的。

前置任务

在配置 IPv6 ND 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数
- 配置接口的 IPv6 地址

数据准备

在配置 IPv6 ND 之前，需准备以下数据。

序号	数据
1	需要配置 IPv6 ND 的接口的编号
2	静态邻居的 IPv6 地址和 MAC 地址
3	RA 消息的发布间隔时间、前缀和存活时间
4	自动配置的标志位
5	ND 的跳数限制
6	DAD 发送次数
7	NS 消息重传时间间隔
8	NUD 可达时间
9	接口 MTU

版权所有 © 华为技术有限公司

配置静态邻居

通过手工配置静态邻居，可以获得邻居的 IPv6 地址和 MAC 地址的映射关系。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 根据不同类型的接口，执行以下命令：

- 配置 VLANIF 接口的静态邻居表项时，执行 **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number* 命令。

----结束

打开 RA 消息的发布开关

打开交换机通告的开关，设备可以发布 RA 报文，为主机提供前缀等信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 执行命令 **undo ipv6 nd ra halt**，使能 RA 消息的发布功能。

----结束

配置 RA 消息的发布周期

交换机周期性的发布 RA 报文，其中包括前缀和一些标志位的信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 执行命令 **ipv6 nd ra** { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }，配置 RA 消息发布间隔时间。

缺省情况下，最大时间间隔是 600 秒，最小时间间隔是 200 秒。

最大时间间隔不能小于最小时间间隔。

当 RA 报文的最大发布间隔设置为小于 9 秒时，将最小发布间隔时间调整为与最大发布间隔时间相同。

----结束

版权所有 © 华为技术有限公司

使能有状态自动配置

使能了有状态自动配置，则主机通过有状态自动配置（例如 DHCP 服务器）来获得 IPv6 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 执行命令 **ipv6 nd autoconfig managed-address-flag**，设置地址有状态自动配置标志位。

如果设置了地址有状态自动配置标志位，主机进行有状态自动配置，否则主机进行无状态自动配置。

步骤 5 执行命令 **ipv6 nd autoconfig other-flag**，设置其他信息有状态自动配置标志位。

如果设置了其他信息有状态自动配置标志位，主机使用有状态自动配置获取其他信息。

----结束

配置需要发布的地址前缀信息

本地链路上的节点可以使用这些前缀完成地址自动配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 4 执行命令 **ipv6 nd ra prefix** { *ipv6-address ipv6*‑*prefix-length* | *ipv6-prefix*/*ipv6*‑*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]，配置 RA 消息中的前缀。

----结束

配置需要发布的其他信息

RA 报文中携带交换机发布报文的跳数限制、前缀选项、邻居可达时间、RA 报文的存活时间。

背景信息

重复地址检测 DAD（Duplicate Address Detect）是 IPv6 进行地址自动配置时的一个过程，可以配置连续发送的 DAD 消息的数量。

设置交换机发送邻居请求 NS（Neighbor Solicitation）消息的时间间隔。缺省情况下，NS 重传间隔时间是 1000 毫秒。

NUD（Neighbor Unreachability Detection）表示邻居不可达性检测。缺省情况下，NUD 可达时间为 30000 毫秒。

版权所有 © 华为技术有限公司

接口的最大传输单元 MTU 确定了接口上的 IP 报文是否需要分片。接口 MTU 的缺省值根据接口类型的不同而不同，GigabitEthernet 的 MTU 为 1500 字节。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 nd hop-limit** *limit*，配置跳数限制。

参数 *limit* 的取值范围是 1 ～ 255。缺省情况下，跳数限制为 64 跳。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 5 执行命令 **ipv6 nd ra router-lifetime** *ra-lifetime*，配置 RA 消息的存活时间。

说明

- 在执行 **ipv6 nd ra** 命令设置 RA 消息的发布间隔时间时，发布间隔时间应该小于或等于 IPv6 RA 消息的存活时间。
- 缺省情况下，RA 消息的发布最大间隔时间为 600 秒，最小间隔时间为 200 秒。
- 缺省情况下，RA 消息的存活时间为 1800 秒。如果配置了 RA 消息的前缀信息，存活时间仍为 1800 秒。

步骤 6 执行命令 **ipv6 nd dad attempts** *value*，配置 DAD 发送次数。

步骤 7 执行命令 **ipv6 nd ns retrans-timer** *interval*，配置 NS 消息重传时间间隔。

步骤 8 执行命令 **ipv6 nd nud reachable-time** *value*，配置 NUD 可达时间。

步骤 9 执行命令 **ipv6 mtu** *mtu*，配置接口 MTU。

----结束

后续处理

修改了 IPv6 的 MTU 值之后，需要在该接口视图下依次执行 **shutdown** 和 **undo shudown** 命令，配置才会生效。

检查配置结果

可以查看 IPv6 邻居发现的配置信息。

前提条件

已经完成 IPv6 邻居发现的所有配置。

操作步骤

- 使用 **display ipv6 neighbors** [[**vid** *vlan-id*] *interface-type interface-number*]命令查看邻居缓存的内容。
- 使用 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令查看接口 IPv6 信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display ipv6 neighbors**，可以看到邻居缓存中有 IPv6 地址和所属接口等信息。

```
<Quidway> display ipv6 neighbors VLANIF10
------------------------------------------------------------
IPv6 Address : 3003::2
Link-layer   : 00e0-fc89-fe6e            State : STALE
Interface    : VLANIF10                   Age   : 7
VPN name     : vpn1                      VLAN  : -

IPv6 Address : FE80::2E0:FCFF:FE89:FE6E
Link-layer   : 00e0-fc89-fe6e            State : STALE
Interface    : VLANIF10                   Age   : 7
VPN name     : vpn1                      VLAN  : -
------------------------------------------------------------
Total: 2       Dynamic: 2       Static: 0
```

执行命令 **display ipv6 interface brief**，能够查看接口配置的 IPv6 地址以及接口状态。

```
<Quidway> display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical             Protocol
VLANIF20         up                    up
[IPv6 Address] 2030::101:101
VLANIF30         up                    up
[IPv6 Address] 2001::1
LoopBack0                  up                   up(s)
[IPv6 Address] Unassigned
```

4.8.5 维护 IPv6

维护 IPv6 包括清除 IPv6 运行信息、监控 IPv6 运行状况。

清除 IPv6 运行信息

背景信息

注意

清除 IPv6 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除数据包的 IPv6 报文处理的统计信息后，请在用户视图下执行 **reset ipv6 statistics** 命令。
- 在确认需要清除 IPv6 邻居缓存项后，请在用户视图下执行 **reset ipv6 neighbors** { **all** | **dynamic** | **static** | **vid** *vlan-id* [*interface-type interface-number*] | *interface-type interface-number* }命令。
- 在确认需要清除所有 TCP6 统计信息后，请在用户视图下执行 **reset tcp ipv6 statistics** 命令。

版权所有 © 华为技术有限公司

- 在确认需要清除所有 UDP6 统计信息后，请在用户视图下执行 **reset udp ipv6 statistics** 命令。

----结束

监控 IPv6 运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 IPv6 的运行情况。

操作步骤

- 在任意视图下执行 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令，查看接口的 IPv6 信息。
- 在任意视图下执行 **display ipv6 statistics** 命令，查看 IPv6 报文的统计信息。
- 在任意视图下执行 **display ipv6 neighbors** [[**vid** *vlan-id*] *interface-type interface-number*]命令，查看邻居缓存的内容。
- 在任意视图下执行 **display tcp ipv6 statistics** 命令，查看相关的 TCP6 统计信息。
- 在任意视图下执行 **display tcp ipv6 status** 命令，查看 TCP6 连接状态。
- 在任意视图下执行 **display udp ipv6 statistics** 命令，查看 UDP6 相关统计信息。
- 在任意视图下执行 **display ipv6 socket** [**socktype** *socket-type*] [*task-id socket-id*]命令，查看指定套接字的相关信息。
- 在任意视图下执行 **display ipv6 fib** [*existing-slot-id*]命令，查看 FIB 信息。

----结束

调试 IPv6

介绍了使用 debugging 命令调试 IPv6。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 IPv6 运行故障时，请在用户视图下执行下面的 **debugging** 命令对 IPv6 进行调试，查看调试信息，定位故障并分析故障原因。

打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南-系统管理》中信息中心的内容。有关 **debugging** 命令的解释请参见《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 在用户视图下执行 **debugging ipv6 icmpv6** 命令，调试 ICMPv6。

版权所有 © 华为技术有限公司

- 在用户视图下执行 **debugging ipv6 nd** 命令，调试 IPv6 的邻居状态和消息。
- 在用户视图下执行 **debugging ipv6 packet** [**error**] [**acl** *acl-number*]命令，调试 IPv6 报文。
- 在用户视图下执行 **debugging ipv6 pathmtu** 命令，调试 PMTU。
- 在用户视图下执行 **debugging tcp ipv6** { **event** | **packet** } [**task-id** *task id* | **socket-id** *socket id*]命令，调试 TCP6。
- 在用户视图下执行 **debugging udp ipv6 packet** [**task-id** *task id* | **socket-id** *socket id*] 命令，调试 UDP6。

----结束

4.8.6 配置举例

举例说明 IPv6 地址的配置。

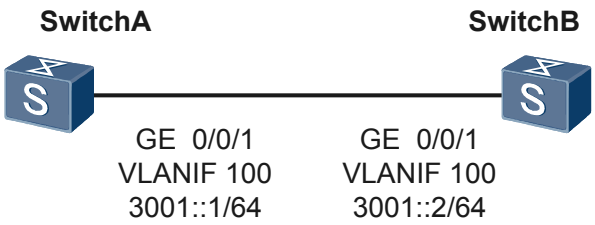
配置接口的 IPv6 地址示例

组网需求

如图 4-23 所示，两台 Switch 通过 GE0/0/1 接口相连，SwitchA 及 SwitchB 的 GE0/0/1 接口分别对应各自的 VLANIF100 接口，为 VLANIF100 接口配置 IPv6 全球单播地址，验证它们之间的三层互通性。

需要配置的全球单播地址为 3001::1/64 和 3001::2/64。

图 4-23 配置接口的 IPv6 地址组网图



配置思路

配置接口的 IPv6 地址思路如下：

1. 使能 Switch 的 IPv6 转发能力
2. 配置接口的 IPv6 全球单播地址

数据准备

为完成此配置例，需准备如下的数据：

- 接口的全球单播地址

版权所有 © 华为技术有限公司

操作步骤

步骤 1 使能 Switch 的 IPv6 转发能力

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
```

步骤 2 配置接口的全球单播地址

配置 SwitchA。

```
[SwitchA] vlan 100
[SwitchA-Vlan100] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ipv6 enable
[SwitchA-Vlanif100] ipv6 address 3001::1/64
[SwitchA-Vlanif100] quit
```

配置 SwitchB。

```
[SwitchB] vlan 100
[SwitchB-Vlan100] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ipv6 enable
[SwitchB-Vlanif100] ipv6 address 3001::2/64
[SwitchB-Vlanif100] quit
```

步骤 3 验证配置结果

如果配置成功，可以查看配置的全球单播地址，以及接口状态为 Up，IPv6 协议状态为 Up。

显示 SwitchA 的接口信息。

```
[SwitchA] display ipv6 interface vlanif 100
Vlanif100 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::218:20FF:FE00:83 [TENTATIVE]
  Global unicast address(es):
    3001::1, subnet is 3001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF00:83
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

显示 SwitchB 的接口信息。

版权所有 © 华为技术有限公司

```
[SwitchB] display ipv6 interface vlanif 100
Vlanif100 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE33:11 [TENTATIVE]
  Global unicast address(es):
    3001::2, subnet is 3001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:2
    FF02::1:FF33:11
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

从 SwitchA 上 PingSwitchB 的链路本地地址，注意需要使用**-i** 参数，来指定链路本地地址的接口。

```
[SwitchA] ping ipv6 FE80::2E0:FCFF:FE33:11 -i vlanif 100
  PING FE80::2E0:FCFF:FE33:11 : 56  data bytes, press CTRL_C to break
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=1 hop limit=64  time = 7 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=3 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=4 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=5 hop limit=64  time = 3 ms

  --- FE80::2E0:FCFF:FE33:11 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/7 ms
```

从 SwitchA 上 PingSwitchB 的全球单播 IPv6 地址。

```
[SwitchA] ping ipv6 3001::2
  PING 3001::2 : 56  data bytes, press CTRL_C to break
    Reply from 3001::2
    bytes=56 Sequence=1 hop limit=64  time = 12 ms
    Reply from 3001::2
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=3 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=4 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=5 hop limit=64  time = 3 ms

  --- 3001::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/4/12 ms
```

----结束

配置文件

- SwitchA 配置文件

```
#
 sysname SwitchA
#
```


版权所有 © 华为技术有限公司

```
ipv6
#
 vlan 100
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::1/64
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- SwitchB 配置文件

```
#
 sysname SwitchB
#
ipv6
#
 vlan 100
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::2/64
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

4.9 IPv6 DNS 配置

通过配置 IPv6 DNS（Domain Name System）实现网络设备通过域名进行通信。

4.9.1 IPv6 DNS 概述

为网络上的设备配置域名后，通过域名解析服务器建立域名与 IPv6 地址的对应关系。用户可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

域名解析分为动态 IPv6 DNS 解析和静态 IPv6 DNS 解析，二者可以相辅相成，在解析域名时，可以首先采用静态解析的方法，如果静态解析不成功，再采用动态解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可以提高域名解析效率。

4.9.2 AC6605 支持的 IPv6 DNS 特性

域名解析分为动态 IPv6 DNS 解析和静态 IPv6 DNS 解析。

IPv6 DNS 与 IPv4 DNS 类似，IPv4 DNS 的配置请参见 **DNS 配置**。

4.9.3 配置 IPv6 DNS

通过配置 IPv6 DNS，建立域名与 IPv6 地址的对应关系，实现设备使用域名与其他设备通信。

建立配置任务

介绍配置 IPv6 DNS 的应用环境、前置任务、数据准备和配置过程。

版权所有 © 华为技术有限公司

应用环境

登录到交换机的本地用户如果使用域名与其他设备通信就需要配置 DNS。IPv6 DNS 表项就是域名与 IPv6 地址的映射。

如果用户使用域名访问其他设备的次数很少，或者没有可用的 DNS 服务器时，需要配置静态 DNS。配置静态 IPv6 DNS 需要网络管理员知道域名与 IPv6 地址的对应关系，且在域名与 IPv6 地址的对应关系变化时，需要手动修改 IPv6 DNS 表项。

如果用户需要使用域名访问很多的设备，且有可用的 DNS 服务器，此时可配置动态 DNS。动态 DNS 需要有 DNS 服务器的支持。

前置任务

在配置 IPv6 DNS 之前，需完成配置本地交换机与 DNS 服务器之间的路由。

数据准备

在配置 IPv6 DNS 之前，需准备以下数据。

序号	数据
1	静态 IPv6 DNS 表项的域名和对应的 IPv6 地址
2	IPv6 DNS 服务器的 IPv6 地址
3	动态 IPv6 DNS 的域名或域名的列表

配置静态 IPv6 DNS 表项

可以通过手动建立域名和 IPv6 地址之间的对应关系表，将一些常用的域名放入表中。当客户端需要域名所对应的 IPv6 地址时，即到静态域名解析表中去查找指定的域名，获得所对应的 IPv6 地址，提高域名解析的效率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6**，使能 IPv6 功能。

步骤 3 执行命令 **ipv6 host** *host-name ipv6-address*，配置主机名和对应 IPv6 地址。

如果一个主机名配置了多个与之对应的 IPv6 地址（最多可配置 8 个 IPv6 地址），当使用主机名查找地址，如 ping 主机时，使用第一个配置的地址。

----结束

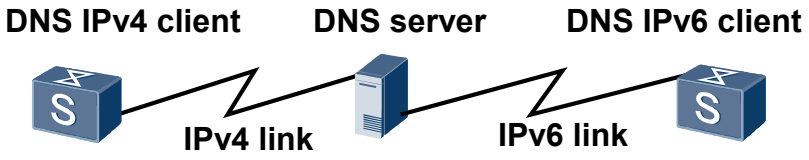
配置动态 IPv6 DNS 服务

动态域名解析需要专用的域名解析服务器，该服务器运行域名解析服务器程序，提供域名和 IPv6 地址的对应关系，负责接收客户端提出的域名解析请求。

版权所有 © 华为技术有限公司

背景信息

图 4-24 连接 IPv4 和 IPv6 网络的 DNS 服务器



注意

如果配置了多个 DNS 服务器，将按配置顺序进行查询直到收到正确的响应报文。如果 IPv4 和 IPv6 服务器都进行了配置，首先向 IPv4 服务器发送 A 查询报文，向 IPv6 服务器发送 AAAA 查询报文。

可在交换机上配置 DNS 域，域名可用来查找。如果主机名的 DNS 查找失败，域名就会加在主机名后的“.”后面，然后继续查找。可以配置比较常见的域名，如“com”或“net”。如果主机名为“huawei”，查找失败后就会再次查询“huawei.com”或“Huawei.net”。

请在交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能动态域名解析功能。

步骤 3 执行命令 **dns server ipv6** *ipv6-address* [*interface-type interface-number*]，配置 IPv6 的 DNS 服务器。

步骤 4 执行命令 **dns server ipv6 source-ip** *ipv6-address*，指定本端交换机的 IPv6 地址。

指定本端交换机的 IPv6 地址后，以指定的 IPv6 地址与 DNS 服务端通信，从而达到进行安全校验的目的。

步骤 5 执行命令 **dns domain** *domain-name*，增加域名后缀。

----结束

检查配置结果

可以查看 IPv6 DNS 的配置信息。

前提条件

已经完成基于 IPv6 的 DNS 的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display ipv6 host** 命令查看静态 IPv6 DNS 表。
- 使用 **display dns server** 命令查看域名服务器的配置信息。
- 使用 **display dns domain** 命令查看域名后缀列表的配置信息。
- 使用 **display dns ipv6 dynamic-host** 命令查看动态域名缓存区信息。

----结束

任务示例

执行 **display ipv6 host** 命令，能得到静态 IPv6 DNS 表项，包括主机名和 IPv6 地址的结果。

```
<Quidway> display ipv6 host
Host                  Age        Flags    IPv6Address (es)
RTB                   0          static   20::1
RTA                   0          static   20::2
```

执行 **display dns server** 命令，能得到所有域名服务器的 IPv6 地址的结果。

```
<Quidway> display dns server
IPv4 Dns Servers :
Domain-server      IpAddress
     1            169.254.65.125
IPv6 Dns Servers:
Domain-server Ipv6Address            (Interface Name)
     1        3001::2
     2        FE80::2                  GigabitEthernet6/0/0
```

执行 **display dns domain** 命令，能得到域名后缀的结果。

```
<Quidway> display dns domain
No                  Domain-name
1                   com
2                   net
```

执行 **display dns ipv6 dynamic-host** 命令，能得到动态域名缓存区内的相关信息的结果。

```
<Quidway> display dns ipv6 dynamic-host
No  Domain-name       Ipv6address      TTL
1   huawei6           3001::2          6
```

4.9.4 维护 IPv6 DNS

维护 IPv6 DNS 包括清除 IPv6 DNS 表项或监控 IPv6 DNS 运行状况。

清除 IPv6 DNS 表项

介绍了使用 reset 命令清除 IPv6 DNS 表项。

背景信息

注意

清除 IPv6 DNS 表项后，以前的信息将无法恢复，务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在确认需要清除 IPv6 DNS 动态域名缓存后，请在用户视图下执行 **reset dns ipv6 dynamic-host** 命令。

----结束

监控 IPv6 DNS 运行状况

介绍了使用 display 命令监控 IPv6 DNS 运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 IPv6 DNS 的运行情况。

操作步骤

- 在任意视图下执行 **display dns domain** 命令，查看域名。
- 在任意视图下执行 **display dns server** 命令，查看域名服务器的配置。
- 在任意视图下执行 **display dns ipv6 dynamic-host** 命令，查看 IPv6 动态域名缓存的内容。
- 在任意视图下执行 **display ipv6 host** 命令，查看静态域名解析表。

----结束

4.9.5 配置举例

举例说明 IPv6 DNS 的配置。

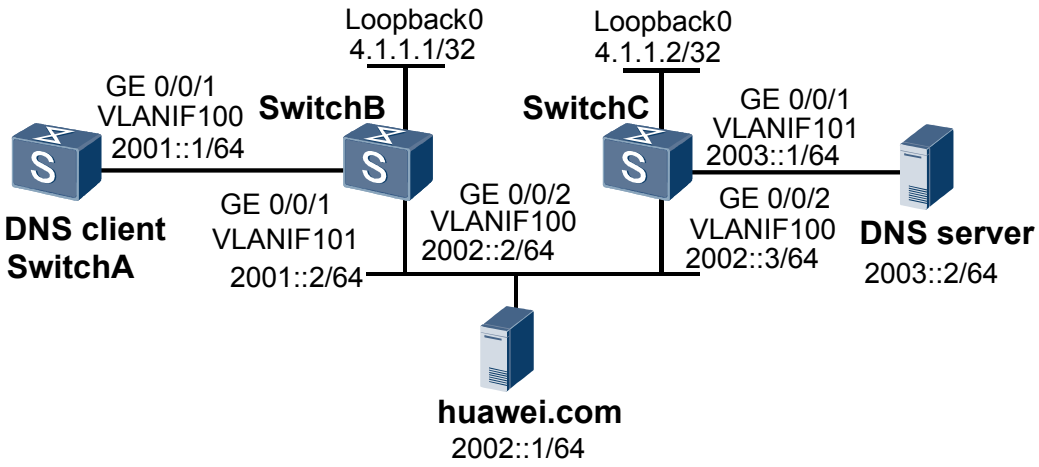
配置 IPv6 DNS 示例

组网需求

如图 4-25 所示，设备 SwitchA 作为 IPv6 DNS Client 端和 IPv6 DNS Server 配合，使得 SwitchA 通过域名（huawei.com）能够访问 IP 地址为 2002::1/64 的主机。

在 SwitchA 上配置 SwitchB 和 SwitchC 的静态 IPv6 DNS 表项，使得 SwitchA 能够使用域名（SwitchB 和 SwitchC）对设备进行管理。

图 4-25 配置 IPv6 DNS 组网图



版权所有 © 华为技术有限公司

配置思路

IPv6 DNS 的配置思路如下：

1. 配置静态 IPv6 DNS 表项
2. 使能 DNS 域名解析功能
3. 配置 IPv6 DNS 服务器的 IPv6 地址
4. 配置域名后缀

数据准备

为完成此配置举例，需要准备如下数据：

- SwitchB 和 SwitchC 的域名名称
- DNS 服务器的 IPv6 地址
- 域名后缀

操作步骤

步骤 1 配置 SwitchA

配置静态 IPv6 DNS 表项。

```
<SwitchA> system-view
[SwitchA] ipv6 host SwitchB 2001::2
[SwitchA] ipv6 host SwitchC 2002::3
```

使能 DNS 域名解析功能。

```
[SwitchA] dns resolve
```

配置 DNS Server 的 IP 地址。

```
[SwitchA] dns server ipv6 2003::2
```

配置域名后缀 net。

```
[SwitchA] dns domain net
```

配置域名后缀 com。

```
[SwitchA] dns domain com
[SwitchA] quit
```

说明

若要完成对域名的解析，还需要配置 SwitchA 至 IPv6 DNS Server 的路由。路由的配置方法请参看《AC6605 无线接入控制器 配置指南-IP 路由》中**配置静态路由举例**。

步骤 2 验证配置结果

在路由设备 SwitchA 上执行 **ping ipv6 huawei.com** 命令，可以 ping 通，且对应的目的地址为 2002::1。

```
<SwitchA> ping ipv6 huawei.com
  Resolved Host ( huawei.com -> 2002::1)
  PING huawei.com : 56  data bytes, press CTRL_C to break
    Reply from 2002::1: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2002::1: bytes=56 Sequence=2 ttl=126 time=4 ms
```


版权所有 © 华为技术有限公司

```
  Reply from 2002::1: bytes=56 Sequence=3 ttl=126 time=4 ms
  Reply from 2002::1: bytes=56 Sequence=4 ttl=126 time=4 ms
  Reply from 2002::1: bytes=56 Sequence=5 ttl=126 time=4 ms

--- huawei.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/6 ms
```

在 SwitchA 用 **display ipv6 host** 命令可以查看到静态 IPv6 DNS 表项中主机名和 IPv6 地址的对应关系。

```
<SwitchA> display ipv6 host
Host              Age        Flags   IPv6Address (es)
SwitchB           0          static  2001::2
SwitchC           0          static  2002::3
```

在 SwitchA 用 **display dns ipv6 dynamic-host** 命令可以查看到动态缓存区中的动态 IPv6 DNS 表项信息。

```
<SwitchA> display dns ipv6 dynamic-host
No  Domain-name           Ipv6address          TTL
1   huawei.com            2002::1              3579
```

说明

显示信息中的 TTL 表示该表项存在的时间，单位是秒。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
 ipv6
#
 ipv6 host SwitchB 2001::2
 ipv6 host SwitchC 2002::3
#
 dns resolve
 dns server ipv6 2003::2
 dns domain net
 dns domain com
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ipv6 enable
 ipv6 address 2001::1/64
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 101
#
 ipv6
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ipv6 enable
 ipv6 address 2002::2/64
#
interface vlanif101
 ipv6 enable
 ipv6 address 2001::2/64
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 100 101
#
 ipv6
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ipv6 enable
 ipv6 address 2002::3/64
#
interface vlanif101
ipv6 enable
 ipv6 address 2003::1/64
#
return
```

4.10 IPv6 over IPv4 隧道配置

IPv6 over IPv4 隧道技术的出现解决了 IPv4 网路向 IPv6 网络过渡的问题。

4.10.1 IPv6 over IPv4 概述

IPv6 报文被封装在 IPv4 报文中，实现 IPv6 报文的透明传输。

在 IPv4 Internet 向 IPv6 Internet 过渡的初期，IPv4 网络已被大量部署，而 IPv6 网络只是散布在世界各地的一些孤岛。采用专用的线路将这些孤岛互连起来，显然是不经济的，通常的做法是采用隧道技术。利用隧道技术可在 IPv4 网络上创建隧道，从而实现 IPv6 孤岛的互连。这类似于在 IP 网络上利用隧道技术部署 VPN 的情况。

在 IPv4 网络上用于连接 IPv6 孤岛的隧道，称为 IPv6 over IPv4 隧道。为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界交换机上启动 IPv4/IPv6 双协议栈。

4.10.2 AC6605 支持的 IPv6 over IPv4 特性

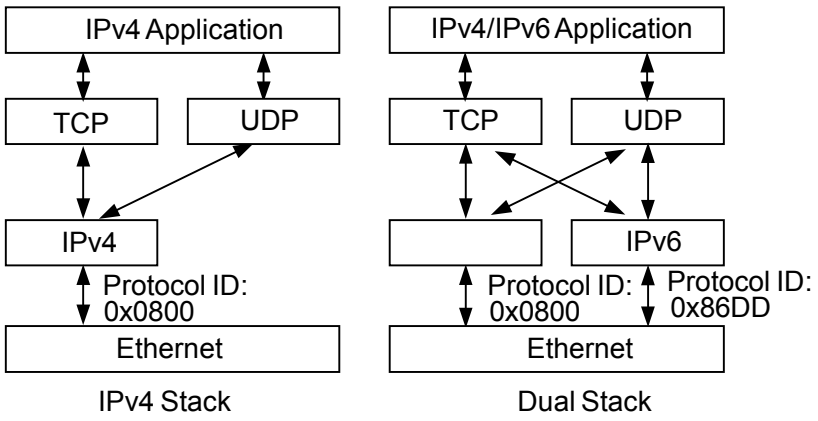
可以配置 IPv6 over IPv4 手动隧道和 6to4 隧道，实现在 IPv4 网络中 IPv6 网络的连通。

版权所有 © 华为技术有限公司

双协议栈

对于 IPv6 节点来说，兼容 IPv4 的最直接有效的办法就是保留一个完整的 IPv4 协议栈，这样的节点即为双协议栈节点。单协议栈和双协议栈结构示例如图 4-26 所示。

图 4-26 单协议栈与双协议栈结构（以太网）



双协议栈具有以下特点：

- 多种链路协议支持双协议栈

  多种链路协议（如以太网）支持双协议栈。图中的链路层是以太网，在以太网帧上，如果协议 ID 字段的值为 0x0800，表示网络层收到的是 IPv4 报文，如果为 0x86DD，表示网络层是 IPv6 报文。

- 多种应用支持双协议栈

  多种应用（如 DNS/FTP/Telnet 等）支持双协议栈。上层应用（如 DNS）可以选用 TCP 或 UDP 作为传输层的协议，但优先选择 IPv6 协议栈，而不是 IPv4 协议栈作为网络层协议。

IPv6 over IPv4 隧道

IPv6 over IPv4 隧道技术的原理如图 4-27 所示。

1. 启动 IPv4/IPv6 双协议栈

   边界交换机启动 IPv4/IPv6 双协议栈。

2. 封装 IPv6 报文

   边界交换机在收到从 IPv6 网络侧来的报文后，如果报文的目的地不是自身，就把收到的 IPv6 报文作为负载，加上 IPv4 报文头，封装到 IPv4 报文里。

3. 传递封装后的报文

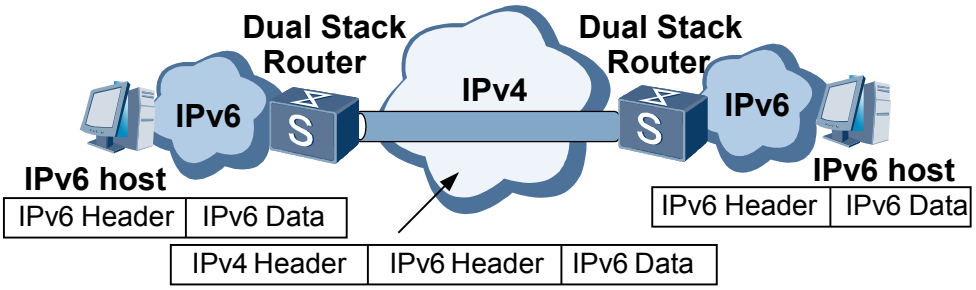
   在 IPv4 网络中，封装后的报文被传递到对端的边界交换机上。

4. 对报文解封装

   对端边界交换机对报文解封装，去掉 IPv4 报文头，然后将解封装后的 IPv6 报文转发到对端的 IPv6 网络中。

版权所有 © 华为技术有限公司

图 4-27 IPv6 over IPv4 隧道原理图



在两个边界交换机之间用来传递 IPv6 报文的虚拟的通道就是 IPv6 over IPv4 隧道。根据创建隧道的方式，可以对隧道进行分类。目前，常用的 IPv6 over IPv4 隧道模式有以下几种。

- IPv6 over IPv4 手动隧道
- 6to4 隧道
- ISATAP 隧道

IPv6 over IPv4 手动隧道

IPv6 over IPv4 手动隧道是在隧道两端的边界交换机上通过人工配置而创建的。它需要静态指定隧道的源 IPv4 地址和目的 IPv4 地址。

手动隧道相当于通过 IPv4 骨干网连接的两个 IPv6 域的永久链路，是边界交换机之间进行定期安全通信的固定通道。

手动隧道可用于 IPv6 孤岛之间的通信，也可在边界交换机与主机之间配置。隧道两端的主机和交换机均需支持 IPv4 和 IPv6 协议栈。

6to4 隧道

6to4 隧道也是一种将多个 IPv6 孤岛通过 IPv4 网络互连的机制。6to4 隧道可在孤立的 IPv6 网络和 IPv4 网络之间的边界交换机上配置。6to4 隧道两端的边界交换机必须同时支持 IPv4 和 IPv6 双协议栈。

6to4 隧道与手动配置隧道的主要区别在于：6to4 隧道可以是点到多点的连接，而手动隧道仅是点到点的连接。所以 6to4 隧道的交换机并不是成对配置的。

6to4 隧道与自动隧道类似，它可自动查找隧道的另一端点，但它不需要指定兼容 IPv4 的 IPv6 地址。

6to4 隧道使用了一种特殊的 IPv6 地址，即 6to4 地址，其格式为：

2002:IPv4 地址:子网 ID:接口 ID

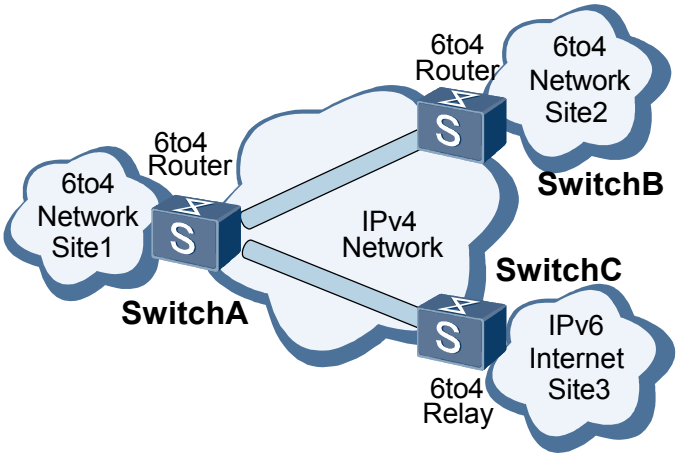
6to4 地址的前缀是 **2002:IPv4 地址**，前缀长度为 48bits。其中 IPv4 地址是为 IPv6 孤岛申请的一个全球唯一的 IPv4 地址。在 IPv6/IPv4 边界交换机与 IPv4 网络链接的物理接口上必须配置该 IPv4 地址。子网 ID 的长度为 16bits，接口 ID 的长度为 64bits，均由用户在 IPv6 孤岛内分配。

如图 4-28 所示，Site1 和 Site2 均为 6to4 网络，6to4 网络内的主机和交换机被分配了 6to4 地址。Site1 内的主机和交换机的 6to4 地址内嵌入的 IPv4 地址就是 SwitchA 到 IPv4 网

版权所有 © 华为技术有限公司

络接口的 IPv4 地址。Site2 内的主机和交换机的 6to4 地址内嵌入的 IPv4 地址就是 SwitchB 到 IPv4 网络接口的 IPv4 地址。SwitchA 和 SwitchB 均为 6to4 交换机。

图 4-28 6to4 隧道和 6to4 中继



Site1 内的主机要访问 Site2 内的主机时，其工作原理如下：

1. IPv6 报文被传送到 SwitchA；
2. SwitchA 检查 IPv6 报文的目的地址，发现是 6to4 地址，从该 6to4 地址中获得 6to4 隧道对端的 IPv4 地址；
3. SwitchA 将该 IPv6 报文封装到 IPv4 报文中，IPv4 报文头的目的地址就是隧道对端的 IPv4 地址，源地址就是隧道本端的 IPv4 地址；
4. SwitchA 将该 IPv4 报文通过 IPv4 网络转发到 SwitchB；
5. SwitchB 进行解封装操作，获得原来的 IPv6 报文，然后将该 IPv6 报文在 Site2 内被送到目的主机。

上面介绍的过程可以实现 6to4 网络之间的通信。为了实现 6to4 网络与本地（Native）IPv6 网络之间的通信，就需要 6to4 中继交换机了。所谓本地 IPv6 网络，就是它内部的主机或交换机均不配置 6to4 地址。

6to4 中继交换机是 6to4 网络与本地 IPv6 网络之间的网关。6to4 中继交换机的一侧连接本地 IPv6 网络，其另一侧连接 IPv4 网络，并与 6to4 交换机建立 6to4 隧道。如图 4-28 所示，6to4 网络内的主机要访问 IPv6 Internet 时，其工作过程如下。

1. IPv6 报文被路由到 SwitchA；
2. SwitchA 与 SwitchC 之间建立 6to4 隧道；
3. IPv6 报文封装在 IPv4 报文中被送到 SwitchC；
4. SwitchC 执行解封装操作，将 IPv6 Internet 内的原 IPv6 报文被送到目的主机。

ISATAP 隧道

ISATAP（Intra-site Automatic Tunnel Addressing Protocol）隧道用于 IPv4 网络中的 IPv4/IPv6 主机访问 IPv6 网络的情况，可以在 ISATAP 主机与 ISATAP 交换机之间建立 ISATAP 隧道。

建立 ISATAP 隧道时，需要使用 ISATAP 格式地址，其结构如下：

版权所有 © 华为技术有限公司

Prefix(64bit)::5EFE:IPv4-Address

在创建 ISATAP 隧道时，由于 IPv4/IPv6 主机和 ISATAP 交换机在同一个 IPv4 网络里，ISATAP 地址中嵌入的 IPv4 地址可以是公网地址，也可以是私网地址。

如图 4-29 所示，IPv4/IPv6 主机获得 IPv6 地址的过程如下：

1. IPv4/IPv6 主机发送交换机请求消息

   IPv4/IPv6 主机使用 ISATAP 格式的链路本地地址向 ISATAP 交换机发送交换机请求消息，该交换机请求消息被封装在 IPv4 报文中。

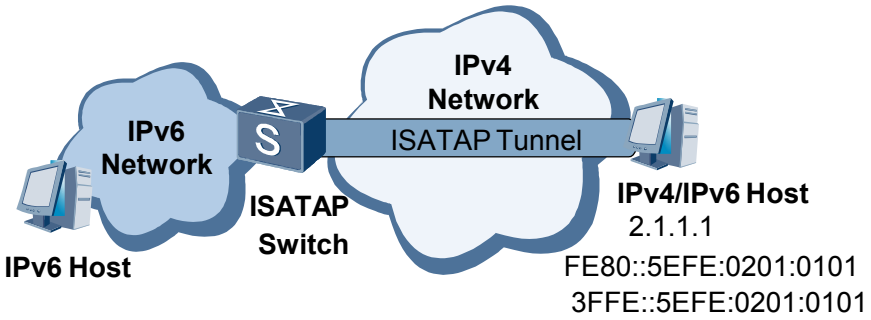
2. ISATAP 交换机响应请求

   ISATAP 交换机使用交换机通告消息响应主机的交换机请求。交换机通告消息中包含 ISATAP 前缀（ISATAP 前缀在交换机上通过人工配置）。

3. IPv4/IPv6 主机得到自己的 IPv6 地址

   IPv4/IPv6 主机将 ISATAP 前缀与 **5EFE**:**IPv4-Address** 组合得到自己的 IPv6 地址，并用此地址访问 IPv6 主机。

图 4-29 ISATAP 隧道



IPv4/IPv6 主机要访问 IPv6 Internet 时，其工作原理如下。

1. IPv4 网络中的 IPv4/IPv6 主机按照上面的过程获得自己的 IPv6 地址。
2. IPv4/IPv6 主机发送访问 IPv6 网络的 IPv6 主机的报文，该报文封装在 IPv4 中。
3. ISATAP 交换机接收该 IPv4 报文后执行解封装操作，将其中的 IPv6 报文发送到 IPv6 网络中的 IPv6 主机。

4.10.3 配置 IPv4/IPv6 双协议栈

为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界交换机上启动 IPv4/IPv6 双协议栈。

建立配置任务

介绍配置 IPv4/IPv6 双协议栈的应用环境、前置任务、数据准备和配置过程。

应用环境

如果交换机既有 IPv4 连接，又有 IPv6 连接，就需要启动 IPv4/IPv6 双协议栈。

版权所有 © 华为技术有限公司

AC6605 中启用 IPv4/IPv6 双协议栈的操作非常简单，只要在系统视图下使能 IPv6 报文转发能力，并在相应的接口上配置有 IPv4 地址或 IPv6 地址。此时，交换机就可在相应的接口上进行 IPv4 和 IPv6 的报文转发。

前置任务

在配置 IPv4/IPv6 双协议栈之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数

数据准备

在配置 IPv4/IPv6 双协议栈之前，需准备以下数据。

序号	数据
1	IPv4 网络侧接口的类型及编号
2	IPv4 网络侧接口的 IPv4 地址及掩码
3	IPv6 网络侧接口的类型及编号
4	IPv6 网络侧接口的 IPv6 地址及前缀

使能 IPv6 报文转发能力

使能 IPv6 报文转发能力即在系统视图下和接口视图下分别使能 IPv6 功能。

背景信息

如果要使能接口对 IPv6 报文进行转发的功能，必须同时使能系统视图下和接口视图下的 IPv6 功能。因为：

- 在系统视图下执行命令 **ipv6**，只是使能了交换机对 IPv6 报文的转发功能，并没有使能接口的 IPv6 功能，也不能进行 IPv6 的相关配置。
- 在接口视图下执行命令 **ipv6 enable**，只是使能了接口的 IPv6 功能，接口的 IPv6 协议状态仍是 Down，交换机不能对 IPv6 报文进行转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6**，使能 IPv6 报文转发能力。

缺省情况下，交换机不使能对 IPv6 报文的转发能力。

如果要对 IPv6 报文进行转发，必须先在系统视图下使能交换机的 IPv6 报文转发能力。否则即使在接口上配置有 IPv6 地址，接口的 IPv6 协议仍处于 Down 状态，交换机无法转发 IPv6 的报文。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进行需要使能 IPv6 功能的 VLANIF 接口视图。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

如果要在接口视图下进行 IPv6 的相关配置，必须先在接口视图下使能 IPv6 功能。

缺省情况下，接口下不使能 IPv6 功能。

----结束

配置接口的 IPv4 和 IPv6 地址

在 IPv4 网络侧和 IPv6 网络侧分别配置 IPv4 地址和 IPv6 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 IPv4 网络侧的接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IPv4 地址。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **interface vlanif** *vlan-id*，进入 IPv6 网络侧的接口视图。

步骤 6 请根据不同情况进行一下配置。

- 配置接口的自动链路本地地址，请执行命令 **ipv6 address auto link-local**。
- 配置接口的链路本地地址，请执行命令 **ipv6 address** *ipv6-address* **link-local**。
- 配置接口的全球单播地址，请执行命令 **ipv6 address** { *ipv6-address* | *prefix-length* }。
- 配置接口的 IPv6 EUI-64 格式地址，请执行命令 **ipv6 address** { *ipv6-address* | *prefix-length* } **eui-64**。

----结束

检查配置结果

前提条件

已经完成上述所有配置。

操作步骤

步骤 1 使用 **display ipv6 interface** 命令查看接口的 IPv6 属性。

----结束

4.10.4 配置 IPv6 over IPv4 隧道

利用 IPv4 网络连接 IPv6 网络。

建立配置任务

介绍配置 IPv6 over IPv4 隧道的应用环境、前置任务、数据准备和配置过程。

版权所有 © 华为技术有限公司

应用环境

IPv6 网络间的通信需要利用穿过 IPv4 网络时，在 IPv4 和 IPv6 的边界交换机上就需要配置 IPv6 over IPv4 隧道。

前置任务

在配置 IPv6 over IPv4 隧道之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使链路层协议状态为 Up
- 配置 IPv4/IPv6 双协议栈

数据准备

在配置 IPv6 over IPv4 隧道之前，需准备以下数据。

配置业务环回聚合接口

背景信息

配置业务环回聚合接口时，请注意以下情况：

- 配置该功能之前请首先创建一个 Eth-Trunk 接口，并增加端口成员，使其处于 UP 状态。
- 在整个设备上只需要一个业务环回聚合接口。

请在 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **service type tunnel**，指定该接口为业务环回接口。

步骤 4 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 5 执行命令 **eth-trunk** *trunk-id*，将当前接口加入到指定 Eth-Trunk 中。

----结束

配置 IPv6 over IPv4 手动隧道

手动隧道是点对点的隧道，隧道的源和目的地都是手动指定的，且同一台设备不能配置同源同目的的两个隧道。手动隧道相当于通过 IPv4 骨干网连接的两个 IPv6 域的永久链路，是边界交换机之间进行定期安全通信的固定通道。

背景信息

配置 IPv6 over IPv4 手动隧道时，请注意以下情况：

- 首先在设备上创建一个唯一的业务环回聚合接口,并保证其处于 UP 状态。

版权所有 © 华为技术有限公司

- 首先创建 Tunnel 接口，然后才能配置 Tunnel 的其他参数。
- 在 Tunnel 两端的交换机上都需要进行下列配置，需要注意的是，本端 tunnel 的源地址就是对端 tunnel 的目的地址，本端 tunnel 的目的地址就是对端 tunnel 的源地址。
- 为了支持动态路由协议，也需要配置 Tunnel 接口的网络地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface tunnel** *interface-number*，创建 Tunnel 接口。

步骤 3 执行命令 **tunnel-protocol ipv6-ipv4**，指定 Tunnel 为手动隧道模式。

步骤 4 执行命令 **source** { *ip-address* | *interface-type interface-number* }，指定 Tunnel 的源地址或源接口。

步骤 5 执行命令 **destination** *dest-ip-address*，指定 Tunnel 的目的地址。

说明

Tunnel 的目的地址可以是物理接口地址，也可以是 Loopback 接口的地址。

步骤 6 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

步骤 7 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }，设置 Tunnel 接口的 IPv6 地址。

----结束

配置 6to4 隧道

6to4 隧道是点对多点的隧道，可以实现孤立的 IPv6 网络之间通过 IPv4 网络连接起来。

背景信息

配置 6to4 隧道时，请注意以下情况：

- 首先创建 Tunnel 接口，然后才能配置 Tunnel 的其他参数。
- 建议 Tunnel 的编号与 Tunnel 的源物理接口的编号相同。
- 在配置 6to4 隧道时，只需确定 Tunnel 的源，Tunnel 的目的地址是从原始的 IPv6 报文的目的地址中获取的。但两个 6to4 隧道的源不允许相同。
- 在边界交换机与 6to4 网络相连的接口上必须配置 6to4 地址，在边界交换机与 IPv4 网络相连的接口上必须配置 IPv4 地址。为了支持路由协议，也需要配置 Tunnel 接口的网络地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface tunnel** *interface-number*，创建 Tunnel 接口。

步骤 3 执行命令 **tunnel-protocol ipv6-ipv4 6to4**，指定 Tunnel 为 6to4 隧道模式。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **source** { *ip-address* | *interface-type interface-number* }，指定 Tunnel 的源地址或源接口。

步骤 5 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

步骤 6 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* }，设置 Tunnel 接口的 IPv6 地址。

----结束

后续处理

通过 6to4 中继访问 IPv6 网络的配置操作与配置 6to4 隧道类似，可参考“配置 6to4 中继示例”。

配置 ISATAP 隧道

ISATAP（Intra-site Automatic Tunnel Addressing Protocol）隧道用于 IPv4 网络中的 IPv4/IPv6 主机访问 IPv6 网络的情况，可以在 ISATAP 主机与 ISATAP 交换机之间建立 ISATAP 隧道。

背景信息

配置 ISATAP 隧道时，请注意以下情况：

- 首先创建 Tunnel 接口，然后才能配置 Tunnel 的其他参数。
- 建议 Tunnel 的编号与 Tunnel 的源物理接口的编号相同。
- Tunnel 的源接口是指转发隧道报文的实际物理接口，在命令中可以指定为接口的地址或接口名。
- 在配置自动隧道时，只需确定 Tunnel 的源，Tunnel 的目的地址是从原始的 IPv6 报文的目的地址中获取的。但两个自动隧道的源不允许相同。
- 在 Tunnel 接口上的配置 IPv6 地址为 ISATAP 地址，前缀长度为 64。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface tunnel** *interface-number*，创建 Tunnel 接口。

步骤 3 执行命令 **tunnel-protocol ipv6-ipv4 isatap**，指定 Tunnel 为 ISATAP 模式。

步骤 4 执行命令 **source** { *ip-address* | *interface-type interface-number* }，指定 Tunnel 的源地址或源接口。

步骤 5 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }，设置 Tunnel 接口的 IPv6 地址。

步骤 6 执行命令 **undo ipv6 nd ra halt**，允许发布交换机通告消息。

----结束

配置 Tunnel 路由

隧道的源端交换机和目的端交换机上必须同时存在转发路由，这样才能保证报文的正常转发。

版权所有 © 华为技术有限公司

背景信息

路由配置包括静态路由和动态路由。

- 配置动态路由时，可以在与私网连接的 Tunnel 接口和交换机接口上使能动态路由协议。
- 配置静态路由时，需要使用 **ipv6 route-static** *dest-ipv6-address prefix-length* { *interface-type interface-number nexthop-ipv6-address* | *nexthop-ipv6-address* }命令手动配置到达目的地址（不是隧道的目的地址，而是封装报文前指定的目的地址）的路由，并将下一跳配置为对端隧道接口的地址。

检查配置结果

前提条件

已经完成 IPv6 over IPv4 隧道的所有配置。

操作步骤

步骤 1 使用 **display ipv6 interface tunnel** *interface-number* 命令查看 Tunnel 接口的 IPv6 属性。

----结束

4.10.5 配置举例

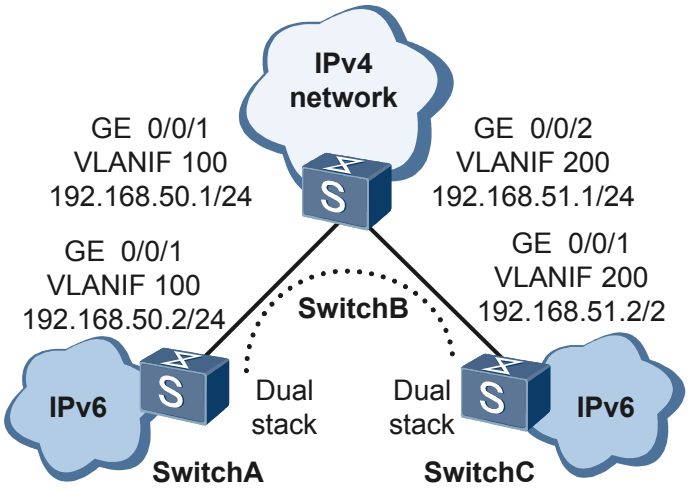
举例说明 IPv6 over IPv4 隧道的配置。

配置 IPv6 over IPv4 手动隧道示例

组网需求

如图 4-30 所示，两个 IPv6 网络分别通过 SwitchA 和 SwitchC 与 IPv4 骨干网络中的 SwitchB 连接，要求在 SwitchA 和 SwitchC 之间配置 IPv6 over IPv4 手动隧道，使两个 IPv6 网络可以互通。

图 4-30 配置 IPv6 over IPv4 手动隧道组网图



版权所有 © 华为技术有限公司

配置思路

配置 IPv6 over IPv4 手动隧道的思路如下：

1. 配置业务环回聚合接口
2. 配置物理接口对应的 VLANIF 接口的 IP 地址
3. 配置隧道接口的 IPv6 地址、源接口、目的地址
4. 配置协议类型为 IPv6-IPv4

数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IP 地址
- 隧道的 IPv6 地址、源接口和目的地址

操作步骤

步骤 1 配置 SwitchA

配置业务环回聚合接口。



注意

此处做业务环回聚合的接口必须是空闲的，没有承载业务的接口。

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-gigabitethernet0/0/3] eth-trunk 1
[Quidway-gigabitethernet0/0/3] quit
```

配置接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
[SwitchA] vlan 100
[SwitchA-Vlan100] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-gigabitethernet0/0/1] port hybrid pvid vlan 100
[SwitchA-gigabitethernet0/0/1] port hybrid untagged vlan 100
[SwitchA-gigabitethernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 192.168.50.2 255.255.255.0
[SwitchA-Vlanif100] quit
```

配置协议类型为 IPv6-IPv4。

```
[SwitchA] interface tunnel 0/0/1
[SwitchA-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
```

绑定 Tunnel 接口和业务环回的 Eth-trunk。

版权所有 © 华为技术有限公司

```
[SwitchA-Tunnel0/0/1] eth-trunk 1
```

配置隧道接口的 IPv6 地址、目的地址。

```
[SwitchA-Tunnel0/0/1] ipv6 enable
[SwitchA-Tunnel0/0/1] ipv6 address 3001::1 64
[SwitchA-Tunnel0/0/1] source vlanif 100
[SwitchA-Tunnel0/0/1] destination 192.168.51.2
[SwitchA-Tunnel0/0/1] quit
```

配置静态路由。

```
[SwitchA] ip route-static 192.168.51.2 255.255.255.0 192.168.50.1
```

步骤 2 配置 SwitchB

配置接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
[SwitchB] vlan 100
[SwitchB-Vlan100] quit
[SwitchB] vlan 200
[SwitchB-Vlan200] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchB-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] ip address 192.168.51.1 255.255.255.0
[SwitchB-Vlanif200] quit
```

步骤 3 配置 SwitchC

配置业务环回聚合接口。



注意

此处做业务环回聚合的接口必须是空闲的，没有承载业务的接口。

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface gigabitethernet0/0/3
[Quidway-GigabitEthernet0/0/3] eth-trunk 1
[Quidway-GigabitEthernet0/0/3] quit
```

配置接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] ipv6
[SwitchC] vlan 200
[SwitchC-Vlan200] quit
[SwitchC] interface gigabitethernet0/0/1
[SwitchC-GigabitEthernet0/0/1] port hybrid pvid vlan 200
```


版权所有 © 华为技术有限公司

```
[SwitchC-GigabitEthernet0/0/1] port hybrid untagged vlan 200
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface vlanif 200
[SwitchC-Vlanif200] ip address 192.168.51.2 255.255.255.0
[SwitchC-Vlanif200] quit
```

配置协议类型为 IPv6-IPv4。

```
[SwitchC] interface tunnel 0/0/1
[SwitchC-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
```

绑定 Tunnel 接口和业务环回的 Eth-trunk。

```
[SwitchC-Tunnel0/0/1] eth-trunk 1
```

配置隧道接口的 IPv6 地址、目的地址。

```
[SwitchC-Tunnel0/0/1] ipv6 enable
[SwitchC-Tunnel0/0/1] ipv6 address 3001::2 64
[SwitchC-Tunnel0/0/1] source vlanif 200
[SwitchC-Tunnel0/0/1] destination 192.168.50.2
[SwitchC-Tunnel0/0/1] quit
```

配置静态路由。

```
[SwitchC] ip route-static 192.168.50.2 255.255.255.0 192.168.51.1
```

步骤 4 检查配置结果

在 SwitchC 上 Ping SwitchA 的 VLANIF100 的 IPv4 地址，可收到返回的报文。

```
[SwitchC] ping 192.168.50.2
  PING 192.168.50.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.50.2: bytes=56 Sequence=1 ttl=255 time=84 ms
    Reply from 192.168.50.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 192.168.50.2: bytes=56 Sequence=3 ttl=255 time=25 ms
    Reply from 192.168.50.2: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 192.168.50.2: bytes=56 Sequence=5 ttl=255 time=24 ms

  --- 192.168.50.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/32/84 ms
```

在 SwitchC 上 Ping 隧道的 SwitchA 接口 Tunnel0/0/1 的 IPv6 地址，可收到返回的报文。

```
[SwitchC] ping ipv6 3001::1
  PING 3001::1 : 56  data bytes, press CTRL_C to break
    Reply from 3001::1
    bytes=56 Sequence=1 hop limit=255  time = 28 ms
    Reply from 3001::1
    bytes=56 Sequence=2 hop limit=255  time = 27 ms
    Reply from 3001::1
    bytes=56 Sequence=3 hop limit=255  time = 26 ms
    Reply from 3001::1
    bytes=56 Sequence=4 hop limit=255  time = 27 ms
    Reply from 3001::1
    bytes=56 Sequence=5 hop limit=255  time = 26 ms
  --- 3001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 26/26/28 ms
```

----结束

版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
ipv6
#
vlan batch 100
#
interface Vlanif100
 192.168.50.2 255.255.255.0
#
interface Eth-Trunk1
 service type tunnel
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 3001::1/64
 tunnel-protocol ipv6-ipv4
 source Vlanif100
 destination 192.168.51.2
#
ip route-static 192.168.51.0 255.255.255.0 192.168.50.1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 200
#
interface Vlanif100
 192.168.50.1 255.255.255.0
#
interface Vlanif200
 192.168.51.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
ipv6
#
vlan batch 200
#
interface Vlanif200
 192.168.51.2 255.255.255.0
#
interface Eth-Trunk1
 service type tunnel
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 3001::2/64
 tunnel-protocol ipv6-ipv4
 source Vlanif200
 destination 192.168.50.2
#
ip route-static 192.168.50.0 255.255.255.0 192.168.51.1
#
return
```

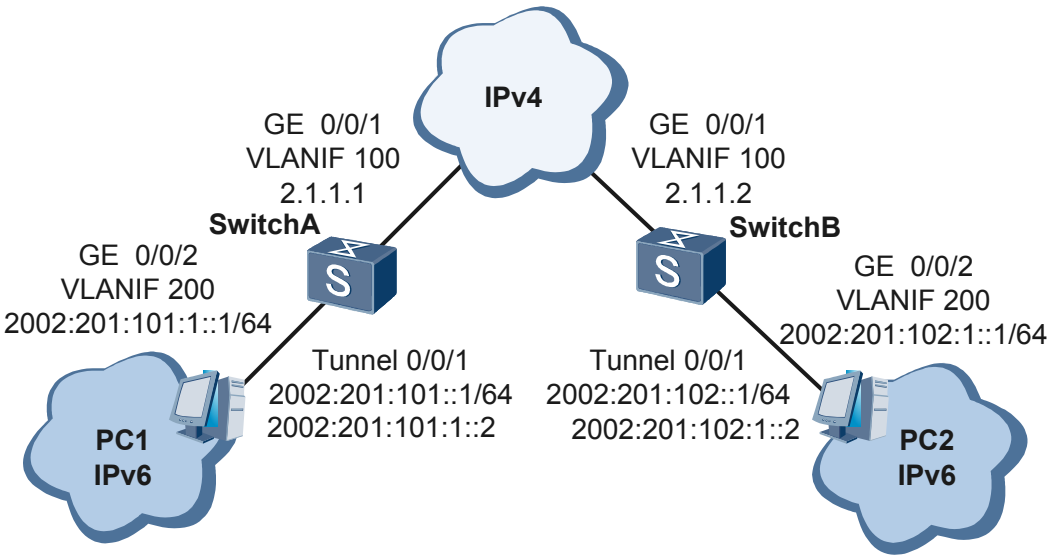
配置 6to4 隧道示例

组网需求

如图 4-31 所示，SwitchA 和 SwitchB 分别与相应的 6to4 网络以及 IPv4 骨干网络相连，要求在 SwitchA 和 SwitchB 之间配置 6to4 隧道，以便两个 6to4 网络内的主机可以互通。

为了让 6to4 网络之间互通，需要为 6to4 网络内的主机配置 6to4 地址。6to4 地址的前缀是 **2002:IPv4 地址:**，前缀长度为 48bits。如图 4-31 所示，SwitchA 与 IPv4 网络连接的接口的 IPv4 地址是 2.1.1.1，那么 SwitchA 所在的 6to4 网络的 6to4 地址前缀应该是 2002:0201:0101::。

图 4-31 配置 6to4 隧道组网图



配置思路

配置 6to4 隧道的思路如下：

版权所有 © 华为技术有限公司

1. 配置业务环回聚合接口
2. 在 Switch 上配置 IPv4/IPv6 双协议栈
3. 在 Switch 上配置 6to4 隧道
4. 在 Switch 上配置相关路由

数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IPv4 地址和 IPv6 地址
- 隧道的源接口

操作步骤

步骤 1 配置 SwitchA。

配置业务环回聚合接口

注意

此处做业务环回聚合的接口必须是空闲的，没有承载业务的接口。

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] eth-trunk 1
[Quidway-GigabitEthernet0/0/3] quit
```

配置 IPv4/IPv6 双协议栈。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
[SwitchA] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 2.1.1.1 8
[SwitchA-Vlanif100] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] ipv6 enable
[SwitchA-Vlanif200] ipv6 address 2002:0201:0101:1::1/64
[SwitchA-Vlanif200] quit
```

配置 6to4 隧道。

```
[SwitchA] interface tunnel 0/0/1
[SwitchA-Tunnel0/0/1] eth-trunk 1
[SwitchA-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[SwitchA-Tunnel0/0/1] ipv6 enable
[SwitchA-Tunnel0/0/1] ipv6 address 2002:0201:0101::1/64
```


版权所有 © 华为技术有限公司

```
[SwitchA-Tunnel0/0/1] source vlanif 100
[SwitchA-Tunnel0/0/1] quit
```

配置到其他 6to4 网络的路由。

```
[SwitchA] ipv6 route-static 2002:: 16 tunnel 0/0/1
```

步骤 2 配置 SwitchB。

配置业务环回聚合接口

注意

此处做业务环回聚合的接口必须是空闲的，没有承载业务的接口。

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] eth-trunk 1
[Quidway-GigabitEthernet0/0/3] quit
```

配置 IPv4/IPv6 双协议栈。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
[SwitchB] vlan batch 100 200
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 2.1.1.2 8
[SwitchB-Vlanif100] quit
[SwitchB] interface gigabitethernet0/0/2
[SwitchB-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchB-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] ipv6 enable
[SwitchB-Vlanif200] ipv6 address 2002:0201:0102:1::1/64
[SwitchB-Vlanif200] quit
```

配置 6to4 隧道。

```
[SwitchB] interface tunnel 0/0/1
[SwitchB-Tunnel0/0/1] eth-trunk 1
[SwitchB-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[SwitchB-Tunnel0/0/1] ipv6 enable
[SwitchB-Tunnel0/0/1] ipv6 address 2002:0201:0102::1/64
[SwitchB-Tunnel0/0/1] source vlanif 100
[SwitchB-Tunnel0/0/1] quit
```

配置到其他 6to4 网络的路由。

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0/0/1
```

说明

SwitchA 和 SwitchB 之间需要有一条可达的路由。本例中需要在 SwitchA 和 SwitchB 的 GigabitEthernet0/0/1 接口上配置路由协议，保证 SwitchA 和 SwitchB 之间路由可达，具体配置方法可参见《AC6605 无线接入控制器 配置指南-IP 路由》。

版权所有 © 华为技术有限公司

步骤 3 检查配置结果

在 SwitchA 上查看 Tunnel0/0/1 的 IPv6 状态为 UP。

```
[SwitchA] display ipv6 interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::201:101 [TENTATIVE]
  Global unicast address(es):
    2002:201:101::1, subnet is 2002:201:101::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

从 SwitchA 可以 Ping 通 SwitchB 的接口 VLANIF200 的 6to4 地址。

```
[SwitchA] ping ipv6 2002:0201:0102:1::1
  PING 2002:0201:0102:1::1 : 56  data bytes, press CTRL_C to break
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=1 hop limit=255  time = 8 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=2 hop limit=255  time = 25 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=3 hop limit=255  time = 4 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=4 hop limit=255  time = 5 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=5 hop limit=255  time = 5 ms

  --- 2002:0201:0102:1::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 4/9/25 ms
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
ipv6
#
vlan batch 100 200
#
interface Vlanif100
 ip address 2.1.1.1 255.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002:201:101:1::1/64
#
interface Eth-Trunk1
 service type tunnel
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
```


版权所有 © 华为技术有限公司

```
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 2002:201:101:1::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source vlanif100
#
ipv6 route-static 2002:: 16 Tunnel 0/0/1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
ipv6
#
vlan batch 100 200
#
interface Vlanif100
 ip address 2.1.1.2 255.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002:201:102:1::1/64
#
interface Eth-Trunk1
 service type tunnel
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 2002:201:102:1::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source vlanif100
#
ipv6 route-static 2002:: 16 Tunnel 0/0/1
#
return
```

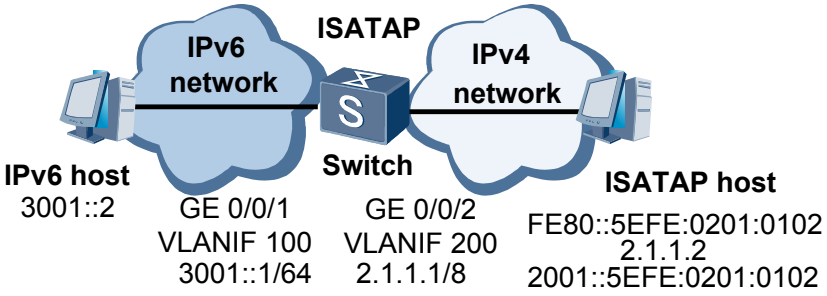
配置 ISATAP 隧道示例

组网需求

如图 4-32 所示，IPv4 网络中的 IPv6 主机为 Windows XP 系统，需要将 IPv6 主机通过边界设备接入到 IPv6 网络。IPv6 主机和边界设备均支持 ISATAP。要求在 IPv6 主机和边界设备之间配置 ISATAP 隧道。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 4-32 配置 ISATAP 隧道组网图



配置思路

配置 ISATAP 隧道的思路如下：

1. 配置业务环回聚合接口
2. 在设备上配置 IPv4/IPv6 双协议栈
3. 在设备上配置 ISATAP 隧道
4. 配置 IPv6 主机到 ISATAP 主机的静态路由

数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IPv4 地址和 IPv6 地址
- 隧道的源接口
- Switch 物理接口所属 VLAN

操作步骤

步骤 1 配置 ISATAP 路由设备

配置业务环回聚合接口

注意

此处做业务环回聚合的接口必须是空闲的，没有承载业务的接口。

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] eth-trunk 1
[Quidway-GigabitEthernet0/0/3] quit
```

使能 IPv4/IPv6 双协议栈，配置各接口地址。

```
<Quidway> system-view
[Quidway] ipv6
```


版权所有 © 华为技术有限公司

```
[Quidway] vlan batch 100 200
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 200
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 200
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ipv6 enable
[Quidway-Vlanif100] ipv6 address 3001::1/64
[Quidway-Vlanif100] quit
[Quidway] interface vlanif 200
[Quidway-Vlanif200] ip address 2.1.1.1 255.0.0.0
[Quidway-Vlanif200] quit
```

配置 ISATAP 隧道。

```
[Quidway] interface tunnel 0/0/2
[Quidway-Tunnel0/0/2] eth-trunk 1
[Quidway-Tunnel0/0/2] tunnel-protocol ipv6-ipv4 isatap
[Quidway-Tunnel0/0/2] ipv6 enable
[Quidway-Tunnel0/0/2] ipv6 address 2001::/64 eui-64
[Quidway-Tunnel0/0/2] source vlanif 200
[Quidway-Tunnel0/0/2] undo ipv6 nd ra halt
[Quidway-Tunnel0/0/2] quit
```

步骤 2 配置 ISATAP 主机

说明

ISATAP 主机需要安装 IPv6 协议，并且使能 IPv6 功能。

使用如下的命令添加一条到边界设备的静态路由（此处主机的伪接口号是 2，可以使用 ipv6 if 命令查看 Automatic Tunneling Pseudo-Interface 对应的接口）。

```
C:\> netsh interface ipv6 isatap set router 2.1.1.1
```

步骤 3 配置 IPv6 网络主机

在 IPv6 网络中的主机上配置一条到边界设备隧道的静态路由，使两个不同网络的 PC 通过 ISATAP 隧道互通。

```
C:\> netsh interface ipv6 set route 2001::/64 3001::1
```

步骤 4 验证配置结果

在 ISATAP 路由设备上查看 Tunnel0/0/2 的 IPv6 状态为 Up。

```
[Quidway] display ipv6 interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::5EFE:201:101 [TENTATIVE]
  Global unicast address(es):
    2001::5EFE:201:101, subnet is 2001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:101
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
```

在 ISATAP 路由设备上 Ping 向 ISATAP 主机上的隧道接口全球单播地址。

版权所有 © 华为技术有限公司

```
[Quidway] ping ipv6 2001::5efe:2.1.1.2
  PING 2001::5efe:2.1.1.2 : 56  data bytes, press CTRL_C to break
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=1 hop limit=64  time = 4 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=5 hop limit=64  time = 2 ms

  --- 2001::5efe:2.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/4 ms
```

在 ISATAP 主机上 Ping 向 ISATAP 路由设备的全球单播地址。

```
C:\> ping6 2001::5efe:2.1.1.1

Pinging 2001::5efe:2.1.1.1
from 2001::5efe:2.1.1.2 with 32 bytes of data:

Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Ping statistics for 2001::5efe:2.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

从 ISATAP 主机上 Ping 向 IPv6 网络主机，执行成功。

```
C:\> ping6 3001::2

Pinging 3001::2 with 32 bytes of data:

Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms

Ping statistics for 3001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

----结束

配置文件

ISATAP 的配置文件

```
#
 sysname Quidway
#
vlan batch 100 200
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::1/64
#
interface Vlanif200
```


版权所有 © 华为技术有限公司

```
 ip address 2.1.1.1 255.0.0.0
#
interface Eth-Trunk1
 service type tunnel
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/2
 eth-trunk 1
 ipv6 enable
 ipv6 address 2001::/64 eui-64
 undo ipv6 nd ra halt
 tunnel-protocol ipv6-ipv4 isatap
 source Vlanif200
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```


版权所有 © 华为技术有限公司

5 IP 路由配置

关于本章

本文档针对 AC6605 的 IP 路由（静态路由、RIP、RIPng、OSPF、OSPFv3、IS-IS、BGP、路由策略）特性，从配置过程和配置举例两方面对特性进行介绍。

5.1 静态路由配置
静态路由适用于结构比较简单的网络。合理的静态路由可以改进网络的性能，并可为重要的应用保证带宽。

5.2 RIP 配置
RIP 可以发布和接收路由信息，影响交换机的数据转发途径，并提供网管功能，主要用于规模较小的网络中。

5.3 RIPng 配置
RIPng 是在 IPv6 网络中应用的 RIP 协议，并在原 RIP 协议基础上进行了一些扩展。

5.4 OSPF 配置
OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议，广泛应用于接入网和城域网中。

5.5 OSPFv3 配置
OSPFv3 是 OSPF Version 3 的简称，通过组建 OSPFv3 网络，在自治域内发现并计算路由信息。OSPFv3 可以应用于大规模网络，最多可支持几百台交换机。

5.6 IS-IS 配置
介绍 IS-IS 协议的基本原理、配置过程和配置举例。

5.7 BGP 配置
BGP 协议通常应用于大型和复杂的网络，用于在 AS 之间传递路由信息。

5.8 路由策略配置
路由策略是为了改变网络流量所经过的途径而对路由信息采用的方法。

5.9 MCE 配置
通常情况下，一台 CE 只能连接一个 VPN，如果用户网络需要划分多个 VPN，则需要多台 CE 设备。MCE 技术可以使一台 CE 同时连接多个 VPN，既可实现不同 VPN 用户间的业务完全隔离，又降低了网络设备的投入成本。

版权所有 © 华为技术有限公司

5.1 静态路由配置

静态路由适用于结构比较简单的网络。合理的静态路由可以改进网络的性能，并可为重要的应用保证带宽。

5.1.1 静态路由概述

静态路由是一种需要管理员手工配置的特殊路由。

当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由的缺点在于：当网络发生故障或者拓扑发生变化后，静态路由不会自动改变，必须有管理员的介入。

5.1.2 AC6605 支持的静态路由特性

系统支持的静态路由特性包括：IPv4 静态路由、IPv6 静态路由、缺省路由、BFD for IPv4 静态路由。

IPv4 静态路由

IPv4 静态路由需要管理员手工配置，适合于一些结构比较简单的 IPv4 网络。

在配置 IPv4 静态路由时，如果指定的目的地址为 0.0.0.0（掩码长度为 0），则表示配置了一条 IPv4 缺省路由。如果报文的目的地址无法匹配路由表中的任何一项，交换机将选择 IPv4 缺省路由来转发 IPv4 报文。

AC6605 支持普通静态路由。

IPv6 静态路由属性及功能

IPv6 静态路由与 IPv4 静态路由类似，也需要管理员手工配置，适合于一些结构比较简单的 IPv6 网络。

在配置 IPv6 静态路由时，如果指定的目的地址为::/0（掩码长度为 0），则表示配置了一条 IPv6 缺省路由。如果报文的目的地址无法匹配路由表中的任何一项，交换机将选择 IPv6 缺省路由来转发 IPv6 报文。

说明

IPv4 静态路由和 IPv6 静态路由之间的主要区别是目的地址和下一跳地址有所不同，IPv6 静态路由是使用 IPv6 地址为下一跳，而 IPv4 静态路由则使用 IPv4 地址为下一跳。

缺省路由

缺省路由是另外一种特殊的路由。通常情况下，管理员可以通过手工方式配置缺省路由；但有些时候，也可以使动态路由协议生成缺省路由，如 OSPF 和 IS-IS。

简单来说，缺省路由是在没有找到匹配的路由表入口项时才使用的路由。在路由表中，缺省路由的目的地址和子网掩码都是 0.0.0.0。可以通过命令 **display ip routing-table** 查看当前是否设置了缺省路由。

版权所有 © 华为技术有限公司

如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取缺省路由。如果没有缺省路由且报文的目的地不在路由表中，那么该报文将被丢弃，并向源端返回一个 ICMP 报文，报告该目的地址或网络不可达。

BFD for IPv4 静态路由

与动态路由协议不同，静态路由自身没有检测机制，当网络发生故障的时候，需要管理员介入。BFD for IPv4 静态路由特性可为公网 IPv4 静态路由绑定 BFD 会话，利用 BFD 会话来检测静态路由所在链路的状态。

BFD for IPv4 静态路由可为每条静态路由绑定一个 BFD 会话。

- 当某条静态路由上的 BFD 会话检测到故障（BFD 会话由 Up 转为 Down），BFD 会将故障上报路由管理系统，由路由管理系统将这条路由设置为“非激活”状态（此条路由不可用，从 IP 路由表中删除）。
- 当某条静态路由上的 BFD 会话协商成功（BFD 会话由 Down 转为 Up），BFD 会上报路由管理系统，由路由管理系统将这条路由设置为“激活”状态（此路由可用，加入 IP 路由表）。

5.1.3 配置 IPv4 静态路由

在 IPv4 网络中，通过配置 IPv4 静态路由，可以准确地控制网络的路由选择。

建立配置任务

在配置 IPv4 静态路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

配置 IPv4 静态路由时，需要了解以下内容：

- 目的地址与掩码

  在 **ip route-static** 命令中，IPv4 地址为点分十进制格式，掩码可以用点分十进制表示，也可用掩码长度（即掩码中连续‘1’的位数）表示。

- 出接口和下一跳地址

  在配置静态路由时，可指定出接口 *interface-type interface-name*，也可指定下一跳地址 *nexthop-address*，是指定出接口还是指定下一跳地址要视具体情况而定。

  实际上，所有的路由项都必须明确下一跳地址。在发送报文时，首先根据报文的目的地址寻找路由表中与之匹配的路由。

  在某些情况下，如链路层被 PPP 封装，即使不知道对端地址，也可以在交换机配置时指定出接口。这样，即使对端地址发生了改变也无须改变该交换机的配置。

- 其它属性

  对于不同的静态路由，可以为它们配置不同的优先级 **preference**，从而更灵活地应用路由管理策略。例如：配置到达相同目的地的多条路由，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

  在使用 **ip route-static** 配置静态路由时，如果将目的地址与掩码配置为全零（0.0.0.0 0.0.0.0），则表示配置的是缺省路由。

版权所有 © 华为技术有限公司

前置任务

在配置 IPv4 静态路由之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

在配置 IPv4 静态路由之前，需要准备以下数据。

序号	数据
1	目的网络地址和掩码
2	下一跳的 IPv4 地址或出接口
3	IPv4 静态路由的优先级

（可选）配置 IPv4 静态路由的缺省优先级

配置 IPv4 静态路由缺省优先级可以影响路由的选路顺序。

背景信息

请在需要配置静态路由，并且需要改变静态路由缺省优先级的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip route-static default-preference** *preference*，配置静态路由的缺省优先级。

缺省情况下，静态路由的缺省优先级为 60。

在配置静态路由时，如果没有显式的指定优先级，就会使用缺省优先级。重新设置缺省优先级后，仅对新增的 IPv4 静态路由有效。

----结束

（可选）静态路由按迭代深度优先选择

配置静态路由按迭代深度优选之后，静态路由模块会选择迭代深度较小的静态路由作为活跃路由，并下发 FIB，其他路由为不活跃路由。

背景信息

配置静态路由后，系统中存在若干同一前缀的静态路由，迭代深度不同。配置了基于迭代深度优选之后，静态路由模块会选择迭代深度较小的静态路由作为活跃路由，并下发 FIB，其他路由为不活跃路由。

请在需要配置静态路由的交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip route-static selection-rule relay-depth**，配置静态路由按迭代深度进行优先选择。

缺省情况下，静态路由不按迭代深度进行优选。

----结束

检查配置结果

IPv4 静态路由配置成功后，可以查看路由的详细信息。

前提条件

已经完成 IPv4 静态路由的所有配置。

操作步骤

- 使用 **display ip routing-table** 命令查看 IPv4 路由表摘要信息。
- 使用 **display ip routing-table verbose** 命令查看 IPv4 路由表详细信息。

----结束

5.1.4 配置 IPv6 静态路由

在 IPv6 网络中，通过配置 IPv6 静态路由，可以准确地控制网络的路由选择。

建立配置任务

在配置 IPv6 静态路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在小型 IPv6 网络中，可以通过配置 IPv6 静态路由达到网络互连的目的。相对使用动态路由协议来说，可以节省带宽。

前置任务

在配置 IPv6 静态路由之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IPv6 地址），使接口的链路协议状态为 Up

数据准备

在配置 IPv6 静态路由之前，需要准备以下数据。

序号	数据
1	目的地址和掩码

版权所有 © 华为技术有限公司

序号	数据
2	下一跳的 IPv6 地址或者出接口
3	IPv6 静态路由的优先级

配置 IPv6 静态路由

配置 IPv6 静态路由需要注意目的地址、出接口和下一跳。

背景信息

请在需要配置 IPv6 静态路由的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 route-static** *dest-ipv6-address prefix-length* { *interface-type interface-number nexthop-ipv6-address*| *nexthop-ipv6-address* } [**preference** *preference* | **tag** *tag*] * [**description** *text*]，配置 IPv6 静态路由。

配置静态路由时，根据实际情况，或者指定出接口，或者指定下一跳地址。如果当输出接口为非 P2P 类型时，则必须指定下一跳地址。

如果没有指定 **preference** 参数，则缺省的优先级为 60。

缺省情况下，没有配置 IPv6 静态路由。

----结束

（可选）配置 IPv6 静态路由的缺省优先级

配置 IPv6 静态路由缺省优先级可以改变静态路由的优先级。

背景信息

请在需要配置 IPv6 静态路由，并且需要改变 IPv6 静态路由缺省优先级的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 route-static default-preference** *preference*，配置 IPv6 静态路由的缺省优先级。

缺省情况下，IPv6 静态路由的缺省优先级为 60。

在配置 IPv6 静态路由时，如果没有显式的指定优先级，就会使用缺省优先级。重新设置缺省优先级后，仅对新增的 IPv6 静态路由有效。

----结束

版权所有 © 华为技术有限公司

检查配置结果

IPv6 静态路由配置成功后，可以查看路由的详细信息。

前提条件

已经完成 IPv6 静态路由的所有配置。

操作步骤

- 使用 **display ipv6 routing-table** 命令查看 IPv6 路由表摘要信息。
- 使用 **display ipv6 routing-table verbose** 命令查看 IPv6 路由表详细信息。

----结束

5.1.5 配置 BFD for 公网 IPv4 静态路由

IPv4 网络中，配置 BFD for 公网 IPv4 静态路由，可以提高路由的收敛速度，增强网络可靠性。

建立配置任务

在配置 BFD 检测静态路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

BFD 能提供 IPv4 转发故障的快速检测，使 IPv4 网络以良好 QoS 实现语音、视频及其它点播业务的传输，从而帮助服务提供商基于 IPv4 网络为客户提供所需的高可靠性、高适用性 VoIP 及其它实时业务。

在静态路由上绑定 BFD 会话，可利用 BFD 会话为公网 IPv4 静态路由提供链路检测机制。一条静态路由可以绑定一条 BFD 会话。

前置任务

在配置 BFD for 公网 IPv4 静态路由之前，需完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up

数据准备

在配置 BFD for 公网 IPv4 静态路由之前，需要准备以下数据。

序号	数据
1	目的网络地址和掩码
2	下一跳的 IPv4 地址或出接口
3	BFD 检测的对端 IP 地址
4	BFD 会话的本地标识符和远端标识符

版权所有 © 华为技术有限公司

配置 BFD 会话

BFD 会话用于快速检测、监控网络中链路的转发连通状况。

背景信息

请参见《AC6605 无线接入控制器 配置指南-可靠性》

配置静态路由绑定 BFD 会话

静态路由绑定 BFD 会话的时候，静态路由和 BFD 会话必须在同一条链路上。

背景信息

请在需要为静态路由绑定 BFD 会话的交换机上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference* | **tag** *tag*] * **track bfd-session** *cfg-name* [**description** *text*]，为公网 IPv4 静态路由绑定 BFD 会话。

说明

为静态路由绑定 BFD 会话的时候，请确保 BFD 会话和静态路由在同一链路上。

----结束

检查配置结果

BFD 检测静态路由配置成功后，可以查看 BFD 会话信息及 BFD 绑定静态路由的情况。

前提条件

已经完成 BFD for 公网 IPv4 静态路由的所有配置。

操作步骤

- 使用 **display bfd session** { **all** | **discriminator** *discr-value* } [**verbose**]命令查看 BFD 会话信息。
- 使用 **display current-configuration | include bfd** 命令查看 BFD for 静态路由的配置。

  只有配置完 BFD 会话参数并成功建立会话后，才能查看到 BFD 会话信息。

  如果 BFD 会话协商成功，可以看到 BFD 会话的状态为 Up，且在系统视图下执行 **display current-configuration | include bfd** 命令，可以查看到 BFD 会话已经绑定。

----结束

5.1.6 配置静态路由举例

配置静态路由、配置 BFD for 静态路由的举例。

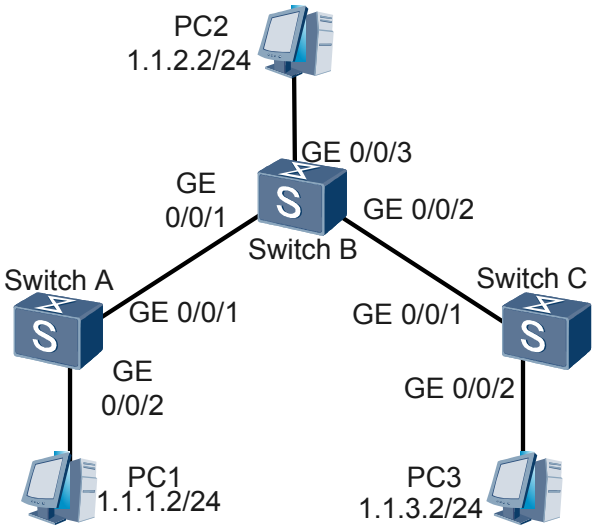
版权所有 © 华为技术有限公司

配置 IPv4 静态路由示例

组网需求

属于不同网段的 PC 通过几台 Switch 相连，要求采用 IPv4 静态路由，使不同网段的任意两台 PC 之间能够互通。

图 5-1 配置 IPv4 静态路由组网图



设备	接口	对应的 VLANIF IP 地址	
SwitchA	GE 0/0/1	VLANIF 10	1.1.4.1/30
SwitchA	GE 0/0/2	VLANIF 30	1.1.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	1.1.4.2/30
SwitchB	GE 0/0/2	VLANIF 20	1.1.4.5/30
SwitchB	GE 0/0/3	VLANIF 40	1.1.2.1/24
SwitchC	GE 0/0/1	VLANIF 20	1.1.4.6/30
SwitchC	GE 0/0/2	VLANIF 50	1.1.3.1/24

配置思路

采用如下的思路配置 IPv4 静态路由：

1. 配置各接口所属 VLAN。
2. 配置各 VLANIF 接口的 IP 地址。
3. 在各主机上配置 IP 缺省网关。
4. 在各台 Switch 上配置 IP 静态路由及缺省路由。

数据准备

为完成此配置例，需准备如下的数据：

版权所有 © 华为技术有限公司

- 各接口所属的 VLAN，具体数据如图 5-1 所示。
- 各 VLAN 接口及主机的 IP 地址，具体数据如图 5-1 所示。
- SwitchA 的下一跳为 1.1.4.2 的缺省路由。
- SwitchB 的目的地址为 1.1.1.0，下一跳为 1.1.4.1 的静态路由。
- SwitchB 的目的地址为 1.1.3.0，下一跳为 1.1.4.6 的静态路由。
- SwitchC 的下一跳为 1.1.4.5 的缺省路由。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置主机

   配置主机 PC1 的缺省网关为 1.1.1.1，主机 PC2 的缺省网关为 1.1.2.1，主机 PC3 的缺省网关为 1.1.3.1。
4. 配置静态路由

   # 在 SwitchA 上配置 IP 缺省路由。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

   # 在 SwitchB 上配置两条 IP 静态路由。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
```

   # 在 SwitchC 上配置 IP 缺省路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
```
5. 验证配置结果

   # 查看 SwitchA 的 IP 路由表。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static 60   0           RD  1.1.4.2         Vlanif10
        1.1.1.0/24  Direct 0    0           D   1.1.1.1         Vlanif30
        1.1.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
        1.1.4.0/30  Direct 0    0           D   1.1.4.1         Vlanif10
        1.1.4.1/32  Direct 0    0           D   127.0.0.1       InLoopBack
        1.1.4.2/32  Direct 0    0           D   1.1.4.2         Vlanif10
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
```

   # 使用 **ping** 命令验证连通性。

```
[SwitchA] ping 1.1.3.1
  PING 1.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.3.1: bytes=56 Sequence=1 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=2 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=3 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=4 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=5 ttl=254 time=62 ms

  --- 1.1.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```


版权所有 © 华为技术有限公司

```
    0.00% packet loss
    round-trip min/avg/max = 62/62/63 ms
```

使用 Tracert 命令验证连通性。

```
[SwitchA] tracert 1.1.3.1
 traceroute to  1.1.3.1(1.1.3.1), max hops: 30 ,packet length: 40
 1 1.1.4.2 31 ms  32 ms  31 ms
 2 1.1.4.6 62 ms  63 ms  62 ms
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 1.1.4.1 255.255.255.252
#
interface Vlanif30
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20 40
#
interface Vlanif10
 ip address 1.1.4.2 255.255.255.252
#
interface Vlanif20
 ip address 1.1.4.5 255.255.255.252
#
interface Vlanif40
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20

#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 40
#
ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
#
return
```


版权所有 © 华为技术有限公司

- SwitchC 的配置文件

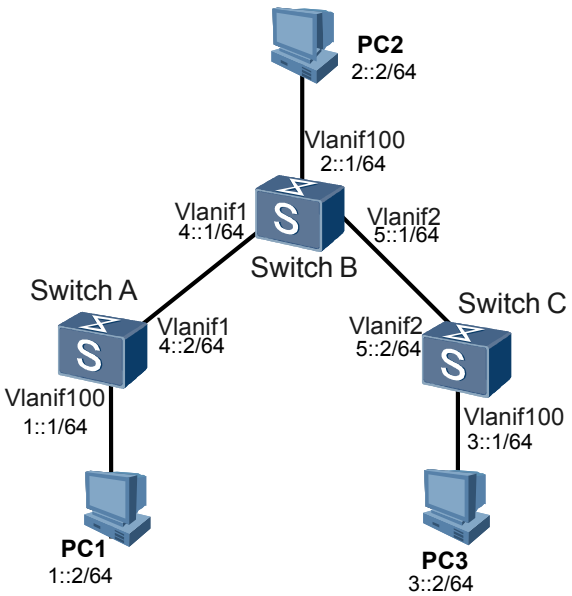
```
#
 sysname SwitchC
#
 vlan batch 20 50
#
interface Vlanif20
 ip address 1.1.4.6 255.255.255.252
#
interface Vlanif50
 ip address 1.1.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 50
  port hybrid untagged vlan 50
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
#
return
```

配置 IPv6 静态路由示例

组网要求

如图 5-2 所示，图中所有 IPv6 地址的前缀长度都为 64。要求各 Switch 之间配置 IPv6 静态路由协议后，可以使所有主机和 Switch 之间互通。

图 5-2 配置 IPv6 静态路由组网图



配置思路

采用如下的思路配置 IPv6 静态路由：

版权所有 © 华为技术有限公司

1. 首先配置各 Switch 的 IPv6 地址，使网络互通。
2. 在各 Switch 上配置到目的地址的 IPv6 静态路由及缺省路由。
3. 在各主机上配置 IPv6 缺省网关，使任意两台主机可以互通。

数据准备

为完成此配置例，需准备如下的数据：

- 主机 PC1 的缺省网关 1::1，主机 PC2 的缺省网关 2::1，主机 PC3 的缺省网关 3::1。

配置步骤

1. 配置各设备的 IPv6 地址（略）
2. 配置 IPv6 静态路由

   # 在 SwitchA 上配置 IPv6 缺省路由。

   ```
   [SwitchA] ipv6 route-static :: 0 4::1
   ```

   # 在 SwitchB 上配置两条 IPv6 静态路由。

   ```
   [SwitchB] ipv6 route-static 1:: 64 4::2
   [SwitchB] ipv6 route-static 3:: 64 5::2
   ```

   # 在 SwitchC 上配置 IPv6 缺省路由。

   ```
   [SwitchC] ipv6 route-static :: 0 5::1
   ```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 ipv6
#
interface Vlanif1
 ipv6 address 4::2/64
#
interface Vlanif100
 ipv6 address 1::1/64
#
ipv6 route-static :: 0 4::1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 ipv6
#
interface Vlanif1
 ipv6 address 4::1/64
#
interface Vlanif2
 ipv6 address 5::1/64
#
interface Vlanif 100
 ipv6 address 2::1/64
#
ipv6 route-static 1:: 64 4::2
ipv6 route-static 3:: 64 5::2
#
return
```


版权所有 © 华为技术有限公司

- SwitchC 的配置文件

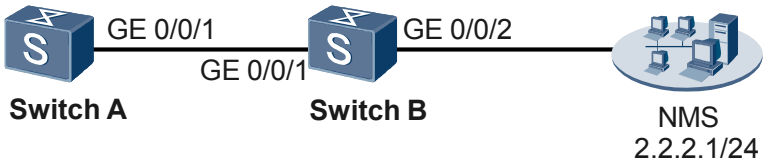
```
#
 sysname SwitchC
#
 ipv6
#
interface Vlanif2
 ipv6 address 5::2/64
#
interface Vlanif1
 ipv6 address 3::1/64
#
ipv6 route-static :: 0 5::1
#
return
```

配置 BFD for IPv4 静态路由示例

组网需求

如图 5-3 所示，SwitchA 通过 SwitchB 和 NMS 跨网段相连。在 SwitchA 上配置静态路由可以与 NMS 进行正常通信。在 SwitchA 和 SwitchB 之间配置 BFD 会话检测链路是否发生故障。

图 5-3 配置 BFD for IPv4 静态路由组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	1.1.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	1.1.1.2/24
SwitchB	GE 0/0/2	VLANIF 20	2.2.2.2/24

配置思路

采用如下思路配置 BFD for IPv4 静态路由：

1. 在 SwitchA 和 SwitchB 上配置 BFD Session，检测 SwitchA 和 SwitchB 之间的链路。
2. 配置 SwitchA 到 NMS 的静态路由并绑定 BFD Session。

数据准备

为完成此配置例，需要准备如下数据：

- 各接口所属的 VLAN，具体数据如图 5-3 所示。
- 各 VLAN 接口及主机的 IP 地址，具体数据如图 5-3 所示。
- BFD 检测的对端 IP 地址。

版权所有 © 华为技术有限公司

- BFD Session 的本地标志符和远端标识符。
- 从 SwitchA 到达 NMS 的静态路由。

配置步骤

以下仅给出 Switch 的配置步骤，图 5-3 中其它设备的配置步骤请参见对应设备的配置手册。

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 SwitchA 和 SwitchB 之间的 BFD 会话

   # 在 SwitchA 上配置与 SwitchB 之间的 BFD Session。

```
<SwitchA> system-view
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd aa bind peer-ip 1.1.1.2
[SwitchA-bfd-session-aa] discriminator local 10
[SwitchA-bfd-session-aa] discriminator remote 20
[SwitchA-bfd-session-aa] commit
[SwitchA-bfd-session-aa] quit
```

   # 在 SwitchB 上配置与 SwitchA 之间的 BFD Session。

```
<SwitchB> system-view
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd bb bind peer-ip 1.1.1.1
[SwitchB-bfd-session-bb] discriminator local 20
[SwitchB-bfd-session-bb] discriminator remote 10
[SwitchB-bfd-session-bb] commit
[SwitchB-bfd-session-bb] quit
```

4. 配置静态缺省路由并绑定 BFD 会话

   # 在 SwitchA 上配置到外部网络的静态缺省路由，并绑定 BFD 会话 aa。

```
[SwitchA] ip route-static 2.2.2.1 24 1.1.1.2 track bfd-session aa
[SwitchA] quit
```

5. 验证配置结果

   # 配置完成后，在 SwitchA 和 SwitchB 上执行 **display bfd session all** 命令，可以看到 BFD 会话已经建立，且状态为 Up。

   以 SwitchA 上的显示为例。

```
<SwitchA> display bfd session all
--------------------------------------------------------------------------------
LocalRemote PeerIPAddressInterface NameStateType
--------------------------------------------------------------------------------
10201.1.1.2--UpS_IP
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 1/0
```

   # 在 SwitchA 上查看 IP 路由表，静态路由存在于路由表中。

```
<SwitchA> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.0/24  Direct  0    0           D   1.1.1.1         Vlanif10
        1.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        1.1.1.2/32  Direct  0    0           D   1.1.1.2         Vlanif10
        2.2.2.0/24  Static  60   0          RD   1.1.1.2         Vlanif10
```


版权所有 © 华为技术有限公司

```
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

在 SwitchA 上打开终端显示调试信息功能。

```
<SwitchA> terminal monitor
<SwitchA> terminal debugging
```

对 SwitchB 的接口 VLANIF10 执行 **shutdown** 命令模拟链路故障。

```
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] shutdown
```

在 SwitchA 上可以看到以下调试信息，表明 BFD 检测到链路故障。

```
<SwitchA>
*0.27708400 SwitchA RM/3/RMDEBUG:
 RM_USR_BFDRefreshRT_H:
 BfdSessionID  = 10
 BfdEvent       = 0X0
 USR : UsrDbID = 0X6, DestAdd = 0X0, Mask    = 0X0, NextHop = 0X1010102
 URT : TableID = 0X1, EntryID = 0XB, ProcID = 0X2, FLAG     = 0X8114000
```

查看 SwitchA 的路由表，发现静态路由 2.2.2.0/24 也不存在了。因为静态路由绑定了 BFD 会话，当 BFD 检测到故障后，就会迅速通知所绑定的静态路由不可用。

```
<SwitchA> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.0/24  Direct  0    0           D  1.1.1.1         Vlanif10
        1.1.1.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
        1.1.1.2/32  Direct  0    0           D  1.1.1.2         Vlanif10
      127.0.0.0/8   Direct  0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

对 SwitchB 的接口 VLANIF10 执行 **undo shutdown** 命令模拟链路恢复正常。

```
[SwitchB-Vlanif10]undo shutdown
```

查看 SwitchA 的路由表，发现静态路由 2.2.2.0/24 重新出现在路由表中。因为当 BFD 检测到链路恢复正常后，就会迅速通知所绑定的静态路由重新生效。

```
<SwitchA> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.0/24  Direct  0    0           D   1.1.1.1         Vlanif10
        1.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        1.1.1.2/32  Direct  0    0           D   1.1.1.2         Vlanif10
        2.2.2.0/24  Static  60   0          RD   1.1.1.2         Vlanif10
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
 bfd
#
interface Vlanif10
```


版权所有 © 华为技术有限公司

```
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
bfd aa bind peer-ip 1.1.1.2
 discriminator local 10
 discriminator remote 20
 commit
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2 track bfd-session aa
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10 20
#
 bfd
#
interface Vlanif10
 ip address 1.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bfd bb bind peer-ip 1.1.1.1
 discriminator local 20
 discriminator remote 10
 commit
#
return
```

5.2 RIP 配置

RIP 可以发布和接收路由信息，影响交换机的数据转发途径，并提供网管功能，主要用于规模较小的网络中。

5.2.1 RIP 概述

RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，在小型网络中有广泛的应用。

路由信息协议 RIP (Routing Information Protocol)是一种较为简单的内部网关协议 IGP (Interior Gateway Protocol)，主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP。

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它通过 UDP 报文进行路由信息的交换，使用的端口号为 520。

RIP 使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在 RIP 中，交换机到与它直接相连网络的跳数为 0，通过一个交换机可达的网络的跳数为 1，其余依此

版权所有 © 华为技术有限公司

类推。为限制收敛时间，RIP 规定度量值取 0 ～ 15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIP 不可能在大型网络中得到应用。

为提高性能，防止产生路由循环，RIP 支持水平分割（Split Horizon）和毒性反转（Poison Reverse）功能。

- 水平分割指的是 RIP 从某个接口学到的路由，不会从该接口再发回给邻居设备。这样不但减少了带宽消耗，还可以防止路由环路。
- 毒性逆转指的是 RIP 从某个接口学到路由后，将该路由的开销设置为 16（即指明该路由不可达），并从原接口发回邻居设备。利用这种方式，可以清除对方路由表中的无用路由。

由于 RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此在实际组网中仍有广泛的应用。

RIP 有两个版本：RIP-1 和 RIP-2。RIP-1 是有类别路由协议（Classful Routing Protocol）。RIP-2 是一种无分类路由协议（Classless Routing Protocol），并且使用 224.0.0.9 作为 RIP 交换机的组播地址。

与 RIP-1 相比，RIP-2 有以下优势：

- 支持外部路由标记（Route Tag），可以在路由策略中根据 Tag 对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，只有支持 RIP-2 的设备才能收到协议报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

5.2.2 AC6605 支持的 RIP 特性

AC6605 中支持的 RIP 特性包括：RIP-1、RIP-2、水平分割、毒性逆转和多实例。

在 AC6605 目前的实现中，支持以下 RIP 特性：

- 支持 RIP-1 和 RIP-2。
- 支持 RIP 多实例。它可以作为 VPN 内部路由协议，在 MPLS L3VPN 网络中的 CE 和 PE 之间运行。

5.2.3 配置 RIP 的基本功能

配置 RIP 的基本功能主要包括启动 RIP、指定运行 RIP 的网段以及版本号，是能够使用 RIP 特性的前提。

建立配置任务

在配置 RIP 基本功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

RIP 基本功能的配置任务包括 RIP 特性配置中涉及的基本配置，完成本节的配置就可以使用 RIP 特性。

版权所有 © 华为技术有限公司

前置任务

在配置 RIP 的基本功能之前，需完成以下任务：

- 配置链路层协议。
- 配置接口的网络层地址，使相邻节点的网络层可达。

数据准备

在配置 RIP 的基本功能之前，需要准备以下数据。

序号	数据
1	RIP 进程号
2	RIP 接口所在的网段
3	RIP 版本号

启动 RIP

创建 RIP 进程是进行所有 RIP 配置的前提。

背景信息

如果在启动 RIP 前在接口视图下配置了 RIP 相关命令，这些配置只有在 RIP 启动后才会生效。

请在需要运行 RIP 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行 **rip** [*process-id*]，启动 RIP，进入 RIP 视图。

RIP 支持多实例，可以将 RIP 进程与 VPN 实例关联。此时，需执行 **rip** [*process-id*] **vpn-instance** *vpn-instance-name* 命令。

----结束

在指定网段使能 RIP

RIP 只在指定网段上的接口运行。对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由转发出去。因此，RIP 启动后必须指定其工作网段。

背景信息

缺省情况下，RIP 启动后在所有接口上禁用。

请在需要运行 RIP 协议的每台交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **network** *network-address*，在指定网段使能 RIP。

network-address 为自然网段的地址。

说明

一个接口只能与一个 RIP 进程相关联。

对于一个配置了多个子接口 IP 地址的物理接口，如果已经宣告该接口上的任一网段到某 RIP 进程，则该接口无法后续再和其他 RIP 进程相关联。

----结束

配置 RIP 的版本号

RIP 的版本包括 RIP-1 和 RIP-2 两种，它们的功能有所不同。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

- 配置全局 RIP 版本号
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。
  3. 执行 **version** { **1** | **2** }命令，指定全局 RIP 版本。
- 配置接口的 RIP 版本号
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入接口视图。
  3. 执行命令 **rip version** { **1** | **2** [**broadcast** | **multicast**] }，指定接口接收的 RIP 版本。

     说明

     缺省情况下，接口接收 RIP-1 和 RIP-2 的报文，只发送 RIP-1 报文。当配置接口版本为 RIP-2 时，同时可以指定报文的发送方式。如果没有配置接口的 RIP 版本号则以全局版本为准，接口下配置的版本号优先级高于全局版本号。

----结束

检查配置结果

RIP 基本功能配置成功后，您可以查看到 RIP 的当前运行状态、配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

任务示例

执行命令 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]，可以看到使能了 RIP 进程的当前运行状态及配置信息。信息显示当前有 2 个 VPN 实例正在运行。第一个是公网实例，第二个实例名称为 **VPN-Instance-1**。

```
<Quidway> display rip
  Public VPN-instance
    RIP process : 6000
       RIP version   : 2
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Summary       : Enabled
       Hostroutes    : Enabled
       Maximum number of balanced paths : 4
       Update time   : 30 sec              Age time : 180 sec
       Suppress time : 0 sec   Garbage-collect time : 120 sec
       Graceful restart  : Disabled
       Silent interfaces : None
       Default Route : Disabled
       Verify-source : Enabled
       Networks : None
       Configured peers             : None
       Number of routes in database : 0
       Number of interfaces enabled : 0
       Triggered updates sent       : 0
       Number of route changes      : 0
       Number of replies to queries : 0
       Number of routes in ADV DB   : 0

    RIP process : 1
       RIP version   : 2
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Summary       : Enabled
       Hostroutes    : Enabled
       Maximum number of balanced paths : 4
       Update time   : 30 sec              Age time : 180 sec
       Suppress time : 0 sec   Garbage-collect time : 120 sec
       Graceful restart  : Disabled
       Silent interfaces : None
       Default Route : Disabled
       Verify-source : Enabled
       Networks :
       10.0.0.0
       Configured peers             : None
       Number of routes in database : 3
       Number of interfaces enabled : 3
       Triggered updates sent       : 0
       Number of route changes      : 4
       Number of replies to queries : 0
       Number of routes in ADV DB   : 2

  Total count for 2 process :
       Number of routes in database : 3
       Number of interfaces enabled : 3
```


版权所有 © 华为技术有限公司

```
    Number of routes sendable in a periodic update : 9
    Number of routes sent in last periodic update : 0
```

执行命令 **display rip** *process-id* **route**，可以看到指定 RIP 进程的所有激活、非激活的路由。

```
<Quidway> display rip 1 route
 Route Flags: R - RIP
              A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 192.4.5.1  on Vlanif10
      Destination/Mask        Nexthop      Cost   Tag      Flags    Sec
        172.4.0.0/16          192.4.5.1       1     0         RA     15
        192.13.14.0/24        192.4.5.1       2     0         RA     15
        192.4.5.0/24          192.4.5.1       1     0         RA     15
```

5.2.4 配置 RIP 的路由属性

在实际应用中，可以通过配置 RIP 的路由属性改变 RIP 的选路策略，以满足复杂网络环境中的需要。

建立配置任务

RIP 的路由属性包括 RIP 协议的优先级、接口的附加度量值和最大等价路由条数。

应用环境

在实际应用中，可以通过配置 RIP 的路由属性改变 RIP 的选路策略，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 通过调整 RIP 接口的附加度量值来影响路由的选择；
- 当多个路由协议发现相同的路由时，通过配置 RIP 的协议优先级来改变路由协议的优先顺序；
- 使用多条等价路由进行负载分担。

前置任务

在配置 RIP 的路由属性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIP 的基本功能**。

数据准备

在配置 RIP 的路由属性之前，需要准备以下数据。

序号	数据
1	接口的附加度量值
2	RIP 协议优先级的值
3	最大等价路由条数

版权所有 © 华为技术有限公司

配置接口的附加度量值

附加路由度量值是在 RIP 路由原来度量值的基础上所增加的度量值（跳数）。对于 RIP 接收和发布路由，可通过不同的命令配置附加度量值。

背景信息

附加路由度量值是在 RIP 路由原来度量值的基础上所增加的度量值（跳数）。

- **rip metricin** 用于在接收到路由后，给其增加一个附加度量值，再加入路由表中，使得路由表中的度量值发生变化。运行该命令会影响到本地设备和其他设备的路由选择。
- **rip metricout** 用于自身路由的发布，发布时增加一个附加的度量值，但路由表中的度量值不会发生变化。运行该命令不会影响本地设备的路由选择，但是会影响其他设备的路由选择。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 执行命令 **rip metricin** *value*，设置接口在接收路由时增加的度量值。

步骤 4 执行命令 **rip metricout** { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }，设置接口在发布路由时增加的度量值。

说明

当用 ACL 或 ip-prefix 方式来设置接口发送 RIP 路由增加的度量值时，指定 *value1* 为通过过滤策略的 RIP 路由增加的度量值，没有通过过滤的 RIP 路由增加的度量值为 1。

----结束

配置 RIP 协议优先级

当有多种协议的路由存在时，通过配置 RIP 的协议优先级，可以调整交换机选择最优路由。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **preference** { *preference* | **route-policy** *route-policy-name* } *，设置 RIP 协议的优先级。

版权所有 © 华为技术有限公司

缺省情况下，RIP 协议的优先级为 100。

----结束

配置最大等价路由条数

通过配置 RIP 最大等价路由条数，可以调整进行负载分担的路由数目。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **maximum load-balancing** *number*，设置 RIP 最大等价路由条数。

----结束

检查配置结果

RIP 的路由属性配置成功后，您可以查看到 RIP 的当前运行状态、配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **database** 命令查看 RIP 发布数据库的所有激活路由。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

任务示例

执行命令 **display rip** *process-id* **database**，可以看到指定 RIP 进程的数据库信息。

```
<Quidway> display rip 100 database
10.0.0.0/8, cost 0, ClassfulSumm
        10.10.10.0/24, cost 0, [A], Rip-interface
        10.137.220.0/23, cost 1, [A], nexthop 10.10.10.2
```

5.2.5 控制 RIP 路由信息的发布

对 RIP 路由信息的发布进行精确的控制，可以满足复杂网络环境中的需要。

版权所有 © 华为技术有限公司

建立配置任务

RIP 路由信息的发布可通过缺省路由、更新报文、引入外部路由信息的方式。

应用环境

在实际应用中，有时候需要对 RIP 路由信息的发布进行更为精确的控制，以满足网络需要。通过本节的配置过程，你可以：

- 向邻居发布缺省路由；
- 抑制接口发送 RIP 更新报文；
- 在多路由协议环境中引入外部路由并对发布的路由进行过滤。

前置任务

在控制 RIP 路由信息的发布之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIP 的基本功能**。

数据准备

在控制 RIP 路由信息的发布之前，需要准备以下数据。

序号	数据
1	需要发布的缺省路由的度量值
2	需要抑制发送 RIP 更新报文的接口编号
3	要引入的外部路由协议名称和进程号

配置 RIP 发布缺省路由

缺省路由是指目的地址为 0.0.0.0 的路由。缺省情况下，RIP 不向其邻居发布缺省路由。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **default-route originate** [**cost** *cost*]，使能当前交换机生成缺省路由向 RIP 邻居发布，并且可设置该路由的度量值。

----结束

版权所有 © 华为技术有限公司

禁止接口发送更新报文

禁止接口发送更新报文，是预防路由环路的一种方式，可通过两种方法来实现。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

- 在 RIP 进程下配置（优先级高）
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。
  3. 请根据需要，设置接口为抑制状态。
     - 执行命令 **silent-interface all**，设置所有接口为抑制状态。
     - 执行命令 **silent-interface** *interface-type interface-number*，禁止一个接口发送更新报文。

     可以设置接口为抑制状态，使其只接收报文，用来更新自己的路由表，但不能发送 RIP 报文。**silent-interface** 的优先级大于在接口下配置的 **rip output**，默认情况下为不抑制状态。
- 在接口视图下配置（优先级低）
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的只能是 VLANIF 接口。
  3. 执行命令 **undo rip output**，禁止接口发送 RIP 更新报文。

     可以对接口单独指定是否发送或接收 RIP 更新报文，其优先级小于 **silent-interface**。默认情况下允许发送 RIP 更新报文。

----结束

配置 RIP 引入外部路由信息

RIP 可以引入其他进程或其他协议学到的路由信息，从而丰富路由表项。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 （可选）执行命令 **default-cost** *cost*，设定路由引入的缺省度量值。

如果在引入路由时没有指定度量值，则使用缺省度量值。

步骤 4 （可选）执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]| *interface-type interface-number*]，对引入的路由信息向外发布时进行过滤。

版权所有 © 华为技术有限公司

由于 RIP 要发布的路由信息中，有可能是引入的其他路由协议的路由信息，所以可通过指定 *protocol* 参数来对这些特定的路由信息进行过滤。如果没有指定 *protocol* 参数，则对所有要发布的路由信息进行过滤，包括引入的路由和本地 RIP 路由（相当于直连路由）。

说明

RIP 协议规定的 Tag 字段长度为 16bits，其他路由协议的 Tag 字段长度为 32bits。如果在引入其他路由协议时，应用的路由策略中使用 Tag，则应确保 Tag 值不超过 65535，否则将导致路由策略失效或者产生错误的匹配结果。

----结束

检查配置结果

控制 RIP 路由信息的发布配置成功后，您可以查看到 RIP 的当前运行状态、配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **database** 命令查看 RIP 发布数据库的所有激活路由。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

任务示例

执行命令 **display rip** *process-id* **database**，可以看到指定 RIP 进程的数据库信息。

```
<Quidway> display rip 100 database
10.0.0.0/8, cost 0, ClassfulSumm
        10.10.10.0/24, cost 0, [A], Rip-interface
        10.137.220.0/23, cost 1, [A], nexthop 10.10.10.2
```

5.2.6 控制 RIP 路由信息的接收

对 RIP 路由信息的接收进行精确的控制，可以满足复杂网络环境中的需要。

建立配置任务

RIP 路由信息的接收可通过更新报文、接收主机路由等方式。

应用环境

在实际应用中，有时候需要对 RIP 路由信息的接收进行更为精确的控制，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 禁止接口接收 RIP 的更新报文；
- 对接收的路由信息进行过滤；

版权所有 © 华为技术有限公司

- 在多路由协议环境中引入外部路由并对接收的路由进行过滤。

前置任务

在控制 RIP 路由信息的接收之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIP 的基本功能**。

数据准备

在控制 RIP 路由信息的接收之前，需要准备以下数据。

序号	数据
1	对路由信息过滤时所需要的相关过滤列表

禁止接口接收更新报文

禁止接口接收更新报文，是预防路由环路的一种方式。

背景信息

通过 **undo rip input** 命令可以禁止接口接收 RIP 更新报文，该命令优先级小于 **silent-interface**。

缺省情况下，允许接收 RIP 更新报文。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 执行命令 **undo rip input**，禁止接口接收 RIP 更新报文。

----结束

禁止 RIP 接收主机路由

禁止 RIP 接收主机路由功能，可以使路由器拒绝接收主机路由，防止路由器因接收到大量无意义路由而浪费网络资源。

背景信息

在某些特殊情况下，交换机会收到大量来自同一网段的主机路由，这些路由对于路由寻址没有多少作用，却占用了大量网络资源。配置了禁止主机路由功能后，交换机能够拒绝它所收到的主机路由。

缺省情况下，允许主机路由加到路由表里。

版权所有 © 华为技术有限公司

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **undo host-route**，禁止主机路由加到路由表里。

----结束

配置 RIP 对接收的路由进行过滤

通过指定访问控制列表和地址前缀列表，可以配置入口过滤策略，对接收的路由进行过滤。在接收路由时，还可以指定只接收来自某个邻居的 RIP 报文。

背景信息

交换机提供路由信息过滤功能，通过指定访问控制列表和地址前缀列表，可以配置入口或出口过滤策略，对接收和发布的路由进行过滤。

在接收路由时，还可以指定只接收来自某个邻居的 RIP 报文。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 请根据需要，配置 RIP 对接收的路由进行过滤。

- 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**，基于 ACL 过滤学到的路由信息。
- 执行命令 **filter-policy gateway** *ip-prefix-name* **import**，基于目的地址前缀过滤邻居发布的路由信息。
- 执行命令 **filter-policy ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] **import** [*interface-type interface-number*]，对指定接口学到的路由进行基于目的地址前缀的过滤和基于邻居的过滤。

说明

当需要对发布的路由进行过滤时，可以执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]。

----结束

检查配置结果

控制 RIP 路由信息的接收配置成功后，您可以查看到 RIP 的当前运行状态、配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **database** [**verbose**]命令查看 RIP 发布数据库的所有激活路由。
- 使用 **display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**]命令查看 RIP 的接口信息。
- 使用 **display rip** *process-id* **neighbor** [**verbose**]命令查看 RIP 的邻居信息。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

任务示例

执行命令 **display rip** *process-id* **database**，可以看到指定 RIP 进程的数据库信息。

```
<Quidway> display rip 100 database
10.0.0.0/8, cost 0, ClassfulSumm
       10.10.10.0/24, cost 0, [A], Rip-interface
       10.137.220.0/23, cost 1, [A], nexthop 10.10.10.2
```

5.2.7 配置 RIP-2 特性

RIP-2 是 RIP version 2 的简称，它与 RIP-1 的不同点在于，RIP-2 支持 VLSM 和 CIDR，并支持验证功能，从而功能更加完善，安全性更高。

建立配置任务

在配置 RIP-2 特性之前，了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

RIP-2 是一种有类别路由协议（Classless Routing Protocol），报文中带有子网掩码信息。因此部署 RIP-2 网络，可以节省 IP 地址，避免浪费 IP 地址。并且对于 IP 地址不连续的网络，不能够部署 RIP-1，此时只能部署 RIP-2。

RIP-2 特性专指一些仅针对 RIP-2 的配置，包括：

- RIP-2 的路由聚合
- RIP-2 报文的认证方式

前置任务

在配置 RIP-2 的基本功能之前，需完成以下任务：

- 配置链路层协议。
- 配置接口的网络层地址，使相邻节点的网络层可达。

数据准备

在配置 RIP-2 的基本功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	RIP-2 进程号
2	RIP-2 接口所在的网段

配置 RIP-2 的路由聚合

RIP-1 自然使能路由聚合功能，并且不能配置。RIP-2 支持 VLSM 和 CIDR，可以通过配置路由聚合，提高其灵活性。当需要将所有子网路由广播出去时，可关闭 RIP-2 的自动路由聚合功能。

背景信息

路由聚合是指：同一自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一条自然掩码的路由发送。这一功能主要用于减小路由表的尺寸，进而减少网络上的流量。

路由聚合对 RIP-1 不起作用。RIP-2 支持 VLSM 和 CIDR。当需要将所有子网路由广播出去时，可关闭 RIP-2 的自动路由聚合功能。

请在运行 RIP-2 协议的交换机上进行以下配置。

注意事项

如果配置了水平分割或毒性反转，有类聚合将失效。因此在向自然网段边界外发送聚合路由时，相关视图下的水平分割和毒性反转功能都应关闭。

操作步骤

- 使能 RIP-2 自动路由聚合
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。
  3. 执行命令 **version** 2，设置 RIP 版本为 RIP-2。
  4. 执行命令 **summary**，使能 RIP-2 自动路由聚合。

     说明

     在 RIP 视图下使用 **summary** 命令进行路由聚合，是使能 RIP-2 基于有类别网络的路由聚合。
- 配置 RIP-2 发布聚合地址
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的只能是 VLANIF 接口。
  3. 执行命令 **rip summary-address** *ip-address mask* [**avoid-feedback**]，配置 RIP-2 发布聚合的本地 IP 地址。

     说明

     在接口视图下使用 **rip summary-address** *ip-address mask* [**avoid-feedback**]命令进行路由聚合，是使能 RIP-2 基于无类别网络的路由聚合。

----结束

版权所有 © 华为技术有限公司

配置 RIP-2 报文的认证方式

RIP-2 支持对协议报文进行认证，并提供简单认证和 MD5 认证两种方式，增强安全性。

背景信息

RIP-2 支持两种认证方式：

- 简单认证。
- MD5 密文认证。

其中，简单认证使未加密的认证字随报文一同传送，不能提供安全保障，所以简单认证不能用于安全性要求较高的情况。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 配置 RIP-2 报文的认证方式。

- 执行命令 **rip authentication-mode simple** *password*，配置 RIP-2 报文为简单认证方式。
- 或执行命令 **rip authentication-mode md5** { **nonstandard** { *password-key1 key-id* } | **usual** *password-key2* }，配置 RIP-2 报文为 MD5 密文认证方式。

说明

如果配置 MD5 认证，则必须配置 MD5 的类型。**usual** 类型支持 IETF 标准认证报文格式，**nonstandard** 类型支持非标准认证报文格式。

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

----结束

检查配置结果

RIP-2 特性配置成功后，您可以查看到 RIP 的当前运行状态、配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **database** [**verbose**]命令查看 RIP 发布数据库的所有激活路由。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

版权所有 © 华为技术有限公司

5.2.8 调整和优化 RIP 网络

在某些特殊的网络环境中配置 RIP 的一些特性功能，例如配置 RIP 定时器、报文的发送间隔、最大数量，可以对 RIP 网络的性能进行调整和优化。

建立配置任务

在配置调整和优化 RIP 网络之前，了解一些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在某些特殊的网络环境中，需要配置 RIP 的一些特性功能，并需要对 RIP 网络的性能进行调整和优化。通过本节的配置过程，你可以：

- 通过调整 RIP 定时器来改变 RIP 网络的收敛速度；
- 通过调整接口发送更新报文的数量和时间间隔来减少对设备资源的消耗和对网络带宽的占用；
- 配置水平分割或毒性反转来防止路由循环；
- 使能 Replay-protect 功能，保证重启 RIP 进程后，邻居双方的正常通信。
- 在安全性较高网络环境中对报文进行有效性检查和验证；
- 在不支持广播或组播报文的链路上运行 RIP。

前置任务

在调整和优化 RIP 网络之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIP 的基本功能**。

数据准备

在调整和优化 RIP 网络之前，需要准备以下数据。

序号	数据
1	各定时器的值
2	接口每次发送更新报文的数量与时间间隔
3	最大等价路由条数
4	报文验证的方式和密码
5	RIP 邻居的 IP 地址

配置 RIP 定时器

RIP 有四个定时器：Update、Age、Suppress 和 Garbage-collect。改变这几个定时器的值，可以影响 RIP 的收敛速度。

版权所有 © 华为技术有限公司

背景信息

RIP 有四个定时器：Update、Age、Suppress 和 Garbage-collect。改变这几个定时器的值，可以影响 RIP 的收敛速度。有关定时器的详细解释，请参见《AC6605 无线接入控制器 特性描述 IP 路由》“定时器”。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **timers rip** *update age suppress garbage-collect*，配置 RIP 定时器的值。

说明

- RIP 定时器的值在更改后立即生效。
- 如果这四个定时器的值如果配置不当，会引起路由不稳定。它们的配置值关系是: *update*<*age*，*suppress*<*garbage-collect*。例如，如果更新时间大于失效时间，那么在更新时间内，如果 RIP 路由发生变化，交换机将无法及时通知邻居。
- 定时器值的调整应考虑网络的性能，并在所有运行 RIP 的交换机上进行统一配置，以免增加不必要的网络流量或引起网络路由震荡。
- 本系统不支持 Suppress 定时器。

缺省情况下，Update 定时器是 30 秒，Age 定时器是 180 秒，Suppress 定时器是 0 秒，Garbage-collect 定时器则是 Update 定时器的 4 倍，即 120 秒。

在实际应用中，Garbage-collect 定时器的超时时间并不是固定的，当 Update 定时器设为 30 秒时，Garbage-collect 定时器可能在 90 到 120 秒之间。

这是因为：RIP 在将不可达路由从路由表中彻底删除前，将通过发送 4 次定时更新报文对外发布这条路由（发送时权值设为 16），从而使所有邻居了解这条路由已经处于不可达状态。由于路由变为不可达状态并不总是恰好在一个更新周期的开始，因此，Garbage-collect 定时器的实际时长是 Update 定时器的 3 ～ 4 倍。

----结束

配置报文的发送间隔和发送报文的最大数量

通过设置 RIP 发送更新报文的时间间隔和每次发送报文的最大数量，可以很好的控制交换机 用于处理 RIP 更新报文的内存资源。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **rip pkt-transmit** { **interval** *interval* | **number** *pkt-count* } *，在该接口上设置 RIP 发送更新报文的时间间隔和每次发送报文的最大数量。

----结束

配置水平分割和毒性反转

通过配置 RIP 的水平分割和毒性反转特性，可以有效的防止路由环路。

背景信息

如果同时配置了毒性反转和水平分割，则只使用毒性反转功能。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 请根据需要选择配置。

- 执行命令 **rip split-horizon**，启动水平分割。
- 执行命令 **rip poison-reverse**，启动毒性反转。

----结束

配置 RIP 对更新报文进行有效性检查

RIP 对更新报文的检查包括 RIP-1 报文的零域检查和 RIP 更新报文的源地址检查两种，它们的功能和适用范围有所不同。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

- 对 RIP-1 报文中的零域进行检查
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。
  3. 执行命令 **checkzero**，对 RIP-1 报文的零域进行检查。

     RIP-1 报文中的有些字段必须为零，称之为零域。RIP-1 在接收报文时将对零域进行检查，零域的值不为零的 RIP-1 报文将不被处理。

     由于 RIP-2 的报文没有零域，此项配置对 RIP-2 无效。
- 对 RIP 更新报文的源地址进行检查
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

版权所有 © 华为技术有限公司

3. 执行命令 **verify-source**，对更新报文的源地址进行检查。

   RIP 在接收报文时将对源地址进行检查，没有通过检查的报文不被处理。缺省情况下进行源地址检查。

----结束

配置 RIP 邻居

通常情况下，RIP 使用广播或组播地址发送报文。如果在不支持广播或组播报文的链路上运行 RIP，则必须手工指定 RIP 的邻居。

背景信息

通常情况下，RIP 使用广播或组播地址发送报文。如果在不支持广播或组播报文的链路上运行 RIP，则必须在链路两端手工相互指定 RIP 的邻居。

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **peer** *ip-address*，配置 RIP 邻居。

----结束

检查配置结果

调整和优化 RIP 网络配置成功后，您可以查看到 RIP 的当前运行状态、路由信息、邻居信息及接口信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 RIP 的当前运行状态及配置信息。
- 使用 **display rip** *process-id* **database** [**verbose**]命令查看 RIP 发布数据库的所有激活路由。
- 使用 **display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**]命令查看 RIP 的接口信息。
- 使用 **display rip** *process-id* **neighbor** [**verbose**]命令查看 RIP 的邻居信息。
- 使用 **display rip** *process-id* **route** 命令查看所有激活、非激活的 RIP 路由。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**]，可以看到在指定接口上的 RIP 信息，此接口状态为 Up。

```
<Quidway> display rip 1 interface vlanif 10
------------------------------------------------------------------------
Interface         IP Address      State    Protocol            MTU
------------------------------------------------------------------------
Vlanif10          1.1.1.2         UP     RIPv1 Compatible     500
```

5.2.9 配置 RIP 的网管功能

通过配置 RIP 和 MIB 绑定，可以通过网管的环境来查看和配置 RIP。

建立配置任务

在配置 RIP 和 MIB 绑定之前，了解该特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

通过本节的配置过程，可以实现 RIP 和 MIB 的绑定。

前置任务

在配置 RIP 的网管功能之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIP 的基本功能**。

数据准备

无

配置 RIP 和 MIB 绑定

配置 RIP 和 MIB 绑定时，需要指定 RIP 的进程号。

背景信息

请在运行 RIP 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip mib-binding** *process-id*，设置 RIP 和 MIB 绑定。

该命令用来设置 MIB 和 RIP 进程号的绑定关系，指定接受 SNMP 请求的 RIP 进程号。

----结束

版权所有 © 华为技术有限公司

检查配置结果

RIP 和 MIB 绑定成功后，您可以查看到 RIP 的当前配置信息里含有相关绑定信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

步骤 1 使用 **display current-configuration** 命令查看交换机当前生效的配置参数。

----结束

5.2.10 配置 RIP 举例

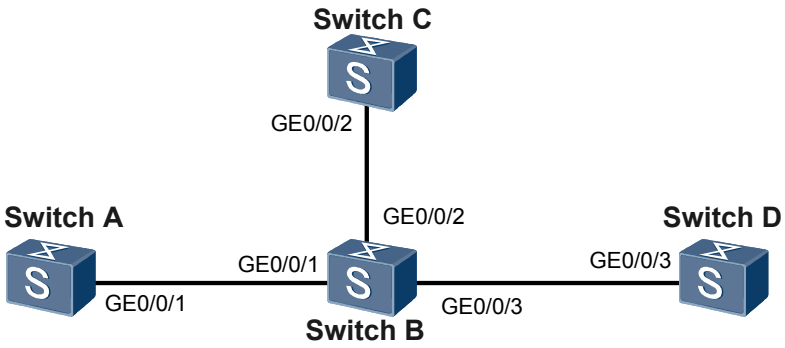
介绍 RIP 的各种组网举例。

配置 RIP 版本示例

组网需求

如图 5-4 所示，要求在 SwitchA、SwitchB、SwitchC 和 SwitchD 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。

图 5-4 配置 RIP 版本组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GigabitEthernet0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	GigabitEthernet0/0/1	VLANIF 10	192.168.1.2/24
SwitchB	GigabitEthernet0/0/2	VLANIF 20	172.16.1.1/24
SwitchB	GigabitEthernet0/0/3	VLANIF 30	10.1.1.1/24
SwitchC	GigabitEthernet0/0/2	VLANIF 20	172.16.1.2/24
SwitchD	GigabitEthernet0/0/3	VLANIF 30	10.1.1.2/24

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 RIP 的版本：

1. 配置各接口的 IP 地址，使网络可达。
2. 在各 Switch 上使能 RIP，配置 RIP 基本功能。
3. 在各 Switch 上配置 RIP-2 版本，查看精确的子网掩码信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属 VLAN，具体数据如图 5-4 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-4 所示。
- 在 SwitchA、SwitchB、SwitchC、SwitchD 上配置 RIPv2 版本。

配置步骤

1. 配置各接口所属 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 RIP 基本功能

   # 配置 SwitchA。

```
[SwitchA] rip
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] quit
```

   # 配置 SwitchB。

```
[SwitchB] rip
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 172.16.0.0
[SwitchB-rip-1] network 10.0.0.0
[SwitchB-rip-1] quit
```

   # 配置 SwitchC。

```
[SwitchC] rip
[SwitchC-rip-1] network 172.16.0.0
[SwitchC-rip-1] quit
```

   # 配置 SwitchD。

```
[SwitchD] rip
[SwitchD-rip-1] network 10.0.0.0
[SwitchD-rip-1] quit
```

   # 查看 SwitchA 的 RIP 路由表。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP
              A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlanif10
      Destination/Mask        Nexthop      Cost   Tag      Flags   Sec
         10.0.0.0/8           192.168.1.2     1     0         RA      14
         172.16.0.0/16        192.168.1.2     1     0         RA      14
         192.168.1.0/24       192.168.1.2     1     0         RA      14
```

   从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

4. 配置 RIP 的版本

   # 在 SwitchA 上配置 RIP-2。

```
[SwitchA] rip
```


版权所有 © 华为技术有限公司

```
[SwitchA-rip-1] version 2
[SwitchA-rip-1] quit
```

在 SwitchB 上配置 RIP-2。

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] quit
```

在 SwitchC 上配置 RIP-2。

```
[SwitchC] rip
[SwitchC-rip-1] version 2
[SwitchC-rip-1] quit
```

在 SwitchD 上配置 RIP-2。

```
[SwitchD] rip
[SwitchD-rip-1] version 2
[SwitchD-rip-1] quit
```

5. 验证配置结果

查看 SwitchA 的 RIP 路由表。

```
[SwitchA] display rip 1 route
  Route Flags: R - RIP
               A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlanif10
      Destination/Mask        Nexthop      Cost   Tag     Flags   Sec
         10.1.1.0/24          192.168.1.2     1     0        RA      32
         172.16.1.0/24        192.168.1.2     1     0        RA      32
         192.168.1.0/24       192.168.1.2     1     0        RA      14
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

说明

由于 RIP 路由信息的老化时间较长，所以在配置 RIP-2 版本后的一段时间里，路由表中可能还会存在 RIP-1 的路由信息。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10 20 30
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
interface Vlanif20
 ip address 172.16.1.1 255.255.255.0
#
interface Vlanif30
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
rip 1
 version 2
 network 192.168.1.0
 network 172.16.0.0
 network 10.0.0.0
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan 20
#
interface Vlanif20
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
rip 1
 version 2
 network 172.16.0.0
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan 30
#
interface Vlanif30
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
rip 1
 version 2
 network 10.0.0.0
#
return
```

配置 RIP 引入外部路由示例

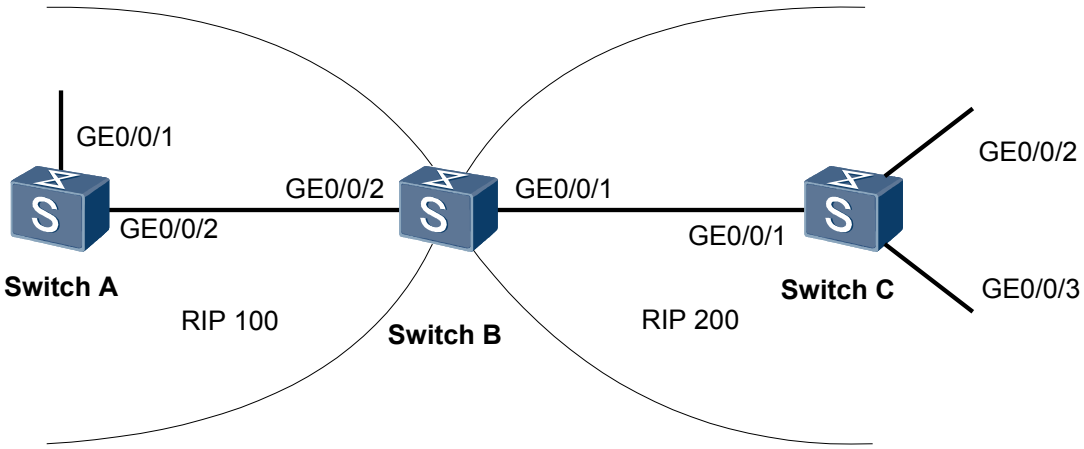
版权所有 © 华为技术有限公司

组网需求

如图 5-5 所示，SwitchB 上运行两个 RIP 进程：RIP100 和 RIP200。SwitchB 通过 RIP100 和 SwitchA 交换路由信息，通过 RIP200 和 SwitchC 交换路由信息。

要求在 SwitchB 上配置路由引入，将两个不同进程的 RIP 路由相互引入到对方的 RIP 进程中，将引入的 RIP200 的路由缺省度量值设为 3。并且需要在 SwitchB 配置过滤策略，对引入的 RIP200 的一条路由（192.168.4.0/24）进行过滤，使其不发布给 SwitchA。

图 5-5 配置 RIP 引入外部路由组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GigabitEthernet0/0/1	VLANIF 50	192.168.0.1/24
SwitchA	GigabitEthernet0/0/2	VLANIF 10	192.168.1.1/24
SwitchB	GigabitEthernet0/0/1	VLANIF 20	192.168.2.1/24
SwitchB	GigabitEthernet0/0/2	VLANIF 10	192.168.1.2/24
SwitchC	GigabitEthernet0/0/1	VLANIF 20	192.168.2.2/24
SwitchC	GigabitEthernet0/0/2	VLANIF 30	192.168.3.1/24
SwitchC	GigabitEthernet0/0/3	VLANIF 40	192.168.4.1/24

配置思路

采用如下的思路配置 RIP 引入外部路由：

1. 在各 Switch 上按照图中数据，分别使能 RIP100 和 RIP200，并指定网段。
2. 配置 SwitchB 将两个不同 RIP 进程的路由分别引入到对方的路由表中，并将引入的 RIP200 的缺省路由权值设为 3。
3. 在 SwitchB 上配置 ACL，对引入的 RIP200 的路由进行过滤。

数据准备

为完成此配置例，需准备如下的数据：

版权所有 © 华为技术有限公司

- 在 SwitchA 上使能 RIP100，指定网段 192.168.1.0，192.168.0.0。
- 在 SwitchB 上使能 RIP100 和 RIP200，指定网段 192.168.1.0，192.168.2.0。
- 在 SwitchC 上使能 RIP200，指定网段 192.168.2.0，192.168.3.0，192.168.4.0。
- 在 SwitchB 上将 RIP200 的路由引入 RIP100，并设置缺省路由权值为 3，配置 ACL2000，拒绝源为 192.168.4.0 网段的路由通过；将 RIP100 的路由引入 RIP200。

配置步骤

1. 配置各接口的 IP 地址（略）
2. 配置 RIP 基本功能

   # 在 SwitchA 上启动 RIP 进程 100。

```
[SwitchA] rip 100
[SwitchA-rip-100] network 192.168.0.0
[SwitchA-rip-100] network 192.168.1.0
[SwitchA-rip-100] quit
```

   # 在 SwitchB 上启动两个 RIP 进程，进程号分别为 100 和 200。

```
[SwitchB] rip 100
[SwitchB-rip-100] network 192.168.1.0
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 192.168.2.0
[SwitchB-rip-200] quit
```

   # 在 SwitchC 上启动 RIP 进程 200。

```
[SwitchC] rip 200
[SwitchC-rip-200] network 192.168.2.0
[SwitchC-rip-200] network 192.168.3.0
[SwitchC-rip-200] network 192.168.4.0
[SwitchC-rip-200] quit
```

   # 查看 SwitchA 的路由表信息。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0           D   192.168.0.1     vlanif50
    192.168.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D   192.168.1.1     vlanif10
    192.168.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0           D   192.168.1.2     vlanif10
```

3. 配置 RIP 引入外部路由

   # 在 SwitchB 上设置缺省路由值为 3，并将两个不同 RIP 进程的路由相互引入到对方的路由表中。

```
[SwitchB] rip 100
[SwitchB-rip-100] default-cost 3
[SwitchB-rip-100] import-route rip 200
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] quit
```

   # 查看路由引入后 SwitchA 的路由表信息。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
```


版权所有 © 华为技术有限公司

```
         Destinations : 10        Routes : 10
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0           D   192.168.0.1     vlanif50
    192.168.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D   192.168.1.1     vlanif10
    192.168.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0           D   192.168.1.2     vlanif10
    192.168.2.0/24  RIP    100  4           D   192.168.1.2     vlanif10
    192.168.3.0/24  RIP    100  4           D   192.168.1.2     vlanif10
    192.168.4.0/24  RIP    100  4           D   192.168.1.2     vlanif10
```

4. 配置 RIP 对引入的路由进行过滤

   # 在 SwitchB 上配置 ACL，并增加一条规则：拒绝源地址为 192.168.4.0/24 的数据包。

```
[SwitchB] acl 2000
[SwitchB-acl-basic-2000] rule deny source 192.168.4.0 0.0.0.255
[SwitchB-acl-basic-2000] rule permit
[SwitchB-acl-basic-2000]  quit
```

   # 在 SwitchB 上按照 ACL 的规则对引入的 RIP 进程 200 的路由 192.168.4.0/24 进行过滤。

```
[SwitchB] rip 100
[SwitchB-rip-100] filter-policy 2000 export
[SwitchB-rip-100] quit
```

5. 验证配置结果

   # 查看过滤后 SwitchA 的路由表。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0           D   192.168.0.1     vlanif50
    192.168.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D   192.168.1.1     vlanif10
    192.168.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0           D   192.168.1.2     vlanif10
    192.168.2.0/24  RIP    100  4           D   192.168.1.2     vlanif10
    192.168.3.0/24  RIP    100  4           D   192.168.1.2     vlanif10
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 50
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif50
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
```


版权所有 © 华为技术有限公司

```
#
rip 100
 network 192.168.0.0
 network 192.168.1.0
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
acl number 2000
 rule 5 deny source 192.168.4.0 0.0.0.255
 rule 10 permit
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
rip 100
 default-cost 3
 network 192.168.1.0
 filter-policy 2000 export
 import-route rip 200
#
rip 200
 network 192.168.2.0
 import-route rip 100
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 20 30 40
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Vlanif40
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
```


版权所有 © 华为技术有限公司

```
rip 200
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
#
return
```

5.3 RIPng 配置

RIPng 是在 IPv6 网络中应用的 RIP 协议，并在原 RIP 协议基础上进行了一些扩展。

5.3.1 RIPng 概述

RIPng 协议是基于 D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离。

RIPng（Routing Information Protocol Next Generation）是对原来的 IPv4 网络中 RIP-2 协议的扩展。大多数 RIP 的概念都可以用于 RIPng。

RIPng 对 RIP 协议的扩展

为了在 IPv6 网络中应用，RIPng 对原有的 RIP 协议进行了修改：

- UDP 端口号：使用 UDP 的 521 端口发送和接收路由信息。
- 组播地址：使用 FF02::9 作为链路本地范围内的 RIPng 路由器组播地址。
- 前缀长度：目的地址使用 128 比特的前缀长度（掩码长度）。
- 下一跳地址：使用 128 比特的 IPv6 地址。
- 源地址：使用链路本地地址 FE80::/10 作为源地址发送 RIPng 路由信息更新报文。

RIPng 工作机制

RIPng 协议是基于 D-V（Distance Vector，距离矢量）算法的路由协议。它通过 UDP 报文交换路由信息，使用的端口号为 521。RIPng 协议用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在 RIPng 协议中，从一个交换机到其直连网络的跳数为 0，而通过另一台交换机到达一个网络的跳数为 1，如此类推。当跳数大于或等于 16 时，目的网络或主机就被定义为不可达。

缺省情况下，RIPng 每 30 秒发送一个路由刷新报文。如果在 180 秒内没有收到网络邻居的路由刷新报文，RIPng 将从邻居学到的所有路由标识为不可达。如果在 300 秒内没有收到邻居的路由刷新报文，RIPng 将从路由表中删除这些路由。

为了避免路由环路，RIPng 支持水平分割和毒性逆转。此外，RIPng 也可以从其它的路由协议中引入路由。

每台运行 RIPng 的交换机都管理着路由数据库，包括到达网络中所有可达目的地址的路由项。这些路由项包括下列信息：

- 目的地址：主机或网络的 IPv6 地址。
- 下一跳地址：要到达目的地址交换机 所通过的下一个交换机 地址。
- 接口：转发 IP 报文所通过的接口。
- 开销：到达目的地址所经过的跳数。整数形式，取值范围是 0 ～ 16，取 16 时目的网络或主机就被定义为不可达。

版权所有 © 华为技术有限公司

- 定时器：从上次更改路由项到现在的时长。如果更改路由项，定时器将重置为 0。
- 路由标记：用来将内部路由协议与外部路由协议区别开来的标签。

5.3.2 AC6605 支持的 RIPng 特性

AC6605 中支持的 RIPng 特性包括：水平分割和毒性逆转。

AC6605 可以通过配置 RIPng 的路由属性改变 RIPng 的选路策略，并对 RIPng 路由信息的发布和接收进行更为精确的控制，以满足复杂网络环境中的需要。在某些特殊的网络环境中可以配置 RIPng 的一些特性功能，从而对 RIPng 网络的性能进行调整和优化。

5.3.3 配置 RIPng 的基本功能

配置 RIPng 的基本功能主要包括创建 RIPng 进程和在接口下使能 RIPng，是能够使用 RIP 特性的前提。

建立配置任务

为了让交换机 学到接口所在网段的路由，必须保证接口的链路状态为 Up。

应用环境

RIPng 基本能力的配置任务包括 RIPng 特性配置中涉及的基本配置，完成本节的配置就可以使用 RIPng 特性。

在 RIPng 的配置中，应该首先在系统视图下使能 RIPng。因为即使在接口视图下可以配置 RIPng 相关的命令，但这些命令只有在系统视图下使能了 RIPng 后才会生效。

前置任务

在配置 RIPng 基本功能之前，需完成以下任务：

- 使能交换机的 IPv6 能力。
- 配置接口的网络层地址，使相邻节点的网络层可达。

数据准备

在配置 RIPng 的基本功能之前，需准备以下数据。

序号	数据
1	RIPng 进程号
2	使能 RIPng 的接口

使能 RIPng 并进入 RIPng 视图

创建 RIPng 进程是进行 RIPng 相关配置的前提。通过此步骤，您还可以进入 RIPng 视图，进行相关配置。

版权所有 © 华为技术有限公司

背景信息

请在需要运行 RIPng 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，使能 RIPng 路由进程，进入 RIPng 视图。

如果只运行一个 RIPng 路由进程，则通常在命令中不指定参数 *process-id*，即默认 *process-id* 为 1。

该进程取消后，在接口上配置的有关于 **ripng** *process-id* **enable** 的命令要重新配置。

----结束

在接口下使能 RIPng

把接口使能到 RIPng 进程中，可以通过 RIPng 交换该接口的路由信息。

背景信息

请在需要运行 RIPng 的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口是交换机的网络侧的接口，即与其他设备互连的接口。为了让交换机学到接口所在网段的路由，必须保证接口的链路状态为 Up。

步骤 3 执行命令 **ripng** *process-id* **enable**，在指定接口上使能 RIPng。

说明

在接口视图下，如果没有使能 IPv6 功能，则此命令不可执行。

如果一台交换机有多个接口与其他设备互连，请重复步骤 2 到步骤 3。

----结束

检查配置结果

RIPng 基本功能配置成功后，您可以查看到 RIPng 的配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display ripng** [*process-id*]命令查看 RIPng 进程的配置信息。
- 使用 **display ripng** *process-id* **route** 命令查看所有激活和非激活 RIPng 路由。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display ripng** [*process-id*]，可以看到指定 RIPng 进程的配置信息。

```
<Quidway> display ripng 100
    RIPng process : 100
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 6
       Update time   : 30 sec   Age time  : 180 sec
       Suppress time : 0 sec   Garbage-Collect time : 120 sec
       Number of periodic updates sent : 0
       Number of trigger updates sent : 1
       Number of routes in database : 1
       Number of interfaces enabled : 1
       Totle Number of routes  : 0
       Totle Number of routes in ADV DB is  : 0
```

执行命令 **display ripng** *process-id* **route**，可以看到指定 RIPng 进程的所有激活和非激活 RIPng 路由信息。

```
<Quidway> display ripng 100 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------
 Peer FE80::200:5EFF:FE04:B602  on Vlanif60
 Dest 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec
 Dest 3FFE:C00:C18:2::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec
 Peer FE80::200:5EFF:FE04:B601  on Vlanif60
 Dest 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec
 Dest 3FFE:C00:C18:3::/64,
     via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec
 Peer FE80::200:5EFF:FE04:3302  on Vlanif60
 Dest 100::/32,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:1::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:2::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:3::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:4::/64,
```

5.3.4 配置 RIPng 的路由属性

通过配置 RIP 路由属性，可以改变路由器或 RIPng 的选路策略。

建立配置任务

RIPng 的路由属性包括 RIPng 协议的优先级、接口的度量值。

应用环境

在实际应用中，可以通过配置 RIPng 的路由属性改变 RIPng 的选路策略，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 通过调整 RIPng 接口的附加度量值来影响路由的选择；
- 当多个路由协议发现相同的路由时，通过配置 RIPng 的协议优先级来改变路由协议的优先顺序；

版权所有 © 华为技术有限公司

- 使用多条等价路由进行负载分担。

前置任务

在配置 RIPng 的路由属性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIPng 的基本功能**。

数据准备

在配置 RIPng 的路由属性之前，需要准备以下数据。

序号	数据
1	接口的附加度量值
2	RIPng 协议优先级的值
3	最大等价路由条数

配置 RIPng 的协议优先级

当有多种协议的路由存在时，通过配置 RIPng 的协议优先级，可以调整路由器选择最优路由。

背景信息

任何路由协议都具备特有的协议优先级，可使路由策略在不同的协议中选择最佳路由。可以手工设置 RIPng 协议的优先级，设置的值越大，其优先级就会越低。

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，使能 RIPng 路由进程，进入 RIPng 视图。

步骤 3 执行命令 **preference** { *preference* | **route-policy** *route-policy-name* } *，设置 RIPng 优先级。

----结束

配置接口的附加度量值

附加路由度量值是在 RIPng 路由原来度量值的基础上所增加的度量值（跳数）。对于 RIPng 接收和发布路由，可通过不同的命令配置附加度量值。

背景信息

附加路由度量值是在 RIPng 路由原来度量值的基础上所增加的度量值（跳数）。

版权所有 © 华为技术有限公司

- **ripng metricin** 用于在接收到路由后，给其增加一个附加度量值，再加入路由表中，使得路由表中的度量值发生变化。运行该命令会影响到本地设备和其他设备的路由选择。
- **ripng metricout** 用于自身路由的发布，发布时增加一个附加的度量值，但路由表中的度量值不会发生变化。运行该命令不会影响本地设备的路由选择，但是会影响其他设备的路由选择。

当用 ACL6 或 ipv6-prefix 方式来设置接口发送 RIPng 路由增加的度量值时，指定 *value1* 为通过过滤策略的 RIPng 路由增加的度量值，没有通过过滤的 RIPng 路由增加的度量值为 1。

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ripng metricin** *value*，设置接收 RIPng 报文时的路由附加度量值。

步骤 4 执行命令 **ripng metricout** { *value* }，设置发送 RIPng 报文时的路由附加度量值。

说明

如果交换机有多个接口与其他 RIPng 路由器连接，则需重复步骤 2 到步骤 4，直到配置完所有链路的开销。

----结束

配置 RIPng 的最大等价路由条数

通过配置 RIPng 最大等价路由条数，可以调整进行负载分担的路由数目。

背景信息

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

步骤 3 执行命令 **maximum load-balancing** *number*，配置 RIPng 的最大等价路由条数。

----结束

检查配置结果

RIPng 的路由属性配置成功后，您可以查看到 RIPng 的配置信息及路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display ripng** [*process-id*]命令查看 RIPng 进程的配置信息。
- 使用 **display ripng** *process-id* **database** 命令查看 RIPng 发布数据库中的路由。
- 使用 **display ripng** *process-id* **route** 命令查看所有激活和非激活 RIPng 路由。

----结束

5.3.5 控制 RIPng 路由信息的发布

对 RIPng 路由信息的发布进行精确的控制，可以满足复杂网络环境中的需要。

建立配置任务

RIPng 路由信息的发布可通过路由聚合、发布缺省路由、引入外部路由信息的方式。

应用环境

在实际应用中，有时候需要对 RIPng 路由信息的发布进行更为精确的控制，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 向邻居发布缺省路由；
- 抑制接口发送 RIPng 更新报文；
- 在多路由协议环境中引入外部路由并对发布的路由进行过滤。

前置任务

在控制 RIPng 路由信息的发布之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIPng 的基本功能**。

数据准备

在控制 RIPng 路由信息的发布之前，需要准备以下数据。

序号	数据
1	需要发布的缺省路由的度量值
2	要引入的外部路由协议名称和进程号

配置 RIPng 路由聚合

配置 RIPng 路由器在接口发布聚合 IPv6 地址，可以节省路由表中 RIPng 路由的空间。您还可以通过配置参数，禁止从接口学习到相同的聚合路由。

背景信息

配置 RIPng 路由器在接口上发布聚合后的 IPv6 前缀信息，而不是具体路由。

版权所有 © 华为技术有限公司

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ripng summary-address** *ipv6-address prefix-length* [**avoid-feedback**]，配置 RIPng 路由聚合。

----结束

配置 RIPng 发布缺省路由

RIPng 缺省路由的发布有两种方式，您可以根据组网的实际情况配置发布缺省路由。您还可以同时指定发布的缺省路由的开销值。

背景信息

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *vlanif vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ripng default-route** { **only** | **originate** } [**cost** *cost*]，配置 RIPng 发布缺省路由。

请根据组网的实际情况配置发布缺省路由。

- **only**：只发布 IPv6 缺省路由（::/0），抑制其它路由的发布。
- **originate**：发布 IPv6 缺省路由（::/0），但不影响其它路由的发布。

生成的 RIPng 缺省路由将强制通过指定接口的路由更新报文发布出去，该路由的发布不考虑其是否已经存在于 IPv6 路由表中。

----结束

配置 RIPng 引入外部路由的缺省权值

通过此配置，可以在 RIPng 从其他路由协议引入路由但没有指定权值的情况下，为引入的外部路由设置缺省 RIPng 权值。

背景信息

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **default-cost** *cost*，设置引入的外部路由的缺省权值。

该命令用于从其他路由协议引入路由但没有指定权值的情况下，为引入的外部路由设置缺省 RIPng 权值。

----结束

配置 RIPng 引入外部路由

和 RIP 协议类似，RIPng 也可以引入外部路由，提供更多路由信息。

背景信息

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

步骤 3 （可选）执行命令 **default-cost** *cost*，设置引入的外部路由的缺省权值。

步骤 4 执行命令 **import-route** *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name*] *，引入外部路由。

如果在路由引入过程中没有显式的指定路由开销，将采用缺省路由开销。

步骤 5 （可选）执行命令 **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]，配置 RIPng 对引入的路由信息进行过滤。

RIPng 可以通过 ACL6 和 IPv6 前缀列表对引入的路由进行过滤，只将符合条件的路由发布（Export）给邻居 RIPng 路由器。如果在此命令中没有指定 *protocol*，则对所有要发布的路由信息进行过滤，包括已引入的路由和本地 RIPng 路由（相当于直连路由）。

----结束

检查配置结果

控制 RIPng 路由信息的发布配置成功后，您可以查看到 RIPng 的路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display ripng** *process-id* **database** 命令查看 RIPng 发布数据库中的路由。
- 使用 **display ripng** *process-id* **route** 命令查看所有激活和非激活 RIPng 路由。

----结束

5.3.6 控制 RIPng 路由信息的接收

对 RIPng 路由信息的接收进行精确的控制，可以满足复杂网络环境中的需要。

版权所有 © 华为技术有限公司

建立配置任务

在配置控制 RIPng 路由信息的接收之前，了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在实际应用中，有时候需要对 RIPng 路由信息的接收进行更为精确的控制，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 禁止接口接收 RIPng 的更新报文；
- 对接收的路由信息进行过滤；
- 在多路由协议环境中引入外部路由并对接收的路由进行过滤。

前置任务

在控制 RIPng 路由信息的接收之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIPng 的基本功能**。

数据准备

在控制 RIngP 路由信息的接收之前，需要准备以下数据。

序号	数据
1	对路由信息过滤时所需要的相关过滤列表

配置 RIPng 对接收的路由信息进行过滤

通过 ACL6 和 IPv6 前缀列表对接收的路由信息过滤，可以有选择的接收路由信息。

背景信息

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

步骤 3 执行命令 **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**，对接收的路由信息进行过滤。

可以使用 ACL6 和 IPv6 前缀列表对接收的路由信息进行过滤，只有通过过滤的路由才能被加入到 RIPng 路由表。

----结束

版权所有 © 华为技术有限公司

检查配置结果

控制 RIPng 路由信息的接收配置成功后，您可以查看到 RIPng 的路由信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display ripng** *process-id* **database** 命令查看 RIPng 发布数据库中的路由。
- 使用 **display ripng** *process-id* **route** 命令查看所有激活和非激活 RIPng 路由。

----结束

5.3.7 调整优化 RIPng 网络

和 RIP 协议类似，您也可以配置 RIPng 定时器、水平分割、毒性逆转、零域检查，对 RIPng 网络的性能进行调整和优化。

建立配置任务

在配置调整和优化 RIPng 网络之前，了解一些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在某些特殊的网络环境中，需要配置 RIPng 的一些特性功能，并需要对 RIPng 网络的性能进行调整和优化。通过本节的配置过程，你可以：

- 通过调整 RIPng 定时器来改变 RIPng 网络的收敛速度；
- 配置水平分割或毒性反转来防止路由循环。

前置任务

在调整和优化 RIPng 网络之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 RIPng 的基本功能**。

数据准备

在调整和优化 RIPng 网络之前，需要准备以下数据。

序号	数据
1	各定时器的值

版权所有 © 华为技术有限公司

配置 RIPng 定时器

RIPng 有四个定时器：Update、Age、Suppress 和 Garbage-collect。请注意 RIPng 四个定时器的值如果配置不当，会引起路由不稳定。

背景信息

说明

请注意 RIPng 四个定时器的值如果配置不当，会引起路由不稳定。它们的关系是 *update<age*，*suppress<garbage-collect*。例如，如果更新时间大于失效时间，那么在更新时间内，如果 RIPng 路由发生变化，交换机将无法及时通知邻居。

本系统不支持设置 Suppress 定时器。

缺省情况下，Update 定时器的值为 30 秒，Age 定时器的值为 180 秒，Suppres 定时器的值为 0 秒，Garbage-collect 定时器的值为 120 秒。

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

步骤 3 执行命令 **timers ripng** *update age suppress garbage-collect*，设置 RIPng 定时器。

----结束

配置水平分割和毒性反转

通过配置 RIPng 的水平分割和毒性反转特性，可以有效的防止路由环路。

背景信息

水平分割，即从某接口学习到的路由将不会再由该接口发送出去，这在某种程度上避免了路由循环。但在特殊情况下，如帧中继和 X.25 等 NBMA 网络中必须禁止水平分割功能，以保证路由的正确发布。

当毒性反转被使能时，从一个接口学到的路由还可以从这个接口向外发布，但此时这些路由的 metric 值已设置为 16，即不可达。

当毒性反转和水平分割都使能的情况下，只采用毒性反转功能。

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 请根据需要选择配置。

- 执行命令 **ripng split-horizon** ，使能水平分割功能。
- 执行命令 **ripng poison-reverse**，使能毒性反转功能。

----结束

版权所有 © 华为技术有限公司

使能 RIPng 报文的零域检查

RIPng 报文中的一些字段必须配置为 0，也称为零域。如果零域中的值不为零，这些报文将被忽略，不做处理。

背景信息

RIPng 报文中的一些字段必须配置为 0，也称为零域。如果零域中的值不为零，这些报文将被忽略，不做处理。

请在运行 RIPng 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ripng** [*process-id*]，进入 RIPng 视图。

步骤 3 执行命令 **checkzero**，使能 RIPng 报文的零域检查。

----结束

检查配置结果

调整和优化 RIP 网络配置成功后，您可以查看到 RIPng 的路由信息、邻居信息及接口信息。

前提条件

完成上述配置后，请执行下面的命令检查配置结果。

操作步骤

- 使用 **display ripng** [*process-id*]命令查看 RIPng 进程的配置信息。
- 使用 **display ripng** *process-id* **database** [**verbose**]命令查看 RIPng 发布数据库中的路由。
- 使用 **display ripng** *process-id* **interface** [*interface-type interface-number*] [**verbose**]命令查看 RIPng 的接口信息。
- 使用 **display ripng** *process-id* **neighbor** [**verbose**]命令查看 RIPng 的邻居信息。
- 使用 **display ripng** *process-id* **route** 命令查看所有激活和非激活 RIPng 路由。

----结束

5.3.8 配置举例

介绍 RIPng 的各种组网举例。

配置 RIPng 对接收的路由进行过滤示例

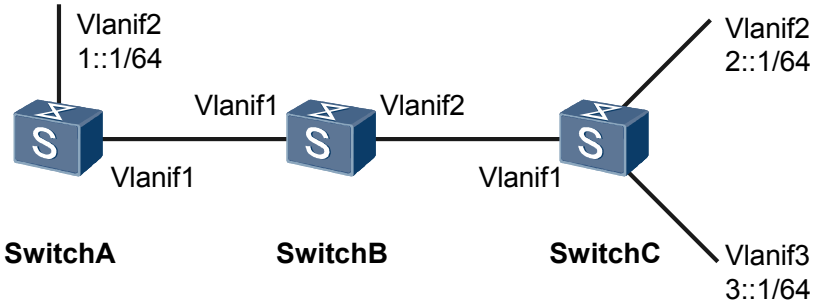
组网要求

如图 5-6 所示，图中所有 IPv6 地址的前缀长度都为 64，且相邻 Switch 之间使用 IPv6 链路本地地址连接。

版权所有 © 华为技术有限公司

要求所有 Switch 通过 RIPng 来学习网络中的 IPv6 路由信息，并且在 SwitchB 上对接收的 SwitchC 的路由（3::/64）进行过滤，使其不加入到 SwitchB 的路由表中，也不发布给 SwitchA。

图 5-6 配置 RIPng 对接收的路由进行过滤组网图



配置思路

采用如下的思路配置 RIPng 对接收的路由进行过滤：

1. 在各 Switch 上使能 RIPng 基本功能，使各 Switch 通。
2. 在 SwitchB 上配置 ACL，对接受的路由进行过滤。

数据准备

为完成此配置例，需准备如下的数据：

- 在各 Switch 上使能进程 RIPng1。
- SwitchB 上配置 ACL6 2000，拒绝接收来自 3::/64 网段的路由。

操作步骤

步骤 1 配置各接口的 IPv6 地址（略）

步骤 2 配置 RIPng 的基本功能

配置 SwitchA。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlanif 2
[SwitchA-Vlanif2] ripng 1 enable
[SwitchA-Vlanif2] quit
[SwitchA] interface vlanif 1
[SwitchA-Vlanif 1] ripng 1 enable
[SwitchA-Vlanif 1] quit
```

配置 SwitchB。

```
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlanif 1
[SwitchB-Vlanif1] ripng 1 enable
[SwitchB-Vlanif1] quit
[SwitchB] interface vlanif 2
[SwitchB-Vlanif2] ripng 1 enable
```


版权所有 © 华为技术有限公司

```
[SwitchB-Vlanif2] quit
```

配置 SwitchC。

```
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlanif 1
[SwitchC-Vlanif1] ripng 1 enable
[SwitchC-Vlanif1] quit
[SwitchC] interface vlanif 2
[SwitchC-Vlanif2] ripng 1 enable
[SwitchC-Vlanif2] quit
[SwitchC] interface vlanif 3
[SwitchC-Vlanif3] ripng 1 enable
[SwitchC-Vlanif3] quit
```

查看 SwitchB 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::F54C:0:9FDB:1  on Vlanif2
 Dest 2::/64,
     via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 3 Sec
 Dest 3::/64,
     via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 3 Sec
 Peer FE80::D472:0:3C23:1  on Vlanif1
 Dest 1::/64,
     via FE80::D472:0:3C23:1, cost  1, tag 0, A, 4 Sec
```

查看 SwitchA 的 RIPng 路由表。

```
[SwitchA] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::476:0:3624:1  on Vlanif1
 Dest 2::/64,
     via FE80::476:0:3624:1, cost  2, tag 0, A, 21 Sec
 Dest 3::/64,
     via FE80::476:0:3624:1, cost  2, tag 0, A, 21 Sec
```

步骤 3 配置 SwitchB 对接收的路由进行过滤

```
[SwitchB] acl ipv6 number 2000
[SwitchB-acl6-basic-2000] rule deny source 3:: 64
[SwitchB-acl6-basic-2000] rule permit
[SwitchB-acl6-basic-2000] quit
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy 2000 import
[SwitchB-ripng-1] quit
```

步骤 4 验证配置结果

查看 SwitchB RIPng 路由表中不再有 3::/64 网段的路由。

```
[SwitchB] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::F54C:0:9FDB:1  on Vlanif2
 Dest 2::/64,
     via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 14 Sec
 Peer FE80::D472:0:3C23:1  on Vlanif1
 Dest 1::/64,
     via FE80::D472:0:3C23:1, cost  1, tag 0, A, 25 Sec
[SwitchA] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::476:0:3624:1  on Vlanif1
 Dest 2::/64,
```


版权所有 © 华为技术有限公司

```
via FE80::476:0:3624:1, cost  2, tag 0, A, 7 Sec
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 ipv6
#
interface Vlanif1
ipv6 address auto link-local
 ripng 1 enable
#
interface Vlanif2
 ipv6 address 1::1/64
 ripng 1 enable
#
ripng 1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 ipv6
#
acl ipv6 number 2000
 rule 0 deny source 3::/64
 rule 1 permit
#
interface Vlanif1
 ipv6 address auto link-local
 ripng 1 enable
#
interface Vlanif2
 ipv6 address auto link-local
 ripng 1 enable
#
ripng 1
 filter-policy 2000 import
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 ipv6
#
interface Vlanif1
 ipv6 address auto link-local
 ripng 1 enable
#
interface Vlanif2
 ipv6 address 2::1/64
 ripng 1 enable
#
interface Vlanif3
 ipv6 address 3::1/64
 ripng 1 enable
#
ripng 1
#
return
```


版权所有 © 华为技术有限公司

5.4 OSPF 配置

OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议，广泛应用于接入网和城域网中。

5.4.1 OSPF 概述

OSPF 是一个基于链路状态的内部网关协议，目前针对 IPv4 协议使用的是 OSPFv2。

OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议。

说明

本章若没有特别说明，下文中所提到的 OSPF 均指 OSPFv2。

OSPF 的特性

OSPF 有以下几条重要的特点：

- 适应范围广——支持各种规模的网络，可支持几百台交换机。
- 快速收敛——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，交换机的链路状态数据库仅需和所在区域的其他交换机保持一致。链路状态数据库的减小大大降低了对交换机内存的占用和 CPU 的消耗。同时，需要在区域间传送的路由信息的减小，降低了网络带宽的占用。
- 等价路由——支持到同一目的地址的多条等价路由。
- 路由分级——使用 4 类不同的路由，按优先顺序分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证——支持基于区域和接口的报文验证，以保证报文交互的安全性。
- 组播发送——在某些类型的链路上以组播地址发送协议报文，减少对其他未使能 OSPF 设备的干扰。

OSPF 协议路由的计算过程

OSPF 协议路由的计算过程可简单描述如下：

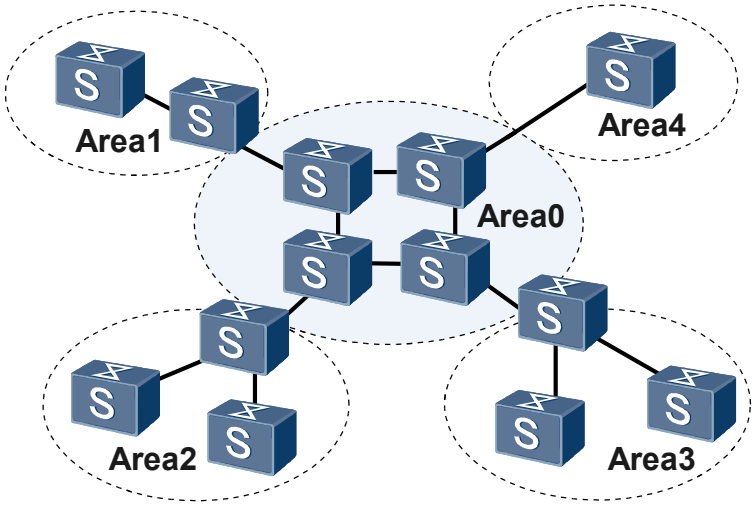
1. 每台 OSPF 设备根据自己周围的网络拓扑结构生成链路状态通告 LSA（Link State Advertisement），并通过更新报文将 LSA 发送给网络中的其它 OSPF 设备。
2. 每台 OSPF 设备都会收集其它交换机发来的 LSA，所有的 LSA 放在一起便组成了链路状态数据库 LSDB（Link State Database）。LSA 是对设备周围网络拓扑结构的描述，LSDB 则是对整个自治系统的网络拓扑结构的描述。
3. OSPF 设备将 LSDB 转换成一张带权的有向图，这张图便是对整个网络拓扑结构的真实反映。同一区域内各个设备得到的有向图是完全相同的。
4. 每台交换机根据有向图，使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。

版权所有 © 华为技术有限公司

OSPF 区域划分

随着网络规模日益扩大，交换机数量的增多会导致 LSDB 非常庞大，导致交换机负担很重。OSPF 协议通过将自治系统划分成不同的区域（Area）来解决上述问题。区域是从逻辑上将交换机划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是交换机，而不是链路。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。如图 5-7 所示。

图 5-7 OSPF 区域划分



划分区域后，可以在区域边界路由器上进行路由聚合，减少通告到其他区域的 LSA 数量。另外，还可以最小化由于网络拓扑变化带来的影响。

交换机的类型

OSPF 交换机根据在 AS 中的不同位置，可以分为以下四类：

- 区域内路由器（Internal Routers）

  该类交换机设备的所有接口都属于同一个 OSPF 区域。

- 区域边界路由器 ABR（Area Border Routers）

  该类交换机设备可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

- 骨干路由器（Backbone Routers）

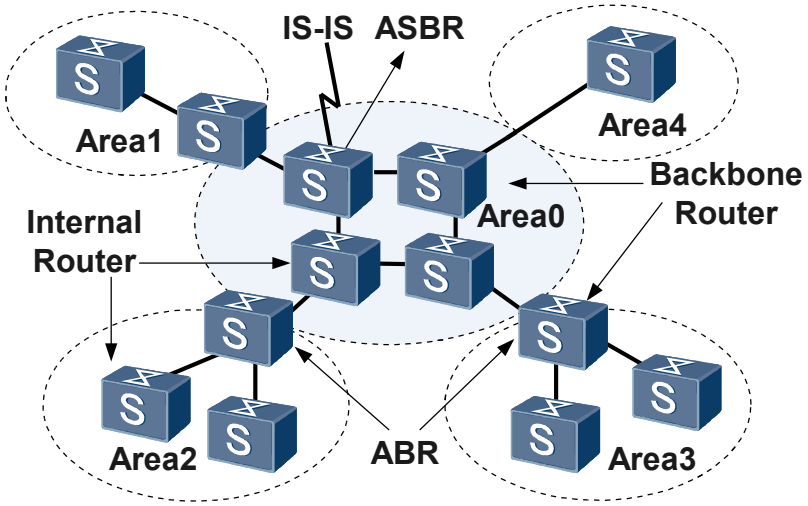
  该类交换机设备至少有一个接口属于骨干区域。因此，所有的 ABR 和位于 Area0 的内部节点都是骨干路由器。

- 自治系统边界路由器 ASBR（AS Boundary Routers）

  与其他 AS 交换路由信息的交换机设备称为 ASBR。ASBR 并不一定位于 AS 的边界，它可能是区域内路由器，也可能是 ABR。只要一台 OSPF 设备引入了外部路由的信息，它就成为 ASBR。

版权所有 © 华为技术有限公司

图 5-8 OSPF 交换机的类型



OSPF 的网络类型

OSPF 根据链路层协议类型将网络分为下列四种类型：

- 广播（Broadcast）类型：当链路层协议是 Gigabitethernet、FDDI 时，OSPF 缺省认为网络类型是 Broadcast。在该类型的网络中：
  - 以组播形式（224.0.0.5：含义是 OSPF 交换机的预留 IP 组播地址）发送 Hello 报文及所有源自 DR 的报文；
  - 以组播形式（224.0.0.6：含义是 OSPF DR 的预留 IP 组播地址）发送 LSU 报文，进而 DR 将该 LSU 报文发送到 224.0.0.5；
  - 以单播形式发送 DD 报文、LSR 报文和所有重传报文；
  - 正常情况下，以组播形式（224.0.0.5）发送 LSAck 报文。当交换机收到重复的 LSA 或达到最大生存时间的 LSA 被删除时，LSAck 以单播形式发送。
- NBMA（Non-Broadcast Multi-Access）类型：当链路层协议是帧中继、ATM 或 X.25 时，OSPF 缺省认为网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文（Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文）。
- 点到多点 P2MP（point-to-multipoint）类型：P2MP 类型是由其他的网络类型强制更改的。在该类型的网络中，以组播形式（224.0.0.5）发送 Hello 报文，以单播形式发送 DD 报文、LSR 报文、LSU 报文、LSAck 报文。
- 点到点 P2P（point-to-point）类型：当链路层协议是 PPP、HDLC 和 LAPB 时，OSPF 缺省认为网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文（Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文）。

5.4.2 AC6605 中支持的 OSPF 特性

AC6605 中支持的 OSPF 特性包括：多进程、验证、热备份、Smart-Discover、VPN 多实例、BFD。

版权所有 © 华为技术有限公司

多进程

OSPF 支持多进程，在同一台交换机上可以运行多个不同的 OSPF 进程，它们之间互不影响，彼此独立。不同 OSPF 进程之间的路由交互相当于不同路由协议之间的路由交互。

交换机的一个接口只能属于某一个 OSPF 进程。

OSPF 多进程的一个典型应用就是在 VPN 场景中 PE 和 CE 之间运行 OSPF 协议，同时 VPN 骨干网上的 IGP 也采用 OSPF。在 PE 上，这两个 OSPF 进程互不影响。

验证功能

OSPF 支持报文验证功能，只有通过验证的 OSPF 报文才能接收，否则将不能正常建立邻居。AC6605 支持两种验证方式：

- 区域验证方式
- 接口验证方式

当两种验证方式都存在时，优先使用接口验证方式。

OSPF 热备份

分布式结构的交换机支持 OSPF 热备份（Hot Standby，HSB）特性。OSPF 将会把主用主控板 AMB（Active Main Board）上必要的信息备份到备用主控板 SMB（Standby Main Board）上。当 AMB 发生故障时，SMB 将会取代它的功能，使 OSPF 可以不受任何影响地正常运行。

OSPF 支持两种不同热备份方式：

- 备份所有 OSPF 数据，一旦发生 AMB 和 SMB 切换，OSPF 能够马上恢复正常运行。
- 只备份 OSPF 配置信息，发生 AMB 和 SMB 切换时，OSPF 进行 Graceful Restart（GR），从邻居那里获得邻接关系，并对 LSDB 进行同步。

Smart-discover

通常情况下，交换机会周期性地从运行 OSPF 协议的接口上发送 Hello 报文。通过 Hello 报文，交换机之间可以建立和维持邻居关系，并且选举出该多址网络（广播型或 NBMA）上的 DR、BDR。当建立邻居关系或者选举多址网络上的 DR、BDR 时，接口每次都需要等到 Hello 定时器到时才能发送 Hello 报文，从而影响了建立邻居关系和选举 DR、BDR 的速度。

说明

- 接口发送 Hello 报文的时间间隔取决于在接口上配置的发送 Hello 报文的时间间隔。
- Hello 报文时间间隔的缺省值因网络类型而异。

通过 Smart-discover 功能，可以解决以上问题：

- 在广播型和 NBMA 网络中，快速的建立起邻居关系和选举出该网络上的 DR、BDR。

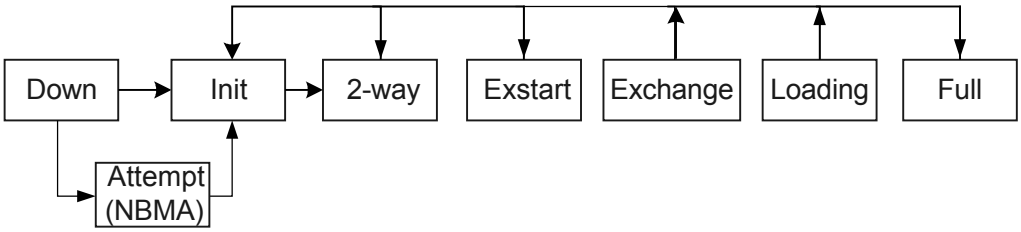
  当邻居状态首次到达 2-way 状态，或者由 2-way 及更高状态回到 Init 状态时，如图 5-9 所示，使能了 Smart-discover 功能的接口一旦收到邻居的 Hello 报文，发现邻居

版权所有 © 华为技术有限公司

状态发生了变化后，会立刻主动的向邻居发送 Hello 报文，而不必等到 Hello 定时器到时再发送。

该多址网络上的 DR、BDR 的接口状态发生变化时，使能了 Smart-discover 功能的接口会主动在该网段发送 Hello 报文，参与到 DR 或者 BDR 的选举中。

图 5-9 邻居状态机的变化



- 在 P2P 或 P2MP 网络中，快速的建立起邻接关系，其原理同广播型和 NBMA 网络。

OSPF VPN 多实例

OSPF 支持多实例，可以运行在 VPN 网络中的 PE-CE 之间。

在 BGP MPLS VPN 网络中，属于同一个 VPN 的多个 Site 可以使用 OSPF 作为内部路由协议。然而，它们会被看作属于不同的自治系统来处理。这样，在一个节点学到的 OSPF 路由，将被作为外部路由传送给另一节点。这种处理方式导致了比较高的 OSPF 路由协议流量，并带来了一些原本可以避免的网络管理问题。

在 AC6605 的实现中，可以在 PE 上通过配置域 ID 来区分 Site 所在的 VPN。属于同一个 VPN 的不同 Site 之间彼此看做是直接相连的。这样，PE 交换机之间交换 OSPF 路由信息时就好象是通过一条专线相连，改善了网络管理并使 OSPF 的应用更为有效。

BFD for OSPF

缺省情况下，在广播网络中，OSPF 发送 Hello 报文的时间间隔为 10 秒钟；在 NBMA 网络中，发送 Hello 报文的时间间隔为 30 秒钟。并且，宣告邻居 Down 掉的时间即相邻交换机失效的时间一般配置为 Hello 报文间隔的 4 倍。若在相邻交换机失效时间内没有收到邻居发来的 Hello 报文，将会删除邻居。即交换机感知到邻居故障的时间最短也是秒级。在高速的网络环境中，这将导致报文大量丢失。

双向转发检测 BFD（Bidirectional Forwarding Detection）就是为解决现有检测机制的不足而产生的。通过配置 BFD 可以设置毫秒级的时间检测间隔。使用 BFD 并不是代替 OSPF 协议本身的 Hello 机制，只是配合 OSPF 协议更快的发现邻接方面出现的故障，并及时通知 OSPF 重新计算相关路由以便正确指导报文的转发。

路由管理模块 RM（Routing Management Module）为 OSPF 提供与 BFD 模块交互的相关服务。OSPF 通过 RM 通知 BFD 来动态创建或删除 BFD session，同时 BFD 的事件消息也通过 RM 传递给 OSPF。

BFD 会话建立与删除的过程如下：

- 创建 BFD 会话的过程：配置了全局 BFD 功能，并使能接口或者进程的 BFD 特性，且 OSPF 邻居的状态为 Full，当满足以上条件时，OSPF 将通过 RM 模块通知 BFD 模块自动建立 BFD 会话并协商 BFD 的相关参数。

版权所有 © 华为技术有限公司

- 删除 BFD 会话的过程：当 BFD 检测到链路发生故障时，BFD 产生 Down 事件通过 RM 模块通知上层协议，此时 OSPF 响应这个事件并马上取消该链路上的邻接关系。这时邻居状态不再为 Full，因为不满足 BFD 会话建立的条件，所以 OSPF 通过 RM 模块通知 BFD 模块删除该 BFD 会话

OSPF 支持在 Broadcast、P2P、P2MP 和 NBMA 链路上动态的创建/删除 BFD 会话。

请根据网络环境配置 BFD，如果时间参数设置不正确将会导致网络震荡。

OSPF-BGP 联动

如果有新的交换机加入到网络中或者交换机重启时，可能会出现在 BGP 收敛期间内网络流量丢失的现象。这是由于 IGP 收敛速度比 BGP 快而造成的。

在存在备份链路的情况下，OSPF-BGP 联动特性可以使得重启交换机或者新加入的交换机在 BGP-OSPF 联动期间启动 stub Router 定时器，在设定的联动时间内保持为 stub 交换机的形式（通过增大该交换机所生成的 LSA 中的链路的度量值到 65535），从而告知其它 OSPF 交换机不要使用这个 Stub 交换机来转发数据。由此确保该交换机不会被用作穿越交换机，从而避免了 BGP 在链路回切时因为其路由收敛速度滞后于 OSPF 路由收敛速度而造成的流量丢失现象。

5.4.3 配置 OSPF 的基本功能

只有配置了基本功能，才可组建 OSPF 网络。

建立配置任务

在接口视图下配置的 OSPF 命令不受 OSPF 是否使能的限制。在关闭 OSPF 后，原来在接口下配置的相关命令仍然存在。

应用环境

在 OSPF 的各项配置任务中，必须先启动 OSPF、指定运行 OSPF 的进程与区域号后，才能配置其它的功能特性。

说明

在同一区域内配置多台交换机时，大多数的配置数据（如定时器、过滤、聚合等）都应该以区域为单位进行统一规划。错误的配置可能会导致相邻交换机之间无法相互传递信息，甚至导致路由信息的阻塞或者自环。

前置任务

在配置 OSPF 的基本功能之前，需完成以下任务：

- 配置链路层协议。
- 配置接口的网络层地址，使各相邻节点网络层可达。

数据准备

在配置 OSPF 的基本功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	交换机的 Switch ID
2	OSPF 进程号
3	如果配置了 OSPF 多实例，需准备 VPN 实例名
4	接口所属的区域编号
5	接口所在网段的 IP 地址

启动 OSPF 并进入 OSPF 视图

创建 OSPF 进程是配置所有 OSPF 特性的首要步骤。通过创建 OSPF 进程，还可以手工指定交换机的 Switch ID。

背景信息

为保证 OSPF 运行的稳定性，在进行网络规划时应该确定交换机 ID 的划分并手工配置。手工配置交换机的 ID 时，必须保证自治系统中任意两台交换机的 ID 都不相同。通常的做法是将交换机的 ID 配置为与该交换机某个接口的 IP 地址一致。

AC6605 支持 OSPF 多进程，当在一台交换机上启动多个 OSPF 进程时，需要指定不同的进程号。OSPF 进程号是本地概念，不影响与其它交换机之间的报文交换。因此，不同的交换机之间，即使进程号不同也可以进行报文交换。

请在需要运行 OSPF 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id* | **router-id** *router-id*]，启动 OSPF 进程，进入 OSPF 视图。

AC6605 支持 OSPF 多实例，可以配置 OSPF 在 VPN 实例中运行，此时需执行命令 **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *。如果指定了 VPN 实例，那么此 OSPF 进程属于指定的 VPN 实例，如果未指定则属于全局实例。

说明

每个 OSPF 进程的 Router ID 要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。建议在 OSPF 设备上单独为每个 OSPF 进程配置全网唯一的 Router ID。

----结束

配置区域所包含的网段

OSPF 协议通过将自治系统划分成不同的区域，和区域中指定运行 OSPF 协议的接口和接口所属的区域，达到在自治区域中发现并计算路由的目的。

背景信息

一个网段只能属于一个区域，或者说每个运行 OSPF 协议的接口必须指明属于某一个特定的区域。该处的网段是指运行 OSPF 协议接口的 IP 地址所在的网段。

版权所有 © 华为技术有限公司

请在需要运行 OSPF 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **network** *ip-address wildcard-mask* [**description** *text*]，配置区域所包含的网段。其中，**description** 字段用来为 OSPF 指定网段配置描述信息。

满足下面两个条件，接口上才能正常运行 OSPF 协议：

- 接口的 IP 地址掩码长度≥**network** 命令指定的掩码长度。
- 接口的主 IP 地址必须在 **network** 命令指定的网段范围内。

缺省情况下，OSPF 以 32 位主机路由的方式对外发布 Loopback 接口的 IP 地址，与 Loopback 接口上配置的掩码长度无关。如果要发布 Loopback 接口的网段路由，需要在接口下配置网络类型为 NBMA 或广播型。请参考**配置 OSPF 接口上网络类型**。

----结束

检查配置结果

OSPF 基本功能配置成功后，您可以查看到统计信息、LSDB 和各区域邻居的信息。

前提条件

已经完成 OSPF 基本功能的所有配置。

操作步骤

- 使用 **display ospf** [*process-id*] **cumulative** 命令查看 OSPF 统计信息。
- 使用 **display ospf** [*process-id*] **lsdb** 命令查看 OSPF 的 LSDB 信息。
- 使用 **display ospf** [*process-id*] **peer** 命令查看 OSPF 邻接点的信息。
- 使用 **display ospf** [*process-id*] **routing** 命令查看 OSPF 路由表的信息。

----结束

任务示例

如果 OSPF 邻居正常建立，执行命令 **display ospf peer**，可以看到 OSPF 邻居的状态为 Full。

```
<Quidway> display ospf peer
         OSPF Process 1 with Router ID 10.1.1.2
                  Neighbors
 Area 0.0.0.0 interface 10.1.1.2(Vlanif10)'s neighbors
 Router ID: 10.1.1.1          Address: 10.1.1.1
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.1.1.1  BDR: None   MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:05
   Authentication Sequence: [ 0 ]
```


版权所有 © 华为技术有限公司

5.4.4 建立或维持 OSPF 邻居或邻接关系

OSPF 网络中，所有路由信息都在邻居或邻接中传递、交换。通过维持邻居或邻接关系，对整网的稳定性起着重要作用。

建立配置任务

在接口上配置的各种参数要和邻接交换机的参数要保持一致。

应用环境

在实际应用中，建立或维持 OSPF 邻居关系是组建 OSPF 网络的重要前提，通过本节的配置，你可以：

- 通过改变 OSPF 报文的定时器，可以调整 OSPF 网络的收敛速度以及协议报文带来的网络负荷。
- 通过配置 OSPF 重传限制 RL-OSPF（Retransmission Limitation for OSPF）可以实现在 OSPF 重传报文时，如果超过了设定的重传次数，OSPF 将断开邻居，避免在邻居收不到报文的情况下，一直重传造成的死循环。
- 在以下两种组网环境中，通过对 LSA 更新和接收时间的合理配置，可以加快网络中路由的收敛速度。
  - 网络相对稳定、对路由收敛时间要求较高的组网环境：指定 LSA 更新或接收时间间隔为 0，使得拓扑或者路由的变化可以立即通过 LSA 发布到网络中，或者拓扑、路由的变化能够立即被感知，从而加快网络中路由的收敛速度。
  - 网络连接或者路由频繁动荡的组网环境：配置合理的 LSA 更新或接收的时间间隔或者使能智能定时器 intelligent-timer，可抑制大量的 LSA 被更新或接收，避免 OSPF 占用过多网络带宽和交换机资源。

前置任务

在建立或维持 OSPF 邻居或邻接关系之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在建立或维持 OSPF 邻居或邻接关系之前，需要准备以下数据。

序号	数据
1	运行 OSPF 协议的接口编号
2	发送 Hello 和 Dead 报文的时间间隔
3	OSPF 的最大重传次数
4	LSA 的时间间隔
5	泛洪更新 LSA 的数量或时间间隔

版权所有 © 华为技术有限公司

配置接口发送 Hello 报文的时间间隔

通过调整 OSPF 邻居之间的 Hello 定时器的时间间隔，可以改变邻居建立的速度，从而影响网络收敛的速度。

背景信息

OSPF 邻居之间的 Hello 定时器的时间间隔要保持一致。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf timer hello** *interval*，配置接口发送 Hello 报文的时间间隔。

缺省情况下，交换机的 P2P、Broadcast 类型接口发送 Hello 报文的时间间隔的值为 10 秒，P2MP、NBMA 类型接口发送 Hello 报文的时间间隔的值为 30 秒。

hello interval 的值越小，发现网络拓扑改变的速度越快，网络的带宽开销也就越大。 接口和邻居交换机上相连接口的 hello interval 参数值要保持一致。

----结束

配置相邻交换机失效的时间

在相邻交换机失效时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf timer dead** *interval*，设置相邻交换机失效的时间。

OSPF 邻居的失效时间是指：在该时间间隔内，若未收到邻居发送的 Hello 报文，就认为该邻居已失效。缺省情况下，交换机的 P2P、Broadcast 类型接口的 OSPF 邻居失效时间为 40 秒，P2MP、NBMA 类型接口的 OSPF 邻居失效时间为 120 秒。

缺省情况下，在同一接口上失效时间是 Hello 间隔时间的 4 倍。

说明

建议配置的实效时间大于 20 秒。如果失效的时间小于 20 秒，可能会造成邻居会话的中断。

----结束

版权所有 © 华为技术有限公司

配置 OSPF 报文重传限制

通过限制重传 DD 报文、Update 报文和 Request 报文的次数，在达到指定的次数后断开邻居。

背景信息

OSPF 报文重传机制，主要针对三种报文：DD 报文、Update 报文和 Request 报文，当这三种报文收不到相应的回馈报文时，使能此特性，限制报文重传的次数，并在达到指定的次数后断开邻居。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **retransmission-limit** [*max-number*]，配置 OSPF 重传限制功能。

缺省情况下，不使能此功能。

----结束

配置 LSA 的时间间隔

可以根据现网中网络连接和交换机资源的情况，配置 LSA 的时间间隔。

背景信息

OSPF 协议规定 LSA 的更新时间间隔 5 秒，是为了防止网络连接或者路由频繁动荡引起的过多占用网络带宽和交换机资源。

在网络相对稳定、对路由收敛时间要求较高的组网环境中，可以指定 LSA 的更新时间间隔为 0 来取消 LSA 的更新时间间隔，使得拓扑或者路由的变化可以立即通过 LSA 发布到网络中，从而加快网络中路由的收敛速度。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

- 配置 LSA 的更新时间间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **lsa-originate-interval** { **0** | **intelligent-timer** *max-interval start-interval hold-interval* [**other-type** *interval*] | **other-type** *interval* [**intelligent-timer** *max-interval start-interval hold-interval*] }，配置 LSA 的更新时间间隔。

     缺省情况下，使能智能定时器 intelligent-timer，更新 LSA 的最长间隔时间为 5000 毫秒、初始间隔时间为 500 毫秒、基数间隔时间为 1000 毫秒（以毫秒为单位的时间间隔）。使能智能定时器后，更新 LSA 的时间间隔的如下所示：

     a. 初次更新 LSA 的间隔时间由 *start-interval* 参数指定。

版权所有 © 华为技术有限公司

b. 第 n（n≥2）次更新 LSA 的间隔时间为 *hold-interval*×2(n-1)。

c. 当 *hold-interval*×2(n-1)达到指定的最长间隔时间 *max-interval* 时，OSPF 连续三次更新 LSA 的时间间隔都是最长间隔时间，之后，再次返回步骤 3.1，按照初始间隔时间 *start-interval* 更新 LSA。

- 配置 LSA 被接收的时间间隔

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
3. 执行命令 **lsa-arrival-interval** { *interval* | **intelligent-timer** *max-interval start-interval hold-interval* }，配置 LSA 被接收的时间间隔。

   在网络相对稳定、对路由收敛时间要求较高的组网环境中，可以指定 LSA 被接收的时间间隔为 0，使得拓扑或者路由的变化能够立即被感知到。

   缺省情况下，使能智能定时器 intelligent-timer，接收 LSA 的最长间隔时间为 1000 毫秒、初始间隔时间为 500 毫秒、基数间隔时间为 500 毫秒（以毫秒为单位的时间间隔）。使能智能定时器后：

   a. 初次接收 LSA 的间隔时间由 *start-interval* 参数指定。

   b. 第 n（n≥2）次接收 LSA 的间隔时间为 *hold-interval*×2(n-1)。

   c. 当 *hold-interval*×2(n-1)达到指定的最长间隔时间 *max-interval* 时，OSPF 连续三次接收 LSA 的时间间隔都是最长间隔时间，之后，再次返回步骤 3.1，按照初始间隔时间 *start-interval* 接收 LSA。

----结束

检查配置结果

OSPF 邻居或邻接关系稳定后，您可以查看到统计信息和各区域邻居的信息。

前提条件

已经完成建立或维持 OSPF 邻居或邻接关系功能的所有配置。

操作步骤

- 使用 **display ospf** [*process-id*] **brief** 命令查看 OSPF 的概要信息。
- 使用 **display ospf** [*process-id*] **peer** 命令查看 OSPF 邻接点的信息。
- 使用 **display ospf** [*process-id*] **cumulative** 命令查看 OSPF 统计信息。

----结束

5.4.5 配置 OSPF 的 STUB 区域

通过将位于 AS 边缘的一些非骨干区域配置成 STUB，可以缩减其路由表规模，减少需要传递的路由信息数量。

建立配置任务

STUB 区域是一种可选的配置属性，但并不是每个区域都符合配置的条件。通常来说，STUB 区域位于自治系统的边界，是那些只有一个 ABR 的非骨干区域。

版权所有 © 华为技术有限公司

应用环境

OSPF 划分区域后，可以减少网络中 LSA 的数量，OSPF 的扩展性也得以增强。对于位于 AS 边缘的一些非骨干区域，为了更多的缩减其路由表规模和降低 LSA 的数量，可以将它们配置为 STUB 区域。

本节将介绍 STUB 区域的配置过程。

前置任务

在配置 OSPF 的 STUB 区域之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在配置 OSPF 的 STUB 区域之前，需要准备以下数据。

序号	数据
1	发送到 STUB 区域缺省路由的开销值

配置当前区域为 Stub 区域

Stub 区域是一种特定的区域，Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，LSA 的数量大大减少。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **stub** [**no-summary**]，配置当前区域为 Stub 区域。

stub 命令只有当在 ABR 上配置时，可选参数 **no-summary** 才能对该区域起作用。

所有连接到 Stub 区域的交换机必须使用 **stub** 命令将该区域配置成 Stub 属性。

----结束

配置发送到 Stub 区域缺省路由的开销

在连接到 Stub 区域的边界路由器上配置发送到 Stub 区域的缺省路由开销。

版权所有 © 华为技术有限公司

背景信息

缺省情况下，发送到 Stub 区域的缺省路由的开销为 1。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **stub** [**no-summary**]，配置当前区域为 Stub 区域。

步骤 5 执行命令 **default-cost** *cost*，配置发送到 Stub 区域缺省路由的开销。

本命令只适用于连接到 Stub 或 NSSA 区域的边界路由器（ABR）。

----结束

检查配置结果

OSPF 的 Stub 区域配置成功后，您可以查看到 LSDB 和 OSPF 路由表信息。

前提条件

已经完成 OSPF 的 STUB 区域的所有配置。

操作步骤

- 使用以下命令查看 OSPF 的 LSDB 信息：
  - **display ospf** [*process-id*] **lsdb** [**brief**]
  - **display ospf** [*process-id*] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [*link-state-id*] [**originate-router** [*advertising-router-id*] | **self-originate**]
- 使用以下命令查看 OSPF 路由表的信息：
  - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
  - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- 使用 **display ospf** [*process-id*] **abr-asbr** [*router-id*]命令查看 OSPF ABR 及 ASBR 信息。

----结束

5.4.6 配置 OSPF 的 NSSA 区域

通过将非骨干区域配置成 NSSA 区域，可以允许引入外部路由，同时增加一类新的 LSA，Type7 NSSA-LSA。

版权所有 © 华为技术有限公司

建立配置任务

NSSA 区域不允许存在 5 类 LSA。Type7 LSA 由 NSSA 的 ASBR 产生，仅在本 NSSA 内传播。

应用环境

Stub 区域不能引入外部路由，为此又产生了 NSSA 区域的概念。NSSA 区域中允许 Type7 LSA 的传播。Type7 LSA 由 NSSA 区域的 ASBR 产生，当 P-bit 被置位且 Forwarding Address 字段不为空的 Tpye7 LSA 到达 NSSA 中负责将 7 类 LSA 转换为 5 类 LSA 的 ABR 时，就会转换成 AS-External LSA，并通告到其他区域。

本节将介绍 NSSA 区域的配置过程。

前置任务

在配置 OSPF 的 NSSA 区域之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在配置 OSPF 的 NSSA 区域之前，需要准备以下数据。

序号	数据
1	发送到 NSSA 区域缺省路由的开销值

配置当前区域为 NSSA 区域

NSSA 区域是 Stub 区域的一种变形，该区域允许自治系统外部路由的引入，由 ASBR 发布 Type 7 LSA 通告给本区域。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **nssa** [**default-route-advertise** | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding**] *，配置一个区域为 NSSA 区域。

所有连接到 NSSA 区域的交换机必须使用 **nssa** 命令将该区域配置成 NSSA 属性。

版权所有 © 华为技术有限公司

配置或取消 NSSA 属性，可能会触发区域更新。只有在上一次区域更新完成后，才能进行再次配置或取消配置操作。

nssa 命令的参数只有配置在特定交换机上时，才有实际意思。

flush-waiting-timer 用来产生老化时间被置为最大值 3600 秒的 Type-5 LSA，以达到及时清除其他交换机上已经没用的 Type-5 LSA 的目的。当 ASBR 同时还是 ABR 时，**flush-waiting-timer** 功能不会生效。命令不能生效的目的是为了防止删除非 NSSA 区域的 Type-5 LSA。

----结束

配置发送到 NSSA 区域缺省路由的开销

在连接到 NSSA 区域的边界路由器上配置发送到 NSSA 区域的缺省路由开销。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **nssa** [**default-route-advertise** | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding**] *，配置 NSSA 区域。

所有连接到 NSSA 区域的交换机必须使用 **nssa** 命令将该区域配置成 NSSA 属性。

nssa 命令只有当在 ABR 上配置时，后面的可选参数才有效。

步骤 5 执行命令 **default-cost** *cost*，配置发送到 NSSA 区域缺省的 Type-3 路由的开销。

该命令只有在 ABR 上配置时才有效。

----结束

检查配置结果

OSPF 的 NSSA 区域配置成功后，您可以查看到 LSDB 和 OSPF 路由表信息。

前提条件

已经完成 OSPF 的 NSSA 区域的所有配置。

操作步骤

- 使用以下命令查看 OSPF 的 LSDB 信息：
  - **display ospf** [*process-id*] **lsdb** [**brief**]

版权所有 © 华为技术有限公司

- **display ospf** [*process-id*] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [*link-state-id*] [**originate-router** [*advertising-router-id*] | **self-originate**]

- 使用以下命令查看 OSPF 的路由表信息：
  - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
  - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- 使用 **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]命令查看 OSPF 的接口信息。

----结束

5.4.7 配置 OSPF 在不同网络类型中的属性

通过配置 OSPF 接口的网络类型和调整属性，可以灵活组建 OSPF 网络。

建立配置任务

OSPF 协议不支持在 NULL 接口上的配置网络类型。

应用环境

OSPF 根据链路层协议类型将网络分为四种不同的类型。由于 NBMA 网络必须是全连通的，所以网络中任意两台交换机之间都必须直接可达。但在很多情况下，这个要求无法满足，这时就需要通过命令强制改变网络的类型。

在 P2MP 网络上，掩码长度不一致的设备不可以建立邻居关系，通过配置，可以允许设备间忽略对 Hello 报文中网络掩码的检查，从而可以正常建立 OSPF 邻居关系。

对于 NBMA 网络，如果部分交换机之间没有直接可达的链路时，应将接口配置成 P2MP 方式。如果交换机在 NBMA 网络中只有一个对端，也可将接口类型改为 P2P 方式。

另外，在配置广播网和 NBMA 网络时，还可以指定各接口的 DR 优先级，以此来影响网络中的 DR/BDR 选择。一般情况下，应该选择性能和可靠性较高的交换机来作为 DR 和 BDR。

前置任务

在配置 OSPF 在不同网络类型中的属性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在配置 OSPF 在不同网络类型中的属性之前，需要准备以下数据。

序号	数据
1	运行 OSPF 的接口编号
2	要使用的网络类型

版权所有 © 华为技术有限公司

序号	数据
3	接口的 DR 优先级
4	NBMA 网络邻居的 IP 地址
5	NBMA 网络发送轮询报文的时间间隔

配置 OSPF 接口上网络类型

OSPF 根据链路层协议类型将网络分为四种不同的类型。通过配置接口的网络类型，可以强制改变接口的网络类型。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }，配置 OSPF 接口的网络类型。

当用户为接口配置了新的网络类型后，原接口的网络类型将被替换。

说明

一般情况下，链路两端的 OSPF 接口的网络类型必须一致，否则双方不可以建立起邻居关系。当且仅当链路两端的 OSPF 接口的网络类型一端是广播网而另一端是 P2P 时，双方仍可以正常的建立起邻居关系，并且网络类型为广播网的接口可以学到正确的 OSPF 路由信息，但是 P2P 端学不到对端的 OSPF 路由信息。

----结束

配置 OSPF 接口的 DR 优先级

当网络类型为广播网或 NBMA 类型时，可以通过配置接口的 DR 优先级来影响网络中 DR/BDR 的选择。

背景信息

当网络类型为广播网或 NBMA 类型时，可以通过配置接口的 DR 优先级来影响网络中 DR/BDR 的选择。数值越大，优先级越高。

缺省情况下，接口的 DR 优先级值为 1。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf dr-priority** *priority*，设置 OSPF 接口的 DR 优先级。

----结束

后续处理

改变优先级后，可以利用下面两种方法重新进行 DR/BDR 的选择，但是这会导致交换机之间的 OSPF 邻接关系中断，一般情况下不推荐使用。

- 重启所有交换机。
- 在建立了 OSPF 邻居的接口上配置 **shutdown**/**undo shutdown** 命令。

配置 NBMA 网络的邻居

网络类型为 NBMA 的接口，无法通过广播 Hello 报文的形式发现相邻交换机，必须手工为该接口指定相邻交换机的 IP 地址，以及该相邻交换机是否有选举权。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **peer** *ip-address* [**dr-priority** *priority*]，配置 NBMA 网络的邻居。

----结束

配置 NBMA 网络中发送轮询报文的时间间隔

在 NBMA 网络上，当邻居失效后，交换机将按设置的轮询时间间隔定期地发送 Hello 报文。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf timer poll** *interval*，在 NBMA 接口上配置发送轮询报文的时间间隔。

----结束

版权所有 © 华为技术有限公司

检查配置结果

OSPF 在不同网络类型中的属性配置成功后，您可以查看到统计信息、LSDB、邻居和接口信息。

前提条件

已经完成 OSPF 在不同网络类型中的属性的所有配置。

操作步骤

- 使用以下命令查看 OSPF 的 LSDB 信息：
  - **display ospf** [*process-id*] **lsdb** [**brief**]
  - **display ospf** [*process-id*] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [*link-state-id*] [**originate-router** [*advertising-router-id*] | **self-originate**]
- 使用 **display ospf** [*process-id*] **peer** [[*interface-type interface-number*] *neighbor-id* | **brief** | **last-nbr-down**]命令查看 OSPF 的邻接点信息。
- 使用 **display ospf** [*process-id*] **nexthop** 查看 OSPF 的下一跳信息。
- 使用以下命令查看 OSPF 的路由表信息：
  - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
  - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- 使用 **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]查看 OSPF 的接口信息。

----结束

任务示例

执行命令 **display ospf interface**，可以看到 OSPF 的接口类型和接口的交换机优先级（用于 DR 选择）。

```
<Quidway> display ospf interface vlanif 10
          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces
 Interface: 11.1.1.1 (Vlanif10)
 Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
Priority: 1
 Designated Router: 11.1.1.2
 Backup Designated Router: 11.1.1.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

5.4.8 配置 OSPF 的路由属性

通过配置 OSPF 的路由属性改变 OSPF 的选路策略，以满足复杂网络环境中的需要。

建立配置任务

在配置 OSPF 路由属性前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用背景

在实际应用中，可以通过配置 OSPF 的路由属性改变 OSPF 的选路策略，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 设置 OSPF 接口的开销值；
- 当多个路由协议发现相同的路由时，通过配置 OSPF 的协议优先级来改变路由协议的优先顺序；
- 使用多条等价路由进行负载分担。

前置任务

在配置 OSPF 的路由属性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在配置 OSPF 的路由属性之前，需要准备以下数据。

序号	数据
1	链路开销
2	OSPF 的优先级
3	最大等价路由条数

配置 OSPF 的链路开销

OSPF 会根据该接口的带宽自动计算其链路开销值，但也可以通过命令配置。

背景信息

配置 OSPF 的链路开销可以通过配置 OSPF 接口的开销值直接实现。

如果没有直接配置 OSPF 接口的开销值，OSPF 会根据该接口的带宽自动计算其开销值。计算公式为：接口开销=带宽参考值/接口带宽，取计算结果的整数部分作为接口开销值（当结果小于 1 时取 1）。通过改变带宽参考值可以间接改变接口的开销值。

缺省情况下，没有配置 OSPF 接口的开销值，OSPF 进程的带宽参考值为 100，从而不同带宽的接口可以根据公式计算出不同的开销值。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

- 配置 OSPF 接口的开销值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

3. 执行命令 **ospf cost** *cost*，设置 OSPF 接口的开销值。

- 配置带宽参考值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **bandwidth-reference** *value*，配置带宽参考值。

     在配置带宽参考值时请注意，必须保证该进程中所有交换机的带宽参考值一致。

----结束

配置 OSPF 的优先级

当多个路由协议发现相同的路由时，通过配置 OSPF 的协议优先级来改变路由协议的优先顺序。

背景信息

由于交换机上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级。在不同协议发现同一条路由时，优先级高的路由将被优选。

在 OSPF 算出等价路由后，配置 **nexthop** 命令可以从这些等价路由中选出优先级别高的作为下一跳。weight 值越小，路由优先级越高。weight 的缺省值是 255，表示等价路由间进行负载分担，不区分优先级。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

- 配置 OSPF 的协议优先级
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **preference** [**ase**] { *preference* | **route-policy** *route-policy-name* } *，配置 OSPF 协议的优先级。
- 配置 OSPF 等价路由的优先级
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **nexthop** *ip-address* **weight** *value*，配置 OSPF 的负载分担优先级。

----结束

配置 OSPF 最大等价路由条数

可以分别设置区域内、区域间和区域外部分别支持的路由最大数目。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **maximum load-balancing** *number*，配置最大等价路由条数。

说明

不同的产品，不同协议，等价路由数量的取值范围和缺省值可能会不同，具体取值可以通过购买许可证文件来调整。

----结束

检查配置结果

调整 OSPF 的路由属性后，您可以查看到 OSPF 路由表、接口和下一跳路由信息。

前提条件

已经完成 OSPF 路由属性的所有配置。

操作步骤

- 使用 **display ospf** [*process-id*] **routing** [[*ip-address* [*mask* | *mask-length*] | **interface** *interface-type interface-number* | **nexthop** *nexthop-address*] | **router-id** [*router-id*]]命令查看 OSPF 的路由表信息。
- 使用 **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]命令查看 OSPF 的接口信息。

----结束

任务示例

执行命令 **display ospf** [*process-id*] **routing** *ip-address*，可以看到路由的收敛优先级。

```
<Quidway> display ospf routing 100.1.1.1

         OSPF Process 1 with Router ID 1.1.1.1

 Destination : 100.1.1.0/24
 AdverRouter : 100.1.1.2              Area       : 0.0.0.0
 Cost        : 1                      Type       : Transit
 NextHop     : 100.1.1.2              Interface  : Vlanif10
```

5.4.9 控制 OSPF 的路由信息

控制 OSPF 的路由信息的发布与接收，并引入其他协议的路由。

建立配置任务

在控制 OSPF 的路由信息前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

通过本节的配置，可以控制 OSPF 的路由信息的发布与接收，并引入其他协议的路由。

版权所有 © 华为技术有限公司

前置任务

在控制 OSPF 路由信息之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在控制 OSPF 路由信息之前，需要准备以下数据。

序号	数据
1	链路开销
2	如果对路由信息进行过滤，则需要对应的过滤列表
3	要引入的路由协议名称和进程号、缺省值

配置 OSPF 路由聚合

AS 被划分成不同的区域后，区域间可以通过路由聚合来减少路由信息，从而减小路由表的规模，提高交换机的性能。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

- 配置 ABR 路由聚合
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **area** *area-id*，进入 OSPF 区域视图。
  4. 执行命令 **abr-summary** *ip-address mask* [[**advertise** | **not-advertise**] | **cost** *cost*] *，配置 OSPF 的 ABR 路由聚合。
- 配置 ASBR 路由聚合
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **asbr-summary** *ip-address mask* [**not-advertise** | **tag** *tag* | **cost** *cost* | **distribute-delay** *interval*] *，配置 OSPF 的 ASBR 路由聚合。

----结束

配置 OSPF 对接收的路由进行过滤

通过对接收的路由设置路由信息的过滤条件，只有通过过滤的路由才被添加到路由表中。

版权所有 © 华为技术有限公司

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**，配置对接收的路由进行过滤。

由于 OSPF 是基于链路状态的动态路由协议，路由信息隐藏在链路状态中，所以不能使用 **filter-policy** 命令对发布和接收的 LSA 进行过滤。该命令实际上是对 OSPF 计算出来的路由进行过滤，只有通过过滤的路由才被添加到路由表中。

filter-policy 命令仅过滤通过 OSPF 加入到本地路由表中的路由，没有通过过滤的路由不会被添加进 OSPF 路由表，也不会对外发布出去。接收到的路由无论是否通过过滤，都不会对 LSDB 有影响。

----结束

配置对 ABR Type3 LSA 进行过滤

通过对 Type3 LSA 设置过滤条件，只有通过过滤的信息才能被接收、发布。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **filter** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**，配置接收并发布 ABR 上产生的 Type3 LSA。

执行命令 **filter** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export**，配置拒绝接收和发布 ABR 上产生的 Type3 LSA。

----结束

配置 OSPF 引入外部路由

通过引入其他路由协议路由，可以扩充 OSPF 路由信息。

背景信息

OSPF 是一个无自环的动态路由协议，但这是针对域内路由和域间路由而言的，其对引入的外部路由环路没有很好的防范机制，所以在配置 OSPF 引入外部路由时一定要慎重，防止人为配置引起的环路。

版权所有 © 华为技术有限公司

请在运行 OSPF 协议的自治系统边界路由器 ASBR 上进行以下配置。

操作步骤

- 配置 OSPF 引入其它协议的路由
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **import-route** { **limit** *limit-number* | { **bgp** [**permit-ibgp**] | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] } [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * }，引入其它协议的路由信息。
  4. （可选）执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]，配置对引入的路由进行过滤，通过过滤的路由才能被发布出去。

     用户可以通过指定 *protocol* [*process-id*]对特定的某一种协议或某一进程的路由信息进行过滤。如果没有指定 *protocol* [*process-id*]，则 OSPF 将对所有引入的路由信息进行过滤。

     说明

     - **import-route** 命令不能引入外部路由的缺省路由。
     - OSPF 对引入的路由进行过滤，是指 OSPF 只将满足条件的外部路由转换为 Type5 LSA 并发布出去。
- 配置 OSPF 引入缺省路由
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 请根据实际情况选择以下配置。
     - 如果要引入缺省路由到 OSPF 进程中，则执行命令 **default-route-advertise** [[**always** | **permit-calculate-other**] | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] *。
     - 如果要指定 Type-3 summary LSA 的缺省开销值，则执行命令 **default-route-advertise summary cost** *cost*。在选用该参数时，必须首先使能 VPN，否则不能配置该命令。

     说明

     OSPF 路由域中在通告缺省路由前，会比较缺省路由的优先级，如果在其中某 OSPF 交换机上同时配置了静态缺省路由，要使 OSPF 通告的缺省路由加入到当前的路由表中，则必须保证所配置的静态缺省路由的优先级比 OSPF 通告的缺省路由的优先级低。
- 配置 OSPF 引入路由时的相关参数
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。
  3. 执行命令 **default** { **cost** { *cost* | **inherit-metric** } | **limit** *limit* | **tag** *tag* | **type** *type* } *，配置引入路由时的参数缺省值（开销、路由数量、标记、类型）。

     当 OSPF 引入外部路由时，可以配置一些额外参数的缺省值，如开销、路由数量、标记和类型。路由标记可以用来标识协议相关的信息，如 OSPF 接收 BGP 时用来区分自治系统的编号。

版权所有 © 华为技术有限公司

缺省情况下，OSPF 引入外部路由的缺省度量值为 1，一次可引入外部路由数量的上限为 2147483647，引入的外部路由类型为 Type2，设置缺省标记值为 1。

说明

可以通过以下三条命令设置引入路由的开销值，其优先级依次递减：

- 通过 **apply cost** 命令设置的路由开销值。
- 通过 **import-route**（OSPF）命令设置的引入路由开销值。
- 通过 **default** 命令设置引入路由的缺省开销值。

----结束

检查配置结果

调整 OSPF 的路由信息后，您可以查看到 OSPF 路由表、接口信息和 ASBR 聚合信息。

前提条件

已经完成控制 OSPF 路由信息的所有配置。

操作步骤

- 使用以下命令查看 OSPF 路由表信息：
  - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
  - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- 使用 **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]命令查看 OSPF 的接口信息。
- 使用 **display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]命令查看 OSPF ASBR 聚合信息。

----结束

任务示例

执行命令 **display ospf interface**，可以看到 OSPF 的接口信息。

```
<Quidway> display ospf interface vlanif 10
         OSPF Process 1 with Router ID 1.1.1.1
                 Interfaces
 Interface: 11.1.1.1 (Vlanif10)
 Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 1.1.1.2
 Backup Designated Router: 1.1.1.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

如果 OSPF 对引入的路由进行聚合，执行命令 **display ospf asbr-summary**，可以看到本交换机引入的路由聚合信息。

```
<Quidway> display ospf asbr-summary
         OSPF Process 1 with Router ID 192.168.1.2
                 Summary Addresses
 Total summary address count: 1
                 Summary Address
 net         : 10.0.0.0
 mask        : 255.0.0.0
```


版权所有 © 华为技术有限公司

```
tag          : 10
status       : Advertise
Cost         : 0 (Not Configured)
delay        : 0 (Not Configured)
The Count of Route is : 2
Destination      Net Mask        Proto      Process   Type      Metric
10.1.0.0         255.255.0.0     Static     1         2         10
10.2.0.0         255.255.0.0     Static     1         2         10
```

5.4.10 调整优化 OSPF 网络

在某些特殊的网络环境中，需要配置 OSPF 的一些特性功能，并需要对 OSPF 网络的性能进行调整和优化。

建立配置任务

在调整优化 OSPF 网络前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在某些特殊的网络环境中，需要配置 OSPF 的一些特性功能，并需要对 OSPF 网络的性能进行调整和优化。通过本节的配置过程，你可以：

- 通过改变 OSPF 的报文定时器，可以调整 OSPF 网络的收敛速度以及协议报文带来的网络负荷。在一些低速链路上，需要考虑接口传送 LSA 的延迟时间。
- 通过调整 SPF 计算间隔时间，可以抑制由于网络频繁变化带来的资源消耗问题。
- 在存在备份链路的情况下，使能了 OSPF-BGP 联动特性的 Stub 交换机可以使重启交换机或者新加入的交换机在 OSPF-BGP 联动期间不会被用作穿越交换机，从而避免了 BGP 在链路回切时由于收敛速度滞后于 OSPF 而造成的流量丢失现象。

前置任务

在调整和优化 OSPF 网络之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在调整和优化 OSPF 网络之前，需要准备以下数据。

序号	数据
1	报文定时器的值
2	DD 报文中的 MTU 值
3	LSDB 中 External LSA 的最大数量
4	验证类型以及验证密码

版权所有 © 华为技术有限公司

配置接口传送 LSA 的延迟时间

因为 OSPF 报文在链路传送时需要花费时间，所以当交换机的一个接口发送 LSA 时，会在其老化时间（age）上增加一定的延迟时间。

背景信息

缺省情况下，传输延迟时间为 1 秒。

说明

在低速链路上需要对该项配置进行重点考虑。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf trans-delay** *interval*，配置接口传送 LSA 的延迟时间。

----结束

配置邻接交换机重传 LSA 的间隔

当一台交换机向它的邻居发送一条 LSA 后，需要等到对方的确认报文。若在重传间隔时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf timer retransmit** *interval*，设置邻接交换机重传 LSA 的间隔。

缺省情况下，重传间隔时间为 5 秒。

说明

相邻交换机重传 LSA 时间间隔的值不要设置得太小，否则将会引起不必要的重传。通常应该大于一个报文在两台交换机之间传送一个来回的时间。

----结束

抑制接口接收和发送 OSPF 报文

如果要使 OSPF 路由信息不被某一网络中的交换机获得且使本地交换机不接收网络中其他交换机发布的路由更新信息，可抑制此接口接收和发送 OSPF 报文。

版权所有 © 华为技术有限公司

背景信息

如果要使 OSPF 路由信息不被某一网络中的交换机获得且使本地交换机不接收网络中其他交换机发布的路由更新信息，可使用 **silent-interface** 命令来抑制此接口接收和发送 OSPF 报文。

不同的进程可以对同一接口抑制发送和接收 OSPF 报文，但 **silent-interface** 命令只对本进程已经使能的 OSPF 接口起作用，对其它进程的接口不起作用。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **silent-interface** { **all** | *interface-type interface-number* }，抑制接口接收和发送 OSPF 报文。

----结束

后续处理

将运行 OSPF 协议的接口指定为 Silent 状态后，该接口的直连路由仍可以发布出去，但接口的 Hello 报文将被阻塞，接口上无法建立邻居关系。这样可以增强 OSPF 的组网适应能力，减少系统资源的消耗。

配置 STUB 路由器

STUB 路由器用来控制流量，它告知其他 OSPF 交换机不要使用这个 STUB 路由器来转发数据，但可以拥有一个到 STUB 路由器的路由。

背景信息

STUB 路由器生成的 Router LSA 中，所有链路的度量值都设置为比较大（65535）。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **stub-router** [**on-startup** [*interval*]]，配置 STUB 路由器。

缺省情况下，交换机保持为 STUB 路由器的时间间隔是 500 秒。

说明

通过此命令配置的 STUB 路由器与 Stub 区域里的交换机没有必然联系。

----结束

版权所有 © 华为技术有限公司

配置 DD 报文中的 MTU

通过使能在 DD 报文中填充接口的实际 MTU，将使用接口的实际 MTU 值填写 DD 报文 Interface MTU 字段。

背景信息



注意

当配置 DD 报文 MTU 值后，会引起邻居关系重新建立。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospf mtu-enable**，使能接口发送 DD 报文时填 MTU 值。

一般情况下，接口发送 DD 报文时不使用接口的实际 MTU 值，而是用 0 代替。配置此命令后，将使用接口的实际 MTU 值填写 DD 报文 Interface MTU 字段。

----结束

配置 LSDB 中 External LSA 的最大数量

通过配置 OSPF 的 LSDB 中 External LSA 的最大条目数，保证路由条数在一个合理的范围内。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **lsdb-overflow-limit** *number*，配置 LSDB 中 External LSA 的最大数量。

----结束

配置兼容 RFC1583 的外部路由选择规则

当多条 LSA 计算出同一条外部路由时，在 RFC2328 中定义的选路规则与 RFC1583 的有所不同，配置此命令可以兼容 RFC1583 中定义的方式。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **rfc1583 compatible**，配置兼容 RFC1583 的外部路由选择规则。

缺省情况下，使能兼容 RFC1583 的选路规则。

----结束

检查配置结果

调整优化 OSPF 网络后，您可以查看到统计信息、请求和重传列表，和 Mesh-Group 的概要信息。

前提条件

已经完成调整优化 OSPF 网络的所有配置。

操作步骤

- 使用 **display ospf** [*process-id*] **brief** 命令查看 OSPF 的概要信息。
- 使用 **display ospf** [*process-id*] **cumulative** 命令查看 OSPF 的统计信息。
- 使用以下命令查看 OSPF 错误信息：
  - **display ospf** [*process-id*] **error** [**lsa**]
  - **display ospf error** [**packet** [*number*]]

----结束

任务示例

执行命令 **display ospf brief**，可以看到 OSPF 报文定时器的详细信息和接口传送 LSA 的延迟时间。

```
<Quidway> display ospf brief

         OSPF Process 1 with Router ID 192.168.10.1
                OSPF Protocol Information

 RouterID: 192.168.10.1     Border Router:  AS
 Multi-VPN-Instance is not enabled
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route Preference: 10
 ASE Route Preference: 150
 SPF Computation Count: 0
 RFC 1583 Compatible
 bfd enabled
 BFD Timers: Tx-Interval 1000 , Rx-Interval 1000 , Multiplier 3
 Area Count: 1   Nssa Area Count: 0
 ExChange/Loading Neighbors: 0

 Area: 0.0.0.1
 Authtype: None   Area flag: Normal
 SPF scheduled Count: 0
 ExChange/Loading Neighbors: 0
```


版权所有 © 华为技术有限公司

5.4.11 配置 OSPF 网管功能

OSPF 同时支持网管功能，可以配置 OSPF MIB 与某一进程绑定，以及发送 Trap 消息和日志功能。

建立配置任务

在配置 OSPF 网管功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

OSPF 同时支持网管功能，可以配置 OSPF MIB 与某一进程绑定，以及发送 Trap 消息和日志功能。

前置任务

在配置 OSPF 的网管功能之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

无

配置 OSPF MIB 绑定

OSPF MIB 是一个虚拟的数据库，是在被管理设备端维护的设备状态信息集。

背景信息

当启动了多个 OSPF 进程时，可以配置 OSPF MIB 对哪个进程进行处理，即绑定在哪个进程。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf mib-binding** *process-id*，配置 OSPF MIB 绑定。

----结束

配置 OSPF TRAP 功能

告警是系统检测到故障而产生的通知，告警中携带对应的故障信息。Trap 信息是交换机发送到网管设备的信息。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable feature-name ospf [trap-name { ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange | ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa | ospfnbrstatechange | ospfnssatranslatorstatuschange | ospforiginatelsa | ospftxretransmit }]**，打开 OSPF 模块的告警开关。

----结束

配置 OSPF 日志信息功能

日志信息记录了用户对交换机的操作（比如命令配置）以及特定事件（比如网络连接失效）等信息。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **enable log** [**config** | **error** | **state** | **snmp-trap**]，使能日志信息。

----结束

检查配置结果

通过配置 OSPF 的网管功能，您可以查看到信息通道的内容、信息中心记录的各项信息、日志缓冲区记录和告警缓冲区记录的信息。

前提条件

已经完成 OSPF 网管功能的所有配置。

操作步骤

- 使用 **display ospf** [*process-id*] **brief** 命令查看 OSPF MIB 绑定信息。
- 使用 **display snmp-agent trap feature-name ospf all** 命令查看 OSPF 模块的所有告警信息。

----结束

5.4.12 提高 OSPF 网络的安全性

在对安全性较高的网络中，可以通过配置 OSPF 验证特性来提高 OSPF 网络的安全性。

建立配置任务

在提高 OSPF 网络的安全性前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

在安全性较高的网络中，可以通过配置 OSPF 验证特性来提高 OSPF 网络的安全性。

前置任务

在提高 OSPF 网络的安全性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达。
- **配置 OSPF 的基本功能**。

数据准备

在提高 OSPF 网络的安全性之前，需要准备以下数据。

序号	数据
1	OSPF 进程号
2	（可选）OSPF 的 VPN 实例名称
3	需要配置验证的 OSPF 区域编号
4	需要配置验证的 OSPF 接口编号
5	验证方式及密码

配置区域验证方式

OSPF 支持报文验证功能，只有通过验证的报文才能接收，否则将不能正常建立邻居关系。

背景信息

OSPF 支持报文验证功能，只有通过验证的报文才能接收，否则将不能正常建立邻居关系。使用区域验证时，一个区域中所有的交换机在该区域下的验证模式和口令必须一致。例如，在 Area0 内所有交换机上配置验证模式为简单验证，口令为 abc。

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，进入 OSPF 进程视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 请根据需求，配置 OSPF 区域的验证模式。

- 执行命令 **authentication-mode simple** [**plain** *plain-text* | **cipher** *cipher-text*]，配置 OSPF 区域的简单验证模式。

版权所有 © 华为技术有限公司

- 执行命令 **authentication-mode** { **md5** | **hmac-md5** } [*key-id* { **plain** *plain-text* | **cipher** *cipher-text* }]，配置 OSPF 区域的 md5 验证模式。

----结束

配置接口验证方式

接口验证方式用于在相邻的交换机之间设置验证模式和口令，优先级高于区域验证方式。

背景信息

请在运行 OSPF 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 请根据需求，配置接口验证方式。

- 执行命令 **ospf authentication-mode simple** [**plain** *plain-text* | **cipher** *cipher-text*]，配置 OSPF 接口的简单验证模式。
- 执行命令 **ospf authentication-mode** { **md5** | **hmac-md5** } [*key-id* { **plain** *plain-text* | **cipher** *cipher-text* }]，配置 OSPF 接口的 MD5 验证模式。
- 执行命令 **ospf authentication-mode null**，不对 OSPF 接口进行验证。

接口验证方式用于在相邻的交换机之间设置验证模式和口令，优先级高于区域验证方式。

同一网段的接口的验证模式和口令必须相同，不同网段可以不同。

----结束

检查配置结果

通过配置 OSPF 的各种性能，提高 OSPF 网络的安全性后，您可以查看到概要统计信息。

前提条件

已经完成提高 OSPF 网络的安全性的所有配置。

操作步骤

- 使用以下命令查看 OSPF 的错误信息：
  - **display ospf** [*process-id*] **error** [**lsa**]
  - **display ospf error** [**packet**[*number*]]

----结束

5.4.13 维护 OSPF

维护 OSPF，包括复位、清除 OSPF。

版权所有 © 华为技术有限公司

复位 OSPF

通过重启 OSPF，达到复位的目的。

背景信息

注意

复位 OSPF 连接（执行 **reset ospf** 命令）会导致交换机之间的 OSPF 邻接关系中断。务必仔细确认是否必须执行复位 OSPF 连接的操作。

如果需要复位 OSPF 连接，可在用户视图下选择执行以下命令。

操作步骤

- 在用户视图下执行 **reset ospf** [*process-id*] **process** [**flush-waiting-timer** *time*]命令重启 OSPF 进程。

----结束

清除 OSPF

清除 OSPF 包括清除 OSPF 的计数器、引入的路由和单板上的统计信息。

背景信息

注意

清除 OSPF 的信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 OSPF 的运行信息后，请在用户视图下执行以下命令。

操作步骤

- 在用户视图下执行 **reset ospf** [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]命令清除 OSPF 计数器。
- 在用户视图下执行 **reset ospf** [*process-id*] **redistribution** 命令清除 OSPF 引入的路由。

----结束

调试 OSPF

只要在用户视图下打开相应模块的调试开关，交换机交换机就能够产生调试信息。调试信息显示被调试模块接受或者发送数据报的信息内容。

版权所有 © 华为技术有限公司

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 OSPF 运行故障时，请在用户视图下执行 **debugging** 命令对 OSPF 进行调试，查看调试信息，定位故障并分析故障原因。打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南 系统管理》中“信息中心配置”的内容。

有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 在用户视图下执行以下命令，打开 OSPF 报文调试信息开关。
  - **debugging ospf** [*process-id*] **packet** [**ack** | **dd** | **hello** | **request** | **update**] [**brief**] [**filter** { **src** | **nbr** } { *acl-number* | **ip-prefix** *ip-prefix-name* }]
  - **debugging ospf packet** [**rcv-dump** [**error**] | **snd-dump**] [**filter** { **src** | **nbr** } { *acl-number* | **ip-prefix** *ip-prefix-name* }

    ]

  说明

  使用 **filter** 参数对 OSPF 报文调试信息进行过滤时，如果要通过 IP 地址过滤，则只有掩码为 32 位的 IP 地址有效。
- 在用户视图下执行 **debugging ospf** [*process-id*] **event** 命令打开 OSPF 事件调试信息。
- 在用户视图下执行 **debugging ospf** [*process-id*] **lsa-originate** 命令打开 OSPF LSA 报文调试信息开关。
- 在用户视图下执行以下命令，打开 OSPF 的 SPF 调试信息开关。
  - **debugging ospf** [*process-id*] **spf** { **all** | **brief** | **intra** }
  - **debugging ospf** [*process-id*] **spf** { **asbr-summary** | **ase** | **net-summary** | **nssa** } [**filter** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }]
- 在用户视图下执行 **debugging ospf** [*process-id*] **bfd** 命令打开 OSPF 的 BFD 调试信息开关。

----结束

5.4.14 配置 OSPF 举例

介绍 OSPF 的各种组网举例。

配置 OSPF 基本功能

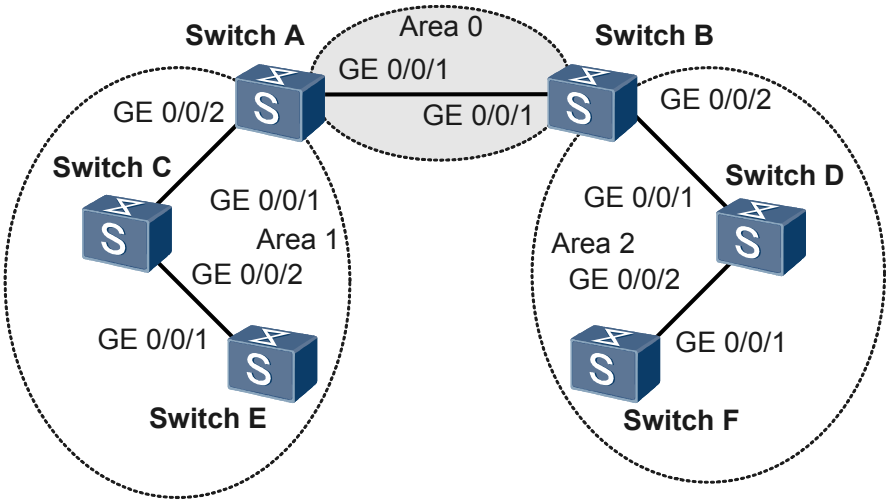
组网需求

如图 5-10 所示，所有的 Switch 都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 SwitchA 和 SwitchB 作为 ABR 来转发区域之间的路由。

版权所有 © 华为技术有限公司

配置完成后，每台 Switch 都应学到自治系统内的到所有网段的路由。

图 5-10 OSPF 基本配置组网图



设备	接口	对应的 VLANIF IP 地址	
Switch A	GE0/0/1	VLANIF 10	192.168.0.1/24
Switch A	GE 0/0/2	VLANIF 20	192.168.1.1/24
Switch B	GE 0/0/1	VLANIF 10	192.168.0.2/24
Switch B	GE 0/0/2	VLANIF 30	192.168.2.1/24
Switch C	GE 0/0/1	VLANIF 20	192.168.1.2/24
Switch C	GE 0/0/2	VLANIF 40	172.16.1.1/24
Switch D	GE 0/0/1	VLANIF 30	192.168.2.2/24
Switch D	GE 0/0/2	VLANIF 50	172.17.1.1/24
Switch E	GE 0/0/1	VLANIF 40	172.16.1.2/24
Switch F	GE 0/0/1	VLANIF 50	172.17.1.2/24

配置思路

采用如下的思路配置 OSPF 基本功能：

1. 配置各接口所属 VLAN ID。
2. 配置各 VLANIF 接口的 IP 地址。
3. 在各 Switch 设备上使能 OSPF，指定不同区域内的网段。
4. 查看路由表及数据库信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-10 所示。

版权所有 © 华为技术有限公司

- 各 VLANIF 接口的 IP 地址，具体数据如图 5-10 所示。
- 各 Switch 设备的 Router ID，OSPF 进程号以及各接口所属的区域。
  - SwitchA 的 Router ID 1.1.1.1，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.0.0/24，在区域 1 的网段 192.168.1.0/24。
  - SwitchB 的 Router ID 2.2.2.2，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.0.0/24，在区域 2 的网段 192.168.2.0/24。
  - SwitchC 的 Router ID 3.3.3.3，运行的 OSPF 进程号 1，在区域 1 的网段 192.168.1.0/24，172.16.1.0/24。
  - SwitchD 的 Router ID 4.4.4.4，运行的 OSPF 进程号 1，在区域 2 的网段 192.168.2.0/24，172.17.1.0/24。
  - SwitchE 的 Router ID 5.5.5.5，运行的 OSPF 进程号 1，在区域 1 的网段 172.16.1.0/24。
  - SwitchF 的 Router ID 6.6.6.6，运行的 OSPF 进程号 1，在区域 2 的网段 172.17.1.0/24。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 OSPF 基本功能

   # 配置 SwitchA。

```
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

   # 配置 SwitchB。

```
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

   # 配置 SwitchC。

```
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

   # 配置 SwitchD。

```
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```


版权所有 © 华为技术有限公司

```
[SwitchD-ospf-1] quit
```

配置 SwitchE。

```
[SwitchE] router id 5.5.5.5
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.1] quit
[SwitchE-ospf-1] quit
```

配置 SwitchF。

```
[SwitchF] router id 6.6.6.6
[SwitchF] ospf
[SwitchF-ospf-1] area 2
[SwitchF-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchF-ospf-1-area-0.0.0.2] quit
[SwitchF-ospf-1] quit
```

4. 验证配置结果

查看 SwitchA 的 OSPF 邻居。

```
[SwitchA] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
                 Neighbors

 Area 0.0.0.0 interface 192.168.0.1(Vlanif10)'s neighbors
 Router ID: 2.2.2.2      Address: 192.168.0.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.0.1  BDR: 192.168.0.2  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 5
   Neighbor is up for 00:15:04
   Authentication Sequence: [ 0 ]

                 Neighbors

 Area 0.0.0.1 interface 192.168.1.1(Vlanif20)'s neighbors
   Router ID: 3.3.3.3       Address: 192.168.1.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.1  BDR: 192.168.1.2  MTU: 0
   Dead timer due in 39  sec
   Neighbor is up for 00:07:32
   Authentication Sequence: [ 0 ]
```

显示 SwitchA 的 OSPF 路由信息。

```
[SwitchA] display ospf routing

         OSPF Process 1 with Router ID 1.1.1.1
                  Routing Tables

 Routing for Network
 Destination      Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24     2    Transit      192.168.1.2     3.3.3.3         0.0.0.1
 172.17.1.0/24     3    Inter-area  192.168.0.2     2.2.2.2         0.0.0.0
 192.168.0.0/24    1    Transit      192.168.0.1     1.1.1.1         0.0.0.0
 192.168.1.0/24    1    Transit      192.168.1.1     1.1.1.1         0.0.0.1
 192.168.2.0/24    2    Inter-area  192.168.0.2     2.2.2.2         0.0.0.0

 Total Nets: 5
 Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

查看 SwitchA 的 LSDB。

```
[SwitchA] display ospf lsdb

         OSPF Process 1 with Router ID 1.1.1.1
                 Link State Database

                         Area: 0.0.0.0
```


版权所有 © 华为技术有限公司

```
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    2.2.2.2          2.2.2.2           317  48    80000003    1
 Router    1.1.1.1          1.1.1.1           316  48    80000002    1
 Network   192.168.0.1      1.1.1.1           316  32    80000001    0
 Sum-Net   172.16.1.0       1.1.1.1           250  28    80000001    2
 Sum-Net   172.17.1.0       2.2.2.2           203  28    80000001    2
 Sum-Net   192.168.2.0      2.2.2.2           237  28    80000002    1
 Sum-Net   192.168.1.0      1.1.1.1           295  28    80000002    1

                    Area: 0.0.0.1
Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.1.2      192.168.1.2       188  48    80000002    1
 Router    5.5.5.5          5.5.5.5           214  36    80000004    1
 Router    3.3.3.3          3.3.3.3           217  60    80000008    1
 Router    1.1.1.1          1.1.1.1           289  48    80000002    1
 Network   172.16.1.1       3.3.3.3           670  32    80000001    0
 Sum-Net   172.17.1.0       1.1.1.1           202  28    80000001    3
 Sum-Net   192.168.2.0      1.1.1.1           242  28    80000001    2
 Sum-Net   192.168.0.0      1.1.1.1           300  28    80000001    1
```

查看 SwitchD 的路由表，并使用 Ping 进行测试连通性。

```
[SwitchD] display ospf routing

          OSPF Process 1 with Router ID 4.4.4.4
                  Routing Tables

 Routing for Network
 Destination        Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24      4     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 172.17.1.0/24      1     Transit     172.17.1.1      4.4.4.4         0.0.0.2
 192.168.0.0/24     2     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.1.0/24     3     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.2.0/24     1     Transit     192.168.2.2     4.4.4.4         0.0.0.2

 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0

[SwitchD] ping 172.16.1.1
  PING 172.16.1.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms

  --- 172.16.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 16/59/94 ms
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
router id 2.2.2.2
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 192.168.0.2 255.255.255.0
#
interface Vlanif30
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

- SwitchD 的配置文件

```
#
```


版权所有 © 华为技术有限公司

```
 sysname SwitchD
#
router id 4.4.4.4
#
 vlan batch 30 50
#
interface Vlanif30
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif50
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
#
return
```

- SwitchF 的配置文件

```
#
 sysname SwitchF
#
router id 6.6.6.6
#
 vlan batch 50
#
interface Vlanif50
 ip address 172.17.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 50
#
ospf 1
 area 0.0.0.2
  network 172.17.1.0 0.0.0.255
#
return
```

配置 OSPF 的 Stub 区域

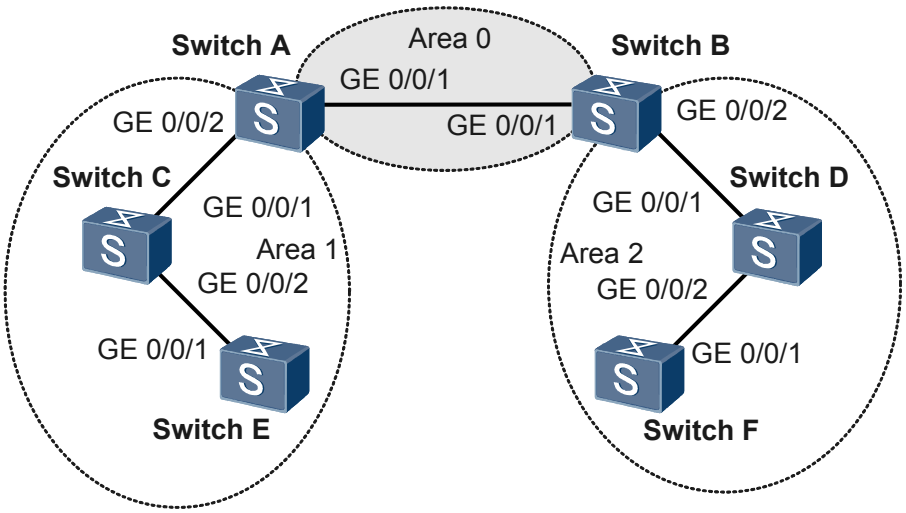
版权所有 © 华为技术有限公司

组网需求

如图 5-11 所示，所有的 Switch 都运行 OSPF，整个自治系统划分为 3 个区域。其中 SwitchA 和 SwitchB 作为 ABR 来转发区域之间的路由，SwitchD 作为 ASBR 引入了外部路由（静态路由）。

要求将 Area1 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

图 5-11 配置 OSPF Stub 区域组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	192.168.0.1/24
SwitchA	GE 0/0/2	VLANIF 20	192.168.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	192.168.0.2/24
SwitchB	GE 0/0/2	VLANIF 30	192.168.2.1/24
SwitchC	GE 0/0/1	VLANIF 20	192.168.1.2/24
SwitchC	GE 0/0/2	VLANIF 40	172.16.1.1/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.2.2/24
SwitchD	GE 0/0/2	VLANIF 50	172.17.1.1/24
SwitchE	GE 0/0/1	VLANIF 40	172.16.1.2/24
SwitchF	GE 0/0/1	VLANIF 50	172.17.1.2/24

配置思路

采用如下的思路配置 OSPF 的 Stub 区域：

1. 在各 Switch 上使能 OSPF，配置 OSPF 基本功能。
2. 在 SwitchD 上配置静态路由，并在 OSPF 中引入。
3. 配置 Area1 为 Stub 区域（需要在 Area1 内所有的 Switch 上配置 **Stub** 命令）。

版权所有 © 华为技术有限公司

4. 在 SwitchA 上配置禁止向 Stub 区域通告 Type3 LSA。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如**图 5-11** 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如**图 5-11** 所示。
- 各 Switch 设备的 Router ID，OSPF 进程号以及各接口所属的区域。
  - SwitchA 的 Router ID 1.1.1.1，运行的 OSPF 进程号 1，区域 0 的网段 192.168.0.0/24，区域 1 的网段 192.168.1.0/24。
  - SwitchB 的 Router ID 2.2.2.2，运行的 OSPF 进程号 1，区域 0 的网段 192.168.0.0/24，区域 2 的网段 192.168.2.0/24。
  - SwitchC 的 Router ID 3.3.3.3，运行的 OSPF 进程号 1，区域 1 的网段 192.168.1.0/24，172.16.1.0/24。
  - SwitchD 的 Router ID 4.4.4.4，运行的 OSPF 进程号 1，区域 2 的网段 192.168.2.0/24，172.17.1.0/24。
  - SwitchE 的 Router ID 5.5.5.5，运行的 OSPF 进程号 1，区域 1 的网段 172.16.1.0/24。
  - SwitchF 的 Router ID 6.6.6.6，运行的 OSPF 进程号 1，区域 2 的网段 172.17.1.0/24。

配置步骤

1. 配置 OSPF 基本功能（请参见举例**配置 OSPF 基本功能**）
2. 配置 SwitchD 引入静态路由

   # 在 SwitchD 引入静态路由，例如。

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
[SwitchD] ospf
[SwitchD-ospf-1] import-route static type 1
[SwitchD-ospf-1] quit
```

   # 查看 SwitchC 的 ABR/ASBR 信息。

```
[SwitchC] display ospf abr-asbr

         OSPF Process 1 with Router ID 3.3.3.3
                Routing Table to ABR and ASBR

 Type        Destination      Area       Cost  Nexthop         RtType
 Intra-area  1.1.1.1          0.0.0.1    1     192.168.1.1     ABR
 Inter-area  4.4.4.4          0.0.0.1    3     192.168.1.1     ASBR
```

   # 查看 SwitchC 的 OSPF 路由表。

```
[SwitchC] display ospf routing

     OSPF Process 1 with Router ID 3.3.3.3
                 Routing Tables

 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
 172.16.1.0/24      1     Transit     172.16.1.1      3.3.3.3         0.0.0.1
 172.17.1.0/24      4     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 192.168.0.0/24     2     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 192.168.1.0/24     1     Transit     192.168.1.2     3.3.3.3         0.0.0.1
 192.168.2.0/24     3     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1

 Routing for ASEs
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
Destination        Cost      Type       Tag         NextHop         AdvRouter
200.0.0.0/8        4       Type1      1           192.168.1.1     4.4.4.4

Total Nets: 6
Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

当 SwitchC 所在区域为普通区域时，可以看到路由表中存在 AS 外部的路由。

3. 配置 Area1 为 Stub 区域

配置 SwitchA。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 SwitchC。

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

配置 SwitchE。

```
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] stub
[SwitchE-ospf-1-area-0.0.0.1] quit
[SwitchE-ospf-1] quit
```

查看 SwitchC 的路由表。

```
[SwitchC] display ospf routing

         OSPF Process 1 with Router ID 3.3.3.3
                 Routing Tables

 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
 0.0.0.0/0           2    Inter-area 192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24       1    Transit     172.16.1.1     3.3.3.3         0.0.0.1
 172.17.1.0/24       4    Inter-area 192.168.1.1     1.1.1.1         0.0.0.1
 192.168.0.0/24      2    Inter-area 192.168.1.1     1.1.1.1         0.0.0.1
 192.168.1.0/24      1    Transit     192.168.1.2    3.3.3.3         0.0.0.1
 192.168.2.0/24      3    Inter-area 192.168.1.1     1.1.1.1         0.0.0.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 4  ASE: 0  NSSA: 0
```

当把 SwitchC 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条通往区域外部的缺省路由。

配置禁止向 Stub 区域通告 Type3 LSA。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

4. 验证配置结果

查看 SwitchC 的 OSPF 路由表。

```
[SwitchC] display ospf routing

         OSPF Process 1 with Router ID 3.3.3.3
                 Routing Tables

 Routing for Network
 Destination        Cost  Type          NextHop         AdvRouter       Area
 0.0.0.0/0           2     Inter-area   192.168.1.1     1.1.1.1         0.0.0.1
```


版权所有 © 华为技术有限公司

```
 172.16.1.0/24       1      Transit        172.16.1.1      3.3.3.3         0.0.0.1
 192.168.1.0/24      1      Transit        192.168.1.2     3.3.3.3         0.0.0.1

 Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

禁止向 Stub 区域通告 Summary-LSA 后，Stub 区域设备的路由表项进一步减少。路由表中已经看不到区域外部的路由，取而代之的是一条通往区域外部的缺省路由。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  stub no-summary
#
return
```

说明

SwitchB 和 SwitchF 的配置文件与前例相同，此处省略。

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1
area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  stub
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 50
#
router id 4.4.4.4
#
interface Vlanif30
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif50
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
ospf 1
 import-route static type 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
ip route-static 200.0.0.0 255.0.0.0 NULL0
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
  stub
#
return
```

配置 OSPF 的 NSSA 区域

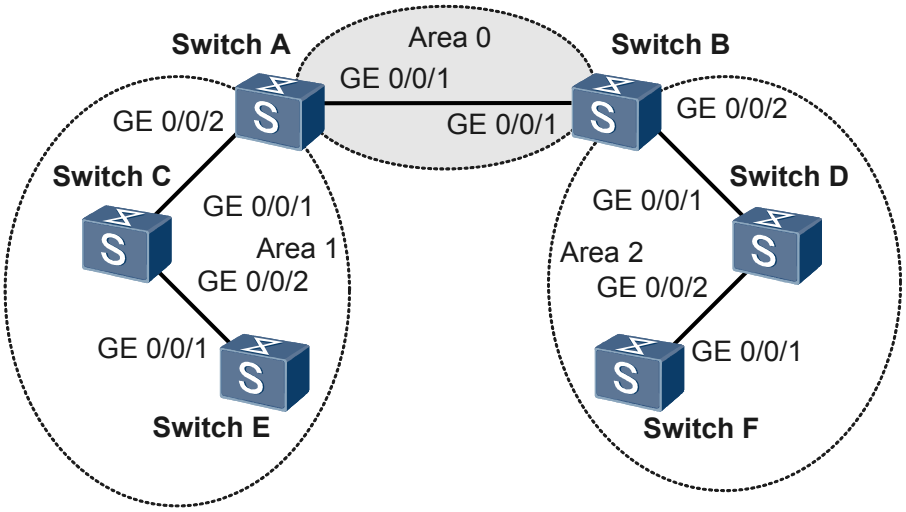
组网需求

如图 5-12 所示，所有的 Switch 都运行 OSPF，整个自治系统划分为 3 个区域。其中 SwitchA 和 SwitchB 作为 ABR 来转发区域之间的路由，SwitchD 作为 ASBR 引入了外部路由（静态路由）。

要求将 Area1 配置为 NSSA 区域，同时将 SwitchC 配置为 ASBR 引入外部路由（静态路由），且路由信息可正确的在 AS 内传播。

版权所有 © 华为技术有限公司

图 5-12 配置 OSPF NSSA 区域组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	192.168.0.1/24
SwitchA	GE 0/0/2	VLANIF 20	192.168.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	192.168.0.2/24
SwitchB	GE 0/0/2	VLANIF 30	192.168.2.1/24
SwitchC	GE 0/0/1	VLANIF 20	192.168.1.2/24
SwitchC	GE 0/0/2	VLANIF 40	172.16.1.1/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.2.2/24
SwitchD	GE 0/0/2	VLANIF 50	172.17.1.1/24
SwitchE	GE 0/0/1	VLANIF 40	172.16.1.2/24
SwitchF	GE 0/0/1	VLANIF 50	172.17.1.2/24

配置思路

采用如下的思路配置 OSPF 的 NSSA 区域：

1. 在各 Switch 上使能 OSPF，配置 OSPF 基本功能。
2. 在 SwitchD 上配置静态路由，并在 OSPF 中引入。
3. 配置 Area1 为 NSSA 区域（需要在 Area1 内所有的设备上配置 **nssa** 命令），查看 SwitchC 的 OSPF 路由信息。
4. 在 SwitchC 上配置静态路由，并在 OSPF 中引入，查看 SwitchD 的 OSPF 路由信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-12 所示。

版权所有 © 华为技术有限公司

- 各 VLANIF 接口的 IP 地址，具体数据如**图 5-12** 所示。
- 各 Switch 备的 Router ID，OSPF 进程号以及各接口所属的区域。
  - SwitchA 的 Router ID 1.1.1.1，运行的 OSPF 进程号 1，区域 0 的网段 192.168.0.0/24，区域 1 的网段 192.168.1.0/24。
  - SwitchB 的 Router ID 2.2.2.2，运行的 OSPF 进程号 1，区域 0 的网段 192.168.0.0/24，区域 2 的网段 192.168.2.0/24。
  - SwitchC 的 Router ID 3.3.3.3，运行的 OSPF 进程号 1，区域 1 的网段 192.168.1.0/24，172.16.1.0/24。
  - SwitchD 的 Router ID 4.4.4.4，运行的 OSPF 进程号 1，区域 2 的网段 192.168.2.0/24，172.17.1.0/24。
  - SwitchE 的 Router ID 5.5.5.5，运行的 OSPF 进程号 1，区域 1 的网段 172.16.1.0/24。
  - SwitchF 的 Router ID 6.6.6.6，运行的 OSPF 进程号 1，区域 2 的网段 172.17.1.0/24。

配置步骤

1. 配置 OSPF 基本功能（请参见举例**配置 OSPF 基本功能**）
2. 配置 SwitchD 引入静态路由（请参见举例**配置 OSPF 的 Stub 区域**）
3. 配置 Area1 区域为 NSSA 区域

   # 配置 SwitchA。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

   # 配置 SwitchC。

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

   # 配置 SwitchE。

```
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] nssa
[SwitchE-ospf-1-area-0.0.0.1] quit
[SwitchE-ospf-1] quit
```

   说明

   建议在 ABR（这里的 SwitchA）上配置 **default-route-advertise no-summary** 参数，这样可以减少 NSSA 区域设备的路由表容量。其他位于 NSSA 区域的设备只需配置 **nssa** 命令就可以。

   # 查看 SwitchC 的 OSPF 路由表。

```
[SwitchC] display ospf routing

         OSPF Process 1 with Router ID 3.3.3.3
                 Routing Tables

 Routing for Network
 Destination        Cost  Type          NextHop         AdvRouter       Area
 0.0.0.0/0           2     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24       1     Transit     172.16.1.1      3.3.3.3         0.0.0.1
 192.168.1.0/24      1     Transit     192.168.1.2     3.3.3.3         0.0.0.1
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

4. 配置 SwitchC 引入静态路由

   # 在 SwitchC 引入静态路由，例如。

```
[SwitchC] ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

5. 验证配置结果

   # 查看 SwitchD 的 OSPF 路由表。

```
[SwitchD] display ospf routing

         OSPF Process 1 with Router ID 4.4.4.4
                 Routing Tables

 Routing for Network
 Destination        Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24      4     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 172.17.1.0/24      1     Transit     172.17.1.1      4.4.4.4         0.0.0.2
 192.168.0.0/24     2     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.1.0/24     3     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.2.0/24     1     Transit     192.168.2.2     4.4.4.4         0.0.0.2
 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop         AdvRouter
 100.0.0.0/8        1         Type2      1           192.168.2.1     1.1.1.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

   在 SwitchD 上可以看到 NSSA 区域引入的一条 AS 外部的路由。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  nssa default-route-advertise no-summary
#
return
```

  说明

  SwitchB、SwitchD 和 SwitchF 的配置文件与前例相同，此处省略。

版权所有 © 华为技术有限公司

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1
 import-route static
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  nssa
#
ip route-static 100.0.0.0 255.0.0.0 NULL0
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
  nssa
#
return
```

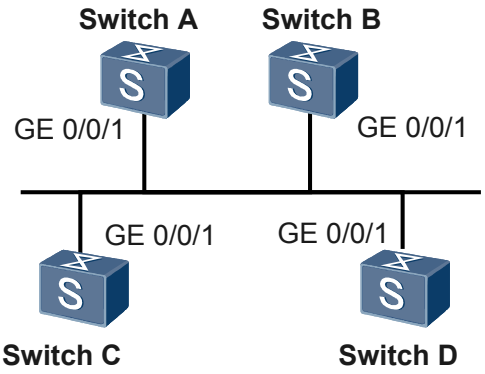
配置 OSPF 的 DR 选择

组网需求

在图 5-13 中，SwitchA 的优先级为 100，它是网络上的最高优先级，所以 SwitchA 被选为 DR；SwitchC 是优先级第二高的，被选为 BDR；SwitchB 的优先级为 0，这意味着它将无法成为 DR 或 BDR；SwitchD 没有配置优先级，取缺省值 1。

版权所有 © 华为技术有限公司

图 5-13 配置 OSPF 的 DR 选择组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchC	GE 0/0/1	VLANIF 10	192.168.1.3/24
SwitchD	GE 0/0/1	VLANIF 10	192.168.1.4/24

配置思路

采用如下的思路配置 OSPF 的 DR 选择：

1. 配置各接口所属 VLAN ID。
2. 配置各 VLANIF 接口的 IP 地址。
3. 配置各台 Switch 上 Router ID，使能 OSPF，指定网段。
4. 在缺省优先级情况下，查看各台 Switch 的 DR/BDR 状态。
5. 配置接口上的 DR 优先级，查看 DR/BDR 状态。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如**图 5-13** 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如**图 5-13** 所示。
- 各 Switch 备的 Router ID，OSPF 进程号，各接口所属的区域以及 DR 优先级。
  - SwitchA 的 Router ID 1.1.1.1，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.1.0/24，DR 优先级 100。
  - SwitchB 的 Router ID 2.2.2.2，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.1.0/24，DR 优先级 0。
  - SwitchC 的 Router ID 3.3.3.3，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.1.0/24，DR 优先级 2。
  - SwitchD 的 Router ID 4.4.4.4，运行的 OSPF 进程号 1，在区域 0 的网段 192.168.1.0/24，DR 优先级取缺省值 1。

版权所有 © 华为技术有限公司

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各接口的 IP 地址（略）
3. 配置 OSPF 基本功能

   # 配置 SwitchA。

```
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # 配置 SwitchB。

```
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # 配置 SwitchC。

```
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

   # 配置 SwitchD。

```
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

   # 查看 DR/BDR 的状态。

```
[SwitchA] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
                Neighbors

 Area 0.0.0.0 interface 192.168.1.1(Vlanif10)'s neighbors
 Router ID: 2.2.2.2      Address: 192.168.1.2
   State: 2-Way  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 32  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:00
   Authentication Sequence: [ 0 ]

 Router ID: 3.3.3.3      Address: 192.168.1.3
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 37  sec
   Retrans timer interval: 5
   Neighbor is up for 00:04:06
   Authentication Sequence: [ 0 ]

 Router ID: 4.4.4.4      Address: 192.168.1.4
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 37  sec
   Retrans timer interval: 5
   Neighbor is up for 00:03:53
```


版权所有 © 华为技术有限公司

```
  Authentication Sequence: [ 0 ]
```

查看 SwitchA 的邻居信息，可以看到 DR 优先级（缺省为 1）以及邻居状态，此时 SwitchD 为 DR，SwitchC 为 BDR。

说明

当优先级相同时，Router ID 高的为 DR。如果 Switch 某个 Gigabitethernet 接口成为 DR 之后，则这台 Switch 的其他广播接口在进行后续的 DR 选择时，具有高优先权。即选择已经是 DR 的 Switch 为 DR，DR 不可抢占。

4. 配置接口上的 DR 优先级

配置 SwitchA。

```
[SwitchA] interface Vlanif 10
[SwitchA-Vlanif10] ospf dr-priority 100
[SwitchA-Vlanif10] quit
```

配置 SwitchB。

```
[SwitchB] interface Vlanif 10
[SwitchB-Vlanif10] ospf dr-priority 0
[SwitchB-Vlanif10] quit
```

配置 SwitchC。

```
[SwitchC] interface Vlanif 10
[SwitchC-Vlanif10] ospf dr-priority 2
[SwitchC-Vlanif10] quit
```

查看 DR/BDR 的状态。

```
[SwitchD] display ospf peer

         OSPF Process 1 with Router ID 4.4.4.4
                Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1
   State: Full  Mode:Nbr is  Slave  Priority: 100
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 31  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
 Router ID: 2.2.2.2      Address: 192.168.1.2
   State: Full  Mode:Nbr is  Slave  Priority: 0
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]

 Router ID: 3.3.3.3      Address: 192.168.1.3
   State: Full  Mode:Nbr is  Slave  Priority: 2
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 33  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:15
   Authentication Sequence: [ 0 ]
```

说明

接口上的 DR 优先级在配置之后并不会立即生效。

5. 重启 OSPF 进程

在各 Switch 的用户视图下，同时执行命令 **reset ospf 1 process**，以重启 OSPF 进程。

6. 验证配置结果

查看 OSPF 邻居状态。

```
[SwitchD] display ospf peer
```


版权所有 © 华为技术有限公司

```
          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1
   State: Full  Mode:Nbr is  Master  Priority: 100
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:07:19
   Authentication Sequence: [ 0 ]

 Router ID: 2.2.2.2      Address: 192.168.1.2
   State: 2-Way  Mode:Nbr is  Slave  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:00
   Authentication Sequence: [ 0 ]

 Router ID: 3.3.3.3      Address: 192.168.1.3
   State: Full  Mode:Nbr is  Slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 37  sec
   Retrans timer interval: 5
   Neighbor is up for 00:07:17
   Authentication Sequence: [ 0 ]
```

查看 OSPF 接口的状态。

```
[SwitchA] display ospf interface

          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     Broadcast    DR       1     100   192.168.1.1     192.168.1.3

[SwitchB] display ospf interface

          OSPF Process 1 with Router ID 2.2.2.2
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State      Cost  Pri   DR              BDR
 192.168.1.2     Broadcast    DROther  1       0     192.168.1.1     192.168.1.3
```

如果邻居的状态是 Full，这说明它和邻居之间形成了邻接关系；如果停留在 2-Way 的状态，则说明他们都不是 DR 或 BDR，两者之间不需要交换 LSA。

如果 OSPF 接口的状态是 DROther，则说明它既不是 DR，也不是 BDR。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 ospf dr-priority 100
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
```


版权所有 © 华为技术有限公司

```
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
router id 2.2.2.2
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
 ospf dr-priority 0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.3 255.255.255.0
 ospf dr-priority 2
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
router id 4.4.4.4
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.4 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

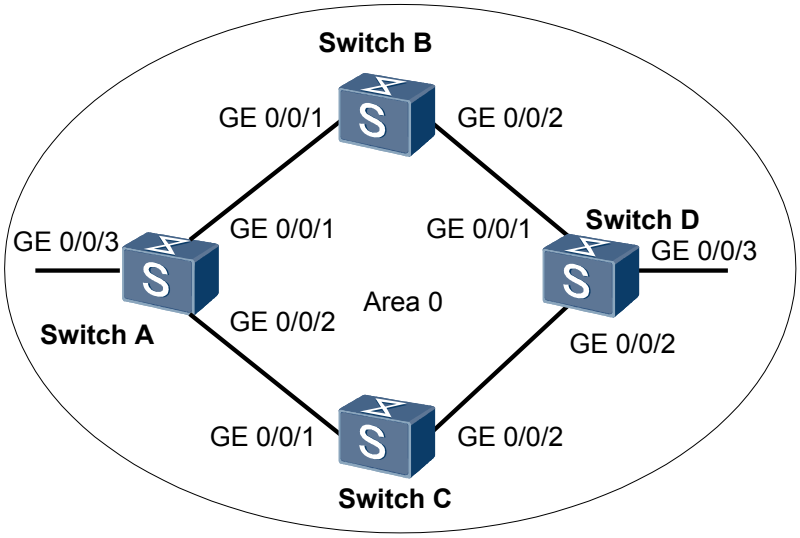
配置 OSPF 负载分担

组网需求

如图 5-14 所示：

- SwitchA、SwitchB、SwitchC 和 SwitchD 之间通过 OSPF 协议达到 IP 网络互连的目的。
- SwitchA、SwitchB、SwitchC 和 SwitchD 同属于区域 0。
- 要求配置负载分担，使得 SwitchA 的流量，可以分别通过 SwitchB 和 SwitchC 发送到 SwitchD。

图 5-14 配置 OSPF 负载分担组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchA	GE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchA	GE 0/0/3	VLANIF 50	172.16.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	GE 0/0/2	VLANIF 30	192.168.0.1/24
SwitchC	GE 0/0/1	VLANIF 20	10.1.2.2/24
SwitchC	GE 0/0/2	VLANIF 40	192.168.1.1/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	GE 0/0/2	VLANIF 40	192.168.1.2/24
SwitchD	GE 0/0/3	VLANIF 60	172.17.1.1/24

配置思路

采用如下的思路配置 OSPF 的负载分担：

版权所有 © 华为技术有限公司

1. 在各台交换机使能 OSPF 基本功能，实现互连。
2. 取消负载分担，查看路由表信息。
3. 在 SwitchA 上配置等价路由优先级（可选配置）。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如**图 5-14** 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如**图 5-14** 所示。
- 各交换机设备的 Router ID，OSPF 进程号以及各接口所属的区域。
  - SwitchA 的 Router ID 1.1.1.1，运行的 OSPF 进程号 1，区域 0 的网段 10.1.1.0/24、10.1.2.0/24 和 172.16.1.0/24。
  - SwitchB 的 Router ID 2.2.2.2，运行的 OSPF 进程号 1，区域 0 的网段 10.1.1.0/24 和 192.168.0.0/24。
  - SwitchC 的 Router ID 3.3.3.3，运行的 OSPF 进程号 1，区域 0 的网段 10.1.2.0/24 和 192.168.1.0/24。
  - SwitchD 的 Router ID 4.4.4.4，运行的 OSPF 进程号 1，区域 0 的网段 172.17.1.0/24、192.168.0.0/24 和 192.168.1.0/24。
- SwitchA 上负载分担数目为 1。
- SwitchC 的等价路由优先级权值为 1。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 OSPF 的基本功能（请参见举例**配置 OSPF 基本功能**）
4. 在 SwitchA 上取消负载分担配置

```
[SwitchA] ospf
[SwitchA-ospf-1] maximum load-balancing 1
[SwitchA-ospf-1] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
        10.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
        10.1.2.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      172.16.1.0/24  Direct  0    0           D   172.16.1.1      Vlanif50
      172.16.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      172.17.1.0/24  OSPF    10   3           D   10.1.1.2        Vlanif10
      192.168.0.0/24 OSPF    10   2           D   10.1.1.2        Vlanif10
      192.168.1.0/24 OSPF    10   2           D   10.1.2.2        Vlanif20
```

从路由表中可以看出，当配置负载分担最大等价路由条数为 1 后，到达目标网段 172.17.1.0 的下一跳为 10.1.1.2。

版权所有 © 华为技术有限公司

说明

由于 OSPF 对等价路由下一跳的选择是随机的，所以上面例子中 10.1.1.2 被选为最优下一跳。

5. 在 SwitchA 上恢复负载分担路由的缺省数量

```
[SwitchA] ospf
[SwitchA-ospf-1] undo maximum load-balancing
[SwitchA-ospf-1] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
        10.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
        10.1.2.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       172.16.1.0/24 Direct  0    0           D   172.16.1.1      Vlanif50
      172.16.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      172.17.1.0/24  OSPF    10   3           D   10.1.1.2        Vlanif10
                     OSPF    10   3           D   10.1.2.2        Vlanif20
    192.168.0.0/24   OSPF    10   2           D   10.1.1.2        Vlanif10
    192.168.1.0/24   OSPF    10   2           D   10.1.2.2        Vlanif20
```

从路由表可以看出，当取消负载分担条数设置即恢复缺省配置后，由于最大等价路由条数的缺省值为 4，因此 SwitchA 的两个下一跳 10.1.1.2（SwitchB）和 10.1.2.2（SwitchC）均成为有效路由。

6. 在 SwitchA 上配置等价路由优先级（可选配置）

如果不希望 SwitchB 和 SwitchC 形成负载分担，可以配置等价路由优先级，指定下一跳。

```
[SwitchA] ospf
[SwitchA-ospf-1] nexthop 10.1.2.2 weight 1
[SwitchA-ospf-1] quit
```

查看 SwitchA 的路由表

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
       10.1.2.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.16.1.0/24 Direct  0  0        D       172.16.1.1      Vlanif50
     172.16.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.17.1.0/24  OSPF    10   3           D   10.1.2.2        Vlanif20
    192.168.0.0/24  OSPF    10   2           D   10.1.1.2        Vlanif10
    192.168.1.0/24  OSPF    10   2           D   10.1.2.2        Vlanif20
```

从路由表中可以看出，当配置等价路由的优先级后，由于下一跳为 10.1.2.2（SwitchC）的优先级（权值为 1）高于下一跳为 10.1.1.2（SwitchB）的优先级，所以 OSPF 优先选择下一跳为 10.1.2.2 为唯一最优路由。

版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 50
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 50
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
sysname SwitchB
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 30
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
#
interface Vlanif40
 ip address 192.168.1.1 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 40 60
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
#
interface Vlanif40
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif60
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 60
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```

5.5 OSPFv3 配置

OSPFv3 是 OSPF Version 3 的简称，通过组建 OSPFv3 网络，在自治域内发现并计算路由信息。OSPFv3 可以应用于大规模网络，最多可支持几百台交换机。

5.5.1 OSPFv3 概述

OSPFv3 使用了与 OSPFv2 相同的基本实现机制，但并不兼容 OSPFv2。

OSPFv3 是 OSPF 版本 3 的简称，主要提供对 IPv6 的支持，遵循的标准为 RFC2740（OSPF for IPv6）。

OSPFv3 和 OSPFv2 在很多方面是相同的：

- Router ID，Area ID，LSA Link State ID 仍然是 32 位的。
- 相同类型的报文：Hello 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。
- 相同的邻居发现机制和邻接（Adjacency）形成机制。

版权所有 © 华为技术有限公司

- 相同的 LSA 扩散（Flooding）机制和老化（Aging）机制。
- 基本相同的 LSA 类型。

OSPFv3 和 OSPFv2 的不同主要有：

- OSPFv3 是基于链路（Link）运行，OSPFv2 是基于网段（Network）运行。
- OSPFv3 在同一条链路上可以运行多个实例。
- OSPFv3 的拓扑关系和 IPv6 地址前缀没有关系。
- 使用 IPv6 的链路本地（Link-local）地址标识邻接的邻居。
- 新增的 3 种不同的 LSA 扩散范围。

5.5.2 AC6605 支持的 OSPFv3 特性

AC6605 中支持的 OSPFv3 特性包括：多进程。

在 AC6605 目前的实现中，支持以下 OSPFv3 特性：

- 支持 RFC2740 规定的基本特性；
- 支持 OSPFv3 STUB 区域；
- 支持 OSPFv3 多进程（Multi-Process），可以在一台交换机上运行多个 OSPFv3 进程；

5.5.3 配置 OSPFv3 基本功能

只有配置了基本功能，才可组建 OSPFv3 网络。

建立配置任务

在各项配置任务中，必须先启动 OSPFv3，指定接口与区域号后，才能配置其它的功能特性。

应用环境

配置 OSPFv3 时，必须先启动 OSPFv3 进程，并指定 Router ID，之后其它的功能才能配置或生效。

在各项配置任务中，必须先启动 OSPFv3，指定接口与区域号后，才能配置其它的功能特性。而配置与接口相关的功能特性不受 OSPFv3 是否使能的限制。

前置任务

在配置 OSPFv3 的基本功能之前，需完成以下任务：

- 各相邻节点网络层可达
- 使能 IPv6 能力

数据准备

在配置 OSPFv3 的基本功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	Router ID
2	OSPFv3 进程号
3	需要使能 OSPFv3 的接口及其所属区域

启动 OSPFv3

创建 OSPFv3 进程是配置所有 OSPFv3 特性的首要步骤。通过创建 OSPFv3 进程，还可以手工指定交换机的 Router ID。

背景信息

OSPFv3 支持多进程，一台交换机上启动的多个 OSPFv3 进程之间由不同的进程号区分。OSPFv3 进程号在启动 OSPFv3 时进行设置，它只在本地有效，不影响与其它交换机之间的报文交换。

Router ID 是一个 32 比特无符号整数，采用 IPv4 地址形式，是一台交换机在自治系统中的唯一标识。OSPFv3 的 Router ID 必须手工配置，如果没有配置 ID 号，OSPFv3 无法正常运行。

手工配置 Router ID 时，必须保证自治系统中任意两台交换机的 Router ID 都不相同。如果在同一台交换机上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。

为保证 OSPFv3 运行的稳定性，在进行网络规划时，应确定交换机 ID 的划分并手工配置。

请在需要运行 OSPFv3 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospfv3** [*process-id*]，启动 OSPFv3，进入 OSPFv3 视图。

步骤 3 执行命令 **router-id** *router-id*，配置 Router ID。

----结束

在接口上使能 OSPFv3

由于接口多实例化，所以在将接口使能到 OSPFv3 时，需要指定是哪个接口实例被使能到 OSPFv3 进程中。

背景信息

在系统视图使能 OSPFv3 后，需要在接口使能 OSPFv3。

由于接口多实例化，所以在将接口使能到 OSPFv3 时，需要指定是哪个接口实例被使能到 OSPFv3 进程中，如果不指定实例 ID，则缺省为 0。建立邻居的接口上使能的实例必须相同。

版权所有 © 华为技术有限公司

请在需要运行 OSPFv3 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id* ，进入 VLANIF 接口视图。

步骤 3 （可选）执行命令 **ospfv3 network-type** { **broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p** } [**instance** *instance-id*]，配置接口的网络类型。

当接口支持多实例化，在将接口使能到 OSPFv3 时，必须指定是哪个接口实例被使能到 OSPFv3 进程中，即必须指定 *instance-id*。如果不指定实例 ID，则缺省为 0，会出现配置的接口的网络类型与实际接口的网络类型不匹配的情况。此时该步骤为必选步骤。

步骤 4 执行命令 **ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]，在 VLANIF 接口上使能 OSPFv3。

区域 ID 可以采用十进制整数或 IPv4 地址形式输入，但显示时使用 IPv4 地址形式。

----结束

进入 OSPFv3 区域视图

OSPFv3 协议通过将自治系统划分成不同的区域，和区域中指定运行 OSPFv3 协议的接口和接口所属的区域，达到在自治区域中发现并计算路由的目的。

背景信息

在配置同一区域内的 OSPFv3 交换机时，应注意：大多数配置数据都应该对区域统一考虑，否则可能会导致相邻交换机之间无法交换信息，甚至导致路由信息的阻塞或者产生路由环。

请在需要运行 OSPFv3 协议的每台交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospfv3** [*process-id*]，进入 OSPFv3 视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPFv3 区域视图。

区域 ID 可以采用十进制整数或 IPv4 地址形式输入，但显示时使用 IPv4 地址形式。

OSPFv3 的区域不能直接删除，当区域视图下的所有配置都删除，且该区域中相关接口的状态都为 DOWN，此区域就会被系统自动删除。

----结束

检查配置结果

OSPFv3 基本功能配置成功后，您可以查看到概要、LSDB、邻居和 OSPFv3 路由表信息。

前提条件

已经完成 OSPFv3 基本功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display ospfv3** [*process-id*]命令查看 OSPFv3 进程的概要信息。
- 使用 **display ospfv3 interface** [**area** *area-id*] [*interface-type interface-number*]命令查看 OSPFv3 接口信息。
- 使用以下命令查看 OSPFv3 的 LSDB 信息:
  - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** } [*link-state-id*]]
  - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- 使用 **display ospfv3** [*process-id*] [**area** *area-id*] **peer** [*interface-type interface-number* [**verbose**] | *neighbor-id*]命令查看 OSPFv3 邻居信息。
- 使用以下命令来查看 OSPFv3 路由表信息：
  - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes**]
- 使用 **display ospfv3** [*process-id*] **path** 命令查看 OSPFv3 的路径信息。

----结束

5.5.4 建立或维持 OSPFv3 邻居或邻接关系

通过建立、维持 OSPFv3 邻居或邻接关系，可以组建 OSPFv3 网络。

建立配置任务

在接口上配置的各种参数要和邻接交换机的参数保持一致。

应用环境

在实际应用中，建立或维持 OSPFv3 邻居关系是组建 OSPFv3 网络的重要前提，通过本节的配置，你可以：

- 通过改变 OSPFv3 报文的定时器，可以调整 OSPFv3 网络的收敛速度以及协议报文带来的网络负荷。
- 通过配置 OSPFv3 重传限制 RL-OSPF（Retransmission Limitation for OSPF）可以实现在 OSPFv3 重传报文时，如果超过了设定的重传次数，OSPFv3 将断开邻居，避免在邻居收不到报文的情况下，一直重传造成的死循环。
- 通过调整 LSA 更新和接收的时间间隔，可以提高 OSPFv3 网络的收敛速度。

前置任务

在建立或维持 OSPFv3 邻居或邻接关系之前，需完成以下任务：

- 使能 IPv6 能力
- **配置 OSPFv3 基本功能**。

数据准备

在建立或维持 OSPFv3 邻居或邻接关系之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	发送 Hello 报文的时间间隔
2	相邻交换机间失效时间
3	相邻交换机重传 LSA 的时间间隔
4	LSA 传送延迟时间

配置接口发送 Hello 报文的时间间隔

通过调整 OSPFv3 邻居之间的 Hello 定时器的时间间隔，可以改变邻居建立的速度，从而影响网络收敛的速度。

背景信息

Hello 报文周期性地被发送至邻居交换机，用于发现与维持邻居关系、选举 DR 与 BDR。根据 RFC2328 的规定，要保持网络邻居间的 Hello 时间间隔一致。需要注意的是，Hello 定时器的值与路由收敛速度、网络负荷大小成反比。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospfv3 timer hello** *interval* [**instance** *instance-id*]，配置接口发送 Hello 报文的时间间隔。

----结束

配置相邻交换机失效的时间

在相邻交换机失效时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。

背景信息

在一定时间间隔内，如果交换机未收到对方的 Hello 报文，则认为对端交换机失效，这个时间间隔被称为相邻交换机间的失效时间。在同一接口上交换机的失效时间应至少为 Hello 间隔时间的 4 倍。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **ospfv3 timer dead** *interval* [**instance** *instance-id*]，配置相邻交换机间失效时间。

----结束

检查配置结果

OSPFv3 邻居或邻接关系稳定后，您可以查看到运行 OSPFv3 的接口和邻居信息。

前提条件

已经完成建立或维持 OSPFv3 邻居或邻接关系的所有配置。

操作步骤

- 使用 **display ospfv3 interface** [**area** *area-id*] [*interface-type interface-number*]命令查看 OSPFv3 接口信息。

----结束

5.5.5 配置 OSPFv3 的区域属性

OSPFv3 支持 Stub 区域和虚连接的配置，其原理及应用环境与 OSPFv2 相同。

建立配置任务

STUB 区域是一种可选的配置属性，但并不是每个区域都符合配置的条件。通常来说，STUB 区域位于自治系统的边界，并且只有一个 ABR 的非骨干区域。

应用环境

OSPFv3 划分区域后，可以减少网络中 LSA 的数量，OSPFv3 的扩展性也得以增强。对于位于 AS 边缘的一些非骨干区域，为了更多的缩减其路由表规模和降低 LSA 的数量，可以将它们配置为 STUB 区域。

前置任务

在配置 OSPFv3 的区域特性之前，需完成以下任务：

- 使能 IPv6 能力
- **配置 OSPFv3 基本功能**

数据准备

在配置 OSPF 区域之前，需要准备以下数据。

序号	数据
1	确定哪些区域需要配置为 STUB 区域
2	发布到 STUB 区域缺省路由的开销值

版权所有 © 华为技术有限公司

配置 OSPFv3 的 Stub 区域

Stub 区域是一种特定的区域，Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，LSA 的数量大大减少。

背景信息

请在运行 OSPFv3 协议的 Stub 域内的每台交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospfv3** [*process-id*]，进入 OSPFv3 视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPFv3 区域视图。

步骤 4 执行命令 **stub** [**no-summary**]，配置一个区域为 Stub 区域。

----结束

检查配置结果

成功配置 OSPFv3 的区域属性后，您可以查看到 LSDB、OSPFv3 路由表和虚连接信息。

前提条件

已经完成 OSPFv3 区域属性的所有配置。

操作步骤

- 使用以下命令查看 OSPFv3 的 LSDB 信息:
  - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** } [*link-state-id*]]
  - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- 使用以下命令来查看 OSPFv3 路由表信息：
  - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes**]

----结束

5.5.6 配置 OSPFv3 的路由属性

通过配置 OSPFv3 的路由属性改变 OSPFv3 的选路策略，以满足复杂网络环境中的需要。

建立配置任务

在配置 OSPFv3 的路由属性前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用背景

在实际应用中，可以通过配置 OSPFv3 的路由属性改变 OSPFv3 的选路策略，以满足复杂网络环境中的需要。通过本节的配置过程，你可以：

- 设置 OSPFv3 接口的开销值；
- 使用多条等价路由进行负载分担。

前置任务

在配置 OSPFv3 的路由属性之前，需完成以下任务：

- 使能 IPv6 能力
- **配置 OSPFv3 基本功能**

数据准备

在配置 OSPFv3 的路由属性之前，需要准备以下数据。

序号	数据
1	链路开销
2	最大等价路由条数

配置 OSPFv3 接口的开销值

OSPFv3 会根据该接口的带宽自动计算其链路开销值，但也可以通过命令配置。

背景信息

用户可以在不同接口上配置 OSPFv3 的链路开销值，从而影响路由的计算。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospfv3 cost** *cost* [**instance** *instance-id*]，设置 OSPFv3 接口的开销。

缺省情况下，OSPFv3 接口的链路开销为 1。

----结束

检查配置结果

配置 OSPFv3 的路由属性后，您可以查看到运行 OSPFv3 的接口、LSDB 和 OSPFv3 路由表信息。

版权所有 © 华为技术有限公司

前提条件

已经完成 OSPFv3 路由属性的所有配置。

操作步骤

- 使用 **display ospfv3 interface** [**area** *area-id*] [*interface-type interface-number*]命令查看 OSPFv3 接口信息。
- 使用以下命令查看 OSPFv3 的 LSDB 信息：
  - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** } [*link-state-id*]]
  - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- 使用以下命令来查看 OSPFv3 路由表信息：
  - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes**]

----结束

5.5.7 控制 OSPFv3 的路由信息

控制 OSPF 路由信息包括路由聚合，对路由的过滤和引入外部路由。

建立配置任务

在控制 OSPFv3 的路由信息前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

通过本节的配置，可以控制 OSPFv3 的路由信息的发布与接收，并引入外部路由。

前置任务

在控制 OSPFv3 的路由信息之前，需完成以下任务：

- 使能 IPv6 能力
- **配置 OSPFv3 基本功能**

数据准备

在控制 OSPFv3 的路由信息之前，需要准备以下数据。

序号	数据
1	聚合后的 IPv6 路由前缀
2	对路由过滤时所应用的过滤列表编号或名称
3	OSPFv3 接口的链路开销

版权所有 © 华为技术有限公司

序号	数据
4	可用的最大等价路由条数
5	要引入的外部路由名称、进程号、开销值

配置 OSPFv3 路由聚合

ABR 将具有相同前缀的路由聚合成一条 LSA 并发布到其他区域，这样可以大幅度减少 LSDB 的规模。

背景信息

如果该区域中存在多个连续的网段，则可以使用 **abr-summary** 命令将它们聚合成一个网段，ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其它区域中 LSDB 的规模。

操作步骤

- 在 ABR 上配置路由聚合

  请在运行 OSPFv3 协议的 ABR 上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospfv3** [*process-id*]，进入 OSPFv3 视图。
  3. 执行命令 **area** *area-id*，进入 OSPFv3 区域视图。
  4. 执行命令 **abr-summary** *ipv6-address prefix-length* [**not-advertise**]，配置 OSPFv3 区域路由聚合。

     如果在命令中使用了关键字 **not-advertise**，则属于这一网段的路由信息将不会被发布出去。

----结束

配置 OSPFv3 对接收的路由进行过滤

通过路由设置路由信息的过滤条件，只有通过过滤的信息才能被发布或接收。

背景信息

OSPFv3 接收到 LSA 后，可以根据一定的过滤条件来决定是否将计算后得到的路由信息加入到本地路由表中。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospfv3** [*process-id*]，进入 OSPFv3 视图。

步骤 3 执行命令 **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**，配置对接收的路由信息进行过滤。

版权所有 © 华为技术有限公司

filter-policy 命令只对 OSPFv3 计算出来的路由进行过滤，没有通过过滤的路由将不被加入到本地路由表中，从而不能指导转发。

----结束

配置 OSPFv3 引入外部路由

通过引入其他路由协议路由，可以扩充 OSPFv3 路由信息。

背景信息

由于 OSPFv3 是基于链路状态的路由协议，不能直接对发布的 LSA 进行过滤，所以只能在 OSPFv3 引入路由时进行过滤，只有符合条件的路由才能变成 LSA 发布出去。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospfv3** [*process-id*]，进入 OSPFv3 视图。

步骤 3 执行命令 **default** { **cost** *cost* | **tag** *tag* | **type** *type* } *，配置引入路由的缺省开销值。

步骤 4 执行命令 **import-route** *protocol* [*process-id*] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] *，引入外部路由信息。

步骤 5 （可选）执行命令 **default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] *，将缺省路由通告到 OSPFv3 路由区域。

步骤 6 （可选）执行命令 **filter-policy** { *acl6-number* |**acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]，对引入的外部路由信息进行过滤。

在 OSPFv3 交换机上配置 **import-route** 命令引入外部路由信息后，这台 OSPFv3 交换机就成为 ASBR。

用户可以通过指定 *protocol* 对特定的某一种路由信息进行过滤。如果没有指定 *protocol*，则 OSPFv3 将对所有引入的路由信息进行过滤。

说明

filter-policy 命令只对本机使用 **import-route** 命令引入的路由（即当本机 OSPFv3 交换机成为 ASBR 时）起作用，它在 OSPF 引入路由时对其进行过滤，被过滤掉的路由也就不会变成 LSA 被 OSPF 发布出去。如果没有配置 **import-route** 命令来引入其它外部路由（包括不同进程的 OSPFv3 路由），则 **filter-policy** 命令失效。

----结束

检查配置结果

控制 OSPFv3 的路由信息后，您可以查看到运行 OSPFv3 的接口、LSDB 和 OSPFv3 路由表信息。

前提条件

已经完成控制 OSPFv3 路由信息的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用以下命令查看 OSPFv3 的路由聚合信息：
  - **display ospfv3** [*process-id*] **abr-summary-list** [*ipv6-address prefix-length*]
- 使用以下命令查看 OSPFv3 的 LSDB 信息：
  - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** } [*link-state-id*]]
  - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- 使用以下命令来查看 OSPFv3 路由表信息：
  - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes**]

----结束

5.5.8 调整和优化 OSPFv3 网络

在特殊的网络环境中配置 OSPFv3 的一些特性功能，对 OSPFv3 网络的性能进行调整和优化。

建立配置任务

在调整和优化 OSPFv3 网络前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

通过改变 OSPFv3 的报文定时器，可以调整 OSPFv3 网络的收敛速度以及协议报文带来的网络负荷。在一些低速链路上，需要考虑接口传送 LSA 的延迟时间。通过调整 SPF 计算间隔时间，可以抑制由于网络频繁变化带来的资源消耗问题。

对于广播网，通过配置接口的 DR 优先级来影响 DR/BDR 的选择。

前置任务

在调整和优化 OSPFv3 网络之前，需完成以下任务：

- 使能 IPv6 能力
- **配置 OSPFv3 基本功能**

数据准备

在调整和优化 OSPFv3 网络之前，需要准备以下数据。

序号	数据
1	OSPFv3 报文定时器的值
2	SPF 定时器的值

版权所有 © 华为技术有限公司

序号	数据
3	接口的 DR 优先级

配置接口的 DR 优先级

当网络类型为广播网或 NBMA 类型时，可以通过配置接口的 DR 优先级来影响网络中 DR/BDR 的选择。

背景信息

交换机接口的 DR 优先级将影响接口在选举 DR 时所具有的资格，优先级为 0 的交换机不会被选举为 DR 或 BDR。

请在运行 OSPFv3 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **ospfv3 dr-priority** *priority* [**instance** *instance-id*]，设置接口在选举 DR 时的优先级。

----结束

后续处理

改变优先级后，可以利用下面两种方法重新进行 DR/BDR 的选择，但是这会导致交换机之间的 OSPFv3 邻接关系中断，一般情况下不推荐使用。

- 重启所有交换机。
- 在建立了 OSPFv3 邻居的接口上配置 **shutdown**/**undo shutdown** 命令。

检查配置结果

调整和优化 OSPFv3 网络后，您可以查看到运行 OSPFv3 的接口、LSDB 和 OSPFv3 路由表信息。

前提条件

已经完成调整和优化 OSPFv3 网络的所有配置。

操作步骤

- 使用 **display ospfv3 interface** [**area** *area-id*] [*interface-type interface-number*]命令查看 OSPFv3 接口信息。
- 使用以下命令查看 OSPFv3 的 LSDB 信息：
  - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-*

版权所有 © 华为技术有限公司

router-id] | { **inter-prefix** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** } [*link-state-id*]]

- **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]

- 使用以下命令来查看 OSPFv3 路由表信息：
  - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes**]

----结束

5.5.9 配置举例

介绍 OSPFv3 的各种组网举例。

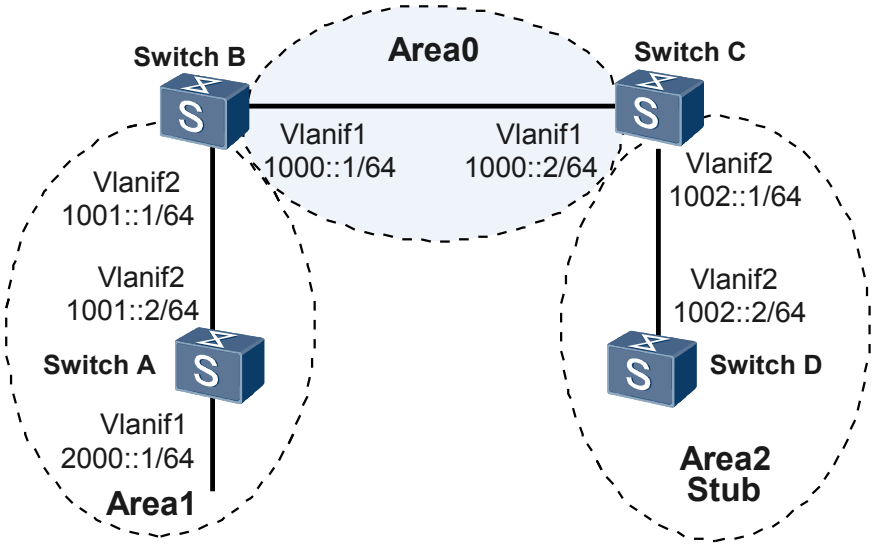
配置 OSPFv3 区域示例

组网需求

如图 5-15 所示，所有的交换机都运行 OSPFv3，整个自治系统划分为 3 个区域。其中 SwitchB 和 SwitchC 作为 ABR 来转发区域之间的路由。

要求将 Area2 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

图 5-15 配置 OSPFv3 区域组网图



配置思路

采用如下的思路配置 OSPFv3 区域：

1. 在各交换机上使能 OSPFv3 的基本功能。

版权所有 © 华为技术有限公司

2. 配置 Area2 为 Stub 区域（需要在 Area2 内所有的交换机上配置 **Stub** 命令），查看 SwitchD 的 OSPFv3 路由表信息。
3. 配置 Area2 为 Totally Stub 区域，查看 SwitchD 的 OSPFv3 路由表信息。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 的 router id 1.1.1.1，所在的区域号 Area1。
- SwitchB 的 router id 2.2.2.2，所在的区域号 Area0 和 Area1。
- SwitchC 的 router id 3.3.3.3，所在的区域号 Area0 和 Area2。
- SwitchD 的 router id 4.4.4.4，所在的区域号 Area2。

操作步骤

步骤 1 配置各接口的 IPv6 地址（略）

步骤 2 配置 OSPFv3 基本功能

配置 SwitchA。

```
[SwitchA] ipv6
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlanif 1
[SwitchA-Vlanif1] ospfv3 1 area 1
[SwitchA-Vlanif1] quit
[SwitchA] interface vlanif 2
[SwitchA-Vlanif2] ospfv3 1 area 1
[SwitchA-Vlanif2] quit
```

配置 SwitchB。

```
[SwitchB] ipv6
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlanif 1
[SwitchB-Vlanif1] ospfv3 1 area 0
[SwitchB-Vlanif1] quit
[SwitchB] interface vlanif 2
[SwitchB-Vlanif2] ospfv3 1 area 1
[SwitchB-Vlanif2] quit
```

配置 SwitchC。

```
[SwitchC] ipv6
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlanif 1
[SwitchC-Vlanif1] ospfv3 1 area 0
[SwitchC-Vlanif1] quit
[SwitchC] interface vlanif 2
[SwitchC-Vlanif2] ospfv3 1 area 2
[SwitchC-Vlanif2] quit
```

配置 SwitchD。

```
[SwitchD] ipv6
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
```


版权所有 © 华为技术有限公司

```
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlanif 2
[SwitchD-Vlanif2] ospfv3 1 area 2
[SwitchD-Vlanif2] quit
```

查看 SwitchB 的 OSPFv3 邻居状态。

```
[SwitchB] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/ -         00:00:34    Vlanif2           0
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
3.3.3.3           1   Full/ -         00:00:32    Vlanif1           0
```

查看 SwitchC 的 OSPFv3 邻居状态。

```
[SwitchC] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/ -         00:00:37    Vlanif1           0
OSPFv3 Area (0.0.0.2)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
4.4.4.4           1   Full/ -         00:00:33    Vlanif2           0
```

查看 SwitchD 的 OSPFv3 路由表信息。

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                                 Metric
     Next-hop
  IA 1000::/64                                   2
          via FE80::1572:0:5EF4:1, Vlanif1
  IA 1001::/64                                   3
          via FE80::1572:0:5EF4:1, Vlanif1
     1002::/64                                   1
          directly-connected, Vlanif1
  IA 2000::/64                                   4
          via FE80::1572:0:5EF4:1, Vlanif1
```

步骤 3 配置 Stub 区域

配置 SwitchD 的 Stub 区域。

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
[SwitchD-ospfv3-1-area-0.0.0.2] quit
```

配置 SwitchC 的 Stub 区域，设置发送到 Stub 区域的缺省路由的开销为 10。

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
[SwitchC-ospfv3-1-area-0.0.0.2] quit
```

查看 SwitchD 的 OSPFv3 路由表信息，可以看到路由表中多了一条缺省路由，它的开销值为直连路由的开销和所配置的开销值之和。

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                                 Metric
     Next-hop
  IA ::/0                                       11
          via FE80::1572:0:5EF4:1, Vlanif1
  IA 1000::/64                                   2
```


版权所有 © 华为技术有限公司

```
          via FE80::1572:0:5EF4:1, Vlanif1
  IA 1001::/64                                3
          via FE80::1572:0:5EF4:1, Vlanif1
     1002::/64                                1
          directly-connected, Vlanif1
  IA 2000::/64                                4
          via FE80::1572:0:5EF4:1, Vlanif1
```

步骤 4 配置 Totally Stub 区域

配置 SwitchC，设置 Area2 为 Totally Stub 区域。

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
[SwitchC-ospfv3-1-area-0.0.0.2] quit
```

步骤 5 验证配置结果

查看 SwitchD 的 OSPFv3 路由表，可以发现路由表项数目减少了，其他非直连路由都被抑制，只有缺省路由被保留。

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                              Metric
     Next-hop
  IA ::/0                                     11
          via FE80::1572:0:5EF4:1, Vlanif1
     1002::/64                                1
          directly-connected, Vlanif1
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 ipv6
#
interface Vlanif1
 ipv6 address 2000::1/64
 ospfv3 1 area 0.0.0.1
#
interface Vlanif2
ipv6 address 1001::2/64
 ospfv3 1 area 0.0.0.1
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 ipv6
#
interface Vlanif1
ipv6 address 1000::1/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif2
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.1
```


版权所有 © 华为技术有限公司

```
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
 area 0.0.0.1
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 ipv6
#
interface Vlanif1
ipv6 address 1000::2/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif2
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.2
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
 area 0.0.0.2
  stub no-summary
  default-cost 10
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 ipv6
#
interface Vlanif2
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.2
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.2
  stub
#
return
```

5.6 IS-IS 配置

介绍 IS-IS 协议的基本原理、配置过程和配置举例。

5.6.1 IS-IS 基本概念

IS-IS 属于内部网关协议，用于自治系统内部。IS-IS 是一种链路状态协议，使用最短路径优先算法进行路由计算。

IS-IS 最初是国际标准化组织 ISO（the International Organization for Standardization）为它的无连接网络协议 CLNP（ConnectionLess Network Protocol）设计的一种动态路由协议。

为了提供对 IP 的路由支持，IETF 在 RFC1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中，称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

版权所有 © 华为技术有限公司

IS-IS 属于内部网关协议 IGP（Interior Gateway Protocol），用于自治系统内部。IS-IS 是一种链路状态协议，使用最短路径优先 SPF（Shortest Path First）算法进行路由计算，与 OSPF 协议有很多相似之处。

IS-IS 区域

为了支持大规模的路由网络，IS-IS 在路由域内采用两级的分层结构。一个大的路由域被分成一个或多个区域（Areas）。区域内的路由通过 Level-1 路由器管理，区域间的路由通过 Level-2 路由器管理。

图 5-16 所示为一个运行 IS-IS 协议的网络，它与 OSPF 的多区域网络拓扑结构非常相似。其中 Area1 是骨干区域，该区域中的所有设备均是 Level-2 路由器。另外 4 个区域为非骨干区域，它们都通过 Level-1-2 路由器与骨干路由器相连。

图 5-16 IS-IS 拓扑结构图之一

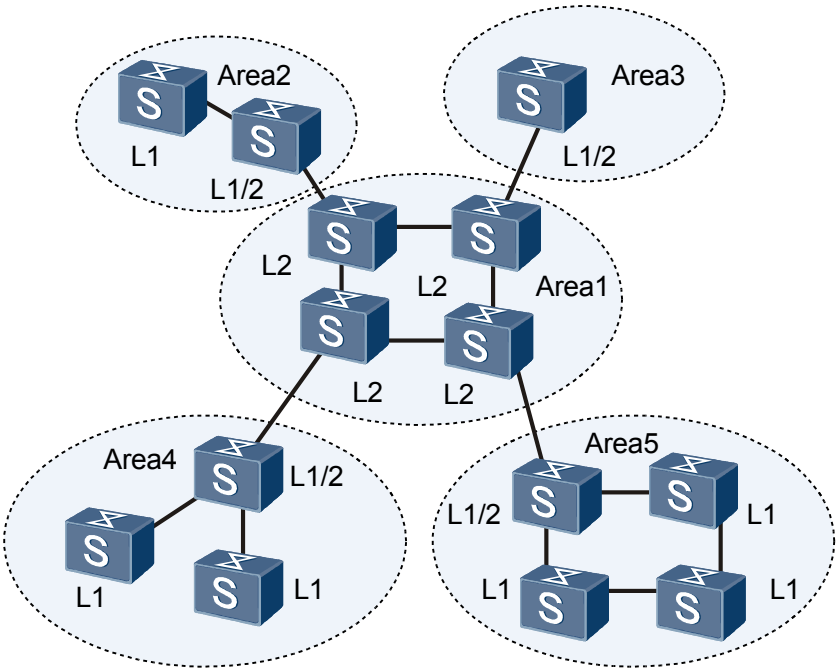
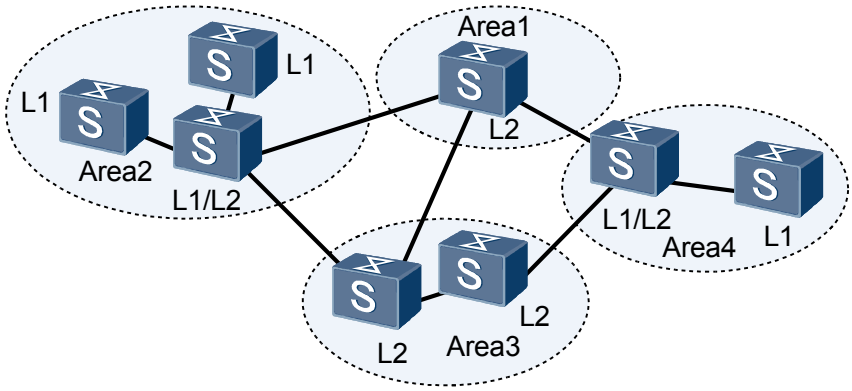


图 5-17 是 IS-IS 的另外一种拓扑结构图。其中 Level-1-2 路由器不只用来连接 Level-1 和 Level-2 路由器，而且还与其他 Level-2 路由器一起构成了 IS-IS 的骨干网。在这个拓扑中，并没有规定哪个区域是骨干区域。所有 Level-2 路由器构成了 IS-IS 的骨干网，他们可以属于不同的区域，但必须是连续的。

版权所有 © 华为技术有限公司

图 5-17 IS-IS 拓扑结构图之二



说明

IS-IS 的骨干网（Backbone）指的不是一个特定的区域。

这种组网方案也体现出 IS-IS 与 OSPF 的不同点。在 OSPF 中，区域之间的路由需要通过骨干区域转发，只有在同一个区域内才使用 SPF 算法。而 IS-IS 不论是 Level-1 还是 Level-2 路由，都采用 SPF 算法，分别生成最短路径树 SPT（Shortest Path Tree）。

网络类型

IS-IS 只支持两种类型的网络，根据物理链路不同可分为：

- 广播链路：如 Gigabitethernet、Token-Ring 等。
- 点到点链路：如 PPP、HDLC 等。

说明

对于 NBMA（Non-Broadcast Multi-Access）网络，如 ATM，需对其配置子接口，并注意子接口类型不能为 P2MP。IS-IS 不能在点到多点链路 P2MP（Point to MultiPoint）上运行。

5.6.2 AC6605 支持的 IS-IS 特性

AC6605 支持的 IS-IS 特性包括：多实例和多进程、热备份、多拓扑、本地 MT、GR、TE 与 DS-TE、管理标记、LSP 分片扩展、动态主机名交换、快速收敛、BFD 和三次握手机制。

多实例和多进程

为了方便管理，提高控制效率，IS-IS 支持多进程多实例和特性。

- 多进程

  为一个指定的 IS-IS 进程关联一组接口，从而保证该进程所有操作都仅限于这一组接口。这样，就可以实现一台交换机有多个 IS-IS 进程，每个进程负责唯一的一组接口。

- 多实例

  对于支持 VPN 的交换机，每个 IS-IS 进程都与一个指定的 VPN 实例相关联，所有附加到该进程的接口都应与这个 VPN 实例相关联。

版权所有 © 华为技术有限公司

IS-IS 热备份

具有分布式结构的交换机可支持 IS-IS 热备份 HSB（Hot Standby）特性。IS-IS 将需要备份的数据从主用主控板 AMB（Active Main Board）备份到备用主控板 SMB（Standby Main Board）。无论何时主用主控板出现故障，备用主控板都会变成激活状态，接替工作，保证 IS-IS 能够正常运行。

IS-IS 支持的 HSB 在运行过程中保持 AMB 和 SMB 上的 IS-IS 配置信息一致。当发生主备板切换时，新主板上的 IS-IS 进行 GR（Graceful Restart），重新向邻居发送建立邻居的请求，同步 LSDB 数据库，从而保证流量不受影响。

说明

IS-IS 热备份和 GR 的详细配置请参考《AC6605 无线接入控制器 配置指南-可靠性》。

多拓扑

IS-IS 对 IPv6 的实现存在如下限制：在 SPF 计算中，IPv4 和 IPv6 的混合拓扑被看成是一个集成的拓扑，这就要求所有的 IPv6 和 IPv4 的拓扑信息必须一致。

但是，IPv4 和 IPv6 协议在网络中的部署可能不一致，所以 IPv6 和 IPv4 的拓扑信息可能不同。如果在一个集成拓扑中进行 SPF 计算，选用同样的最短路径转发报文，就会导致不支持 IPv6 的交换机收到 IPv6 报文时因无法转发而将其丢弃。

多拓扑 MT（Multi-Topology）用来解决上述问题。IS-IS MT 是指在一个 IS-IS 域内运行多个独立的 IP 拓扑，例如 IPv4 和 IPv6 拓扑，不同拓扑运行各自的 SPF 计算。这有利于在路由计算中根据实际组网情况来单独考虑 IPv4 和 IPv6 网络，实现网络的相互屏蔽。

本地组播拓扑

当网络中同时部署了组播和 MPLS TE-Tunnel 时，组播的功能可能会受到 TE-Tunnel 的影响，导致业务不可用。

因为在 TE-Tunnel 上配置了 IGP Shortcut 后，IGP 计算出来的路由的出接口可能不再是实际的物理接口，而是 TE-Tunnel 接口。这样，交换机根据到达组播源地址的单播路由，从 TE-Tunnel 接口发送组播加入报文，那么被 TE-Tunnel 跨越的交换机就无法感知到该组播加入报文，因而不会建立组播转发表项。由于 TE-Tunnel 是单向的，从组播源发出的组播数据会直接通过物理接口发送到这些被跨越的交换机，但因为这些交换机上并没有组播转发表项，导致组播数据报文丢弃，从而造成业务不可用。

使能本地组播拓扑（Local Multicast-Topology）后，可以为组播创建单独的 MIGP 路由表，指导组播报文正确的转发。

说明

有关本地 MT 的详细介绍请参见《AC6605 无线接入控制器 特性描述-IP 路由》中“IS-IS”。

IS-IS GR

Graceful Restart 指的是平缓重启交换机 的一种功能，可以保证流量转发不中断，网络不会因为交换机 的短时间重启而引起路由震荡。

若 IS-IS 协议不以 GR 方式重启，会重置 IS-IS 会话，重新生成链路状态协议数据报文 LSP（Link State Protocol Data Unit）和泛洪 LSP，进而在整个区域引发 SPF 计算，引起整个区域的路由震荡和转发中断。IETF 针对这种情况为 IS-IS 制定了 GR 规范（RFC3847），对保留 FIB 表和未保留 FIB 表的协议重启都进行了处理。

版权所有 © 华为技术有限公司

说明

有关 IS-IS GR 的详细介绍请参见《AC6605 无线接入控制器 特性描述-IP 路由》中“IS-IS”。

IS-IS TE

IS-IS TE（Traffic Engineering，流量工程）支持建立和维护 TE 的 LSP（Label Switched Path，标签交换路径）。

MPLS 在构建 CR LSP（Constraint-based Routed LSP，基于约束路由的 LSP）时，需要了解本区域中所有链路的流量属性信息。它可以通过 IS-IS 来获取链路的流量工程信息。

管理标记

管理标记简化了管理，允许在 IS-IS 域中通过 IP 地址前缀发布进行控制。该标记用来携带关于 IP 地址前缀的管理信息，其用途包括控制不同级别和不同区域间的路由引入，各种路由协议，同一交换机上运行的 IS-IS 多实例，以及 TAG 的承载。

管理标记值与某些属性相关联。如果 IS-IS 要发布可达的 IP 地址前缀具有该属性，IS-IS 就会将管理标记加入到该前缀的 IP 可达信息 TLV 中。这样，管理标记就会随着前缀发布到整个路由域。

LSP 分片扩展

当 IS-IS 要发布的 LSP 中的信息量变大时，以同一系统的多个 LSP 分片的形式发布。LSP 分片由 LSP 的 LSP 标识符字段进行标识，这个字段的长度是 1 字节，因此，IS-IS 路由器可产生的分片数最大为 256。

IS-IS LSP 分片扩展特性可使 IS-IS 路由器生成更多的 LSP 分片。该特性可通过使能网络管理器，为交换机配置附加的系统 ID 实现。每个系统 ID 都代表一个虚拟系统，每个虚拟系统都可生成 256 个 LSP 分片。通过增加附加的系统 ID（最多可配置 50 个虚拟系统），IS-IS 路由器可最多生成 13056 个 LSP 分片。

- 相关术语
  - 初始系统（Originating System）

    初始系统是实际运行 IS-IS 协议的交换机。本手册描述的方法允许一个单独的 IS-IS 进程像多个虚拟交换机 一样发布 LSP，而“Originating System”指的是那个“真正”的 IS-IS 进程。
  - 系统 ID（Normal System-ID）

    初始系统的系统 ID。
  - 附加系统 ID（Additional System-ID）

    附加系统 ID 由网络管理器分配。每个附加系统 ID 都允许生成 256 个额外的或扩展的 LSP 分片。附加系统 ID 和普通系统 ID 一样，在整个路由域中必须唯一。
  - 虚拟系统（Virtual System）

    由附加系统 ID 标识的系统，用来生成扩展 LSP 分片。这些分片在其 LSP ID 中携带附加系统 ID。
- 操作模式

  IS-IS 路由器可以在两种模式下运行 LSP 分片扩展特性：
  - mode-1：用于网络中的部分交换机不支持 LSP 分片扩展特性的情况。在该模式下，初始系统向 LSP 中的每个虚拟系统发布一条链路，然后每个虚拟系统也向

版权所有 © 华为技术有限公司

初始系统发布一条链路。这些虚拟系统就好象网络中与初始系统相连的交换机。这种模式有一个局限就是虚拟系统的 LSP 报文只能发布路由信息。

- mode-2：用于网络中所有交换机都支持 LSP 分片扩展特性的情况。在该模式下，网络中所有交换机都知道虚拟系统生成的 LSP 实际属于初始系统，而且对虚拟系统发布的 LSP 报文的链路状态信息没有限制。

动态主机名交换机制

动态主机名交换机制是为了方便对 IS-IS 网络的维护和管理而引入的，它为 IS-IS 路由器提供了一种从主机名到 System ID 映射的服务。这个动态的主机名信息在 LSP 中以一个动态主机名 TLV 的形式发布。

这个机制同时还提供将主机名与广播网中的 DIS（Designated Intermediate System）相关联的服务，并将此信息通过伪节点的 LSP 以动态主机名 TLV 的形式发布出去。

在维护和管理中，使用主机名比使用 System ID 会更直观，也更容易记忆。配置此功能后，当在交换机上使用显示命令查看 IS-IS 相关信息时，看到的是交换机的主机名，而不再是 System ID。

IS-IS 快速收敛

- I-SPF（Incremental SPF）

  I-SPF 是指增量路由计算，它每次只对变化的一部分路由进行计算，而不是对全部路由重新计算。

  在 ISO-10589 中定义使用 Dijkstra 算法进行路由计算。当网络拓扑中有一个节点发生变化时，这种算法需要重新计算网络中的所有节点，计算时间长，占用过多的 CPU 资源，影响整个网络的收敛速度。

  I-SPF 改进了这个算法，除了第一次计算时需要计算全部节点外，每次只计算受影响的节点，而最后生成的最短路径树 SPT 与原来的算法所计算的结果相同，大大降低了 CPU 的占用率，提高了网络收敛速度。

- PRC（Partial Route Calculation）

  部分路由计算 PRC 的原理与 I-SPF 相同，都是只计算变化的那一部分，但 PRC 不需要计算节点路径，而是根据 I-SPF 算出来的 SPT 来更新叶子（路由）。

  在路由计算中，叶子代表路由，节点则代表交换机。如果 I-SPF 计算后的 SPT 改变，PRC 会只处理那个变化的节点上的所有叶子；如果经过 I-SPF 计算后的 SPT 并没有变化，则 PRC 只处理变化的叶子信息。

  比如一个节点使能一个 IS-IS 接口，则整个网络拓扑的 SPT 是不变的，这时 PRC 只更新这个节点的接口路由，从而节省 CPU 占用率。

  PRC 和 I-SPF 配合使用可以将网络的收敛性能进一步提高，它是原始 SPF 算法的改进，所以已经代替了原有的算法。

  说明

  在 AC6605 的实现中，仅使用 I-SPF 和 PRC 作为 IS-IS 路由计算的算法。

- LSP 快速扩散

  按 RFC 协议的实现，当 IS-IS 收到其它交换机 发来的 LSP 时，如果此 LSP 比自己 LSDB 中的 LSP 要新，则是用一个定时器定期将 LSDB 内的 LSP 扩散出去，所以 LSDB 的同步会比较缓慢。

  LSP 快速扩散特性改进了这种方式，配置此特性的交换机收到一个或多个比较新的 LSP 时，在路由计算之前，先将小于指定数目的 LSP 扩散出去，加快 LSDB 的同步过程。这种方式可以提高整个网络的收敛速度。

版权所有 © 华为技术有限公司

- 智能定时器

  改进了路由算法后，如果触发路由计算的间隔较长，同样会影响网络的收敛速度。使用毫秒级定时器可以缩短这个间隔时间，但如果网络变化比较频繁，又会造成过度占用 CPU 资源。SPF 智能定时器既可以对少量的外界突发事件进行快速响应，又可以避免过度的占用 CPU。

  通常情况下，一个正常运行的 IS-IS 网络是稳定的，发生大量的网络变动的几率很小，IS-IS 路由器不会频繁的进行路由计算，所以第一次触发的时间可以设置的非常短（毫秒级）。如果拓扑变化比较频繁，智能定时器会随着计算次数的增加，间隔时间也会逐渐延长，避免占用大量的 CPU 资源。

  与 SPF 智能定时器类似的还有 LSP 生成智能定时器。在 IS-IS 协议中，当 LSP 生成定时器到期时，系统会根据当前拓扑重新生成一个自己的 LSP。原有的实现机制是采用间隔时间定长的定时器，不能同时满足快速收敛和低 CPU 占用率的需要。为此将 LSP 生成定时器也设计成智能定时器，使其可以对于突发事件（如接口 Up/Down）快速响应，加快网络的收敛速度。同时，当网络变化频繁时，智能定时器的间隔时间会自动延长，避免过度占用 CPU 资源。

  说明

  请根据网络的实际情况和交换机 的性能，谨慎配置此类定时器。

BFD for IS-IS

AC6605 支持使用 BFD 对 IS-IS 邻居关系进行检测。BFD 能够快速检测到 IS-IS 邻居间的链路故障，并上报给 IS-IS 协议，从而实现 IS-IS 协议的快速收敛。

说明

由于 IS-IS 只能建立单跳邻居，BFD 只对 IS-IS 邻居间的单跳链路进行检测。

- 静态 BFD

  静态 BFD 是指通过命令行手工配置 BFD 会话参数，包括配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求。

  这种方式的缺点是建立和删除 BFD 会话时都需要手工触发，缺乏灵活性。而且有可能造成人为的配置错误，比如配置了错误的本地标识符或者远端标识符时，BFD 会话将不能正常工作。

  AC6605 支持用静态 BFD for IS-IS 检测 IPv4 网络。

- 动态 BFD

  动态 BFD 会话指的是由路由协议动态触发建立 BFD 会话。

  路由协议在建立了新的邻居关系时，将邻居的参数及检测参数（包括目的地址、源地址等）通告给 BFD，BFD 根据收到的参数建立起会话。动态 BFD 比静态 BFD 更具有灵活性。

  通常情况下，IS-IS 设定发送 Hello 报文的时间间隔为 10 秒，宣告邻居失效的时间即邻居保持时间一般配置为 Hello 报文间隔的 3 倍，所以邻居故障感知时间为秒级，由此可能会出现高速的网络环境中大量报文丢失的问题。

  动态 BFD（Bidirectional Forwarding Detection）能够提供轻负荷、快速（毫秒级）的通道故障检测。使用动态 BFD 并不是代替 IS-IS 协议本身的 Hello 机制，而是配合 IS-IS 协议更快的发现邻居设备或链路出现的故障，并及时通知 IS-IS 重新计算相关路由以便正确指导报文的转发。

  AC6605 支持采用动态 BFD for IS-IS 检测 IPv4 网络。

版权所有 © 华为技术有限公司

说明

有关 BFD for IS-IS 的详细介绍请参见《AC6605 无线接入控制器 特性描述-IP 路由》中“IS-IS”。

三次握手机制（3-Way Handshake）

IS-IS 协议在点到点链路上需要一个可靠的链路层协议。ISO 10589 中的 IS-IS 的 2 次握手机制（2-Way Handshake）使用 Hello 报文来建立相邻交换机间点到点链路的邻接关系。这种机制中，只要交换机收到对端发来的 Hello 报文，就宣布邻居为 Up 状态，建立邻接关系。

这种机制存在明显缺陷。例如，邻接关系建立后，当链路状态反复波动引起 CSNP 报文丢失，导致 LSDB 在一个完整的 LSP 更新周期内不能达到同步；当交换机间存在两条及以上的链路时，如果某条链路上到达对端的单向状态为 Down，而另一条链路同方向的状态为 Up，这样交换机之间还是能建立起邻接关系。SPF 在计算时会使用另一条链路上的参数，这导致没有检测到故障的交换机在转发报文时仍然试图通过状态为 Down 的链路。

三次握手机制解决了上述不可靠点到点链路中存在的问题。这种方式下，交换机只有在知道邻居交换机也接收到它的报文时，才宣布邻居交换机处于 Up 状态，从而建立邻接关系。同时，三次握手机制中使用 32 比特的扩展 Circuit ID，打破了目前由本地 8 比特 Circuit ID 字段限制的 255 个点到点链路。

5.6.3 配置 IS-IS 的基本功能

只有配置了基本功能，才可组建 IS-IS 网络。

建立配置任务

在配置 IS-IS 基本功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

配置 IS-IS 时，必须先启动 IS-IS 进程，指定 NET，并在接口上使能 IS-IS 之后，其它的功能才能配置或生效。

前置任务

在配置 IS-IS 的基本功能之前，需完成以下任务：

- 配置链路层协议。
- 配置接口的网络层地址，使相邻节点网络层可达。

数据准备

在配置 IS-IS 的基本功能之前，需要准备以下数据。

序号	数据
1	进程号

版权所有 © 华为技术有限公司

序号	数据
2	NET
3	交换机及接口的 Level 级别

启动 IS-IS 进程

创建 IS-IS 进程是配置所有 IS-IS 特性的第一步。

背景信息

创建一个 IS-IS 路由进程，并在可能和其他交换机存在关联关系的接口上激活这个路由进程，才可以启动运行 IS-IS 协议。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，使能 IS-IS 路由进程，进入 IS-IS 视图。

参数 *process-id* 用来指定一个 IS-IS 进程。如果不指定参数 *process-id*，则系统默认的进程为 1。IS-IS 进程可以与 VPN 实例相关联，此时需要执行命令 **isis** [*process-id*] [**vpn-instance** *vpn-instance-name*] *。

----结束

配置网络实体名称

通过配置网络实体名称，指定区域地址和系统 ID，是配置所有 IS-IS 特性的第二步。

背景信息

网络实体名称 NET（Network Entity Title）同时定义了当前 IS-IS 的区域地址和交换机的系统 ID。在一台交换机的一个进程中最多可以配置 3 个 NET，它们的区域地址可以不同，但是系统 ID 必须相同。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **network-entity** *net*，设置网络实体名称。

版权所有 © 华为技术有限公司

注意

建议将 Loopback 接口的地址转化为 NET，保证 NET 在网络中的唯一性。如果网络中的 NET 不唯一，容易引发路由振荡，因此要做好前期网络规划。

IS-IS 在建立 Level-2 邻居时，不检查区域地址是否相同，而在建立 Level-1 邻居时，区域地址必须相同，否则无法建立邻居。

----结束

配置交换机的 Level 级别

通过配置交换机 的 IS-IS 级别，确定邻接关系的 IS-IS 级别。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **is-level** { **level-1** | **level-1-2** | **level-2** }，设置交换机的 Level 级别。

缺省情况下，交换机的 Level 级别为 **level-1-2**。

----结束

在指定接口上使能 IS-IS

只有在具体接口上使能 IS-IS 进程，才能运行 IS-IS 协议。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **isis enable** [*process-id*]，设置指定接口上使能 IS-IS。

要使对端学到接口所在网段的路由，则必须保证使能了 IS-IS 的该接口为 UP 状态。

如果不指定参数 *process-id*，则默认将接口加入到 IS-IS 路由进程 1 中。

----结束

版权所有 © 华为技术有限公司

检查配置结果

IS-IS 基本功能配置成功后，可以查看到使能 IS-IS 的接口信息、LSDB 信息、邻居信息、路由信息和统计信息。

前提条件

已经完成 IS-IS 基本功能的所有配置。

操作步骤

- 使用 **display isis interface** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看使能了 IS-IS 的接口信息。
- 使用 **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*]命令查看 IS-IS 的链路状态数据库。
- 使用 **display isis peer** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看 IS-IS 的邻居信息。
- 使用 **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]]* 命令查看 IS-IS 路由信息。
- 使用以下命令查看 IS-IS 进程的统计信息：
  - **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]
  - **display isis statistics packet** [**interface** *interface-type interface-number*]
  - **display isis** *process-id* **statistics** [**level-1** | **level-2** | **level-1-2** | **packet**]

----结束

任务示例

如果 IS-IS 邻居正常建立，执行命令 **display isis interface**，可以看到本交换机的 IPv4 邻居状态为 Up。

```
<Quidway> display isis interface
                    Interface information for ISIS(1)
                    ----------------------------------
 Interface       Id          IPV4.State            MTU  Type  DIS
 Vlanif10        001         Mtu:Up/Lnk:Dn/IP:Dn   1497 L1/L2 No/No
```

5.6.4 建立或维持 IS-IS 邻居或邻接关系

针对影响 IS-IS 邻居关系保持的参数配置进行介绍。

建立配置任务

在配置影响 IS-IS 邻居关系建立和维持的各种特性前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

本节主要介绍建立或维持 IS-IS 邻居或邻接关系的配置，具体有：

版权所有 © 华为技术有限公司

- 调整各种 IS-IS 报文的定时器，包括 Hello 报文、CSNP 报文和 LSP 等。
- 调整 LSP 的各种参数。

前置任务

在建立或维持 IS-IS 邻居或邻接关系之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在建立或维持 IS-IS 邻居或邻接关系之前，需完成以下任务：

序号	数据
1	IS-IS 报文定时器的参数
2	LSP 的参数

配置 IS-IS 报文定时器

Hello 报文定时器、CSNP 报文定时器和 LSP 报文定时器。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

- 配置 Hello 报文发送间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **isis timer hello** *hello-interval* [**level-1** | **level-2**]，设置接口上 Hello 报文发送间隔。

     广播链路上存在 Level-1 和 Level-2 两种 Hello 报文，不同类型的报文可以设置不同的值。如果不指定级别，则默认为 Level-1 和 Level-2 同时配置。在点到点链路上，只有一种 Hello 报文，不需要使用参数 **level-1** 和 **level-2**。

     说明

     参数 **level-1** 和 **level-2** 仅在广播接口上是可配置的。
- 配置 Hello 报文失效数目
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **isis timer holding-multiplier** *number* [**level-1** | **level-2**]，设置 Hello 报文失效数目。

     如果命令中不指定级别，则默认为 Level-1 和 Level-2 同时配置。

版权所有 © 华为技术有限公司

说明

参数 **level-1** 和 **level-2** 仅在广播接口上是可见的。

IS-IS 协议通过 Hello 报文的收发来维护与相邻交换机的邻居关系，当本端交换机在一段时间内没有收到对端发送的 Hello 报文时，将认为邻居交换机已经失效。

在 IS-IS 中，本端交换机与相邻交换机保持为邻居关系的时间长短可以通过设置 Hello 报文的失效数目和 Hello 报文的时间间隔来控制。

- 配置 CSNP 报文发送间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **isis timer csnp** *csnp-interval* [**level-1** | **level-2**]，设置接口上 CSNP 报文发送间隔。

  CSNP 报文是 DIS（Designated IS）在广播型网络上同步链路状态数据库 LSDB 所发送的报文。如果命令中不指定 Level-1 或 Level-2，则默认为设置当前级别的 CSNP 报文广播间隔。
- 配置接口的 LSP 重传间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **isis enable**，在 VLANIF 接口下使能 IS-IS 功能。
  4. 执行命令 **isis circuit-type p2p**，设置接口网络类型为 P2P 类型。
  5. 执行命令 **isis timer lsp-retransmit** *retransmit-interval*，设置 LSP 在点到点链路上的重传间隔。

  在点到点的链路中，本端发送的 LSP 如果一段时间内没有收到应答，则认为原先发送的 LSP 丢失或被丢弃，为保证发送的可靠性，本端交换机会根据重传间隔将原先的 LSP 重新发送一次。缺省情况下，LSP 在点到点链路上的重传间隔是 5 秒。

  在广播链路上发送的 LSP 报文不需要应答。
- 配置接口发送 LSP 的最小间隔时间
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **isis timer lsp-throttle** *throttle-interval* [**count** *count*]，设置发送 LSP 的最小间隔时间。

     count：用来指定在 *throttle-interval* 时间间隔内发送 LSP 报文的最大包数。整数形式，取值范围是 1 ～ 1000。

  可以设置 IS-IS 在接口上发送 LSP 报文的最小间隔时间，即两个连续的 LSP 之间的时延。该时间也是一个 CSNP 报文的多个分片之间的发送间隔。

----结束

配置 LSP 的参数

通过配置 LSP 生成定时器，调整 IS-IS 网络生成 LSP 报文的时间；通过配置 IS-IS 产生和接收 LSP 的大小，影响 LSP 报文的接收。

版权所有 © 华为技术有限公司

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

- 配置 LSP 刷新周期
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **timer lsp-refresh** *refresh-time*，设置 LSP 刷新周期。

  为了保证整个区域中的 LSP 能够保持同步，IS-IS 周期性发送当前全部 LSP。

  LSP 刷新周期的缺省值为 900 秒，最大有效时间的缺省值为 1200 秒。配置时请注意，必须保证刷新周期比 LSP 的最大有效时间少 300 秒以上，使得原有的 LSP 过期之前，新的 LSP 可以到达区域内所有交换机。

  说明

  网络规模越大，LSP 刷新周期与 LSP 最大有效时间之间的差值也越大。
- 配置 LSP 最大有效时间
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **timer lsp-max-age** *age-time*，设置 LSP 最大有效时间。

  交换机生成系统 LSP 时，会在 LSP 中填写此 LSP 的最大有效时间。当此 LSP 被其它交换机接收后，它的有效时间会随着时间的变化不断减小。如果交换机一直没有收到更新的 LSP，而此 LSP 的有效时间已减少到 0，LSP 再保持 60 秒，若还未收到新的 LSP，那么此 LSP 将被从 LSDB 中删除。
- 配置 LSP 生成所使用的智能定时器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **timer lsp-generation** *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**]，设置 LSP 生成所使用的智能定时器。

  如果没有指定 Level，则认为同时设置 Level-1 和 Level-2。

  初次产生同一 LSP（或者 LSP 分片）的延迟时间为 *init-interval*，第二次产生同一 LSP（或者 LSP 分片）的延迟时间为 *incr-interval*。随后，每变化一次，延迟时间都增大为前一次的两倍，直到 *max-interval*。稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval*。

  在不使用 *incr-interval* 的情况下，初次产生同一 LSP（或者 LSP 分片）仍然使用 *init-interval* 作为延迟时间，随后都是使用 *max-interval* 作为延迟时间。同样，稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval*。

  在只使用 *max-interval* 的情况下，智能定时器退化为一般的一次性触发定时器。
- 配置 LSP 的大小
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **lsp-length originate** *max-size*，设置生成 LSP 的大小。

版权所有 © 华为技术有限公司

4. 执行命令 **lsp-length receive** *max-size*，设置接收 LSP 的大小。

说明

设置 *max-size* 参数时请注意，生成 LSP 的 *max-size* 必须小于等于接收 LSP 的 *max-size*。

使用 **lsp-length** 命令设置的 *max-size* 值必须满足以下要求，否则接口的 MTU 状态会被认为是 Down。

- 以太网接口的 MTU 值大于等于 *max-size*+3。
- P2P 接口的 MTU 值大于等于 *max-size*。

----结束

检查配置结果

配置好影响 IS-IS 邻居关系的各种特性后，可以查看接口发送 IS-IS 报文的各种参数和统计信息。

前提条件

已经完成建立或维持 IS-IS 邻居或邻接关系的所有配置。

操作步骤

- 使用 **display isis interface** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看使能了 IS-IS 的接口信息。
- 使用以下命令查看 IS-IS 进程的统计信息：
  - **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]
  - **display isis statistics packet** [**interface** *interface-type interface-number*]
  - **display isis** *process-id* **statistics** [**level-1** | **level-2** | **level-1-2** | **packet**]

----结束

任务示例

配置接口 VLANIF10 的 Hello 报文发送间隔为 15，Hello 报文失效数目为 10，Level-1 CSNP 报文的发送间隔为 123，发送 LSP 的最小时间间隔为 159，检查结果如下：

```
<Quidway> display isis interface verbose
                    Interface information for ISIS(1)
                    ----------------------------------
 Interface       Id      IPV4.State          MTU  Type  DIS
 Vlanif10        001 Mtu:Up/Lnk:Dn/IP:Dn     1497 L1/L2 No/No
  Description                : HUAWEI, Quidway Series, Vlanif10 Interface
  SNPA Address               : 00e0-095b-4201
  IP Address                 : 123.1.1.1
  Csnp Timer Value           :  L1   123  L2    10
  Hello Timer Value          :  L1    15  L2    15
  DIS Hello Timer Value      :  L1     5  L2     5
  Hello Multiplier Value     :  L1    10  L2    10
  LSP-Throttle Timer         :  L12  159
  Cost                       :  L1    10  L2    10
  Priority                   :  L1    64  L2    64
  Retransmit Timer Value     :  L12    5
  Bandwidth-Value            :  Low 100000000  High         0
  Static Bfd                 :  NO
  Dynamic Bfd                :  NO
  Fast-Sense Rpr             :  NO
```


版权所有 © 华为技术有限公司

5.6.5 配置 IS-IS 在不同网络类型中的属性

由于 IS-IS 在不同网络类型中应用时有不同的特点，因此，本节介绍不同网络类型中 IS-IS 的属性特点和配置方法。

建立配置任务

在配置 IS-IS 在不同网络类型中的属性前了解此特性的应用环境、配置这些特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

IS-IS 在不同的网络类型中表现出不同的属性，本节主要介绍配置 IS-IS 在不同网络类型中的属性的任务，包括：

- 通过改变以太接口的链路类型为 P2P，可以在以太接口上模拟 P2P 接口。
- 控制 DIS 的选举。
- 检测 PPP 链路协议的 OSI 网络协商状态。
- 两台交换机在 P2P 接口建立邻居时，配置忽略 IP 地址的检查，可以使不在同一网段的两个 P2P 接口之间建立邻居。

前置任务

在配置 IS-IS 不同网络类型中的属性的任务之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在配置 IS-IS 不同网络类型中的属性之前，需要准备以下数据。

序号	数据
1	接口的网络类型
2	接口的 DIS 优先级

配置 IS-IS 接口上的网络类型

通过将 IS-IS 接口的网络类型模拟为 P2P，使链路两端的接口网络类型一致，以保证 IS-IS 邻居关系成功建立。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **isis circuit-type p2p**，设置接口的网络类型为 P2P。

缺省情况下，接口网络类型根据物理接口决定。

在使能 IS-IS 的接口上，当接口网络类型发生改变时，相关配置发生改变，具体如下。

- 使用 **isis circuit-type p2p** 命令将广播网接口模拟成 P2P 接口时，接口发送 Hello 报文的间隔时间、宣告邻居失效前 IS-IS 没有收到的邻居 Hello 报文数目、点到点链路上 LSP 报文的重传间隔时间以及 IS-IS 各种认证均恢复为缺省配置，而 DIS 优先级、DIS 名称、广播网络上发送 CSNP 报文的间隔时间等配置均失效。
- 使用 **undo isis circuit-type** 命令恢复接口的网络类型时，接口发送 Hello 报文的间隔时间、宣告邻居失效前 IS-IS 没有收到的邻居 Hello 报文数目、点到点链路上 LSP 报文的重传间隔时间、IS-IS 各种认证、DIS 优先级和广播网络上发送 CSNP 报文的间隔时间均恢复为缺省配置。

说明

链路两端的 IS-IS 接口的网络类型必须一致，否则双方不可以建立起邻居关系。

----结束

配置接口的 DIS 优先级

通过配置广播网络类型中接口的 DIS 优先级，影响广播网 DIS 选举。

背景信息

Level-1 和 Level-2 的 DIS 是分别选举的，可以设置为不同的优先级。如果命令中没有指定 level-1 或 level-2，则为 Level-1 和 Level-2 设置同样的优先级。

DIS 的选举优先根据其优先级的大小进行选举。接口 DIS 优先级最高的 IS 被选举为 DIS，如果 DIS 优先级相同，则其中接口 MAC 地址最大的接口会被选中；如果接口的 DIS 优先级是 0，仍然会参与 DIS 的选举，这点和 OSPF 不同。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **isis dis-priority** *priority* [**level-1** | **level-2**]，设置用来选举 DIS 的优先级，数值越大优先级越高。

----结束

后续处理

说明

DIS 优先级仅对广播类型的网络有意义。

版权所有 © 华为技术有限公司

如果通过 **isis circuit-type** 命令将广播接口模拟为 P2P 接口，则 **isis dis-priority** 命令在该接口失效；如果通过 **undo isis circuit-type** 命令将该接口恢复为广播接口，则 DIS 优先级也恢复为缺省优先级。

检查配置结果

配置好 IS-IS 在不同网络类型中的属性后，可以查看使能了 IS-IS 的接口信息。

前提条件

已经完成 IS-IS 在不同网络类型中的属性的所有配置。

操作步骤

步骤 1 使用 **display isis interface** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看使能了 IS-IS 的接口信息。

----结束

任务示例

配置接口 VLANIF10 为广播类型，并配置该接口的 DIS 优先级为 100。检查配置结果为：

```
<Quidway> display isis interface verbose
                      Interface information for ISIS(1)
                      ---------------------------------
 Interface       Id      IPV4.State           MTU  Type  DIS
 Vlanif10        001         Up                  1497 L1/L2 No/No
  Description                : HUAWEI, Quidway Series, Vlanif10 Interface
  SNPA Address               : 00e0-095b-4201
  IP Address                 : 123.1.1.1
  Csnp Timer Value           :  L1   123  L2    10
  Hello Timer Value          :  L1    15  L2    15
  DIS Hello Timer Value      :  L1     5  L2     5
  Hello Multiplier Value     :  L1    10  L2    10
  LSP-Throttle Timer         :  L12  159
  Cost                       :  L1    10  L2    10
  Retransmit Timer Value     :  L12    5
  Bandwidth-Value            :  Low 100000000  High         0
  Static Bfd                 :  NO
  Dynamic Bfd                :  NO
  Fast-Sense Rpr             :  NO
  Extended-Circuit-Id Value  :  0000000001
```

5.6.6 配置 IS-IS 的路由属性

通过配置 IS-IS 的路由属性，可以影响 IS-IS 的选路。

建立配置任务

在配置 IS-IS 的路由属性前了解这些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

本节主要介绍如何改变路由信息的属性，包括配置 IS-IS 协议的优先级、接口的开销和 IS-IS 路由的收敛优先级。

版权所有 © 华为技术有限公司

前置任务

在配置 IS-IS 路由的属性之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在配置 IS-IS 路由的属性之前，需要准备以下数据。

序号	数据
1	IS-IS 的协议优先级
2	各接口的开销
3	IS-IS 路由的收敛优先级

配置 IS-IS 接口的开销

通过配置 IS-IS 接口的开销，可以影响 IS-IS 路由的开销，进而影响 IS-IS 路由选择。

背景信息

IS-IS 有三种方式来确定接口的链路开销，按照优先级由高到低分别是：

- 接口开销：为单个接口设置链路开销。
- 全局开销：为所有接口设置链路开销。

如果没有显式的配置任何命令，则 IS-IS 接口的默认开销为 10，开销类型是 narrow。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

- 配置 IS-IS 开销的类型
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **cost-style** { **narrow** | **wide** | **wide-compatible** | { { **narrow-compatible** | **compatible** } [**relax-spf-limit**] } }，设置 IS-IS 开销的类型。

  对于不同的开销类型，其接口开销的取值范围有所不同，接收到的路由开销取值范围也有所不同。

  - narrow 类型：接口开销取值范围为 1 ～ 63。接收到的路由开销值最大为 1023。
  - narrow-compatible 和 compatible 类型：接口开销取值范围为 1 ～ 63。接收到的路由开销值和参数 **relax-spf-limit** 有关。
    - 不设置 **relax-spf-limit** 参数：

      如果路由开销值小于等于 1023，且该路由经过的所有接口的链路开销值都小于等于 63：这条路由的开销值按照实际值接收。

华为专有和保密信息
版权所有 © 华为技术有限公司

如果路由开销值小于等于 1023，但该路由经过的所有接口中有的接口链路开销值大于 63：交换机只能学到该接口所在网段的路由和接口所引入的路由，这条路由的开销值按照实际值接收，之后通过此接口转发的路由将被丢弃。

如果路由开销值大于 1023：交换机只能学到路由开销值第一次超过 1023 的那个接口（该接口之前的所有接口的链路开销值小于等于 63）的路由。该接口所在网段的路由和引入的路由均可以被学习到，路由的开销值按照 1023 接收，之后通过此接口转发的路由将被丢弃。

- 设置 **relax-spf-limit** 参数：

  对接口的链路开销值和路由开销值均没有限制，按照实际的路由开销值正常接收该路由。

- wide 和 wide-compatible 类型：接口开销取值范围是 1 ～ 16777215。配置为最大值 16777215 时，该链路上生成的邻居 TLV（cost 为 16777215）不能用于路由计算，仅用于传递 TE 相关信息。接收到的路由开销值最大为 0xFFFFFFFF。

- 配置 IS-IS 接口的开销
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **isis cost** *cost* [**level-1** | **level-2**]，设置 IS-IS 接口的开销。

     使用此命令可以单独为某接口配置开销值。
- 配置 IS-IS 的全局开销
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **circuit-cost** *cost* [**level-1** | **level-2**]，设置 IS-IS 全局开销。

     使用此命令可以一次性改变所有接口的开销值。

----结束

配置 IS-IS 优先级

通过配置 IS-IS 协议优先级和 IS-IS 路由的各种优先级，可以影响 IS-IS 的路由选择和路由收敛。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

- 配置 IS-IS 协议优先级
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **preference** *preference*，配置 IS-IS 协议优先级。

     该命令用来为 IS-IS 路由协议设置优先级，配置值越小，优先级越高。

     缺省情况下，IS-IS 协议的优先级为 15。

  一台交换机可同时运行多个路由协议，当多个路由协议都发现到同一目的地的路由时，将选用优先级高的协议发现的路由。

版权所有 © 华为技术有限公司

- 配置 IS-IS 特定路由的优先级
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **preference route-policy** *route-policy-name*，通过路由策略为特定的路由设置优先级。

----结束

检查配置结果

配置完 IS-IS 的路由属性后，可以查看接口的 IS-IS 开销和 IS-IS 路由的各种优先级信息。

前提条件

已经完成 IS-IS 路由属性的所有配置。

操作步骤

步骤 1 使用 **display isis interface** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看使能了 IS-IS 的接口信息。

步骤 2 使用 **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | { **level-1** | **level-2** } | *ip-address* [*mask* | *mask-length*]]* 命令查看 IS-IS 路由的优先级信息。

----结束

任务示例

将接口 VLANIF10 的 IPv4 开销都配置为 20。检查配置结果为：

```
<Quidway> display isis interface verbose

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          MTU  Type  DIS
 Vlanif10        001         Up              1497 L1/L2 No/No
  Description                : HUAWEI, Quidway Series, Vlanif10 Interface
  SNPA Address               : 00e0-c72d-da01
  IP Address                 : 123.1.1.1
  Csnp Timer Value           :  L1    10  L2    10
  Hello Timer Value          :  L1    10  L2    10
  DIS Hello Timer Value      :  L1     3  L2     3
  Hello Multiplier Value     :  L1     3  L2     3
  LSP-Throttle Timer         :  L12   50
  Cost                       :  L1    20  L2    20
  Retransmit Timer Value     :  L12    5
  Bandwidth-Value            :  Low 100000000  High         0
  Static Bfd                 :  NO
  Dynamic Bfd                :  NO
  Fast-Sense Rpr             :  NO
```

配置 IS-IS 引入路由 10.10.10.0/24 的收敛优先级为 **Critical**。检查配置结果为：

```
<Quidway> display isis route verbose

                      Route information for ISIS(1)
                      -----------------------------

                  ISIS(1) Level-2 Forwarding Table
```


版权所有 © 华为技术有限公司

```
------------------------------

IPV4 Dest  : 10.10.10.0/24      Int. Cost : 20            Ext. Cost : NULL
Admin Tag  : -                  Src Count : 2             Flags     : A/-/-
Priority   : Critical
NextHop    :                    Interface :               ExitIndex :
   1.1.1.2                       Vlanif10                    0x80000001

IPV4 Dest  : 1.1.1.0/24         Int. Cost : 10            Ext. Cost : NULL
Admin Tag  : -                  Src Count : 2             Flags     : D/-/L
Priority   : Medium
NextHop    :                    Interface :               ExitIndex :
   Direct                        Vlanif10                    0x00000000

IPV4 Dest  : 20.20.20.0/24      Int. Cost : 20            Ext. Cost : NULL
Admin Tag  : -                  Src Count : 2             Flags     : A/-/-
Priority   : Low
NextHop    :                    Interface :               ExitIndex :
   1.1.1.2                       Vlanif10                    0x80000001

    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

5.6.7 控制 IS-IS 路由信息的发布

通过控制 IS-IS 路由渗透、配置 IS-IS 路由聚合和生成缺省路由，可以有效控制不同级别、不同区域的 IS-IS 路由信息的发布，灵活控制 IS-IS 路由表项的数量。

建立配置任务

在配置控制 IS-IS 的路由信息的各种特性前了解这些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

本节主要介绍如何控制 IS-IS 的路由信息的发布，例如发布聚合路由，生成缺省路由和配置路由渗透。

前置任务

在配置 IS-IS 路由信息的发布之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在配置 IS-IS 路由信息的发布之前，需要准备以下数据。

序号	数据
1	需聚合的路由
2	路由渗透的类型

版权所有 © 华为技术有限公司

配置 IS-IS 生成缺省路由

通过配置 IS-IS 生成缺省路由，控制 IS-IS 的路由信息发布。

背景信息

交换机的级别决定生成的缺省路由发布的级别，该命令产生的缺省路由只被发布给同级别的交换机。通过使用路由策略，可以强制 IS-IS 只在路由表中有匹配的路由项时才生成缺省路由。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **default-route-advertise** [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] * [**avoid-learning**]，设置生成缺省路由。

----结束

控制 Level-2 区域的路由渗透到 Level-1 区域

通过控制 IS-IS 路由渗透（Level-2 to Level-1），可以将 Level-2 级别的路由信息和其他区域的 level-1 级别的路由信息渗透到 Level-1 区域。

背景信息

通过 IS-IS 路由渗透功能，Level-1-2 路由器可以将自己 Level-2 中符合要求的路由信息渗透到 Level-1 区域，并在 Level-1 的 LSP 中发布出去。

请在运行 IS-IS 协议的 Level-1-2 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **import-route isis level-2 into level-1** [**tag** *tag* | **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }] *，使能 IS-IS 路由渗透，将 Level-2 区域和其他 Level-1 区域的路由渗透到交换机所在的 Level-1 区域。

该命令配置在与外部区域相连的 Level-1-2 路由器上。缺省情况下，Level-2 区域的路由信息不渗透到 Level-1 区域。

----结束

检查配置结果

配置完 IS-IS 路由渗透、路由聚合和生成缺省路由后，可以通过查看 IS-IS 路由表和 IS-IS 路由详细信息来检查配置结果。

版权所有 © 华为技术有限公司

前提条件

已经完成控制 IS-IS 路由信息发布的所有配置。

操作步骤

- 使用 **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]]* 命令查看 IS-IS 路由信息。
- 使用 **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看 IS-IS 的链路状态数据库。

----结束

任务示例

配置 IS-IS 进程 1 的路由 Level-2 渗透到 Level-1。检查配置结果如下：

```
<Quidway> display isis route
                        Route information for ISIS(1)
                        ------------------------------
                       ISIS(1) Level-1 Forwarding Table
                       --------------------------------
 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop          Flags
-------------------------------------------------------------------------------
10.10.20.0/24        20         NULL    Vlanif10         10.10.10.1       A/-/L
10.10.10.0/24        10         NULL    Vlanif10         Direct           D/-/L
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs,U-Up/Down Bit Set
                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------
 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop          Flags
-------------------------------------------------------------------------------
10.10.20.0/24        20         NULL    Vlanif10         10.10.10.1       A/-/L
10.10.10.0/24        10         NULL    Vlanif10         Direct           D/-/L
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

5.6.8 控制 IS-IS 路由信息的接收

通过 IS-IS 对路由信息的过滤，可以控制加入 IP 路由表的 IS-IS 路由数量和 IS-IS 加入 IS-IS 路由表的其他路由的数量。

建立配置任务

在配置控制 IS-IS 路由信息的接收前了解这些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

本节主要介绍如何控制 IS-IS 的路由信息的接收，例如对接收的路由进行过滤以及引入外部路由等。

前置任务

在配置 IS-IS 路由信息的接收之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。

版权所有 © 华为技术有限公司

- 配置 IS-IS 的基本功能。

数据准备

在配置 IS-IS 路由信息的接收之前，需要准备以下数据。

序号	数据
1	过滤路由信息时所需要的过滤列表
2	要引入的外部路由协议名称及进程号

配置 IS-IS 对接收的路由信息进行过滤

通过配置 IS-IS 对接收的路由是否加入 IP 路由表，来控制加入 IP 路由表的 IS-IS 路由数量，减少 IP 路由表的规模。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**，配置 IS-IS 对接收的路由是否加入 IP 路由表进行过滤。

----结束

配置 IS-IS 引入外部路由

通过配置 IS-IS 引入路由，IS-IS 可以学到其他协议或其他 IS-IS 进程的路由信息。

背景信息

IS-IS 将其它路由协议或其他 IS-IS 进程发现的路由当作外部路由处理。在引入外部路由时，可指定引入路由的缺省开销。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 配置 IS-IS 引入外部路由。

当需要对引入路由的开销进行设置时，使用命令 **import-route** *protocol* [*process-id*] [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 引入外部路由。

版权所有 © 华为技术有限公司

当需要保留引入路由的原有开销时，使用命令 **import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **bgp** } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 引入外部路由。

步骤 4 执行命令 **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]，对已引入的路由在向外发布时进行过滤。

如果 **import-route** 命令中不指定引入的级别，则默认为引入路由到 Level-2 路由表中。

----结束

检查配置结果

配置完 IS-IS 对接收路由的过滤和引入外部路由的过滤后，可以通过查看 IS-IS 路由表和 IP 路由表来检查配置结果。

前提条件

已经完成控制 IS-IS 路由信息接收的所有配置。

操作步骤

- 使用 **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看 IS-IS 的链路状态数据库。
- 使用 **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]]* 命令查看 IS-IS 路由信息。

----结束

任务示例

如果 IS-IS 邻居正常建立，执行命令 **display isis route** 可以看到，本交换机的 IS-IS 进程 1 引入了一条静态路由 169.1.1.0/24。

```
<Quidway> display isis route
                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------
 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop          Flags
-------------------------------------------------------------------------------
 123.1.1.0/24         10         NULL    Vlanif10        Direct           D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set
                        ISIS(1) Level-2 Redistribute Table
                        ----------------------------------
 Type IPV4 Destination     IntCost    ExtCost Tag
-------------------------------------------------------------------------------
 S    169.1.1.0/24         0          NULL
            Type: D-Direct, I-ISIS, S-Static, O-OSPF, B-BGP, R-RIP, U-UNR
```

5.6.9 调整和优化 IS-IS

通过调整和优化 IS-IS，使得 IS-IS 可以满足复杂网络环境的需要。

版权所有 © 华为技术有限公司

建立配置任务

在配置调整和优化 IS-IS 前了解这些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

本节主要介绍优化和调整 IS-IS 网络的配置。具体有：

- 配置 IS-IS 接口的 Level 级别和接口的状态。
- 调整 SPF 的各项参数。
- 介绍了 IS-IS 动态主机名映射和验证功能的配置，以便满足用户对易维护性和安全性的要求。

前置任务

在调整和优化 IS-IS 之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在调整和优化 IS-IS 之前，需要准备以下数据。

序号	数据
1	接口的 Level 级别
2	System ID 和主机名的映射

配置 IS-IS 接口的 Level 级别

通过配置 IS-IS 接口的级别，来控制 IS-IS 接口与对端建立的邻居关系的级别。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入接口视图。

步骤 3 执行命令 **isis circuit-level** [**level-1** | **level-1-2** | **level-2**]，设置接口的 Level 级别。

缺省情况下，接口的 Level 级别为 **level-1-2**。

版权所有 © 华为技术有限公司

说明

只有当交换机是 Level-1-2 类型时，改变接口线路的 Level 级别才有意义，否则将由交换机的 Level 级别决定所能建立的邻接关系层次。

----结束

配置 IS-IS 接口为抑制状态

通过配置 IS-IS 接口抑制，使接口只发布直连路由但不收发 IS-IS。有效控制 IS-IS 网络中无用报文的传播。

背景信息

当 IS-IS 网络与其他自治系统连接时，为了让区域内的交换机学到出口路由，需要在该出口上使能 IS-IS 协议。但这样会让该接口向其所在网段发布 IS-IS Hello 报文，这是没有必要的。此时可以在此接口上执行 **isis silent** 命令，启动 IS-IS 的接口抑制功能。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **isis silent**，配置 IS-IS 接口为抑制状态。

IS-IS 接口为抑制状态时，此接口不再接收或发送 IS-IS 报文，但接口所在网段的路由仍可以被发布到域内的其他交换机。

说明

如果该区域接口上的 IS-IS 协议状态为 Down，会导致区域内的交换机学习不到出口路由。

----结束

配置 SPF 的参数

通过配置 SPF 参数，调整 IS-IS 路由计算的间隔时间，避免过于频繁的路由计算引起网络振荡。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

- 配置 SPF 智能定时器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **timer spf** *max-interval* [*init-interval* [*incr-interval*]]，设置 SPF 智能定时器。

  智能定时器的变化规律如下

版权所有 © 华为技术有限公司

- 初次进行 SPF 计算的延迟时间为 *init-interval*；第二次进行 SPF 计算的延迟时间为 *incr-interval*。随后，每变化一次，SPF 计算的延迟时间增大为前一次的两倍，直到 *max-interval*。稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval*。
- 在不使用 *incr-interval* 的情况下，初次进行 SPF 计算用 *init-interval* 作为延迟时间，随后都是使用 *max-interval* 作为延迟时间。稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval*。
- 在只使用 *max-interval* 的情况下，智能定时器退化为一般的一次性触发定时器。

- 配置每次 SPF 计算的持续时间
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **spf-slice-size** *duration-time*，设置每次 SPF 计算的持续时间。

  当路由表中的路由数目很多时（超过 15 万条），IS-IS 的 SPF 计算可能会长时间占用 CPU 资源，为防止这种情况的发生，可以设置每次 SPF 计算的持续时间。

----结束

配置 LSP 快速扩散

通过配置 LSP 快速扩散，可以提高 IS-IS 网络的收敛速度。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **flash-flood** [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] *，使能 LSP 快速扩散。

使用 **flash-flood** 命令可以加速 LSP 的扩散（Flooding）速度。用户可以通过参数 *lsp-count* 指定每次扩散的 LSP 数量，这个数量是针对所有接口的。如果需要发送的 LSP 的数量大于 *lsp-count*，则就发送 *lsp-count* 个 LSP。如果配置了定时器，在路由计算之前如果这个定时器未超时，则立即扩散；否则在该定时器超时的时候发送。

配置 LSP 快速扩散时，如果不指定 level-1 或 level-2，则默认为 level-1 和 level-2 都配置快速扩散。

----结束

配置 IS-IS 动态主机名映射

通过配置 IS-IS 动态主机名映射，提高 IS-IS 网络的维护性和方便性。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

- 为本地 IS 配置主机名称
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **is-name** *symbolic-name*，为本地 IS 配置主机名称。

     本地 IS-IS 进程配置一个名称，并且使能系统 ID 到主机名的映射。配置的名称以 LSP 报文的形式发布给区域中的其它交换机。

     要想使能 IS-IS 进程的动态主机名映射，必须先配置该命令，否则，IS-IS 相关显示命令的输出信息中将无法显示系统 ID 与名称的映射关系。
- 为远端 IS 配置主机名称
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。
  3. 执行命令 **is-name map** *system-id symbolic-name*，为远端 IS 配置主机名称。

     在本地为远端的 IS-IS 路由器配置一个名称，每个 SystemID 只能对应一个名称。

     如果网络中任何一台路由器在 LSP 报文中发布了主机名与系统 ID 的映射关系，该映射关系将覆盖本地交换机的静态映射。
- 为 DIS 配置主机名称
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **isis dis-name** *symbolic-name*，为 DIS 配置主机名称。

     该配置仅在 DIS 上有效。在接口上配置此命令，可将配置的名称以本地交换机伪节点的 LSP 报文的形式发布给与该接口相连的网络，从而将配置的名称与指定交换机的 System ID 相关联。但该命令在点到点接口上无效。

----结束

配置 LSDB 过载标志位

设置了过载标志位的 LSDB 的 LSP 会在网络中扩散，但是在计算通过超载交换机 的路由时不会被采用。

背景信息

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **set-overload** [**allow** { **interlevel** | **external** } *]，设置过载标志位。

----结束

版权所有 © 华为技术有限公司

后续处理

虽然设置了过载标志位的 LSP 会在网络中扩散，但是在计算通过超载交换机的路由时不会被采用。即，对交换机设置过载位后，其它交换机在进行 SPF 计算时不会考虑这台交换机。但该交换机的直连路由不会被忽略。

如果 IS-IS 域中的某台交换机发生问题，会导致整个区域路由的计算错误。在故障排除过程中，通过给怀疑有问题的交换机设置过载标志位，可以将其从 IS-IS 网络中暂时隔离，以便于进行故障定位。

配置邻接状态输出开关

打开邻接状态输出开关后，IS-IS 邻接状态的变化会输出到配置终端上，直至邻接状态输出开关被关闭。

背景信息

在本地 terminal monitor 开关已开启的情况下，当打开邻接状态输出开关后，IS-IS 邻接状态的变化会输出到配置终端上，直至邻接状态输出开关被关闭。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 执行命令 **log-peer-change**，打开邻接状态输出开关。

----结束

检查配置结果

配置完调整和优化 IS-IS 后，可以参看 IS-IS 的动态主机名、SPF 计算日志、SPF 树和 IS-IS 的统计信息。

前提条件

已经完成调整和优化 IS-IS 的所有配置。

操作步骤

- 使用 **display isis name-table** [*process-id* | **vpn-instance** *vpn-instance-name*] 命令查看本地交换机名称到系统 ID 的映射关系表。
- 使用 **display isis spf-log** [*process-id* | **vpn-instance** *vpn-instance-name*] [[**level-1** | **level-2**] | **verbose**] *命令查看 IS-IS 的 SPF 计算日志记录。
- 使用 **display isis** [*process-id*] **spf-tree statistics** [**level-1** | **level-2**] [**vpn-instance** *vpn-instance-name*] 命令查看 IS-IS 的 SPF 树。
- 使用以下命令查看 IS-IS 进程的统计信息：
  - **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

版权所有 © 华为技术有限公司

- **display isis statistics packet** [**interface** *interface-type interface-number*]
- **display isis** *process-id* **statistics** [**level-1** | **level-2** | **level-1-2** | **packet**]

----结束

任务示例

执行命令 **display isis name-table 1** 可以看到本地交换机的 IS 主机名是 abc。

```
<Quidway> display isis name-table 1

                    Name table information for ISIS(1)

System ID           Hostname                        Type
------------------------------------------------------------------------------
1111.1111.1111      abc                             DYNAMIC
```

5.6.10 提高 IS-IS 网络的安全性

在对安全性较高的网络中，可以通过配置 IS-IS 认证来提高 IS-IS 网络的安全性。

建立配置任务

在配置提高 IS-IS 网络的安全性前了解这些特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在安全性较高的网络中，可以通过配置 IS-IS 认证，来提高 IS-IS 网络的安全性。IS-IS 的认证方式有：区域认证、路由域认证和接口认证。

前置任务

在配置 IS-IS 的认证之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- **配置 IS-IS 的基本功能**。

数据准备

在配置 IS-IS 的认证特性之前，需要准备以下数据。

序号	数据
1	认证方式及认证密码

配置区域或路由域的认证

通过配置 IS-IS 区域或路由域认证，可以封装认证信息到 LSP 或 SNP 报文中，确保报文扩散的安全性。

版权所有 © 华为技术有限公司

背景信息

缺省情况下，不对发送的 IS-IS 报文封装认证信息，也不对收到的报文做认证检查。

如果需要区域认证，区域认证密码就会按照设定的方式封装到 Level-1 的 LSP、CSNP、PSNP 报文中。同一区域的所有交换机的区域认证方式和密码都必须一致，IS-IS 报文才会正常扩散。

同样，如果需要路由域认证，路由域认证密码会按照设定的方式封装到 Level-2 的报文中。认证过程及参数配置和区域验证相同。同一路由域的所有交换机的域认证方式和密码都必须一致，IS-IS 报文才会正常扩散。

无论是否通过区域认证或者路由域认证，均不影响 Level-1 或者 Level-2 邻居关系的建立。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，进入 IS-IS 视图。

步骤 3 配置区域认证模式。

- 当需要配置 **simple** 或 **md5** 密码时，执行命令 **area-authentication-mode** { **simple** *password* | **md5** *password-key* } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]，设置区域认证模式。

注意

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

步骤 4 配置路由域认证模式。

- 当需要配置 **simple** 或 **md5** 密码时，执行命令 **domain-authentication-mode** { **simple** *password* | **md5** *password-key* } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]，设置路由域认证模式。

注意

由于符号$@$@用于升级时区分新老密码类型，MD5 密码不允许同时以$@$@开始和结束。

认证支持以下几种组合形式：

- 对发送的 LSP 和 SNP 都封装认证信息，并检查收到的 LSP 和 SNP 是否通过认证，丢弃没有通过认证的报文。该情况下不配置参数 **snp-packet** 或 **all-send-only**。
- 对发送的 LSP 封装认证信息并检查收到的 LSP，对发送的 SNP 不封装认证信息，也不检查收到的 SNP。该情况下需要配置参数 **snp-packet authentication-avoid**。

版权所有 © 华为技术有限公司

- 对发送的 LSP 和 SNP 都封装认证信息，只检查收到的 LSP，不检查收到的 SNP。该情况下需要配置参数 **snp-packet send-only**。
- 对发送的 LSP 和 SNP 都封装认证信息，不检查收到的 LSP 和 SNP。该情况下需要配置参数 **all-send-only**。

配置区域或路由域的认证时，参数 **ip** 和 **osi** 的选择不受实际的网络环境影响。

----结束

配置接口的认证

通过配置 IS-IS 接口认证，可以封装认证信息到 Hello 报文中，以确认邻居的有效性和正确性。

背景信息

在接口上配置的认证用在 Hello 报文中，以确认邻居的有效性和正确性。

请在运行 IS-IS 协议的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 配置接口的 IS-IS 认证模式和密码。

- 当需要配置 **simple** 或 **md5** 密码时，执行命令 **isis authentication-mode** { **simple** *password* | **md5** *password-key* } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]。



注意

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

- 如果配置了 **send-only** 则表示仅对发送的 Hello 封装认证信息，而不检查收到的 Hello 报文是否通过了认证。只有不需要进行认证检查或者认证通过才能建立起邻居关系。
- 如果没有配置 **send-only**，此时应保证同一网络所有接口的相同级别的认证密码一致。

当 IS-IS 接口线路类型为 Level-1-2 时，如果不选择参数 **level-1** 或 **level-2**，则为 Level-1 和 Level-2 的 Hello 报文都配置认证模式和密码。

配置接口的认证时，参数 **ip** 和 **osi** 的选择不受实际的网络环境影响。

说明

参数 **level-1** 和 **level-2** 仅在以太网接口上是可见的，而且必须先使用 **isis enable** 命令在该接口上使能 IS-IS。

----结束

检查配置结果

通过配置 IS-IS 的各种认证，可以提高 IS-IS 网络的安全性。

版权所有 © 华为技术有限公司

前提条件

已经完成提高 IS-IS 网络安全性的所有配置。

操作步骤

步骤 1 使用 **display isis peer** [*process-id* | **vpn-instance** *vpn-instance-name*][**verbose**] 命令查看 IS-IS 的邻居信息。

----结束

任务示例

配置接口 VLANIF20 的验证模式为 simple，密码为 123，保证邻居的验证信息配置相同，则两端可以建立邻居关系。检查配置结果为：

```
<Quidway> display isis  peer 1 verbose
                        Peer information for ISIS(1)
  System Id    Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0000.0000.0040 Vlanif20           0000.0000.0040.04 Up   7s       L1(L1L2) 64
  MT IDs supported     : 0(UP)
  Area Address(es)   :10
  Peer IP Address(es): 12.40.41.1
  Uptime             : 00:01:08
  Adj Protocol       :  IPV4
  Restart Capable    :  Yes
  Suppressed Adj     :  NO
0000.0000.0040 Vlanif20           0000.0000.0040.04 Up   8s       L2(L1L2) 64
  MT IDs supported     : 0(UP)
  Area Address(es)   :10
  Peer IP Address(es): 12.40.41.1
  Uptime             : 00:01:14
  Adj Protocol       :  IPV4
  Restart Capable    :  Yes
  Suppressed Adj     :  NO
Total Peer(s): 2
```

5.6.11 维护 IS-IS 配置

维护 IS-IS，包括复位和清除 IS-IS。

复位 IS-IS 数据结构

通过重启 IS-IS，达到复位的目的。可以选择以 GR 的方式复位 IS-IS。

背景信息

注意

复位 IS-IS 数据结构后，以前所有的结构信息、邻接关系将全部重新建立，务必仔细确认。

在确认需要复位 IS-IS 的数据结构后，请在用户视图下执行以下命令。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 使用 **reset isis all** [*process-id* | **vpn-instance** *vpn-instance-name*] * 命令复位 IS-IS 的数据结构。

缺省情况下，不复位 IS-IS 的数据结构。

----结束

复位 IS-IS 特定邻居

通过重启 IS-IS 邻居，可以复位 IS-IS 邻居关系，达到使新的配置生效的目的。

背景信息

注意

复位 IS-IS 特定邻居（执行 **reset isis peer** 命令）会导致交换机之间的 IS-IS 特定邻居关系中断。务必仔细确认是否必须执行复位 IS-IS 特定邻居的操作。

当 IS-IS 路由策略或协议发生变化后，需要通过复位 IS-IS 特定邻居使新的配置生效。如果需要复位 IS-IS 特定邻居，可在用户视图下选择执行以下命令。

操作步骤

步骤 1 使用 **reset isis peer** *system-id* [*process-id* | [**vpn-instance** *vpn-instance-name*] *]命令复位 IS-IS 的特定邻居。

----结束

调试 IS-IS

只要在用户视图下打开相应模块的调试开关，交换机就能够产生调试信息。调试信息显示被调试模块接受或者发送数据报的信息内容。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 IS-IS 运行故障时，请在用户视图下执行 **debugging** 命令对 IS-IS 进行调试，查看调试信息，定位故障并分析故障原因。打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南-系统管理》的内容。

有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 -Debugging 参考》。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **debugging isis all** [*process-id*]命令打开 IS-IS 的所有调试信息开关。
- 使用 **debugging isis adjacency** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的邻接调试信息开关。
- 使用 **debugging isis authentication-error** [*process-id*]命令打开 IS-IS 的认证错误调试信息开关。
- 使用 **debugging isis bfd** [*process-id*]命令打开 IS-IS 进程的 BFD 调试开关。
- 使用 **debugging isis checksum-error** [*process-id*]命令打开 IS-IS 的 LSP 校验错误调试信息开关。
- 使用 **debugging isis circuit-information** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的接口级别信息调试开关。
- 使用 **debugging isis configuration-error** [*process-id*]命令打开 IS-IS 的配置错误调试信息开关。
- 使用 **debugging isis datalink-receiving-packet** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的链路层接收报文调试信息开关。
- 使用 **debugging isis datalink-sending-packet** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的链路层发送报文调试信息开关。
- 使用 **debugging isis event** [*process-id*]命令打开 IS-IS 的事件调试信息开关。
- 使用 **debugging isis general-error** [*process-id*]命令打开 IS-IS 的一般错误调试信息开关。
- 使用 **debugging isis interface-information** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的接口信息调试开关。
- 使用 **debugging isis memory-allocating** [*process-id*]命令打开 IS-IS 的内存分配调试信息开关。
- 使用 **debugging isis miscellaneous-errors** 命令打开 IS-IS 的混杂错误调试信息开关。
- 使用 **debugging isis receiving-packet-content** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的接收报文内容调试信息开关。
- 使用 **debugging isis self-originate-update** [*process-id*]命令打开 IS-IS 的本地更新报文调试信息开关。
- 使用 **debugging isis sending-packet-content** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的发送报文内容调试信息开关。
- 使用 **debugging isis sending-packet-regular-content** [*process-id*]命令打开 IS-IS 的发送报文的正常信息开关。
- 使用 **debugging isis snp-packet** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的 SNP 报文调试信息开关。
- 使用 **debugging isis spf-event** [*process-id*]命令打开 IS-IS 的 SPF 事件调试信息开关。
- 使用 **debugging isis** [*process-id*] **spf-prc** [**policy** [**ipv4-acl** *acl-number* | **ip-prefix** *ip-prefix-name*]]命令打开 IS-IS 的 SPF-PRC 开关。
- 使用 **debugging isis spf-summary** [*process-id*]命令打开 IS-IS 的 SPF 汇总调试信息开关。
- 使用 **debugging isis spf-timer** [*process-id*]命令打开 IS-IS 的 SPF 时钟调试信息开关。

版权所有 © 华为技术有限公司

- 使用 **debugging isis task-error** [*process-id*]命令打开 IS-IS 的任务错误调试信息开关。
- 使用 **debugging isis timer** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的时钟调试信息开关。
- 使用 **debugging isis update-packet** [*process-id* | **interface** *interface-type interface-number*]命令打开 IS-IS 的更新报文调试信息开关。
- 使用以下命令打开 IS-IS 的更新进程调试信息开关：
  - **debugging isis** [*process-id*] **update-process** [**policy** [**ipv4-acl** *acl-number* | **ip-prefix** *ip-prefix-name*]]
  - **debugging isis update-process interface** [*interface-type interface-number*]

----结束

5.6.12 配置 IS-IS 举例

介绍 IS-IS 的各种组网举例。

IS-IS 基本配置

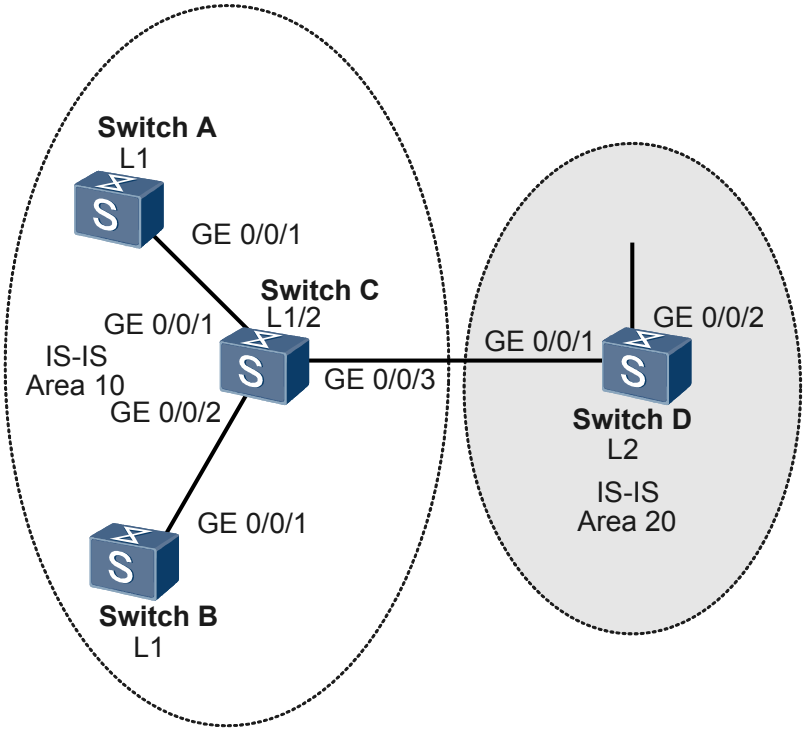
组网需求

如图 5-18 所示：

- SwitchA、SwitchB、SwitchC 和 SwitchD 属于同一自治系统，要求他们之间通过 IS-IS 协议达到 IP 网络互连的目的。
- SwitchA、SwitchB 和 SwitchC 的区域号是 10，SwitchD 的区域号是 20。
- SwitchA 和 SwitchB 是 Level-1 设备，SwitchC 是 Level-1-2 设备，SwitchD 是 Level-2 设备。

版权所有 © 华为技术有限公司

图 5-18 IS-IS 基本配置组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	GE 0/0/1	VLANIF 20	10.1.2.2/24
SwitchC	GE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchC	GE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchC	GE 0/0/3	VLANIF 30	192.168.0.1/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	GE 0/0/2	VLANIF 40	172.16.1.1/24

配置思路

采用如下的思路配置 IS-IS 的基本功能：

1. 配置各物理接口所属的 VLAN。
2. 配置各 VLANIF 接口的 IP 地址。
3. 在各 Switch 上运行 IS-IS 进程，指定网络实体，配置 level 级别。
4. 查看各 Switch 的 IS-IS 数据库信息及路由表信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-18 所示。

版权所有 © 华为技术有限公司

- 各 VLANIF 接口的 IP 地址，具体数据如图 5-18 所示。
- 四台 Switch 的 system id、级别和所属区域号。
  - SwitchA 的 system id 0000.0000.0001，区域号 Area10，为 Level-1 设备。
  - SwitchB 的 system id 0000.0000.0002，区域号 Area10，为 Level-1 设备。
  - SwitchC 的 system id 0000.0000.0003，区域号 Area10，为 Level-1-2 设备。
  - SwitchD 的 system id 0000.0000.0004，区域号 Area20，为 Level-2 设备。

配置步骤

1. 配置各接口所属的 VLAN ID（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 在各 Switch 上运行 IS-IS 进程，指定网络实体，配置 level 级别

   # 配置 SwitchA。
   ```
   [SwitchA] isis 1
   [SwitchA-isis-1] is-level level-1
   [SwitchA-isis-1] network-entity 10.0000.0000.0001.00
   [SwitchA-isis-1] quit
   ```
   # 配置 SwitchB。
   ```
   [SwitchB] isis 1
   [SwitchB-isis-1] is-level level-1
   [SwitchB-isis-1] network-entity 10.0000.0000.0002.00
   [SwitchB-isis-1] quit
   ```
   # 配置 SwitchC。
   ```
   [SwitchC] isis 1
   [SwitchC-isis-1] network-entity 10.0000.0000.0003.00
   [SwitchC-isis-1] quit
   ```
   # 配置 SwitchD。
   ```
   [SwitchD] isis 1
   [SwitchD-isis-1] is-level level-2
   [SwitchD-isis-1] network-entity 20.0000.0000.0004.00
   [SwitchD-isis-1] quit
   ```
4. 在各接口上使能 IS-IS 进程，使能 IS-IS small-hello。

   # 配置 SwitchA。
   ```
   [SwitchA] interface vlanif 10
   [SwitchA-Vlanif10] isis enable 1
   [SwitchA-Vlanif10] quit
   ```
   # 配置 SwitchB。
   ```
   [SwitchB] interface vlanif 20
   [SwitchB-Vlanif20] isis enable 1
   [SwitchB-Vlanif20] quit
   ```
   # 配置 SwitchC。
   ```
   [SwitchC] interface vlanif 10
   [SwitchC-Vlanif10] isis enable 1
   [SwitchC-Vlanif10] quit
   [SwitchC] interface vlanif 20
   [SwitchC-Vlanif20] isis enable 1
   [SwitchC-Vlanif20] quit
   [SwitchC] interface vlanif 30
   [SwitchC-Vlanif30] isis enable 1
   [SwitchC-Vlanif30] quit
   ```
   # 配置 SwitchD。
   ```
   [SwitchD] interface vlanif 30
   [SwitchD-Vlanif30] isis enable 1
   [SwitchD-Vlanif30] quit
   [SwitchD] interface vlanif 40
   [SwitchD-Vlanif40] isis enable 1
   ```


版权所有 © 华为技术有限公司

```
[SwitchD-Vlanif40] quit
```

5. 验证配置结果

查看各 SwitchIS-IS LSDB 信息。

```
[SwitchA] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000006   0xbf7d        649           68       0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        545           68       0/0/0
0000.0000.0003.00-00  0x00000008   0x3340        582           111      1/0/0
0000.0000.0003.01-00  0x00000004   0xa7dd        582           55       0/0/0
0000.0000.0003.02-00  0x00000002   0xc0c4        524           55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchB] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00   0x00000006   0xbf7d        642           68       0/0/0
0000.0000.0002.00-00*  0x00000003   0xef4d        538           68       0/0/0
0000.0000.0003.00-00   0x00000008   0x3340        574           111      1/0/0
0000.0000.0003.01-00   0x00000004   0xa7dd        582           55       0/0/0
0000.0000.0003.02-00   0x00000002   0xc0c4        524           55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchC] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xbf7d        638           68       0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        533           68       0/0/0
0000.0000.0003.00-00* 0x00000008   0x3340        569           111      1/0/0
0000.0000.0003.01-00* 0x00000005   0xa7dd        569           55       0/0/0
0000.0000.0003.02-00* 0x00000003   0xc0c4        569           55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload

                        Level-2 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00* 0x00000008   0x55bb        650           100      0/0/0
0000.0000.0003.03-00* 0x00000003   0xef91        650           55       0/0/0
0000.0000.0004.00-00  0x00000005   0x651         629           84       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchD] display isis lsdb

                      Database information for ISIS(1)
```


版权所有 © 华为技术有限公司

```
                              ------------------------------

                          Level-2 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0003.00-00  0x00000008   0x55bb        644           100     0/0/0
0000.0000.0003.03-00  0x00000003   0xef91        644           55      0/0/0
0000.0000.0004.00-00* 0x00000005   0x651         624           84      0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
```

查看各 SwitchIS-IS 路由信息。Level-1 设备的路由表中应该有一条缺省路由，且下一跳为 Level-1-2 设备，Level-2 设备应该有所有 Level-1 和 Level-2 的路由。

```
[SwitchA] display isis route

                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-1 Forwarding Table
                       --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
0.0.0.0/0            10         NULL     Vlanif10        10.1.1.1        A/-/-/-
 10.1.1.0/24         10         NULL     Vlanif10        Direct          D/-/L/-
 10.1.2.0/24         20         NULL     Vlanif10        10.1.1.1        A/-/-/-
 192.168.0.0/24      20         NULL     Vlanif10        10.1.1.1        A/-/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
[SwitchC] display isis route

                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-1 Forwarding Table
                       --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 10.1.1.0/24         10         NULL     Vlanif10        Direct          D/-/L/-
 10.1.2.0/24         10         NULL     Vlanif20        Direct          D/-/L/-
 192.168.0.0/24      10         NULL     Vlanif30        Direct          D/-/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set


                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 10.1.1.0/24         10         NULL     Vlanif10          Direct        D/-/L/-
 10.1.2.0/24         10         NULL     Vlanif20          Direct        D/-/L/-
 192.168.0.0/24      10         NULL     Vlanif30          Direct        D/-/L/-
 172.16.0.0/16       20         NULL     Vlanif40          192.168.0.2   A/-/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route

                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------
 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
 192.168.0.0/24      10         NULL     Vlanif30        Direct          D/-/L/-
 10.1.1.0/24         20         NULL     Vlanif30        192.168.0.1     A/-/-/-
 10.1.2.0/24         20         NULL     Vlanif30        192.168.0.1     A/-/-/-
 172.16.0.0/16       10         NULL     Vlanif40        Direct          A/-/-/-

    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 20
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0002.00
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10 20 30
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 40
#
isis 1
 is-level level-2
network-entity 20.0000.0000.0004.00
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.16.1.1 255.255.0.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
Return
```

配置 IS-IS 的路由聚合

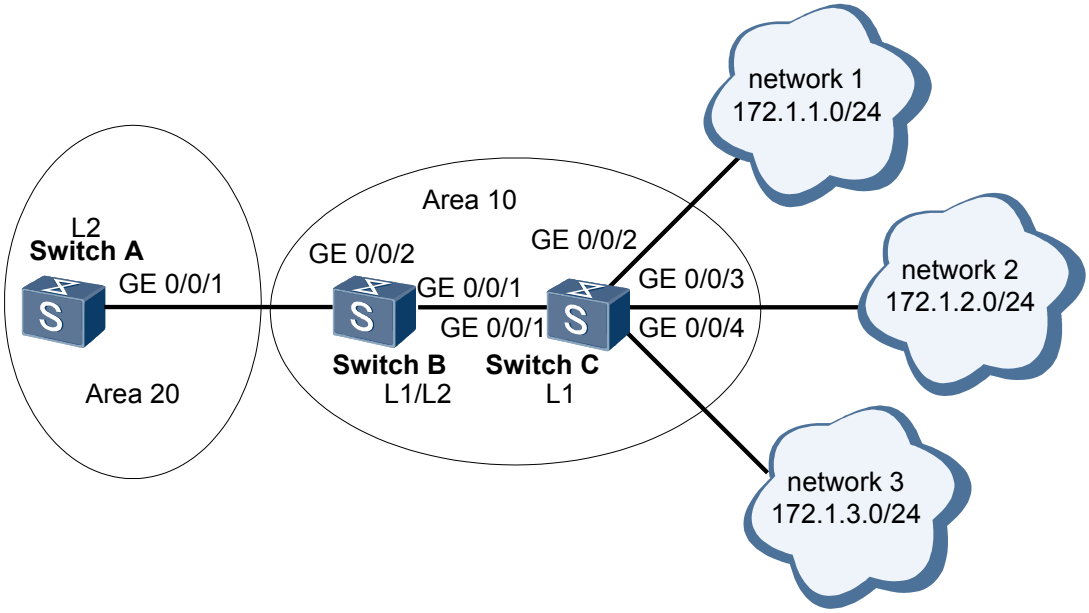
组网需求

如图 5-19 所示：

- SwitchA、SwitchB 和 SwitchC 都运行 IS-IS 路由协议实现互连。
- SwitchA 的区域号 20，SwitchB 和 SwitchC 的区域号是 10。
- SwitchA 是 L2 设备，SwitchB 是 L1/2 设备，SwitchC 是 L1 设备。
- 区域 10 内的地址可以汇总为 172.1.0.0/16。

版权所有 © 华为技术有限公司

图 5-19 配置 IS-IS 的路由聚合组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 50	172.2.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	172.1.4.2/24
SwitchB	GE 0/0/2	VLANIF 50	172.2.1.2/24
SwitchC	GE 0/0/1	VLANIF 10	172.1.4.1/24
SwitchC	GE 0/0/2	VLANIF 20	172.1.1.1/24
SwitchC	GE 0/0/3	VLANIF 30	172.1.2.1/24
SwitchC	GE 0/0/4	VLANIF 40	172.1.3.1/24

配置思路

采用如下的思路配置 IS-IS 的路由聚合：

1. 在各交换机上配置 IS-IS 基本功能，实现互连。
2. 查看 SwitchA 的 IS-IS 路由表信息。
3. 在 SwitchB 上配置路由聚合。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-19 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-19 所示。
- 三台交换机的 system id、级别和所属区域号。
- SwitchA 的 system id 0000.0000.0001，区域号 Area20，为 Level-2 设备。
- SwitchB 的 system id 0000.0000.0002，区域号 Area10，为 Level-1-2 设备。

版权所有 © 华为技术有限公司

- SwitchC 的 system id 0000.0000.0003，区域号 Area10，为 Level-1 设备。

配置步骤

1. 配置各物理接口所属的 VLAN ID（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 IS-IS 基本功能

   # 配置 SwitchA。

```
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-2
[SwitchA-isis-1] network-entity 20.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 50
[SwitchA-Vlanif50] isis enable 1
[SwitchA-Vlanif50] quit
```

   # 配置 SwitchB。

```
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] isis enable 1
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] isis enable 1
[SwitchB-Vlanif50] quit
```

   # 配置 SwitchC。

```
[SwitchC] isis 1
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] isis enable 1
[SwitchC-Vlanif10] quit
```

   VLANIF20、VLANIF30 和 VLANIF40 的配置与 VLANIF10 相同，不再赘述。

4. 查看 SwitchA 的 IS-IS 路由表信息

```
[SwitchA]display isis route

                      Route information for ISIS(1)
                      ------------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 172.1.1.0/24         20         NULL    Vlanif50        172.2.1.2       A/-/-/-
 172.1.2.0/24         20         NULL    Vlanif50        172.2.1.2       A/-/-/-
 172.1.3.0/24         20         NULL    Vlanif50        172.2.1.2       A/-/-/-
 172.1.4.0/24         20         NULL    Vlanif50        172.2.1.2       A/-/-/-
 172.2.1.0/24         10         NULL    Vlanif50        Direct           D/-/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

5. 在 SwitchB 上配置路由聚合

   # 在 SwitchB 上将 172.1.1.0/24、172.1.2.0/24、172.1.3.0./24、172.1.4.0/24 聚合成 172.1.0.0/16。

```
[SwitchB] isis 1
[SwitchB-isis-1] summary 172.1.0.0 255.255.0.0 level-1-2
[SwitchB-isis-1] quit
```


版权所有 © 华为技术有限公司

6. 验证配置结果

查看 SwitchA 的路由表，可以看到 172.1.1.0/24、172.1.2.0/24、172.1.3.0/24 和 172.1.4.0/24 聚合成了 172.1.0.0/16 一条路由。

```
[SwitchA] display isis route

                      Route information for ISIS(1)
                      ------------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 172.1.0.0/16         20         NULL    Vlanif50        172.2.1.2       A/-/-/-
 172.2.1.0/24         10         NULL    Vlanif50        Direct           D/-/L/-
/
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 50
#
isis 1
 is-level level-2
network-entity 20.0000.0000.0001.00
#
interface Vlanif50
 ip address 172.2.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 50
#
isis 1
network-entity 10.0000.0000.0002.00
 summary 172.1.0.0 255.255.0.0 level-1-2
#
interface Vlanif10
 ip address 172.1.4.2 255.255.255.0
 isis enable 1
#
interface Vlanif50
 ip address 172.2.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```


版权所有 © 华为技术有限公司

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10 20 30 40
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
 ip address 172.1.4.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 172.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 172.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.1.3.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 40
#
return
```

配置 IS-IS 的 DIS 选择

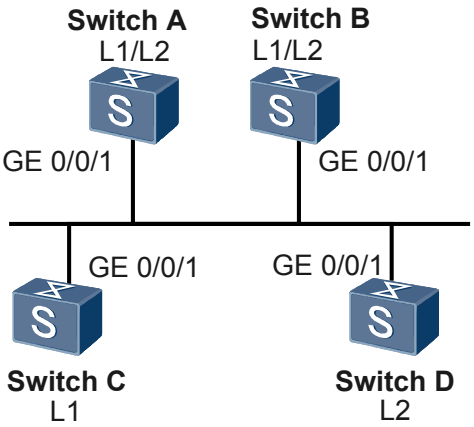
组网需求

如图 5-20 所示：

- SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 IS-IS 路由协议以实现互连。
- SwitchA、SwitchB、SwitchC 和 SwitchD 的区域号是 10。
- SwitchA 和 SwitchB 是 Level-1-2 设备，SwitchC 是 Level-1 设备，SwitchD 是 Level-2 设备。
- 要求通过改变接口的 DIS 优先级，将 SwitchA 配置为 Level-1-2 的 DIS。

版权所有 © 华为技术有限公司

图 5-20 配置 IS-IS 的 DIS 选择组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchC	GE 0/0/1	VLANIF 10	10.1.1.3/24
SwitchD	GE 0/0/1	VLANIF 10	10.1.1.4/24

配置思路

采用如下的思路配置 IS-IS 的 DIS 选择：

1. 在各交换机上配置 IS-IS 基本功能，实现互连。
2. 缺省优先级情况下，查看各台交换机上 IS-IS 接口的信息。
3. 配置交换机的 DIS 优先级。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-20 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-20 所示。
- 四台交换机的 system id、级别和所属区域号。
  - SwitchA 的 system id 0000.0000.0001，区域号 Area10，DIS 优先级 100，为 Level-1-2 设备。
  - SwitchB 的 system id 0000.0000.0002，区域号 Area10，为 Level-1-2 设备。
  - SwitchC 的 system id 0000.0000.0003，区域号 Area10，为 Level-1 设备。
  - SwitchD 的 system id 0000.0000.0004，区域号 Area10，为 Level-2 设备。

配置步骤

1. 配置各接口所属的 VLAN ID（略）
2. 配置各 VLANIF 接口的 IP 地址（略）

版权所有 © 华为技术有限公司

3. 查看各台交换机上 VLANIF10 的 MAC 地址

查看 SwitchA 上接口 VLANIF10 的 MAC 地址。

```
[SwitchA] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.1        0200-0000-dc00              I -         Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

查看 SwitchB 上接口 VLANIF10 的 MAC 地址。

```
[SwitchB] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.2        00e0-fccd-acdf              I -         Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

查看 SwitchC 上接口 VLANIF10 的 MAC 地址。

```
[SwitchC] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.3        00e0-1396-1600              I -         Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

查看 SwitchD 上接口 VLANIF10 的 MAC 地址。

```
[SwitchD] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.4        00e0-fcfd-305c              I -         Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

4. 配置 IS-IS 基本功能

配置 SwitchA。

```
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis enable 1
[SwitchA-Vlanif10] quit
```

配置 SwitchB。

```
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] isis enable 1
[SwitchB-Vlanif10] quit
```

配置 SwitchC。

```
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] isis enable 1
[SwitchC-Vlanif10] quit
```

配置 SwitchD。

```
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 10.0000.0000.0004.00
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] isis enable 1
```


版权所有 © 华为技术有限公司

```
[SwitchD-Vlanif10] quit
```

查看 SwitchA 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer

                      Peer information for ISIS(1)
                      ----------------------------

  System Id    Interface         Circuit Id          State HoldTime Type      PRI
0000.0000.0002 Vlanif10          0000.0000.0002.01 Up    9s       L1(L1L2) 64
0000.0000.0003 Vlanif10          0000.0000.0002.01 Up    27s      L1        64
0000.0000.0002 Vlanif10          0000.0000.0004.01 Up    28s      L2(L1L2) 64
0000.0000.0004 Vlanif10          0000.0000.0004.01 Up    8s       L2        64
```

查看 SwitchA 的 IS-IS 接口信息。

```
[SwitchA] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU  Type  DR
 Vlanif10        001         Up              1427 L1/L2 No/No
```

查看 SwitchB 的 IS-IS 接口信息。

```
[SwitchB] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU  Type  DR
 Vlanif10        001         Up              1427 L1/L2 Yes/No
```

查看 SwitchD 的 IS-IS 接口信息。

```
[SwitchD] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU  Type  DR
 Vlanif10        001         Up              1427 L1/L2 No/Yes
```

说明

从接口信息中可以看到，在使用缺省 DIS 优先级的情况下，在 Level-1 级别的设备中，SwitchB 上接口的 MAC 地址最大，因此 SwitchB 为 Level-1 的 DIS；在 Level-2 级别的设备中，SwitchD 上接口的 MAC 地址最大，因此 SwitchD 为 Level-2 的 DIS。Level-1 和 Level-2 的伪节点分别是 0000.0000.0002.01 和 0000.0000.0004.01。

5. 配置 SwitchA 的 DIS 优先级

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis dis-priority 100
[SwitchA-Vlanif10] quit
```

查看 SwitchA 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer

                      Peer information for ISIS(1)
                      ----------------------------

  System Id    Interface         Circuit Id          State HoldTime Type      PRI
0000.0000.0002 Vlanif10          0000.0000.0001.01   Up    21s      L1(L1L2) 64
0000.0000.0003 Vlanif10          0000.0000.0001.01   Up    27s      L1        64
0000.0000.0002 Vlanif10          0000.0000.0001.01   Up    28s      L2(L1L2) 64
0000.0000.0004 Vlanif10          0000.0000.0001.01   Up    30s      L2        64
```

6. 验证配置结果

查看 SwitchA 的 IS-IS 接口信息。

```
[SwitchA] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU   Type  DR
 Vlanif10        001         Up              1427  L1/L2 Yes/Yes
```

从上述信息中可以看到，在改变 IS-IS 接口的 DIS 优先级后，SwitchA 立即成为 Level-1-2 的 DIS，且伪节点是 0000.0000.0001.01。

版权所有 © 华为技术有限公司

查看 SwitchB 的 IS-IS 邻居和接口信息

```
[SwitchB] display isis peer

                      Peer information for ISIS(1)
                      ----------------------------

  System Id    Interface          Circuit Id          State HoldTime Type      PRI
0000.0000.0001 Vlanif10           0000.0000.0001.01    Up   7s       L1(L1L2) 100
0000.0000.0003 Vlanif10           0000.0000.0001.01    Up   25s      L1         64
0000.0000.0001 Vlanif10           0000.0000.0001.01    Up   7s       L2(L1L2) 100
0000.0000.0004 Vlanif10           0000.0000.0001.01    Up   25s      L2         64
[SwitchB] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU   Type  DR
 Vlanif10        001         Up              1427  L1/L2 No/No
```

查看 SwitchD 的 IS-IS 邻居和接口信息

```
[SwitchD] display isis peer

                      Peer information for ISIS(1)
                      ----------------------------

  System Id    Interface          Circuit Id          State HoldTime Type     PRI
0000.0000.0001 Vlanif10           0000.0000.0001.01    Up   9s       L2      100
0000.0000.0002 Vlanif10           0000.0000.0001.01    Up   28s      L2      64
[SwitchD] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------

 Interface       Id      IPV4.State          MTU   Type  DR
 Vlanif10        001         Up              1427  L1/L2 No/No
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
isis 1
network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 isis dis-priority 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10
#
isis 1
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
 ip address 10.1.1.3 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 10
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0004.00
#
interface Vlanif10
 ip address 10.1.1.4 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

配置 IS-IS 的负载分担

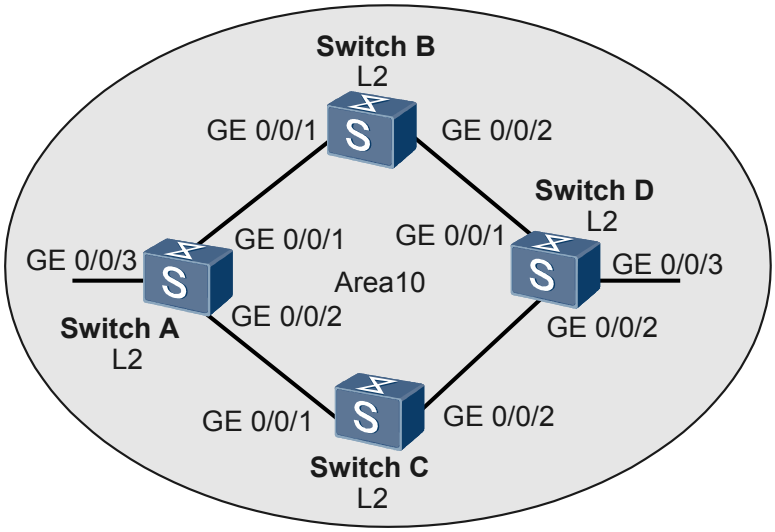
组网需求

如图 5-21 所示：

- SwitchA、SwitchB、SwitchC 和 SwitchD 之间通过 IS-IS 协议达到 IP 网络互连的目的。
- SwitchA、SwitchB、SwitchC 和 SwitchD 的区域号是 10，都是 Level-2 设备。
- 要求配置负载分担，使得 SwitchA 的流量，可以分别通过 SwitchB 和 SwitchC 发送到 SwitchD。

版权所有 © 华为技术有限公司

图 5-21 配置 IS-IS 的负载分担组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchA	GE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchA	GE 0/0/3	VLANIF 50	172.16.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	GE 0/0/2	VLANIF 30	192.168.0.1/24
SwitchC	GE 0/0/1	VLANIF 20	10.1.2.2./24
SwitchC	GE 0/0/2	VLANIF 40	192.168.1.1/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	GE 0/0/2	VLANIF 40	192.168.1.2/24
SwitchD	GE 0/0/3	VLANIF 60	172.17.1.1/24

配置思路

采用如下的思路配置 IS-IS 的负载分担：

1. 在各交换机上配置 IS-IS 基本功能，实现互连。
2. 配置负载分担数目为 1，查看路由表信息。
3. 在 SwitchA 上配置负载分担功能，查看路由表信息。
4. 在 SwitchA 上配置等价路由优先级（可选配置）。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-21 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-21 所示。

版权所有 © 华为技术有限公司

- 四台交换机的 system id、级别和所属区域号。
  - SwitchA 的 system id 0000.0000.0001，区域号 Area10，为 Level-2 设备。
  - SwitchB 的 system id 0000.0000.0002，区域号 Area10，为 Level-2 设备。
  - SwitchC 的 system id 0000.0000.0003，区域号 Area10，为 Level-2 设备。
  - SwitchD 的 system id 0000.0000.0004，区域号 Area10，为 Level-2 设备。
- SwitchA 上负载分担数目为 1。
- SwitchA 的路由负载分担方式。
- SwitchC 的等价路由优先级权值为 1。

配置步骤

1. 配置各接口所属的 VLAN ID（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 IS-IS 的基本功能（略）
4. 在 SwitchA 上配置负载分担数目为 1

```
[SwitchA] isis 1
[SwitchA-isis-1] maximum load-balancing 1
[SwitchA-isis-1] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display isis route

                      Route information for ISIS(1)
                      -----------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost   ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.1.0/24       20        NULL    Vlanif20        10.1.2.2        A/-/-/-
 10.1.1.0/24           10        NULL    Vlanif10         Direct          D/-/L/-
 172.16.1.0/24        10        NULL    Vlanif50        Direct          D/-/L/-
 172.17.1.0/24        30        NULL    Vlanif10        10.1.1.2         A/-/-/-
 10.1.2.0/24           10        NULL    Vlanif20         Direct          D/-/L/-
 192.168.0.0/24       20        NULL    Vlanif10        10.1.1.2         A/-/-/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

从路由表中可以看出，当配置负载分担最大等价路由条数为 1 后，到达目标网段 172.17.1.0 的下一跳为 10.1.1.2。这是由于 SwitchB 的 system ID 较小，所以 IS-IS 优先选择下一跳为 10.1.1.2 为唯一最优路由。

5. 在 SwitchA 上恢复负载分担路由的缺省数量

```
[SwitchA] isis 1
[SwitchA-isis-1] undo maximum load-balancing
[SwitchA-isis-1] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display isis route

                      Route information for ISIS(1)
                      -----------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost   ExtCost ExitInterface   NextHop        Flags
-------------------------------------------------------------------------------
 192.168.1.0/24       20        NULL    Vlanif20        10.1.2.2       A/-/-/-
 10.1.1.0/24           10        NULL    Vlanif10         Direct          D/-/L/-
```


版权所有 © 华为技术有限公司

```
172.16.1.0/24        10         NULL     Vlanif50         Direct           D/-/L/-
172.17.1.0/24        30         NULL     Vlanif10         10.1.1.2         A/-/-/-
                                                Vlanif20         10.1.2.2
10.1.2.0/24           10         NULL     Vlanif20         Direct           D/-/L/-
192.168.0.0/24       20         NULL     Vlanif10         10.1.1.2         A/-/-/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

从路由表可以看出，当恢复负载分担的缺省值后，由于最大等价路由条数的缺省值为 6，因此 SwitchA 的两个下一跳 10.1.1.2（SwitchB）和 10.1.2.2（SwitchC）均成为有效路由。

6. 在 SwitchA 上配置等价路由优先级（可选配置）

   如果我们不希望 SwitchB 和 SwitchC 形成负载分担，可以配置等价路由优先级，指定下一跳。

```
[SwitchA] isis
[SwitchA-isis-1] nexthop 10.1.2.2 weight 1
[SwitchA-isis-1] quit
```

7. 验证配置结果

   # 查看 SwitchA 的路由表。

```
[SwitchA] display isis route
                      Route information for ISIS(1)
                      ------------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.1.0/24       20         NULL     Vlanif20        10.1.2.2        A/-/-/-
 10.1.1.0/24           10         NULL     Vlanif10        Direct          D/-/L/-
 172.16.1.0/24        10         NULL     Vlanif50        Direct          D/-/L/-
 172.17.1.0/24        30         NULL     Vlanif20        10.1.2.2        A/-/-/-
 10.1.2.0/24           10         NULL     Vlanif20        Direct          D/-/L/-
 192.168.0.0/24       20         NULL     Vlanif10        10.1.1.2        A/-/-/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

从路由表中可以看出，当配置等价路由的优先级后，由于下一跳为 10.1.2.2（SwitchC）的优先级（权值为 1）高于下一跳为 10.1.1.2（SwitchB）的优先级，所以 IS-IS 优先选择下一跳为 10.1.2.2 为唯一最优路由。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 50
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0001.00
 nexthop 10.1.2.2 weight
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 30
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
isis 1
is-level level-2
 network-entity 10.0000.0000.0003.00
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
return
```


版权所有 © 华为技术有限公司

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 40 60
#
isis 1

 is-level level-2
 network-entity 10.0000.0000.0004.00
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif60
 ip address 172.17.1.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 60
#
return
```

5.7 BGP 配置

BGP 协议通常应用于大型和复杂的网络，用于在 AS 之间传递路由信息。

5.7.1 BGP 概述

BGP 协议主要用于控制路由的传播和选择最佳路由。

BGP（Border Gateway Protocol）是一种用于自治系统 AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是 BGP-1（RFC1105）、BGP-2（RFC1163）和 BGP-3（RFC1267），当前使用的版本是 BGP-4（RFC4271）。

BGP-4 作为事实上的 Internet 外部路由协议标准，被广泛应用于 ISP（Internet Service Provider）之间。

说明

下文中若不做特殊说明，所指的 BGP 均为 BGP-4。

BGP 特性描述如下：

- BGP 是一种外部网关协议（EGP），与 OSPF、RIP 等内部网关协议（IGP）不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。
- BGP 使用 TCP 作为其传输层协议（端口号 179），提高了协议的可靠性。
- BGP 支持无类别域间路由 CIDR（Classless Inter-Domain Routing）。

版权所有 © 华为技术有限公司

- 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。
- BGP 路由通过携带 AS 路径信息彻底解决路由环路问题。
- BGP 提供了丰富的路由策略，能够对路由实现灵活的过滤和选择。
- BGP 易于扩展，能够适应网络新的发展。

BGP 在交换机上以下列两种方式运行：

- IBGP（Internal BGP）
- EBGP（External BGP）

当 BGP 运行于同一自治系统内部时，被称为 IBGP；当 BGP 运行于不同自治系统之间时，称为 EBGP。

5.7.2 AC6605 中支持的 BGP 特性

系统支持的 BGP 特性包括：负载分担、路由聚合、团体、路由反射器、MP-BGP、BFD for BGP、BGP GR 和 BGP NSR。

几种主要的路由属性

- 源（Origin）属性
- AS 路径（AS_Path）属性
- 下一跳（Next_Hop）属性
- MED（Multi-Exit-Discriminator）属性
- 本地优先级（Local_Pref）属性
- 团体（Community）属性

BGP 选择路由的策略

在 AC6605 的实现中，当到达同一目的地存在多条活跃路由时，BGP 采取如下策略进行路由选择：

1. 优选协议首选值（PrefVal）最高的路由。

   协议首选值（PrefVal）是华为设备的特有属性，该属性仅在本地有效。
2. 优选本地优先级（Local_Pref）最高的路由。

   如果路由没有本地优先级，BGP 选路时将该路由按缺省的本地优先级 100 来处理。通过执行 **default local-preference** 命令可以修改 BGP 路由的缺省本地优先级。
3. 优选本地生成的路由（本地生成的路由优先级高于从邻居学来的路由）。

   本地生成的路由包括通过 **network** 命令或 **import-route** 命令引入的路由、手动聚合路由和自动聚合路由。

   a. 优选聚合路由（聚合路由优先级高于非聚合路由）。

   b. 通过 **aggregate** 命令生成的手动聚合路由的优先级高于通过 **summary automatic** 命令生成的自动聚合路由。

   c. 通过 **network** 命令引入的路由的优先级高于通过 **import-route** 命令引入的路由。
4. 优选 AS 路径（AS_Path）最短的路由。
   - AS_Path 的长度不包括 AS_CONFED_SEQUENCE 和 AS_CONFED_SET。

版权所有 © 华为技术有限公司

- AS_SET 的长度为 1，无论 AS_SET 中包括多少 AS 号。
- 执行 **bestroute as-path-ignore** 命令后，BGP 选路时，忽略 AS_Path 的比较。

5. 比较 Origin 属性，依次优选 Origin 类型为 IGP、EGP、Incomplete 的路由。
6. 优选 MED（Multi Exit Discriminator）值最低的路由。
   - BGP 只比较来自同一个 AS（不包括联盟的子 AS）的路由的 MED 值。即，只有两条路由的 AS_SEQUENCE（不包括 AS_CONFED_SEQUENCE）属性的第一个 AS 号相同时，BGP 才会比较二者的 MED 值。
   - 如果路由没有 MED 属性，BGP 选路时将该路由的 MED 值按缺省值 0 来处理；执行 **bestroute med-none-as-maximum** 命令后，BGP 选路时将该路由的 MED 值按最大值 4294967295 来处理。
   - 执行 **compare-different-as-med** 命令后，BGP 将强制比较来自不同自治系统中的邻居的路由的 MED 值。除非能够确认不同的自治系统采用了同样的 IGP 和路由选择方式，否则不要使用 **compare-different-as-med** 命令（可能产生环路）。
   - 执行 **bestroute med-confederation** 命令后，只有当 AS_Path 中不包含外部 AS 号（不属于联盟的子 AS），且 AS_CONFED_SEQUENCE 的第一个 AS 号相同时，才能比较 MED 值的大小。
   - 执行 **deterministic-med** 命令后，将消除路由接收顺序对选路结果的影响。
7. 优选从 EBGP 邻居学来的路由（EBGP 路由优先级高于 IBGP 路由）。

   依次优选 EBGP 路由、IBGP 路由、LocalCross 路由、RemoteCross 路由。

   PE 上某个 VPN 实例的 VPNv4 路由的 ERT 匹配其他 VPN 实例的 IRT 后复制到该 VPN 实例，称为 LocalCross；从远端 PE 学习到的 VPNv4 路由的 ERT 匹配某个 VPN 实例的 IRT 后复制到该 VPN 实例，称为 RemoteCross。
8. 优选到 BGP 下一跳 IGP Metric 较小的路由。

   说明

   如果配置了负载分担，当上述所有规则相同，且存在多条 As_Path 完全相同的外部路由，则根据配置的路由条数选择多条路由进行负载分担。
9. 优选 Cluster_List 最短的路由。
10. 优选 Router ID 最小的交换机发布的路由。

    说明

    如果路由携带 Originator_ID 属性，选路过程中将比较 Originator_ID 的大小（不再比较 Router ID），并优选 Originator_ID 最小的路由。
11. 比较对等体的 IP Address，优选从具有较小 IP Address 的对等体学来的路由。

应用 BGP 负载分担时的选路策略

在 BGP 中，由于协议本身的特殊性，它产生的路由的下一跳地址可能不是当前交换机直接相连的邻居。常见的一个场景是，IBGP 之间发布路由信息时不改变下一跳。这种情况下，为了能够将报文正确转发出去，交换机必须先找到一个直接可达的地址，通过这个地址到达路由表中指示的下一跳。在上述过程中，去往直接可达地址的路由被称为依赖路由，BGP 路由依赖于这些路由指导报文转发。根据下一跳地址找到依赖路由的过程就是路由迭代（iteration）。

AC6605 支持基于迭代的 BGP 负载分担，即，如果依赖路由本身是负载分担的（假设有三个下一跳地址），则 BGP 也会生成相同数量的下一跳地址来指导报文转发。需要说明的是，基于迭代的 BGP 负载分担并不需要命令配置，这一特性在 AC6605 上始终启用。

BGP 的负载分担与 IGP 的负载分担在实现方法上有所不同：

版权所有 © 华为技术有限公司

- 在 IGP 中，对到达同一目的地址的不同路由，IGP 根据本身的路由算法计算路由的度量值（metric），在度量值相等的路由间进行负载分担。
- BGP 由于本身并没有路由算法，不能根据一个明确的度量值决定是否对路由进行负载分担。但 BGP 有很多路由属性，这些属性在 BGP 选路策略中的优先顺序是不同的。对 BGP 负载分担的处理则是加入到这些选路策略中的，即在所有高优先级路由属性相同的情况下，BGP 根据所配置的最大负载分担的路由条数进行负载分担。

说明

- 缺省情况下，BGP 只对 AS_Path 属性完全相同的路由进行负载分担。可以使用 **bestroute as-path-ignore** 命令配置 BGP 在进行负载分担时不比较路由的 AS_Path 属性。
- BGP 负载分担特性同样适用于联盟内部的自治系统之间。

BGP 发布路由的策略

在 AC6605 的实现中，BGP 发布路由时采用如下策略：

- 存在多条活跃路由时，BGP 发言者（BGP Speaker）只将最优路由发布给对等体；
- BGP 发言者只把自己优选的路由发布给对等体；
- BGP 发言者从 EBGP 获得的路由会向它所有 BGP 对等体发布，但不会向通告该路由的对等体发布（包括 EBGP 对等体和 IBGP 对等体）；
- BGP 发言者从 IBGP 获得的路由不向它的 IBGP 对等体发布；
- BGP 发言者从 IBGP 获得的路由发布给它的 EBGP 对等体；
- 连接一旦建立，BGP 发言者将把自己所有 BGP 优选的路由发布给新对等体。

路由聚合

在大规模的网络中，BGP 路由表十分庞大，使用路由聚合（Route Aggregation）可以大大减小路由表的规模。

路由聚合实际上是将多条路由合并的过程。这样 BGP 在向对等体通告路由时，可以只通告聚合后的路由，而不是将所有的具体路由都通告出去。

AC6605 支持自动聚合和手动聚合方式。使用后者还可以控制聚合路由的属性，以及决定是否发布具体路由。

IBGP 和 IGP 同步

同步是指 IBGP 和 IGP 之间的同步，其目的是为了避免出现误导外部 AS 交换机的现象。

如果设置了同步特性，在 IBGP 路由加入路由表并发布给 EBGP 对等体之前，会先检查 IGP 路由表。只有在 IGP 也知道这条 IBGP 路由时，它才会被加入到路由表，并发布给 EBGP 对等体。

在下面的情况中，可以安全地关闭同步特性。

- 本 AS 不是过渡 AS
- 本 AS 内所有交换机建立 IBGP 全连接

对等体组

对等体组（Peer Group）是一些具有某些相同策略的对等体的集合。当一个对等体加入对等体组中时，此对等体将获得与所在对等体组相同的配置。当对等体组的配置改变时，组内成员的配置也相应改变。

版权所有 © 华为技术有限公司

在大型 BGP 网络中，对等体的数量会很多，其中很多对等体具有相同的策略，在配置时会重复使用一些命令，利用对等体组在很多情况下可以简化配置。

另外，将多个对等体加入同一对等体组中还可以提高路由发布效率。

团体

对等体组可以使一组对等体共享相同的策略，而利用团体属性可以使多个 AS 中的一组 BGP 交换机共享相同的策略。团体是一个路由属性，在 BGP 对等体之间传播，它并不受到 AS 范围的限制。

BGP 交换机在将带有团体属性的路由发布给其它对等体之前，可以改变此路由原有的团体属性。

除了使用公认的团体属性外，用户还可以使用团体属性过滤器过滤自定义扩展团体属性，以便更为灵活的控制路由策略。

路由反射器

为保证 IBGP 对等体之间的路由同步，需要在 IBGP 对等体之间建立全连接关系。假设在一个 AS 内部有 n 台交换机，那么应该建立的 IBGP 连接数就为 n(n-1)/2。当 IBGP 对等体数目很多时，对网络资源和 CPU 资源的消耗都很大。

利用路由反射可以解决这一问题。在一个 AS 内，其中一台交换机作为路由反射器 RR（Route Reflector），其它交换机作为客户机（Client）与路由反射器之间建立 IBGP 连接。路由反射器在客户机之间传递（反射）路由信息，各个客户机之间不需要建立 BGP 连接。

既不是反射器也不是客户机的 BGP 交换机被称为非客户机（Non-Client）。非客户机与路由反射器之间，以及所有的非客户机之间仍然必须建立全连接关系。

MP-BGP 概述

传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就受到一定限制。

为了提供对多种网络层协议的支持，IETF 对 BGP-4 进行了扩展，形成 MP-BGP，目前的 MP-BGP 标准是 RFC2858（Multiprotocol Extensions for BGP-4，BGP-4 的多协议扩展）。

MP-BGP 前向兼容，即支持 BGP 扩展的交换机与不支持 BGP 扩展的交换机可以互通。

MP-BGP 的扩展属性

BGP-4 使用的报文中，与 IPv4 相关的三种路由属性都由 Update 报文携带，这三种路由属性分别是：NLRI（Network Layer Reachability Information）、路径属性中的 Next_Hop、路径属性中的 Aggregator（该属性中包含形成聚合路由的 BGP 发言者的 IP 地址）。

为实现对多种网络层协议的支持，BGP-4 需要将网络层协议的信息反映到 NLRI 及 Next_Hop。MP-BGP 中引入了两个新的路径属性：

- MP_REACH_NLRI：Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。

版权所有 © 华为技术有限公司

- MP_UNREACH_NLRI：Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

这两种属性都是可选非过渡（Optional non-transitive）的，因此，不提供多协议能力的 BGP 发言者将忽略这两个属性，不把它们传递给其它邻居。

地址族

BGP 采用地址族（Address Family）来区分不同的网络层协议，关于地址族的一些取值可以参考 RFC1700（Assigned Numbers）。AC6605 实现多种 MP-BGP 扩展应用，例如对 VPN 的扩展、对 IPv6 的扩展等，不同的扩展应在各自的地址族视图下配置。

BFD for BGP 特性

AC6605 支持在 IPv4 中使用 BFD（Bidirectional Forwarding Detection）为 BGP 邻居关系提供更快速的链路故障检测。

BFD 能够快速检测到 BGP 对等体间的链路故障，并报告给 BGP 协议，从而实现 BGP 路由的快速收敛。

BGP GR

当 BGP 协议重启时会导致对等体关系重新建立和转发中断，使能平滑重启 GR（Graceful Restart）功能后可以避免流量中断。

BGP 安全

- 通过 MD5 和 Key-Chain 对 BGP 邻居的合法性进行验证,防止报文假冒和非法篡改。
- 限制从对等体接收的路由数量，防止资源耗尽性攻击。请参考：**配置 BGP 路由信息的接收策略**。
- AS_Path 长度保护。通过在入口和出口两个方向对 AS_Path 的长度进行限定，直接丢弃 AS_Path 超限的报文。请参考：**配置 AS_Path 属性**。

5.7.3 配置 BGP 的基本功能

只有配置了基本功能，才可以组建 BGP 网络。

建立配置任务

在配置 BGP 的基本功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

本节讲述最基本的 BGP 网络配置过程。

由于 BGP 使用 TCP 连接，所以在配置 BGP 时需要指定对等体的 IP 地址。BGP 对等体不一定就是相邻的交换机，利用逻辑链路也可以建立 BGP 对等体关系。有时为了增强 BGP 连接的稳定性，通常使用 Loopback 接口地址建立连接。

如果需要 BGP 发布本地路由和引入缺省路由，请完成本节配置后参见**配置 BGP 发布本地路由**和**配置 BGP 引入缺省路由**。

版权所有 © 华为技术有限公司

BGP 扩展地址族视图下的多数命令与 BGP 视图下的命令相同，但在扩展地址族视图下配置的命令仅在相应的具体应用中有效。

说明

- 在本节中，不对 BGP 和 MP-BGP 进行严格的区分，命令的适用情况请参考所在的视图。
- 为方便配置，BGP-IPv4 单播地址族视图下的命令可以在 BGP 视图下执行，但在配置文件中这些命令仍位于 BGP-IPv4 单播地址族视图下。

前置任务

在配置 BGP 基本功能之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

在配置 BGP 的基本功能之前，需要准备以下数据。

序号	数据
1	本地 AS 号和 Router ID
2	对等体的 IPv4 地址和 AS 号
3	更新报文的源接口

启动 BGP 进程

启动 BGP 进程是配置所有 BGP 特性的首要步骤。启动 BGP 进程时需指定设备所属的 AS 号。

背景信息

请在需要建立 BGP 连接的交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，启动 BGP（指定本地 AS 编号），进入 BGP 视图。

步骤 3 （可选）执行命令 **router-id** *ipv4-address*，配置 BGP 的 Router ID。

配置或改变 BGP 的 Router ID 会导致交换机之间的 BGP Peer 关系重置。

窍门

为了增加网络的可靠性，建议将 Router ID 手工配置为 Loopback 接口的地址。如果没有配置，则 BGP 会自动选取系统视图下的 Router ID 作为 BGP 协议的 Router ID。系统视图下的 Router ID 选择规则，请参见《AC6605 无线接入控制器 命令参考》。

----结束

版权所有 © 华为技术有限公司

配置 BGP 对等体

配置 BGP 对等体且对等体建立成功后，设备之间才可以交换 BGP 路由信息。

操作步骤

- 配置 IBGP 对等体
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，指定对等体的 IP 地址及其所属的 AS 编号。

     所指定对等体所属的 AS 编号应该和本地 AS 号相同。

     当所指定的对等体的 IP 地址为 Loopback 接口地址，需要再**配置 BGP 连接所使用的本地接口**，以保证 Peer 的正确建立。
  4. （可选）执行命令 **peer** { *ipv4-address* | *group-name* } **description** *description-text*，配置对等体或对等体组的描述信息。

     此命令是可选配置，通过配置描述信息可以方便管理。
- 配置 EBGP 对等体
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，指定对等体的 IP 地址及其所属的 AS 编号。

     所指定对等体所属的 AS 编号应该和本地 AS 号不同。

     当所指定的对等体的 IP 地址为 Loopback 接口地址，需要再**配置 BGP 连接所使用的本地接口**，以保证 Peer 的正确建立。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **ebgp-max-hop** [*hop-count*]，配置 EBGP 连接的最大跳数。

     缺省情况下，EBGP 对等体之间的最大跳数是 1。

     通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 **peer ebgp-max-hop** 命令允许它们之间经过多跳建立 TCP 连接。

     说明

     BGP 使用 Loopback 口建立 EBGP 邻居时，必须配置命令 **peer ebgp-max-hop**（其中 *hop-count*≥2），否则邻居无法建立。
  5. （可选）执行命令 **peer** { *ipv4-address* | *group-name* } **description** *description-text*，配置对等体或对等体组的描述信息。

     此命令是可选配置，通过配置描述信息可以方便管理。

----结束

（可选）配置 BGP 连接所使用的本地接口

两台设备通过多链路建立多个对等体时，需要在设备上配置 BGP 连接所使用的本地接口。

版权所有 © 华为技术有限公司

背景信息

当指定对等体的 IP 地址为非直连的物理链路时，请在交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **peer** { *ipv4-address* | *group-name* } **connect-interface** *interface-type interface-number* [*ipv4-source-address*]，指定 BGP 连接所使用的建立 TCP 连接会话的源接口和源地址。

缺省情况下，BGP 使用与邻居直连的物理接口作为 TCP 连接的本地接口。

为了提高 BGP 连接的可靠性和稳定性，可将 BGP 连接所使用的本地接口配置成 Loopback 接口，这样当网络中存在冗余链路时，不会因为其中某个接口或链路的故障而使 BGP 连接中断。

说明

两台交换机通过多链路建立多个对等体时，建议使用 **peer connect-interface** 指定建立 BGP 连接的接口。

----结束

检查配置结果

BGP 的基本功能配置成功后，可以查看 BGP 对等体的信息。

前提条件

已经完成 BGP 的基本功能的所有配置。

操作步骤

- 使用 **display tcp status** 命令查看 TCP 连接信息。
- 使用 **display bgp peer** [**verbose**]命令查看 BGP 对等体信息。
- 使用 **display bgp peer** *ipv4-address* { **log-info** | **verbose** }命令查看 BGP 对等体信息。

----结束

5.7.4 配置 BGP 的路由属性

BGP 具有很多路由属性，通过配置这些属性可以改变 BGP 的选路策略。

建立配置任务

在配置 BGP 的路由选择前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

BGP 具有很多路由属性，通过配置这些属性可以改变 BGP 的选路策略。

版权所有 © 华为技术有限公司

- BGP 协议优先级

  通过配置 BGP 协议优先级，可以影响 RM 对 BGP 和其他路由协议之间进行路由选路。
- BGP 路由信息的首选值

  通过配置路由信息首选值，当 BGP 路由表中存在到相同目的地址的路由时，优先选择首选值高的路由。
- Local_Pref 属性

  通过配置 Local_Pref 属性值，作用同路由信息首选值，但优先级比它低。
- MED 属性

  通过配置 MED 属性，用于 EBGP 对等体判断流量进入 AS 时的选择 MED 最小的路由。
- Next_Hop 属性

  利用 Next_Hop 属性的变化，可以灵活控制 BGP 的路由选择。
- 团体属性

  团体属性可以简化路由策略的管理。但它比对等体组的管理范围要大得多，它是对多个 BGP 路由器的路由策略进行控制。
- AS_Path 属性

  AS_Path 属性用于防止路由环路和控制路由选择。

前置任务

在配置 BGP 的选路策略之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点的网络层可达
- **配置 BGP 的基本功能**

数据准备

在配置 BGP 选路策略之前，需要准备以下数据。

序号	数据
1	AS 号
2	BGP 协议优先级的值
3	Local_Pref 值
4	MED 值
5	如果使用团体，需要所应用的路由策略名称

配置 BGP 协议优先级

通过配置 BGP 协议优先级，可以影响 BGP 和其他路由协议间的路由选择。

背景信息

请在 BGP 交换机上进行下列配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **preference** { *external internal local* | **route-policy** *route-policy-name* }，设定 BGP 协议的优先级。

BGP 有三种路由：

- 从外部对等体学到的路由（EBGP）
- 从内部对等体学到的路由（IBGP）
- 本地产生的路由（Local Origined），是指通过聚合命令（**summary automatic** 自动聚合和 **aggregate** 手动聚合）所聚合的路由。

可以为这三种路由设定不同的优先级。

另外，还可以通过应用路由策略，为符合匹配条件的特定路由配置优先级。对于不符合匹配条件的路由，则使用缺省优先级。

说明

目前不支持通过 **peer route-policy** 命令在对等体上应用路由策略来设置 BGP 协议的优先级。

----结束

配置 BGP 路由信息的首选值

通过配置路由信息首选值，当 BGP 路由表中存在到相同目的地址的路由时，优先选择首选值高的路由。

背景信息

请在 BGP 路由器上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **peer** { *group-name* | *ipv4-address* } **preferred-value** *value*，为对等体配置首选值。

缺省情况下，从邻居学来的路由的初始首选值为 0。

----结束

配置本机的缺省 Local_Pref 属性值

Local_Pref 属性用于判断流量离开 AS 时的最佳路由。当 BGP 的设备通过不同的 IBGP 对等体得到目的地址相同但下一跳不同的多条路由时，将优先选择 Local_Pref 属性值较高的路由。

版权所有 © 华为技术有限公司

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **default local-preference** *preference*，配置本机的缺省 Local_Pref 属性值。

----结束

配置 MED 属性

MED 属性相当于 IGP 使用的度量值。通过配置 MED 属性，用于 EBGP 对等体判断流量进入 AS 时的选择 MED 最小的路由。

操作步骤

- 配置本机的缺省 MED 值

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **default med** *med*，配置缺省 MED 值。

- 比较来自不同 AS 的路由的 MED 值

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **compare-different-as-med**，比较来自不同 AS 的 MED 值。

     一般情况下，BGP 路由器只比较来自同一 AS（不同对等体）的路由的 MED 属性值。可以通过配置命令来允许 BGP 比较来自不同 AS 的路由的 MED 属性值。

- 配置 MED 值丢失时的处理方式

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **bestroute med-none-as-maximum**，设置当路由没有 MED 值时将其作为最大值处理。

版权所有 © 华为技术有限公司

当路由属性中没有 MED 值时，如果配置了该命令，则 BGP 在选路时将 MED 值作为最大值处理，否则将 MED 当作 0 处理。

----结束

配置 Next_Hop 属性

利用 Next_Hop 属性的变化，可以灵活控制 BGP 的路由选择。

操作步骤

- 向 IBGP 对等体发布路由时，修改下一跳地址

  请在 IBGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **next-hop-local**，配置发布路由时将自身地址作为下一跳。

     在某些组网环境中，为保证 IBGP 邻居能够找到正确的下一跳，可以配置向 IBGP 对等体发布路由时，改变下一跳地址为自身地址。

     缺省情况下，向 IBGP 对等体发布路由时，不修改下一跳地址。

     说明

     如果配置了 BGP 负载分担，则不论是否配置了 **peer next-hop-local** 命令，本地交换机向 IBGP 对等体组发布路由时都先将下一跳地址改变为自身地址。

- 向 IBGP 对等体发布从 IGP 学到的路由时，不修改下一跳地址

  请在引入 IGP 的 IBGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **next-hop-invariable**，配置发布引入的 IGP 路由时不改变该 IGP 路由的下一跳地址。

     缺省情况下，对等体在发布所引入的 IGP 路由时会将下一跳地址改为本地与对端连接的接口地址。

----结束

配置 AS_Path 属性

AS_Path 属性用于防止路由环路和控制路由选择。

操作步骤

- 允许本地 AS 编号重复出现

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
4. 执行命令 **peer** { *ipv4-address* | *group-name* } **allow-as-loop** [*number*]，允许本地 AS 编号重复出现。

   通常情况下，BGP 会检查对等体发来的路由的 AS_Path 属性，如果其中已存在本地 AS 编号，则 BGP 会忽略此路由，以免形成路由环路。

   但在某些特殊应用中，使用此命令可以允许对等体发来的路由的 AS_Path 属性中已存在本地 AS 编号，同时还可以设置允许本地 AS 编号重复出现的次数。

- 配置不将 AS_Path 属性作为选路条件

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **bestroute as-path-ignore**，不将 AS_Path 属性作为选路条件。

- 配置伪 AS 编号

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** { *ipv4-address* | *group-name* } **fake-as** *fake-as-number*，配置伪 AS 编号。

     使用此命令可以将本地真实的 AS 编号隐藏，位于其他 AS 内的 EBGP 对等体只能看到这个伪 AS 编号，即其他 AS 内的对等体在指定本端对等体所在的 AS 编号时，应该设置成这个伪 AS 编号。

     说明

     本命令只能应用于 EBGP 对等体。

- 替换 AS_Path 属性中的 AS 编号

  请在 BGP 交换机上进行下列配置。

  注意

  请谨慎配置命令 **peer substitute-as**，如果配置不当会引起路由环路。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **substitute-as**，替换 AS_Path 属性中的 AS 编号。

版权所有 © 华为技术有限公司

执行命令后，如果 AS_Path 属性中含有对等体所在的 AS 的编号，则在通告给对等体之前，将这些 AS 编号用本地 AS 编号替换。

- 配置 AS_Path 属性中仅携带公有 AS 编号

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **public-as-only**，配置 AS_Path 属性中仅携带公有 AS 编号。

     通常情况下，AS 编号的取值范围是 1 ～ 4294967295，其中公有 AS 编号范围是 1 ～ 64511，65536（x.y 形式为：1.0）～ 4294967295（x.y 形式为：65535.65535），私有 AS 编号范围是 64512 ～ 65534，65535 则作为保留 AS 编号在特殊应用中使用。

     公有 AS 编号可以直接在 Internet 上使用，由因特网地址分配组织 IANA（Internet Assigned Number Authority）管理和分配。私有 AS 编号不能直接发布到 Internet 上，它仅在内部路由域中使用。

     通常情况下，BGP 在向对等体发布路由时携带 AS 编号（可能是公有的 AS 编号，也可能是私有的 AS 编号）。某些情况下，私有 AS 编号信息并不需要被传播出去，这时可以使用此命令配置 AS_Path 属性中仅携带公有 AS 编号。

     该命令只能应用于 EBGP 对等体。

----结束

检查配置结果

BGP 的路由属性配置成功后，可以查看路由的各属性相关信息。

前提条件

已经完成 BGP 路由属性的所有配置。

操作步骤

- 使用 **display bgp paths** [*as-regular-expression*]命令查看 AS 路径信息。
- 使用 **display bgp routing-table different-origin-as** 命令查看源 AS 不一致（目的地址相同）的路由。
- 使用 **display bgp routing-table regular-expression** *as-regular-expression* 命令查看匹配 AS 正则表达式的路由信息。
- 使用 **display bgp routing-table** [*network*] [*mask* | *mask-length*] [**longer-prefixes**]命令查看 BGP 路由表中的信息。
- 使用 **display bgp routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]命令查看指定 BGP 团体的路由信息。
- 使用 **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }命令查看匹配指定 BGP 团体属性过滤器的路由。

----结束

版权所有 © 华为技术有限公司

5.7.5 配置 BGP 过滤器

充分利用 BGP 路由策略，可以灵活的对特定路由进行发送和接收。

建立配置任务

在配置 BGP 路由策略前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

BGP 通过强大的过滤器功能，可以灵活的对特定路由进行发送和接收。

- 相关访问列表

  BGP 有两种专有的访问列表：AS 路径过滤器和团体属性过滤器，在显示 BGP 运行状态和路由策略中都可以使用。

  AS 路径过滤器用来匹配 BGP 路由信息的 AS_Path 属性，过滤掉不符合条件的路由信息。在同一个过滤器编号下，可以定义多条规则（permit 或 deny）。

  团体属性过滤器是标识一系列团体属性信息的列表，分为标准团体访问列表与扩展团体访问列表两种。

- 相关路由策略

  路由策略用来匹配给定的路由信息或者路由信息的某些属性，并在条件满足时改变这些路由信息的属性。匹配条件可以使用前面几种列表。

  一个路由策略可由多个节点构成，每个节点又包括：

  - **If-match** 子句：定义匹配规则，即路由信息通过当前 Route-policy 所需满足的条件，匹配对象是路由信息的某些属性。
  - **Apply** 子句：指定动作，也就是在满足由 **if-match** 子句指定的过滤条件后所执行的一些配置命令，对路由的一些属性进行修改。

- 对接收的路由信息进行控制

  BGP 可以对接收的全局路由信息或者只对某个对等体（组）发来的路由信息进行过滤或使用路由策略。

  由于可能会受到服务攻击，BGP 从邻居接收到任意数量的路由，大量消耗交换机的资源。无论过量 BGP 路由是因为恶意攻击还是因为某错误配置导致，管理员都必须根据网络规划和交换机容量，对运行时所使用的资源进行限制。BGP 可提供 Peer 级的控制，限定邻居发来的路由数量。

- 复位 BGP 连接

  BGP 的选路策略改变后，为了使新的策略生效，必须复位 BGP 连接，但这样会造成短暂的 BGP 连接中断。在 AC6605 的实现中，BGP 支持 Route-refresh 能力。当策略改变后，系统可以在不中断 BGP 连接的情况下，自动对 BGP 路由表进行动态刷新。

  对于邻居是支持 Route-refresh 的交换机，可以执行 **refresh bgp** 命令手工对 BGP 连接进行软复位，完成对路由表的刷新。

  对于邻居是不支持 Route-refresh 的交换机，针对该邻居执行 **peer keep-all-routes** 命令，即可完成对 BGP 路由表的刷新。

前置任务

在配置 BGP 过滤器之前，需完成以下任务：

版权所有 © 华为技术有限公司

- 配置 BGP 的基本功能

数据准备

在控制 BGP 路由信息的发布与接收之前，需要准备以下数据。

序号	数据
1	团体属性值
2	访问列表编号
3	路由策略的名称、节点序号、匹配条件
4	过滤方向（发布/接收）和所使用的路由策略名称

配置 BGP 路由信息的发布策略

配置路由的发布策略后，只有符合条件的路由信息才会进入 BGP 本地路由表，发布给 BGP 对等体。

操作步骤

- 配置 BGP 对全局发布的路由信息进行过滤

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]，对发布的路由信息进行过滤。

     BGP 对引入的路由信息进行过滤后，只有符合条件的路由信息才会进入 BGP 本地路由表，发布给 BGP 对等体。

     指定 *protocol* 参数可以只对特定路由协议的信息进行过滤；如果没有指定此参数，则对所有要发布的 BGP 路由信息进行过滤，包括引入的路由和使用 **network** 命令发布的本地路由。

     说明

     在 **filter-policy** 命令中，如果使用了 ACL 且 ACL 过滤规则中没有指定某个 VPN 实例，则 BGP 是对所有地址族下的路由信息进行过滤，包括来自公网和私网的路由信息。如果 ACL 过滤规则中指定了 VPN 实例，则 BGP 仅对来自该 VPN 的数据流量进行过滤，而不是对路由信息进行过滤。

- 配置对特定对等体发布的路由信息应用路由策略

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

版权所有 © 华为技术有限公司

4. 执行命令 **peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export**，配置出方向路由策略。

   说明

   命令 **peer route-policy export** 中所应用的路由策略不支持将特定接口作为匹配条件，即不支持在路由策略中使用 **if-match interface** 命令。

- 配置对特定对等体发布的路由信息应用过滤器

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 选择执行如下命令，对特定的对等体配置基于不同的过滤器进行路由过滤。
     - 基于 ACL：执行命令 **peer** { *ipv4-address* | *group-name* } **filter-policy** { *acl-number* | **acl-name** *acl-name* } **export**
     - 基于 AS 路径过滤器：执行命令 **peer** { *ipv4-address* | *group-name* } **as-path-filter** *as-path-filter-number* **export**
     - 基于前缀列表：执行命令 **peer** { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **export**

     对等体组的成员可以与所在的组使用不同的出方向路由更新策略，即对外发布路由时，各对等体组可以选择自己的策略。

----结束

配置 BGP 路由信息的接收策略

只有满足接收策略的路由才能被 BGP 接收，并加到路由表中。

操作步骤

- 配置 BGP 对全局接收的路由信息进行过滤

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**，对接收的所有 BGP 路由信息进行过滤。

     对 BGP 接收的路由进行过滤，只有满足某些条件的路由才能被 BGP 接收，并加到路由表中。

- 配置对特定对等体接收的路由信息应用路由策略

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import**，对接收的路由信息应用路由策略。

版权所有 © 华为技术有限公司

说明

命令 **peer route-policy import** 中所应用的路由策略不支持将特定接口作为匹配条件，即不支持在路由策略中使用 **if-match interface** 命令。

- 配置对特定对等体接收的路由信息应用过滤器

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 选择执行如下命令，配置基于不同的过滤器过滤从对等体接收的路由信息。
     - 基于 ACL：执行命令 **peer** { *ipv4-address* | *group-name* } **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**
     - 基于 AS 路径过滤器：执行命令 **peer** { *ipv4-address* | *group-name* } **as-path-filter** *as-path-filter-number* **import**
     - 基于地址前缀列表：执行命令 **peer** { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **import**

  对等体组的成员可以与所在的组使用不同的入方向路由策略，即接收路由时，各对等体可以选择自己的策略。

- 限制从对等体接收的路由数量

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** { *group-name* | *ipv4-address* } **route-limit** *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *times*]，设置允许从对等体（组）收到的路由数量。

     该命令提供 Peer 级的控制，并可根据实际需求选择配置具体参数，来控制 Peer 路由数超限后的行为：

     - 设置 **alert-only** 参数：邻居不中断连接也不再接收超限后的路由，产生告警并记入日志。
     - 设置 **idle-forever** 参数：邻居中断连接，不自动重新尝试建连，产生告警并记入日志。此时通过 **display bgp peer** [**verbose**]查看，可见 peer 的状态为 Idle。如果需要恢复 BGP 连接，可执行命令 **reset bgp**。
     - 设置 **idle-timeout** 参数：邻居中断连接，定时器到时后重新尝试建连，产生告警并记入日志。此时通过 **display bgp peer** [**verbose**]查看，可见 peer 的状态为 Idle。如果需要在定时器到时前恢复 BGP 连接，可执行命令 **reset bgp**。
     - 如果不设置以上三个参数：邻居断连，30 秒后重新尝试建连，产生告警并记入日志。

----结束

配置 BGP 软复位

当策略改变后，系统可以在不中断 BGP 连接的情况下，自动对 BGP 路由表进行动态刷新。

版权所有 © 华为技术有限公司

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

- 使能 Route-refresh 能力
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** { *ipv4-address* | *group-name* } **capability-advertise** { **route-refresh** | **4-byte-as** | **conventional** }，使能 Route-refresh 能力。

     在所有 BGP 交换机使能 Route-refresh 能力的情况下，如果 BGP 的路由策略发生了变化，本地交换机会向对等体发布 Route-refresh 消息，收到此消息的对等体会将其路由信息重新发给本地 BGP 交换机。这样，在不中断 BGP 连接的情况下，就可以对 BGP 路由表进行动态更新，并应用新的策略。
- 保留对等体的所有路由更新
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *ipv4-address* | *group-name* } **keep-all-routes**，保留对等体的所有路由更新。

     配置此命令后，不论是否使用了过滤策略，都将保存指定对等体发来的所有路由更新。当本地路由策略改变时，这些信息可以用来重新生成 BGP 路由。
- 软复位 BGP 连接
  1. 执行命令 **refresh bgp** [**vpn-instance** *vpn-instance-name*] { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }，软复位 BGP 连接。

     请在用户视图下执行 **refresh bgp** 命令。

----结束

检查配置结果

BGP 过滤器配置成功后，可以查看与指定过滤器匹配的路由信息。

前提条件

已经完成 BGP 过滤器的所有配置。

操作步骤

- 使用 **display bgp network** 命令查看 BGP 发布的路由信息。
- 使用 **display bgp routing-table as-path-filter** *as-path-filter-number* 命令查看与指定 AS 路径过滤器匹配的路由信息。
- 使用 **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }命令查看匹配指定 BGP 团体属性过滤器的路由。

版权所有 © 华为技术有限公司

- 使用 **display bgp routing-table peer** *ipv4-address* { **advertised-routes** | **received-routes** } [**statistics**]命令查看 BGP 对等体发布或者收到的路由信息。

----结束

5.7.6 控制路由信息的发布

BGP 可以针对某个对等体对要发布的路由信息进行过滤或使用路由策略。

建立配置任务

在配置控制路由信息的发布前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

- BGP 路由聚合

  在中型或大型 BGP 网络中，在向对等体发布路由信息时，需要配置路由聚合，减小对等体路由表中的路由数量。BGP 支持两种聚合方式：自动聚合和手动聚合。
- 对发布的路由信息进行控制

  BGP 可以针对某个对等体（组）对要发布的路由信息进行过滤或使用路由策略。

前置任务

在配置控制 BGP 路由信息的发布之前，需完成以下任务：

- **配置 BGP 的基本功能**

数据准备

在控制 BGP 路由信息的发布与接收之前，需要准备以下数据。

序号	数据
1	聚合方式和聚合后的路由

配置 BGP 发布本地路由

要发布的本地路由必须存在于本地的 IP 路由表中，使用路由策略可以更为灵活的控制所发布的路由。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

版权所有 © 华为技术有限公司

步骤 3 （可选）执行命令 **ipv4-family unicast**，进入 BGP-IPv4 单播地址族视图。

缺省情况下，系统默认配置在 IPv4 单播地址族视图下。

步骤 4 执行命令 **network** *ipv4-address* [*mask* | *mask-length*] [**route-policy** *route-policy-name*]，配置 BGP 发布精确匹配的本地路由。

指定的目的地址和前缀长度必须与本地 IP 路由表中对应的表项完全一致，路由才能正确发布。如果网络掩码没有指定，此路由将被按照自然网段精确匹配。

要发布的本地路由必须存在于本地的 IP 路由表中，使用路由策略可以更为灵活的控制所发布的路由。

----结束

配置 BGP 路由聚合

配置路由聚合，可以减小对等体路由表中的路由数量。BGP 支持两种聚合方式：自动聚合和手动聚合。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

- 配置自动聚合
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **summary automatic**，配置子网路由自动聚合。

     该命令对 BGP 引入的路由进行聚合，引入的路由可以是直连路由、静态路由、RIP 路由、OSPF 路由、IS-IS 路由。但该命令对 **network** 命令引入的路由无效。
- 配置手动聚合
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **aggregate** *ipv4-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*] *，配置手动路由聚合。

     手动聚合对 BGP 本地路由表中已经存在的路由表项有效，例如 BGP 路由表中不存在路由 10.1.1.1/24，即使配置了命令 **aggregate 10.1.1.1 16** 对其进行聚合，BGP 也不会将这条聚合路由发布出去。

     使用手动聚合时可以应用多种策略，并可以设置路由的属性。

----结束

版权所有 © 华为技术有限公司

配置向对等体发送缺省路由

不论本地路由表中是否存在缺省路由，都将向指定对等体发布一条下一跳地址为本地地址的缺省路由。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **peer** { *group-name* | *ipv4-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all** { *ipv4-address1* { *mask1* | *mask-length1* } } &<1-4> | **conditional-route-match-any** { *ipv4-address2* { *mask2* | *mask-length2* } } &<1-4>]，向对等体或对等体组发送缺省路由。

说明

执行 **peer default-route-advertise** 命令后，不论本地路由表中是否存在缺省路由，都将向指定对等体发布一条下一跳地址为本地地址的缺省路由。

----结束

检查配置结果

控制路由信息的发布配置成功后，可以查看与指定过滤器匹配的发布路由信息。

前提条件

已经完成控制路由信息的发布的所有配置。

操作步骤

- 使用 **display bgp network** 命令查看 BGP 发布的路由信息。
- 使用 **display bgp routing-table cidr** 命令查看 CIDR 路由信息。
- 使用 **display bgp routing-table peer** *ipv4-address* { **advertised-routes** | **received-routes** } [**statistics**]命令查看 BGP 对等体发布或者收到的路由信息。

----结束

5.7.7 控制路由信息的引入

通过引入其它协议的路由，可以丰富 BGP 路由表。在引入 IGP 路由时，还可以针对不同的路由协议来对路由信息进行过滤。

建立配置任务

在配置控制路由信息的引入前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

BGP 可以向邻居 AS 发送本地 AS 内部网络的路由信息，但 BGP 不是自己去发现 AS 内部的路由信息，而是引入 IGP 的路由信息到 BGP 路由表中，并发布给对等体。在引入 IGP 路由时，还可以针对不同的路由协议来对路由信息进行过滤。

前置任务

在配置控制路由信息的引入之前，需完成以下任务：

- **配置 BGP 的基本功能**

数据准备

无

配置 BGP 引入缺省路由

BGP 引入缺省路由时，只用于引入本地路由表中已经存在的缺省路由。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **default-route imported**，允许 BGP 引入缺省路由。

----结束

配置 BGP 引入路由

BGP 可以引入其它协议的路由。当引入动态路由协议时，需要指定协议进程号。使用路由策略可以更为灵活的引入所需路由。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **import-route** *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *，配置 BGP 引入其他协议的路由。

版权所有 © 华为技术有限公司

说明

引入 IS-IS、OSPF 或 RIP 时，需要指定协议进程号。

如果没有配置 **default-route imported** 命令，则使用 **import-route** 命令引入其他协议的路由时，不能引入缺省路由。

----结束

检查配置结果

控制路由信息的引入配置成功后，可以查看与指定过滤器匹配的引入路由信息。

前提条件

已经完成控制路由信息的引入的所有配置。

操作步骤

- 使用 **display bgp routing-table as-path-filter** *as-path-filter-number* 命令查看与指定 AS 路径过滤器匹配的路由信息。
- 使用 **display bgp routing-table cidr** 命令查看 CIDR 路由信息。
- 使用 **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }命令查看匹配指定 BGP 团体属性过滤器的路由。

----结束

5.7.8 配置 BGP 对等体间连接参数

通过配置 BGP 对等体间连接参数，可以对 BGP 网络的性能进行调整和优化。

建立配置任务

在配置 BGP 对等体间连接参数前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当对等体间建立了 BGP 连接后，它们定时向对端发送 Keepalive 消息，以防止交换机认为 BGP 连接已中断。若交换机在设定的连接保持时间（Hold time）内未收到对端的 Keepalive 消息或任何其它类型的报文，则认为此 BGP 连接已中断，从而退出此 BGP 连接。

交换机在与对等体建立 BGP 连接时，将比较双方保持时间，以数值较小者作为协商后的保持时间。如果协商结果为 0，则不发送 Keepalive 消息，且不检测 Hold time 是否超时。

定时器取值的改变会造成短暂的 BGP 连接中断，这是因为对等体双方要重新进行协商。

前置任务

在配置 BGP 对等体间连接参数之前，需完成以下任务：

版权所有 © 华为技术有限公司

- **配置 BGP 的基本功能**

数据准备

在配置 BGP 对等体间连接参数之前，需要准备以下数据。

序号	数据
1	BGP 定时器的值
2	发送更新报文的时间间隔

配置 BGP 定时器

合理的定时器可以增强网络性能。需要注意，改变 BGP 定时器的值会导致对等体关系中断。

背景信息

注意

改变定时器的值（执行 **timer** 或 **peer timer** 命令）会导致交换机之间的 BGP Peer 关系中断。务必仔细确认是否必须改变定时器的值。

操作步骤

- 配置全局定时器

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **timer keepalive** *keepalive-time* **hold** *hold-time*，配置 BGP 定时器。

     合理的最大 Keepalive 消息发送间隔为保持时间的三分之一，且该发送间隔不能小于 1 秒，因此，保持时间如果不为 0，则最小为 3 秒。缺省情况下，存活时间为 60 秒，保持时间为 180 秒。

     说明

     建议配置的保持时间大于 20 秒。如果保持时间小于 20 秒，可能会造成邻居会话的中断。

     以下两种定时器取值配置需要尽量避免：

     - *keepalive-time* 值和 *hold-time* 值同时取 0，这种配置将导致 BGP 定时器无效，即 BGP 不会根据定时器检测链路故障。
     - *hold-time* 值远大于 *keepalive-time* 值，如 **timer keepalive 1 hold 65535**，过长的保持时间不能保证及时检测到链路的故障。

     当对等体建立连接之后，实际的 *keepalive-time* 值和 *hold-time* 值是通过双方协商来确定的。其中，取对等体双方的 Open 报文中的 *hold-time* 的较小值为最终

版权所有 © 华为技术有限公司

的 *hold-time* 值；取（协商的 *hold-time* 值÷3）和本地配置的 *keepalive-time* 值中较小的作为最终的 *keepalive-time* 值。

- 配置对等体的定时器

  请在 BGP 交换机上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **peer** { *ipv4-address* | *group-name* } **timer keepalive** *keepalive-time* **hold** *hold-time*，配置对等体或对等体组的 keepalive 发送间隔和保持时间。

     存活时间和保持时间的取值关系同**配置全局定时器**。

     对等体定时器的优先级高于全局定时器。

----结束

配置更新报文的发送时间间隔

路由变化时，交换机会发送 Update 报文通知对等体。但如果同一路由频繁变化时，为避免每次变化交换机都要发送 Update 报文给对等体，可以配置发送该同一路由的 Update 报文的时间间隔。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **peer** { *ipv4-address* | *group-name* } **route-update-interval** *interval*，配置更新报文的发送时间间隔。

----结束

使能 EBGP 连接快速复位

使能 EBGP 连接快速复位后，当 EBGP 链路出现故障时，BGP 可以迅速感知并立即复位该接口上的 BGP 连接。

背景信息

请在 BGP 交换机上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ebgp-interface-sensitive**，使能 EBGP 连接快速复位。

版权所有 © 华为技术有限公司

- 使能此功能后，当 EBGP 链路出现故障时，BGP 可以迅速感知并立即复位该接口上的 BGP 连接。
- 去使能此功能后，可以防止路由振荡带来的 BGP 会话的反复重建与删除，一定程度上节约了网络带宽。

----结束

检查配置结果

BGP 对等体间连接参数配置成功后，可以查看 BGP 对等体和对等体组信息。

前提条件

已经完成 BGP 对等体间连接参数的所有配置。

操作步骤

- 使用 **display bgp peer [verbose]**命令查看 BGP 对等体信息。

----结束

任务示例

配置完成后，在系统视图下，执行 **display bgp peer verbose** 命令，可以看到以上配置的存活时间和保持时间、更新报文的发送时间间隔等。

```
<Quidway> display bgp peer verbose

        BGP Peer is 10.1.1.1,  remote AS 100
        Type: IBGP link
        BGP version 4, Remote router ID 1.1.1.1
        Update-group ID: 0
        BGP current state: Established, Up for 00h00m05s
        BGP current event: RecvKeepalive
        BGP last state: OpenConfirm
        BGP Peer Up count: 2
        Received total routes: 0
        Received active routes total: 0
        Advertised total routes: 0
        Port:  Local - 55219    Remote - 179
                Configured: Active Hold Time: 100 sec   Keepalive Time:30 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 100 sec   Keepalive Time:30 sec
        Peer optional capabilities:
        Peer supports bgp multi-protocol extension
        Peer supports bgp route refresh capability
        Peer supports bgp 4-byte-as capability
        Address family IPv4 Unicast: advertised and received
 Received: Total 2 messages
                Update messages               0
                Open messages                 1
                KeepAlive messages            1
                Notification messages         0
                Refresh messages              0
 Sent: Total 2 messages
                Update messages               0
                Open messages                 1
                KeepAlive messages            1
                Notification messages         0
                Refresh messages              0
 Authentication type configured: None
 Last keepalive received: 2010/11/17 15:51:57 UTC-08:00
 Minimum route advertisement interval is 20 seconds
```


版权所有 © 华为技术有限公司

```
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

5.7.9 配置 BFD for BGP

通过配置 BFD for BGP 功能，为 BGP 提供更为快速的故障检测机制，提高网络收敛速度。

建立配置任务

在配置 BFD for BGP 前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

BGP 协议通过周期性的向对等体发送 Keepalive 报文来实现邻居检测机制。但这种机制检测到故障所需时间比较长，超过 1 秒钟。当数据达到吉比特速率级时，这么长的检测时间将导致大量数据丢失，无法满足电信级网络高可靠性的需求。

因此，BGP 协议通过引入 BFD for BGP 特性，利用 BFD 的快速检测机制，迅速发现 BGP 对等体间链路的故障，从而提高网络收敛速度。

前置任务

在配置 BFD for BGP 特性之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up
- **配置 BGP 的基本功能**

数据准备

在配置 BFD for BGP 之前，需准备以下数据。

序号	数据
1	启用 BFD 特性的接口的类型和编号
2	BFD 的相关检测参数：最小接收间隔、最大接收间隔、检测时间倍数

配置公网 BFD for BGP

通过配置 BFD for BGP，可以快速检查 BGP 路由的状态。当对等体的状态是 Established 时，BFD 会话才能被创建。

背景信息

请在链路两端需要建立 BFD 会话的 BGP 路由器上均进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，对本节点使能全局 BFD 能力。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 5 （可选）执行命令 **peer** { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *命令，指定需要建立 BFD 会话的各个参数值。

步骤 6 执行命令 **peer** { *group-name* | *ipv4-address* } **bfd enable**，配置对等体或对等体组的 BFD 功能，建立 BFD 会话。

如果在对等体组上配置了 BFD 特性，则属于该对等体组且没有使能 **peer bfd block** 的 peer 都将创建 BFD 会话。

说明

- BGP 会话处于 Established 状态时，BFD 会话才能够建立。
- 如果 peer 上配置 BFD 参数，建立的 BFD 会话以 peer 上的配置为准。

步骤 7 （可选）执行命令 **peer** *ipv4-address* **bfd block**，阻止对等体从对等体组中继承 BFD 功能。

当 Peer 加入了 Group 且这个 Group 使能了 BFD 特性，Peer 会继承这个 Group 的 BFD 特性，创建 BFD 会话。如果不希望 Peer 从 Group 继承 BFD 特性，可以阻止对等体从对等体组中继承 BFD 功能。

说明

peer bfd block 命令和 **peer bfd enable** 命令是两条互斥命令，配置 **peer bfd block** 命令后，会自动删除 BFD 会话。

----结束

配置私网 BFD for BGP

在 VPN 网络中，通过配置 BFD for BGP，可以快速检测私网 BGP 路由的状态。当对等体的状态是 Established 时，BFD 会话才能被创建。

背景信息

请在链路两端需要建立 BFD 会话的 BGP 交换机上均进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，对本节点使能全局 BFD 能力。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 5 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例视图。

版权所有 © 华为技术有限公司

步骤 6 （可选）执行命令 **peer** { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *命令，指定需要建立 BFD 会话的各个参数值。

步骤 7 执行命令 **peer** { *group-name* | *ipv4-address* } **bfd enable**，配置对等体或对等体组的 BFD 功能，建立 BFD 会话。

如果在对等体组上配置了 BFD 特性，则属于该对等体组且没有使能 **peer bfd block** 的 peer 都将创建 BFD 会话。

说明

- BGP 会话处于 Established 状态时，BFD 会话才能够建立。
- 如果 peer 上配置 BFD 参数，建立的 BFD 会话以 peer 上的配置为准。

步骤 8 （可选）执行命令 **peer** *ipv4-address* **bfd block**，阻止对等体从对等体组中继承 BFD 功能。

当 Peer 加入了 Group 且这个 Group 使能了 BFD 特性，Peer 会继承这个 Group 的 BFD 特性，创建 BFD 会话。如果不希望 Peer 从 Group 继承 BFD 特性，可以阻止对等体从对等体组中继承 BFD 功能。

说明

peer bfd block 命令和 **peer bfd enable** 命令是两条互斥命令，配置 **peer bfd block** 命令后，会自动删除 BFD 会话。

----结束

检查配置结果

BFD for BGP 配置成功后，可以查看 BGP 建立的 BFD 会话信息。

前提条件

已经完成 BFD for BGP 的所有配置。

操作步骤

- 使用 **display bgp bfd session** { [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** *ipv4-address* | **all** }命令查看 BGP 建立的 BFD 会话信息。
- 使用 **display bgp** [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** [[*ipv4-address*] **verbose**]命令查看 BGP 对等体信息。

----结束

5.7.10 配置 BGP 负载分担

通过配置 BGP 负载分担，可以合理利用网络资源。

建立配置任务

在配置 BGP 负载分担前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

只有路由属性中，**5.7.2 AC6605 中支持的 BGP 特性**中“BGP 选择路由的策略”所描述的前 8 个属性完全相同，且 AS-Path 属性也相同时，才能成为 BGP 等价路由，实现 BGP 的负载分担。

前置任务

在配置 BGP 负载分担之前，需完成以下任务：

- **5.7.3 配置 BGP 的基本功能**

数据准备

在配置 BGP 负载分担之前，需要准备以下数据。

序号	数据
1	配置负载分担的路由条数

配置 BGP 负载分担的路由条数

BGP 邻居之间存在多条等价链路时，可以实现负载分担。

操作步骤

- 配置 BGP 路由负载分担的路由条数

  请在 BGP 路由器上进行下列配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **maximum load-balancing** *number*，配置 BGP 负载分担的路由条数。

     缺省情况下，BGP 负载分担的路由条数为 1。

----结束

检查配置结果

BGP 负载分担配置成功后，可以查看路由的分担信息。

前提条件

已经完成 BGP 负载分担的所有配置。

操作步骤

- 使用 **display bgp routing-table** [*network*] [*mask* | *mask-length*] [**longer-prefixes**]命令查看 BGP 路由表中的信息。

版权所有 © 华为技术有限公司

- 使用 **display ip routing-table** [**verbose**]命令查看路由表信息。

----结束

5.7.11 配置 BGP 安全性

为提高 BGP 的安全性，可以在建立 TCP 连接时进行认证。

建立配置任务

在配置提高 BGP 网络的安全性前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

- BGP 验证

  BGP 使用 TCP 作为传输层协议，为提高 BGP 的安全性，可以在建立 TCP 连接时进行 MD5 认证。但 BGP 的 MD5 认证并不能对 BGP 报文认证，它只是为 TCP 连接设置 MD5 认证密码，由 TCP 完成认证。如果认证失败，则不建立 TCP 连接。

前置任务

在配置 BGP 的安全性之前，需完成以下任务：

- **配置 BGP 的基本功能**

数据准备

在配置 BGP 安全性之前，需要准备以下数据。

序号	数据
1	各交换机的 BGP 对等体的 IP 地址或者对等体组的名称
2	MD5 验证密码
3	Key-Chain 认证的名称

配置 MD5 验证

BGP 的 MD5 认证只是为 TCP 连接设置 MD5 认证密码，由 TCP 完成认证。如果认证失败，则不建立 TCP 连接。

背景信息

请在 BGP 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **peer** { *ipv4-address* | *group-name* } **password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置 MD5 认证密码。

说明

当在 BGP 视图下配置时，对 MP-BGP 的 VPNv4 扩展同样有效，因为它们使用同一个 TCP 连接。

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

----结束

检查配置结果

BGP 网络安全性配置成功后，可以查看对等体的认证信息。

前提条件

已经完成 BGP 安全性的所有配置。

操作步骤

- 使用 **display bgp peer** [*ipv4-address*] **verbose** 命令查看 BGP 对等体的信息。

----结束

5.7.12 BGP 维护

BGP 维护包括复位 BGP 连接和清除 BGP 的统计信息。

复位 BGP 连接

可以选择以 GR 的方式复位 BGP。复位 BGP 连接会导致对等体关系中断。

背景信息

注意

复位 BGP 连接（执行 **reset bgp** 命令）会导致交换机之间的 BGP Peer 关系中断。务必仔细确认是否必须执行复位 BGP 连接的操作。

当 BGP 路由策略（交换机不支持 Router Refresh）发生变化后，需要通过复位 BGP 连接使新的配置生效。如果需要复位 BGP 连接，可在用户视图下选择执行以下命令。

操作步骤

- 在确认需要复位所有 BGP 连接后，请在用户视图下执行 **reset bgp all** 命令。
- 在确认需要复位与指定 AS 之间的 BGP 连接后，请在用户视图下执行 **reset bgp** *as-number* 命令。

版权所有 © 华为技术有限公司

- 在确认需要复位与指定对等体的 BGP 连接后，请在用户视图下执行 **reset bgp** *ipv4-address* 命令。
- 在确认需要复位所有 EBGP 连接后，请在用户视图下执行 **reset bgp external** 命令。
- 在确认需要复位与指定对等体组的 BGP 连接后，请在用户视图下执行 **reset bgp group** *group-name* 命令。
- 在确认需要复位所有 IBGP 连接后，请在用户视图下执行 **reset bgp internal** 命令。

----结束

调试 BGP

只要在用户视图下打开相应模块的调试开关，设备就能够产生调试信息。调试信息显示被调试模块接受或者发送数据报的信息内容。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 BGP 运行故障时，请在用户视图下执行表中的 **debugging** 命令对 BGP 进行调试，查看调试信息，定位故障并分析故障原因。打开调试开关的操作步骤请参考《AC6605 无线接入控制器 配置指南-系统管理》中“维护与调试”的内容。

有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 命令参考》。

操作步骤

- 在用户视图下执行 **debugging bgp all** 命令，打开 BGP 所有调试信息开关。
- 在用户视图下执行 **debugging bgp event** 命令，打开 BGP 事件调试信息开关。
- 在用户视图下执行 **debugging bgp** { **keepalive** | **open** | **packet** | **route-refresh** } [**receive** | **send**] [**verbose**]命令，打开 BGP 报文调试信息开关。
- 在用户视图下执行 **debugging bgp update** [**ipv4** | **vpn-instance** *vpn-instance-name*] [**peer** *ipv4-address* | **acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]命令，打开 BGP 更新报文调试信息开关。

----结束

5.7.13 配置 BGP 举例

介绍 BGP 的各种组网举例。

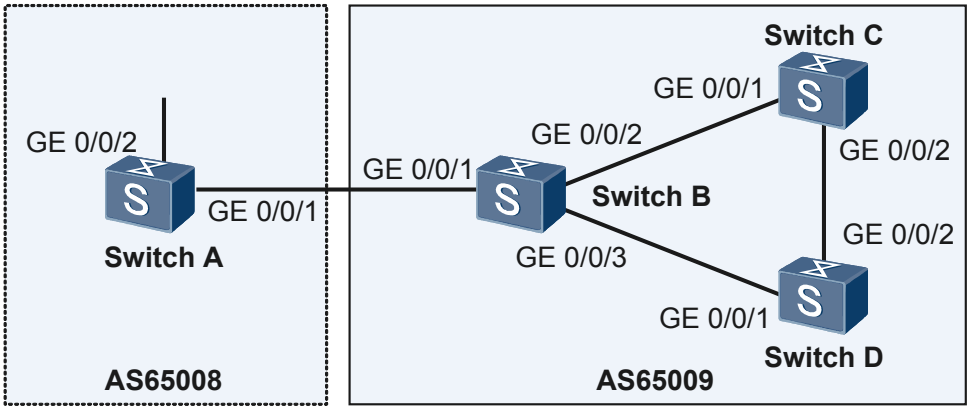
配置 BGP 的基本功能示例

组网需求

如图 5-22 所示，所有 Switch 均运行 BGP 协议，SwitchA 和 SwitchB 之间建立 EBGP 连接，SwitchB、SwitchC 和 SwitchD 之间建立 IBGP 全连接。

版权所有 © 华为技术有限公司

图 5-22 配置 BGP 基本组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	200.1.1.2/24
SwitchA	GE 0/0/2	VLANIF 50	8.1.1.1/8
SwitchB	GE 0/0/1	VLANIF 10	200.1.1.1/24
SwitchB	GE 0/0/2	VLANIF 20	9.1.3.1/24
SwitchB	GE 0/0/3	VLANIF 30	9.1.1.1/24
SwitchC	GE 0/0/1	VLANIF 20	9.1.3.2/24
SwitchC	GE 0/0/2	VLANIF 40	9.1.2.1/24
SwitchD	GE 0/0/1	VLANIF 30	9.1.1.2/24
SwitchD	GE 0/0/2	VLANIF 40	9.1.2.2/24

配置思路

采用如下的思路配置 BGP 的基本功能：

1. 在 SwitchB、SwitchC、SwitchD 之间配置 IBGP 连接。
2. 在 SwitchA 和 SwitchB 之间配置 EBGP 连接。
3. 在 SwitchA 上通过 **network** 命令发布路由，查看 SwitchA、SwitchB、SwitchC 的路由表信息。
4. 在 SwitchB 上配置 BGP 引入直连路由，查看 SwitchA、SwitchC 的路由表信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-22 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-22 所示。
- SwitchA 的 Router ID 1.1.1.1，所在的 AS 号 65008。
- SwitchB、SwitchC、SwitchD 的 router id 分别为 2.2.2.2、3.3.3.3、4.4.4.4，所在的 AS 号 65009。

版权所有 © 华为技术有限公司

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 IBGP 连接

   # 配置 SwitchB。

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] peer 9.1.3.2 as-number 65009
```

   # 配置 SwitchC。

```
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 9.1.3.1 as-number 65009
[SwitchC-bgp] peer 9.1.2.2 as-number 65009
[SwitchC-bgp] quit
```

   # 配置 SwitchD。

```
[SwitchD] bgp 65009
[SwitchD-bgp]  router-id 4.4.4.4
[SwitchD-bgp] peer 9.1.1.1 as-number 65009
[SwitchD-bgp] peer 9.1.2.1 as-number 65009
[SwitchD-bgp] quit
```

4. 配置 EBGP

   # 配置 SwitchA。

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
```

   # 配置 SwitchB。

```
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] quit
```

   # 查看 BGP 对等体的连接状态。

```
[SwitchB] display bgp peer

 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3                 Peers in established state : 3

  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  9.1.1.2         4 65009       49       62     0 00:44:58 Established       0
  9.1.3.2         4 65009       56       56     0 00:40:54 Established       0
  200.1.1.2       4 65008       49       65     0 00:44:03 Established       1
```

   可以看出，SwitchB 到其它 Switch 的 BGP 连接均已建立。

5. 配置 SwitchA 发布路由 8.0.0.0/8

   # 配置 SwitchA 发布路由。

```
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-af-ipv4] network 8.0.0.0 255.0.0.0
[SwitchA-bgp-af-ipv4] quit
[SwitchA-bgp] quit
```

   # 查看 SwitchA 路由表信息。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
```


版权所有 © 华为技术有限公司

```
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>  8.0.0.0         0.0.0.0         0                    0      i
```

查看 SwitchB 的路由表。

```
[SwitchB] display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>  8.0.0.0         200.1.1.2       0                    0      65008i
```

查看 SwitchC 的路由表。

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 1

 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  8.0.0.0         200.1.1.2       0          100        0      65008i
```

从路由表可以看出，SwitchC 虽然学到了 AS65008 中的 8.0.0.0 的路由，但因为下一跳 200.1.1.2 不可达，所以也不是有效路由。

6. 配置 BGP 引入直连路由

配置 SwitchB。

```
[SwitchB] bgp 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] import-route direct
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

查看 SwitchA 的 BGP 路由表。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 4

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>  8.0.0.0           0.0.0.0         0                      0      i
 *>  9.1.1.0/24        200.1.1.1       0                      0      65009?
 *>  9.1.3.0/24        200.1.1.1       0                      0      65009?
 *   200.1.1.0         200.1.1.1       0                      0      65009?
```

查看 SwitchC 的路由表。

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 4
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 * i  8.0.0.0         200.1.1.2       0          100        0      65008i
```


版权所有 © 华为技术有限公司

```
 *>i  9.1.1.0/24      9.1.3.1         0          100        0      ?
   i  9.1.3.0/24      9.1.3.1         0          100        0      ?
 *>i  200.1.1.0       9.1.3.1         0          100        0      ?
```

可以看出，到 8.0.0.0 的路由变为有效路由，下一跳为 SwitchA 的地址。

使用 Ping 进行验证。

```
[SwitchC] ping 8.1.1.1
  PING 8.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=254 time=47 ms
    Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=254 time=16 ms
    Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=254 time=31 ms

  --- 8.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 16/31/47 ms
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 50
#
interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
interface Vlanif50
 ip address 8.1.1.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 50
#
bgp 65008
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  network 8.0.0.0
  peer 200.1.1.1 enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20 30
#
interface Vlanif10
 ip address 200.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 9.1.3.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.1 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
 router-id 2.2.2.2
 peer 9.1.1.2 as-number 65009
 peer 9.1.3.2 as-number 65009
 peer 200.1.1.2 as-number 65008
#
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 9.1.1.2 enable
  peer 9.1.3.2 enable
  peer 200.1.1.2 enable
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 9.1.3.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
bgp 65009
 router-id 3.3.3.3
 peer 9.1.3.1 as-number 65009
 peer 9.1.2.2 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  peer 9.1.3.1 enable
  peer 9.1.2.2 enable
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 40
#
interface Vlanif30
 ip address 9.1.1.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.2 255.255.255.0
```


版权所有 © 华为技术有限公司

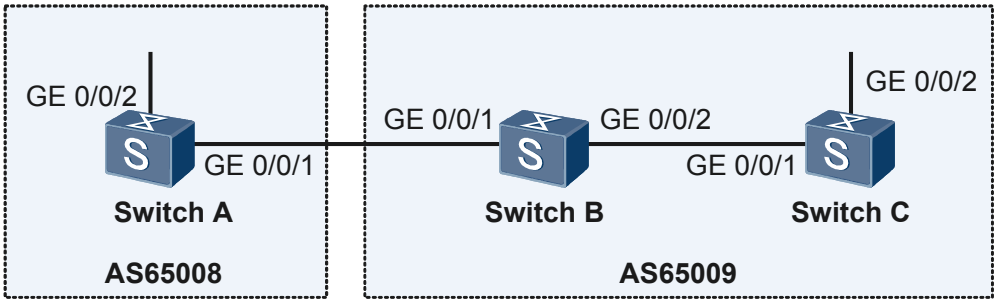
```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
bgp 65009
 router-id 4.4.4.4
 peer 9.1.1.1 as-number 65009
 peer 9.1.2.1 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  peer 9.1.1.1 enable
  peer 9.1.2.1 enable
#
return
```

配置 BGP 与 IGP 交互示例

组网需求

如图 5-23 所示，在 AS65009 内使用 OSPF 作为 IGP 协议，SwitchA 和 SwitchB 建立 EBGP 连接，SwitchC 仅运行 OSPF 而不运行 BGP。

图 5-23 配置 BGP 与 IGP 交互配置组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	3.1.1.2/24
SwitchA	GE 0/0/2	VLANIF 30	8.1.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	3.1.1.1/24
SwitchB	GE 0/0/2	VLANIF 20	9.1.1.1/24
SwitchC	GE 0/0/1	VLANIF 20	9.1.1.2/24
SwitchC	GE 0/0/2	VLANIF 40	9.1.2.1/24

配置思路

采用如下的思路配置 BGP 与 IGP 交互：

版权所有 © 华为技术有限公司

1. 在 SwitchB 和 SwitchC 上配置 OSPF 协议。
2. 在 SwitchA 和 SwitchB 上配置 EBGP 连接。
3. 在 SwitchB 上配置 BGP 与 OSPF 互相引入，查看路由信息。
4. 在 SwitchB 上配置 BGP 路由聚合，简化 BGP 路由表。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-23 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-23 所示。
- SwitchA 的 Router ID 1.1.1.1，所在 AS 号 65008。
- SwitchB、SwitchC 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 OSPF

   # 配置 SwitchB。

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # 配置 SwitchC。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

4. 配置 EBGP 连接

   # 配置 SwitchA。

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 3.1.1.1 as-number 65009
[SwitchA-bgp]  ipv4-family unicast
[SwitchA-bgp-af-ipv4] network 8.1.1.0 255.255.255.0
[SwitchA-bgp-af-ipv4] quit
[SwitchA-bgp] quit
```

   # 配置 SwitchB。

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 3.1.1.2 as-number 65008
```

5. 配置 BGP 与 IGP 交互

   # 在 SwitchB 上配置 BGP 引入 OSPF 路由。

```
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] import-route ospf 1
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # 查看 SwitchA 的路由表。

```
[SwitchA] display bgp routing-table
```


版权所有 © 华为技术有限公司

```
 Total Number of Routes: 3

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>   8.1.1.0/24         0.0.0.0         0                      0      i
 *>   9.1.1.0/24         3.1.1.1         0                      0      65009?
 *>   9.1.2.0/24         3.1.1.1         2                      0      65009?
```

在 SwitchB 上配置 OSPF 引入 BGP 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

查看 SwitchC 的路由表。

```
[SwitchC] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        8.1.1.0/24  O_ASE   150  1           D   9.1.1.1         Vlanif20
        9.1.1.0/24  Direct  0    0           D   9.1.1.2         Vlanif20
        9.1.1.2/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        9.1.2.0/24  Direct  0    0           D   9.1.2.1         Vlanif40
        9.1.2.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

6. 配置路由自动聚合

配置 SwitchB。

```
[SwitchB] bgp 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] summary automatic
[SwitchB-bgp-af-ipv4]  quit
[SwitchB-bgp] quit
```

查看 SwitchA 的 BGP 路由表。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.1.1.0/24         0.0.0.0         0                      0      i
 *>   9.0.0.0            3.1.1.1                                0      65009?
```

使用 Ping 进行验证。

```
[SwitchA] ping -a 8.1.1.1 9.1.2.1
  PING 9.1.2.1: 56  data bytes, press CTRL_C to break
    Reply from 9.1.2.1: bytes=56 Sequence=1 ttl=254 time=15 ms
    Reply from 9.1.2.1: bytes=56 Sequence=2 ttl=254 time=31 ms
    Reply from 9.1.2.1: bytes=56 Sequence=3 ttl=254 time=47 ms
    Reply from 9.1.2.1: bytes=56 Sequence=4 ttl=254 time=46 ms
    Reply from 9.1.2.1: bytes=56 Sequence=5 ttl=254 time=47 ms
  --- 9.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```


版权所有 © 华为技术有限公司

```
  round-trip min/avg/max = 15/37/47 ms
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 3.1.1.2 255.255.255.0
#
interface Vlanif30
 ip address 8.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65008
 router-id 1.1.1.1
 peer 3.1.1.1 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  network 8.1.1.0 255.255.255.0
  peer 3.1.1.1 enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 3.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 9.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bgp 65009
 router-id 2.2.2.2
 peer 3.1.1.2 as-number 65008
 #
 ipv4-family unicast
  undo synchronization
  summary automatic
  import-route ospf 1
  peer 3.1.1.2 enable
#
ospf 1
 import-route bgp
 area 0.0.0.0
```


版权所有 © 华为技术有限公司

```
  network 9.1.1.0 0.0.0.255
return
```

- SwitchC 的配置文件

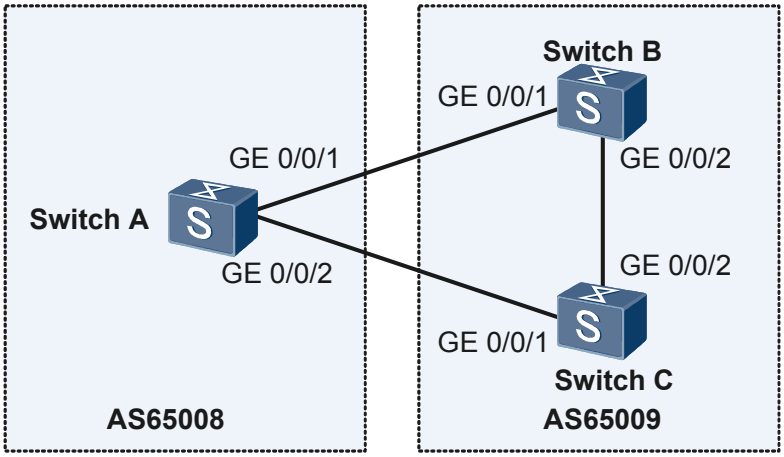
```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 9.1.1.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.0
  network 9.1.1.0 0.0.0.255
  network 9.1.2.0 0.0.0.255
#
return
```

配置 BGP 负载分担和 MED 属性示例

组网需求

如图 5-24 所示，图中所有 Switch 配置 BGP，SwitchA 在 AS65008 中，SwitchB 和 SwitchC 在 AS65009 中。SwitchA 与 SwitchB、SwitchC 之间运行 EBGP，SwitchB 和 SwitchC 之间运行 IBGP。

图 5-24 配置 BGP 路径选择的组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	200.1.1.2/24
SwitchA	GE 0/0/2	VLANIF 20	200.1.2.2/24

版权所有 © 华为技术有限公司

SwitchB	GE 0/0/1	VLANIF 10	200.1.1.1/24
SwitchB	GE 0/0/2	VLANIF 30	9.1.1.1/24
SwitchC	GE 0/0/1	VLANIF 20	200.1.2.1/24
SwitchC	GE 0/0/2	VLANIF 30	9.1.1.2/24

配置思路

采用如下的思路配置 BGP 负载分担和 MED 属性：

1. 在 SwitchA 和 SwitchB、SwitchA 和 SwitchC 之间配置 EBGP 连接；在 SwitchB 和 SwitchC 之间配置 IBGP 连接。
2. 在 SwitchA 上配置负载分担功能及 MED 值，查看路由信息。

数据准备

为完成此配置例，需准备如下的数据：

- 各接口所属的 VLAN ID，具体数据如图 5-24 所示。
- 各 VLANIF 接口的 IP 地址，具体数据如图 5-24 所示。
- SwitchA 的 Router ID 为 1.1.1.1，所在 AS 号 65008，负载分担条数 2。
- SwitchB、SwitchC 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009，SwitchB 的缺省 MED 值 100。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 BGP 连接

   # 配置 SwitchA。

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
[SwitchA-bgp] peer 200.1.2.1 as-number 65009
[SwitchA-bgp] quit
```

   # 配置 SwitchB。

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # 配置 SwitchC。

```
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 200.1.2.2 as-number 65008
[SwitchC-bgp] peer 9.1.1.1 as-number 65009
[SwitchC-bgp] ipv4-family unicast
[SwitchC-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
```


版权所有 © 华为技术有限公司

```
[SwitchC-bgp-af-ipv4] quit
[SwitchC-bgp] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24        200.1.1.1       0                     0       65009i
 *                        200.1.2.1       0                     0       65009i
```

从路由表中可以看出，到目的地址 9.1.1.0/24 有两条有效路由，其中下一跳为 200.1.1.1 的路由是最优路由（因为 SwitchB 的 Router ID 要小一些）。

4. 配置负载分担

配置 SwitchA。

```
[SwitchA] bgp 65008
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-af-ipv4] maximum load-balancing 2
[SwitchA-bgp-af-ipv4] quit
[SwitchA-bgp] quit
```

查看 SwitchA 的路由表。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.1.1       0                     0       65009i
 *>                        200.1.2.1       0                     0       65009i
```

从路由表中可以看到，BGP 路由 9.1.1.0/24 存在两个下一跳，分别是 200.1.1.1 和 200.1.2.1，且都是最优路由。

5. 配置 MED 属性

通过策略配置 SwitchB 发送给 SwitchA 的 MED 值。

```
[SwitchB] route-policy 10 permit node 10
[SwitchB-route-policy] apply cost 100
[SwitchB-route-policy] quit
[SwitchB] bgp 65009
[SwitchB-bgp] peer 200.1.1.2 route-policy 10 export
```

查看 SwitchA 的路由表。

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.2.1       0                     0       65009i
 *                        200.1.1.1       100                   0       65009i
```


版权所有 © 华为技术有限公司

从路由表中可以看出，由于下一跳为 200.1.1.1（SwitchB）的路由 MED 值为 100，而下一跳为 200.1.2.1 的 MED 值为 0，所以 BGP 优先选择 MED 值较小的路由。

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 200.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bgp 65008
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
 peer 200.1.2.1 as-number 65009
 #
 ipv4-famlily unicast
  undo synchronization
  maximum load-balancing 2
  peer 200.1.1.1 enable
  peer 200.1.2.1 enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 200.1.1.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
 router-id 2.2.2.2
 peer 200.1.1.2 as-number 65008
 peer 9.1.1.2 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  network 9.1.1.0 255.255.255.0
  peer 200.1.1.2 enable
  peer 200.1.1.2 route-policy 10 export
```


版权所有 © 华为技术有限公司

```
  peer 9.1.1.2 enable
#
route-policy 10 permit node 10
 apply cost 100
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20 30
#
interface Vlanif10
 ip address 200.1.2.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
 router-id 3.3.3.3
 peer 9.1.1.1 as-number 65009
 peer 200.1.2.2 as-number 65008
 #
 ipv4-family unicast
  undo synchronization
  network 9.1.1.0 255.255.255.0
  peer 9.1.1.1 enable
  peer 200.1.2.2 enable
#
return
```

5.8 路由策略配置

路由策略是为了改变网络流量所经过的途径而对路由信息采用的方法。

5.8.1 路由策略概述

使用路由策略可以严格控制网络中路由的发送和接收。

路由策略

路由策略（Routing Policy）是为了改变网络流量所经过的途径而对路由信息采用的方法。主要通过应用路由属性（包括可达性）来实现。

交换机在发布和接收路由时应用的策略，目的是通过应用路由属性而过滤路由。目前实施路由策略的手段主要是对路由信息进行过滤。例如：

- 只接收或发布一部分满足条件的路由信息。
- 一种路由协议（如 RIP）可能需要引入其它路由协议发现的路由信息，从而丰富自己的路由知识；交换机在引入其它路由协议的路由信息时，可能需要只引入一部分满足条件的路由信息，并对所引入的路由信息的某些属性进行设置，以使其满足本协议的要求。

版权所有 © 华为技术有限公司

为实现路由策略，首先定义将要实施路由策略的路由特征，即定义一组匹配规则和设置规则，然后将它们应用于路由的发布、接收和引入等过程的路由策略中。

路由策略与策略路由的区别

策略路由 PBR（Policy Based Routing）与单纯依照 IP 报文的目的地址查找 FIB 表进行转发不同，是一种依据用户制定的策略而进行路由选择的机制。PBR 支持基于到达报文的源地址和报文长度信息，依据用户制定的策略进行路由选择，可应用于安全、负载分担等目的。

路由策略与策略路由是两种不同的机制，主要区别如表 5-1。

表 5-1 路由策略与策略路由的区别

路由策略	策略路由
基于目的地址按路由表转发	基于策略的转发，失败后再查找路由表转发
基于控制平面，为路由协议和路由表服务	基于转发平面，为转发策略服务
与路由协议结合完成策略	需要手工逐跳配置，以保证报文按策略转发

5.8.2 AC6605 支持的路由策略特性

配置路由策略时，可选择使用的过滤器：访问控制列表、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy。

过滤器

在 AC6605 中，提供了访问控制列表、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy 七种过滤器供路由协议引用。下面对各种过滤器逐个进行介绍。

- 访问控制列表 ACL

  访问控制列表包括针对 IPv4 报文的 ACL（Access Control List），和针对 IPv6 报文的 ACL。按照 ACL 用途，ACL 可以分为 3 种类型：基于接口的 ACL（Interface-based ACL）、基本 ACL（Basic ACL）和高级 ACL（Advanced ACL）。用户在定义 ACL 时可以指定 IP 地址和子网范围用于匹配路由信息的目的网段地址或下一跳地址。

  ACL 的有关配置请参见《AC6605 无线接入控制器 配置指南-IP 业务》中的描述。

- 地址前缀列表（IP-Prefix List）

  地址前缀列表包括 IPv4 地址前缀列表和 IPv6 地址前缀列表，作用比较灵活。

  一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个索引号来标识，索引号指明了进行匹配检查的顺序。

  在匹配的过程中，交换机按升序依次检查由 index-number 标识的各个表项。只要有某一表项满足条件，就意味着本次匹配过程结束，而不再进行下一个表项的匹配。具体配置请参见配置地址前缀列表。

版权所有 © 华为技术有限公司

- AS 路径过滤器（AS-Path-Filter）

  BGP 的路由信息中，包含一个自治系统路径域。AS-Path-Filter 就是针对自治系统路径域指定匹配条件。

  AS 路径过滤器的配置请参见 **BGP 配置**。

- 团体属性过滤器（Community-filter）

  团体属性过滤器仅用于 BGP。BGP 的路由信息中，包含一个团体属性域，用来标识一个团体。团体属性过滤器就是针对团体属性域指定匹配条件。

  团体属性过滤器的配置请参见 **BGP 配置**。

- 扩展团体属性过滤器（Extcommunity-Filter）

  扩展团体属性过滤器仅用于 BGP。BGP 的扩展团体只支持 VPN 的 RT（Route-Target）扩展团体。扩展团体属性过滤器就是针对这种扩展团体属性指定匹配条件。

  扩展团体属性过滤器的配置请参见 **BGP 配置**。

- Route-Policy

  Route-Policy 是一种比较复杂的过滤器，它不仅可以匹配给定路由信息的某些属性，还可以在条件满足时改变路由信息的属性。Route-Policy 可以使用前面几种过滤器定义自己的匹配规则。

  一个 Route-Policy 可以由多个节点（node）构成，不同节点之间是“或”的关系。系统按节点序号依次检查各个节点，如果通过了其中一节点，就意味着通过该策略，不再对其他节点进行匹配。

  每个节点可以由一组 **if-match** 和 **apply** 子句组成。**if-match** 子句定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **if-match** 子句是“与”的关系，只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配。**apply** 子句指定动作，也就是在通过节点的匹配后，对路由信息的一些属性进行设置。具体配置请参见**配置 Route-Policy**。

路由策略的应用

路由策略主要有两种应用方式：

- 路由协议在引入其它路由协议发现的路由时，通过应用路由过滤器只引入满足条件的路由信息。
- 路由协议在发布或接收本路由协议发现的路由时，通过应用路由过滤器对信息进行过滤，只接收或发布满足给定条件的路由信息。

各协议路由策略应用的具体配置请参考相关的路由协议配置。

说明

路由策略发生变化后，缺省情况下，RM 将立即通知协议应用新策略。

5.8.3 配置地址前缀列表

地址前缀列表在应用时，其匹配对象为路由的目的地址。

建立配置任务

在配置地址前缀列表前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

在应用路由策略之前，必须先设置好匹配规则，即过滤器。地址前缀列表的作用类似ACL，比较灵活。地址前缀列表在应用于路由信息的过滤时，其匹配对象为路由信息的目的地址域。

前置任务

无

数据准备

在配置地址前缀列表之前，需要准备以下数据。

序号	数据
1	地址前缀列表名称
2	匹配的地址范围

配置 IPv4 地址前缀列表

地址前缀列表匹配的对象是 IP 地址前缀，由 IP 地址和掩码长度共同定义。

背景信息

请在需要应用地址前缀列表的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]，配置 IPv4 地址前缀列表。

掩码长度范围可以表示为 *mask-length* <= *greater-equal-value* <= *less-equal-value* <= 32。如果只指定了 **greater-equal**，前缀范围为[*greater-equal-value*，32]；如果只指定了 **less-equal**，前缀范围为[*mask-length*，*less-equal-value*]。

IPv4 地址前缀列表由列表名标识，每个前缀列表可以包含多个表项。各表项可以独立指定一个网络前缀形式的匹配范围，并使用索引号标识。比如下面这个名称为 abcd 的 IPv4 地址前缀列表：

```
#
ip ip-prefix abcd index 10 permit 1.0.0.0 8
ip ip-prefix abcd index 20 permit 2.0.0.0 8
```

在匹配过程中，系统按索引号升序依次检查各个表项，只要有一个表项满足条件，就认为通过该过滤列表，不再去匹配其他表项。

AC6605 默认所有未匹配的路由将被拒绝通过过滤列表。如果所有表项都配置成 **deny** 模式，则任何路由都不能通过该过滤列表。因此，需要在多条 **deny** 模式的表项后定义一条 **permit 0.0.0.0 0 less-equal 32** 表项，允许其它所有 IPv4 路由信息通过。

版权所有 © 华为技术有限公司

说明

如果定义了一个以上的前缀列表表项，则至少应该有一个表项的匹配模式为 **permit** 模式。

----结束

检查配置结果

地址前缀列表配置成功后，可以查看地址前缀列表的相关信息。

前提条件

已经完成地址前缀列表的所有配置。

操作步骤

- 使用 **display ip ip-prefix** [*ip-prefix-name*]命令查看 IPv4 地址前缀列表信息。

----结束

任务示例

执行命令 **display ip ip-prefix p1** 命令，可以看到名称为 p1 的地址前缀列表的相关信息。

```
<Quidway> display ip ip-prefix p1
Prefix-list p1
Permitted 5
Denied 2
index: 10      permit  192.168.0.0/16          ge  17  le  18
```

5.8.4 配置 Route-Policy

Route-Policy 的每个节点可以由一组 if-match 子句和 apply 子句组成。

建立配置任务

在配置 Route-Policy 前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

Route-Policy 用来匹配给定的路由信息或者路由信息的某些属性，并在条件满足时改变这些路由信息的属性。

一个 Route-Policy 可由多个节点构成，每个节点又分为：

- **If-match** 子句：定义匹配规则，即路由信息通过当前 Route-Policy 所需满足的条件，匹配对象是路由信息的某些属性。
- **Apply** 子句：指定动作，即执行的一些配置命令，对路由的一些属性进行修改。

Route-Policy 的特性描述请参见《AC6605 无线接入控制器 特性描述-IP 路由》中的描述。

前置任务

在配置 Route-Policy 之前，需完成以下任务：

版权所有 © 华为技术有限公司

- 配置地址前缀列表
- 配置路由协议

数据准备

在配置 Route-Policy 之前，需要准备以下数据。

序号	数据
1	Route-Policy 的名称、节点序号
2	匹配条件
3	要修改的路由属性值

创建 Route-Policy

通过应用 Route-Policy，可根据组网需求来设置引入路由的相关属性。

背景信息

请在需要应用 Route-Policy 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node*，创建 Route-Policy 的节点，并进入 Route-Policy 视图。

- **permit** 指定节点的匹配模式为允许。当路由项通过该节点的过滤后，将执行该节点的 **apply** 子句，不进入下一个节点的测试；如果路由项没有通过该节点过滤，将进入下一个节点继续测试。
- **deny** 指定节点的匹配模式为拒绝，这时 **apply** 子句不会被执行。当路由项满足该节点的所有 **if-match** 子句时，将被拒绝通过该节点，不进入下一个节点；如果路由项不满足该节点的任何 **if-match** 子句，将进入下一个节点继续测试。

说明

AC6605 默认所有未匹配的路由将被拒绝通过 Route-Policy。如果 Route-Policy 中定义了一个以上的节点，则各节点中至少应该有一个节点的匹配模式是 **permit**。

当 Route-Policy 用于路由信息过滤时，如果某路由信息没有通过任一节点，则认为该路由信息没有通过该 Route-Policy。如果 Route-Policy 的所有节点都是 **deny** 模式，则没有路由信息能通过该 Route-Policy。

当引用 Route-Policy 进行路由信息过滤时，*node* 的值小的节点先进行测试。

----结束

（可选）配置 If-match 子句

If-match 子句用来定义 Route-Policy 匹配条件，匹配对象是路由信息的一些属性。

版权所有 © 华为技术有限公司

背景信息

请在需要应用 Route-Policy 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node*，进入 Route-Policy 视图。

步骤 3 选择执行下列命令，配置 Route-Policy 中的 If-match 子句。

- 匹配 ACL：**if-match acl** { *acl-number* | *acl-name* }
- 匹配路由信息的路由权值：**if-match cost** *cost*
- 匹配路由信息的出接口：**if-match interface** *interface-type interface-number*
- 匹配 IPv4 的路由信息（下一跳或源地址）：**if-match ip** { **next-hop** | **route-source** } { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }
- 匹配地址前缀列表：**if-match ip-prefix** *ip-prefix-name*

  说明

  对于同一个 Route-Policy 节点，命令 **if-match acl** 和命令 **if-match ip-prefix** 不能同时配置，后配置的命令会覆盖先配置的命令。
- 匹配路由信息的类型
  - 匹配 OSPF 各类型路由信息：**if-match route-type** { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }
  - 匹配 IS-IS 各 level 路由信息：**if-match route-type** { **is-is-level-1** | **is-is-level-2** }
- 匹配路由信息的标记域：**if-match tag** *tag*

步骤 3 中各命令之间无顺序关系。在一个节点中，可以没有 **if-match** 子句，也可以有多个 **if-match** 子句。

说明

- 对于同一个 Route-Policy 节点，在匹配的过程中，各个 **if-match** 子句间是“与”的关系，即路由信息必须同时满足所有匹配条件，才可以执行 **apply** 子句的动作。但命令 **if-match route-type** 和 **if-match interface** 除外，这两个命令的各自 **if-match** 子句间是“或”的关系，与其它命令的 **if-match** 子句间仍是“与”的关系。
- 如不指定 **if-match** 子句，则所有路由信息都会通过该节点的过滤。

----结束

（可选）配置 Apply 子句

Apply 子句用来为 Route-Policy 指定动作，来对路由信息的属性进行设置。

背景信息

请在需要应用 Route-Policy 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node*，进入 Route-Policy 视图。

步骤 3 选择执行下列命令，配置 Route-Policy 中的 apply 子句。

- 设置路由信息的开销值：**apply cost** [+ | -] *cost*
- 设置路由信息的开销类型
  - 设置 IS-IS 的开销类型：**apply cost-type** { **external** | **internal** }
  - 设置 OSPF 的开销类型：**apply cost-type** { **type-1** | **type-2** }
- 设置 IPv4 路由信息的下一跳地址：**apply ip-address next-hop** { **peer-address** | *ipv4-address* }
- 设置路由协议的优先级：**apply preference** *preference*
- 设置路由信息的标记域：**apply tag** *tag*

步骤 3 各命令之间没有顺序关系。

----结束

检查配置结果

Route-Policy 配置成功后，可以查看 Route-Policy 的相关信息。

前提条件

已经完成 Route-Policy 的所有配置。

操作步骤

- 使用 **display route-policy** [*route-policy-name*]命令查看 Route-Policy。

----结束

5.8.5 对接收的路由应用路由过滤器

在路由协议中应用路由策略相关的过滤器，过滤接收的路由。

建立配置任务

在对接收的路由应用路由过滤器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在定义了路由策略相关的过滤器（地址前缀列表、ACL、Route-Policy 等）后，需要在协议中引入这些过滤器。

- 对接收的路由进行过滤

  应用各协议中的 **filter-policy** 命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

  过滤接收路由的命令是 **filter-policy import**。

  对于距离矢量协议和链路状态协议，**filter-policy** 命令的操作过程是不同的：

版权所有 © 华为技术有限公司

- 距离矢量协议

  距离矢量协议是基于路由表生成路由的。因此过滤器会影响从邻居接收的路由和向邻居发布的路由。

- 链路状态协议

  链路状态路由协议是基于链路状态数据库来生成路由的，**filter-policy** 不影响链路状态通告或链路状态数据库的完整性，因此在接收和发布时的影响是不同的。

  在接收路由时，**filter-policy** 只能决定哪些路由从协议路由表安装到本地核心路由表，即只影响本地核心路由表，不影响协议路由表；

说明

- BGP 具有强大的过滤功能，BGP 相关的策略配置请参见 **BGP 配置**。
- 在路由协议 RIP、OSPF、IS-IS、BGP 中，都有相应的 **filter-policy** 和 **import-route** 命令及其应用，请参见各章节中相关配置。

前置任务

在应用路由策略相关过滤器之前，需完成以下任务：

- **配置地址前缀列表**
- 配置 ACL 列表
- **配置 Route-Policy**

数据准备

在应用路由策略相关过滤器之前，需要准备以下数据。

序号	数据
1	地址前缀列表名称
2	ACL 列表名称
3	Route-policy 的名称和 node 号

对 RIP 接收的路由进行过滤

应用过滤器可以控制 RIP 路由的接收。

背景信息

请在配置 RIP 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，启动 RIP 进程，进入 RIP 视图。

步骤 3 执行命令（根据实际情况选择其中之一）：

版权所有 © 华为技术有限公司

- **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import** [*interface-type interface-number*]
- **filter-policy gateway** *ip-prefix-name* **import**
- **filter-policy ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] **import** [*interface-type interface-number*]

配置对接收的路由进行过滤。

----结束

对 OSPF 接收的路由进行过滤

应用过滤器可以控制 OSPF 路由的接收。

背景信息

请在配置 OSPF 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，启动 OSPF 进程，进入 OSPF 视图。

步骤 3 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**，配置对接收的路由进行过滤。

----结束

对 IS-IS 接收的路由进行过滤

应用过滤器可以控制 IS-IS 路由的接收。

背景信息

请在配置 IS-IS 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，启动 IS-IS 进程，进入 IS-S 视图。

步骤 3 执行命令 **filter-policy** { **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**，配置对接收的路由进行过滤。

----结束

对 BGP 接收的路由进行过滤

应用过滤器可以控制 BGP 路由的接收。

版权所有 © 华为技术有限公司

操作步骤

- 过滤从全局接收的路由

  请在配置 BGP 的交换机上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**，配置对接收的路由进行过滤。

- 过滤从对等体接收的路由

  请在配置 BGP 的交换机上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *group-name* | *ipv4-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**，配置从对等体接收的路由进行过滤。

----结束

检查配置结果

对接收的路由应用路由过滤器配置成功后，可以查看各协议路由表的相关信息。

前提条件

已经完成对接收的路由应用路由过滤器的所有配置。

操作步骤

- 使用 **display rip** *process-id* **route** 命令查看 RIP 协议路由表信息。
- 使用 **display ospf** [*process-id*] **routing** 命令查看 OSPF 协议路由表信息。
- 使用 **display isis** [*process-id*] **route** 命令查看 ISIS 协议路由表信息。
- 使用 **display bgp routing-table** 命令查看 BGP 协议路由表信息。
- 使用 **display ip routing-table** 命令查看公网 IPv4 路由表信息。

  在邻居交换机上执行命令 **display ip routing-table**，可以看到匹配邻居过滤条件的路由已经被过滤掉或已经执行了 **apply** 动作。

----结束

5.8.6 对发布的路由应用路由过滤器

在路由协议中应用路由策略相关的过滤器，过滤发布的路由。

建立配置任务

在对发布的路由应用路由过滤器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

在定义了路由策略相关的过滤器（地址前缀列表、ACL、Route-Policy 等）后，需要在协议中引入这些过滤器。

- 对发布的路由进行过滤

  应用各协议中的 **filter-policy** 命令引用 ACL 和地址前缀列表，对发布的路由进行过滤，仅发布满足条件的部分路由。

  过滤发布路由的命令是 **filter-policy export**。

  对于距离矢量协议和链路状态协议，**filter-policy** 命令的操作过程是不同的：

  - 距离矢量协议

    距离矢量协议是基于路由表生成路由的。因此过滤器会影响从邻居接收的路由和向邻居发布的路由。

  - 链路状态协议

    链路状态路由协议是基于链路状态数据库来生成路由的，**filter-policy** 不影响链路状态通告或链路状态数据库的完整性，因此在接收与发布时的影响是不同的。

    在发布路由时，**filter-policy export** 可以用来控制是否发布协议引入路由（如引入的 RIP 路由）。如果不通过 **import** 命令引入则不会将 LSA/LSP 加入到 LSDB 中，但不影响向其他交换机发布的链路状态通告。

说明

- BGP 具有强大的过滤功能，BGP 相关的策略配置请参见 **BGP 配置**。
- 在路由协议 RIP、OSPF、IS-IS、BGP 中，都有相应的 **filter-policy** 和 **import-route** 命令及其应用，请参见各章节中相关配置。

前置任务

在应用路由策略相关过滤器之前，需完成以下任务：

- **配置地址前缀列表**
- 配置 ACL 列表
- **配置 Route-Policy**

数据准备

在应用路由策略相关过滤器之前，需要准备以下数据。

序号	数据
1	地址前缀列表名称
2	ACL 列表名称
3	Route-policy 的名称和 node 号

对 RIP 发布的路由进行过滤

应用过滤器可以控制 RIP 路由的发布。

版权所有 © 华为技术有限公司

背景信息

请在配置 RIP 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，启动 RIP 进程，进入 RIP 视图。

步骤 3 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]，配置对发布的路由进行过滤。

----结束

对 OSPF 发布的路由进行过滤

应用过滤器可以控制 OSPF 路由的发布。

背景信息

请在配置 OSPF 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，启动 OSPF 进程，进入 OSPF 视图。

步骤 3 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]，配置对发布的路由进行过滤。

----结束

对 IS-IS 发布的路由进行过滤

应用过滤器可以控制 IS-IS 路由的发布。

背景信息

请在配置 IS-IS 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，启动 IS-IS 进程，进入 IS-S 视图。

步骤 3 执行命令 **filter-policy** { **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]，配置对发布的路由进行过滤。

----结束

对 BGP 发布的路由进行过滤

应用过滤器可以控制 BGP 路由的发布。

版权所有 © 华为技术有限公司

操作步骤

- 过滤全局的路由

  请在配置 BGP 的交换机上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]，对发布的路由信息进行过滤。

     对于 BGP 引入的路由，只有符合条件的路由信息才能进入 BGP 本地路由表，发布给 BGP 对等体。

     - 指定 *protocol* 参数可以只对特定路由协议的信息进行过滤；
     - 如果没有指定此参数，则对所有要发布的 BGP 路由信息进行过滤，包括引入的路由和使用 **network** 命令发布的本地路由。

     说明

     不同协议的 **filter-policy export** 命令对待发布路由的影响范围不同：

     - 对于链路状态协议，只对引入的路由信息进行过滤。
     - 对于距离矢量协议，会对引入的路由信息、本协议发现的路由信息进行过滤。

- 过滤向对等体发布的路由

  请在配置 BGP 的交换机上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **peer** { *group-name* | *ipv4-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* } **export**，配置向对等体发布的路由进行过滤。

----结束

检查配置结果

对发布的路由应用路由过滤器配置成功后，可以查看各协议路由表的相关信息。

前提条件

已经完成对发布的路由应用路由过滤器的所有配置。

操作步骤

- 使用 **display rip** *process-id* **route** 命令查看 RIP 协议路由表信息。
- 使用 **display ospf** [*process-id*] **routing** 命令查看 OSPF 协议路由表信息。
- 使用 **display isis** [*process-id*] **route** 命令查看 ISIS 协议路由表信息。
- 使用 **display bgp routing-table** 命令查看 BGP 协议路由表信息。
- 使用 **display ip routing-table** 命令查看公网 IPv4 路由表信息。

版权所有 © 华为技术有限公司

在邻居交换机上执行命令 **display ip routing-table**，可以看到匹配邻居过滤条件的路由已经被过滤掉或已经执行了 **apply** 动作。

----结束

5.8.7 对引入的路由应用路由过滤器

在路由协议中应用路由策略相关的过滤器，过滤引入的路由。

建立配置任务

在对引入的路由应用路由过滤器前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在定义了路由策略相关的过滤器（地址前缀列表、ACL、Route-Policy 等）后，需要在协议中引入这些过滤器。

- 引入外部路由时应用策略
  - 应用各协议中的 **import-route** 命令，在各个协议中引入所需的外部路由，同时可以使用 Route-Policy 过滤器对引入的路由进行严格控制。
  - 通常在引入外部路由后，可以应用 **filter-policy export** 命令对引入的路由信息在向外发布时，进行过滤。

说明

- BGP 具有强大的过滤功能，BGP 相关的策略配置请参见 **BGP 配置**。
- 在路由协议 RIP、OSPF、IS-IS、BGP 中，都有相应的 **filter-policy** 和 **import-route** 命令及其应用，请参见各章节中相关配置。

前置任务

在应用路由策略相关过滤器之前，需完成以下任务：

- **配置地址前缀列表**
- 配置 ACL 列表
- **配置 Route-Policy**

数据准备

在应用路由策略相关过滤器之前，需要准备以下数据。

序号	数据
1	地址前缀列表名称
2	ACL 列表名称
3	Route-policy 的名称和 node 号

版权所有 © 华为技术有限公司

对 RIP 引入外部路由时应用策略

通过应用过滤器，RIP 可以选择引入外部路由。

背景信息

请在配置 RIP 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*]，使能 RIP 路由进程，进入 RIP 视图。

步骤 3 执行命令 **import-route bgp** [**cost** { *cost* | **transparent** } | **route-policy** *route-policy-name*] * 或 **import-route** { { **static** | **direct** } | { { **rip** | **ospf** | **isis** } [*process-id*] } } [**cost** *cost* | **route-policy** *route-policy-name*] *，引入外部路由信息。

----结束

对 OSPF 引入外部路由时应用策略

通过应用过滤器，OSPF 可以选择引入外部路由。

背景信息

请在配置 OSPF 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id*]，使能 OSPF 路由进程，进入 OSPF 视图。

步骤 3 执行命令 **import-route** { **limit** *limit-number* | *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] * }，引入外部路由信息。

----结束

对 IS-IS 引入外部路由时应用策略

通过应用过滤器，IS-IS 可以选择引入外部路由。

背景信息

请在配置 IS-IS 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **isis** [*process-id*]，使能 IS-IS 路由进程，进入 IS-IS 视图。

步骤 3 配置 IS-IS 引入外部路由。

版权所有 © 华为技术有限公司

- 当需要对引入路由的开销进行设置时，执行命令 **import-route** *protocol* [*process-id*] [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 引入外部路由。
- 当需要保留引入路由的原有开销时，执行命令 **import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **bgp** } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 引入外部路由。

----结束

对 BGP 引入外部路由时应用策略

通过应用过滤器，BGP 可以选择引入外部路由。

背景信息

请在配置 BGP 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **import-route** *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *，引入外部路由信息。

----结束

检查配置结果

对引入的路由应用路由过滤器配置成功后，可以查看各协议路由表的相关信息。

前提条件

已经完成对引入的路由应用路由过滤器的所有配置。

操作步骤

- 使用 **display rip** *process-id* **route** 命令查看 RIP 协议路由表信息。
- 使用 **display ospf** [*process-id*] **routing** 命令查看 OSPF 协议路由表信息。
- 使用 **display isis** [*process-id*] **route** 命令查看 ISIS 协议路由表信息。
- 使用 **display bgp routing-table** 命令查看 BGP 协议路由表信息。
- 使用 **display ip routing-table** 命令查看公网 IPv4 路由表信息。

  在邻居交换机上执行命令 **display ip routing-table**，可以看到匹配邻居过滤条件的路由已经被过滤掉或已经执行了 **apply** 动作。

----结束

5.8.8 控制路由策略生效时间

为了保障网络的稳定性，修改路由策略时需要控制路由策略的生效时间。

版权所有 © 华为技术有限公司

建立配置任务

在配置控制路由策略生效时间前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在实际应用中，当多条相互配合的路由策略的配置发生变化时，如果每完成一条配置，RM（Routing Management Module）就立即通知各协议重新应用策略。不完整的策略则会造成路由振荡和中间结果处理时间的浪费，造成网络的不稳定。

AC6605 系统对路由策略的变化处理规则如下：

- 缺省情况下，路由策略变化后，RM 将立即通知协议应用新策略。
- 如果配置了路由策略生效时间，当路由策略的相关命令配置变化后，RM 并不立即通知协议进行处理，而是等待所配置的时长，然后再通知各协议应用变化后的策略。
- 如果在等待时间内路由策略的配置又发生了改变，RM 将重置定时器，重新开始计时。

可以根据实际情况，应用命令选择延迟等待时间的长短。

前置任务

无

数据准备

在配置路由策略生效时间之前，需要准备以下数据。

序号	数据
1	路由策略应用的延迟时间

配置路由策略应用延迟时间

修改多条相互配合的路由策略时，需要控制路由策略的生效时间。

背景信息

请在需要改变路由策略应用延迟时间的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **route-policy-change notify-delay** *delay-time*，设置路由策略应用延迟时间。

延迟时间的取值范围是 1 秒～ 180 秒。

缺省情况下，路由策略变化后，RM 将立即通知协议应用新策略。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **quit**，退回用户视图。

步骤 4 （可选）执行命令 **refresh bgp all** { **export** | **import** }，配置 BGP 协议立即应用新策略。

如果配置策略命令后，需要立即看到策略过滤的效果。可以通过执行这个命令，配置 BGP 协议立即应用新策略。

受该定时器影响的相关的策略有访问控制列表、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy。

----结束

检查配置结果

路由策略生效时间配置成功后，可以查看配置的路由策略生效时间。

前提条件

已经完成控制路由策略生效时间的所有配置。

操作步骤

- 使用 **display current-configuration | include notify-delay** 命令查看路由策略应用延迟时间。

----结束

任务示例

可以看到目前配置的路由策略延迟时间，例如：

```
<Quidway> display current-configuration | include notify-delay
route-policy-change notify-delay 10
```

5.8.9 路由策略维护

路由策略的维护包括清除地址前缀列表统计数据及路由策略的调试。

背景信息

注意

清除地址前缀列表的统计数据后，以前的数据信息将无法恢复，务必仔细确认。

缺省情况下，不清除地址前缀列表的统计数据。

操作步骤

- 在确认需要清除 IPv4 地址前缀列表统计数据，请在用户视图下执行 **reset ip ip-prefix** [*ip-prefix-name*]命令。

----结束

版权所有 © 华为技术有限公司

5.8.10 配置路由策略举例

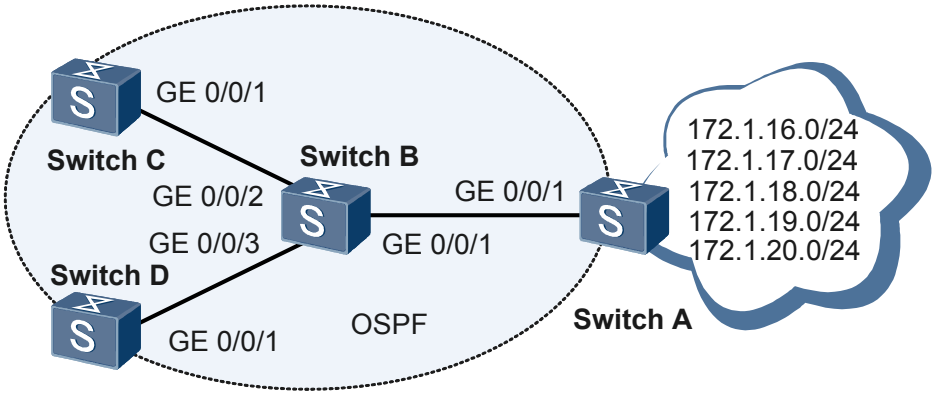
介绍路由策略的各种组网举例。

对接收和发布的路由进行过滤示例

组网需求

如图 5-25，运行 OSPF 协议的网络中，SwitchA 从 Internet 网络接收路由，并为 SwitchB 提供了部分 Internet 路由。要求 SwitchA 仅提供 172.1.17.0/24、172.1.18.0/24、172.1.19.0/24 给 SwitchB，SwitchC 仅接收路由 172.1.18.0/24，SwitchD 接收 SwitchB 提供的全部路由。

图 5-25 配置对接收和发布的路由过滤组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchB	GE 0/0/2	VLANIF 20	192.168.2.1/24
SwitchB	GE 0/0/3	VLANIF 30	192.168.3.1/24
SwitchC	GE 0/0/1	VLANIF 20	192.168.2.2/24
SwitchD	GE 0/0/1	VLANIF 30	192.168.3.2/24

配置思路

采用如下的思路配置对路由进行过滤：

1. 配置各接口所属 VLAN ID。
2. 配置各 VLANIF 接口的 IP 地址。
3. 在 SwitchA、SwitchB、SwitchC 和 SwitchD 上配置 OSPF 基本功能。
4. 在 SwitchA 上配置静态路由，并将这些路由引入 OSPF 路由。
5. 在 SwitchA 上配置路由发布策略，在 SwitchB 上查看过滤结果。

版权所有 © 华为技术有限公司

6. 在 SwitchC 上配置路由接收策略，在 SwitchC 上查看过滤结果。

数据准备

为完成此配置例，需准备如下数据：

- SwitchA 引入的 5 条静态路由。
- SwitchA、SwitchB、SwitchC 和 SwitchD 位于 OSPF 骨干区域（Area0）。
- 地址前缀列表名称，待过滤路由。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）
3. 配置 OSPF 基本功能

   # SwitchA 的配置

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # SwitchB 的配置

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # SwitchC 的配置

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

   # SwitchD 的配置

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

4. 在 SwitchA 上配置 5 条静态路由，并在将这些静态路由引入到 OSPF 协议中。

```
[SwitchA] ip route-static 172.1.16.0 24 NULL 0
[SwitchA] ip route-static 172.1.17.0 24 NULL 0
[SwitchA] ip route-static 172.1.18.0 24 NULL 0
[SwitchA] ip route-static 172.1.19.0 24 NULL 0
[SwitchA] ip route-static 172.1.20.0 24 NULL 0
[SwitchA] ospf
[SwitchA-ospf-1] import-route static
[SwitchA-ospf-1] quit
```

   # 在 SwitchB 上查看 IP 路由表，可以看到 OSPF 引入的 5 条静态路由。

```
[SwitchB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13
```


版权所有 © 华为技术有限公司

```
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8    Direct 0    0           D  127.0.0.1       InLoopBack0
        127.0.0.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.1.0/24   Direct 0    0           D  192.168.1.2     Vlanif10
      192.168.1.2/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.2.0/24   Direct 0    0           D  192.168.2.1     Vlanif30
      192.168.2.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.3.0/24   Direct 0    0           D  192.168.3.1     Vlanif20
      192.168.3.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
       172.1.16.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.17.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.18.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.19.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.20.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
```

5. 配置路由发布策略。

   # 在 SwitchA 上配置地址前缀列表 a2b。

```
[SwitchA] ip ip-prefix a2b index 10 permit 172.1.17.0 24
[SwitchA] ip ip-prefix a2b index 20 permit 172.1.18.0 24
[SwitchA] ip ip-prefix a2b index 30 permit 172.1.19.0 24
```

   # 在 SwitchA 上配置发布策略，引用地址前缀列表 a2b 进行过滤。

```
[SwitchA] ospf
[SwitchA-ospf-1] filter-policy ip-prefix a2b export static
```

   # 在 SwitchB 上查看 IP 路由表，可以看到 SwitchB 仅接收到列表 a2b 中定义的 3 条路由。

```
[SwitchB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11       Routes : 11

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8    Direct 0    0           D  127.0.0.1       InLoopBack0
        127.0.0.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.1.0/24   Direct 0    0           D  192.168.1.2     Vlanif10
      192.168.1.2/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.2.0/24   Direct 0    0           D  192.168.2.1     Vlanif30
      192.168.2.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.3.0/24   Direct 0    0           D  192.168.3.1     Vlanif20
      192.168.3.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
       172.1.17.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.18.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
       172.1.19.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
```

6. 配置路由接收策略

   # 在 SwitchC 上配置地址前缀列表 in。

```
[SwitchC] ip ip-prefix in index 10 permit 172.1.18.0 24
```

   # 在 SwitchC 上配置接收策略，引用地址前缀列表 in 进行过滤。

```
[SwitchC] ospf
[SwitchC-ospf-1] filter-policy ip-prefix in import
```

   # 查看 SwitchC 的 IP 路由表，可以看到 SwitchC 的本地核心路由表中，仅接收了列表 in 定义的 1 条路由。

```
[SwitchC] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8    Direct 0    0           D  127.0.0.1       InLoopBack0
```


版权所有 © 华为技术有限公司

```
      127.0.0.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.2.0/24   Direct 0    0           D  192.168.2.2     Vlanif20
    192.168.2.2/32   Direct 0    0           D  127.0.0.1       InLoopBack0
     172.1.18.0/24   O_ASE  150  1           D  192.168.2.1     Vlanif20
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
ospf 1
 filter-policy ip-prefix a2b export static
 import-route static
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
 ip ip-prefix a2b index 10 permit 172.1.17.0 24
 ip ip-prefix a2b index 20 permit 172.1.18.0 24
 ip ip-prefix a2b index 30 permit 172.1.19.0 24
#
 ip route-static 172.1.16.0 255.255.255.0 NULL0
 ip route-static 172.1.17.0 255.255.255.0 NULL0
 ip route-static 172.1.18.0 255.255.255.0 NULL0
 ip route-static 172.1.19.0 255.255.255.0 NULL0
 ip route-static 172.1.20.0 255.255.255.0 NULL0
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20 30
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
  network 192.168.3.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 1
 filter-policy ip-prefix in import
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
 ip ip-prefix in index 10 permit 172.1.18.0 24
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
#
return
```

在路由引入时应用路由策略示例

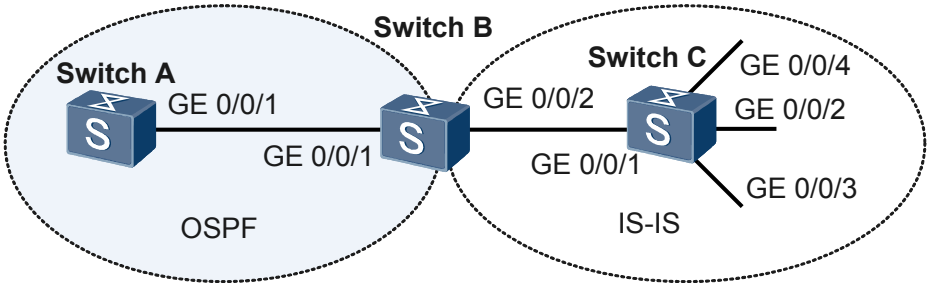
组网需求

如图 5-26 所示，SwitchB 与 SwitchA 之间通过 OSPF 协议交换路由信息，与 SwitchC 之间通过 IS-IS 协议交换路由信息。

要求在 SwitchB 上配置路由引入，将 IS-IS 路由引入到 OSPF 中去，并同时使用路由策略设置路由的属性。其中，设置 172.17.1.0/24 的路由的开销为 100，设置 172.17.2.0/24 的路由的 Tag 属性为 20。

版权所有 © 华为技术有限公司

图 5-26 配置在路由引入时应用路由策略组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	GE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchB	GE 0/0/2	VLANIF 20	192.168.2.2/24
SwitchC	GE 0/0/1	VLANIF 20	192.168.2.1/24
SwitchC	GE 0/0/2	VLANIF 30	172.17.1.1/24
SwitchC	GE 0/0/3	VLANIF 40	172.17.2.1/24
SwitchC	GE 0/0/4	VLANIF 50	172.17.3.1/24

配置思路

采用如下的思路配置在路由引入时应用路由策略：

1. 配置各接口所属 VLAN ID。
2. 配置各 VLANIF 接口的 IP 地址。
3. 在 SwitchB 和 SwitchC 上配置 IS-IS 基本功能。
4. 在 SwitchA 和 SwitchB 上配置 OSPF，引入 IS-IS 路由。
5. 在 SwitchB 上配置路由策略，并在 OSPF 引入 IS-IS 路由时应用路由策略，查看路由信息。

数据准备

为完成此配置例，需准备如下数据：

- SwitchC 的 IS-IS 级别 Level-2，system ID 0000.0000.0001；SwitchB 的 IS-IS 级别 Level-2，system ID 0000.0000.0002；SwitchB、SwitchC 所在的区域号 Area10。
- SwitchA 和 SwitchB 位于 OSPF 骨干区域（Area0）。
- 配置过滤列表及地址前缀列表名称，172.17.1.0/24 路由的开销值 100，172.17.2.0/24 路由的 Tag 属性值 20。

配置步骤

1. 配置各接口所属的 VLAN（略）
2. 配置各 VLANIF 接口的 IP 地址（略）

版权所有 © 华为技术有限公司

3. 配置 IS-IS 路由协议

配置 SwitchC。

```
[SwitchC] isis
[SwitchC-isis-1] is-level level-2
[SwitchC-isis-1] network-entity 10.0000.0000.0001.00
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 20
[SwitchC-Vlanif20] isis enable
[SwitchC-Vlanif20] quit
[SwitchC] interface vlanif 30
[SwitchC-Vlanif30] isis enable
[SwitchC-Vlanif30] quit
[SwitchC] interface vlanif 40
[SwitchC-Vlanif30] isis enable
[SwitchC-Vlanif30] quit
[SwitchC] interface vlanif 50
[SwitchC-Vlanif30] isis enable
[SwitchC-Vlanif30] quit
```

配置 SwitchB。

```
[SwitchB] isis
[SwitchB-isis-1] is-level level-2
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] isis enable
[SwitchB-Vlanif20] quit
```

4. 配置 OSPF 路由协议及路由引入

配置 SwitchA，启动 OSPF。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 SwitchB，启动 OSPF，并引入 IS-IS 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] import-route isis 1
[SwitchB-ospf-1] quit
```

查看 SwitchA 的 OSPF 路由表，可以看到引入的路由。

```
[SwitchA] display ospf routing

         OSPF Process 1 with Router ID 192.168.1.1
                 Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1  Stub       192.168.1.1     192.168.1.1     0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop         AdvRouter
 192.168.2.0/24     1         Type2      1           192.168.1.2     192.168.1.2
 172.17.1.0/24      1         Type2      1           192.168.1.2     192.168.1.2
 172.17.2.0/24      1         Type2      1           192.168.1.2     192.168.1.2
 172.17.3.0/24      1         Type2      1           192.168.1.2     192.168.1.2

 Routing for NSSAs
 Destination        Cost      Type       Tag         NextHop         AdvRouter

 Total Nets: 5
 Intra Area: 1  Inter Area: 0  ASE: 4  NSSA: 0
```


版权所有 © 华为技术有限公司

5. 配置过滤列表

   # 配置编号为 2002 的 ACL，允许 172.17.2.0/24 通过。

```
[SwitchB] acl number 2002
[SwitchB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
[SwitchB-acl-basic-2002] quit
```

   # 配置名为 prefix-a 的地址前缀列表，允许 172.17.1.0/24 通过。

```
[SwitchB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

6. 配置 Route-Policy

```
[SwitchB] route-policy isis2ospf permit node 10
[SwitchB-route-policy] if-match ip-prefix prefix-a
[SwitchB-route-policy] apply cost 100
[SwitchB-route-policy] quit
[SwitchB] route-policy isis2ospf permit node 20
[SwitchB-route-policy] if-match acl 2002
[SwitchB-route-policy] apply tag 20
[SwitchB-route-policy] quit
```

7. 在路由引入时应用 Route-Policy

   # 配置 SwitchB，设置在路由引入时应用 Route-Policy。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route isis 1 route-policy isis2ospf
[SwitchB-ospf-1] quit
```

   # 查看 SwitchA 的 OSPF 路由表，可以看到目的地址为 172.17.1.0/24 的路由的开销为 100，目的地址为 172.17.2.0/24 的路由的标记域（Tag）为 20，而其他路由的属性未发生变化。

```
[SwitchA] display ospf routing

         OSPF Process 1 with Router ID 192.168.1.1
                  Routing Tables
 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1     Stub       192.168.1.1     192.168.1.1     0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop          AdvRouter
 192.168.2.0/24     1          Type2      1           192.168.1.2      192.168.1.2
 172.17.1.0/24      100        Type2      1           192.168.1.2      192.168.1.2
 172.17.2.0/24      1          Type2      20          192.168.1.2      192.168.1.2
 172.17.3.0/24      1          Type2      1           192.168.1.2      192.168.1.2

 Routing for NSSAs
 Destination        Cost      Type       Tag         NextHop         AdvRouter

 Total Nets: 5
 Intra Area: 1  Inter Area: 0  ASE: 4  NSSA: 0
```

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
ospf 1
```


版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
acl number 2002
 rule 5 permit source 172.17.2.0 0.0.0.255
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 1
 import-route isis 1 route-policy isis2ospf
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
route-policy isis2ospf permit node 10
 if-match ip-prefix prefix-a
 apply cost 100
#
route-policy isis2ospf permit node 20
 if-match acl 2002
 apply tag 20
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20 30 40 50
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0001.00
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 172.17.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.17.2.1 255.255.255.0
 isis enable 1
#
```


版权所有 © 华为技术有限公司

```
interface Vlanif50
 ip address 172.17.3.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

5.9 MCE 配置

通常情况下，一台 CE 只能连接一个 VPN，如果用户网络需要划分多个 VPN，则需要多台 CE 设备。MCE 技术可以使一台 CE 同时连接多个 VPN，既可实现不同 VPN 用户间的业务完全隔离，又降低了网络设备的投入成本。

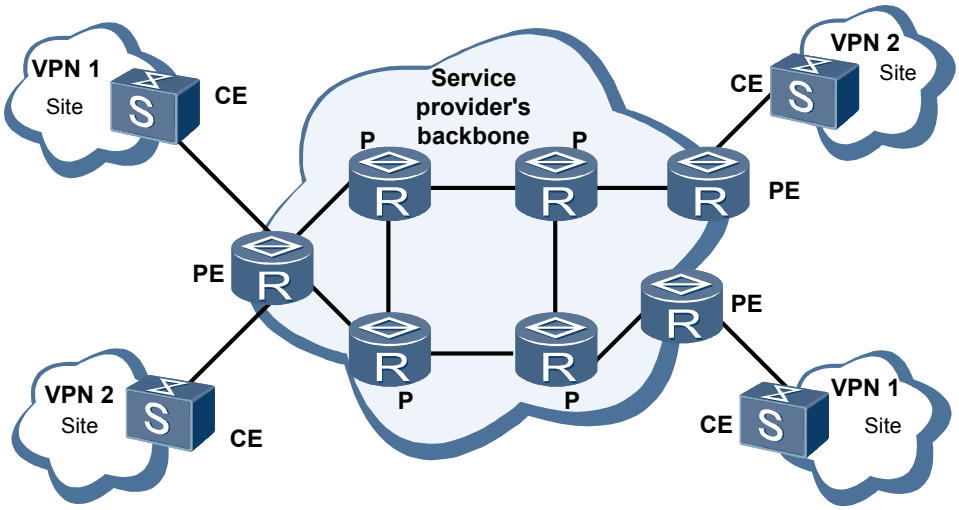
5.9.1 MCE 概述

多 VPN 实例用户边缘设备 MCE（Multi-VPN-Instance CE），通过在 CE 设备上使用路由多实例，实现不同业务或用户的隔离。

产生背景

BGP/MPLS IP VPN 以隧道的方式解决了在公网中传送私网数据的问题。但传统的 BGP/MPLS IP VPN 架构要求每个 VPN 实例单独使用一个 CE 与 PE 相连，如图 5-27 所示。

图 5-27 传统 BGP/MPLS IP VPN 模型

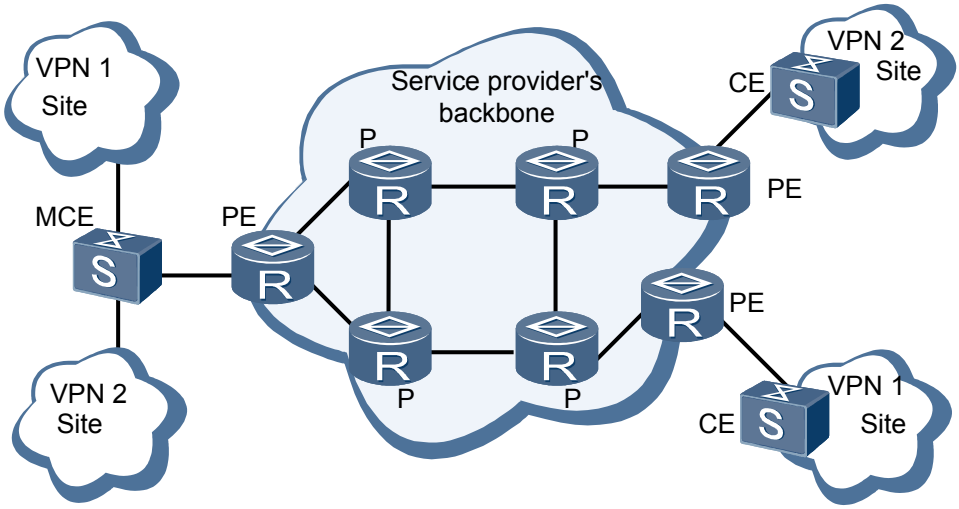


版权所有 © 华为技术有限公司

随着用户业务的不断细化和安全需求的提高，很多情况下一个私有网络内的用户需要划分成多个 VPN，不同 VPN 用户间的业务需要完全隔离。此时，为每个 VPN 单独架设一台 CE 将加大用户的设备开支和维护成本；而多个 VPN 共用一台 CE，使用同一个路由转发表，又无法保证数据的安全性。

如图 5-28 所示，使用 MCE（Multi-VPN-Instance CE）技术，可以有效解决多 VPN 网络带来的用户数据安全与网络成本之间的矛盾。MCE 通过将 VLANIF 接口与 VPN 绑定，并为每个 VPN 创建和维护独立的路由转发表（Multi-VRF），实现不同 VPN 之间的业务完全隔离。

图 5-28 MCE 典型组网图



基本概念

- CE（Customer Edge）

  用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。

- MCE（Multi-VPN-Instance CE）

  配置了 MCE 功能的 CE 设备。在 MCE 设备上允许多个 VPN 同时接入，不同 VPN 之间的业务完全隔离

- PE（Provider Edge）

  服务提供商边缘路由器，是服务提供商网络的边缘设备，与 CE、MCE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。

- P（Provider）

  服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。

- Site

  指相互之间具备 IP 连通性的一组 IP 系统，并且，这组 IP 系统的 IP 连通性不需通过服务提供商网络实现。Site 通过 CE 或 MCE 连接到服务提供商网络。

版权所有 © 华为技术有限公司

5.9.2 AC6605 支持的 MCE 特性

当 AC6605 作为 MCE 设备时，MCE 和 PE 之间、MCE 和 Site 之间可以运行多种路由协议，包括：静态路由、RIP、OSPF、IS-IS、BGP。

5.9.3 配置 VPN 实例

配置 VPN 实例的具体步骤及方法。

建立配置任务

应用环境

如果需要用一台 CE 同时连接多个 VPN，并且要实现这些 VPN 之间的业务完全隔离，则需要配置 MCE 功能。配置 MCE 功能，首先要在 MCE 设备和 PE 设备上配置 VPN 实例。

前置任务

在配置 VPN 实例前，需完成以下任务。

- 在 MCE 设备上创建 VLAN，并将连接 Site 的接口和连接 PE 的接口加入该 VLAN。
- 在 PE 设备上创建 VLAN，并将连接 MCE 的子接口加入该 VLAN。
- 在 Site 内和 MCE 相连的设备上创建 VLAN，并将该设备上和 MCE 相连的接口加入该 VLAN。

数据准备

在配置 VPN 实例前，需准备以下数据：

序号	数据
1	VPN 实例的名称
2	VPN 实例的 RD（Route Distinguisher）
3	（可选）VPN 实例的描述信息
4	（可选）VPN 实例的最大路由数
5	VPN 实例对应的 VLAN 的 ID

创建 VPN 实例

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要进行类似配置，但由于设备厂家、型号不同，配置命令和方法可能不完全相同，具体的配置方法请参见对应产品的手册。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip vpn-instance** *vpn-instance-name*，创建 VPN 实例，并进入 VPN 实例视图。

说明

VPN 实例的名字区分大小写。例如，“vpn1”和“VPN1”将被认为是不同的 VPN 实例。

步骤 3 执行命令 **route-distinguisher** *route-distinguisher*，配置 VPN 实例的 RD。

RD 没有缺省值，必须在创建 VPN 实例时配置。

VPN 实例只有配置了 RD 后才生效。同一设备上的不同 VPN 实例的 RD 不能相同。

在配置 RD 之前，除了描述信息外，不能配置其他任何参数。

RD 一旦配置后，如果要修改，只能将其所属的 VPN 实例删除，重新创建。

步骤 4 （可选）执行命令 **description** *description*，配置 VPN 实例的描述信息。

缺省情况下，VPN 实例没有描述信息。

描述信息的作用类似于主机名和接口描述信息，可用来记录 VPN 实例与某个 VPN 的关系等信息。

步骤 5 （可选）执行命令 **routing-table limit** *number* { *alert-percent* | **simply-alert** }，配置 VPN 实例的最大路由数。

缺省情况下，不限制 VPN 实例的最大路由数。

为防止引入的路由数量过多，可以配置一个 VPN 实例能够支持的最大路由数。

----结束

配置 VPN 实例与 VLANIF 接口绑定

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要将连接 MCE 的接口和 VPN 实例绑定，具体的配置方法请参见对应产品的手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **ip binding vpn-instance** *vpn-instance-name*，配置 VPN 实例与 VLANIF 接口绑定。

缺省情况下，VLANIF 接口不绑定到任何 VPN 实例。

说明

执行 **ip binding vpn-instance** 命令将删除 VLANIF 接口上已经配置的 IP 地址、路由协议等三层特性，如果需要，应重新配置。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

----结束

检查配置结果

完成上述配置后，请在 MCE 上执行 **display ip vpn-instance** [**verbose**] [*vpn-instance-name*]命令检查配置结果。

如果配置正确，执行命令 **display ip vpn-instance**，能够看到 VPN 已被正确创建，VPN 名称、RD、描述信息、最多可以支持的路由数、接口配置正确。

```
<Quidway> display ip vpn-instance verbose
  Total VPN-Instances configured : 1

  VPN-Instance Name and ID : vpn1, 1
  Create date : 2008/09/10 16:58:42
  Up time : 0 days, 21 hours, 42 minutes and 10 seconds
  Log Interval : 5
```

5.9.4 在 MCE 与 Site 间配置路由多实例

介绍 MCE 与 Site 之间，静态路由、RIP、OSPF、IS-IS 和 BGP 的配置方法。

在 MCE 与 Site 间配置路由多实例任务中，**(可选)配置 MCE 与 Site 间使用静态路由**～**(可选)配置 MCE 与 Site 间使用 BGP** 是并列关系，用户根据需要选一配置即可。

建立配置任务

应用环境

如果需要用一台 CE 同时连接多个 VPN，并且要实现这些 VPN 之间的业务完全隔离，则需要配置 MCE 功能。配置 MCE 功能，首先要在 MCE 设备和 PE 设备上 **5.9.3 配置 VPN 实例**，然后需要执行本配置任务，在 MCE 与 Site 间配置路由多实例。

前置任务

在 MCE 与 Site 间配置路由多实例前，需完成以下任务。

- **5.9.3 配置 VPN 实例**

数据准备

在 MCE 与 Site 间配置路由多实例前，需准备以下数据：

序号	数据
1	VPN 实例的名称
2	（可选）去往 Site 的静态的目的地址、目的 VPN 的名称、掩码或掩码长度、下一跳的 IP 地址、路由的优先级、路由的描述信息
3	（可选）RIP 进程号、VPN 实例绑定的 VLANIF 接口所在的网段地址、MCE 和 PE 之间运行的路由协议的种类和进程号、引入路由的开销值、引入路由时使用的路由策略名称

版权所有 © 华为技术有限公司

序号	数据
4	（可选）OSPF 进程号、OSPF 路由器 ID、OSPF 区域编号、VPN 实例绑定的 VLANIF 接口所在的网段地址、MCE 和 PE 之间运行的路由协议的种类和进程号、引入路由的开销值、引入路由的度量值类型、引入路由的外部 LSA 中的标记、引入路由时使用的路由策略名称
5	（可选）IS-IS 进程号、IS-IS 进程的网络实体名称、VPN 实例绑定的 VLANIF 接口的编号、MCE 和 PE 之间运行的路由协议的种类和进程号、引入路由的开销类型和开销值、引入的路由的管理标签号、存放引入路由的路由表的级别
6	（可行）自治系统号、CE 和 MCE 相连的 VLANIF 接口的 IP 地址、MCE 和 PE 之间运行的路由协议的种类和进程号、引入路由的 MED 度量值、引入路由时使用的路由策略名称

(可选)配置 MCE 与 Site 间使用静态路由

背景信息

在 MCE 设备上进行以下配置。

在 Site 设备上只需要正常配置路由协议即可，无须特殊配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip route-static vpn-instance** *vpn-source-name destination-address* { *mask* | *mask-length* }{ *interface-type interface-number* [*gateway-address*] | **vpn-instance** *vpn-destination-name gateway-address* | *gateway-address* } [**preference** *preference*] [**track bfd-session** *cfg-name*] [**description** *description*]，配置去往 Site 的静态路由。

在本设备上必须指定下一跳地址。

----结束

(可选)配置 MCE 与 Site 间使用 RIP

背景信息

在 MCE 上进行以下配置。

在 Site 设备上只需要正常配置路由协议即可，无须特殊配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*] **vpn-instance** *vpn-instance-name*，创建并使能和 VPN 实例使用的 RIP 进程，同时进入 RIP 视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **network** *network-address*，在 VPN 实例绑定的 VLANIF 接口的 IP 地址所属网段使能 RIP 路由。

步骤 4 （可选）执行命令 **import-route** { { **static** | **direct** } | { { **rip** | **ospf** | **isis** } [*process-id*] } } [**cost** *cost* | **route-policy** *route-policy-name*] *，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 PE 之间使用的是其它路由协议，则需要执行本步骤。

----结束

(可选)配置 MCE 与 Site 间使用 OSPF

背景信息

在 MCE 设备上进行以下配置。

在 Site 设备上只需要正常配置路由协议即可，无须特殊配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *，创建 VPN 实例使用的 OSPF 进程，并进入 OSPF 视图。

说明

在本步骤中，**vpn-instance** *vpn-instance-name* 参数必须给出。

步骤 3 （可选）执行命令 **import-route** { **limt** *limt-number* | *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name* |**tag** *tag* | **type** *type*] * }，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 PE 之间使用的是其它路由协议，则需要执行本步骤。

步骤 4 执行命令 **area** { *area-id* | *area-id-address* }，创建 OSPF 区域，并进入 OSPF 区域视图。

步骤 5 执行命令 **network** *ip-address wildcard-mask*，在 VPN 实例绑定的 VLANIF 接口的 IP 地址所属的网段使能 OSPF 路由。

----结束

(可选)配置 MCE 与 Site 间使用 IS-IS

背景信息

在 MCE 设备上进行以下配置。

在 Site 设备上只需要正常配置路由协议即可，无须特殊配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入和 VPN 实例绑定的 VLANIF 接口视图。

步骤 3 执行命令 **isis enable** [*process-id*]，在 VLANIF 接口上使能 IS-IS。

缺省情况下，VLANIF 接口不使能 IS-IS。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **isis** [*process-id*] **vpn-instance** *vpn-instance-name*，创建 VPN 实例使用的 IS-IS 进程，并进入 IS-IS 视图。

步骤 5 执行命令 **network-entity** *net*，配置网络实体名称。

缺省情况下，IS-IS 路由进程没有网络实体名称。

步骤 6 （可选）执行命令 **import-route** *protocol* [*process-id*] [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 PE 之间使用的是其它路由协议，则需要执行本步骤。

----结束

(可选)配置 MCE 与 Site 间使用 BGP

背景信息

在 MCE 设备上进行以下配置。

在 Site 设备上只需要正常配置路由协议即可，无须特殊配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，启动 BGP 并进入 BGP 视图。

缺省情况下，系统不运行 BGP。

步骤 3 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例视图。

步骤 4 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 Site 中和 MCE 相连的设备配置为 VPN 私网对等体。

步骤 5 （可选）执行命令 **import-route** *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 PE 之间使用的是其它路由协议，则需要执行本步骤。

步骤 6 执行命令 **peer** *ipv4-address* **allow-as-loop** [*number*]，配置允许路由环路。

缺省情况下，不允许路由环路。

说明

通常情况下，BGP 通过 AS 号检测路由环路。如果在 MCE 和 Site 之间运行 BGP，当 MCE 将路由信息通告给 Site 时带上本自治系统的 AS 号，再从 Site 接收路由更新时，路由更新消息中会带有本自治系统的 AS 号，这样 MCE 就不能接收这条路由更新信息，此时需要配置允许路由环路。

----结束

检查配置结果

完成上述配置后，在 MCE 上执行命令 **display ip routing-table vpn-instance**，在显示信息中可以看到去往本端 VPN 的路由。以 MCE 和 Site 之间使用 RIP 为例，显示信息如下：

```
[MCE] display ip routing-table vpn-instance vpnb
```


版权所有 © 华为技术有限公司

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: vpnb
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      172.16.0.0/16  Direct 0    0           D  172.16.1.2      Vlanif10
      172.16.1.1/32  Direct 0    0           D  172.16.1.1      Vlanif10
      172.16.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      172.18.0.0/16  Direct 0    0           D  172.18.1.2      Vlanif30
      172.18.1.1/32  Direct 0    0           D  172.18.1.1      Vlanif30
      172.18.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.0.0/16 RIP    100  1           D  172.16.1.1      Vlanif10
```

5.9.5 在 MCE 与 PE 间配置路由多实例

介绍 MCE 与 PE 之间，静态路由、RIP、OSPF、IS-IS 和 BGP 的配置方法。

在 MCE 与 PE 间配置路由多实例任务中，**(可选)配置 MCE 与 PE 间使用静态路由**～**(可选)配置 MCE 与 PE 间使用 BGP** 是并列关系，用户根据需要选一配置即可。

建立配置任务

应用场景

如果需要用一台 CE 同时连接多个 VPN，并且要实现这些 VPN 之间的业务完全隔离，则需要配置 MCE 功能。配置 MCE 功能，首先要在 MCE 设备和 PE 设备上 **5.9.3 配置 VPN 实例**，然后需要执行本配置任务，在 MCE 与 PE 间配置路由多实例。

前置任务

在 MCE 与 PE 间配置路由多实例前，需完成以下任务：

- **5.9.3 配置 VPN 实例**

数据准备

在 MCE 与 PE 间配置路由多实例前，需准备以下数据。

序号	数据
1	VPN 实例的名称
2	（可选）去往 PE 的静态的目的地址、目的 VPN 的名称、掩码或掩码长度、下一跳的 IP 地址、路由的优先级、路由的描述信息
3	（可选）RIP 进程号、VPN 实例绑定的 VLANIF 接口所在的网段地址、MCE 和 Site 之间运行的路由协议的种类和进程号、引入路由的开销值、引入路由时使用的路由策略名称
4	（可选）OSPF 进程号、OSPF 路由器 ID、OSPF 区域编号、VPN 实例绑定的 VLANIF 接口所在的网段地址、MCE 和 Site 之间运行的路由协议的种类和进程号、引入路由的开销值、引入路由的度量值类型、引入路由的外部 LSA 中的标记、引入路由时使用的路由策略名称

版权所有 © 华为技术有限公司

序号	数据
5	（可选）IS-IS 进程号、IS-IS 进程的网络实体名称、VPN 实例绑定的 VLANIF 接口的编号、MCE 和 Site 之间运行的路由协议的种类和进程号、引入路由的开销类型和开销值、引入的路由的管理标签号、存放引入路由的路由表的级别
6	（可行）自治系统号、CE 和 MCE 相连的 VLANIF 接口的 IP 地址、MCE 和 Site 之间运行的路由协议的种类和进程号、引入路由的 MED 度量值、引入路由时使用的路由策略名称

(可选)配置 MCE 与 PE 间使用静态路由

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上可以使用静态路由，也可以使用 RIP、OSPF、IS-IS 或 BGP，具体的配置方法请参见对应产品的用户手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip route-static vpn-instance** *vpn-source-name destination-address* { *mask* | *mask-length* }{ *interface-type interface-number* [*gateway-address*] | **vpn-instance** *vpn-destination-name gateway-address* | *gateway-address* } [**preference** *preference*] [**track bfd-session** *cfg-name*] [**description** *description*]，配置去往 PE 的静态路由。

在本设备上必须指定下一跳地址。

----结束

(可选)配置 MCE 与 PE 间使用 RIP

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要进行类似配置，具体的配置方法请参见对应产品的用户手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rip** [*process-id*] **vpn-instance** *vpn-instance-name*，创建并使能 VPN 实例使用的 RIP 进程，同时进入 RIP 视图。

步骤 3 执行命令 **network** *network-address*，在 VPN 实例绑定的 VLANIF 接口的 IP 地址所属的网段使能 RIP 路由。

步骤 4 （可选）执行命令 **import-route** { { **static** | **direct** } | { { **rip** | **ospf** | **isis** } [*process-id*] } } [**cost** *cost* | **route-policy** *route-policy-name*] *，配置从其它路由协议引入路由。

版权所有 © 华为技术有限公司

在本 VPN 中，如果 MCE 和 Site 之间使用的是其它路由协议，则需要执行本步骤。

----结束

(可选)配置 MCE 与 PE 间使用 OSPF

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要进行类似配置，具体的配置方法请参见对应产品的用户手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *，创建 VPN 实例使用的 OSPF 进程，并进入 OSPF 视图。

说明

在本步骤中，**vpn-instance** *vpn-instance-name* 参数必须给出。

步骤 3 （可选）执行命令 **import-route** { **limt** *limt-number* | *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name* |**tag** *tag* | **type** *type*] * }，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 Site 之间使用的是其它路由协议，则需要执行本步骤。

步骤 4 执行命令 **area** { *area-id* | *area-id-address* }，创建 OSPF 区域，并进入 OSPF 区域视图。

步骤 5 执行命令 **network** *ip-address wildcard-mask*，在 VPN 实例绑定的 VLANIF 接口的 IP 地址所属的网段使能 OSPF 路由。

----结束

(可选)配置 MCE 与 PE 间使用 IS-IS

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要进行类似配置，具体的配置方法请参见对应产品的用户手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入和 VPN 实例绑定的 VLANIF 接口视图。

步骤 3 执行命令 **isis enable** [*process-id*]，在 VLANIF 接口上使能 IS-IS。

缺省情况下，VLANIF 接口不使能 IS-IS。

步骤 4 执行命令 **isis** [*process-id*] **vpn-instance** *vpn-instance-name*，创建 VPN 实例使用的 IS-IS 进程，并进入 IS-IS 视图。

步骤 5 执行命令 **network-entity** *net*，配置网络实体名称。

版权所有 © 华为技术有限公司

缺省情况下，IS-IS 路由进程没有网络实体名称。

步骤 6 （可选）执行命令 **import-route** *protocol* [*process-id*] [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 Site 之间使用的是其它路由协议，则需要执行本步骤。

----结束

(可选)配置 MCE 与 PE 间使用 BGP

背景信息

在 MCE 设备上进行以下配置。

在 PE 设备上也需要进行类似配置，具体的配置方法请参见对应产品的用户手册。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp** *as-number*，启动 BGP 并进入 BGP 视图。

缺省情况下，系统不运行 BGP。

步骤 3 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例视图。

步骤 4 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 PE 配置为 VPN 私网对等体。

步骤 5 （可选）执行命令 **import-route** *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *，配置从其它路由协议引入路由。

在本 VPN 中，如果 MCE 和 Site 之间使用的是其它路由协议，则需要执行本步骤。

----结束

检查配置结果

在 PE 上执行 **display ip routing-table vpn-instance vpnb** 命令，可以看到去往本端 VPN 的路由。以华为 AC6605 设备为例，显示信息如下：

```
[PE1] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: vpnb
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

172.18.0.0/16       Direct  0    0           D   172.18.1.1      GigabitEthernet8/
0/0.1
172.18.1.1/32       Direct  0    0           D   127.0.0.1       InLoopBack0
172.18.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
192.168.0.0/16      O_ASE   150  1           D   172.16.1.1      GigabitEthernet8/
0/0.1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

5.9.6 MCE 配置举例

介绍 MCE 的组网举例。

版权所有 © 华为技术有限公司

配置 MCE 示例

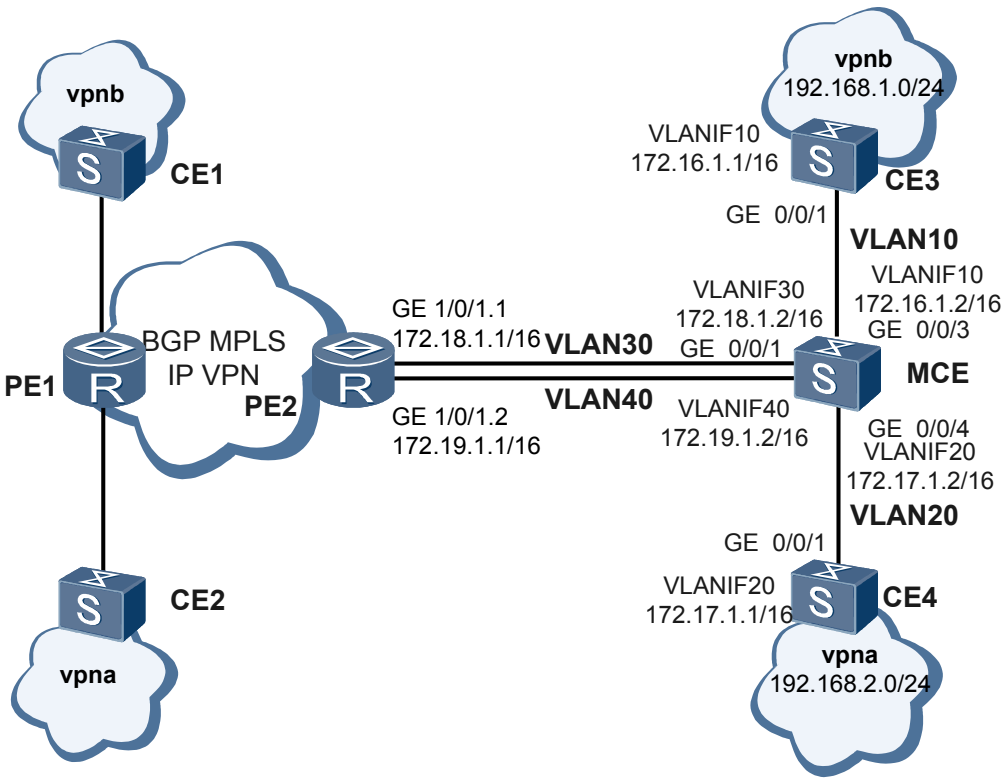
组网需求

如图 5-29 所示，组网情况如下：

- CE1、CE2、CE3、CE4 是 VPN 用户边界设备。
- CE1 和 CE3 同属于 VPN 实例 vpnb，CE2 和 CE4 同属于 VPN 实例 vpna。
- PE1 和 PE2 是骨干网的边界路由器。PE1 和 PE2 之间的骨干网配置了 BGP/MPLS IP VPN。
- MCE 是用作 VPN 多实例交换的设备。
- MCE 和 CE3、CE4 之间运行 RIP 路由协议。
- MCE 和 PE2 之间运行 OSPF 路由协议。

要求：在 MCE 设备上实现 VPN 之间的路由隔离，并通过 OSPF 将各 VPN 的路由发布到 PE2 设备上。

图 5-29 配置 MCE 示例组网图



配置思路

采用如下的思路配置 MCE：

版权所有 © 华为技术有限公司

1. 在 MCE、PE2、CE3、CE4 上创建 VLAN，并将这些设备之间互连的接口加入 VLAN。
2. 在 MCE 和 PE2 上创建并配置 VPN 实例。
3. 在 MCE 和 PE2 之间配置 OSPF 路由多实例。
4. 在 MCE 和 CE3、CE4 之间配置 RIP。

数据准备

为完成此配置例，需准备如下的数据：

- MCE、PE2、CE3、CE4 之间的 VLAN 如图 5-29 所示。
- 各 VLANIF 接口的 IP 地址如图 5-29 所示。

配置步骤

1. 创建 VLAN，并将这些设备之间互连的接口加入 VLAN。

   # 在 MCE 上创建 VLAN。

```
<Quidway> system-view
[Quidway] sysname MCE
[MCE] vlan batch 10 20 30 40
```

   # 在 MCE 上将接口加入 VLAN。

```
[MCE] interface gigabitethernet 0/0/1
[MCE-GigabitEthernet0/0/1] port link-type trunk
[MCE-GigabitEthernet0/0/1] port trunk allow-pass vlan 30 40
[MCE-GigabitEthernet0/0/1] quit
[MCE] interface gigabitethernet 0/0/3
[MCE-GigabitEthernet0/0/3] port link-type trunk
[MCE-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[MCE-GigabitEthernet0/0/3] quit
[MCE] interface gigabitethernet 0/0/4
[MCE-GigabitEthernet0/0/4] port link-type trunk
[MCE-GigabitEthernet0/0/4] port trunk allow-pass vlan 20
[MCE-GigabitEthernet0/0/4] quit
```

   # 在 PE2 上创建子接口，并将子接口加入 VLAN。

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] interface gigabitethernet 1/0/1.1
[PE2-GigabitGigabitethernet1/0/1.1] vlan-type dot1q 30
[PE2-GigabitGigabitethernet1/0/1.1] quit
[PE2] interface gigabitethernet 1/0/1.2
[PE2-GigabitGigabitethernet1/0/1.2] vlan-type dot1q 40
[PE2-GigabitGigabitethernet1/0/1.2] quit
```

   # 在 CE3 上创建 VLAN。

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] vlan 10
```

   # 在 CE3 上将接口加入 VLAN。

```
[CE3-A] interface gigabitethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port link-type trunk
[CE3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[CE3-GigabitEthernet0/0/1] quit
```

   # 在 CE4 上创建 VLAN。

   和 CE3 上的配置类似，此处不在赘述,略。

   # 在 CE4 将接口加入 VLAN。

版权所有 © 华为技术有限公司

和 CE3 上的配置类似，此处不在赘述,略。

2. 创建并配置 VPN 实例。

在 MCE 上创建 VPN 实例。

```
[MCE] ip vpn-instance vpna
[MCE-vpn-instance-vpna] route-distinguisher 100:1
[MCE-vpn-instance-vpna] quit
[MCE] ip vpn-instance vpnb
[MCE-vpn-instance-vpnb] route-distinguisher 100:2
[MCE-vpn-instance-vpnb] quit
```

在 MCE 上配置 VPN 实例和 VLANIF 接口绑定，并配置 VLANIF 接口的 IP 地址。

```
[MCE] interface vlanif 10
[MCE-Vlanif10] ip binding vpn-instance vpnb
[MCE-Vlanif10] ip address 172.16.1.2 16
[MCE-Vlanif10] quit
[MCE] interface vlanif 20
[MCE-Vlanif20] ip binding vpn-instance vpna
[MCE-Vlanif20] ip address 172.17.1.2 16
[MCE-Vlanif20] quit
[MCE] interface vlanif 30
[MCE-Vlanif30] ip binding vpn-instance vpnb
[MCE-Vlanif30] ip address 172.18.1.2 16
[MCE-Vlanif30] quit
[MCE] interface vlanif 40
[MCE-Vlanif40] ip binding vpn-instance vpna
[MCE-Vlanif40] ip address 172.19.1.2 16
[MCE-Vlanif40] quit
```

在 PE2 上创建 VPN 实例。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:1
[PE2-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE2-vpn-instance-vpnb] route-distinguisher 100:2
[PE2-vpn-instance-vpnb] quit
```

在 PE2 上配置子接口和 VPN 实例绑定，并配置子接口的 IP 地址。

```
[PE2] interface gigabitethernet 1/0/1.1
[PE2-GigabitGigabitethernet1/0/1.1] ip binding vpn-instance vpnb
[PE2-GigabitGigabitethernet1/0/1.1] ip address 172.18.1.1 255.255.0.0
[PE2-GigabitGigabitethernet1/0/1.1] quit
[PE2] interface gigabitethernet 1/0/1.2
[PE2-GigabitGigabitethernet1/0/1.2] ip binding vpn-instance vpna
[PE2-GigabitGigabitethernet1/0/1.2] ip address 172.19.1.1 255.255.0.0
[PE2-GigabitGigabitethernet1/0/1.2] quit
```

3. 在 MCE 和 PE2 之间配置 OSPF 路由多实例。

在 PE2 上配置 OSPF 路由多实例。

```
[PE2] ospf 100 vpn-instance vpna
[PE2-ospf-100] area 0
[PE2-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[PE2-ospf-100-area-0.0.0.0] quit
[PE2-ospf-100] quit
[PE2] ospf 200 vpn-instance vpnb
[PE2-ospf-200] area 0
[PE2-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[PE2-ospf-200-area-0.0.0.0] quit
[PE2-ospf-200] quit
```

在 MCE 上配置 OSPF 路由多实例。

```
[MCE] ospf 100 vpn-instance vpna
[MCE-ospf-100] area 0
[MCE-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[MCE-ospf-100-area-0.0.0.0] quit
[MCE-ospf-100] quit
[MCE] ospf 200 vpn-instance vpnb
```


版权所有 © 华为技术有限公司

```
[MCE-ospf-200] area 0
[MCE-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[MCE-ospf-200-area-0.0.0.0] return
```

4. 在 MCE 和 CE3、CE4 之间配置 RIP。

   # 在 MCE 上配置 RIP-2。

```
[MCE] rip 100 vpn-instance vpna
[MCE-rip-100] version 2
[MCE-rip-100] network 172.17.0.0
[MCE-rip-100] import-route ospf 100
[MCE-rip-100] quit
[MCE] rip 200 vpn-instance vpnb
[MCE-rip-200] version 2
[MCE-rip-200] network 172.16.0.0
[MCE-rip-200] import-route ospf 200
```

   # 在 CE3 上配置 RIP-2。

```
[CE3] rip 200
[CE3-rip-200] version 2
[CE3-rip-200] network 172.16.0.0
[CE3-rip-200] network 192.168.1.0
[CE3-rip-200] import-route
```

   # 在 CE4 上配置 RIP-2。

```
[CE4] rip 100
[CE4-rip-100] version 2
[CE4-rip-100] network 172.17.0.0
[CE4-rip-100] network 192.168.2.0
[CE4-rip-100] import-route direct
```

   # 在 MCE 上引入 RIP 路由

```
[MCE] ospf 100
[MCE-ospf-100] import-route rip 100
[MCE-ospf-100] quit
[MCE] ospf 200
[MCE-ospf-200] import-route rip 200
```

5. 检查配置结果。

   # 完成上述配置后，在 MCE 上执行命令 **display ip routing-table vpn-instance** 命令，可以看到去往本端 VPN 的路由。

   以 vpnb 为例：

```
[MCE] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: vpnb
         Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

      172.16.0.0/16  Direct 0    0           D  172.16.1.2      Vlanif10
      172.16.1.1/32  Direct 0    0           D  172.16.1.1      Vlanif10
      172.16.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      172.18.0.0/16  Direct 0    0           D  172.18.1.2      Vlanif30
      172.18.1.1/32  Direct 0    0           D  172.18.1.1      Vlanif30
      172.18.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      192.168.0.0/16 RIP    100  1           D  172.16.1.1      Vlanif10
```

配置文件

- MCE 的配置文件

```
#
 sysname MCE
#
 vlan batch 10 20 30 40
#
```


版权所有 © 华为技术有限公司

```
ip vpn-instance vpna
 route-distinguisher 100:1
#
ip vpn-instance vpnb
 route-distinguisher 100:2
#
interface Vlanif10
 ip binding vpn-instance vpnb
 ip address 172.16.1.2 255.255.0.0
#
interface Vlanif20
 ip binding vpn-instance vpna
 ip address 172.17.1.2 255.255.0.0
#
interface Vlanif30
 ip binding vpn-instance vpnb
 ip address 172.18.1.2 255.255.0.0
#
interface Vlanif40
 ip binding vpn-instance vpna
 ip address 172.19.1.2 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 100 vpn-instance vpna
 import-route rip 100
 area 0.0.0.0
  network 172.17.0.0 0.0.255.255
  network 172.19.0.0 0.0.255.255
#
ospf 200 vpn-instance vpnb
 import-route rip 200
 area 0.0.0.0
  network 172.16.0.0 0.0.255.255
  network 172.18.0.0 0.0.255.255
#
rip 100 vpn-instance vpna
 version 2
 network 172.17.0.0
 import-route ospf 100
#
rip 200 vpn-instance vpnb
 version 2
 network 172.16.0.0
 import-route ospf 200
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
ip vpn-instance vpna
 route-distinguisher 100:1
#
ip vpn-instance vpnb
 route-distinguisher 100:2
#
interface GigabitGigabitethernet1/0/1.1
 vlan-type dot1q 30
```


版权所有 © 华为技术有限公司

```
 ip binding vpn-instance vpnb
 ip address 172.18.1.1 255.255.0.0
#
interface GigabitGigabitethernet1/0/1.2
 vlan-type dot1q 40
 ip binding vpn-instance vpna
 ip address 172.19.1.1 255.255.0.0
#
#
ospf 100 vpn-instance vpna
 area 0.0.0.0
  network 172.19.0.0 0.0.255.255
#
ospf 200 vpn-instance vpnb
 area 0.0.0.0
  network 172.18.0.0 0.0.255.255
#
return
```

说明

只列出了和 MCE 相关的配置文件。BGP/MPLS IP VPN 的配置方法请参见对应设备的手册。

- CE3 的配置文件

```
#
 sysname CE3
#
vlan batch 10
#
interface Vlanif10
 ip address 172.16.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
rip 200
 version 2
 network 172.16.0.0
 network 192.168.1.0
 import-route direct
#
return
```

- CE4 的配置文件

```
#
 sysname CE4
#
vlan batch 20
#
interface Vlanif20
 ip address 172.17.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
rip 100
 version 2
 network 172.17.0.0
 network 192.168.2.0
 import-route direct
#
return
```


版权所有 © 华为技术有限公司

6 组播配置

关于本章

本文档针对 AC6605 的组播业务，从基本原理、协议实现过程、配置步骤和配置举例方面介绍了 IP 组播网络的配置方法。

本文档提供了 AC6605 组播业务的配置方法。

6.1 IP 组播配置指导
介绍在 IPv4 网络中使用的组播地址，各种组播协议在网络中的应用位置、功能和典型配置方案。

6.2 IGMP Snooping 配置
介绍 IGMP Snooping 特性的配置方法和维护命令，并提供配置举例。

6.3 组播 VLAN 配置
介绍组播 VLAN 的配置方法、维护命令，并提供配置举例。

6.4 可控组播配置
介绍了可控组播的原理，及配置步骤。

6.5 IGMP 配置
介绍 IGMP 的配置方法、维护命令，并提供配置举例。

6.6 PIM-DM（IPv4）配置
通过配置 PIM 协议，可以实现 AS 域内组播路由与数据转发。PIM-DM 是密集模式的域内组播路由协议，适用于组成员分布相对密集的小型网络。

6.7 PIM-SM（IPv4）配置
通过配置 PIM 协议，可以实现 AS 域内组播路由与数据转发。PIM-SM 是稀疏模式的域内组播路由协议，适用于组成员分布相对分散、范围较广的大规模网络。

6.8 MSDP 配置
通过配置 MSDP 协议，可以实现 PIM-SM 域间组播路由与数据转发、PIM-SM 域内的 Anycast RP。

6.9 IPv4 组播路由管理
系统可同时维护多个组播路由协议，通过控制平面与转发平面之间的信息交互，控制组播路由和转发。

6.10 MLD Snooping 配置

版权所有 © 华为技术有限公司

介绍了 MLD（Multicast Listener Discovery）Snooping 在 AC6605 设备上的实现和配置方法。

版权所有 © 华为技术有限公司

6.1 IP 组播配置指导

介绍在 IPv4 网络中使用的组播地址，各种组播协议在网络中的应用位置、功能和典型配置方案。

6.1.1 IP 组播概述

组播（Multicast）是一种点对多点的数据传输模式。在数据传输的同时，能够保障信息的安全性且只占用有限的网络带宽。

IPv4 和 IPv6 上应用的组播技术统称为 IP 组播。

当前应用 IP 组播技术实现的互联网信息服务包括：IPTV、实时视/音频会议、远程教育、远程医疗等。

6.1.2 AC6605 支持的 IP 组播特性

AC6605 目前支持在 IPv4 网络上构建组播服务，但不支持在 IPv4 混合网络上构建组播服务。

6.1.3 IPv4 组播配置指导

介绍 IPv4 网络中使用的组播地址、组播协议及典型配置方案。

IPv4 组播地址

IPv4 组播地址范围是：224.0.0.0 ～ 239.255.255.255，范围及含义见**表 6-1**。

组播数据业务可用的组地址范围是：224.0.1.0 ～ 239.255.255.255。任何用户主机（或其他接收设备），加入此范围内的某组播组，就成为了该组成员，可以识别并接收以该 IP 组播地址为目的地址的 IP 报文。网络中的组成员可能广泛分布在网络中的任何地方，用户主机可以在任何时刻加入和离开组播组。

表 6-1 IPv4 组播地址的范围及含义

D 类地址范围	含义
224.0.0.0 ～ 224.0.0.255	本地链路的保留组地址。英特网地址分配组织（IANA）为路由协议预留的组播地址（也称为永久组地址），用于标识一组特定的网络设备，不用于组播转发。
224.0.1.0 ～ 231.255.255.255 233.0.0.0 ～ 238.255.255.255	任意源组播地址。全网范围内有效。
232.0.0.0 ～ 232.255.255.255	指定源组播地址。缺省的 SSM 组地址范围，全网范围内有效。

版权所有 © 华为技术有限公司

D 类地址范围	含义
239.0.0.0 ～ 239.255.255.255	管理范围组地址。缺省的 BSR 管理域组地址范围，仅在 BSR 管理域内有效，属于私有地址。在不同的 BSR 管理域内使用相同的地址不会冲突。

IPv4 组播协议

实现一套完整的 IPv4 组播服务，需要部署在网络各个位置的多种组播协议相互配合，共同运作，如图 6-1 所示。

图 6-1 IPv4 组播协议的应用位置

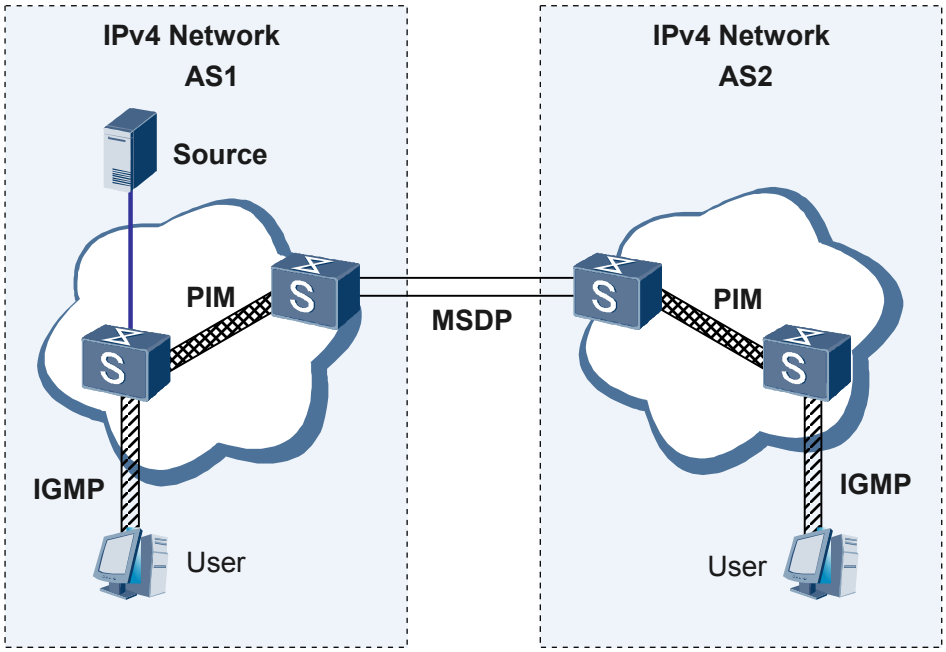


表 6-2 IPv4 组播协议

应用位置	目的	组播协议
用户主机与组播交换机之间	将用户主机接入组播网络： ● 在主机侧实现组播组成员动态加入与离开。 ● 在交换机侧实现组成员关系的维护与管理，同时支持与上层组播路由协议的信息交互。	IGMP（Internet Group Management Protocol）组播组管理协议

华为专有和保密信息
版权所有 © 华为技术有限公司

应用位置	目的	组播协议
域内组播交换机之间	组播路由与转发： ● 按需创建组播路由。 ● 动态响应网络拓扑变化，维护组播路由表。 ● 按照路由表项执行转发。	PIM（Protocol Independent Multicast）协议无关组播，包括 DM（Dense Mode）密级模式和 SM（Sparse Mode）稀疏模式两种
域间组播交换机之间	域间组播源信息共享： ● 源所在域内的交换机将本地源信息传播给其他域内的交换机。 ● 不同域的交换机之间传递源信息。	MSDP（Multicast Source Discovery Protocol）组播源发现协议

典型配置方案

注意

请务必根据网络实际情况和具体的业务需求，有针对性的定制配置方案。本节配置方案仅供参考。

将网络环境分为两类，分别适用不同的配置方案。具体配置方法请参见《AC6605 无线接入控制器 配置指南-组播》中的相应章节。

说明

配置 IP 组播之前，首先确保网络中单播路由正常。

小规模网络

适用于局域网内部的组播数据传输，不与 Internet 互通。比如实验网。

请务必遵循如下配置顺序：

1. 全网 AC6605 使能组播功能。
2. 在所有 AC6605 接口上使能 PIM-DM。
3. 在连接用户主机的 AC6605 接口上使能 IGMP。

大规模网络

适用于 ISP 网络上承载的组播业务，与 Internet 互通。

请务必遵循如下顺序。

1. 全网 AC6605 使能组播功能。
2. 在所有 AC6605 接口上使能 PIM-SM。
3. 在连接用户主机的 AC6605 接口上使能 IGMP。
4. 配置 RP，可以选用静态 RP 或者 C-RP。

版权所有 © 华为技术有限公司

5. 划分 PIM-SM 域。
6. 在 PIM-SM 域内配置 MSDP，实现 Anycast RP。
7. 在 PIM-SM 域间配置 MSDP，通常配合使用 MBGP。

控制组播转发

IP 组播使用组播路由表和转发表来指导组播报文转发。通过配置 RPF 路由策略可以调整组播数据的传输路线，通过配置转发策略和转发表的容量可以在一定程度上限制组播转发的范围。

6.2 IGMP Snooping 配置

介绍 IGMP Snooping 特性的配置方法和维护命令，并提供配置举例。

6.2.1 IGMP Snooping 概述

介绍 IGMP Snooping 协议的功能和优点。

IGMP Snooping 功能

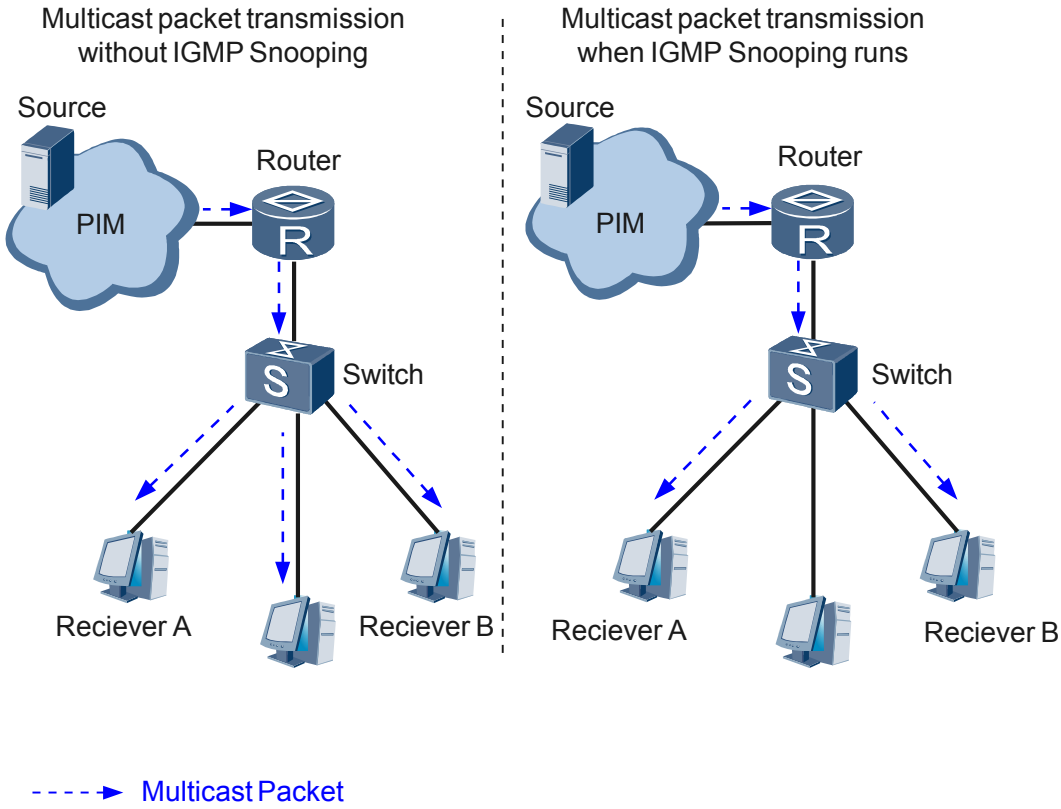
IGMP Snooping(Internet Group Management Protocol Snooping)是一种二层组播协议，通过侦听上层路由器和用户主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文的转发。

在网络运行环境中，当上游设备将组播报文转发下来以后，处于接入边缘的设备负责将组播报文转发给组播用户，使用户收看所点播的节目。如图 6-2 所示，缺省情况下，组播数据在数据链路层被广播，造成带宽浪费，并使付费和未付费用户都能收看所点播的节目。

在二层设备上配置 IGMP Snooping 后，已知组播组的组播数据不会在数据链路层被广播，而会发给指定的接收者，使只有付费的用户才能收看所点播的节目。

版权所有 © 华为技术有限公司

图 6-2 二层设备运行 IGMP Snooping 前后的对比



IGMP Snooping 优势

IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，有以下优点：

- 减少了二层网络中的广播报文，节约带宽
- 增强了组播信息的安全性
- 为实现每台用户主机的单独计费提供了方便

6.2.2 AC6605 支持的 IGMP Snooping 特性

介绍 IGMP Snooping 特性在 AC6605 中的支持情况。

IGMP Snooping

AC6605 支持配置基于 VLAN 的 IGMP Snooping 功能。

IGMP Snooping 通过侦听上层路由器和主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文的转发，实现二层组播。

通过配置成员接口静态加入组播组，实现用户长期稳定接收组播数据报文。

当二层网络变化时，配置主动发送 IGMP Query 报文，使 AC6605 感知二层网络拓扑变化，按照新的网络拓扑正确转发组播数据，从而保证业务不间断。

版权所有 © 华为技术有限公司

端口快速离开

端口快速离开是指当交换机某端口收到主机发送的离开某指定组播组的 IGMP Leave 消息时，就将该端口从指定组播组的出端口信息中删除。在组播应用于 IPTV 的场景下，需要配置端口快速离开机制，在这种场景中交换机端口一般只连接一个用户主机，快速离开可以保证用户切换频道的速度。

IGMP Snooping 端口快速离开有以下优点：

- 减小响应延迟。
- 节省因各种消息而占用的网络带宽。

IGMP Snooping 查询器

在运行了 IGMP 的组播网络中，会有一台三层组播设备充当 IGMP 查询器，负责发送 IGMP 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。

在一个没有三层组播设备的网络中，二层设备通常并不支持 IGMP，因此无法实现 IGMP 查询器的相关功能。为了解决这个问题，可以在二层设备上使能 IGMP Snooping 查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。

IGMP Snooping Proxying

通过在边缘设备上配置 IGMP Snooping Proxying 功能，可以减少其上游三层设备收到的 IGMP 报告报文和离开报文的数量，有效提高其上游三层设备的整体性能。配置了 IGMP Snooping Proxying 功能的设备，在其上游设备看来，相当于一台主机；而在其下游主机看来，则相当于一台查询器。

IGMP Snooping 策略

IGMP Snooping 支持用户通过命令配置组播组策略，使 VLAN 内的端口只能加入符合 ACL 规则的组播组。通过组播组策略，可以限制用户加入组播组范围，提高了组播的可控性和安全性。

IGMP Snooping SSM Mapping 功能

SSM 模型中，如果接收者主机上运行的是 IGMPv3，则可以在 IGMPv3 的组播数据报文中直接指定组播源的地址；如果某些接收者主机只能运行 IGMPv1 或 IGMPv2，则在 IGMPv1 或 IGMPv2 的组播数据报文中无法指定组播源的地址。配置 IGMP Snooping SSM Mapping 功能，可以使组播组与组播源之间能够建立一一对应的映射关系，将 IGMPv1 或 IGMPv2 数据报文中所包含的（*,G）信息映射为(S,G)信息，提供 SSM 组播服务。

静态组播 MAC 地址

在二层组播中，除了可通过二层组播协议（如 IGMP Snooping）动态建立组播 MAC 地址表项外，还可以通过手工方式配置组播 MAC 地址表项，将端口与组播 MAC 地址进行静态绑定，以便灵活控制组播信息送达的目的端口，组播报文只会向配置了该组播 MAC 地址的端口转发。

6.2.3 配置基于 VLAN 的 IGMP Snooping

介绍如何配置基于 VLAN 的 IGMP Snooping。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

在网络运行环境中，当上游设备将组播报文转发下来以后，处于接入边缘的设备负责将组播报文转发给组播用户，使用户收看所点播的节目。缺省情况下，组播数据在数据链路层被广播，造成带宽浪费，并使付费和未付费用户都能收看所点播的节目。

在二层设备上配置 IGMP Snooping 后，已知组播组的组播数据不会在数据链路层被广播，而会发给指定的接收者，使只有付费的用户才能收看所点播的节目。

前置任务

在配置基于 VLAN 的 IGMP Snooping 功能之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。
- 接口加入 VLAN。

数据准备

在配置基于 VLAN 的 IGMP Snooping 功能之前，需要准备以下数据。

序号	数据
1	VLAN 编号
2	（可选）IGMP 报文的版本
3	相关功能的接口类型和编号
4	（可选）查询器的参数：通用查询时间间隔、健壮系数、最大响应时间和最后成员查询时间间隔
5	（可选）应用组播过滤策略的 ACL 规则
6	（可选）IGMP 报文抑制时间
7	（可选）路由器接口老化时间
8	（可选）IGMP 查询报文的源 IP 地址

配置 VLAN 的 IGMP Snooping 基本功能

背景信息

缺省情况下 AC6605 的 IGMP Snooping 功能处于关闭状态，因此需要使能全局 IGMP Snooping 功能。

用户可以选择组播数据的转发模式，组播流可以按 IP 地址转发，也可以按 MAC 地址转发。由于组播 IP 地址映射到 MAC 地址时，可能出现 32 个 IP 地址映射到同一个 MAC

版权所有 © 华为技术有限公司

地址上，因此建议选择 IP 地址转发模式，否则可能造成未点播的用户也会收到组播数据。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **igmp-snooping enable**，使能全局 IGMP Snooping 功能。

步骤 3 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 4 （可选）执行命令 **l2-multicast forwarding-mode** { **ip** | **mac** }，配置 VLAN 中组播流是按 IP 地址还是 MAC 地址转发。

缺省情况下，组播流是按 IP 地址转发。

注意

配置 VLAN 中组播数据转发模式需要在没有使能该 VLAN 的 IGMP Snooping 功能时进行。配置完成后需要使能 IGMP Snooping 功能才会生效。

步骤 5 执行命令 **igmp-snooping enable**，使能 VLAN 的 IGMP Snooping 功能。

说明

可以在系统视图下使用 **igmp-snooping enable** [**vlan** *vlan-id1* [**to** *vlan-id2*] & <1-10>]命令，使能多个 VLAN 的 IGMP Snooping 功能。

如果 VLAN 配置 igmp-snooping 功能之后，则不能配置 N:1 VLAN Mapping 功能和 VLAN Stacking 功能。

步骤 6 （可选）执行命令 **igmp-snooping version** { **1** | **2** |**3** }，配置 IGMP Snooping 可以处理的 IGMP 版本。

缺省情况下，AC6605 可以处理 IGMPv1 和 IGMPv2 的报文，但无法处理 IGMPv3 的报文。

说明

当 VLAN 内的转发模式为基于 MAC 地址转发时，无法配置 IGMPv3 版本。

----结束

（可选）配置静态路由器接口

背景信息

如果需要增强对用户接收组播数据的控制，可以禁止接口的动态学习功能。接口的动态学习功能被禁止后，只能通过手工进行静态配置。

禁止 VLAN 的路由器接口动态学习功能，VLAN 不再监听 IGMP Query 报文，只能手工配置静态路由器接口。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **undo igmp-snooping router-learning**，禁止路由器接口动态学习功能。

缺省情况下，VLAN 的路由器接口动态学习功能处于使能状态。

步骤 4 执行命令 **quit**，退出 VLAN 视图。

步骤 5 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 接口、Eth-Trunk 接口。该接口是 AC6605 与上层路由器相连接的接口。

步骤 6 执行命令 **igmp-snooping static-router-port vlan** { { *vlan-id* [**to** *vlan-id*] } &<1-10> }，配置接口为静态路由器接口。

----结束

（可选）配置成员接口功能

背景信息

成员接口用来接收发往某组播组或组播源组的组播数据，缺省情况下为动态成员接口。当动态成员接口在其老化时间超时前没有收到该组播组的 IGMP 成员关系报告报文，设备将把该接口从该组播组所对应转发表项的出接口列表中删除。

当某个 VLAN 内的每个接口下都只有一个接收者主机时，可以使能该 VLAN 的接口快速离开功能。接口快速离开是指当设备从成员接口收到 IGMP Leave 消息时，不再等待转发表项老化，而是立即将该接口对应的转发表项从组播转发表中删除。

如果接口所连接的主机需要固定接收发往某组播组或组播源组的组播数据，可以配置该接口静态加入该组播组或组播源组，成为静态成员接口，静态成员接口不会老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 配置成员接口老化时间。请参见**（可选）配置 IGMP Snooping 查询器**。

如果组播组成员的变动比较频繁，可以把动态成员接口老化时间设置小一些，反之亦然。

步骤 4 （可选）执行命令 **igmp-snooping prompt-leave** [**group-policy** *acl-number*]，配置成员接口快速离开。

缺省情况下，不允许成员接口快速离开。

如果不指定 **group-policy** *acl-number* 参数，则 AC6605 只要从该 VLAN 内的成员接口收到离开消息，就对该接口做快速离开处理。

版权所有 © 华为技术有限公司

说明

在 AC6605 的实现中，默认 ACL 规则 **permit** 对所有组播组都适用，如果要配置针对某个组的快速离开功能，需要结合 **rule deny source any** 命令一起使用。

步骤 5 执行命令 **quit**，返回系统视图。

步骤 6 （可选）配置静态成员接口

1. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

   这里的接口可以是 GE 接口、Eth-Trunk 接口。

2. （可选）执行命令 **undo igmp-snooping learning vlan** { *vlan-id* { [*&<1－10>*][**to** *vlan-id*] | **all** } }， 禁止组播成员接口动态学习功能。

   缺省情况下，使能接口的转发表项动态学习功能。禁止组播成员接口动态学习功能之后，如果要完成组播数据的转发，接口只能静态加入组播组。

3. 执行命令 **l2-multicast static-group** { [**source-address** *source-ip-address*] **group-address** *group-ip-address* } **vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }，配置接口静态加入组播组，接口成为静态成员接口。也可以通过命令 **l2-multicast static-group group-address** *group-ip-address1* to *group-ip-address2* **vlan** *vlan-id* 批量将接口加入组播组。

   说明

   接口静态加入组播组之后，配置 limit-action 功能不生效。

----结束

（可选）配置 IGMP Snooping 查询器

背景信息

当上层路由器的 IGMP 报文因为某些原因不能到达 AC6605（例如未运行 IGMP 协议），或上层路由器的组播转发表项不需要动态学习而是静态配置时，可在本 AC6605 上配置查询器，代替上层路由器发送 IGMP Query 消息，同时根据网络需要，可以调整查询器的参数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping querier enable**，使能查询器功能。

缺省情况下，查询器功能处于禁止状态。

步骤 4 （可选）执行命令 **igmp-snooping query-interval** *query-interval*，配置查询器发送通用查询报文的时间间隔。

缺省情况下，通用查询时间间隔为 60 秒。

步骤 5 （可选）执行命令 **igmp-snooping robust-count** *robust-count*，配置查询器的 IGMP 健壮系数。

缺省情况下，IGMP 健壮系数为 2。

版权所有 © 华为技术有限公司

步骤 6 （可选）执行命令 **igmp-snooping max-response-time** *max-response-time*，配置查询器最大响应时间。

缺省情况下，IGMP 查询报文的最大响应时间是 10 秒。

说明

最大响应时间应小于通用查询时间间隔。

当 AC6605 收到主机的 IGMP Report 报文后，成员接口老化时间设置为：IGMP 健壮系数 × 通用查询时间间隔 + 最大响应时间。当参数都取缺省值时，成员接口老化时间缺省值为 130 秒。

步骤 7 （可选）执行命令 **igmp-snooping lastmember-queryinterval** *lastmember-queryinterval*，配置查询器发送特定组查询报文时间间隔。

缺省情况下，特定组查询时间间隔为 1 秒。

说明

当 AC6605 收到主机的 IGMP Leave 报文后，重置成员接口老化时间设置为：最后成员查询时间间隔（即特定组查询消息发送时间间隔） × IGMP 健壮系数。

由于运行 IGMPv1 时，主机离开组播组时不发送 IGMP Leave 报文，因此只有当 VLAN 内可以处理 IGMPv2 报文时，本配置才有意义。

----结束

（可选）配置接口加入最大组播组数量

背景信息

如果限制用户点播组播节目的数量，可配置接口加入的组播组最大数量，控制接口上的数据流量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 接口、Eth-Trunk 接口。

步骤 3 执行命令 **igmp-snooping group-limit** *group-limit* **vlan** {*vlan-id* [**to** *vlan-id*] } &<1-10>，配置接口加入的组播组最大数量。

----结束

（可选）配置组播组策略

背景信息

VLAN 的组播组策略主要用于对 VLAN 内的主机加入的组播组进行限制，并可对主机可以加入的组播组数量进行限制。

说明

创建 VLAN 的组播组策略的 ACL 时，**rule** 命令必须使用 **deny** 参数对某些组播组进行限制，即只能通过配置 VLAN 的组播组策略禁止 VLAN 内的主机访问全部或指定组播组。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping group-policy** *acl-number* [**version** *number*]，配置组播组策略，使 VLAN 内的接口只能动态加入符合 ACL 规则的组播组。

缺省情况下，VLAN 没有配置组播组策略，即 VLAN 内的主机可以加入任何组播组。如果不指定应用组播组策略的 IGMP 报文版本，则 AC6605 对接收到的所有 IGMP 报文都应用该组播组策略。

说明

当配置的 group-policy 为高级 ACL 规则时，无论 ACL 规则配置什么协议字段，该 ACL 都默认会对组播组生效。

----结束

（可选）配置 IGMP 报文抑制功能

背景信息

当二层设备收到来自某组播组成员的 IGMP 成员关系报告报文时，会将该报文转发给与其直连的三层设备。这样，当二层设备上存在属于某组播组的多个成员时，与其直连的三层设备会收到这些成员发送的相同 IGMP 成员关系报告报文。

当使能了 Report 和 Leave 报文的抑制功能后，在一个查询间隔内二层设备只会把收到的某组播组内的第一个 IGMP 成员关系报告报文（Report 和 Leave 报文）转发给三层设备，而不继续向三层设备转发来自同一组播组的其它 IGMP 成员关系报告报文，这样可以减少网络中的报文数量。

在报文抑制时间内，AC6605 对用户发送的连续相同的 IGMP 报文只向上层设备转发一份，减少冗余报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping report-suppress**，配置 VLAN 内对 Report 和 Leave 报文的抑制功能。

在配置了此命令后，AC6605 只会在组播组的第一个成员加入和最后一个成员离开时，向上游设备发送一条 Report 和 Leave 报文。

步骤 4 （可选）执行命令 **igmp-snooping suppress-time** *suppress-time*，配置当前 VLAN 内的 IGMP 报文抑制时间。

缺省情况下，IGMP 报文抑制时间为 10 秒。对 IGMP Report、IGMP Leave 报文的抑制时间最好等于当前 VLAN 的最大响应时间。

----结束

版权所有 © 华为技术有限公司

（可选）配置丢弃未知组播数据报文

背景信息

如果收到未知组播数据报文，缺省情况下在 VLAN 内广播。如果组播业务比较稳定，比如说静态二层组播业务，对于未知组播报文可以无需处理，可以配置丢弃未知组播数据报文。如果组播业务不太稳定，有组播用户频繁加入和退出的情况，对于未知组播报文必须进行处理，否则可能会导致部分用户无法接收到组播数据，必须配置丢弃未知组播数据报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **multicast drop-unknown**，配置丢弃未知组播数据报文。

----结束

（可选）配置主动发送 IGMP Query 报文

背景信息

当二层网络拓扑发生变化时，VLAN 报文的转发路径可能发生变化，配置主动发送 IGMP Query 报文，使 AC6605 感知二层网络拓扑变化，当组成员主机回应 IGMP Report 报文，AC6605 根据 IGMP Report 更新组成员接口信息，将组播数据流迅速切换到新的转发路径上，按照新的网络拓扑正确转发组播数据，从而保证业务不间断。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **igmp-snooping send-query enable**，配置 AC6605 的 IGMP Snooping 功能响应二层网络拓扑变化事件。

说明

响应二层网络拓扑变化事件功能一般结合环网使用，当环网的拓扑发生变化时，AC6605 发送源 IP 地址为 192.168.0.1 的 IGMP 查询报文。该源地址可以通过 **igmp-snooping send-query source-address** *source-address* 命令进行修改。

----结束

（可选）配置对 IGMP 报文中 Router-Alert 选项的处理方式

背景信息

Router Alert 是一种标示协议报文的特殊机制，如果一个报文中带有 Router Alert 选项，则表示该报文需要被上送到路由协议层去处理。

缺省情况下设备不对 Router-Alert 选项进行检查，IGMP 报文中无论是否携带有 Router-Alert 选项，设备都会将其送给上层协议进行处理。为了提高设备性能、减少不必要的

版权所有 © 华为技术有限公司

开支，同时出于协议安全性的考虑，可以配置设备接收或发送未携带 Router-Alert 选项的 IGMP 报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping require-router-alert**，配置接收的 IGMP 报文的 IP 头中必须带有 Router Alert。如果 AC6605 从当前 VLAN 内接收的 IGMP 报文的 IP 头中不带有 Router Alert，则 AC6605 不对报文进行处理，直接丢弃。

缺省情况下，AC6605 从 VLAN 内接收的 IGMP 报文的 IP 头中可以不带有 Router Alert。

步骤 4 执行命令 **igmp-snooping send-router-alert**，配置在 AC6605 发送的 IGMP 报文的 IP 头中携带 Router Alert 选项。使用 **undo igmp-snooping send-router-alert** 命令可以禁止在发送的 IGMP 报文的 IP 头中携带 Router Alert。

缺省情况下，AC6605 向 VLAN 内发送的 IGMP 报文的 IP 报文头中带有 Router Alert。

----结束

（可选）配置 VLAN 的 IGMP Snooping Proxy

背景信息

在 AC6605 上配置 IGMP Proxy 功能后，AC6605 可以代替上游路由器向下游发送 IGMP Query 消息、也可以代替下游主机向上游路由器发送 IGMP Report 和 IGMP Leave 消息，有效节约上游路由器和 AC6605 之间的带宽，缓解上游路由器的压力。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping proxy**，使能 IGMP Snooping Proxy 功能。

说明

开启 IGMP Snooping Proxy 功能后，交换机会定时以广播的方式向 VLAN 内所有接口发送 IGMP 查询报文，包括 VLAN 内的路由器接口，此时可能会引起 IGMP 查询器重新选举。如果组播网络中已经存在查询器，使用 **igmp-snooping proxy-uplink-port** 命令禁止向路由器接口发送 IGMP 查询报文。

在同一 VLAN 内，IGMP-Snooping Proxy 功能和 IGMP-Snooping Querier 功能不能同时配置。

----结束

（可选）配置接口下的二层组播数据过滤

背景信息

当网络管理员希望拒绝某特定的组播数据报文时，可以在 AC6605 端口上对来自某 VLAN 的 UDP 报文进行过滤。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 接口、Eth-Trunk 接口。

步骤 3 执行命令 **multicast-source-deny vlan** { *vlan-id1* [**to** *vlan-id2*] } & <1-10>，对端口下某 VLAN 的二层组播数据进行过滤。

----结束

检查配置结果

前提条件

已完成基于 VLAN 的 IGMP Snooping 配置。

操作步骤

- 使用命令 **display igmp-snooping configuration** 查看 IGMP Snooping 的配置信息。
- 使用命令 **display igmp-snooping** [**vlan** *vlan-id*]查看 VLAN 的 IGMP Snooping 配置信息。
- 使用命令 **display igmp-snooping statistics vlan** [*vlan-id*]查看 VLAN 的 IGMP Snooping 统计信息。
- 使用命令 **display igmp-snooping port-info** [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]查看组播组的成员接口信息。
- 使用命令 **display igmp-snooping router-port vlan** *vlan-id* 查看路由器接口信息。
- 使用命令 **display igmp-snooping querier vlan** [*vlan-id*]查看 IGMP Snooping 查询器使能信息。
- 使用命令 **display l2-multicast forwarding-table vlan** *vlan-id* [**source-address** *source-address* **group-address** | **group-address**]查看 VLAN 的组播转发表信息。

----结束

任务示例

说明

没有使能 VLAN 下的 IGMP Snooping 功能时，各项配置也可以进行，但是不能生效。执行 **display igmp-snooping** 命令也无效，即没有显示任何配置信息。

在配置成功时，执行 **display igmp-snooping** [**vlan** *vlan-id*]命令，应得到以下结果：

- VLAN 的 IGMP Snooping 功能应处于使能状态。
- 可以处理的 IGMP 报文的版本配置正确。
- VLAN 的组播策略应配置正确。
- VLAN 内的接口快速离开应配置正确。
- 路由器接口老化时间、最后成员查询时间间隔、通用查询时间间隔、最大响应时间、报文抑制时间和 IGMP 健壮系数配置正确。
- Router Alert 配置正确。

版权所有 © 华为技术有限公司

例如：

```
<Quidway> display igmp-snooping vlan 3
  IGMP Snooping Information for VLAN 3
    IGMP Snooping is Enabled
    IGMP Version is Set to default 2
    IGMP Query Interval is Set to default 125
    IGMP Max Response Interval is Set to default 10
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1
    IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
    IGMP Filter Group-Policy is Set to default : Permit All
    IGMP Prompt Leave Disable
    IGMP Router Alert is Not Required
    IGMP Send Router Alert Enable
    IGMP Proxy Enable
    IGMP Report Suppress Disable
    IGMP Suppress Time is set to default 10 seconds
    IGMP Router Port Learning Enable
    IGMP Querier Disable
    IGMP SSM-Mapping Disable
```

执行 **display igmp-snooping router-port vlan** *vlan-id* 命令，查看路由器接口信息。

```
<Quidway> display igmp-snooping router-port vlan 3
Port Name                 UpTime   Expires     Flags
-------------------------------------------------------------
VLAN 3, 2 router-port(s)
GE0/0/1                   1d:22h    00:01:20    DYNAMIC
GE0/0/2                   2d:10h    --          STATIC
```

执行 **display igmp-snooping port-info** [**vlan** *vlan-id*] [**group-address** *group-address*] [**verbose**]命令，查看成员接口信息。

```
<Quidway> display igmp-snooping port-info
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 101, 1 Entry(s)
                     (*, 225.0.0.1)  GE0/0/1                       -D-
                                              1 port(s)
 VLAN 102, 1 Entry(s)
                     (*, 225.0.0.1)  GE0/0/24                      -D-
                                              1 port(s)
 ----------------------------------------------------------------------
```

在使能查询器使能配置成功时，执行命令 **display igmp-snooping querier vlan** [*vlan-id*]，显示查询器使能正确。

```
<Quidway> display igmp-snooping querier vlan
VLAN                          Querier-state
-----------------------------------------------
3                              Enable
 total entry 1
```

执行命令 **display l2-multicast forwarding-table vlan** 7，查看 VLAN7 的组播转发表信息。

```
<Quidway> display l2-multicast forwarding-table vlan 7
VLAN ID : 7, Forwarding Mode : IP
------------------------------------------------------------------------
                      (Source, Group)     Interface            Out-Vlan
------------------------------------------------------------------------
               (1.1.1.1, 232.1.1.1)     GigabitEthernet0/0/1          7
------------------------------------------------------------------------
Total Group(s) : 1
```


版权所有 © 华为技术有限公司

6.2.4 配置静态组播 MAC 地址

介绍配置组播静态 MAC 地址的方法。

应用环境

二层交换机在接收到一个目的 MAC 地址为非 IP 组播 MAC 地址的数据帧时，在以前学习的 MAC 地址表中就不会找到对应的表项，交换机就会采用广播方式把组播报文在 VLAN 内进行广播，这样一来不但会造成带宽的极大浪费，而且影响网络安全。

可以通过在接口配置组播静态 MAC 地址，该组播报文只会向配置了该组播 MAC 地址的端口转发。

前置任务

在配置静态组播 MAC 地址之前，需要完成以下任务：

- 配置静态组播 MAC 的接口所属 VLAN 已经创建，并且接口已经加入到 VLAN。

数据准备

在配置静态组播 MAC 地址之前，需要准备以下数据。

序号	数据
1	需要配置静态组播 MAC 地址的接口编号
2	接口所属的 VLAN 的编号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 通过以下两种方式配置静态组播 MAC 地址：

- 在单个接口上配置静态组播 MAC 地址。
  1. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 GE 接口、Eth-Trunk 接口。
  2. 执行命令 **mac-address multicast** *mac-address* **vlan** *vlan-id*，在接口上配置静态组播 MAC 地址。
- 将静态组播 MAC 地址批量配置到多个接口上。

  执行命令 **mac-address multicast** *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1－10> **vlan** *vlan-id*，静态组播 MAC 地址批量配置到多个接口上。

  接口编号必须连续，而且不允许跨板，*interface-number2* 必须大于 *interface-number1*。

配置完静态组播 MAC 地址之后，对应组播 MAC 地址的报文只向配置此组播 MAC 的接口转发。

配置静态组播 MAC 地址时，请注意以下事项：

- VLAN 已经创建，并且配置静态组播 MAC 地址接口已经加入 VLAN。

版权所有 © 华为技术有限公司

- MAC 地址必须为组播 MAC 地址，即首字节 01 开头。
- 不允许配置为 IP 组播 MAC 地址，即 0100-5E00-0000 ～ 0100-5E00-7FFF（IPv4 组播地址）和 3333-xxxx-xxxx（IPv6 组播地址）。
- VLAN 不能是 Super VLAN、专线 VLAN、SEP 和 RRPP 的控制 VLAN。

----结束

检查配置结果

- 使用命令 **display mac-address multicast** [*mac-address*] [**vlan** *vlan-id*]查看当前配置的静态组播 MAC 表项信息。
- 使用命令 **display mac-address multicast** [**vlan** *vlan-id*] **total-number** 查看系统当前配置的静态组播 MAC 表项数量。

查看 VLAN 10 中的配置的组播 MAC 地址表项。

```
<Quidway> display mac-address multicast vlan 10
-------------------------------------------------------------------------
 MAC Address          VLANID         Out-Interface
-------------------------------------------------------------------------
 0111-1111-2222       10             GigabitEthernet0/0/1
                                     GigabitEthernet0/0/2
                                            2 port(s)
-------------------------------------------------------------------------
 Total Group(s) : 1
```

查看 VLAN 10 中的配置的组播 MAC 地址表项数目。

```
<Quidway> display mac-address multicast vlan 10 total-number
Total number of mac-address : 3
```

6.2.5 配置二层组播 SSM Mapping 功能

介绍二层组播 SSM Mapping 功能的配置方法。

建立配置任务

应用环境

当与用户相连的交换机配置组地址与源地址的映射使能了 IGMPv3 版本，在需要将 SSM 组策略范围外的组播地址映射到指定的组播源时，就要配置 SSM Mapping 功能。

当使能了 IGMPv3 版本的交换机收到 SSM 组地址范围内的 IGMPv2 报文，需要自动映射到指定的源时，也需配置 SSM Mapping 功能。

前置任务

在配置组播 SSM Mapping 功能之前，需完成以下任务：

- 全局使能 IGMP Snooping 功能。

数据准备

在配置组播 SSM Mapping 功能之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	（可选）ACL 规则
2	（可选）SSM 组策略
3	建立映射组播地址

（可选）配置 SSM 组策略

背景信息

如果用户加入的组播组地址为 ASM 型，需要先在 VLAN 上配置 SSM 组策略，将组播组地址加入到 SSM 组地址范围。

说明

创建 SSM 策略的 ACL 时，rule 命令必须使用参数 permit 并指定组播地址才能生效。如果配置参数 deny 或指定的地址不是组播地址，配置不生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping ssm-policy** *basic-acl-number*,配置 SSM 组策略。

缺省情况下，SSM 组范围是 232.0.0.0 ～ 232.255.255.255。执行本命令配置 SSM 策略后，该策略允许的组都将作为 SSM 范围内的组对待。

----结束

（可选）配置二层组播 SSM Mapping

背景信息

配置 SSM Mapping 功能，可以使组播组与组播源之间能够建立一一对应的映射关系。

使能全局及 VLAN 的 IGMP Snooping 功能，并配置 VLAN 内 IGMP Snooping 的版本为 3，才能支持 SSM Mapping 功能。

如果配置了组播 VLAN 复制功能，只需在组播 VLAN 内配置 SSM Mapping 即可。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping version 3**，配置 VLAN 内 IGMP Snooping 的版本号为 3。

默认版本号为 2，但是 IGMPv2 版本不支持 SSM Mapping 功能。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **igmp-snooping ssm-mapping enable**，使能 VLAN 内的 SSM Mapping 功能。

缺省情况下，组播 SSM Mapping 功能未使能。

步骤 5 执行命令 **igmp-snooping ssm-mapping** *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*，配置指定范围内组播组地址与源地址映射。

指定范围的组播组地址为 SSM Policy 范围内的组播组地址。SSM Policy 配置方法请参见**（可选）配置 SSM 组策略**。

----结束

检查配置结果

前提条件

已完成组播 SSM Mapping 功能的全部配置。

操作步骤

- 使用 **display igmp-snooping port-info** 命令查看端口表项信息。

----结束

任务示例

执行命令 **display igmp-snooping port-info**，可以查看对应的端口表项信息。例如：

```
<Quidway> display igmp-snooping port-info vlan 10
------------------------------------------------------------------------------
                   (Source, Group)  Port                            Flag
 Flag: S:Static     D:Dynamic     M: Ssm-mapping
------------------------------------------------------------------------------
VLAN 10, 3 Entry(s)
                    (*, 225.1.1.1)  GE0/0/2                         --M
                                                1 port(s)
                    (*, 225.1.1.2)  GE0/0/2                         --M
                                                1 port(s)
                    (*, 225.1.1.3)  GE0/0/2                         --M
                                                1 port(s)
------------------------------------------------------------------------------
```

6.2.6 维护

清除 IGMP Snooping 的统计数据，调试 IGMP Snooping。

清除组播转发表中的静态表项

背景信息

注意

静态表项被清除后无法自动恢复，直到再次被配置。确认需要清除组播转发表中的静态表项后，再执行以下命令。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 接口、Eth-Trunk 接口。

步骤 3 执行命令 **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1-10> } 取消接口静态加入组播组的配置。也可以通过命令 **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id* 批量取消接口上加入的组播组地址。

----结束

清除组播转发表项

背景信息

注意

执行本命令会引起该 VLAN 内的主机接收某些组播流暂时性中断，直到主机再次发出 IGMP 成员报告消息，AC6605 重新生成转发表项后，主机才能再收到组播流。

操作步骤

- 在用户视图下使用命令 **reset igmp-snooping group** { **all** | **vlan** { *vlan-id* | **all** } }清除组播转发表中的动态转发表项。

  说明

  执行本命令不清除静态转发表项和动态路由器端口表项。

----结束

清除 IGMP Snooping 统计信息

背景信息

注意

清除 IGMP Snooping 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

- 在用户视图下使用命令 **reset igmp-snooping statistics** { **all** | **vlan** { *vlan-id* | **all** } }清除 IGMP Snooping 统计信息。

----结束

调试 IGMP Snooping

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging igmp-snooping all** 命令关闭所有调试开关。

操作步骤

- 在用户视图下，使用命令 **debugging igmp-snooping** { **all** | **aps** | **event** | **fwd** | **general** | **leave** [*basic-acl-number*] | **mvlan** | **packet** [*advance-acl-number*] | **query** [*advance-acl-number*] | **report** [*advance-acl-number*] | **syn** | **timer** }打开 IGMP Snooping 的调试信息开关。

----结束

6.2.7 配置举例

介绍二层组播的配置举例。

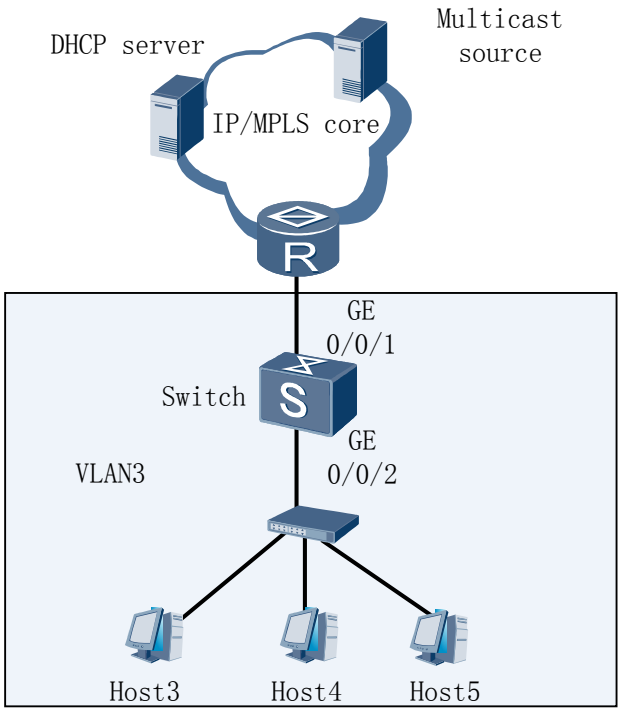
配置 IGMP Snooping 示例

组网需求

如图 6-3 所示，Switch 的 GE0/0/1 连接组播源侧路由器，GE0/0/2 接口连接用户主机，要求通过配置 IGMP Snooping 功能实现 VLAN3 中的三台主机能长期接收组地址为 225.1.1.1 ～ 225.1.1.3 的组播数据。

版权所有 © 华为技术有限公司

图 6-3 配置基于 VLAN 的 IGMP Snooping 组网图



配置思路

采用如下的思路配置 VLAN 中 IGMP Snooping 的功能：

1. 创建 VLAN 并将接口加入 VLAN。
2. 使能全局和 VLAN 的 IGMP Snooping 功能。
3. 配置静态路由器接口。
4. 配置静态组播组 225.1.1.1 ～ 225.1.1.3。

数据准备

为完成此配置举例，需要准备以下数据：

- GE0/0/2 和 GE0/0/1 对应 VLAN 编号为 3。
- 静态路由器接口为 GE0/0/1。
- 静态组播组地址为 225.1.1.1 ～ 225.1.1.3。

操作步骤

步骤 1 创建 VLAN，配置接口加入 VLAN。

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] quit
[Switch] interface gigabitethernet 0/0/1
[Switch - GigabitEthernet0/0/1] port hybrid tagged vlan 3
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[Switch-GigabitEthernet0/0/2] port hybrid tagged vlan 3
[Switch-GigabitEthernet0/0/2] quit
```

步骤 2 使能 IGMP Snooping 功能。

使能全局的 IGMP Snooping 功能。

```
[Switch] igmp-snooping enable
```

使能 VLAN3 的 IGMP Snooping 功能。

```
[Switch] vlan 3
[Switch-vlan3] igmp-snooping enable
[Switch-vlan3] quit
```

步骤 3 配置 GE0/0/1 为 VLAN3 的静态路由器接口。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 3
[Switch-GigabitEthernet0/0/1] quit
```

步骤 4 配置静态组播组。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.1 vlan 3
[Switch-GigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.2 vlan 3
[Switch-GigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.3 vlan 3
[Switch-GigabitEthernet0/0/2] quit
```

步骤 5 验证配置结果。

#查看 IGMP Snooping 非缺省配置信息。

```
[Switch] display igmp-snooping vlan configuration
IGMP Snooping Configuration for VLAN 3
     igmp-snooping enable
```

由显示信息可知，VLAN 的 IGMP Snooping 功能已使能。

验证静态路由器接口配置。

在 Switch 执行命令 **display igmp-snooping router-port vlan 3**。

```
[Switch] display igmp-snooping router-port vlan 3
 Port Name                 UpTime    Expires   Flags
 ----------------------------------------------------------------------
 VLAN 3, 1 router-port(s)
 GE0/0/1                   2d:10h    --        STATIC
```

由显示信息可知，接口 GE0/0/1 已被配置为静态路由器接口。

验证静态组播组的成员接口信息。

```
[Switch] display igmp-snooping port-info
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 3, 3 Entry(s)
                     (*, 225.1.1.1)  GE0/0/2                       S--
                                                 1 port(s)
                     (*, 225.1.1.2)  GE0/0/2                       S--
                                                 1 port(s)
                     (*, 225.1.1.3)  GE0/0/2                       S--
                                                 1 port(s)
 ----------------------------------------------------------------------
```

由显示信息可知，225.1.1.1 ～ 225.1.1.3 已被配置为静态表项。

查看组播转发表项。

版权所有 © 华为技术有限公司

```
[Switch] display l2-multicast forwarding-table vlan 3

VLAN ID : 3, Forwarding Mode : IP
------------------------------------------------------------------------
                    (Source, Group)    Interface             Out-Vlan
------------------------------------------------------------------------
                       Router-port     GigabitEthernet0/0/1          3
                     (*, 225.1.1.1)    GigabitEthernet0/0/1          3
                                       GigabitEthernet0/0/2          3
                     (*, 225.1.1.2)    GigabitEthernet0/0/1          3
                                       GigabitEthernet0/0/2          3
                     (*, 225.1.1.3)    GigabitEthernet0/0/1          3
                                       GigabitEthernet0/0/2          3
------------------------------------------------------------------------
Total Group(s) : 3
------------------------------------------------------------------------
```

由显示信息可知 225.1.1.1 ～ 225.1.1.3 的数据在转发表中对应的 VLAN 和端口。

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 3
#
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 3
 igmp-snooping static-router-port vlan 3
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 3
 l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 3
 #
 return
```

配置 IGMP Snooping 的 SSM Mapping 功能示例

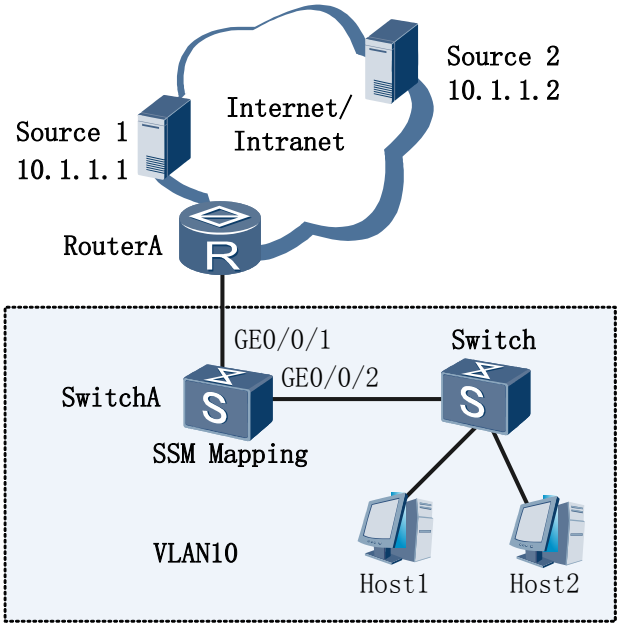
组网需求

如图 6-4 所示的组网中，Switch 和用户主机 Host1 和 Host2 运行的软件版本都为 IGMPv2，组播源侧最后一跳路由器 RouterA 运行 IGMPv3。SwitchA 为 AC6605 设备，SwitchA 的 GE0/0/1 接口连接 RouterA，GE0/0/2 接口与用户直连的交换机相连，加入 VLAN10。SwitchA 的 GE0/0/1 接口为静态路由器接口，成员接口 GE0/0/2 静态加入组播组地址 224.1.1.1。GE0/0/1 和 GE0/0/2 都加入同一 VLAN10，并且上层设备 RouterA 已部署 IGMP SSM Mapping 功能。

在 VLAN 内 SwitchA 上配置 IGMP Snooping 的 SSM Mapping 功能，与三层 IGMP SSM Mapping 对应一致，使组播组与组播源之间能够建立一一对应的映射关系，将 IGMPv1 或 IGMPv2 数据报文中所包含的（*,G）信息映射为(S,G)信息，实现用户 Host1 和 Host2 不升级主机，在当前运行的 IGMPv2 版本上指定组播源，点播相应的节目，为其提供 SSM 组播服务。

版权所有 © 华为技术有限公司

图 6-4 配置组播 SSM Mapping 功能组网图



配置思路

采用如下的思路配置 IGMP Snooping 的 SSM Mapping 功能：

1. 配置 IGMP Snooping 的基本功能，实现用户接收组播源数据。
2. 配置 IGMP Snooping 的 SSM 组策略，实现用户所在的 ASM 类型组播组地址加入到 SSM 组地址范围内。
3. 配置 IGMP Snooping 的 SSM Mapping 功能，实现用户接收指定组播源数据。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 的 GE0/0/1 接口、GE0/0/2 接口加入的 VLAN 编号 10。
- SwitchA 运行版本为 IGMPv3，Switch、Host1 和 Host2 运行版本为 IGMPv2。
- 指定组播源地址 10.1.1.2。

操作步骤

步骤 1 配置 VLAN

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤 2 使能全局和 VLAN 下 IGMP Snooping 功能

配置 SwitchA。

```
[SwitchA] igmp-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
```

步骤 3 SwitchA 运行 IGMP 版本号为 IGMPv3，用户主机运行 IGMP 版本号为 IGMPv2，且不允许将用户主机升级到 IGMPv3

配置 SwitchA。

```
[SwitchA-vlan10] igmp-snooping version 3
[SwitchA-vlan10] quit
```

步骤 4 VLAN10 内配置 GE0/0/1 接口为静态路由器接口

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤 5 配置 IGMP Snooping 的 SSM 组策略和 SSM Mapping 功能

```
[SwitchA] acl number 2008
[SwitchA-acl-basic-2008] rule 5 permit source 224.1.1.1 0
[SwitchA-acl-basic-2008] quit
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping ssm-policy 2008
[SwitchA-vlan10] igmp-snooping ssm-mapping enable
[SwitchA-vlan10] igmp-snooping ssm-mapping 224.1.1.1 24 10.1.1.2
[SwitchA-vlan10] quit
```

步骤 6 检查配置结果

在 SwitchA 上使用 **display igmp-snooping vlan configuration** 命令，查看 VLAN 内配置情况。

```
[SwitchA] display igmp-snooping vlan configuration
 IGMP Snooping Configuration for VLAN 10
     igmp-snooping enable
     igmp-snooping version 3
     igmp-snooping ssm-mapping enable
     igmp-snooping ssm-policy 2008
     igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
```

当 SwitchA 收到加入组播组 224.1.1.1 的 Report 报文时，执行 **display igmp-snooping port-info** 命令，查看端口信息。

```
[SwitchA] display igmp-snooping port-info
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 10, 1 Entry(s)
                     (10.1.1.2, 224.1.1.1)  GE0/0/2                --M
                                                    1 port(s)
 ----------------------------------------------------------------------
```

----结束

配置文件

- SwitchA 的配置文件

版权所有 © 华为技术有限公司

```
#
 sysname SwitchA
#
 vlan batch 10
#
 igmp-snooping enable
#
acl number 2008
 rule 5 permit source 224.1.1.1 0
#
vlan 10
 igmp-snooping enable
 igmp-snooping ssm-mapping enable
 igmp-snooping version 3
 igmp-snooping ssm-policy 2008
 igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping static-router-port vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

6.3 组播 VLAN 配置

介绍组播 VLAN 的配置方法、维护命令，并提供配置举例。

6.3.1 组播 VLAN 概述

组播 VLAN 复制功能可以使三层设备只需把组播数据传送给该组播 VLAN，而不必再为每个用户 VLAN 都复制一份组播报文，减少带宽浪费。

在传统的组播点播方式下，属于不同 VLAN 的用户分别进行同一组播源点播时，需要上游路由器为每个用户 VLAN 都复制一份组播数据，再将数据分别传送给各个 VLAN。这种方式既造成了网络带宽的浪费，又增加了上游设备的额外负担。

在配置了组播 VLAN 功能后，当属于不同 VLAN 的用户分别进行同一组播源的点播时，可以在交换机上将这些 VLAN 都配置为一个组播 VLAN 的用户 VLAN，上层路由器只需把组播数据传给组播 VLAN 即可，而不必再为每个 VLAN 都复制一份。交换机从上游路由器接收到组播报文时，会将其分发给该组播 VLAN 内那些有接收者的用户 VLAN。

6.3.2 AC6605 支持的组播 VLAN 特性

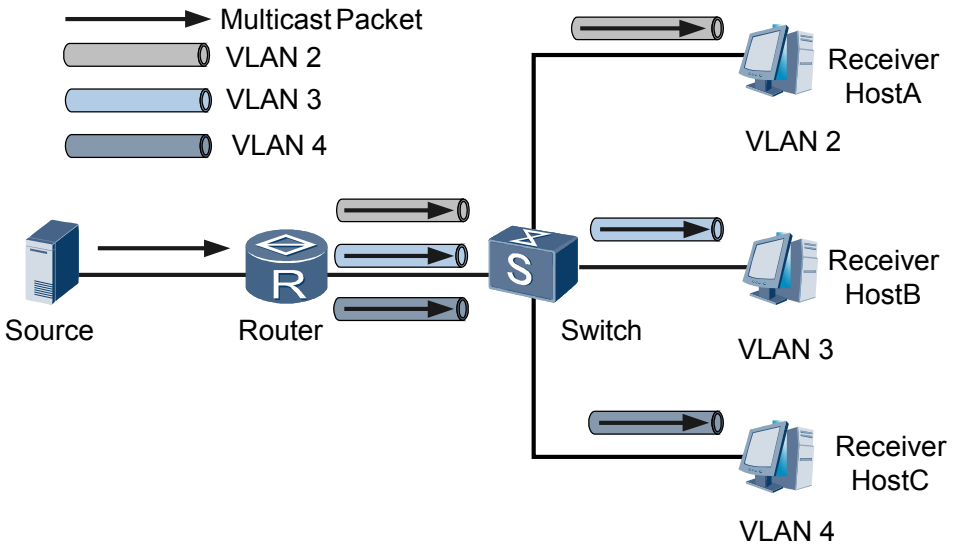
介绍组播 VLAN 复制特性在 AC6605 中的支持情况。

基于用户 VLAN 的组播 VLAN 复制

如图 6-5 所示，在传统的组播点播方式下，当属于不同 VLAN 的主机 ReceiverA、ReceiverB 和 ReceiverC 同时点播同一组播组时，三层设备（Router）需要把组播数据在每个用户 VLAN（即主机所属的 VLAN）内都复制一份发送给二层设备（Switch）。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

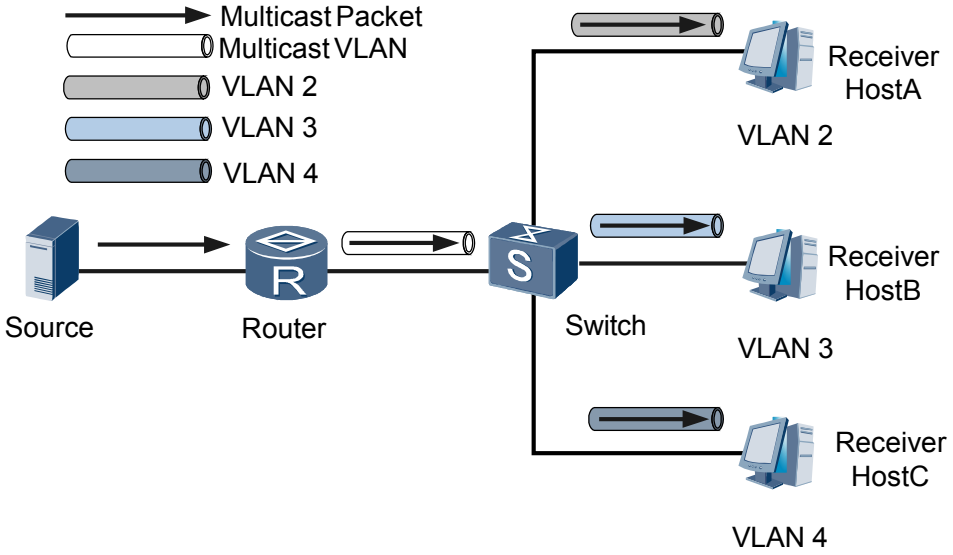
版权所有 © 华为技术有限公司

图 6-5 未运行组播 VLAN 时的组播数据传输



可以使用组播 VLAN 功能解决这个问题。图 6-6 所示，在二层设备上配置了组播 VLAN 后，三层设备（Router）只需把组播数据在组播 VLAN 内复制一份发送给二层设备（Switch），而不必在每个用户 VLAN 内都复制一份，从而节省了网络带宽，也减轻了三层设备的负担。

图 6-6 运行组播 VLAN 时的组播数据传输



组播 VLAN 复制支持以下 2 种方式：

- 组播 VLAN 与用户 VLAN 一对多
- 组播 VLAN 与用户 VLAN 多对多

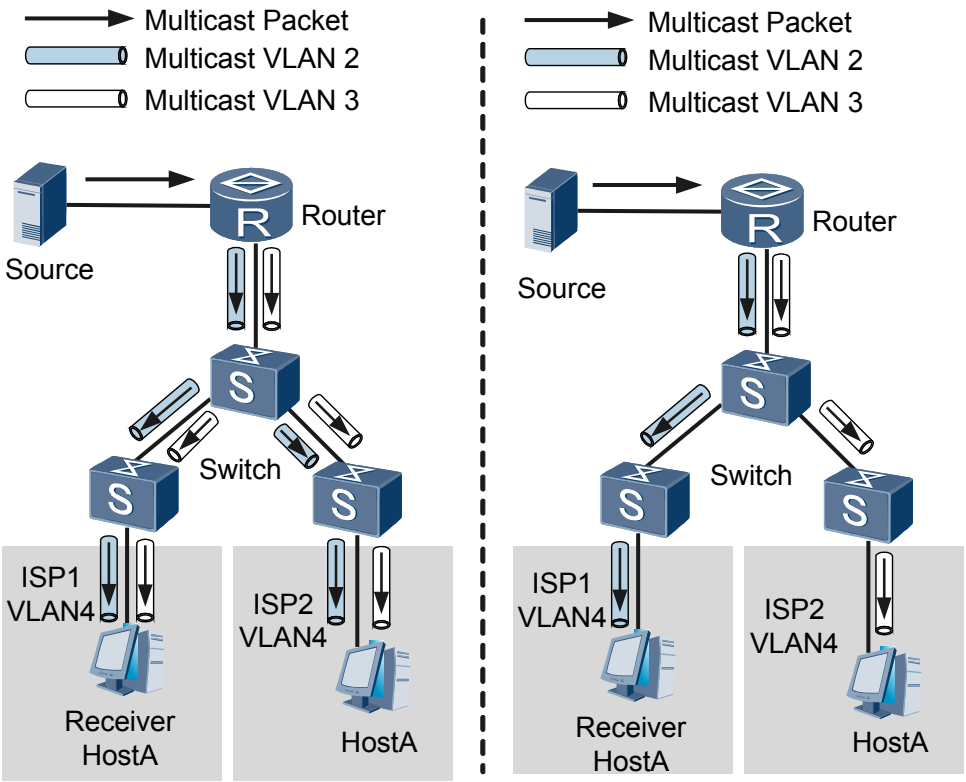
基于接口的组播 VLAN 复制

如果网络中的组播业务批发给了多个 ISP，为每个 ISP 分配了一个组播 VLAN 来实现组播数据和组播路由的隔离。由于将不同接口下用户的组播业务批发给了不同的 ISP，这

版权所有 © 华为技术有限公司

样就可能存在不同接口下的用户 VLAN 相同，如果只配组播 VLAN，这样一个 ISP 的组播报文会发送到不属于此 ISP的用户，影响到 ISP 的利益，此时可以通过在端口下绑定用户 VLAN 与组播 VLAN 来解决此问题。如图 6-7 所示，在接口下对组播 VLAN 和用户 VLAN 进行绑定，组播 VLAN 只把组播报文复制到指定接口下的用户 VLAN。

图 6-7 配置基于接口的组播 VLAN 复制前后对比



6.3.3 配置基于用户 VLAN 的组播 VLAN 复制

介绍配置基于用户 VLAN 的组播 VLAN 复制功能的方法。

建立配置任务

应用环境

在传统的组播点播方式下，属于不同 VLAN 的用户分别进行同一组播源点播时，需要上游路由器为每个用户 VLAN 都复制一份组播数据。这种方式既造成了网络带宽的浪费，又增加了上游设备的额外负担。

通过组播 VLAN 复制功能，可以对组播源和组播组成员进行管理和控制，实现不同 VLAN 内的用户接收相同的组播流，同时也可以减少带宽浪费。

组播 VLAN 复制功能中的 VLAN 分为组播 VLAN 和用户 VLAN。组播 VLAN 是 AC6605 与组播源相连的接口所属的 VLAN，用于实现组播流的汇聚；用户 VLAN 是与组播组成员主机相连的接口所属的 VLAN，用于接收组播 VLAN 的数据流。

版权所有 © 华为技术有限公司

前置任务

在配置组播 VLAN 复制之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 使能全局视图下的 IGMP Snooping 功能。

数据准备

在配置组播 VLAN 复制功能之前，需要准备以下数据。

序号	数据
1	组播 VLAN 的编号
2	用户 VLAN 的编号
3	接口的类型和编号

配置基于用户 VLAN 的组播 VLAN 复制

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping enable**，使能 VLAN 的 IGMP Snooping 功能。

步骤 4 执行命令 **multicast-vlan enable**，使能组播 VLAN 复制功能，并将当前 VLAN 配置为组播 VLAN。

缺省情况下，组播 VLAN 复制功能处于禁止状态。

在已使能了 IP 组播路由的设备上不允许再配置组播 VLAN。

步骤 5 执行命令 **multicast-vlan user-vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }，配置组播 VLAN 和用户 VLAN 的对应关系。

参数 *vlan-id1* 和 *vlan-id2* 为用户 VLAN 的编号。*vlan-id2* 应该大于 *vlan-id1*。

说明

配置用户 VLAN 和组播 VLAN 对应关系时，需要先创建此用户 VLAN，并且用户 VLAN 已经使能 IGMP Snooping。用户 VLAN 不能是组播 VLAN 或其它组播 VLAN 的用户 VLAN。

----结束

配置接口加入 VLAN

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行以下操作，将网络侧接口加入组播 VLAN。

1. 执行命令 **interface** *interface-type interface-number*，进入网络侧接口视图。
2. 将网络侧接口加入以 Trunk 方式或 hybrid 方式加入组播 VLAN。详细配置过程请参见**基于端口划分 VLAN**。
3. 执行命令 **quit**，返回系统试图。

步骤 3 执行以下操作，将用户侧接口加入用户 VLAN。

1. 执行命令 **interface** *interface-type interface-number*，进入用户侧接口视图。
2. 将用户侧接口以 Trunk 方式或 hybrid 方式加入用户 VLAN。详细配置过程请参见**基于端口划分 VLAN**。

----结束

检查配置结果

前提条件

已经完成组播 VLAN 复制功能的配置。

操作步骤

- 使用命令 **display multicast-vlan vlan** [*vlan-id*]查看组播 VLAN 的信息。

----结束

任务示例

执行命令 **display multicast-vlan vlan** [*vlan-id*]，可以看到组播 VLAN 信息。

```
<Quidway> display multicast-vlan vlan 3
 Multicast-vlan         : 3
 User-vlan Number       : 2
 IGMP snooping state    : Enable
 MLD  snooping state    : Disable
 User-vlan              Snooping-state
 ------------------------------------------------
 100                    IGMP Enable /MLD Disable
 200                    IGMP Enable /MLD Disable
```

执行命令 **display user-vlan vlan** [*vlan-id*]，可以看到用户 VLAN 信息。

```
<Quidway> display user-vlan vlan
 Total user vlan   2
 user-vlan  snooping-state            multicast-vlan   snooping-state
 ------------------------------------------------------------
 100        IGMP Enable /MLD Disable   3               IGMP Enable /MLD Disable
 200        IGMP Enable /MLD Disable   3               IGMP Enable /MLD Disable
```

6.3.4 配置基于接口的组播 VLAN 复制

配置基于接口的组播 VLAN 复制功能。

建立配置任务

版权所有 © 华为技术有限公司

应用环境

如果网络中的组播业务批发给了多个 ISP，为每个 ISP 分配了一个组播 VLAN 来实现组播数据和组播路由的隔离。由于将不同接口下用户的组播业务批发给了不同的 ISP，这样就可能存在不同接口下的用户 VLAN 相同，如果只配组播 VLAN，这样一个 ISP 的组播报文会发送到不属于此 ISP 的用户，影响到 ISP 的利益，此时可以通过在端口下绑定用户 VLAN 与组播 VLAN 来解决此问题，组播 VLAN 只把组播报文复制到指定接口下的用户 VLAN。

前置任务

在配置基于端口的组播 VLAN 复制之前，需要完成以下任务：

- 连接 Switch 接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 使能全局视图下的 IGMP Snooping 功能。

数据准备

在配置基于端口的组播 VLAN 复制功能之前，需要准备以下数据。

序号	数据
1	组播 VLAN 的编号
2	用户 VLAN 的编号
3	接口的类型和编号

创建组播 VLAN

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping enable**，使能 VLAN 的 IGMP Snooping 功能。

----结束

配置接口下绑定组播 VLAN 与用户 VLAN

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **l2-multicast-bind vlan** *vlanid1* [**to** *vlanid2*] **mvlan** *mvlanid*，在端口下绑定组播 VLAN 与用户 VLAN。

需要在用户侧接口绑定组播 VLAN 和用户 VLAN。

版权所有 © 华为技术有限公司

需要先创建用户 VLAN，且不能是组播 VLAN 或其它组播 VLAN 的用户 VLAN。

----结束

配置接口加入 VLAN

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行以下操作，将网络侧接口加入组播 VLAN。

1. 执行命令 **interface** *interface-type interface-number*，进入网络侧接口视图。
2. 将网络侧接口加入以 Trunk 方式或 hybrid 方式加入组播 VLAN。详细配置过程请参见**基于端口划分 VLAN**。
3. 执行命令 **quit**，返回系统试图。

步骤 3 执行以下操作，将用户侧接口加入用户 VLAN。

1. 执行命令 **interface** *interface-type interface-number*，进入用户侧接口视图。
2. 将用户侧接口以 Trunk 方式或 hybrid 方式加入用户 VLAN。详细配置过程请参见**基于端口划分 VLAN**。

----结束

检查配置结果

操作步骤

- 使用命令 **display l2-multicast-bind** [**mvlan** *vlan-id*]查看组播 VLAN 与端口的绑定信息。

----结束

任务示例

执行命令 **display l2-multicast-bind** [**mvlan** *vlan-id*]，可以看到组播 VLAN 信息。例如：

```
<Quidway> display l2-multicast-bind mvlan 90
  Port                          Startvlan      Endvlan        Mvlan
 ------------------------------------------------------------------
  GigabitEthernet0/0/1          901            --             90
Total Table(s) : 1
```

6.3.5 配置组播 VLAN 多对多

介绍组播 VLAN 多对多配置方法。

建立配置任务

版权所有 © 华为技术有限公司

应用环境

配置组播 VLAN 多对一后，一个用户 VLAN 只能加入一个组播 VLAN，只能加入一个组播 VLAN 的组播组，用户则无法再加入其它组播组接收其它组播 VLAN 的节目。为了解决此问题，可以配置组播 VLAN 多对多功能，将用户 VLAN 加入多个组播 VLAN，为用户指定可以接受的组播组数据。

当一个用户 VLAN 需要对应多个组播 VLAN 时，需要配置组播流触发机制，即在组播 VLAN 中配置静态流，并在用户 VLAN 中使能静态流触发机制。

前置任务

在配置组播 VLAN 多对多之前，需要完成以下任务：

- 连接 Switch 接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 接口已经加入组播 VLAN 和用户 VLAN。

数据准备

在配置组播 VLAN 多对多之前，需要准备以下数据。

序号	数据
1	组播 VLAN 的编号
2	用户 VLAN 的编号
3	接口的类型和编号
4	组播 VLAN 的静态流组播组地址

使能用户 VLAN 组播流触发功能

前提条件

只有在用户 VLAN 使能了组播流触发机制，一个用户 VLAN 才能对应多个组播 VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **igmp-snooping enable**，使能全局的 IGMP Snooping 功能。

步骤 3 执行命令 **vlan** *vlan-id*，创建用户 VLAN 并进入 VLAN 视图。

步骤 4 执行命令 **igmp-snooping enable**，使能用户 VLAN 的 IGMP Snooping 功能。

步骤 5 执行命令 **multicast flow-trigger enable**，VLAN 内使能组播流触发。

此命令只能在用户 VLAN 下配置。

----结束

版权所有 © 华为技术有限公司

配置用户 VLAN 加入多个组播 VLAN

前提条件

如果用户 VLAN 下的用户需接收多个组播 VLAN 下的组播数据，则可以重复执行以下步骤，将用户 VLAN 加入到多个组播 VLAN。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping enable**，使能 VLAN 的 IGMP Snooping 功能。

步骤 4 执行命令 **multicast-vlan enable**，使能组播 VLAN 复制功能，并将当前 VLAN 配置为组播 VLAN。

在已使能了 IP 组播路由的设备上不允许再配置组播 VLAN。

步骤 5 执行命令 **multicast-vlan user-vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }，配置用户 VLAN 加入指定组播 VLAN。

用户 VLAN 加入多个组播 VLAN 之前，需要先在用户 VLAN 内用 **multicast flow-trigger enable** 命令使能组播流触发功能。

----结束

配置组播 VLAN 静态流

背景信息

当某个用户 VLAN（如 UVLAN）要求加入多个组播 VLAN（MVLAN1 ～ MVLANn）时，先要在 UVLAN 上通过 **multicast flow-trigger enable** 命令使能流触发，然后在 UVLAN 需要加入的各个 MVLAN 上配置静态流。这样就在 UVLAN 和 MVLAN 之间建立了基于（UVLAN，Source，Group）的映射关系，在 UVLAN 向该 MVLAN 发起点播请求时生成组播表项，实现 UVLAN 和 MVLAN 的多对多映射。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入组播 VLAN 视图。

只能在组播 VLAN 面配置组播静态流。

步骤 3 执行命令 **multicast static-flow** { *ipv4-group-address* [**source** *ipv4 -source-address*] | **ipv6** *ipv6-group-address* [**source** *ipv6 -source-address*] }，配置组播 VLAN 静态流。

配置组播静态流之后，用户 VLAN 下的用户可以加入组播静态流指定的组播组，并接收其组播数据。

说明

所有组播 VLAN 的静态流不能重复，组播组相同但源 IP 不同的两条流也视为不重复。

----结束

版权所有 © 华为技术有限公司

检查配置结果

操作步骤

- 使用命令 **display multicast static-flow** [**mvlan** *vlan-id*]查看组播 VLAN 下配置的静态流。

----结束

任务示例

执行命令 **display multicast static-flow** [**mvlan** *vlan-id*]，可以查看组播 VLAN 下配置的静态流。

```
<Quidway> display multicast static-flow
 ------------------------------------------------------------------------
 Vlan                                          (Source, Group)
 ------------------------------------------------------------------------
  10                                           (*, 225.1.1.1)
 ------------------------------------------------------------------------
 Total Table(s) : 1
```

6.3.6 配置举例

介绍组播 VLAN 复制功能的配置举例。

配置基于用户 VLAN 的组播 VLAN 复制示例

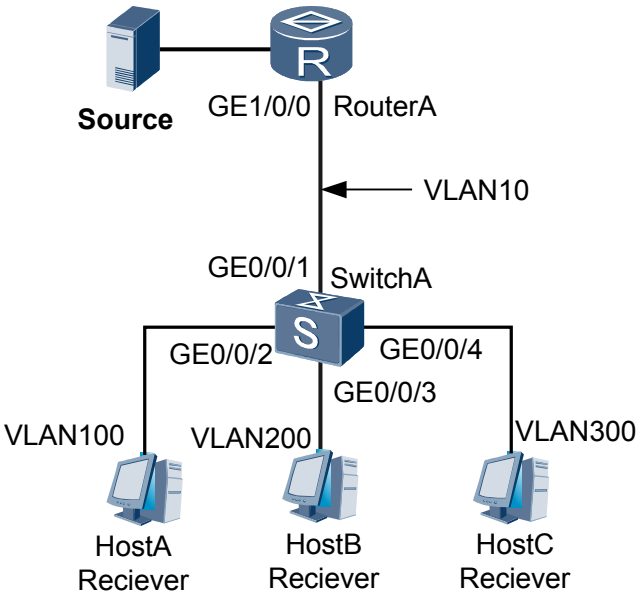
组网需求

如图 6-8 所示，RouterA 与组播源相连，通过 GE1/0/0 接口和 SwitchA 的 GE0/0/1 接口相连。SwitchA 的 GE0/0/1 属于 VLAN10。用户主机 HostA、HostB 和 HostC 连接到 SwitchA 的 GE0/0/2、GE0/0/3 和 GE0/0/4 接口，并分别属于 VLAN100、VLAN200 和 VLAN300。

要求通过配置基于用户 VLAN 的组播 VLAN，使 RouterA 通过组播 VLAN 向 SwitchA 下分属不同用户 VLAN 的主机分发组播数据。

版权所有 © 华为技术有限公司

图 6-8 配置基于用户 VLAN 的组播 VLAN 复制功能组网图



配置思路

采用如下的思路配置基于用户 VLAN 的组播 VLAN 复制：

1. 在系统视图下使能 IGMP Snooping。
2. 创建组播 VLAN，并在组播 VLAN 下使能 IGMP Snooping。
3. 创建用户 VLAN，并在用户 VLAN 下使能 IGMP Snooping。
4. 在组播 VLAN 下面绑定用户 VLAN。
5. 将接口分别以 Hybrid 方式加入 VLAN。

数据准备

为完成此配置举例，需要准备以下数据：

- 和路由器相连的接口及所属的 VLAN
- 用户接口及所属的 VLAN

操作步骤

步骤 1 在系统视图下使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
```

步骤 2 创建组播 VLAN，并在组播 VLAN 下使能 IGMP Snooping 功能。

```
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] multicast-vlan enable
[SwitchA-vlan10] quit
```

步骤 3 创建用户 VLAN，并在组播 VLAN 下使能 IGMP Snooping 功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] igmp-snooping enable
```


版权所有 © 华为技术有限公司

```
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] igmp-snooping enable
[SwitchA-vlan200] quit
[SwitchA] vlan 300
[SwitchA-vlan300] igmp-snooping enable
[SwitchA-vlan300] quit
```

步骤 4 在组播 VLAN 10 下面绑定用户 VLAN 100、VLAN 200 和 VLAN 300。

```
[SwitchA] vlan 10
[SwitchA-vlan10] multicast-vlan user-vlan 100 200 300
[SwitchA-vlan10] quit
```

步骤 5 把接口以 Hybrid 方式加入 VLAN。

把 GE0/0/1 接口加入组播 VLAN 10。

```
[SwitchA] interface gigabitethernet0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

把 GE0/0/2、GE0/0/3、GE0/0/4 接口分别加入用户 VLAN 100、VLAN 200、VLAN 300。

```
[SwitchA] interface gigabitethernet0/0/2
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 100
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet0/0/3
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 200
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 200
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet0/0/4
[SwitchA-GigabitEthernet0/0/4] port hybrid pvid vlan 300
[SwitchA-GigabitEthernet0/0/4] port hybrid untagged vlan 300
[SwitchA-GigabitEthernet0/0/4] quit
```

步骤 6 验证配置结果，在 SwitchA 可以查看到组播 VLAN 和用户 VLAN 的信息。

```
[SwitchA] display multicast-vlan vlan
Total multicast vlan   1
 multicast-vlan     user-vlan number     snooping-state
 ------------------------------------------------------------------
 10                 3                    IGMP Enable /MLD Disable
[SwitchA] display user-vlan vlan
 Total user vlan   3
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 200        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 300        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 100 200 300
#
 igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 multicast-vlan enable
```


版权所有 © 华为技术有限公司

```
 multicast-vlan user-vlan 100 200 300
#
vlan 100
 igmp-snooping enable
#
vlan 200
 igmp-snooping enable
#
vlan 300
 igmp-snooping enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
return
```

配置基于接口的组播 VLAN 复制示例

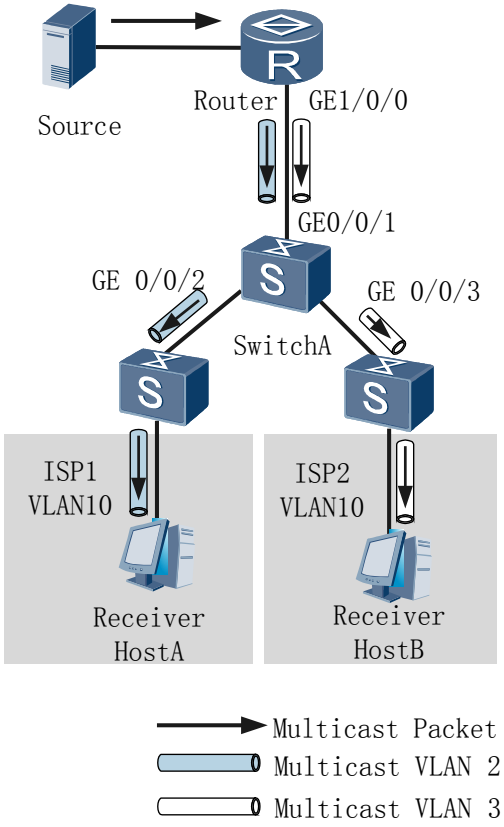
组网需求

在如图 6-9 所示的网络中，SwitchA 上的 GE0/0/1 接口连接路由器，GE0/0/2 和 GE0/0/3 接口下的业务分别批发给 ISP1 和 ISP2，ISP1 和 ISP2 分别通过组播 VLAN 2 和组播 VLAN 3 接收组播数据。GE0/0/2 和 GE0/0/3 接口下用户 VLAN 重复，都为 VLAN 10。

为了防止不同 ISP 的组播报文会发送到不属于此 ISP 的用户，影响到 ISP 的利益，在接口下绑定用户 VLAN 与组播 VLAN 来解决此问题，指定属于本 ISP 的组播数据只转发到连接本 ISP 用户的接口。

版权所有 © 华为技术有限公司

图 6-9 配置基于接口的组播 VLAN 复制组网图



配置思路

采用如下的思路配置基于接口组播 VLAN 复制：

1. 在系统视图下使能 IGMP Snooping 功能。
2. 创建组播 VLAN 2 和组播 VLAN 3，并在组播 VLAN 下使能 IGMP Snooping。
3. 创建用户 VLAN 10。
4. 在 GE0/0/2 接口和 GE0/0/3 接口下对组播 VLAN 和用户 VLAN 分别进行绑定。
5. 将接口分别以 Hybrid 方式加入 VLAN。

数据准备

为完成此配置举例，需要准备以下数据：

- 和路由器相连的接口及所属的 VLAN
- 用户接口及所属的 VLAN

操作步骤

步骤 1 配置组播 VLAN 2 和组播 VLAN 3，并在组播 VLAN 下使能 IGMP Snooping 功能。

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
[SwitchA] vlan 2
```


版权所有 © 华为技术有限公司

```
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] igmp-snooping enable
[SwitchA-vlan3] quit
```

步骤 2 创建用户 VLAN 10。

```
[Switch] vlan batch 10
```

步骤 3 在 GE0/0/2 接口和 GE0/0/3 接口下分别对组播 VLAN 和用户 VLAN 进行绑定。

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] l2-multicast-bind vlan 10 mvlan 2
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] l2-multicast-bind vlan 10 mvlan 3
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤 4 将 GE0/0/1 接口加入组播 VLAN，将 GE0/0/2 和 GE0/0/3 加入用户 VLAN。

以 Trunk 方式把 GE0/0/1 加入组播 VLAN 2 和组播 VLAN 3。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 3
[SwitchA-GigabitEthernet0/0/1] quit
```

把 GE0/0/2、GE0/0/3 接口分别以 Hybrid 方式加入用户 VLAN 10。

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤 5 验证配置结果。

在 SwitchA 上是使用 **display l2-multicast-bind** [**mvlan** *vlan-id*]命令查看接口下用户 VLAN 与组播 VLAN 的绑定信息。

```
[SwitchA] display l2-multicast-bind
------------------------------------------------------------------------
Port                          Startvlan        Endvlan        Mvlan
------------------------------------------------------------------------
GigabitEthernet0/0/2                    10             --            2
GigabitEthernet0/0/3                    10             --            3
------------------------------------------------------------------------
Total Table(s) : 2
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname Switch
#
 vlan batch 2 3 10
#
 igmp-snooping enable
#
vlan 2
 igmp-snooping enable
#
vlan 3
```


版权所有 © 华为技术有限公司

```
 igmp-snooping enable
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 2
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 3
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 3
#
return
```

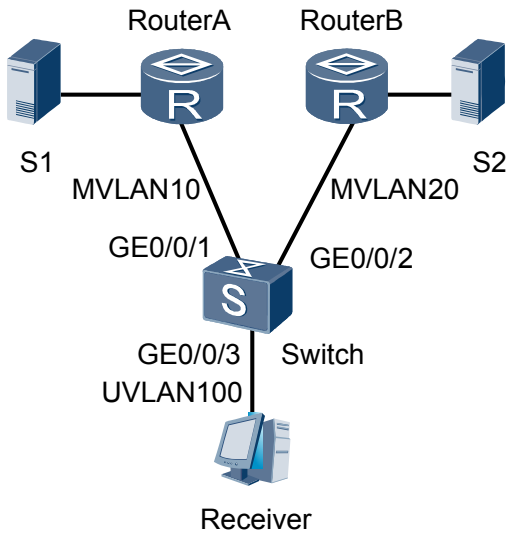
配置组播 VLAN 多对多示例

组网需求

如图 6-10 所示，交换机 Switch 通过 GE0/0/1 接口和 RouterA 相连，通过组播 VLAN 10 接收来自 RouterA 的组播数据；通过 GE0/0/2 接口和 RouterB 相连，通过组播 VLAN 20 接口接收来自 RouterB 的组播数据；通过 GE0/0/3 连接用户。

要求用户即能够接收来自 RouterA 的组播组 225.1.1.1 的数据，又能够接收来自 RouterB 的组播组 225.1.2.1 的数据。

图 6-10 配置基于用户 VLAN 的组播 VLAN 复制功能组网图



配置思路

采用如下的思路配置组播 VLAN 多对多：

1. 在系统视图下使能 IGMP Snooping。
2. 创建组播 VLAN，并在组播 VLAN 下使能 IGMP Snooping。

版权所有 © 华为技术有限公司

3. 创建用户 VLAN，并在用户 VLAN 下使能 IGMP Snooping，并在用户 VLAN 下使能组播流触发功能。
4. 用户 VLAN 加入多个组播 VLAN，并且在组播 VLAN 下配置静态组播流。
5. 将接口分别以 Hybrid 方式加入 VLAN。

数据准备

为完成此配置举例，需要准备以下数据：

- 和路由器相连的接口及所属的组播 VLAN
- 用户接口及所属的用户 VLAN

操作步骤

步骤 1 在系统视图下使能 IGMP Snooping。

```
<Switch> system-view
[Switch] igmp-snooping enable
```

步骤 2 创建组播 VLAN 10 和组播 VLAN 20，并在组播 VLAN 下使能 IGMP Snooping 功能。

```
[Switch] igmp-snooping enable
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] multicast-vlan enable
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] igmp-snooping enable
[Switch-vlan20] multicast-vlan enable
[Switch-vlan20] quit
```

步骤 3 创建用户 VLAN 100，在用户 VLAN 下使能 IGMP Snooping 功能,并在用户 VLAN 下使能组播流触发功能。

```
[Switch] vlan 100
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] multicast flow-trigger enable
[Switch-vlan100] quit
```

步骤 4 用户 VLAN 100 加入组播 10 和组播 VLAN 20，并且在组播 VLAN 下配置静态组播流。

```
[Switch] vlan 10
[Switch-vlan10] multicast-vlan user-vlan 100
[Switch-vlan10] multicast static-flow 225.1.1.1
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] multicast-vlan user-vlan 100
[Switch-vlan20] multicast static-flow 225.1.2.1
[Switch-vlan20] quit
```

步骤 5 把接口以 Hybrid 方式加入 VLAN。

把 GE0/0/1 接口加入组播 VLAN 20，GE0/0/2 接口加入组播 VLAN 10。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[Switch-GigabitEthernet0/0/2] port hybrid untagged vlan 20
[Switch-GigabitEthernet0/0/2] quit
```

把 GE 0/0/3 接口分别加入用户 VLAN 100。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port hybrid pvid vlan 100
```


版权所有 © 华为技术有限公司

```
[Switch-GigabitEthernet0/0/3] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/3] quit
```

步骤 6 验证配置结果

在 Switch 使用 **display user-vlan vlan** 命令可以查看到用户 VLAN 同时就加入到了组播 VLAN 10 和组播 VLAN 20。

```
[Quidway] display user-vlan vlan
 Total user vlan   2
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 100        IGMP Enable /MLD Disable  20              IGMP Enable /MLD Disable
```

使用 **display multicast static-flow** 命令可以查看到组播 VLAN 下面配置的组播静态流信息，说明用户 VLAN 下用户可以加入指定的组播组。

```
[Quidway] display multicast static-flow
 ------------------------------------------------------------------------
 Vlan                                          (Source, Group)
 ------------------------------------------------------------------------
  10                                            (*, 225.1.1.1)
  20                                            (*, 225.1.2.1)
 ------------------------------------------------------------------------
 Total Table(s) : 2
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 10 20 100
#
 igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 multicast-vlan enable
 multicast static-flow 225.1.1.1
 multicast-vlan user-vlan 100
#
vlan 20
 igmp-snooping enable
 multicast-vlan enable
 multicast static-flow 225.1.2.1
 multicast-vlan user-vlan 100
#
vlan 100
 igmp-snooping enable
 multicast flow-trigger enable
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
```


版权所有 © 华为技术有限公司

```
#
return
```

6.4 可控组播配置

介绍了可控组播的原理，及配置步骤。

6.4.1 概述

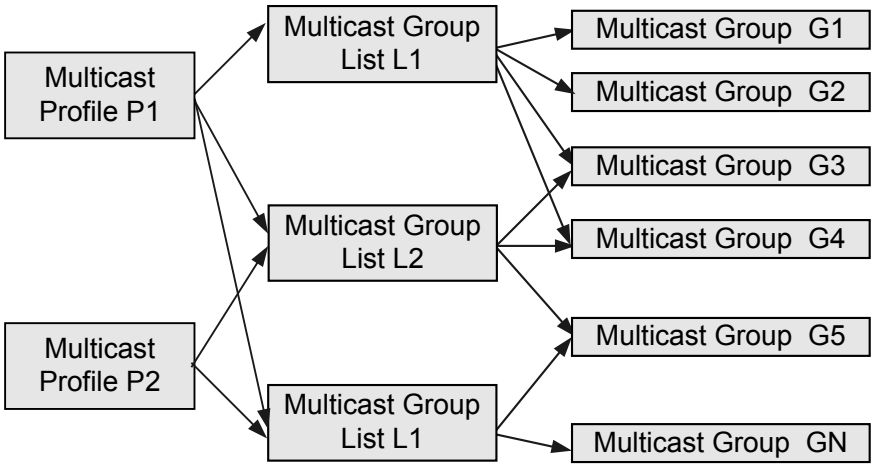
传统的组播业务是不可控的，用户可以通过发送 IGMP Report 报文来加入某个组播组，从而接收该组播组的组播报文。随着 IPTV 业务的逐步开展，这种不可控的组播业务已经无法适应运营需求。IPTV 业务是以盈利为目的的电信业务，用户只有通过缴纳费用才能收看某个节目（加入组播组），如果不能对用户进行鉴权，则无法满足 IPTV 的运营需求。可控组播正是在这种背景下提出的，其核心思想就是控制用户加入某个组播组的权限。当用户请求加入某个组播组时，交换机设备必须对这个请求进行鉴权，拒绝非法或越权的请求。

6.4.2 基本原理

S-switch 提供的可控组播机制

AC6605 提供了基于 VLAN 的可控组播机制，通过配置组播模板（Multicast Profile）来实现对用户组播权限的控制。为了更灵活的配置用户的组播权限，AC6605 提供了包括组播组、组播组列表、组播模板在内的三级控制机制，如图 6-11 所示。

图 6-11 可控组播的分级控制机制



组播组

一个组播组对应一个组播地址，例如 224.1.1.1。可理解为 IPTV 的一个频道（Channel）或者节目（Program）。

版权所有 © 华为技术有限公司

组播组列表

组播组列表是一系列组播组的集合。一个组播组列表可包含若干个组播组，例如图 6-11 中，组播组列表 L1 包含了组播组 G1、G2、G3、G4。一个组播组也可以被若干个组播组列表包含，例如组播组 G3 被组播组列表 L1、L2 所包含。

组播模板

组播模板定义了用户组播权限的框架，它是一系列组播组列表的集合。一个组播模板可包含若干个组播组列表，例如图 6-11 中，组播模板 P1 包含了组播组列表 L1、L2、L3。一个组播组列表也可以被若干个组播模板包含，例如组播组列表 L2 被组播模板 P1、P2 所包含。加入模板的列表都有其属性（观看或预览），如果列表是以观看属性加入模板，则模板的用户可观看列表下的所有组播组；如果列表是以预览属性加入模板，则模板的用户只能预览列表下的所有组播组。

控制流程

AC6605 的可控组播通过拦截 IGMP Report 报文，控制二层组播转发表项的生成来达到组播控制目的。当收到用户的 IGMP Report 报文后，根据报文所属的 VLAN 找到其使用的模板，如果组播组不在模板的列表下，则认为用户对该组没有权限，拦截此 IGMP Report 报文，不让其生成转发表项，从而使用户接收不到该组播组的数据流。如果组播组在模板的列表下，则看列表以哪种方式加入模板，如果列表以观看方式加入模板，则让 IGMP Report 报文通过。如果列表以预览方式加入模板，也让 IGMP Report 报文通过，但同时启动一个定时器，当预览时间超时就删除该组播组的转发表项，并拦截该组播组后续的 IGMP Report 报文。从而实现预览功能。

6.4.3 配置可控组播功能

介绍可控组播的配置方法。

建立配置任务

应用环境

当需要对用户加入组播组的权限进行控制时，可以配置可控组播。

前置任务

在配置可控组播之前，需先配置二层组播（IGMP Snooping 或 IGMP Proxy），实现组播报文的正常转发。

说明

在组播 VLAN 中，可控组播功能需要配置在用户 VLAN 上。

数据准备

在配置可控组播之前，需准备以下数据。

序号	数据
1	组播组的名称和 IP 地址

版权所有 © 华为技术有限公司

序号	数据
2	组播列表名称
3	组播模板名称
4	应用组播模板的用户 VLAN

配置组播组

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **btv**，进入 BTV 视图。

步骤 3 执行命令 **multicast-group** *group-name* { **ip-address** *multicast-group-address* [**source** *ipv4-source-address*] | **ipv6-address** *mld-group-address* [**source** *ipv6-source-address*] }，配置组播组。

缺省情况下，AC6605 中未配置组播组。

说明

如果用户接入使用的是 IGMP v2 版本，可以不需要配置 *source-address* 参数，如果使用的是 IGMP v3 版本，必须配置 *source-address* 参数。

如果已配置好组播组，且存在的地址都相同，则 *group-name* 的功能为修改组播组名称。

----结束

配置组播列表

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **btv**，进入 BTV 视图。

步骤 3 执行命令 **multicast-list** *list-name*，创建组播组列表并进入组播组列表视图。

步骤 4 执行命令 **add multicast-group** { **name** *group-name* | **index** *start-index* **to** *end-index* }，引用组播组。

缺省情况下，AC6605 中未配置组播列表。

----结束

配置组播模板

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **btv**，进入 BTV 视图。

步骤 3 执行命令 **multicast-profile** *profile-name*，创建组播模板并进入组播模板视图。

步骤 4 执行命令 **add multicast-list** { **name** *list-name* | **index** *start-index* **to** *end-index* } { **watch** | **preview** }，引用组播组列表。

缺省情况下，AC6605 中未配置组播模板。

步骤 5 （可选）执行命令 **max-program-num** *max-value*，配置用户同时接收的组播组的最大个数。

说明

缺省情况下，用户可同时接收的组播组最大个数为 8。

步骤 6 执行命令 **multicast-preview interval** *interval*，配置用户两次预览组播组的时间间隔。

步骤 7 执行命令 **multicast-preview minutes** *minutes*，配置用户每次预览组播组的时间长度。

步骤 8 执行命令 **multicast-preview times** *times*，配置用户每天可预览组播组的次数。

----结束

VLAN 上应用组播模板

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图

步骤 3 执行命令 **attach multicast-profile** *profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *，配置 VLAN 与组播模板的绑定关系。

缺省情况下，AC6605 中未配置 VLAN 与组播模板的绑定关系。

一个 VLAN 下面可以绑定多个组播模板。

说明

可控组播配置支持方式为 P+V 方式，即为接口+VLAN 的控制方式。在此方式下如果多个用户侧接口绑定在同一个 VLAN 中做组播点播，需要配置 **interface** *interface-type interface-number* 为这些接口分别指定组播模板。

步骤 4 （可选）执行命令 **max-program-num** *max-value* [**interface** *interface-type interface-number* | **mac-address** *mac-address*]*，配置用户同时接收的组播组最大个数。

说明

缺省情况下，用户可同时接收的组播组最大个数为 8。

如果在 VLAN 和该 VLAN 所绑定的组播模板上都配置了用户同时接收的组播组最大个数，仅 VLAN 上配置的生效；如果在 VLAN 上未配置用户同时接收的组播组最大个数，主要分以下两种情况：

- 该 VLAN 只绑定了一个组播模板，组播模板上配置的生效。
- 该 VLAN 绑定了多个组播模板，组播模板上配置的都不会生效，取缺省值 8。

----结束

版权所有 © 华为技术有限公司

检查配置结果

操作步骤

步骤 1 使用 **display multicast-group** [*group-name*]命令查看组播组配置信息。

步骤 2 使用 **display multicast-list** [*list-name*]命令查看组播组列表配置信息。

步骤 3 使用 **display multicast-profile** [*profile-name* [**verbose**]]命令查看组播模板配置信息。

步骤 4 使用 **display multicast-profile-apply** 命令查看 VLAN 应用模板。

----结束

6.4.4 配置举例

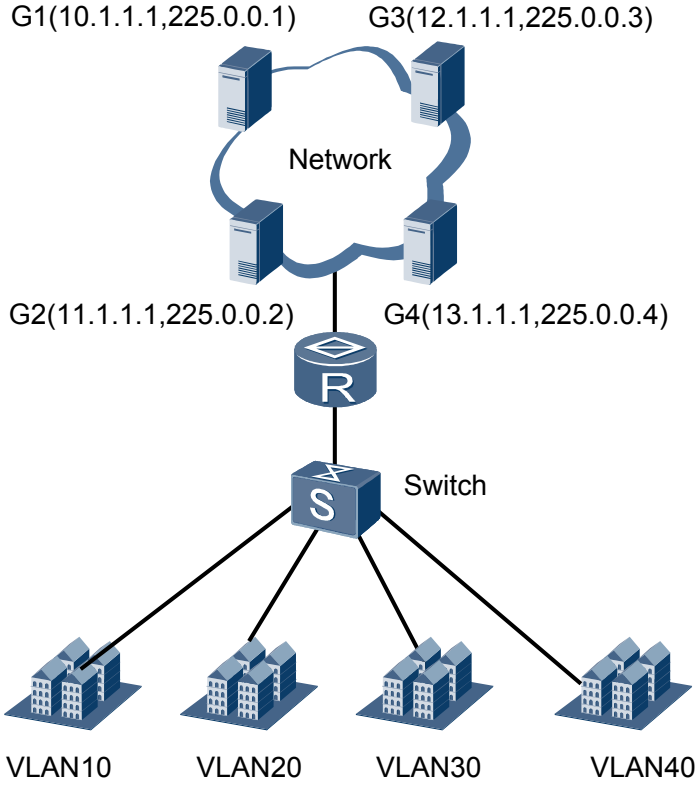
介绍可控组播配置示例。

配置可控组播示例

配置需求

如图 6-12 所示，路由器连接的网络上有组播组 G1(225.0.0.1)、G2（225.0.0.2）、G3（225.0.0.3）和 G4（225.0.0.4）。现在控制 VlAN1 和 VLAN2 的用户只能观看 G1 和 G2；VlAN3 和 VlAN4 的用户可观看所有的组播组。

图 6-12 可控组播基本配置组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置可控组播的基本功能：

1. 配置用户 VLAN。
2. 配置 IGMP Snooping。
3. 配置可控组播。
   - 配置两个组播列表 L1（G1, G2）和 L2（G3，G4）。
   - 配置两个模板 P1 和 P2。

数据准备

为完成此配置例，需准备如下的数据：

- 各组播组的名称。
- 各组播列表的名称。
- 各组播模板的名称。

配置步骤

1. 配置用户 VLAN，并将接口加入用户 VLAN（略）。
2. 配置 IGMP Snooping。

```
<Switch> system-view
[Switch] igmp-snooping enable
[Switch] vlan 1
[Switch-vlan1] igmp-snooping enable
[Switch-vlan1] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] igmp-snooping enable
[Switch-vlan3] quit
[Switch] vlan 4
[Switch-vlan4] igmp-snooping enable
[Switch-vlan4] quit
```

3. 配置可控组播。

   # 配置组播组。

```
[Switch] btv
[Switch-btv] multicast-group G1 ip-address 225.0.0.1
[Switch-btv] multicast-group G2 ip-address 225.0.0.2
[Switch-btv] multicast-group G3 ip-address 225.0.0.3
[Switch-btv] multicast-group G4 ip-address 225.0.0.4
```

   # 配置组播组列表。

```
[Switch-btv] multicast-list L1
[Switch-btv-list-L1] add multicast-group name G1
[Switch-btv-list-L1] add multicast-group name G2
[Switch-btv-list-L1] quit
[Switch-btv] multicast-list L2
[Switch-btv-list-L2] add multicast-group name G3
[Switch-btv-list-L2] add multicast-group name G4
[Switch-btv-list-L2] quit
```

   # 配置组播模板。

```
[Switch-btv] multicast-profile P1
```


版权所有 © 华为技术有限公司

```
[Switch-btv-profile-P1] add multicast-list name L1 watch
[Switch-btv-profile-P1] quit
[Switch-btv] multicast-profile P2
[Switch-btv-profile-P2] add multicast-list name L1 watch
[Switch-btv-profile-P2] add multicast-list name L2 watch
[Quidway-btv-profile-P2] quit
[Quidway-btv] quit
```

在 VLAN 下应用组播模板。

```
[Switch] vlan 1
[Switch-vlan1] attach multicast-profile P1
[Switch-vlan1] quit
[Switch] vlan 2
[Switch-vlan2] attach multicast-profile P1
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] attach multicast-profile P2
[Switch-vlan3] quit
[Switch] vlan 4
[Switch-vlan4] attach multicast-profile P2
[Switch-vlan4] quit
```

检验配置效果

```
[Switch-btv] display multicast-profile-apply
-------------------------------------------------------------------------------
  Vlan-id  Port                          SMAC           Max-User Index Profile-name
 -------------------------------------------------------------------------------
  Vlan1    --                            --              8       1    P1
  Vlan2    --                            --              8       1    P1
  Vlan3    --                            --              8       2    P2
  Vlan4    --                            --              8       2    P2

Total: 4

[Switch-btv] display multicast-profile
 -------------------------------------------------------------------------------
 Index        Profile-Name                    Multicast-list  Attach-User
 -------------------------------------------------------------------------------
  1             P1                               1              2
  2             P2                               2              2

 Total: 2
[Switch-btv] display multicast-list
 -------------------------------------------------------------------------
 Index        Multicast-list-name             Multicast-group
 -------------------------------------------------------------------------
  1            L1                                  2
  2            L2                                  2

 Total: 2

[Switch-btv] display multicast-group
-------------------------------------------------------------------------
 Index        Multicast-group-name              Address
 -------------------------------------------------------------------------
  1           G1                               225.0.0.1
  2           G2                               225.0.0.2
  3           G3                               225.0.0.3
  4           G4                               225.0.0.4

 Total: 4
```

配置文件

```
 sysname Switch
#
 vlan batch 1 to 4
#
```


版权所有 © 华为技术有限公司

```
 igmp-snooping enable
#
 btv
 multicast-group  G1 ip-address 225.0.0.1
 multicast-group  G2 ip-address 225.0.0.2
 multicast-group  G3 ip-address 225.0.0.3
 multicast-group  G4 ip-address 225.0.0.4
 #
 multicast-list  L1
  add multicast-group name G1
  add multicast-group name G2
 multicast-list  L2
  add multicast-group name G3
  add multicast-group name G4
 #
 multicast-profile  P1
  add  multicast-list name L1 watch
 multicast-profile  P2
  add  multicast-list name L1 watch
  add  multicast-list name L2 watch
#
vlan 1
 igmp-snooping enable
 attach multicast-profile P1
#
vlan 2
 igmp-snooping enable
 attach multicast-profile P1
#
vlan 3
 igmp-snooping enable
 attach multicast-profile P2
#
vlan 4
 igmp-snooping enable
 attach multicast-profile P2
#
return
```

6.5 IGMP 配置

介绍 IGMP 的配置方法、维护命令，并提供配置举例。

6.5.1 IGMP 概述

简要介绍 IGMP 的基本原理。

IGMP（Internet Group Management Protocol）作为因特网组管理协议，是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议，它用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

AC6605 作为路由交换机，也支持 IP 组播功能，当配置了 IGMP 协议时，可将它作为组播交换机。IGMP 协议是 IP 组播在末端网络上使用的主机对 AC6605 的信令机制，分为两个功能部分：主机侧和交换机侧。

说明

- 主机支持 IGMP 的具体情况和所使用的操作系统有关。
- 下文中所称的“交换机”指的是配置了三层组播协议，具有组播路由器功能的 AC6605。

- 所有参与组播传输的接收者主机必须应用 IGMP 协议。主机可以在任意时间、任意位置、成员总数不受限制地加入或退出组播组。

版权所有 © 华为技术有限公司

- 支持组播的三层设备通过 IGMP 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而各主机只需要保存自己加入了哪些组播组。

到目前为止，IGMP 有三个版本：IGMPv1 版本（由 RFC1112 定义）、IGMPv2 版本（由 RFC2236 定义）和 IGMPv3（由 RFC3376 定义）版本。所有 IGMP 版本都支持 ASM（Any-Source Multicast）模型。IGMPv3 可以直接应用于 SSM（Source-Specific Multicast）模型，而 IGMPv1 和 IGMPv2 则需要 SSM-Mapping 技术的支持。

6.5.2 AC6605 支持的 IGMP 特性

介绍 IGMP 特性在 AC6605 中的支持情况。

IGMP 基本功能

AC6605 支持的 IGMP 基本功能有：

- 支持 IGMPv1、IGMPv2 和 IGMPv3，版本可配置。
- 支持静态 IGMP。
- 允许配置接口加入的组播组范围。

Router-Alert 选项可选

由于 IGMPv2 和 v3 版本中包含指定组、指定源/组的查询报文，这些组是千变万化的，AC6605 不可能加入所有组，所以 IGMP 通过 Router-Alert 选项来将送往本地的没有加入的组报文送到上层协议进行处理。

用户可以根据需要配置是否在发送的 IGMP 报文中包含 Router-Alert 选项、是否要求接收的 IGMP 报文必须包含 Router-Alert 选项。

IGMP 查询控制器

对于 IGMPv1，用户可以设置普遍组查询消息的发送间隔、健壮系数。

说明

IGMPv1 不支持查询器选举，需要配置 PIM 协议，选举查询器。

对于 IGMPv2，用户可以配置普遍组查询消息的发送间隔、健壮系数、IGMP 查询报文的最大响应时间、IGMP 快速离开等功能。

对于 IGMPv3，用户可以配置普遍组查询消息的发送间隔、健壮系数、IGMP 查询报文的最大响应时间等功能。

SSM-Mapping

用户可以通过在 AC6605 上配置 SSM-Mapping 功能，向运行 IGMPv1 或 IGMPv2 的主机提供 SSM 服务。

IGMP Limit

IGMP Limit 功能可用于 IPv4 PIM-SM 和 IPv4 PIM-DM 网络中。

当用户希望限制用户接入的数量时，可以配置 IGMP Limit 功能。

- 配置全局 IGMP 组成员关系个数限制

版权所有 © 华为技术有限公司

- 配置基于接口的 IGMP 组成员关系个数限制

说明

若需要在同一交换机上配置基于全局和接口的 IGMP Limit 功能时，建议全局 IGMP 组成员关系个数限制值>基于接口 IGMP 组成员关系个数限制值。

6.5.3 配置 IGMP 基本功能

介绍 IGMP 的应用和配置方法。

建立配置任务

应用环境

IGMP 应用在 AC6605 与用户主机相连的网段，在 AC6605 和用户主机上都需要运行 IGMP。下面只介绍如何在 AC6605 上配置 IGMP。

配置 IGMP 之前，必须先使能 IP 组播路由功能。IP 组播路由是配置一切组播功能的前提。如果停止 IP 组播路由，组播所有相关配置将无法生效。

在连接用户主机的 VLANIF 接口上使能 IGMP，由于不同版本的 IGMP 协议报文不相同，因此需要为 AC6605 和主机配置匹配的版本（AC6605 侧的高版本可以兼容主机侧的低版本）。执行此操作之后，才能进行 IGMP 的其他配置。

运行 IGMP 的主机会对 AC6605 的 IGMP 查询报文进行响应，如果超时无响应，AC6605 就认为该网段没有该组播组的成员，从而取消相应的数据转发。

为了让接口所连接网络上的主机加入指定的组播组，并接收这些组的报文，可以在对应接口上设置一个 ACL 规则作为过滤器，以限制接口所服务的组播组范围。

前置任务

在配置 IGMP 的基本功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。
- 配置单播路由协议，使各节点间 IP 路由可达。

数据准备

在配置 IGMP 基本功能之前，需要准备以下数据。

序号	数据
1	和主机通信的接口所在 VLAN 编号
2	IGMP 版本
3	组播组地址、组播源地址
4	组播组过滤的 ACL 规则

版权所有 © 华为技术有限公司

使能 IP 组播功能

背景信息

IP 组播功能是配置其他组播协议的前提条件。在与用户主机相连的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **multicast routing-enable**，使能 IP 组播路由功能。

缺省情况下，AC6605 未使能 IP 组播路由功能。

----结束

使能 IGMP 功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp enable**，使能 IGMP 功能。

缺省情况下，接口上未使能 IGMP 功能。

----结束

（可选）配置 IGMP 版本

背景信息

注意

务必保证同一网段的所有 AC6605 接口配置相同的 IGMP 版本，缺省采用 IGMPv2 版本。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

此接口是 AC6605 与用户主机通信的接口。

版权所有 © 华为技术有限公司

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp version** { **1** | **2** | **3** }，配置接口的 IGMP 版本。

----结束

（可选）配置静态 IGMP 组

背景信息

将接口静态加入某组播组后，AC6605 就认为此接口所在网段上一直存在该组播组的成员，从而接收发往该组的组播数据。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

此接口是 AC6605 与用户主机通信的接口。

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp static-group** *group-address* [**source** *source-address*]，配置接口静态加入组播组或组播源组。

如果选用 Loopback 接口，AC6605 将组播数据引入后不会立即转发出去，当有用户点播到该组数据才转发。这样可以减少带宽占用率。VLANIF 接口会立即转发。

缺省情况下，接口未以静态方式加入任何组播组。

----结束

（可选）配置 IGMP 组策略

背景信息

为了让接口所连接网络上的主机加入指定的组播组，并接收这些组的报文，可以在对应接口上设置一个 ACL 规则，对收到的报文进行过滤，以限制接口所服务的组播组范围。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

此接口是 AC6605 与用户主机通信的接口。

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp group-policy** *acl-number* [**1** | **2** | **3**]，配置接口可以加入的组播组范围。

缺省情况下，接口可以加入任何组播组。

----结束

版权所有 © 华为技术有限公司

检查配置结果

前提条件

已完成 IGMP 基本功能配置。

操作步骤

- 使用命令 **display igmp interface** [*interface-type interface-number*] [**verbose**]查看接口上的 IGMP 配置和运行信息。
- 使用命令 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * **static** 查看静态 IGMP 组播组的成员信息。
- 使用命令 **display igmp group**[*group-address* | **interface** *interface-type interface-number*] * [**verbose**]查看动态加入的 IGMP 组播组成员信息。

----结束

任务示例

执行命令 **display igmp interface vlanif** 3，可以查看 VLANIF3 接口上的 IGMP 配置信息。

```
<Quidway> display igmp interface vlanif 3
Interface information
 Vlanif10(100.0.0.3):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: -
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 100.0.0.3 (this router)
```

执行命令 **display igmp group static** 可以查看静态 IGMP 组播组的信息。

```
<Quidway> display igmp group static
Static join group information
  Total 2 entries, Total 2 active entries
  Group Address   Source Address  Interface          Expires
  225.0.0.10      0.0.0.0         Loop1              never
  232.1.1.20      10.0.0.1        Vlanif3            never
```

6.5.4 配置 IGMP 性能参数

介绍 IGMP 性能参数的配置方法。

背景信息

缺省情况下，IGMP 可以正常工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。用户可以根据需要选择执行下面的配置任务。

版权所有 © 华为技术有限公司

说明

- 在 IGMP 视图下的配置全局有效，在接口视图下的配置只对该接口有效。
- 如果接口视图和 IGMP 视图下都配置了命令，则优先选择接口视图下配置的值。接口视图下没有配置命令时，IGMP 视图下配置的值有效。

建立配置任务

应用环境

由于 IGMPv2 和 v3 版本中包含指定组、指定源组的查询报文，这些组是千变万化的，AC6605 不可能加入所有组，所以 IGMP 就需要借助 Router-Alert 选项来将送往本地的没有加入的组报文送到上层协议进行处理。

在与接收者相连的共享网段上，由 IGMP 查询器周期性地发送查询报文，当得到某一组成员报告时，刷新该网段相应的组成员关系信息。如果非查询器在“IGMP 查询器存活时间”之内没有收到普遍查询报文，则认为查询器故障，将自动发起新一轮的查询器选举过程。

在有些情况下，一台主机对应一个端口，因此查询器仅对应一个接收者主机，当接收者主机在多个组播组间频繁切换时，可以在查询器上启动快速离开组机制。

前置任务

在配置 IGMP 报文选项和相关定时器之前，需要完成以下任务：

- 配置单播路由协议，使各节点间 IP 路由可达。
- **6.5.3 配置 IGMP 基本功能**。

数据准备

在配置 IGMP 报文选项和相关定时器之前，需要准备以下数据。

序号	数据
1	是否需要报文中包含 Router-Alert 选项
2	IGMP 普遍组查询消息的发送间隔
3	IGMP 健壮系数
4	IGMP 查询消息的最大响应时间
5	其他 IGMP 查询器存活时间
6	IGMP 指定组查询消息的发送间隔
7	限定快速离开应用范围的 ACL

配置 IGMP 报文选项

版权所有 © 华为技术有限公司

背景信息

Router-Alert 选项要求 AC6605 将送往本地的没有加入的 IGMP 组报文送到上层协议进行处理。缺省情况下，AC6605 将发送的 IGMP 报文中携带 Router-Alert 选项，但不对此选项进行检查，即处理所有接收到的 IGMP 报文，包括无 Router-Alert 选项的 IGMP 报文。如果配置 **require-router-alert**，则检查此选项。

Router-Alert 选项可以在全局和接口下配置。

- 全局的配置在各接口上都有效。
- 接口的配置只在指定接口上有效。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 配置全局性 IGMP 报文选项
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **require-router-alert**，配置 AC6605 忽略未包含 Router-Alert 选项的 IGMP 报文。
  4. 执行命令 **send-router-alert**，配置 AC6605 在发送的 IGMP 报文头中包含 Router-Alert 选项。

     说明

     执行 **send-router-alert** 命令后查看当前配置，不会显示相关信息。执行 **undo send-router-alert** 命令才会显示相关配置信息。
- 配置接口下 IGMP 报文选项
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     此接口是 AC6605 与用户主机通信的接口。

     AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **igmp require-router-alert**，配置 AC6605 忽略未包含 Router-Alert 选项的 IGMP 报文。
  4. 执行命令 **igmp send-router-alert**，配置 AC6605 在发送的 IGMP 报文头中包含 Router-Alert 选项。

     说明

     执行 **igmp send-router-alert** 命令后查看当前配置，不会显示相关信息。执行 **undo igmp send-router-alert** 命令才会显示相关配置信息。

----结束

配置 IGMPv1 查询器

背景信息

IGMP 查询器可以在全局和接口下配置。

- 全局的配置在各接口上都有效。

版权所有 © 华为技术有限公司

- 接口的配置只在指定接口上有效。针对接口的取值优于全局值，未配置接口值时继承全局值。

当 IGMP 版本为 IGMPv1 时，可配置的 IGMP 的查询器包括 IGMP 普遍组查询消息的发送时间间隔和 IGMP 健壮系数。

操作步骤

- 配置全局性 IGMP 查询器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **timer query** *interval*，配置 AC6605 发送 IGMP 普遍组查询消息的时间间隔。

     缺省情况下，IGMP 普遍组查询时间间隔为 60 秒。
  4. 执行命令 **robust-count** *robust-value*，配置 IGMP 健壮系数。

     当系统启动时发送“健壮系数”次的“普遍组查询消息”，发送间隔为“IGMP 普遍组查询消息的发送间隔”的 1/4。缺省情况下，IGMP 健壮系数为 2。
- 配置接口下 IGMP 查询器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     此接口是 AC6605 与用户主机通信的接口。

     AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **igmp timer query** *interval*，配置 AC6605 发送 IGMP 普遍组查询消息的时间间隔。

     缺省情况下，IGMP 普遍组查询时间间隔为 60 秒。
  4. 执行命令 **igmp robust-count** *robust-value*，配置 IGMP 健壮系数。

     当系统启动时发送“健壮系数”次的“普遍组查询消息”，发送间隔为“IGMP 普遍组查询消息的发送间隔”的 1/4。缺省情况下，IGMP 健壮系数为 2。

----结束

配置 IGMPv2/v3 查询器

背景信息

IGMP 查询器可以在全局和接口下配置。

- 全局的配置在各接口上都有效。
- 接口的配置只在指定接口上有效。针对接口的取值优于全局值，未配置接口值时继承全局值。

当 IGMP 版本为 IGMPv2 或 IGMPv3 时，可配置的 IGMP 的查询器参数包括 IGMP 普遍组查询消息的发送间隔、IGMP 指定组查询消息的发送间隔、IGMP 查询报文最大响应时间、其他 IGMP 查询器的存活时间和 IGMP 健壮系数。

版权所有 © 华为技术有限公司

说明

实际配置中，要确保“IGMP 查询报文最大响应时间”<“IGMP 普遍组查询消息发送间隔”<“其他 IGMP 查询器存活时间”。

操作步骤

- 配置全局性 IGMP 查询器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **timer query** *interval*，配置 AC6605 发送 IGMP 普遍组查询消息的时间间隔。

     缺省情况下，IGMP 普遍组查询消息发送时间间隔为 60 秒。
  4. 执行命令 **robust-count** *robust-value*，配置 IGMP 健壮系数。
     - 当系统启动时发送“健壮系数”次的“普遍组查询消息”，发送时间间隔为“IGMP 普遍组查询消息发送间隔”的 1/4。
     - 当 AC6605 收到离开消息后，发送“健壮系数”次的“IGMP 指定组查询消息”，发送间隔为“IGMP 指定组查询消息发送间隔”。

     缺省情况下，IGMP 健壮系数为 2。
  5. 执行命令 **max-response-time** *interval*，配置 IGMP 查询报文的最大响应时间。

     缺省情况下，IGMP 查询报文的最大响应时间为 10 秒。
  6. 执行命令 **timer other-querier-present** *interval*，配置其他 IGMP 查询器的存活时间。

     缺省情况下，“其他 IGMP 查询器存活时间”＝“健壮系数”*“普遍组查询消息发送间隔”+（1/2）*“最大响应时间”。当等式右边的参数都取缺省值时，“其他 IGMP 查询器存活时间”的值为 125 秒。
  7. 执行命令 **lastmember-queryinterval** *interval*，配置 AC6605 发送 IGMP 指定组查询消息的时间间隔。

     缺省情况下，IGMP 指定组查询消息的发送间隔为 1 秒。
- 配置接口下 IGMP 查询器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     此接口是 AC6605 与用户主机通信的接口。

     AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **igmp timer query** *interval*，配置 AC6605 发送 IGMP 普遍组查询消息的时间间隔。

     缺省情况下，IGMP 普遍组查询消息发送时间间隔为 60 秒。
  4. 执行命令 **igmp robust-count** *robust-value*，配置 IGMP 健壮系数。
     - 当系统启动时发送“健壮系数”次的“普遍组查询消息”，发送时间间隔为“IGMP 普遍组查询消息发送间隔”的 1/4。
     - 当 AC6605 收到离开消息后，发送“健壮系数”次的“IGMP 指定组查询消息”，发送间隔为“IGMP 指定组查询消息发送间隔”。

版权所有 © 华为技术有限公司

缺省情况下，IGMP 健壮系数为 2。

5. 执行命令 **igmp max-response-time** *interval*，配置 IGMP 查询报文的最大响应时间。

   缺省情况下，IGMP 查询报文的最大响应时间为 10 秒。

6. 执行命令 **igmp timer other-querier-present** *interval*，配置其他 IGMP 查询器的存活时间。

   缺省情况下，“其他 IGMP 查询器存活时间”＝“健壮系数”*“普遍组查询消息发送间隔”+（1/2）*“最大响应时间”。当等式右边的参数都取缺省值时，“其他 IGMP 查询器存活时间”的值为 125 秒。

7. 执行命令 **igmp lastmember-queryinterval** *interval*，配置 AC6605 发送 IGMP 指定组查询报文的时间间隔。

   缺省情况下，IGMP 指定组查询消息的发送间隔为 1 秒。

8. 执行命令 **igmp on-demand**，配置接口上的（S，G）表项永不超时，接口不向外发送 IGMP 查询报文。

   缺省情况下，接口发送查询报文，参与查询器选举。

   说明

   igmp on-demand 命令只在 IGMPv2 和 IGMPv3 支持。

----结束

配置 IGMP 快速离开

背景信息

IGMP 快速离开是指当查询器收到来自主机的离开消息后，不再发送最后成员查询消息，而是直接向上游设备报告离开通告。这样一方面减小了响应延迟，另一方面节省了因各种消息而占用的网络带宽。

说明

- IGMP 快速离开功能仅适用于 IGMPv2 版本。
- 应用 IGMPv1 或 IGMPv3 版本时，如果查询当前配置有 IGMP 快速离开的信息，也是不生效的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

此接口是 AC6605 与用户主机通信的接口。

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp prompt-leave** [**group-policy** *basic-acl-number*]，配置接口无需发送最后组查询消息就立刻离开组。

缺省情况下，AC6605 在接收到主机发送的离开消息后发送最后成员查询消息。

----结束

版权所有 © 华为技术有限公司

检查配置结果

前提条件

已完成 IGMP 基本功能及参数配置。

操作步骤

- 使用命令 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * [**static** | **verbose**]查看 IGMP 组播组的成员信息。
- 使用命令 **display igmp interface** [*interface-type interface-number*] [**verbose**]查看接口上 IGMP 配置和运行信息。
- 使用命令 **display igmp routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]]* [**static**]查看 IGMP 路由表信息。

  在配置成功时，执行上面的命令，应能得到如下的结果：

  - 查看 IGMP 组播组的成员信息，组播组的成员信息应配置正确。
  - 查看 IGMP 配置和运行信息，AC6605 接口 IGMP 信息应配置正确。
  - 查看 IGMP 路由表信息，（*，G）或（S，G）项的 Downstream List（下游接口列表）中应有对应的组播转发接口。

----结束

任务示例

执行命令 **display igmp group interface vlanif 3 static** 可以查看 VLANIF3 接口的 IGMP 配置信息。

```
<Quidway> display igmp group interface vlanif 3 static
Static join group information
 Total 2 entries
 Specified interface state:UP
 Total 2 entries matched

  Group Address   Source Address  Expires
  232.1.1.1       10.0.0.1        never
  225.0.0.10      0.0.0.0         never
```

执行命令 **display igmp routing-table** 可以查看 IGMP 路由表信息。

说明

在使能 PIM 后，才会生成 IGMP 路由表信息。

```
<Quidway> display igmp routing-table
 Total 1 entry

 00001. (*, 225.0.0.10)
       List of 1 downstream interface
        Vlanif3 (100.0.0.3),
                  Protocol: STATIC
```

6.5.5 配置 SSM Mapping

介绍 SSM Mapping 的应用和配置方法。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

在提供 SSM 模式组播服务的网段中，由于各种可能的限制，某些用户主机必须运行 IGMPv1 或 v2。为保证向这些用户提供 SSM 服务，需要在 AC6605 上配置 SSM 静态映射功能。

前置任务

在配置 SSM Mapping 之前，需要完成以下任务：

- 配置单播路由协议，使各节点间 IP 路由可达。
- 使能 IGMP 功能。

数据准备

在配置 SSM Mapping 之前，需要准备以下数据。

序号	数据
1	需要使能 SSM Mapping 功能的接口
2	组播组地址和掩码、组播源地址和掩码

使能 SSM Mapping 功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

此接口是 AC6605 与用户主机通信的接口。

AC6605 支持 IGMP 的接口为 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **igmp enable**，使能 IGMP 功能。

步骤 4 执行命令 **igmp version 3**，配置 IGMP 版本号为 3。

为保证该网段内运行任意版本 IGMP 的用户主机都能得到 SSM 服务，建议在 AC6605 的接口上运行 IGMPv3。

步骤 5 执行命令 **igmp ssm-mapping enable**，使能 SSM Mapping 功能。

----结束

配置 SSM Mapping 策略

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **igmp**，进入 IGMP 视图。

步骤 3 执行命令 **ssm-mapping** *group-address* { *mask* | *mask-length* } *source-address*，配置组到源的映射。

SSM 组地址范围为 232.0.0.0 ～ 232.255.255.255。多次配置，可以实现同一个组到多个源的映射。

- *group-address* { *mask* | *mask-length* }为组地址和掩码。
- *source-address* 为与组建立映射关系的源地址。

----结束

检查配置结果

前提条件

已完成 SSM Mapping 的配置。

操作步骤

- 使用命令 **display igmp group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]查看特定源/组地址的信息。
- 使用命令 **display igmp ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }查看特定源/组地址的 SSM Mapping 信息。

----结束

任务示例

执行命令 **display igmp ssm-mapping group** [*group-address*]可以查看指定组地址对应的 SSM 映射信息。

```
<Quidway> display igmp ssm-mapping group 232.0.0.1
IGMP SSM-Mapping conversion table
 Total 2 entries    2 entries matched

 00001. (10.0.0.1, 232.0.0.1)

 00002. (10.0.0.2, 232.0.0.1)

 Total 2 entries matched
```

执行命令 **display igmp ssm-mapping interface** *interface-type interface-number* 可以查看指定接口上的 SSM 映射信息。

```
<Quidway> display igmp ssm-mapping interface vlanif 3
Info: IGMP SSM-Mapping is enabled
```

6.5.6 维护 IGMP

介绍如何维护 IGMP。

版权所有 © 华为技术有限公司

清除 IGMP 组信息

背景信息

注意

执行 **reset igmp group** 命令将删除接口上已经动态加入的 IGMP 组，可能导致接收者无法正常接收组播信息，请慎用。

在用户视图下执行以下命令清除 IGMP 组信息。

操作步骤

- 使用命令 **reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }清除接口上已经动态加入的 IGMP 组。

----结束

监控 IGMP 运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 IGMP 的运行状况。

操作步骤

- 使用命令 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]查看 IGMP 组播组信息。
- 使用命令 **display igmp group ssm-mapping** [**verbose**]查看配置了 SSM 映射的组播组信息。
- 使用命令 **display igmp interface** [*interface-type interface-number*] [**verbose**]查看接口上 IGMP 配置和运行信息。
- 使用命令 **display igmp routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]]* [**static**]查看 IGMP 路由表信息。
- 使用命令 **display igmp ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }查看特定源/组地址的 SSM 映射信息。

----结束

调试 IGMP

版权所有 © 华为技术有限公司

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

- 使用命令 **debugging igmp** { **all** | **event** | **leave** [*basic-acl-number*] | **report** [*advanced-acl-number*] | **query** [*basic-acl-number*] | **timer** }打开 IGMP 调试信息开关。
- 使用命令 **debugging igmp ssm-mapping** [*advanced-acl-number*]打开 SSM Mapping 调试信息开关。

----结束

6.5.7 配置举例

介绍 IGMP 的配置举例。

配置 IGMP 基本功能示例

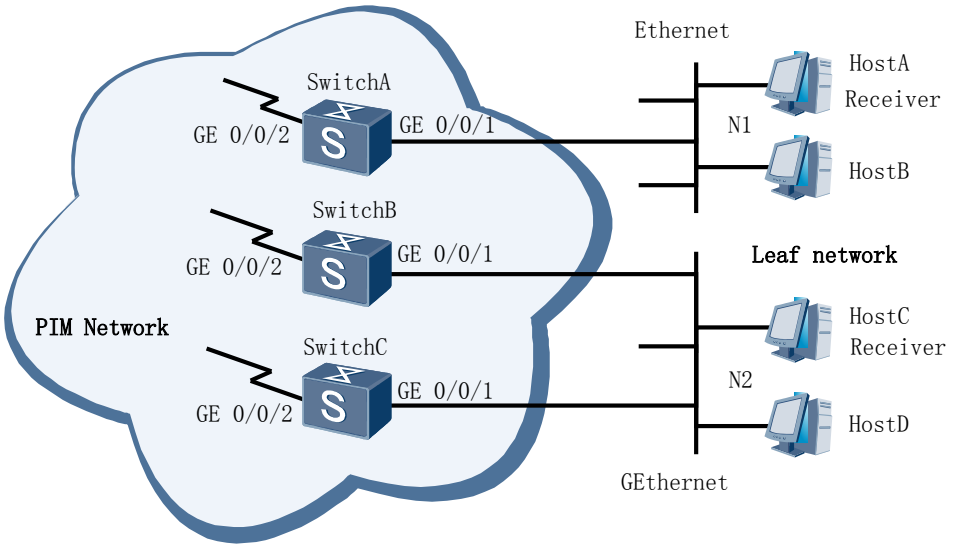
组网需求

已知如图 **6-13** 所示的网络中，单播路由正常。要求在该网络中部署组播功能，使用户主机能够接收视频点播信息。

当某个接口下的用户需要长期接收热点节目时，将该接口静态加入组播组。如下网络中，HostA 需要长期接收组播组 225.1.1.1 的数据，则将 SwitchA 的接口 GE0/0/1 配置成静态加入组播组 225.1.1.1。

版权所有 © 华为技术有限公司

图 6-13 配置 IGMP 的基本功能组网图



交换机	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF10	10.110.1.1/24
SwitchA	GE0/0/2	VLANIF11	192.168.1.1/24
SwitchB	GE0/0/1	VLANIF20	10.110.2.1/24
SwitchB	GE0/0/2	VLANIF21	192.168.2.1/24
SwitchC	GE0/0/1	VLANIF30	10.110.3.1/24
SwitchC	GE0/0/2	VLANIF31	192.168.3.1/24

配置思路

采用如下思路配置 IGMP 的基本功能：

1. 在所有为组播服务的 Switch 使能组播功能。
2. 在所有 Switch 接口上使能 PIM-SM 功能。
3. 在连接用户主机的 Switch 接口上使能 IGMP 功能。
4. 将 A 的 VLANIF10 接口静态加入组播组 225.1.1.1。

数据准备

为完成此配置举例，需要准备如下数据：

- Switch 与用户主机之间运行的 IGMP 版本号。
- 静态组播组地址：225.1.1.1。

说明

配置用例中，只列出了与 IGMP 配置相关的命令。

操作步骤

步骤 1 配置各 Switch 接口 IP 地址和单播路由协议。

版权所有 © 华为技术有限公司

按照图 6-13 配置各接口的 IP 地址和掩码，并配置各 Switch 之间采用 OSPF 进行互连，确保网络中各 Switch 间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。具体配置过程略。

接口 IP 地址的配置方法，请参见《AC6605 无线接入控制器 配置指南-基础配置》中 **4.1.3 配置接口的 IP 地址**，OSPF 的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 路由》中 **OSPF 配置**。

步骤 2 使能组播功能，并在所有接口上使能 PIM-SM 功能。

在 SwitchA 上使能组播功能，在所有接口上使能 PIM-SM 功能。SwitchB 和 SwitchC 上的配置过程与此完全相同，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 11
[SwitchA-Vlanif11] pim sm
[SwitchA-Vlanif11] quit
```

步骤 3 在主机侧接口上使能 IGMP 功能。

在 SwitchA 的 VLANIF10 接口上使能 IGMP 功能，并配置 IGMP 版本为 v2。SwitchB 和 SwitchC 上的配置过程与此完全相同，配置过程略。

说明

缺省情况下 IGMP 版本就是 IGMPv2，这里也可以不配置。如果使用其他版本，则一定要配置 **igmp version**。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp enable
[SwitchA-Vlanif10] igmp version 2
[SwitchA-Vlanif10] quit
```

步骤 4 将 SwitchA 的 VLANIF10 接口静态加入组播组 225.1.1.1，使该接口下的用户能长期接收发往组播 225.1.1.1 的数据。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp static-group 225.1.1.1
```

步骤 5 验证配置结果。

通过使用 **display igmp interface** 命令可以查看各接口上 IGMP 的配置和运行情况。例如 A 的 VLANIF10 接口上 IGMP 的显示信息如下：

```
[SwitchA] display igmp interface vlanif 10
Vlanif 10(10.110.1.1):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Querier for IGMP: 10.110.1.1 (this router)
```

在 SwitchA 上通过使用命令 **display igmp routing-table** 可以查看，接口 VLANIF10 是否静态加入组播组 225.1.1.1。如果 SwitchA 上有（*，225.1.1.1）表项，且下游接口是 VLANIF10，协议类型为“static”，则表明 VLANIF10 静态加入组播组 225.1.1.1 配置成功。

```
[SwitchA] display igmp routing-table
Routing table of VPN-Instance: public net
```


版权所有 © 华为技术有限公司

```
Total 1 entry
00001. (*, 225.1.1.1)
    List of 1 downstream interface
    Vlanif10 (10.110.1.1),
    Protocol: STATIC
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 11
#
 multicast routing-enable
#
interface Vlanif10
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp static-group 225.1.1.1
#
interface Vlanif11
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 20 21
#
 multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif21
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 21
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 30 31
#
 multicast routing-enable
#
interface Vlanif30
 ip address 10.110.3.2 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif31
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 30
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

配置 SSM Mapping 示例

组网需求

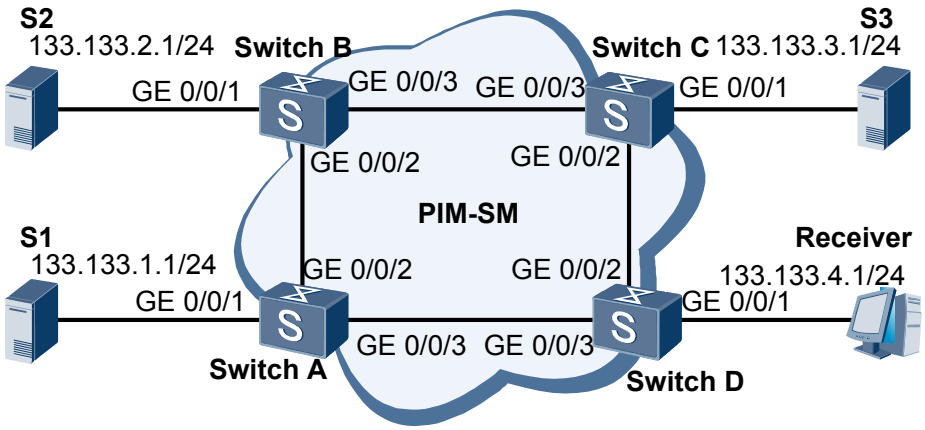
已知如图 6-14 所示的组播网络中，运行 PIM-SM 协议，同时采用 ASM 和 SSM 模式提供组播服务。与用户主机 Receiver 相连的交换机接口上运行 IGMPv3，Receiver 上的 IGMP 的版本为 v2，不能升级到 IGMPv3。

当前网络中的 SSM 组地址范围是 232.1.1.0/24，S1、S2 和 S3 都向该范围内的组播组发送组播数据。要求 Receiver 只接收来自 S1 和 S3 的组播数据。

解决方案：在 SwitchD 上配置 SSM Mapping 功能。

版权所有 © 华为技术有限公司

图 6-14 配置 SSM Mapping 功能组网图



Switch	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF10	133.133.1.2/24
SwitchA	GE0/0/2	VLANIF20	192.168.1.1/24
SwitchA	GE0/0/3	VLANIF30	192.168.4.2/24
SwitchB	GE0/0/1	VLANIF11	133.133.2.2/24
SwitchB	GE0/0/2	VLANIF20	192.168.1.2/24
SwitchB	GE0/0/3	VLANIF31	192.168.2.1/24
SwitchC	GE0/0/1	VLANIF12	133.133.3.2/24
SwitchC	GE0/0/2	VLANIF21	192.168.3.1/24
SwitchC	GE0/0/3	VLANIF31	192.168.2.2/24
SwitchD	GE0/0/1	VLANIF13	133.133.4.2/24
SwitchD	GE0/0/2	VLANIF21	192.168.3.2/24
SwitchD	GE0/0/3	VLANIF30	192.168.4.1/24

配置思路

采用如下思路配置 SSM Mapping 功能：

1. 在连接用户主机的交换机接口上使能 SSM Mapping 功能；
2. 在该 PIM-SM 域内的所有交换机配置 SSM 组播组地址范围；
3. 在使能了 SSM Mapping 功能的交换机配置 SSM Mapping 静态映射规则。

数据准备

为完成此配置举例，需要准备如下数据：

- SSM 组播组范围
- Source 1 和 Source 3 的 IP 地址

说明

配置用例中，只列出了与 SSM Mapping 配置相关的命令。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 VLAN，配置各接口加入 VLAN（略）。

步骤 2 按照图 6-14 所示配置各 VLANIF 接口的 IP 地址和单播路由协议（略）。

步骤 3 在连接用户主机的接口上使能 IGMP 功能和 SSM Mapping 功能。

```
[SwitchD] multicast routing-enable
[SwitchD] interface vlanif 13
[SwitchD-Vlanif13] igmp enable
[SwitchD-Vlanif13] igmp version 3
[SwitchD-Vlanif13] igmp ssm-mapping enable
[SwitchD-Vlanif13] quit
```

步骤 4 配置 SSM 组播组地址范围。

在所有交换机配置 SSM 组播组地址范围为 232.1.1.0/24。SwitchB、SwitchC 和 SwitchD 上的配置过程与 SwitchA 上的配置完全相同，配置过程略。

```
[SwitchA] acl number 2000
[SwitchA-Acl-Basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-Acl-Basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
```

步骤 5 在连接用户主机的交换机上配置 SSM Mapping 静态映射规则。

将 232.1.1.0/24 范围内的组播组映射到 Source 1 和 Source 3。

```
[SwitchD] igmp
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.1.1
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.3.1
```

查看 SwitchD 上特定源/组地址的 SSM Mapping 信息。

```
[SwitchD] display igmp ssm-mapping group
IGMP SSM-Mapping conversion table of VPN-Instance: public net
Total 2 entries
Total 2 entries matched
 00001. (133.133.1.1, 232.1.1.0)
 00002. (133.133.3.1, 232.1.1.0)
```

步骤 6 验证配置结果。

Receiver 加入组 232.1.1.1。

通过使用 **display igmp group ssm-mapping** 命令，可以查看交换机特定源/组地址的信息。SwitchD 上特定源/组地址信息显示如下：

```
[SwitchD] display igmp group ssm-mapping
IGMP SSM mapping interface group report information of VPN-Instance: public net
 Vlanif10 (133.133.4.2):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.1.1.1       133.133.4.1     00:01:44    00:00:26

[SwitchD] display igmp group ssm-mapping verbose
Interface group report information of VPN-Instance: public net
 Vlanif10 (133.133.4.2):
  Total entry on this interface: 1
  Total 1 IGMP SSM-Mapping Group reported
   Group: 232.1.1.1
     Uptime: 00:01:52
     Expires: 00:00:18
     Last reporter: 133.133.4.1
     Last-member-queryCounter: 0
     Last-member-query-timer-expiry: off
```


版权所有 © 华为技术有限公司

```
    Group mode: exclude
    Version1-host-present-timer-expiry: off
    Version2-host-present-timer-expiry: 00:00:17
```

通过使用 **display pim routing-table** 命令，可以查看 PIM-SM 组播路由表。SwitchD 上 PIM-SM 组播路由表信息显示如下：

```
[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 2 (S, G) entries
 (133.133.1.1, 232.1.1.1)
    RP: 192.168.3.2
    Protocol: pim-ssm, Flag:EXT NIIF
    UpTime: 00:11:25
    Upstream interface: Vlanif30
        Upstream neighbor: 192.168.4.2
        RPF prime neighbor: 192.168.4.2
    Downstream interface(s) information :
    Total number of downstreams: 1
        1: Vlanif13
            Protocol: igmp, UpTime: 00:11:25, Expires:-

 (133.133.3.1, 232.1.1.1)
    RP: 192.168.3.2
    Protocol: pim-ssm, Flag:EXT NIIF
    UpTime: 00:11:25
    Upstream interface: Vlanif21
        Upstream neighbor: 192.168.3.1
        RPF prime neighbor: 192.168.3.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif13
            Protocol: igmp, UpTime: 00:11:25, Expires:-
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 133.133.1.2 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20
#
interface GigabitEthernet0/0/3
```


版权所有 © 华为技术有限公司

```
 port hybrid tagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 133.133.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 11 20 31
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif11
 ip address 133.133.2.2 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 11
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 133.133.2.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 12 21 31
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif12
 ip address 133.133.3.2 255.255.255.0
 pim sm
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif21
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 12
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 21
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 133.133.3.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 13 21 30
#
 multicast routing-enable
#
interface Vlanif13
 ip address 133.133.4.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
#
interface Vlanif21
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 13
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 21
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 133.133.4.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 c-bsr vlanif30
 c-rp vlanif30
```


版权所有 © 华为技术有限公司

```
 ssm-policy 2000
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
igmp
 ssm-mapping 232.1.1.0 255.255.255.0 133.133.1.1
 ssm-mapping 232.1.1.0 255.255.255.0 133.133.3.1
#
return
```

6.6 PIM-DM（IPv4）配置

通过配置 PIM 协议，可以实现 AS 域内组播路由与数据转发。PIM-DM 是密集模式的域内组播路由协议，适用于组成员分布相对密集的小型网络。

6.6.1 PIM-DM 概述

在组成员分布非常稠密，每个网段都可能存在组成员的网络中，PIM-DM 通过周期性的“扩散—剪枝”，构建并维护一棵连接组播源和组成员的单向无环 SPT。

注意

本章只关注 IPv4 组播网络中 PIM-DM 的配置。

PIM（Protocol Independent Multicast）称为协议无关组播，表示为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何一种单播路由协议。组播路由和单播路由协议无关，只要通过单播路由协议能够产生相应组播路由表项即可。

PIM 借助 RPF（Reverse Path Forwarding）机制实现组播报文转发。RPF 机制利用现存的单播路由信息在网络中构建组播转发树。当一个组播报文到达交换机时，首先进行 RPF 检查。如果 RPF 检查失败，则将该报文丢弃。

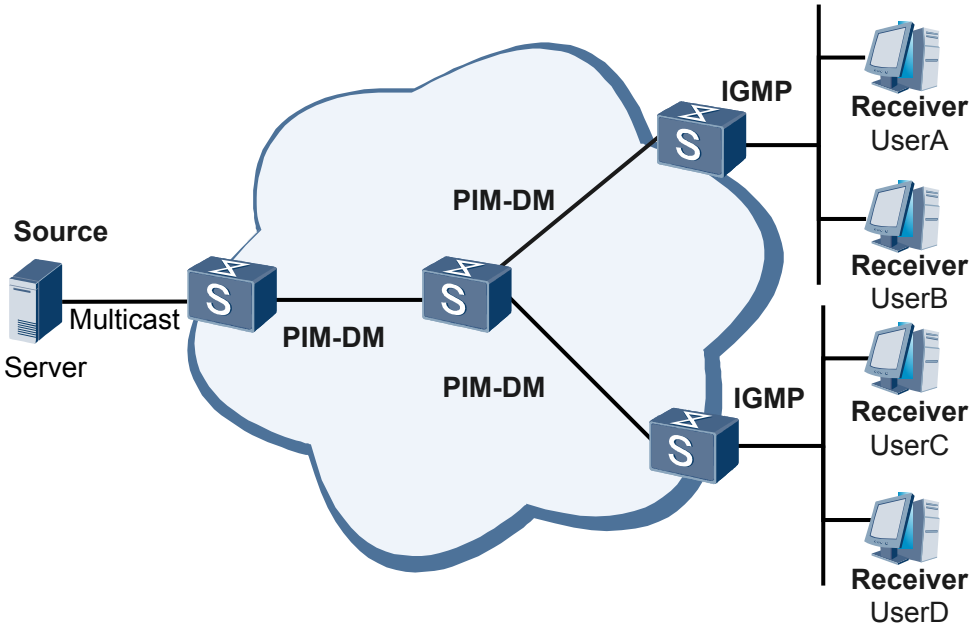
说明

关于 RPF 的详细说明请参见 **6.9 IPv4 组播路由管理**。

PIM-DM（Protocol Independent Multicast Dense Mode）称为协议独立组播－密集模式，属于密集模式的组播路由协议，适用于组成员分布相对密集的小型网络。PIM-DM 在组播网络中的作用和位置如**图 6-15** 所示。

版权所有 © 华为技术有限公司

图 6-15 PIM-DM 在组播网络中的应用示意图



对于组成员分布相对分散、范围较广、大规模的网络适用 PIM-SM（Protocol Independent Multicast-Sparse Mode）。有关 PIM-SM 的配置方法，请参见 **6.7 PIM-SM（IPv4）配置**。

6.6.2 AC6605 支持的 PIM-DM 特性

系统采用 PIM-DM 的缺省值可以正常工作，允许用户根据具体环境适当调整邻居、剪枝、状态刷新、嫁接和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-DM 的安全性。

控制组播源转发

用户可以配置组播源生存时间和组播源的过滤规则。

调整邻居控制参数

用户可以调整以下邻居控制参数：

- 发送 Hello 消息的时间间隔。
- 保持邻居为可达状态的超时时间。
- 是否接收不包含 Generation ID 选项的 Hello 消息。
- 触发 Hello 消息的最大时延。
- 邻居过滤功能。接口只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

调整剪枝控制参数

用户可以调整以下参数：

版权所有 © 华为技术有限公司

- 下游接口保持剪枝状态的时间间隔。
- 在 LAN 内，当前交换机从接收到下游发送的剪枝消息到开始实施剪枝动作的延迟时间。
- 否决剪枝时间。

调整状态刷新控制参数

用户可以禁止或使能状态刷新功能、配置发送 PIM 状态刷新消息的时间间隔、配置接收下一个状态刷新消息的最小时间间隔、在源直连交换机上配置转发状态刷新消息的 TTL 值。

调整嫁接控制参数

用户可以调整重传 Graft 消息的时间间隔。

调整 Assert 控制参数

用户可以调整交换机保持 Assert 状态的时间，落选交换机在此时间内禁止下游接口转发组播数据，超时后恢复转发。

防止主机恶意攻击功能

用户主机发送大量恶意的 PIM Hello 报文可能导致交换机瘫痪。在与用户相连的接口上配置 PIM Silent 功能，可以防止交换机受到攻击。

6.6.3 配置 PIM-DM 基本功能

在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-DM，PIM-DM 网络就可以正常运行了。

建立配置任务

在配置 PIM-DM 基本功能之前，需配置 IPv4 单播路由协议。

应用环境

PIM-DM 适用于规模较小且网络中绝大多数网段都存在接收者的网络。

前置任务

在配置 PIM-DM 基本功能之前，需配置 IPv4 单播路由协议。

数据准备

在配置 PIM-DM 基本功能之前，需准备以下数据。

序号	数据
1	欲启动 PIM-DM 功能的接口类型和编号

版权所有 © 华为技术有限公司

使能 IPv4 组播路由

使能 IPv4 组播路由是配置所有 IPv4 组播特性的首要步骤。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **multicast routing-enable**，使能公网实例 IP 组播路由。

----结束

使能 PIM-DM 功能

接口上使能了 PIM-DM 后，才可以和其他设备建立 PIM 邻居。

背景信息

说明

当交换机被部署在 PIM-DM 域中时，建议在全部非边界接口上使能 PIM-DM 功能。

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim dm**，使能 PIM-DM 功能。在接口上使能了 PIM-DM 功能后，交换机之间建立 PIM 邻居，从而才能对来自 PIM 邻居的协议报文进行处理。

使用命令 **undo pim dm** 可以取消接口上的 PIM-DM 功能。

----结束

检查配置结果

配置 PIM-DM 基本功能成功后，可以通过命令查看 PIM 接口、PIM 邻居和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看所有实例接口上的 PIM 信息。
- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看所有实例的 PIM 邻居信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行 **display pim interface verbose** 命令，查看公网实例下接口上的 PIM 详细信息。

```
<Quidway> display pim interface verbose
VPN-Instance: public net
 Interface: Vlanif117, -
     PIM version: 2
     PIM mode: Dense
     PIM state: down
     PIM DR: -
     PIM DR Priority (configured): 1
     PIM neighbor count: -
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): -
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): -
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): -
     PIM neighbor tracking (configured): disabled
     PIM generation ID: -
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM state-refresh processing: enabled
     PIM state-refresh interval: 60 s
     PIM graft retry interval: 3 s
     PIM state-refresh capability on link: capable
     PIM BFD: disabled
     PIM dr-switch-delay timer : not configured
     Number of routers on link not using DR priority: -
     Number of routers on link not using LAN delay: -
     Number of routers on link not using neighbor tracking: -
     ACL of PIM neighbor policy: -
     ACL of PIM ASM join policy: -
     ACL of PIM SSM join policy: -
```

6.6.4 调整组播源控制参数

设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置源生存时间和源地址过滤规则。

应用环境

此配置在所有应用 PIM-DM 的网络中均适用。

PIM 交换机对流经自己的组播数据进行检查，通过比较是否符合过滤规则，判断组播报文是否继续转发。这时，可以将交换机看作组播数据的过滤器。过滤器的存在一方面有助于实现数据流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。

前置任务

在控制组播源转发之前，需完成以下任务：

- 配置某单播路由协议

版权所有 © 华为技术有限公司

- 配置 PIM-DM 基本功能

数据准备

在控制组播源转发之前，需准备以下数据。

序号	数据
1	组播源生存时间
2	组播源地址过滤规则

配置源生存时间

设备为每个(S,G)表项建立一个定时器。如果设备在“源生存时间”内没有收到 S 发出的组播报文，则认为(S,G)表项失效，组播源停止向组 G 发送组播数据。

背景信息

在 PIM 交换机上进行如下配置。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **source-lifetime** *interval*，配置组播源生存时间，如果交换机在“组播源生存时间”之内没有收到（S，G）报文，则认为组播源停止向组 G 发送组播数据，（S，G）表项失效。

在使能了状态刷新的情况下，组播源生存时间会延长 *interval* 参数定义的时间。

----结束

配置源地址过滤规则

通过配置 ACL 规则，设备会根据源地址或源/组地址过滤接收的组播报文。

背景信息

在 PIM 交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **source-policy** *acl-number*，配置过滤器。设置过滤器的位置离组播源距离越近，过滤效果越明显。

版权所有 © 华为技术有限公司

如果配置的是基本 ACL，则只转发源地址属于过滤规则允许范围的组播报文。

如果配置的是高级 ACL，则只转发源地址和组地址都属于过滤规则允许范围内的组播报文。

----结束

检查配置结果

调整组播源控制参数成功后，可以通过命令查看 PIM 路由表中的表项是否符合要求。

操作步骤

- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.6.5 调整邻居控制参数

设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数，通过 Hello 消息中携带的控制参数来控制邻居关系。

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要调整 Hello 消息的相关参数来控制邻居关系，配置邻居过滤功能来提高安全性。

应用环境

PIM 交换机之间通过交互 Hello 消息建立邻居关系，协商各类控制参数。

交换机在系统缺省值的控制下可以正常工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

版权所有 © 华为技术有限公司

前置任务

在调整邻居控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整邻居控制参数之前，需准备以下数据。

序号	数据
1	邻居的超时时间
2	发送 Hello 消息的时间间隔
3	触发 Hello 消息的最大延迟
4	过滤 PIM 邻居的 ACL 号或 ACL 名字

配置发送 Hello 报文的时间间隔

发送 Hello 消息的时间间隔可以在全局和接口两种情况下配置。接口配置优于 PIM 视图下的配置，接口上未配置时 PIM 视图下的配置生效。

背景信息

在 PIM-DM 交换机上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局性
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **timer hello** *interval*，配置发送 Hello 消息的时间间隔。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim timer hello** *interval*，配置发送 Hello 消息的时间间隔。
  4. 执行命令 **pim triggered-hello-delay** *interval*，配置触发 Hello 消息的最大延迟，避免多个 PIM 交换机同时发送 Hello 消息而导致冲突。

----结束

版权所有 © 华为技术有限公司

配置邻居超时时间

邻居超时时间可以在全局和接口两种情况下配置。若超时设备仍没有收到 Hello 消息则认为邻居不可达。PIM 邻居超时时间应大于发送 Hello 消息的时间间隔。

背景信息

在 PIM-DM 交换机上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局性
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。

----结束

拒绝接收无 Generation-ID 的 Hello 报文

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变。可以配置 PIM 接口拒绝无 Generation ID 参数的 Hello 消息，从而实时了解上游邻居的状态。

背景信息

在 PIM-DM 交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim require-genid**，配置 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

版权所有 © 华为技术有限公司

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变（重启）。如果交换机不希望从上游收到数据，则在收到来自上游的数据报文后发送 Prune 消息。

----结束

配置邻居过滤

为了防止未知设备参与 PIM 协议，需要过滤 PIM 邻居。接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

背景信息

为了防止未知交换机参与 PIM 协议，需要过滤 PIM 邻居。

在运行 PIM-DM 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim neighbor-policy** *basic-acl-number*，配置邻居过滤。

----结束

检查配置结果

调整邻居控制参数成功后，可以通过命令查看 PIM 接口和 PIM 邻居是否符合要求。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看 PIM 邻居信息。

----结束

6.6.6 调整剪枝控制参数

当下游接口上最后一个组成员离开时，设备的上游接口发送 Prune 消息请求上游设备执行剪枝，同网段其他仍需要该组数据的下游设备必须发送 Join 消息来否决剪枝。

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置接口保持剪枝状态的时间、LAN 内传输 Prune 消息的延迟时间和否决剪枝的时间间隔。

版权所有 © 华为技术有限公司

应用环境

当交换机上的最后一个组成员离开时，交换机从上游接口发出 Prune 消息，请求上游交换机执行剪枝操作，停止向该交换机转发组播数据。当该网段中还存在其他下游交换机时，其他下游交换机必须发送 Join 消息，否决剪枝操作。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

剪枝的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

前置任务

在调整剪枝控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整剪枝控制参数之前，需准备以下数据。

序号	数据
1	Prune 状态的超时时间
2	传递 Prune 剪枝消息的延迟时间
3	否决剪枝的时间

配置接口保持剪枝状态的时间

接口保持剪枝状态的超时时间可以在全局和接口两种情况下配置。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。

背景信息

在 PIM-DM 交换机上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime join-prune** *interval*，配置下游接口保持剪枝状态的时间。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。
- 接口

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

   这里的接口可以是 VLANIF 接口和 Loopback 接口。
3. 执行命令 **pim holdtime join-prune** *interval*，配置下游接口保持 Prune 状态的时间。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。

----结束

配置 LAN 内传输 Prune 消息的延迟时间

LAN 内传输 Prune 消息的延迟时间可以在全局和接口两种情况下配置。当同一链路中的所有设备的 lan-delay 值不同时，将进行协商从中选取最大值。

背景信息

在 PIM-DM 交换机上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option lan-delay** *interval*，配置在 LAN 内传输 Prune 消息的延迟时间。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option lan-delay** *interval*，配置在 LAN 内传输 Prune 消息的延迟时间。

----结束

配置否决剪枝的时间间隔

当一台设备从上游接口接收到剪枝消息时，说明该 LAN 内还存在着其他的下游设备。如果该下游设备仍然需要接收组播数据，则必须在否决剪枝的时间内向上游发送 Join 消息。

背景信息

在 PIM-DM 交换机上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。

版权所有 © 华为技术有限公司

3. 执行命令 **hello-option override-interval** *interval*，配置否决剪枝的时间。

   当一台交换机从上游接口接收到剪枝消息时，说明该 LAN 内还存在着其他的下游交换机。如果这台交换机仍然需要接收组播数据，则必须在 override-interval 时间内向上游发送 Join 消息。

- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option override-interval** *interval*，配置否决剪枝的时间。

----结束

检查配置结果

调整剪枝控制参数成功后，可以通过命令查看 PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** | **state-refresh** | } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.6.7 调整状态刷新控制参数

周期性的“扩散-剪枝”将造成很大的网络资源浪费。为防止被剪枝接口因为剪枝状态超时而恢复转发，系统启用了状态刷新功能，周期性的发送 State-Refresh 消息，刷新接口剪枝状态，维持 SPT 树。

版权所有 © 华为技术有限公司

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置发送 State-Refresh 消息的时间间隔、接收下一个 State-Refresh 消息的时间和 State-Refresh 消息的 TTL 值。

应用环境

在 PIM-DM 网络中，周期性的泛滥-剪枝将造成很大的网络资源浪费。为防止被剪枝接口因为状态超时而恢复转发，AC6605 允许用户启用状态刷新功能，周期性的发送 State-Refresh 消息，刷新接口剪枝状态，维持 SPT 树。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果具体网络没有特殊要求，推荐采用缺省值。

前置任务

在调整状态刷新控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整状态刷新控制参数之前，需准备以下数据。

序号	数据
1	发送 PIM 状态刷新消息的时间间隔
2	接收下个状态刷新消息前的等待时间
3	转发状态刷新消息的 TTL 值

禁止状态刷新功能

禁止该功能后，接口不转发 State-Refresh 消息。

背景信息

在 PIM-DM 域内所有交换机上进行如下配置。

说明

缺省情况下，接口启动 PIM-DM 状态刷新功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **undo pim state-refresh-capable**，禁止 PIM-DM 状态刷新功能。禁止该功能的接口不转发状态刷新消息。

说明

使用命令 **pim state-refresh-capable** 可以重新启动接口上的 PIM-DM 状态刷新功能。

----结束

配置发送状态刷新消息的时间间隔

为了避免被剪枝接口因剪枝状态超时而恢复转发，状态刷新消息的发送间隔时间应小于保持剪枝状态的超时时间。

背景信息

在 PIM-DM 域内所有交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-interval** *interval*，配置发送 PIM 状态刷新消息的时间间隔。

说明

- 此命令适用于与组播源相连的第一跳交换机上。
- 状态刷新消息的发送间隔时间应该小于保持 Prune 状态的超时时间。
- 使用 **holdtime join-prune** 命令可以配置保持 Prune 状态的超时时间。

----结束

配置接收下一个状态刷新消息的时间

设备可能在很短的时间内收到来自多个设备的 State-Refresh 消息，而其中有些消息是重复的。状态刷新定时器超时前收到的重复消息被丢弃，超时后允许接收下一个 State-Refresh 消息。

背景信息

在 PIM-DM 域内所有交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-rate-limit** *interval*，配置接收下个状态刷新消息前的等待时间。

----结束

版权所有 © 华为技术有限公司

配置状态刷新消息的 TTL 值

设备在接收到 State-Refresh 消息后会将 TTL 值减 1，然后向下游转发，直到 TTL 值变为 0。当网络规模很小时，State-Refresh 消息将在网络中循环传递。可以根据网络规模大小配置合适的 TTL值。

背景信息

在 PIM-DM 域内所有交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-ttl** *ttl-value*，配置转发状态刷新消息的 TTL 值。

说明

此命令只在源直连交换机上配置有效。

----结束

检查配置结果

调整状态刷新控制参数成功后，可以通过命令查看 PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** | **state-refresh** | } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table brief** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

版权所有 © 华为技术有限公司

6.6.8 调整嫁接控制参数

为使网络中出现的新的组成员能够快速的接收到组播数据，设备会主动从上游接口发出Graft 消息，请求上游设备向该网段转发组播数据。

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置重传 Graft 消息的时间间隔。

应用环境

在 PIM-DM 网络中，如果未启用状态刷新功能，被剪枝接口必须等到状态超时后才会恢复转发。如果启用了状态刷新功能，则有可能永远也不会恢复转发。

为使网络中出现的新的组成员能够快速的接收到组播数据，PIM-DM 交换机会主动从上游接口发出 Graft 消息，请求上游交换机向该网段转发组播数据。上游交换机收到 Graft 消息后，立即回复 Graft-Ack 消息，并将收到该 Graft 消息的接口恢复转发。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果具体网络没有特殊要求，推荐采用缺省值。

前置任务

在调整嫁接控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整嫁接控制参数之前，需准备以下数据。

序号	数据
1	重传 Graft 嫁接消息的时间间隔

配置重传 Graft 嫁接消息的时间间隔

当有成员加入曾经被剪枝的组时，设备发出 Graft 消息，并等待上游确认。如果在一定时间内没有收到确认消息，设备将重传嫁接消息，直到收到上游的确认消息。

背景信息

在 PIM-DM 交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim timer graft-retry** *interval*，配置重传 Graft 嫁接消息的时间间隔。

当交换机在指定时间内都没有接收到来自上游的 Graft-Ack 嫁接确认消息，则会重发 Graft 嫁接消息，以期待嫁接操作得到上游交换机的确认。

----结束

检查配置结果

调整嫁接控制参数成功后，可以通过命令查看未确认的 PIM-DM 嫁接信息、PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** | **state-refresh** | } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.6.9 调整 Assert 控制参数

当设备从下游接口接收到组播数据时，说明该网段中还存在其他的上游设备。设备从该接口发出 Assert 消息，参与竞选唯一上游。

建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置保持 Assert 状态的时间。

版权所有 © 华为技术有限公司

应用环境

当 PIM-DM 交换机从下游接口接收到组播数据时，说明该网段中还存在其他的上游交换机。交换机从该接口发出 Assert 消息，参与竞选唯一上游。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 Assert 控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整 Assert 控制参数之前，需准备以下数据。

序号	数据
1	保持 Assert 状态的时间

配置保持 Assert 状态的时间

落选设备保持 Assert 状态的时间内禁止下游接口转发组播数据，超时后恢复转发。

背景信息

在 PIM-DM 交换机上进行如下配置。

说明

Assert 控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime assert** *interval*，配置保持 Assert 状态的时间。落选交换机在此时间内禁止下游接口转发组播数据，超时后恢复转发。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

这里的接口可以是 VLANIF 接口和 Loopback 接口。

3. 执行命令 **pim holdtime assert** *interval*，配置保持 Assert 状态的时间。落选交换机在此时间内禁止下游接口转发组播数据，超时后恢复转发。

----结束

检查配置结果

调整 Assert 控制参数成功后，可以通过命令查看 PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** | **state-refresh** | } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.6.10 配置防止主机恶意攻击功能（PIM Silent）

设备直连用户主机的接口上需要使能 PIM 协议，当恶意主机模拟 PIM Hello 报文，大量发送时，有可能导致设备瘫痪。为了避免这样的情况发生，可以将该接口设置为 PIM Silent 状态。

建立配置任务

网络中 PIM-DM 和 IGMP 的基本功能都已配置后，将 PIM Silent 特性配置在与主机相连的接口上，该接口使能了 PIM-DM 和 IGMP。

版权所有 © 华为技术有限公司

应用环境

在接入层上，交换机直连用户主机的接口上需要使能 PIM 协议，在该接口上可以建立 PIM 邻居，处理各类 PIM 协议报文。此配置同时存在着安全隐患：当恶意主机模拟 PIM Hello 报文，大量发送时，有可能导致交换机瘫痪。

为了避免这样的情况发生，可以将该接口设置为 PIM Silent 状态（即 PIM 消极状态）。当接口进入 PIM 消极状态后，禁止接收和转发任何 PIM 协议报文，删除该接口上的所有 PIM 邻居以及 PIM 状态机。同时，该接口上的 IGMP/MLD 功能不受影响。

该功能的使用环境是：

- 同时支持 IPv4 和 IPv6。
- 仅适用于与用户主机网段直连的交换机接口，且该用户网段只与这一台交换机相连。

注意

如果在与交换机相连的接口上启动该功能，将导致 PIM 邻居无法正常建立，引发组播故障。如果用户网段与多台交换机相连，在多个交换机接口上配置 PIM Silent，则这些接口都不会发送 Assert 消息，导致该网段存在多个组播数据转发接口，从而引发组播故障。

前置任务

在配置防止主机恶意攻击功能之前，需要完成以下任务：

- 配置单播路由协议，使网络畅通。
- 配置 PIM-DM
- 配置 IGMP

数据准备

在配置防止主机恶意攻击功能之前，需要准备以下数据。

序号	数据
1	与用户主机相连的交换机接口编号

配置 PIM Silent

配置 PIM Silent 后，接口禁止接收和转发任何 PIM 协议报文，删除该接口上的所有 PIM 邻居以及 PIM 状态机，并自动成为 DR。同时，该接口上的 IGMP 功能不受影响。

背景信息

在连接主机网段的接口上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim silent**，使能 PIM Silent 功能。可以有效的防范恶意主机 Hello 报文攻击，保护接入交换机。

----结束

检查配置结果

配置 PIM Silent 成功后，可以通过命令查看 PIM 接口信息。

前提条件

已经完成防止主机恶意攻击功能（PIM Silent）功能的所有配置。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看 PIM 接口信息。

----结束

任务示例

执行命令 **display pim interface verbose**，可以看到使能了此配置。

```
<Quidway> display pim interface Vlanif 10 verbose
VPN-Instance: public net
 Interface: Vlanif10, -
     PIM version: 2
     PIM mode: Dense
     PIM state: down
     PIM DR: -
     PIM DR Priority (configured): 1
     PIM neighbor count: -
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): -
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): -
     PIM hello override interval (configured): 2500 ms
     PIM Silent: enabled
     PIM neighbor tracking (negotiated): -
     PIM neighbor tracking (configured): disabled
     PIM generation ID: -
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM state-refresh processing: enabled
     PIM state-refresh interval: 60 s
     PIM graft retry interval: 3 s
     PIM state-refresh capability on link: capable
     PIM BFD: disabled
     PIM dr-switch-delay timer : not configured
     Number of routers on link not using DR priority: -
```


版权所有 © 华为技术有限公司

```
Number of routers on link not using LAN delay: -
Number of routers on link not using neighbor tracking: -
ACL of PIM neighbor policy: -
ACL of PIM ASM join policy: -
ACL of PIM SSM join policy: -
```

6.6.11 维护 PIM-DM（IPv4）

PIM-DM 的维护包括：清除 PIM 统计信息、监控 PIM 的运行状况。

清除 PIM 控制报文统计信息

需要重新统计 PIM 控制报文数量时，可以将已有 PIM 控制报文统计数清零，注意清除后无法恢复。此操作不影响 PIM 的正常运行。

背景信息



注意

清除接口上的 PIM 控制报文统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除接口上的 PIM 控制报文统计信息后，请在用户视图下执行 **reset pim control-message counters** [**interface** *interface-type interface-number*]命令。

----结束

监控 PIM 运行状况

在 PIM 日常维护中，可以在任意视图下选择执行 display 命令，了解 PIM 的运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 PIM 的运行状况。

操作步骤

- 在任意视图下执行 **display pim claimed-route** [*source-address*]命令，查看 PIM 使用的单播路由信息。
- 在任意视图下执行 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** } | **interface** *interface-type interface-number*] *命令，查看发送和接收 PIM 控制报文的数目信息。
- 在任意视图下执行 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令，查看接口上的 PIM 信息。
- 在任意视图下执行 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令，查看 PIM 邻居信息。命令，查看 PIM 邻居信息。
- 在任意视图下执行以下命令，查看 PIM 协议组播路由表的内容。

版权所有 © 华为技术有限公司

- **display pim routing-table brief** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

----结束

调试 PIM

出现 PIM 运行故障时，可以在用户视图下打开相应的 debugging 调试开关，查看发送和接收的报文内容，从而定位故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 PIM 运行故障时，请在用户视图下执行下面的 **debugging** 命令对 PIM 进行调试，查看调试信息，并定位故障的原因。

有关 **debugging** 命令的解释请参见《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 在用户视图下执行 **debugging pim** [**vpn-instance** *vpn-instance-name* |**all-instance**] **all** 命令，打开 PIM 所有调试信息开关。
- 在用户视图下执行 **debugging pim event** [*advanced-acl-number*]命令，打开 PIM 事件调试信息开关。
- 在用户视图下执行 **debugging pim routing-table** [*advanced-acl-number*]命令，打开 PIM 路由调试信息开关。
- 在用户视图下执行 **debugging pim neighbor** [*basic-acl-number* | [**receive** | **send**]] * 命令，打开 PIM 邻居调试信息开关。
- 在用户视图下执行 **debugging pim assert** [*advanced-acl-number* | [**receive** | **send**]] * 命令，打开 PIM Assert 调试信息开关。
- 在用户视图下执行 **debugging pim join-prune** [*advanced-acl-number* | [**receive** | **send**]] * 命令，打开 PIM Join/Prune 调试信息开关。
- 在用户视图下执行 **debugging pim state-refresh** [*advanced-acl-number* | [**receive** | **send**]] * 命令，打开 PIM State-Refresh 调试信息开关。

----结束

6.6.12 配置举例

通过配置举例，可以了解如何构建基本的 PIM-DM 网络。

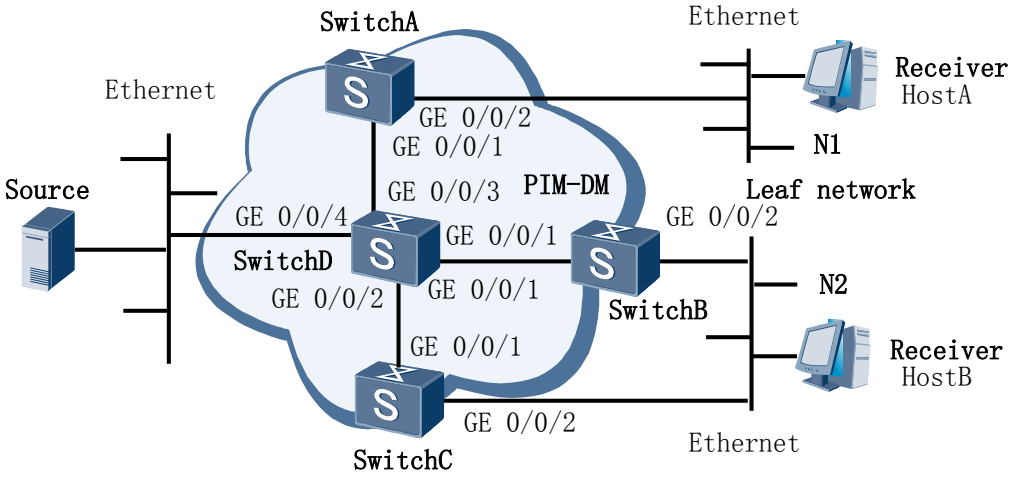
版权所有 © 华为技术有限公司

配置 PIM-DM 组播网络示例

组网需求

在如图 6-16 所示的试验网中部署组播功能。已知网络中单播运行正常。要求通过在 Switch 进行适当配置，使网络中的用户主机能够通过组播方式接收视频点播信息。

图 6-16 配置 PIM-DM 基本功能组网图



Switch	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF100	192.168.1.1/24
	GE0/0/2	VLANIF101	10.110.1.1/24
SwitchB	GE0/0/1	VLANIF200	192.168.2.1/24
	GE0/0/2	VLANIF102	10.110.2.1/24
SwitchC	GE0/0/1	VLANIF300	192.168.3.1/24
	GE0/0/2	VLANIF102	10.110.2.2/24
SwitchD	GE0/0/1	VLANIF200	192.168.2.2/24
	GE0/0/2	VLANIF300	192.168.3.2/24
	GE0/0/3	VLANIF100	192.168.1.2/24
	GE0/0/4	VLANIF103	10.110.5.1/24

配置思路

由于网络环境是规模较小的试验网，采用 PIM-DM 协议配置组播功能。在 SwitchA 与主机相连的 VLANIF 接口上使能 PIM Silent，防范 Hello 报文攻击。

1. 配置 Switch 的接口 IP 地址和单播路由协议。组播域内路由协议 PIM 是依赖单播路由协议，单播路由正常是组播协议正常工作的基础。
2. 在 Switch 上使能组播功能。
3. 在接口上使能 PIM-DM 功能。

数据准备

为完成此配置举例，需要准备如下数据：

版权所有 © 华为技术有限公司

- 组播组 G 地址：225.1.1.1/24。
- 组播源 S 地址：10.110.5.100/24。
- Switch 和用户主机之间运行的 IGMP 版本号为 2。

说明

配置用例中，只列出了与 PIM-DM 配置相关的命令。

操作步骤

步骤 1 配置各接口的 IP 地址和单播路由协议。

按照图 6-16 配置各 Switch 接口的 IP 地址和掩码，配置各 Switch 间采用 OSPF 进行互连，确保网络中各 Switch 间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。具体配置过程略。

接口 IP 地址的配置方法，请参见《AC6605 无线接入控制器 配置指南-基础配置》中 **4.1.3 配置接口的 IP 地址**，OSPF 的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 路由》中 **5.4 OSPF 配置**。

步骤 2 使能组播功能，并在各接口上使能 PIM-DM 功能。

在 SwitchA 上使能组播功能，在各接口上使能 PIM-DM 功能。SwitchB、SwitchC 和 SwitchD 上的配置过程与 SwitchA 上的配置相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] pim dm
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim dm
[SwitchA-Vlanif101] quit
```

步骤 3 在与主机相连的接口上使能 PIM Silent，配置 IGMP。

在 SwitchA 连接用户主机的 VLANIF 接口上使能 PIM Silent，配置 IGMP 功能。SwitchB 和 SwitchC 上的配置过程与 SwitchA 上的配置相似，配置过程略。

```
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim silent
[SwitchA-Vlanif101] igmp enable
[SwitchA-Vlanif101] quit
```

步骤 4 验证配置结果。

通过使用 **display pim interface** 命令可以查看 Switch 接口上 PIM 的配置和运行情况。例如 SwitchD 上 PIM 配置的显示信息如下：

```
[SwitchD] display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif103        up        0         30         1      10.110.5.1(local)
Vlanif100        up        0         30         1      192.168.1.2(local)
Vlanif200        up        1         30         1      192.168.2.2(local)
Vlanif300        up        1         30         1      192.168.3.2(local)
```

通过使用 **display pim neighbor** 命令可以查看 Switch 之间的 PIM 邻居关系。例如 SwitchD 上 PIM 邻居关系的显示信息如下：

```
[SwitchD] display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 3

 Neighbor        Interface         Uptime       Expires      Dr-Priority   BFD-Session
```


版权所有 © 华为技术有限公司

```
192.168.1.1      Vlanif100          00:02:22    00:01:27      1             N
192.168.2.1      Vlanif200          00:00:22    00:01:29      1             N
192.168.3.1      Vlanif300          00:00:23    00:01:31      1             N
```

通过使用 **display pim routing-table** 命令可以查看 PIM 协议组播路由表。假如 HostA 需要接收组播组 G（225.1.1.1/24）的信息。当组播源 S（10.110.5.100/24）向组播组 G 传送组播报文时，通过扩散生成 SPT，SPT 路径中 SwitchA 和-SwitchD 上都存在（S，G）表项，HostA 加入组播组 G，在 SwitchA 上生成（*，G）表项，SwitchB 和 SwitchC 上的显示信息和 SwitchA 类似。显示信息如下：

```
[SwitchA] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
     UpTime: 03:54:19
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif101
             Protocol: igmp, UpTime: 01:38:19, Expires: never

(10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: Vlanif100
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: Vlanif101
              Protocol: pim-dm, UpTime: 00:00:44, Expires: never

[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: LOC ACT
     UpTime: 01:35:25
     Upstream interface: Vlanif103
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
        1: Vlanif100
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
        2: Vlanif200
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 multicast routing-enable
#
vlan batch 100 101
#
interface Vlanif100
```


版权所有 © 华为技术有限公司

```
 ip address 192.168.1.1 255.255.255.0
 pim dm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim dm
 pim silent
 igmp enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 200 102
#
interface Vlanif102
 ip address 10.110.2.1 255.255.255.0
 pim dm
 igmp enable
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
 pim dm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 multicast routing-enable
#
vlan batch 102 300
#
interface Vlanif102
 ip address 10.110.2.2 255.255.255.0
 pim dm
 igmp enable
#
interface Vlanif300
```


版权所有 © 华为技术有限公司

```
 ip address 192.168.3.1 255.255.255.0
 pim dm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 multicast routing-enable
#
vlan batch 100 103 200 300
#
interface Vlanif 100
 ip address 192.168.1.2 255.255.255.0
 pim dm
#
interface Vlanif 103
 ip address 10.110.5.1 255.255.255.0
 pim dm
#
interface Vlanif 200
 ip address 192.168.2.2 255.255.255.0
 pim dm
#
interface Vlanif 300
 ip address 192.168.3.2 255.255.255.0
 pim dm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid tagged vlan 100
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

6.7 PIM-SM（IPv4）配置

通过配置 PIM 协议，可以实现 AS 域内组播路由与数据转发。PIM-SM 是稀疏模式的域内组播路由协议，适用于组成员分布相对分散、范围较广的大规模网络。

6.7.1 PIM-SM 概述

在组成员分布非常稀疏，几乎所有网段均不存在组成员的网络中，RP 是 PIM-SM 网络的转发核心，网络中所有 PIM 设备都知道 RP 的位置，组成员和组播源的信息都向 RP 汇聚。

PIM（Protocol Independent Multicast）称为协议无关组播，表示为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何单播路由协议。组播路由和单播路由协议无关，只是通过单播路由表产生相应组播路由表项。

PIM 借助 RPF（Reverse Path Forwarding）机制实现组播报文转发。RPF 机制利用现存的单播路由信息在网络中构建组播转发树。当一个组播报文到达交换机时，首先进行 RPF 检查。RPF 检查通过，则创建相应组播路由表项，从而进行组播报文转发。RPF 检查失败，则将该报文丢弃。

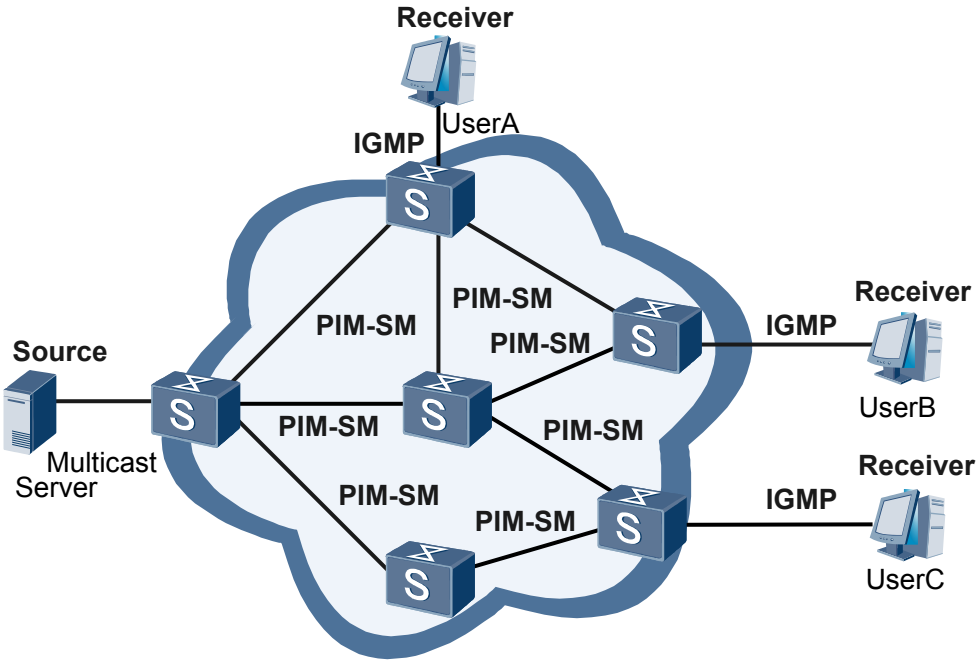
说明

关于 RPF 的详细说明请参见《AC6605 **IPv4 组播路由管理**》。

PIM-SM（Protocol Independent Multicast-Sparse Mode）称为协议无关组播－稀疏模式，属于稀疏模式的组播路由协议。PIM-SM 的工作过程主要有：邻居发现、Assert、DR 选举、RP 发现、加入、剪枝、注册、SPT 切换。

如图 6-17 所示，PIM-SM 适用于组成员分布相对分散、范围较广、大规模的网络。

图 6-17 PIM-SM 在组播网络中的应用



版权所有 © 华为技术有限公司

说明

- 对于组成员分布相对密集的小型网络适用 PIM-DM（Protocol Independent Multicast Dense Mode）。
- 使用 PIM-SM 协议，可以构建 ASM（Any-Source Multicast）和 SSM（Source-Specific Multicast）两种组播模型。

6.7.2 AC6605 支持的 PIM-SM 特性

系统允许用户根据具体环境适当调整邻居、转发、DR、RP、加入、注册和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-SM 的安全性。PIM-SM 网络支持 SSM、PIM BFD、PIM GR 和 SPT 切换。

PIM-SM 基本功能

PIM-SM 支持 ASM 和 SSM 两种组播模型，用户可以根据需要配置 ASM 或 SSM 组地址的范围。

静态 RP

用户可以在 PIM-SM 域的所有交换机上指定静态 RP。当域内存在动态 RP 时，缺省的是动态 RP 优先，但用户可以通过配置来优先使用静态 RP。

控制组播源

用户可以通过配置组播源地址过滤规则来控制组播源。还可以通过策略过滤 Register 报文，抑制 PIM-SM 注册消息。

调整 PIM-SM 邻居参数

用户可以调整 PIM-SM 邻居之间的控制参数，包括：

- 发送 Hello 报文的时间间隔。
- 保持邻居状态为可达的超时时间。
- 是否接收包含 Generation ID 的 Hello 消息。
- 触发 Hello 消息的最大延迟时间。
- 竞选 DR 的优先级。
- DR 切换延迟时间。
- 邻居过滤功能。接口上只与符合过滤规则的地址建立邻居关系。

调整转发控制参数

用户可以调整转发控制参数，包括：

- 发送 Join 消息的时间间隔。
- 下游接口保持转发状态的时间。
- 否决剪枝的时间。
- 过滤 Join/Prune 消息中的 Join 信息。
- 邻居检查功能。接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果不是则不处理。

版权所有 © 华为技术有限公司

调整 Assert 控制参数

用户可以配置交换机接口保持 Assert 状态的时间。

调整 SPT 切换参数

用户可以调整检测组播数据转发速率的时间间隔和 SPT 切换的条件。

PIM BFD

AC6605 支持 PIM 邻居之间动态创建 BFD 会话检测邻居之间的链路状态，一旦有故障，BFD 会把结果直接通告给 PIM。

6.7.3 配置 PIM-SM 基本功能

在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-SM，在网络中配置静态 RP 或动态 RP，PIM-SM 网络就可以正常运行了。

建立配置任务

在配置 PIM-SM 基本功能之前，需配置 IPv4 单播路由协议。

应用环境

一个 PIM-SM 网络可以同时采用 ASM 与 SSM 模型为用户主机提供组播服务。首先必须在网络中配置完备的 ASM 模型部件，包括 RP。然后根据实际需要调整 SSM 组地址范围。

说明

SSM 模型需要 IGMPv3 版本的支持。如果用户主机必须运行 IGMPv1 或 v2，则需要在交换机接口上配置 IGMP SSM Mapping。

交换机通过 IGMP 得知用户希望加入的组播组 G。

- 如果 G 在 SSM 组地址范围内，且用户通过 IGMPv3 加入组 G 时明确指定了 S。则采用 SSM 模型提供组播服务。
- 如果 G 在 SSM 组地址范围内，且交换机上静态配置了（S，G）SSM Mapping 规则。则采用 SSM 模型提供组播服务。
- 如果 G 在 SSM 组地址范围外，则采用 ASM 模型提供组播服务。

PIM-SM 中的 ASM 模型支持两种获得 RP 的方法，用户根据需要选择配置即可：

- 静态 RP：必须在 PIM-SM 域内的每一台交换机上手动配置 RP。对于大型 PIM 网络，配置静态 RP 将会非常繁琐。所以，通常只将静态 RP 作为动态 RP 的备份，用来提高网络的健壮性，增强组播网络的运营管理能力。

一个组播组可能同时属于动态 RP 和静态 RP 的服务范围。缺省情况下，交换机优先选取动态 RP，如果配置了静态 RP 优先，则优先选用静态 RP。

不同的组播组对应不同的 RP，与所有组播组对应同一个 RP 相比，可以减轻单个 RP 的负荷，增强网络的健壮性。

前置任务

在配置 PIM-SM 基本功能之前，需完成以下任务：

版权所有 © 华为技术有限公司

- 配置单播路由协议

数据准备

在配置 PIM-SM 基本功能之前，需准备以下数据。

序号	数据
1	静态 RP 地址
2	定义了静态 RP 所服务的组播组范围的 ACL
3	C-RP 的优先级
4	定义了 C-RP 所服务的组播组范围的 ACL
5	C-RP 发送 Advertisement 宣告消息的间隔时间
6	BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间
7	C-BSR 的哈希掩码长度
8	C-BSR 的优先级
9	SSM 组地址范围

使能 IP 组播路由

使能 IPv4 组播路由是配置所有 IPv4 组播特性的首要步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **multicast routing-enable**，使能公网实例 IP 组播路由。

----结束

使能 PIM-SM 功能

接口上使能了 PIM-SM 后，才可以和其他设备建立 PIM 邻居。

背景信息

说明

当交换机被部署在 PIM-SM 域中时，建议在全部非边界接口上使能 PIM-SM 功能。

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim sm**，使能 PIM-SM 功能。在接口上使能了 PIM-SM 功能后，交换机之间建立 PIM 邻居，从而才能对来自 PIM 邻居的协议报文进行处理。

----结束

（可选）配置静态 RP

当网络内仅有一个 RP 时，可以手工配置静态 RP，这样可以避免 C-RP 和 BSR 之间频繁的信息交互占用带宽。PIM-SM 域内所有设备都必须配置完全相同的静态 RP。

背景信息

注意

在 PIM-SM 网络中同时配置静态 RP 和动态 RP，容易引发网络故障，请慎重选择是否进行此项配置。若希望在 PIM-SM 网络中仅使用动态 RP，则跳过此项配置。

在 PIM-SM 域中所有交换机上进行如下配置。未配置静态 RP 的交换机不能参与此 PIM-SM 域内的组播转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **static-rp** *rp-address basic-acl-number* [**preferred**]，指定静态 RP。重复执行该命令可以为交换机配置多个静态 RP。

----结束

（可选）配置动态 RP

在 PIM-SM 域内选择几台 PIM 设备配置 C-RP，从 C-RP 中竞选产生 RP。必须同时配置 C-BSR，由 C-BSR 竞选产生 BSR，BSR 负责收集并发布网络中的 C-RP 信息。系统支持 Auto-RP 监听功能。

背景信息

注意

此项配置只适用于动态 RP，若希望网络中仅使用静态 RP，请跳过此项配置。

在 PIM-SM 域中有待成为 RP 的交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **c-rp** *interface-type interface-number* [**group-policy** *basic-acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *，配置 C-RP。

- *interface-type interface-number* 为 C-RP 所在接口，该接口必须使能 PIM-SM。
- **priority** *priority* 为 C-RP 的竞选优先级，数值越大，优先级越低。缺省值是 0。

  在 RP 选举中，优先级较高的 C-RP 较优；优先级相同的情况下，执行 Hash 函数，计算结果较大者获胜；如果 Hash 函数计算结果也相同，比较 IP 地址，IP 地址较高者较优。

  说明

  推荐将 Loopback 接口配置为 RP。

  如果配置了接口地址借用，不建议将地址相同的接口同时配置为 C-RP。因为若优先级不相同，BSR 会认为 C-RP 的配置在不停的被修改。
- **holdtime** *hold-interval* 为 BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间。缺省值是 150 秒。
- **advertisement-interval** *adv-interval* 为 C-RP 发送 Advertisement 宣告消息的时间间隔。缺省值是 60 秒。

步骤 4 执行命令 **c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]，配置 C-BSR。

- *interface-type interface-number* 为 C-BSR 所在接口，该接口必须使能 PIM-SM。
- *hash-length* 为哈希掩码长度。交换机根据组地址 G、C-RP 的地址和 *hash-length*，运用 Hash 函数，对希望为组 G 服务且优先级相同的 C-RP 逐一进行计算，并比较计算结果。计算结果最大者成为真正为组 G 提供服务的 RP。
- *priority* 为候选优先级，数值越大，优先级越高。缺省值是 0。

  在 BSR 选举中，优先级较大者较优；优先级相同的情况下，IP 地址较高者较优。

步骤 5 （可选）执行命令 **bsm semantic fragmentation**，使能 BSR 报文分片功能。

推荐网络中所有设备都使能 BSR 报文分片功能，可以解决 IP 分片时，分片信息丢失而导致所有分片不可用的问题。

步骤 6 （可选）执行命令 **auto-rp listening enable**，使能 Auto-RP 监听功能。

当交换机与支持 Auto-RP 的设备互通时，需要配置此命令。

----结束

（可选）配置 SSM 组播组地址范围

SSM 的组地址缺省范围是 232.0.0.0/8，可以手工配置 SSM 组播组地址范围。需要确保网络内所有设备配置的 SSM 组地址范围都一致。

背景信息

在 PIM-SM 网络中的所有交换机上进行如下配置。此项配置可选，缺省范围是 232.0.0.0/8。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **ssm-policy** *basic-acl-number*，配置 SSM 组地址范围。

说明

确保网络内所有交换机上配置的 SSM 组地址范围都一致。

----结束

检查配置结果

配置 PIM-SM 基本功能成功后，可以通过命令查看 BSR、RP、PIM 接口、PIM 邻居和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看 PIM 邻居信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *
- 使用 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

6.7.4 调整组播源控制参数

设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置源生存时间和源地址过滤规则。

版权所有 © 华为技术有限公司

应用环境

本节所有配置同时适用于 ASM 模型和 SSM 模型。

PIM 交换机对流经自己的组播数据进行检查，通过比较是否符合过滤规则，判断组播报文是否继续转发。这时，可以将交换机看作组播数据的过滤器。过滤器的存在一方面有助于实现数据流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在控制组播源转发之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在控制组播源转发之前，需准备以下数据。

序号	数据
1	组播源生存时间
2	组播源地址过滤规则

配置源生存时间

设备为每个(S,G)表项建立一个定时器。如果设备在“源生存时间”内没有收到 S 发出的组播报文，则认为(S,G)表项失效，从而无法接收到组 G 发送的组播数据。

背景信息

在 PIM 交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **source-lifetime** *interval*，配置组播源生存时间，超时则（S，G）表项失效。

----结束

配置源地址过滤

通过配置 ACL 规则，设备会根据源地址或源/组地址过滤接收的组播报文。

版权所有 © 华为技术有限公司

背景信息

在 PIM 交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **source-policy** *acl-number*，配置过滤器。

如果配置的是基本 ACL，则只转发源地址属于过滤规则允许范围的组播报文。

如果配置的是高级 ACL，则只转发源地址和组地址都属于过滤规则允许范围内的组播报文。

----结束

检查配置结果

调整组播源控制参数成功后，可以通过命令查看 PIM 路由表中的表项是否符合要求。

操作步骤

- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.7.5 调整 C-RP 和 C-BSR 的控制参数

使用动态 RP 时，可以根据实际网络情况调整 C-RP 和 C-BSR 的各项参数。如无特殊要求，推荐使用缺省值。

建立配置任务

使用动态 RP 配置 PIM-SM 基本功能后，可以根据实际需要调整 C-RP 和 C-BSR 的参数、配置 BSR 服务边界和合法 BSR、C-RP 的地址范围。

应用环境

本节介绍在 ASM 模型中如何通过命令调整 C-RP 和 C-BSR 的控制参数。

说明

此项配置仅适用于 BSR-RP，若希望 PIM-SM 网络中仅使用静态 RP，请跳过本节。

版权所有 © 华为技术有限公司

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 C-RP 和 C-BSR 的控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整 RP 和 BSR 的各项参数之前，需准备以下数据。

序号	数据
1	C-RP 的优先级
2	C-RP 发送 Advertisement 宣告消息的间隔时间
3	BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间
4	C-BSR 的哈希掩码长度
5	C-BSR 的优先级
6	C-BSR 发送 Bootstrap 自举消息的间隔时间
7	保持来自 BSR 的 Bootstrap 自举消息的时间
8	定义了合法 BSR 的地址范围的 ACL

调整 C-RP 参数

C-RP 向 BSR 周期性发送 Advertisement 消息，Advertisement 消息中携带 C-RP 优先级等信息。可以在配置了 C-RP 的设备上调整 C-RP 优先级、发送 Advertisement 消息的周期、Advertisement 消息的有效时间。

背景信息

在已经配置了 C-RP 的交换机上进行如下配置。

说明

此项配置可以重新设置 C-RP 的各项参数。此项配置可选。如果没有特殊要求，推荐使用缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **c-rp priority** *priority*，配置 C-RP 优先级。

步骤 4 执行命令 **c-rp advertisement-interval** *interval*，配置 C-RP 发送 Advertisement 宣告消息的间隔时间。

步骤 5 执行命令 **c-rp holdtime** *interval*，配置保持来自 C-RP 的 Advertisement 宣告消息的时间。该参数值必须大于“C-RP 发送 Advertisement 宣告消息的间隔时间”。

C-RP 向竞选获胜的 BSR 周期性地发送 Advertisement 宣告消息。BSR 接收到这些宣告消息后，从中会读出 C-RP 的保持时间，即在此时间段内 C-RP 有效，超过该时间段，此 C-RP 老化。

----结束

调整 C-BSR 参数

最初，每个 C-BSR 都认为自己是 BSR，向所有设备发送 Bootstrap 消息。可以在配置了 C-BSR 的设备上调整 Bootstrap 消息中携带的 C-BSR 哈希掩码长度、C-RP 优先级、发送 Bootstrap 消息的周期、Bootstrap 消息的有效时间。

背景信息

在已经配置了 C-BSR 的交换机上进行如下配置。

说明

此项配置可以重新设置 C-BSR 的各项参数。此项配置可选。如果没有特殊要求，推荐使用缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **c-bsr hash-length** *hash-length*，配置 C-BSR 的哈希掩码长度。

步骤 4 执行命令 **c-bsr priority** *priority*，配置 C-BSR 的优先级。

步骤 5 执行命令 **c-bsr interval** *interval*，配置 BSR 发送 Bootstrap 自举消息的间隔时间。

步骤 6 执行命令 **c-bsr holdtime** *interval*，配置保持来自 BSR 的 Bootstrap 自举消息时间。

BSR 周期性地向网络发送自举消息，接收到该消息的交换机会将自举消息保持一段时间，在该时间内 BSR 选举过程暂停；如果保持时间超时，则 C-BSR 之间会触发新一轮 BSR 选举过程。

说明

确保“保持来自 BSR 的 Bootstrap 自举消息时间”大于“BSR 发送 Bootstrap 自举消息的间隔时间”，否则，将导致 BSR 选举不稳定。

----结束

配置 BSR 服务边界

可以在接口上配置 BSR 服务边界，Bootstrap 消息无法通过 BSR 服务边界。众多 BSR 边界接口将网络划分成不同的 PIM-SM 域。

版权所有 © 华为技术有限公司

背景信息

在有待成为 BSR 服务边界的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim bsr-boundary**，配置 BSR 服务边界。BSR 消息无法通过 BSR 区域边界。

缺省情况下，网络中的所有 PIM-SM 交换机都能收到 BSR 消息。

----结束

（可选）配置合法 BSR 的地址范围

在所有设备上通过 ACL 设置 C-BSR 地址的过滤策略，只有 Bootstrap 消息的源地址在合法地址范围内时，才接收 Bootstrap 消息，从而防止 BSR 欺骗。

背景信息

在 PIM-SM 域中所有交换机上进行如下配置。

说明

缺省情况下,不检查 BSR 报文源地址,一律接收。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **bsr-policy** *basic-acl-number*，限定合法 BSR 地址范围。当交换机接收到封装了 Bootstrap 消息的 IP 报文时，检查报文源地址。如果源地址在合法地址范围之外，则丢弃该报文，从而防止 BSR 欺骗。

----结束

（可选）配置合法 C-RP 的地址范围

在所有 C-BSR 上通过 ACL 设置 C-RP 地址和 C-RP 所服务的组地址的过滤策略，只有 C-RP 地址和所服务的组地址都在合法地址范围内时，才将 C-RP 信息收入 RP-Set，从而防止 C-RP 欺骗。

背景信息

在 PIM-SM 域中所有 C-BSR 上进行如下配置。

说明

缺省情况下，不检查 Advertisement 消息包含的 C-RP 地址和所服务的组地址，一律收入 RP-Set。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **crp-policy** *advanced-acl-number*，限定合法的 C-RP 地址范围及其服务的组播组地址范围。当交换机接收到 Advertisement 消息时，检查消息中包含的 C-RP 地址和所服务的组地址。只有 C-RP 地址和所服务的组地址都在合法地址范围之内时，才收入 RP-Set，从而防止 C-RP 欺骗。

----结束

检查配置结果

调整 C-RP 和 C-BSR 的控制参数成功后，可以通过命令查看 BSR 和 RP 的信息，接口上是否配置了 BSR 服务边界。

操作步骤

- 使用 **display pim bsr-info** 命令查看 PIM-SM 域中 BSR 自举交换机的信息。
- 使用 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

6.7.6 配置 BSR 管理域

将 PIM-SM 网络划分为多个 BSR 管理域和一个 Global 域，可以分担单一 BSR 的管理压力，还可以使用私有组地址为特定区域的用户提供专门服务。

建立配置任务

使用动态 RP 配置 PIM-SM 基本功能后，可以根据实际需要配置 BSR 管理域。每个 BSR 管理域中维护一个 BSR，为特定范围的组播组服务，不属于任何 BSR 管理域的组播组，都属于 Global 域的服务范围。

应用环境

本节介绍在 ASM 模型中如何通过命令配置 BSR 管理域。

缺省情况下，PIM-SM 网络中只有一个 BSR，整个网络都在该 BSR 的管理范围内。为了更好的、有针对性地管理网络，可以在 PIM-SM 网络中设置多个 BSR 管理域。每个 BSR 管理域中维护一个 BSR，为特定范围的组播组服务，属于此范围的组播报文无法通过 BSR 管理域边界。

不同的 BSR 管理域服务的组播组范围可以重叠，该组播组只在本管理域内有效，相当于私有组地址。

不属于任何 BSR 管理域的组播组，一律属于 Global 域的服务范围。Global 域中维护一个 BSR，为所有剩余的组播组服务。

将一个统一的 PIM-SM 网络划分为多个 BSR 管理域和一个 Global 域，一方面有效分担单一 BSR 的管理压力，另一方面可以使用私有组地址为特定区域提供专门服务。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

版权所有 © 华为技术有限公司

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置 BSR 管理域之前，需完成以下任务：

- 配置单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在配置 BSR 管理域之前，需准备以下数据。

序号	数据
1	候选 PIM-SM 某管理域 BSR 的优先级和哈希掩码长度
2	候选 Global 域 BSR 的优先级和哈希掩码长度

使能 BSR 管理域

在 PIM-SM 网络中所有设备上使能 BSR 管理域功能。

背景信息

在 PIM-SM 网络中所有交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **c-bsr admin-scope**，使能在 PIM-SM 网络的中划分 BSR 管理域。

----结束

配置 BSR 管理域边界

在接口上配置 BSR 管理域边界后，属于该 BSR 管理域的组播报文无法通过此边界。

背景信息

在有待成为 BSR 服务边界的交换机上进行如下配置。

说明

BSR 管理域边界之外的交换机不能转发属于此 BSR 管理域的组播报文。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **multicast boundary** *group-address* { *mask* | *mask-length* }，配置 BSR 管理域边界。属于该 BSR 管理域的组播报文无法通过此边界。

----结束

调整 C-BSR 参数

可以根据实际需要调整 BSR 管理域和 Global 域的 C-BSR 参数。

背景信息

在所有 C-BSR 上进行如下配置。

说明

C-BSR 参数在三种情况配置：

- 全局。请参见**调整 C-RP 和 C-BSR 的控制参数**。全局值在 Global 域和各 BSR 域中都有效。
- BSR 管理域。针对 BSR 管理域的取值优于全局值，未配置 BSR 管理域值时继承全局值。
- Global 域。针对 Global 域的取值优于全局值，未配置 Global 域值时继承全局值。

操作步骤

- BSR 管理域
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **c-bsr group** *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *，配置 C-BSR 参数。
     - *group-address* { *mask* | *mask-length* }为 C-BSR 服务的组播组范围。有效的组范围在 239.0.0.0/8 之内。
     - **hash-length** *hash-length* 为 C-BSR 的哈希掩码长度。
     - **priority** *priority* 为 C-BSR 的优先级。
- Global 域
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *，配置 C-BSR 参数。
     - **hash-length** *hash-length* 为 C-BSR 的哈希掩码长度。
     - **priority** *priority* 为 C-BSR 的优先级。

----结束

检查配置结果

配置 BSR 管理域成功后，可以通过命令查看 BSR 和 RP 的信息。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display pim bsr-info** 命令查看 PIM-SM 域中 BSR 的信息。
- 使用 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

6.7.7 调整邻居控制参数

设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数。可以根据实际需要调整 Hello 消息中携带的参数，若无特殊要求推荐采用缺省值。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要调整 Hello 消息的相关参数来控制邻居关系，配置跟踪下游邻居和邻居过滤功能。

应用环境

本节所有配置同时适用于 ASM 模型和 SSM 模型。

PIM 交换机之间通过交互 Hello 消息建立邻居关系，协商各类控制参数，并选举 DR。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置邻居控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整邻居控制参数之前，需准备以下数据。

序号	数据
1	竞选成为 DR 的优先级
2	等待接收邻居发送 Hello 消息的超时时间
3	发送 Hello 消息的时间间隔
4	触发 Hello 消息的最大延迟
5	DR 切换延迟，即当接口由 DR 变成非 DR 时，原有表项仍然有效的时间
6	过滤 PIM 邻居的 ACL 号或 ACL 名字

版权所有 © 华为技术有限公司

配置 PIM 邻居控制参数

发送 Hello 消息的时间间隔可以在全局和接口两种情况下配置。接口配置优于 PIM 视图下的配置，接口上未配置时 PIM 视图下的配置生效。

背景信息

在 PIM-SM 交换机上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **timer hello** *interval*，配置发送 Hello 消息的时间间隔。
  4. 执行命令 **hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim timer hello** *interval*，配置发送 Hello 消息的时间间隔。
  4. 执行命令 **pim triggered-hello-delay** *interval*，配置触发 Hello 消息的最大延迟，避免多个 PIM 交换机同时发送 Hello 消息而导致冲突。
  5. 执行命令 **pim hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。
  6. 执行命令 **pim require-genid**，配置接收的 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

     缺省情况下，交换机接受无 Generation ID 选项的 Hello 消息。

----结束

配置竞选 DR 的控制参数

竞选 DR 的控制参数可以在全局和接口两种情况下配置。

背景信息

在 PIM-SM 交换机上进行如下配置。

版权所有 © 华为技术有限公司

说明

竞选 DR 的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option dr-priority** *priority*，配置竞选 DR 的优先级。

     当同一网段内的所有 PIM 交换机都支持 DR 优先级的时候，由优先级较高的交换机接口充当 DR，优先级相同时由 IP 地址较大的交换机接口充当 DR；只要有一台 PIM 交换机不支持 DR 优先级，则由 IP 地址较大的交换机接口充当 DR。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option dr-priority** *priority*，配置竞选 DR 的优先级。

     当同一网段内的所有 PIM 交换机都支持 DR 优先级的时候，由优先级较高的交换机接口充当 DR，优先级相同时由 IP 地址较大的交换机接口充当 DR；只要有一台 PIM 交换机不支持 DR 优先级，则由 IP 地址较大的交换机接口充当 DR。
  4. 执行命令 **pim timer dr-switch-delay** *interval*，配置 DR 切换延迟，并指定延迟时间。当接口由 DR 变成非 DR 时，原有表项仍然有效直到延迟时间超时。

     缺省情况下，当接口由 DR 变为非 DR 时，立即删除 PIM 路由表项。

----结束

使能跟踪下游邻居功能

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变。可以配置 PIM 接口拒绝无 Generation ID 参数的 Hello 消息，从而实时了解上游邻居的状态。

背景信息

在运行 PIM-SM 的交换机上进行如下配置。

说明

配置跟踪下游邻居功能可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

版权所有 © 华为技术有限公司

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option neighbor-tracking**，使能跟踪下游邻居功能，记录已经发送了加入报文并且该加入状态还没有超时的下游邻居信息。

     说明

     除非共享网段中的所有 PIM 交换机都使能该能力，否则邻居跟踪功能无法实现。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option neighbor-tracking**，使能跟踪下游邻居功能，记录已经发送了加入报文并且该加入状态还没有超时的下游邻居信息。

     说明

     除非共享网段中的所有 PIM 交换机都使能该能力，否则邻居跟踪功能无法实现。

----结束

配置邻居过滤

为了防止未知设备参与 PIM 协议，需要过滤 PIM 邻居。接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

背景信息

为了防止未知交换机参与 PIM 协议，阻止本交换机成为 DR，需要过滤 PIM 邻居。

在运行 PIM-SM 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim neighbor-policy** *basic-acl-number*，配置邻居过滤。

----结束

检查配置结果

调整邻居控制参数成功后，可以通过命令查看 PIM 接口和 PIM 邻居是否符合要求。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。

版权所有 © 华为技术有限公司

- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看 PIM 邻居信息。

----结束

6.7.8 调整源注册控制参数

与组播源直连的 DR 将接收到的组播数据逐一封装到 Register 消息中，以单播方式发送到 RP。RP 将解封装后的组播数据沿 RPT 转发到接收者。系统允许配置 Register 消息过滤和注册抑制功能。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置 Register 消息的过滤规则和校验方式，配置注册抑制。

应用环境

本节介绍在 ASM 模型中如何通过命令配置源注册控制参数。

在 PIM-SM 网络中，与组播源 S 直连的 DR 将接收到的组播数据逐一封装到 Register 消息中，以单播方式发送到 RP。RP 将解封装后的组播数据沿 RPT 转发到接收者。

当 RP 上的 SPT 切换完成后，组播数据以组播方式沿 SPT 到达 RP。这时，RP 向组播源侧 DR 发送 Register-stop 消息，SDR 停止发送 Register 注册消息并进入注册抑制状态。在注册抑制期间，SDR 向 RP 周期性的发送空注册消息以通告组播源仍处于激活状态；注册抑制超时后，SDR 重新开始发送 Register 注册消息。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置源注册控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在配置源注册控制参数之前，需准备以下数据：

序号	数据
1	RP 过滤 Register 注册报文的 ACL 规则
2	是否仅根据 Register 注册报文头信息计算校验和
3	保持 Register 注册抑制状态的超时时间
4	向 RP 发送空 Register 注册消息的时间间隔

版权所有 © 华为技术有限公司

配置 PIM-SM 注册报文

可以在所有可能成为 RP 的设备上，配置 Register 消息过滤规则。缺省情况下根据整个 Register 消息来计算校验和，可以配置仅根据 Register 注册消息头信息来计算校验和。

背景信息

在所有可能成为 RP 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **register-policy** *advanced-acl-number*，配置过滤 Register 注册报文的规则。RP 根据此规则来过滤接收到的注册报文。

步骤 4 执行命令 **register-header-checksum**，配置仅根据 Register 注册消息头信息来计算校验和。未通过校验的 Register 注册消息将被丢弃。缺省情况下根据整个消息来计算校验和。

----结束

配置 PIM-SM 注册抑制

可以在所有可能成为组播源侧 DR 的设备上，配置保持注册抑制状态的超时时间和发送空注册消息的时间间隔。

背景信息

在所有可能成为组播源侧 DR 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **register-suppression-timeout** *interval*，配置保持注册抑制状态的超时时间。

步骤 4 执行命令 **probe-interval** *interval*，配置发送空注册消息的时间间隔。

----结束

检查配置结果

调整源注册控制参数成功后，可以通过命令查看 PIM 接口信息。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。

----结束

版权所有 © 华为技术有限公司

6.7.9 调整转发控制参数

设备向上游发送 Join 消息请求转发组播数据，发送 Prune 消息请求停止转发组播数据。可以根据实际需要调整转发控制参数，若无特殊需要，推荐使用缺省值。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要调整维护转发关系的控制参数，配置 Join 信息过滤和邻居检查功能来提高安全性。

应用环境

若无特殊说明，本节各项配置同时适用于 ASM 模型和 SSM 模型。

当交换机上出现第一个组成员时，交换机从上游接口发出 Join 消息，请求上游交换机向该网段转发组播报文。

当交换机上的最后一个组成员离开时，交换机从上游接口发出 Prune 消息，请求上游交换机执行剪枝操作，停止向该网段转发组播报文。当该网段中还存在其他下游交换机时，其他下游交换机必须发送 Join 消息，否决剪枝操作。

在 ASM 模型中，交换机周期性的向 RP 发送 Join 消息，避免 RPT 分支因为超时而被删除。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整转发控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整转发控制参数之前，需准备以下数据。

序号	数据
1	传递 Prune 剪枝消息的延迟时间
2	否决剪枝的时间
3	Prune 状态的超时时间
4	发送 Join 消息的时间间隔
5	过滤 Join 信息的 ACL 号或 ACL 名字
6	接收或发送 Join/Prune 报文和 Assert 报文时，是否进行邻居检查

版权所有 © 华为技术有限公司

配置维持转发关系的控制参数

转发控制参数可以在全局和接口两种情况下配置。转发控制参数包括：发送 Join/Prune 消息的周期和下游接口保持 Join/Prune 状态的时间。

背景信息

在 PIM-SM 交换机上进行如下配置。

说明

维持转发关系的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime join-prune** *interval*，配置下游接口保持加入/剪枝状态的时间。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim timer join-prune** *interval*，配置发送 Join/Prune 消息的时间间隔。
  4. 执行命令 **pim holdtime join-prune** *interval*，配置下游接口保持加入/剪枝状态的时间。
  5. 执行命令 **pim require-genid**，配置接收的 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

     当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居丢失或上游邻居状态已经改变。交换机立即向上游发送 Join/Prune 消息进行状态刷新。

     缺省情况下，交换机接受无 Generation ID 选项的 Hello 消息。

----结束

配置剪枝控制参数

剪枝控制参数可以在全局和接口两种情况下配置。剪枝控制参数包括：在 LAN 内传输消息的延迟时间和否决剪枝的时间间隔。

背景信息

在 PIM-SM 交换机上进行如下配置。

版权所有 © 华为技术有限公司

说明

剪枝的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option override-interval** *interval*，配置否决剪枝的时间。

     当一台交换机从上游接口接收到剪枝消息时，说明该 LAN 内还存在着其他的下游交换机。如果这台交换机仍然需要接收组播数据，则必须在 override-interval 时间内向上游发送 Join 消息。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim hello-option override-interval** *interval*，配置否决剪枝的时间。

----结束

配置 Join 信息过滤

接口上接收的 Join/Prune 消息中包含 Join 信息和 Prune 信息。可以通过配置 ACL 来过滤 Join 信息，设备根据符合过滤规则的 Join 信息建立 PIM 表项。

背景信息

接口上接收的 Join/Prune 消息中包含 Join 信息和 Prune 信息。可以通过配置 ACL 来过滤 Join 信息，交换机根据符合过滤规则的 Join 信息建立 PIM 表项，从而防止非法用户加入。

在运行 PIM-SM 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim join-policy** { **asm** *basic-acl-number* | **ssm** *advanced-acl-number* }，配置 Join 信息过滤。

----结束

版权所有 © 华为技术有限公司

配置邻居检查功能

接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果不是则不处理。

背景信息

缺省情况下，接收或发送 Join/Prune 消息和 Assert 消息时，不检查该消息是否来自 PIM 邻居或发送给 PIM 邻居。

如果需要配置 PIM 邻居检查功能，建议在与用户相连的设备上配置，在网络内部设备上不推荐使用此功能。接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果是则处理，否则丢弃。

在运行 PIM-SM 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **neighbor-check** { **receive** | **send** }，配置邻居检查功能。

可以同时使能接收和发送 Join/Prune 消息和 Assert 消息时的邻居检查功能。

----结束

检查配置结果

调整转发控制参数成功后，可以通过命令查看 PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

版权所有 © 华为技术有限公司

- **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.7.10 调整 Assert 控制参数

当设备从下游接口接收到组播数据时，说明该网段中还存在其他的上游设备。设备从该接口发出 Assert 消息，参与竞选唯一上游。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置保持 Assert 状态的时间。

应用环境

本节所有配置项同时适用于 ASM 模型和 SSM 模型。

当 PIM-SM 交换机从下游接口接收到组播数据时，说明该网段中还存在其他的上游交换机。交换机从该接口发出 Assert 消息，参与竞选唯一上游。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 Assert 控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整 Assert 控制参数之前，需准备以下数据。

序号	数据
1	保持 Assert 状态的时间

配置保持 Assert 状态的时间

落选设备保持 Assert 状态的时间内禁止下游接口转发组播数据，超时后恢复转发。

背景信息

在 PIM-SM 域内所有交换机上进行如下配置。

版权所有 © 华为技术有限公司

说明

Assert 控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime assert** *interval*，配置保持 Assert 状态的时间。落选交换机在此时间内禁止下游接口转发组播数据，超时后恢复转发。
- 接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  3. 执行命令 **pim holdtime assert** *interval*，配置保持 Assert 状态的时间。落选交换机在此时间内禁止下游接口转发组播数据，超时后恢复转发。

----结束

检查配置结果

调整 Assert 控制参数成功后，可以通过命令查看 PIM 接口、PIM 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** } | **interface** *interface-type interface-number*] *命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

版权所有 © 华为技术有限公司

- **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

6.7.11 调整 SPT 切换控制参数

当组播流量变大时，RP 上的负担增大，容易引发故障。PIM-SM 允许在组播报文速率较大时，由 RP 或组成员端 DR 触发 SPT 切换。

建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要调整 SPT 切换控制参数。

应用环境

本节介绍在 ASM 模型中如何通过命令调整 SPT 切换控制参数。

在 PIM-SM 组播转发中，每一个组播组只对应一棵 RPT。最初，所有组播源（无论数量有多少，无论分布在哪里），先将数据封装在注册消息中单播发往 RP，解封装后再沿 RPT 转发。

从而可以看出使用 RPT 转发组播数据的三个缺点：

- 源端 DR 和 RP 必须进行繁琐的封装/解封装处理。
- 转发路径不一定是从源到接收者的最短路径。
- 当组播流量变大时，RP 上的负担增大，容易引发故障。

针对此问题的解决方法是：

- RP 发起 SPT 切换：向源发起加入，沿最短路径构造从源端 DR 到 RP 的组播路由。后续组播报文直接沿此路径转发。
- 组成员端 DR 发起 SPT 切换：组成员端 DR 检测组播数据转发速率，当发现超过阈值则立即发起 SPT 切换。组成员端 DR 向源发起加入，沿最短路径构造从源端 DR 到组成员端 DR 的组播路由。后续组播报文直接沿此路径转发。

交换机在系统缺省值的控制下可以正常的工作。同时，AC6605 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 SPT 切换控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整 SPT 切换控制参数之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	PIM 叶子交换机从 RPT 向 SPT 切换的报文速率阈值
2	从 RPT 向 SPT 切换的组过滤策略、排序规则
3	RPT 切换到 SPT 前检查组播数据速率门限的时间间隔

（可选）配置永远不发起 SPT 切换

可以在组成员端 DR 上配置永远不发起 SPT 切换。

背景信息

在所有可能成为组成员端 DR 的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **spt-switch-threshold infinity** [**group-policy** *basic-acl-number* [**order** *order-value*]]，配置永远不发起 SPT 切换。

----结束

检查配置结果

调整 SPT 切换控制参数成功后，可以通过命令查看 PIM 路由表是否符合要求。

操作步骤

- 使用以下命令查看 PIM 路由表：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

----结束

版权所有 © 华为技术有限公司

6.7.12 配置 PIM BFD

当 BFD 检测到对端故障以后上报 PIM 模块，PIM 模块立即触发新一轮的 DR 竞选过程，而不是等到邻居关系超时，这将很大程度上缩小组播数据传输的中断时间，提高组播网络的可靠性。

建立配置任务

配置 PIM-SM 基本功能后，可以配置 PIM BFD 来提高 PIM 网络的可靠性，并可以根据实际需要调整 BFD 检测参数。

应用环境

正常情况下，如果共享网段上的当前 DR 出现故障，其他 PIM 邻居会等到邻居关系超时才触发新一轮的 DR 竞选过程，组播数据传输中断的时间将会不小于邻居关系的超时时间，通常是秒级。

BFD 的特点是快速故障检测，可以达到毫秒级。利用 BFD 来检测共享网段上 PIM 邻居的状态，当 BFD 检测到对端故障以后上报 PIM 模块，PIM 模块立即触发新一轮的 DR 竞选过程，而不是等到邻居关系超时，这将很大程度上缩小组播数据传输的中断时间，提高组播网络的可靠性。

PIM BFD 也适用于共享网段上 Assert 竞选的过程，可以快速响应 Assert Winner 接口故障。

前置任务

在配置 PIM BFD 功能之前，需完成以下任务：

- 配置单播路由协议
- **配置 PIM-SM 基本功能**
- 系统视图下使能 BFD 功能。

数据准备

在配置 PIM BFD 功能之前，需准备以下数据。

序号	数据
1	BFD 检测消息的最小发送间隔、最小接收间隔、本地检测倍数

配置 PIM BFD

在互为 PIM 邻居的设备相连的接口上使能 PIM BFD。

背景信息

说明

该功能只适用于 NBMA 接口和 Broadcast 接口，且不能在 MTunnel 接口下使能该功能。

在互为 PIM 邻居的交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 执行命令 **pim bfd enable**，使能 PIM BFD 功能。

缺省情况下，未使能 PIM BFD。

----结束

（可选）调整 BFD 检测参数

可以根据实际情况调整 PIM BFD 参数，包括：PIM BFD 检测消息的最小发送间隔、最小接收间隔和本地检测倍数。

背景信息

在互为 PIM 邻居的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的只能是 VLANIF 接口。

步骤 3 执行命令 **pim bfd** { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *，调整 PIM BFD 参数：PIM BFD 检测消息的最小发送间隔、最小接收间隔、本地检测倍数。不执行此命令时，以上参数取缺省值。

当其他协议配置了同样的 BFD 参数时，PIM BFD 配置的参数可能会受到影响。

----结束

检查配置结果

配置 PIM BFD 成功后，可以通过命令查看 PIM BFD session 信息。

操作步骤

- 使用以下命令查看 PIM BFD session 信息：
  - **display pim bfd session statistics**
  - **display pim bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *

----结束

版权所有 © 华为技术有限公司

6.7.13 配置防止主机恶意攻击功能（PIM Silent）

设备直连用户主机的接口上需要使能 PIM 协议，当恶意主机模拟 PIM Hello 报文，大量发送时，有可能导致设备瘫痪。为了避免这样的情况发生，可以将该接口设置为 PIM Silent 状态。

建立配置任务

网络中 PIM-SM 和 IGMP 的基本功能都已配置后，将 PIM Silent 特性配置在与主机相连的接口上，该接口使能了 PIM-SM 和 IGMP。

应用环境

在接入层上，交换机直连用户主机的接口上需要使能 PIM 协议，在该接口上可以建立 PIM 邻居，处理各类 PIM 协议报文。此配置同时存在着安全隐患：当恶意主机模拟发送 PIM Hello 报文时，有可能导致交换机瘫痪。

为了避免这样的情况发生，可以将该接口设置为 PIM Silent 状态（即 PIM 消极状态）。当接口进入 PIM 消极状态后，禁止接收和转发任何 PIM 协议报文，删除该接口上的所有 PIM 邻居以及 PIM 状态机，该接口作为静态 DR 立即生效。同时，该接口上的 IGMP/MLD 功能不受影响。

该功能仅适用于与用户主机网段直连的交换机接口，且该用户网段只与这一台交换机相连。

注意

如果在与交换机相连的接口上启动该功能，将导致 PIM 邻居无法正常建立，引发组播故障。

如果用户网段与多台交换机相连，在多个交换机接口上配置 PIM Silent，则这些接口都成为了静态 DR，将导致该网段中同时存在多个 DR，从而引发组播故障。

前置任务

在配置防止主机恶意攻击功能之前，需要完成以下任务：

- 配置单播路由协议，使网络畅通。
- 配置 PIM-SM
- 配置 IGMP

数据准备

在配置防止主机恶意攻击功能之前，需要准备以下数据。

序号	数据
1	与用户主机相连的交换机接口编号

版权所有 © 华为技术有限公司

配置 PIM Silent

配置 PIM Silent 后，接口禁止接收和转发任何 PIM 协议报文，删除该接口上的所有 PIM 邻居以及 PIM 状态机，并自动成为 DR。同时，该接口上的 IGMP 功能不受影响。

背景信息

在与用户主机网段直连的接口上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **pim silent**，使能 PIM Silent 功能。可以有效的防范恶意主机 Hello 报文攻击，保护接入交换机。

----结束

检查配置结果

配置 PIM Silent 成功后，可以通过命令查看 PIM 接口信息。

前提条件

已经完成防止主机恶意攻击功能（PIM Silent）功能的所有配置。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看 PIM 接口信息。

----结束

任务示例

执行命令 **display pim interface verbose**，可以看到使能了此配置。

```
<SwitchA> display pim interface verbose
 VPN-Instance: public net
 Interface: Vlanif10, 2.2.2.2
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 2.2.2.2 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: enabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0X2649E5DA
     PIM require-genid: disabled
     PIM hello hold interval: 105 s
```


版权所有 © 华为技术有限公司

```
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
PIM BFD: disabled
PIM dr-switch-delay timer : not configured
Number of routers on link not using DR priority: 0
Number of routers on link not using LAN delay: 0
Number of routers on link not using neighbor tracking: 1
ACL of PIM neighbor policy: -
ACL of PIM ASM join policy: -
ACL of PIM SSM join policy: -
```

6.7.14 维护 PIM-SM（IPv4）

PIM-SM 的维护包括：清除 PIM 统计信息、监控 PIM 的运行状况。

清除 PIM 控制报文统计信息

需要重新统计 PIM 控制报文数量时，可以将已有 PIM 控制报文统计数清零，注意清除后无法恢复。此操作不影响 PIM 的正常运行。

背景信息



注意

清除接口上的 PIM 控制报文统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除接口上的 PIM 控制报文统计信息后，请在用户视图下执行 **reset pim control-message counters** [**interface** *interface-type interface-number*]命令。

----结束

监控 PIM-SM 的运行状况

在 PIM 日常维护中，可以在任意视图下选择执行 display 命令，了解 PIM 的运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 PIM-SM 的运行状况。

操作步骤

- 在任意视图下执行 **display pim claimed-route** [*source-address*]命令，查看 PIM 使用的单播路由信息。
- 在任意视图下执行 **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** } | **interface** *interface-type interface-number*] *命令，查看发送和接收 PIM 控制报文的数目信息。

版权所有 © 华为技术有限公司

- 在任意视图下执行 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令，查看接口上的 PIM 信息。
- 在任意视图下执行 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令，查看 PIM 邻居信息。
- 在任意视图下执行以下命令，查看 PIM 协议组播路由表的内容：
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]
  - **display pim routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *
- 在任意视图下执行 **display pim rp-info** [*group-address*]命令，查看组播组对应的 RP 信息。
- 在任意视图下执行 **display pim rp-info** [*group-address*]命令，查看组播组对应的 RP 信息。

----结束

调试 PIM

出现 PIM 运行故障时，可以在用户视图下打开相应的 debugging 调试开关，查看发送和接收的报文内容，从而定位故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

- 在用户视图下执行 **debugging pim all** 命令，打开 PIM 协议的所有调试信息开关。
- 在用户视图下执行 **debugging pim event** [*advanced-acl-number*]命令，打开 PIM 协议的事件调试信息开关。
- 在用户视图下执行 **debugging pim routing-table** [*advanced-acl-number*]命令，打开 PIM 路由表状态改变调试信息开关。

版权所有 © 华为技术有限公司

- 在用户视图下执行 **debugging pim neighbor** [*basic-acl-number* | [**receive** | **send**]] * 命令，打开 PIM 协议中和邻居信息有关的调试信息开关。
- 在用户视图下执行 **debugging pim assert** [*advanced-acl-number* | [**receive** | **send**]] * 命令，打开 PIM 协议中和 Assert 信息有关的调试信息开关。
- 在用户视图下执行 **debugging pim rp** [**receive** | **send**]命令，打开 PIM 协议中和 BSR、RP 有关的调试信息开关。
- 在用户视图下执行 **debugging pim join-prune** [*advanced-acl-number* | [**receive** | **send**]] *命令，打开 PIM 协议中和加入、剪枝信息有关的调试信息开关。
- 在用户视图下执行 **debugging pim register** [*advanced-acl-number*]命令，打开 PIM 协议中和注册信息有关的调试信息开关。
- 在用户视图下执行 **debugging pim msdp** [*advanced-acl-number*]命令，打开 PIM 协议中和 MSDP 交互信息的调试信息开关。
- 在用户视图下执行 **debugging pim bfd** { **all** | **create** | **delete** | **event** }命令，打开 PIM BFD 功能所有调试信息开关。

----结束

6.7.15 配置举例

通过配置举例，可以了解如何构建基本的 PIM-SM 网络、配置 PIM-SM 常用功能。

配置 PIM-SM 组播网络示例

组网需求

在如图 6-18 所示的 ISP 网络中部署组播业务。已知该网络中已经部署了完备的 IGP，单播运行正常，并接入 Internet。要求通过在 Switch 进行适当配置，使网络中的用户主机能够通过组播方式接收视频点播信息。

图 6-18 配置 PIM-SM 典型组播网络组网图

Ethernet

Switch	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF100	192.168.9.1/24
	GE0/0/2	VLANIF101	10.110.1.1/24
	GE0/0/3	VLANIF200	192.168.1.1/24
SwitchB	GE0/0/1	VLANIF300	192.168.2.1/24
	GE0/0/2	VLANIF102	10.110.2.1/24
SwitchC	GE0/0/1	VLANIF102	10.110.2.2/24
	GE0/0/2	VLANIF400	192.168.3.1/24
SwitchD	GE0/0/1	VLANIF500	192.168.4.2/24
	GE0/0/2	VLANIF200	192.168.1.2/24
	GE0/0/3	VLANIF103	10.110.5.1/24
	GE0/0/4	VLANIF104	10.110.4.1/24
SwitchE	GE0/0/1	VLANIF400	192.168.3.2/24
	GE0/0/2	VLANIF300	192.168.2.2/24
	GE0/0/3	VLANIF100	192.168.9.2/24

版权所有 © 华为技术有限公司

GE0/0/4	VLANIF500	192.168.4.1/24

配置思路

由于 ISP 网络接入 Internet，为了易于业务拓展，采用 PIM-SM 协议配置组播功能，同时使用 ASM 和 SSM 模型提供组播服务。

1. 配置 Switch 的接口 IP 地址和单播路由协议。组播域内路由协议 PIM 是依赖单播路由协议，单播路由正常是组播协议正常工作的基础。
2. 在所有提供组播服务的 Switch 上使能组播功能。使能组播功能是配置 PIM-SM 的前提。
3. 在 Switch 所有接口上使能 PIM-SM 功能。使能 PIM-SM 功能之后才能配置 PIM-SM 的其他功能。

   说明

   如果该接口下还需要配置 IGMP 协议，必须先使能 PIM-SM，才能使能 IGMP 协议。两者顺序不能颠倒，否则 PIM-SM 功能配置会不成功。
4. 在与主机侧相连的 Switch 接口上使能 IGMP。接收者能通过发送 IGMP 消息自由加入或者离开某个组播组。叶结点 Switch 通过 IGMP 协议来维护组成员关系列表。
5. 配置 RP。在 PIM-SM 网络中，RP 是 RPT 树的根节点。建议 RP 的位置配置在组播流量分支较多的设备上，如本图中的 SwitchE 的位置。

   说明

   - 用户侧的 DR 得到新的 IGMP 成员关系创建(*,G)表项后，向 RP 发送加入/剪枝消息，沿路更新共享树。
   - 组播数据源刚开始向组发送数据时，由其 DR 向 RP 单播发送注册消息，RP 将其解封装后沿共享树分发给其组成员，同时 RP 向组播源侧 DR 发送注册-停止消息。注册停止后，可以由 RPT 向 SPT 切换。
6. （可选）在与 Internet 相连的接口上配置 BSR 边界，BSM 消息不能通过该边界，使 BSR 只为该 PIM-SM 域服务，增加组播可控性。
7. （可选）在各 Switch 上设置 SSM 组地址范围。使 PIM-SM 域内的 Switch 为 SSM 组地址范围内的组播组服务，实现可控组播。

说明

配置步骤中，只列出了与 PIM-SM 配置相关的命令。

数据准备

为完成此配置举例，需要准备如下数据：

- 组播组 G 地址：225.1.1.1/24。
- 组播源 S 地址：10.110.5.100/24。
- Switch 接口和用户主机之间运行的 IGMP 版本号为 3。
- SSM 组地址范围：232.1.1.0/24。

操作步骤

步骤 1 配置各接口的 IP 地址和单播路由协议。

版权所有 © 华为技术有限公司

按照图 6-18 配置各 Switch 口的 IP 地址和掩码，配置各 Switch 间采用 OSPF 进行互连，确保网络中各 Switch 间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。具体配置过程略。

接口 IP 地址的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 业务》中 **4.1 IP 地址配置**，OSPF 的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 路由》中 **5.4 OSPF 配置**。

步骤 2 使能组播功能，在各接口上使能 PIM-SM 功能。

在所有 Switch 使能组播功能，在各接口上使能 PIM-SM 功能。SwitchB、SwitchC、SwitchD 和 SwitchE 上的配置过程与 SwitchA 上的配置相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim sm
[SwitchA-Vlanif101] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] pim sm
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] pim sm
[SwitchA-Vlanif200] quit
```

步骤 3 在连接用户主机的接口上使能 IGMP 功能。

在 SwitchA 连接用户主机的接口上使能 IGMP 功能。SwitchB 和 SwitchC 上的配置过程与 SwitchA 上的配置相似，配置过程略。

```
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] igmp enable
[SwitchA-Vlanif101] igmp version 3
```

步骤 4 配置 RP。

说明

配置 RP 有两种方式：静态 RP 和动态 RP 两种。可以同时配置，也可以只配置其中一种。同时配置两种 RP 时，可以通过参数调整优先选择哪种 RP。

本实例同时配置两种 RP，并通过参数配置，优选动态 RP，静态 RP 作为备份。

配置动态 RP 需要在 PIM-SM 域的一个或多个 Switch 上进行如下配置。本例中在 SwitchE 上配置 RP 通告的服务范围，及 C-BSR 和 C-RP 的位置。

```
[SwitchE] acl number 2008
[SwitchE-acl-basic-2008] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2008] quit
[SwitchE] pim
```

配置静态 RP 需要在所有 Switch 配置。SwitchB、SwitchC、SwitchD 和 SwitchE 上的配置过程与 SwitchA 上的配置相似，配置过程略。

说明

如果命令 **static-rp X.X.X.X** 后面选择参数 preferred，优先选择静态 RP 作为本 PIM-SM 域的 RP。

```
[SwitchA] pim
[SwitchA-pim] static-rp 192.168.2.2
```

步骤 5 配置 SSM 组播组地址范围。

在所有 Switch 配置 SSM 组播组地址范围为 232.1.1.0/24。SwitchB、SwitchC、SwitchD 和 SwitchE 上的配置过程与 SwitchA 上的配置完全相同，配置过程略。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
```

步骤 6 验证配置结果。

通过使用 **display pim interface** 命令可以查看接口上 PIM 的配置和运行情况。例如 SwitchC 上 PIM 的显示信息如下：

```
[SwitchC] display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif102        up      0         30         1         10.110.2.2    (local)
Vlanif400        up      1         30         1         192.168.3.1
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100 101 200
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif100
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 #
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```


版权所有 © 华为技术有限公司

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 102 300
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif 102
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Vlanif300
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 102 400
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif102
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Vlanif400
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
```


版权所有 © 华为技术有限公司

```
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 103 104 200 500
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif103
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
interface Vlanif104
 ip address 10.110.4.1 255.255.255.0
 pim sm
 #
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 104
 port hybrid untagged vlan 104
#
ospf 1
 area 0.0.0.0
  network 10.110.4.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 100 300 400 500
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
acl number 2008
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface Vlanif100
 ip address 192.168.9.2 255.255.255.0
 pim sm
#
interface Vlanif300
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlanif400
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
  static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

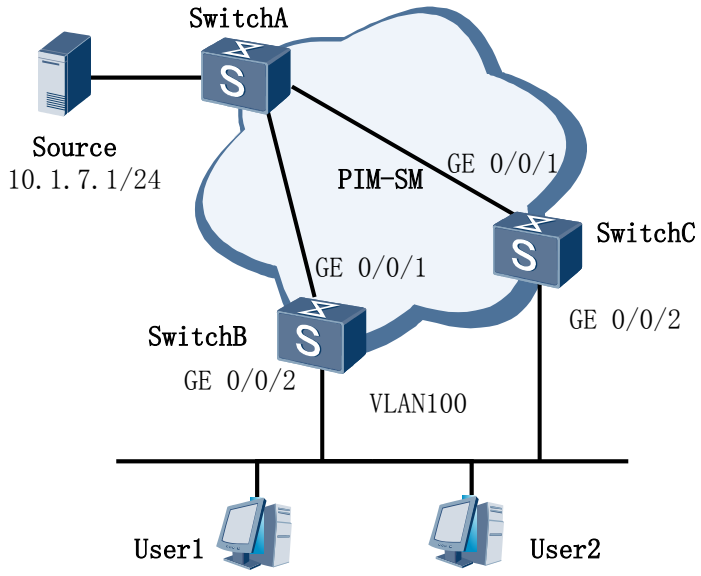
配置 PIM BFD 示例

组网需求

在图 6-19 所示的组播网络中，Switch 之间运行 PIM-SM 协议。用户主机正常接收来自组播源 Source 的视频点播。SwitchA 是组播源侧 DR，SwitchB 和 SwitchC 同时连接用户主机网段。要求当 DR 变化时，快速响应。

版权所有 © 华为技术有限公司

图 6-19 配置共享网段应用 PIM BFD 组网图



配置思路

采用如下的思路配置 PIM BFD 的基本功能：

1. 在 Switch 接用户主机网段的接口上配置 PIM BFD 功能。

数据准备

为完成此配置举例，需要准备如下数据：

- PIM BFD session 的多种参数

说明

配置步骤中，只列出了与 PIM-SM BFD 配置相关的命令。

操作步骤

步骤 1 配置各接口的 IP 地址和单播路由协议。

按照图 6-19 配置各 Switch 口的 IP 地址和掩码，配置各 Switch 间采用 OSPF 进行互连，确保网络中各 Switch 间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。具体配置过程略。

接口 IP 地址的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 业务》中 **4.1 IP 地址配置**，OSPF 的配置方法，请参见《AC6605 无线接入控制器 配置指南-IP 路由》中 **5.4 OSPF 配置**。

步骤 2 使能全局 BFD，在接口下配置 PIM BFD。

在 SwitchB 和 SwitchC 上全局使能 BFD，并在连接用户主机网段的接口上使能 PIM BFD 功能，配置 PIM BFD 参数。SwitchC 的配置过程与 SwitchB 相似，配置过程略。

```
[SwitchB] bfd
[SwitchB-bfd] quit
```


版权所有 © 华为技术有限公司

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim bfd enable
[SwitchB-Vlanif100] pim bfd min-tx-interval 200 min-rx-interval 200 detect-multiplie 3
```

步骤 3 验证配置结果。

使用 **display pim interface verbose** 命令，可以查看 PIM 接口上的详细信息。SwitchB 上的 PIM 接口信息表明用户主机网段的 DR 为 SwitchC。

```
[SwitchB] display pim interface vlanif100 verbose
VPN-Instance: public net
 Interface: Vlanif100, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM Hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM Hello override interval (negotiated): 2500 ms
     PIM Hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0XF5712241
     PIM Hello hold interval: 105 s
     PIM Hello assert interval: 180 s
     PIM triggered Hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: enable
     PIM BFD min-tx-interval: 200 ms
     PIM BFD min-rx-interval: 200 ms
     PIM BFD detect-multiplier: 3
     PIM dr-switch-delay timer : 20 s
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 2
```

使用 **display pim bfd session** 显示各 Switch 的 BFD Session 信息，查看 BFD Session 是否建立。

```
[SwitchB] display pim  bfd session
VPN-Instance: public net
Total 1 BFD session Created

Vlanif100 (10.1.1.1): Total 1 BFD session Created

Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
10.1.1.2     200           200           3            8192/8192        Up
```

使用 **display pim routing-table** 命令可以查看 PIM 路由表。SwitchC 作为 DR，存在（S，G）和（*，G）表项。显示信息如下：

```
[Switch] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 10.1.5.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface:     vlanif200,
         Upstream neighbor: 10.1.2.2
         RPF neighbor: 10.1.2.2
     Downstream interface(s) information:
```


版权所有 © 华为技术有限公司

```
    Total number of downstreams: 1
        1: Vlanif100,
            Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.1.7.1, 225.1.1.1)
    RP: 10.1.5.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: vlanif200
        Upstream neighbor: 10.1.2.2
        RPF neighbor: 10.1.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif100
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

----结束

配置文件

- SwitchA 只需配置 PIM SM 的基本功能，在本例中不重点关注，配置文件略。
- SwitchB 的配置文件如下。SwitchC 的配置文件与 SwitchB 相似，内容略。

```
#
 sysname SwitchB
#
 vlan batch 100 200
#
 multicast routing-enable
#
bfd
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 pim sm
 igmp enable
 pim bfd enable
 pim bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier 3
#
interface Vlanif200
 ip address 10.1.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 200
#
interface GigabitEthernet/0/2
 port hybrid tagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
return
```

6.8 MSDP 配置

通过配置 MSDP 协议，可以实现 PIM-SM 域间组播路由与数据转发、PIM-SM 域内的 Anycast RP。

6.8.1 MSDP 概述

MSDP 的实现方式是在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，MSDP 对等体之间通过交互 SA 消息来传递(S,G)信息，从而共享组播源，主机可以接收其他 PIM-SM 域的组播源数据。

版权所有 © 华为技术有限公司

在基本的 PIM-SM 模式下，组播源只向本域内的 RP（Rendezvous Point）注册，且域间组播源信息隔离。因此 RP 知道且仅知道本域内的组播源，只能在本域内建立组播分发树，将本域内的组播源发出的数据分发给本域内的用户。

如果能够加载一种机制，将其它域内的组播源信息传递给本域内的 RP，则本域内的 RP 就可以向其他域内的组播源发起加入过程、建立组播分发树、实现组播数据跨域传输，从而使本域内的组成员主机接收到其他域的组播源发出的数据。

MSDP（Multicast Source Discovery Protocol）是能够解决上述问题的一种机制，成为基于多个 PIM-SM 域互连而开发的一种域间组播解决方案。

MSDP 的实现方式是在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，MSDP 对等体之间通过交互 SA（Source Active）消息，将（S，G）信息从“组播源 S 注册的 RP”传递给其他的“组 G 成员主机加入的 RP”。

MSDP 对等体之间使用 TCP 连接，对接收到的 SA 消息执行 RPF 检查。

说明

MSDP 只适用于 PIM-SM 域，仅对 ASM（Any-Source Multicast）模型有意义。

6.8.2 AC6605 支持的 MSDP 特性

系统通过 MSDP 实现 PIM-SM 域间组播和 PIM-SM 域内 Anycast RP。用户可以控制 MSDP 对等体连接，调整 SA 消息参数，配置 MSDP 对等体认证和 SA 消息的过滤策略来提高 MSDP 安全性。系统支持多实例的 MSDP。

PIM-SM 域间组播

在组播网络被划分成多个 PIM-SM 域时，使用 MSDP 沟通各个域内的 RP，共享组播源信息。最终使一个域内的用户接收到其它域内组播源发送的组播数据。

用户可以配置 AS 域内的 MSDP 对等体、AS 域间的 MSDP 对等体和静态 RPF 对等体。

PIM-SM 域内 Anycast RP

在 PIM-SM 域中应用 Anycast RP，可以实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

用户可以将 Loopback 接口作为 C-RP 或者静态 RP 的接口、为 SA 消息指定逻辑 RP 地址。

MSDP 对等体连接参数可配置

AC6605 提供 MSDP 会话的开启和关闭功能，同时可以配置交换机向远端 MSDP 对等体发出 TCP 连接请求的重试周期。

SA 消息缓存可配置

缺省情况下，交换机上启动了 SA-Cache 功能，可以在本地保存 SA 消息中携带的（S，G）信息。当有接收需求时，交换机直接从 SA-Cache 中获得可用的（S，G）信息。

用户可以配置缓存（S，G）项的最大数量，可以有效的防止 DoS（Deny of Service）攻击。

版权所有 © 华为技术有限公司

AC6605 允许用户关闭交换机的 SA-Cache 功能。SA-Cache 关闭后，交换机在本地不保存 SA 消息中携带的（S，G）信息。当有接收需求时，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。这将延迟接收者获取组播源信息的时间。

SA 请求可控制

某些交换机不允许在本地启动 SA-Cache 功能或 SA-Cache 的容量设置较小。当有新的接收需求时，交换机无法立即获取有效的（S，G）信息，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。

如果远端 MSDP peer 上启动了 SA-Cache 功能，且 SA-Cache 的容量设置较大，用户可以在本地交换机上配置“发送 SA 请求消息”以缩减接收者获取组播源信息的时间。

同时用户还可以在远端 MSDP Peer 上配置接收 SA 请求消息的过滤规则。

传输突发性组播数据

当某些组播源发送组播数据的时间间隔大于（S，G）表项的超时时间时，一旦有突发性组播数据，源端 DR 只能将组播数据逐个封装在注册报文中，发给源 RP。源 RP 使用 SA 消息将（S，G）信息传输到远端 RP。然后，远端 RP 向组播源的方向发起（S，G）加入，创建 SPT。由于（S，G）表项超时，远端用户将永远无法收到 S 发出的组播数据。

AC6605 支持传输突发组播数据功能，用户在源 RP 上启动“在 SA 消息中封装组播数据报文”功能后，源 RP 会将组播数据报文封装在 SA 消息中，发送出去。远端 RP 接收到该 SA 消息后解封装，将组播数据沿 RPT 传输给本域内用户。

同时，配置“TTL 阈值”可以限制封装在 SA 消息中的组播数据报文的传输范围。当 MSDP Peer 接收到封装了组播数据报文的 SA 消息后，检查组播数据报文 IP 头的 TTL 值。如果组播数据报文的 TTL 值小于或等于阈值，则不向特定的远端对等体转发。如果大于阈值，则将组播数据报文 IP 头的 TTL 值减 1，再使用 SA 消息携带组播数据报文发送出去。

SA 消息的创建、接收和转发可控制

缺省情况下，MSDP 交换机接收通过 RPF 检查的所有 SA 消息，并向所有 MSDP 对等体转发。

AC6605 允许用户使用以下三种方式配置过滤规则，控制 SA 消息在 MSDP 对等体间的传递。

- 在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些（S，G）信息发布出去。
- 配置“从远端 MSDP 对等体接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达交换机时，依据此规则决定是否接收。
- 配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

MSDP 认证

配置 MSDP MD5 或 Key-Chain 认证，可以提高 MSDP 对等体之间建立 TCP 连接的安全性。MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。

版权所有 © 华为技术有限公司

6.8.3 配置 PIM-SM 域间组播

介绍如何在 AS 域内配置 MSDP 对等体、在 AS 域间配置 MSDP 对等体及静态 RPF 对等体，实现 PIM-SM 域间组播。

建立配置任务

配置 PIM-SM 域间组播前，需要实现 PIM-SM 域内组播。

应用环境

当一个大的组播网络被划分成多个 PIM-SM 域时，需要使用 MSDP 沟通各个域内的 RP，共享组播源信息。最终使一个域内的用户接收到其它域内组播源发送的组播数据。

为了保证网络中所有 RP 都能参与源信息共享，且尽量缩小“MSDP 连通图”的规模，建议在且仅在网络中所有 RP（包括静态 RP 和 C-RP）上配置 MSDP 对等体。

为了保证 MSDP 对等体之间传递的 SA 消息不被 RPF 规则阻断，且尽量减少冗余流量，推荐采用如下配置方案。

- 将属于同一个 AS 的所有 MSDP 对等体加入同一个 Mesh Group。
- 在跨 AS 的 MSDP 对等体之间：（在以下两种方法中选择其一）
  - 建立 MBGP 对等体且使用相同的接口地址。
  - 相互指定对方为静态 RPF 对等体。

说明

使用 BGP 和 MBGP 都可以建立跨 AS 的 EBGP 对等体。由于 MBGP 不影响网络中的单播拓扑，所以推荐使用 MBGP。

前置任务

在配置 PIM-SM 域间组播之前，需完成以下任务：

- 配置单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播

数据准备

在配置 PIM-SM 域间组播之前，需准备以下数据。

序号	数据
1	远端 MSDP 对等体地址
2	连接远端 MSDP 对等体的接口类型和编号
3	MSDP 对等体描述信息
4	Mesh Group 名称

版权所有 © 华为技术有限公司

配置 AS 内的 MSDP 对等体

AS 内存在多个 PIM-SM 域，或 PIM-SM 域中存在多个为不同组播组服务的 RP 时，推荐在所有 RP（包括静态 RP 和 C-RP）之间配置 MSDP 对等体，并将所有 MSDP 对等体加入同一个 Mesh Group。

背景信息

在属于同一 AS 的所有 PIM-SM 域的 RP 上，进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，启动公网实例的 MSDP 功能，并进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **connect-interface** *interface-type interface-number*，配置 MSDP 对等体连接。

- *peer-address* 为远端 MSDP 对等体地址。
- *interface-type interface-number* 为连接远端 MSDP 对等体的本地接口。

说明

系统不向私网发布 MTI 接口上的路由，因此不要以 MTI 接口的地址建立 MSDP Peer 连接。

步骤 4 （可选）执行命令 **peer** *peer-address* **description** *text*，为远端 MSDP 对等体添加描述信息。

此项配置有助于区分远端 MSDP 对等体，管理与远端 MSDP 对等体之间的连接。

- *peer-address*：远端 MSDP 对等体的地址。
- *text*：描述性文本，最长为 80 个字符。

步骤 5 执行命令 **peer** *peer-address* **mesh-group** *name*，配置远端 MSDP 对等体加入 Mesh Group，即承认远端 MSDP 对等体为 Mesh Group 成员。

- *peer-address* 为远端 MSDP 对等体地址。
- *name* 为 Mesh Group 的名称。同一 Mesh group 的组成员使用相同的 Mesh Group 名称。

配置注意事项：

- Mesh Group 所有成员之间必须两两建立 MSDP 对等体连接。
- Mesh Group 所有成员之间必须两两承认对方为 Mesh Group 成员。
- 一个 MSDP 对等体只能属于一个 Mesh Group。如果多次配置同一 MSDP Peer 加入不同的 Mesh Group，最后一个配置有效。

----结束

在 MBGP 对等体上配置跨 AS 的 MSDP 对等体

可以在建立了 MBGP 对等体关系的不同 AS 的 RP 之间配置 MSDP 对等体，实现不同 AS 的 PIM-SM 域之间共享组播源信息。

版权所有 © 华为技术有限公司

背景信息

在位于不同 AS 的两个 RP 上建立 MBGP 对等体关系。然后，再进行如下配置。

说明

如果这两个 RP 之间已经建立了 BGP 对等体，则不必再建立 MBGP 对等体。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，启动公网实例的 MSDP 功能，并进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **connect-interface** *interface-type interface-number*，配置 MSDP 对等体连接。

- *peer-address* 为远端 MSDP 对等体地址，与远端 BGP 或 MBGP 地址相同。
- *interface-type interface-number* 为连接远端 MSDP 对等体的本地接口，与本地 BGP 或 MBGP 接口相同。

步骤 4 （可选）执行命令 **peer** *peer-address* **description** *text*，为 MSDP 对等体添加描述信息。

此项配置有助于区分远端 MSDP 对等体，管理与远端 MSDP 对等体之间的连接。

- *peer-address*：远端 MSDP 对等体的地址。
- *text*：描述性文本，最长为 80 个字符。

----结束

配置静态 RPF 对等体

可以在不同 AS 的 RP 之间配置静态 RPF 对等体，实现不同 AS 的 PIM-SM 域之间共享组播源信息。

背景信息

说明

如果已经执行了“**在 MBGP 对等体上配置跨 AS 的 MSDP 对等体**”，请跳过此项配置。

在位于不同 AS 的两个 RP 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，启动公网实例的 MSDP 功能，并进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **connect-interface** *interface-type interface-number*，配置 MSDP 对等体连接。

- *peer-address* 为远端 MSDP 对等体地址。
- *interface-type interface-number* 为连接远端 MSDP 对等体的本地接口。

步骤 4 （可选）执行命令 **peer** *peer-address* **description** *text*，为远端 MSDP 对等体添加描述信息。

此项配置有助于区分远端 MSDP 对等体，管理与远端 MSDP 对等体之间的连接。

版权所有 © 华为技术有限公司

- *peer-address* 为远端 MSDP 对等体的地址。
- *text* 为描述性文本，最长为 80 个字符。

步骤 5 执行命令 **static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]，静态指定远端 MSDP 对等体为 RPF 对等体。*peer-address* 为远端 MSDP 对等体地址。

----结束

检查配置结果

配置 PIM-SM 域间组播成功后，可以通过命令查看 MSDP 对等体的概要信息和详细信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp brief**，查看与本机建立了 MSDP 对等体关系的所有远端 Peer 的简要状态信息。例如：

```
<Quidway> display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  2            2            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.2.1           UP        01:07:08     200        8           0
  192.168.4.2           UP        00:06:39     100        13          0
```

6.8.4 配置 PIM-SM 域内 Anycast RP

Anycast RP 是指在同一个 PIM-SM 域内设置多个具有相同地址的 RP，并且在这些 RP 之间建立 MSDP 对等体关系，从而实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

建立配置任务

在 PIM-SM 域内各设备单播互通，使能了组播路由且各接口使能了 PIM-SM，网络中未配置 RP 的情况下配置 Anycast RP。

应用环境

在传统的 PIM-SM 域中，每个组播组都只能映射到一个 RP。当网络负载较大或者流量过于集中时，可能导致 RP 交换机的压力过大，RP 失效后收敛较慢，组播转发路径非最优等问题。

在 PIM-SM 域中应用 Anycast RP，可以实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

推荐的配置方案如下。

版权所有 © 华为技术有限公司

- 在 PIM-SM 域中的多台交换机上，各准备一个 Loopback 接口，配置相同的 IP 地址，并使用单播路由发布出去。
- 在这些交换机上配置该 Loopback 接口为 C-RP，或在 PIM-SM 域中的所有交换机上配置该地址为静态 RP。
- 在这些交换机之间建立 MSDP 对等体。如果这些交换机的总数超过三个，建议两两之间建立 MSDP 对等体关系并加入同一个 Mesh Group。
- 为在这些 MSDP 对等体之间传递的 SA 消息指定逻辑 RP 地址。

前置任务

在配置 Anycast RP 之前，需完成以下任务：

- 配置单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，未配置 RP

数据准备

在配置 Anycast RP 之前，需准备以下数据。

序号	数据
1	RP 地址
2	本端 MSDP 对等体的接口、地址
3	远端 MSDP 对等体接口、地址
4	MSDP 对等体描述信息

配置 RP 接口地址

在 PIM-SM 域内有待建立 Anycast RP 的多台设备上，各准备一个 Loopback 接口，配置相同的 IP 地址。使用单播路由将 RP 接口地址发布出去，确保网络各个位置的设备都有到达该 RP 接口地址的路由。

背景信息

使用当前网络中的单播路由协议，将新配置的 RP 接口地址公布出去。确保网络各个位置的交换机上都有到达该 RP 地址的路由。

在 PIM-SM 域内有待建立 Anycast-RP 的多台交换机上，分别进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface loopback** *interface-number*，进入 Loopback 接口视图。

由于网络中将同时存在多个 RP 使用相同的 IP 地址，所以选择将 RP 配置在 Loopback 接口上。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 Loopback 接口地址。

- *ip-address*：RP 的地址。在多台设备上配置 RP 接口，使用相同的 IP 地址。
- *mask* | *mask-length*：Loopback 接口地址掩码。

步骤 4 执行命令 **pim sm**，为 RP 接口使能 PIM-SM。

说明

配置动态 RP 前需要在接口上使能此命令。若配置静态 RP，不需要使能此命令。

----结束

配置 C-RP

若选择 C-RP，则只在有待建立 Anycast RP 的设备上将 Loopback 接口地址配置为候选 RP 接口。

背景信息

说明

- 当 PIM-SM 网络使用静态 RP 时，跳过此项配置。
- 当 PIM-SM 网络使用 BSR-RP 时，必须执行此项配置。执行此项配置之前，需要先配置 BSR 和 BSR 边界，且 BSR 的地址不能与该 C-RP 地址相同。

在 PIM-SM 域内有待建立 Anycast-RP 的多台交换机上，分别进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **c-rp loopback** *interface-number*，指定该 Loopback 接口为候选 RP 接口。

----结束

配置静态 RP

若使用静态 RP，则需要在 PIM-SM 域内的所有设备上将 Loopback 接口地址配置为 RP。

背景信息

说明

- 当 PIM-SM 网络使用 BSR-RP 时，跳过此项配置。
- 当 PIM-SM 网络使用静态 RP 时，必须执行此项配置。

在本 PIM-SM 域内所有交换机上，分别进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pim** ，进入 PIM 视图。

步骤 3 执行命令 **static-rp** *rp-address*，配置静态 RP 的地址为 Loopback 接口地址。

----结束

版权所有 © 华为技术有限公司

配置 MSDP 对等体

在 RP 之间建立 MSDP 对等体。如果这些设备的总数超过三个，建议两两之间建立 MSDP 对等体关系并加入同一个 Mesh Group。

背景信息

在有待建立 Anycast-RP 的多台交换机上，分别进行如下配置。

说明

如果配置了相同 IP 地址的 RP 的交换机不只两台，确保这些交换机之间使用 MSDP 对等体连通。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，启动公网实例的 MSDP 功能，并进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **connect-interface** *interface-type interface-number*，创建 MSDP 对等体连接。

- *peer-address*：远端 MSDP 对等体地址。
- *interface-type interface-number*：本地接口。

步骤 4 （可选）执行命令 **peer** *peer-address* **description** *text*，为 MSDP 对等体添加描述信息。

此项配置有助于区分远端 MSDP 对等体，管理与远端 MSDP 对等体之间的连接。

- *peer-address*：远端 MSDP 对等体的地址。
- *text*：描述性文本，最长为 80 个字符。

步骤 5 （可选）执行命令 **peer** *peer-address* **mesh-group** *name*，配置远端 MSDP 对等体加入 Mesh Group，即承认远端 MSDP 对等体为 Mesh Group 成员。

如果建立 Anycast-RP 的交换机只有两个，则不必执行此项配置。

- *peer-address*：远端 MSDP 对等体地址。
- *name*：Mesh Group 的名称。同一 Mesh group 的组成员使用相同的 Mesh Group 名称。

配置注意事项：

- Mesh Group 所有成员之间必须两两建立 MSDP 对等体连接。
- Mesh Group 所有成员之间必须两两承认对方为 Mesh Group 成员。
- 一个 MSDP 对等体只能属于一个 Mesh Group。如果多次配置同一 MSDP Peer 加入不同的 Mesh Group，最后一个配置有效。

----结束

为 SA 消息指定逻辑 RP 地址

MSDP 对等体对接收到的 SA 消息进行 RPF 检查，如果发现 SA 消息中携带的对端 RP 地址与本地 RP 地址相同，将会丢弃该 SA 消息。所以，需要在有待建立 Anycast RP 的设备上为 SA 消息指定逻辑 RP 地址。

版权所有 © 华为技术有限公司

背景信息

MSDP 对等体对接收到的 SA 消息进行 RPF 检查。如果发现 SA 消息中携带的对端 RP 地址与本地 RP 地址相同，将会丢弃该 SA 消息。

在有待建立 Anycast-RP 的多台交换机上，分别进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **originating-rp** *interface-type interface-number*，配置逻辑 RP 接口，不能与实际 RP 接口相同。建议配置为 MSDP 对等体接口。

使用 **originating-rp** 命令后，交换机发出的 SA 消息将携带逻辑 RP 地址，取代 SA 消息报文头中的 RP 地址，到达对端后能够通过 RPF 检查。

说明

系统不向私网发布 MTI 接口上的路由，因此不要将 MTI 接口的地址作为“逻辑 RP”。

----结束

检查配置结果

配置 PIM-SM 域内 Anycast RP 成功后，可以通过命令查看 MSDP 对等体的概要信息和详细信息、PIM 路由表项对应的 RP 信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display pim routing-table** 命令查看 PIM 路由表项对应的 RP 信息。

----结束

任务示例

在各个 RP 上执行命令 **display msdp brief**，查看远端 MSDP Peer 的简要状态信息。例如：

```
<Quidway> display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  2.2.2.2              UP        00:10:17      ?        0           0
```

在各个 RP 上执行命令 **display pim routing-table**，查看路由表项对应的 RP 信息。

```
<Quidway> display pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry
(10.11.1.2, 225.1.1.1)
     RP: 7.7.7.7 (local)
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:01:57
     Upstream interface: Vlanif10
         Upstream neighbor: 10.3.1.2
         RPF prime neighbor: 10.3.1.2
     Downstream interface(s) information:
```


版权所有 © 华为技术有限公司

```
Total number of downstreams: 1
    1: Vlanif20
        Protocol: pim-sm, UpTime:  - , Expires:  -
```

6.8.5 管理 MSDP 对等体连接

MSDP 对等体之间使用 TCP 连接，用户可以断开或重建 TCP 连接来灵活控制 MSDP 对等体间的会话。还可以调整 MSDP 对等体连接的重试周期。

建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要管理 MSDP 对等体连接。

应用环境

MSDP 对等体之间使用 TCP 连接（端口 639）。用户可以断开或重建 TCP 连接，灵活**控制 MSDP 对等体之间的会话**。

当新创建了 MSDP 对等体、或重新启动某被关闭的 MSDP 对等体连接、或故障的 MSDP 对等体尝试恢复工作时，需要迅速在 MSDP 对等体之间建立 TCP 连接。用户可以灵活的**调整 MSDP 对等体连接的重试周期**。

前置任务

在配置管理 MSDP 对等体连接之前，需完成以下任务：

- 配置单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域间组播**或**配置 PIM-SM 域内 Anycast RP**

数据准备

在配置管理 MSDP 对等体连接之前，需准备以下数据。

序号	数据
1	远端 MSDP 对等体地址
2	本端交换机的接口类型和编号

控制 MSDP 对等体之间的会话

在创建了 MSDP 对等体的设备上关闭 MSDP 对等体连接，对等体之间不再传递 SA 消息，并不再重试建立连接。用户可以根据需要重新启动 MSDP 对等体连接。

背景信息

在创建了 MSDP 对等体的交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **shutdown** *peer-address*，关闭与远端 MSDP 对等体之间的会话。

- *peer-address* 为远端 MSDP 对等体地址。
- 关闭与远端 MSDP 对等体之间的会话后，TCP 连接断开，对等体之间不再传递 SA 消息，并不再重试建立连接，但配置信息会保留。
- 执行命令 **undo shutdown** *peer-address*，可以打开与远端 MSDP 对等体之间会话，重新建立 TCP 连接。

----结束

调整 MSDP 对等体连接的重试周期

当新创建了 MSDP 对等体、重新启动被关闭的 MSDP 对等体连接、或故障的 MSDP 对等体尝试恢复工作时，需要迅速在 MSDP 对等体之间建立 TCP 连接。用户可以灵活的调整 MSDP 对等体连接的重试周期。

背景信息

在创建了 MSDP 对等体的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **timer retry** *interval*，配置交换机向远端 MSDP 对等体发出 TCP 连接请求的重试周期。

----结束

检查配置结果

管理 MSDP 对等体连接后，可以通过命令查看 MSDP 对等体的概要信息和详细信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp brief**，查看与远端 MSDP 对等体之间的连接状态简要信息。例如：

```
<Quidway> display msdp brief
MSDP Peer Brief Information
  Configured   Up          Listen       Connect      Shutdown     Down
```


版权所有 © 华为技术有限公司

```
2            2            0            0            0            0

Peer's Address     State     Up/Down time     AS     SA Count    Reset Count
192.168.2.1          UP       01:07:08     200        8            0
192.168.4.2          UP       00:06:39     100        13           0
```

6.8.6 配置 SA 缓存

SA 缓存用来在本地保存 SA 消息中携带的(S,G)信息，有接收需求时，设备直接从 SA 缓存中获得可用的(S,G)信息。

建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 缓存。

应用环境

缺省情况下，配置了 MSDP Peer 的交换机上启动了 SA-Cache 功能，可以在本地保存 SA 消息中携带的（S，G）信息。当有接收需求时，交换机直接从 SA-Cache 中获得可用的（S，G）信息。

同时配置缓存（S，G）项的最大数量，可以有效的防止 DoS（Deny of Service）攻击。

AC6605 允许用户关闭交换机的 SA-Cache 功能。SA-Cache 关闭后，交换机在本地不保存 SA 消息中携带的（S，G）信息。当有接收需求时，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。这将延迟接收者获取组播信息的时间。

前置任务

在配置 SA 缓存之前，需完成以下任务：

- 配置某单播路由协议，实现域内网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域间组播**或**配置 PIM-SM 域内 Anycast RP**

数据准备

在配置 SA 缓存之前，需准备以下数据。

序号	数据
1	SA 缓存的（S, G）项最大数量

配置缓存（S，G）项的最大数量

配置 SA 缓存(S,G)表项的最大数量可以防止 DoS 攻击。

背景信息

在配置了 MSDP Peer 的交换机上，进行如下的配置。

版权所有 © 华为技术有限公司

说明

当不进行此项配置时，使用系统缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-cache-maximum** *sa-limit*，限制被缓存的（S，G）项的最大数量。

- *peer-address* 为远端 MSDP Peer 地址。
- *sa-limit* 为缓存（S，G）项的最大数量。配置值小于 cache 规格时按配置值生效，配置值大于 cache 规格时按规格生效。

----结束

关闭 SA-Cache 功能

系统允许用户关闭 SA Cache 功能。有接收需求时，必须等待其 MSD 对等体在下一个周期发来的 SA 消息，这将延迟接收者获取组播信息的时间。

背景信息

在配置了 MSDP Peer 的交换机上，进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **undo cache-sa-enable**，关闭 SA-Cache 功能。

说明

在 MSDP 视图下执行命令 **cache-sa-enable**，可以重新启动 SA-Cache 功能。

----结束

检查配置结果

配置 SA 缓存成功后，可以通过命令查看 MSDP 对等体的概要信息和详细信息。

操作步骤

- 使用 **display msdp sa-cache** [*group-address* | *source-address* | { *2-byte-as-number* | *4-byte-as-number* }] *命令查看公网实例的 SA 缓存中的（S，G）项。
- 使用 **display msdp sa-count** [*2-byte-as-number* | *4-byte-as-number*]命令查看公网实例的 SA 缓存中的（S，G）项的数量。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display msdp sa-cache**，查看 SA 缓存中的（S，G）信息。

```
<Quidway> display msdp sa-cache
MSDP Source-Active Cache Information : public net
MSDP Total Source-Active Cache - 3 entries
MSDP matched 3 entries

(8.8.8.8, 225.0.0.200)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 10
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.201)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 1.0
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.202)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 65535.65535
 Uptime: 00:00:33, Expires: 00:05:27
```

执行命令 **display msdp sa-count**，查看 SA 缓存中的（S，G）项的数量。

```
<Quidway> display msdp sa-count
MSDP Source-Active Count Information: public net
Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5
Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                      3
  Total 5 Source-Active entries matched
```

6.8.7 配置 SA 请求

远端 MSDP 对等体的 SA Cache 容量较大时，在本地设备上配置“发送 SA 请求消息”可以缩减接收者获取组播源信息的时间。可以在指定的远端 MSDP 对等体上配置接收 SA 请求消息的过滤规则。

建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 请求。

应用环境

某些交换机 SA-Cache 的容量设置较小。当有新的接收需求时，交换机无法立即获取有效的（S，G）信息，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。

如果远端 MSDP peer 上启动了 SA-Cache 功能，且 SA-Cache 的容量设置较大，则在本地交换机上配置“发送 SA 请求消息”可以缩减接收者获取组播源信息的时间。

- 当本地交换机上有新的接收需求时，主动向某指定远端 MSDP peer 发送 SA 请求消息。
- 远端 MSDP peer 一旦接收到 SA 请求消息，立即回复 SA 消息，携带符合需求的（S，G）信息。如果远端 MSDP peer 上配置了“SA 请求消息过滤规则”，则对从指定对等体发来的 SA 请求消息执行检查，根据检查结果决定是否给予回复。

版权所有 © 华为技术有限公司

前置任务

在配置“SA 请求”之前，需完成以下任务：

- 配置某单播路由协议，实现域内网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域间组播**或**配置 PIM-SM 域内 Anycast RP**

数据准备

在配置“SA 请求”之前，需准备以下数据。

序号	数据
1	远端 MSDP peer 地址
2	接收 SA 请求消息的过滤列表

在本地交换机上配置“发送 SA 请求消息”

当设备接收到一个新的组加入消息，并且本地表项和 SA 缓存中都没有该(S,G)时，设备可以立即向指定的 MSDP 对等体发送 SA 请求消息，而不是等待下一周期 SA 消息的到来。

背景信息

在本地交换机上，进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **request-sa-enable**，配置“发送 SA 请求消息”。

peer-address 为远端 MSDP 对等体地址。当本地交换机接收到一个新的组加入消息时，只向 *peer-address* 发送 SA 请求消息。

----结束

（可选）在远端 MSDP peer 上配置接收 SA 请求消息的过滤规则

可以在指定的远端 MSDP 对等体上配置本地设备发出的 SA 请求消息的过滤策略。若 SA 请求消息通过过滤，立即回复 SA 消息。

背景信息

在命令 **peer** *peer-address* **request-sa-enable** 中指定远端 MSDP Peer 的交换机上，进行如下的配置。当不进行此项配置时，一旦有 SA 请求消息到达，交换机立即回复 SA 消息，携带符合需求的（S，G）信息。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-request-policy** [**acl** *basic-acl-number*]，配置接收 SA 请求消息的过滤规则。

- *peer-address* 为发出 SA 请求消息的 MSDP 对等体地址。
- **acl** 为过滤策略。如果没有指定 ACL 则忽略从该 peer 发来的所有 SA 请求；如果指定了 ACL 则仅接收符合规则的 SA 请求消息，其它的被忽略。

----结束

检查配置结果

配置 SA 请求成功后，可以通过命令查看 MSDP 对等体的详细信息和 SA 缓存信息。

操作步骤

- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。
- 使用 **display msdp sa-cache** [*group-address* | *source-address* | { *2-byte-as-number* | *4-byte-as-number* }] *命令查看所有实例的 SA 缓存。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Information about SA-Requests 字段检查本节配置是否生效。例如：

```
<Quidway> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: Vlanif10 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 16/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: configured
    Peer authentication type: Key-Chain
```


版权所有 © 华为技术有限公司

6.8.8 配置过滤 SA 消息的规则

缺省情况下，所有通过 RPF 检查的 SA 消息都会被接收并向其他 MSDP 对等体转发。配置创建、接收或转发 SA 消息的过滤策略可以控制 SA 消息在 MSDP 对等体间的传递。

建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 消息的过滤规则。

应用环境

缺省情况下，MSDP 的交换机接收通过 RPF 检查的所有 SA 消息，并向所有 MSDP 对等体转发。AC6605 允许用户使用以下三种方式配置过滤规则，控制 SA 消息在 MSDP 对等体间的传递。

- 在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些（S，G）信息发布出去。
- 配置“从远端 MSDP 对等体接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达交换机时，依据此规则决定是否接收。
- 配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

前置任务

在配置“控制 SA 消息的创建与转发”之前，需完成以下任务：

- 配置某单播路由协议，实现域内网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域间组播**或**配置 PIM-SM 域内 Anycast RP**

数据准备

在配置“控制 SA 消息的创建与转发”之前，需准备以下数据。

序号	数据
1	创建 SA 消息的过滤列表
2	接收 SA 消息的过滤列表
3	转发 SA 消息的过滤列表
4	远端 MSDP peer 地址

配置创建 SA 消息的规则

在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些(S,G)信息发布出去。

版权所有 © 华为技术有限公司

背景信息

在配置了 MSDP Peer 的源 RP 上，进行如下的配置。

说明

当不进行此项配置时，源 RP 创建的 SA 消息中包含所有本地活动源信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **import-source** [**acl** *acl-number*]，配置创建 SA 消息的组播源过滤规则。

- **acl** 为组播源过滤列表。MSDP 创建 SA 消息时只包含符合指定过滤规则的本地源信息，从而可以控制本地（S，G）信息的外流。
- 如果执行不带 **acl** 参数的 **import-source** 命令，SA 消息将不通告任何本地活动源信息。

----结束

配置接收 SA 消息的规则

在远端 MSDP 对等体上配置“接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达设备时，依据此规则决定是否接收。

背景信息

在配置了 MSDP Peer 的交换机上，进行如下的配置。

说明

当不进行此项配置时，交换机接收所有通过 RPF 检查的 SA 消息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-policy import** [**acl** { *advanced-acl-number* }]，配置从远端 MSDP 对等体接收 SA 消息的过滤规则。

- *peer-address* 为远端 MSDP 对等体地址。
- **acl** 指定高级过滤列表。在来自 *peer-address* 的 SA 消息中，选择接收通过该 ACL 规则过滤的（S，G）信息。
- 如果执行不带 **acl** 参数的 **peer** *peer-address* **sa-policy import** 命令，则交换机不接收来自 *peer-address* 的任何（S，G）信息。

----结束

配置转发 SA 消息的规则

在本地设备上配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

版权所有 © 华为技术有限公司

背景信息

在配置了 MSDP Peer 的交换机上，进行如下的配置。

说明

当不进行此项配置时，交换机转发所有通过 RPF 检查的 SA 消息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-policy export** [**acl** *advanced-acl-number*]，配置向远端 MSDP 对等体转发 SA 消息的过滤规则。

- *peer-address* 为远端 MSDP 对等体地址。
- **acl** 指定高级过滤列表。只有通过该 ACL 规则过滤的（S，G）信息才向 *peer-address* 转发。
- 如果执行不带 **acl** 参数的 **peer** *peer-address* **sa-policy export** 命令，则交换机不向 *peer-address* 转发任何（S，G）信息。

----结束

检查配置结果

配置过滤 SA 消息的规则成功后，可以通过命令查看 MSDP 对等体的详细信息和 SA 缓存信息。

操作步骤

- 使用 **display msdp sa-cache** [*group-address* | *source-address* | { *2-byte-as-number* | *4-byte-as-number* }] *命令查看公网实例的 SA 缓存。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Information about (Source, Group)-based SA filtering policy 字段，检查本节配置是否生效。例如：

```
<Quidway> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: Vlanif10 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: 3000
    Export policy: 3002
```


版权所有 © 华为技术有限公司

```
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 10
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 16/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
Peer authentication: unconfigured
Peer authentication type: none
```

执行命令 **display msdp sa-cache**，查看 SA 缓存中的（S，G）信息。

- 如果指定了 *group-address*，则显示指定组对应的（S，G）表项。
- 如果指定了 *source-address*，则显示指定源对应的（S，G）表项。
- 如果指定了 *2-byte-as-number* 或 *4-byte-as-number*，则显示源 RP 属于指定 AS 的（S，G）表项。

```
<Quidway> display msdp sa-cache
MSDP Source-Active Cache Information of VPN-Instance: public net
MSDP Total Source-Active Cache - 3 entries
MSDP matched 3 entries

(8.8.8.8, 225.0.0.200)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 10
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.201)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 1.0
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.202)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 65535.65535
 Uptime: 00:00:33, Expires: 00:05:27
```

6.8.9 配置 MSDP 认证

MSDP 对等体认证包括 MSDP MD5 认证和 Key-Chain 认证，只能选择其中一种认证方式。

建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 MSDP 认证来提高 MSDP 对等体之间建立 TCP 连接的安全性。

应用环境

配置认证可以提高 MSDP 对等体之间建立 TCP 连接的安全性。

前置任务

在配置 MSDP 认证之前，需完成以下任务：

- 配置某单播路由协议，实现域内网络层互通

版权所有 © 华为技术有限公司

- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域间组播**或**配置 PIM-SM 域内 Anycast RP**

数据准备

在配置 MSDP 认证之前，需要准备以下数据。

序号	数据
1	需要配置 MSDP 认证的对等体地址
2	MSDP MD5 认证的密码
3	MSDP Key-Chain 认证的 Key-Chain 名称

配置 MSDP MD5 认证

MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。可以一端为明文形式，一端为密文形式。

背景信息

缺省情况下，没有配置 MSDP MD5 认证。

在配置了 MSDP 对等体的交换机上，进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置 MSDP MD5 认证。

密码不支持空格，区分大小写。

MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。可以一端为明文形式，一端为密文形式。

说明

MSDP MD5 认证与 MSDP Key-Chain 认证互斥。

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

----结束

配置 MSDP Key-Chain 认证

MSDP 对等体两端必须都配置 Key-Chain 认证，且配置的 Key-Chain 必须使用相同的加密算法和密码，才能正常建立 TCP 连接，交互 MSDP 消息。

版权所有 © 华为技术有限公司

背景信息

缺省情况下，没有配置 MSDP Key-Chain 认证。

在配置了 MSDP 对等体的交换机上，进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **keychain** *keychain-name*，配置 MSDP Key-Chain 认证。

MSDP 对等体两端必须都配置 Key-Chain 认证，且配置的 Key-Chain 必须使用相同的加密算法和密码，才能正常建立 TCP 连接，交互 MSDP 消息。

配置 MSDP Key-Chain 认证前，必须配置 *keychain-name* 对应的 Key-Chain，否则 TCP 连接不能正常建立。

说明

MSDP MD5 认证与 MSDP Key-Chain 认证互斥。

----结束

检查配置结果

配置 MSDP 认证成功后，可以通过命令查看 MSDP 对等体的简要信息和详细信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Peer authentication 和 Peer authentication type 字段，检查本节配置是否生效。例如：

```
<Quidway> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: Vlanif10 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: 3000
    Export policy: 3002
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 10
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
```


版权所有 © 华为技术有限公司

```
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 16/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
  Peer authentication: configured
  Peer authentication type: KeyChain
```

6.8.10 维护 MSDP

MSDP 的维护包括：清除 MSDP 对等体统计信息、清除 SA-Cache 中缓存的(S,G)信息、监控 MSDP 的运行状况。

清除 MSDP 对等体统计信息

清除 MSDP 对等体的统计信息时，可根据实际情况选择重置或不重置 MSDP 对等体之间的 TCP 连接，注意清除后无法恢复。重置 TCP 连接会影响 MSDP 的运行。

背景信息

注意

清除 MSDP 对等体统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要重置与指定 MSDP 对等体的 TCP 连接，并清除指定 MSDP 对等体的所有统计信息后，请在用户视图下执行 **reset msdp peer** [*peer-address*]命令。
- 在确认需要在不重置 MSDP 对等体的情况下清除一个或多个 MSDP 对等体的统计信息后，请在用户视图下执行 **reset msdp statistics** [*peer-address*]命令。
- 在确认需要清除接收、发送和丢弃的 MSDP 报文的计数后，请在用户视图下执行 **reset msdp control-message counters** [**peer** *peer-address*]命令。

----结束

清除 SA-Cache 中缓存的（S，G）信息

需要重置 SA Cache 中的内容时，可以清除 SA Cache 中缓存的所有(S,G)信息，注意清除后无法恢复。

背景信息

注意

清除 SA-Cache 中缓存的（S，G）信息后，以前的（S，G）信息将无法恢复，务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在确认需要清除 SA-Cache 中缓存的（S，G）信息后，请在用户视图下执行 **reset msdp sa-cache** [*group-address*]命令。

----结束

监控 MSDP 的运行状况

在 MSDP 日常维护中，可以在任意视图下选择执行 display 命令，了解 MSDP 的运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 MSDP 的运行状况。

操作步骤

- 在任意视图下执行 **display msdp brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]命令，查看 MSDP 对等体状态的简要信息。
- 在任意视图下执行 **display msdp peer-status** [*peer-address*]命令，查看公网实例的 MSDP 对等体状态的详细信息。
- 在任意视图下执行 **display msdp sa-cache** [*group-address* | *source-address* | { *2-byte-as-number* | *4-byte-as-number* }] *命令,查看 SA 缓存中的（S，G）信息。
- 在任意视图下执行 **display msdp sa-count** [*2-byte-as-number* | *4-byte-as-number*]命令，查看 MSDP 缓存中的（S，G）项的数量。
- 在任意视图下执行 **display msdp control-message counters** [**peer** *peer-address* | **message-type** { **source-active** | **sa-request** | **sa-response** | **keepalive** | **notification** | **traceroute-request** | **traceroute-reply** | **data-packets** | **unknown-type** }] *命令，查看接收、发送和丢弃的 MSDP 报文的计数。

----结束

调试 MSDP

出现 MSDP 运行故障时，可以在用户视图下打开相应的 debugging 调试开关，查看发送和接收的报文内容，从而定位故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

- 在用户视图下执行 **debugging msdp all** 命令，打开 MSDP 的所有调试信息开关。

版权所有 © 华为技术有限公司

- 在用户视图下执行 **debugging msdp connect** 命令，打开 MSDP 对等体的 TCP 连接重置调试信息开关。
- 在用户视图下执行 **debugging msdp event** 命令，打开 MSDP 的事件调试信息开关。
- 在用户视图下执行 **debugging msdp packet** 命令，打开 MSDP 的报文调试信息开关。
- 在用户视图下执行 **debugging msdp source-active** 命令，打开 MSDP 的活跃源调试信息开关。

----结束

6.8.11 配置举例

通过配置举例，可以了解如何通过 MBGP 对等体实现 PIM-SM 域间组播、通过静态 RPF 对等体实现 AS 间组播、配置 PIM-SM 域内 Anycast RP。

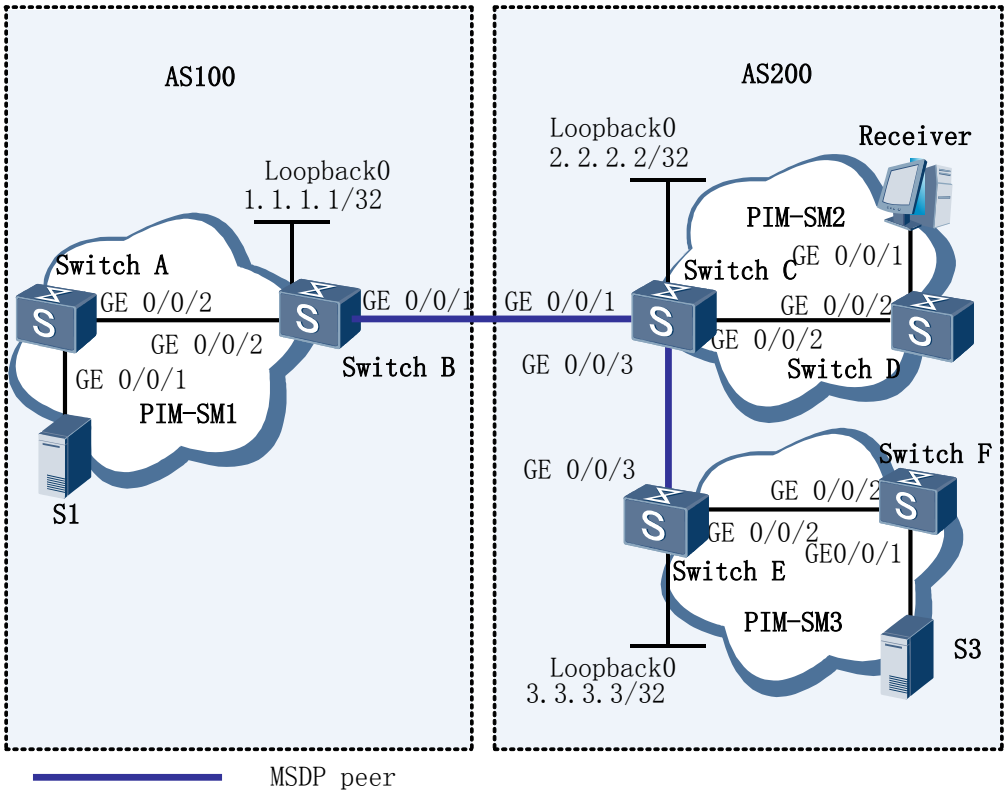
配置 MSDP 基本功能示例

组网需求

如图 6-20 所示，网络中存在两个自治系统 AS。每个 AS 包含一个或多个 PIM-SM 域，每个 PIM-SM 域拥有 0 个或 1 个组播源和接收者。要求：PIM-SM2 域内的 Receiver 既能接收到 PIM-SM3 域 S3 发送的组播数据，又能接收到 PIM-SM1 域 S1 发送的组播数据。

版权所有 © 华为技术有限公司

图 6-20 配置 MSDP 基本功能组网图



Switch	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF101	10.110.1.1/24
SwitchA	GE0/0/2	VLANIF100	192.168.1.1/24
SwitchB	GE0/0/1	VLANIF200	192.168.2.1/24
SwitchB	GE0/0/2	VLANIF100	192.168.1.2/24
SwitchC	GE0/0/1	VLANIF200	192.168.2.2/24
SwitchC	GE0/0/2	VLANIF300	192.168.3.1/24
SwitchC	GE0/0/3	VLANIF400	192.168.4.1/24
SwitchD	GE0/0/1	VLANIF102	10.110.2.1/24
SwitchD	GE0/0/2	VLANIF300	192.168.3.2/24
SwitchE	GE0/0/2	VLANIF500	192.168.5.1/24
SwitchE	GE0/0/3	VLANIF400	192.168.4.2/24
SwitchF	GE0/0/1	VLANIF103	10.110.3.1/24
SwitchF	GE0/0/2	VLANIF500	192.168.5.2/24

配置思路

在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系：

1. 配置各 Switch 接口 IP 地址，为保证 AS 内单播路由畅通，在自治系统内配置 OSPF 协议。
2. 为保证 AS 间单播路由畅通，在 AS 之间配置 EBGP 对等体，将 BGP 与 OSPF 互相引入。

版权所有 © 华为技术有限公司

3. 启动组播功能，在各接口上启动 PIM-SM 功能，配置域边界，在主机侧接口上使能 IGMP 功能。
4. 配置 CBSR、C-RP。将 PIM-SM1 域和 PIM-SM2 域的 RP 配置在 ASBR 上。
5. 在各个域的 RP 之间建立 MSDP 对等体关系。AS 间的 MSDP 对等体与 EBGP 对等体使用相同的接口地址。根据 RPF 规则，接收从到达源 RP 的路由下一跳发来的 SA 消息。

数据准备

为完成此配置举例，需要准备如下数据：

- 组播组 G 地址：225.1.1.1/24。
- SwitchA 和 SwitchB 所在 AS 号为 100。SwitchB 的 router id 为 1.1.1.1。
- SwitchC 和 SwitchD 所在 AS 号为 200。SwitchC 的 router id 为 2.2.2.2。
- SwitchE 和 SwitchF 在 AS 号为 200。

说明

配置用例中，只列出了与配置 MSDP 相关的命令。

操作步骤

步骤 1 配置各 Switch 接口 IP 地址和单播路由协议。

按照图 6-20 配置各 Switch 口的 IP 地址和掩码，配置各 Switch 间采用 OSPF 进行互连。确保 AS 内网络层互通，且各 Switch 之间能够借助单播路由协议实现动态路由更新。具体配置过程略。

步骤 2 在 AS 之间配置 EBGP 对等体，将 BGP 与 OSPF 互相引入。

在 SwitchB 上配置 EBGP 协议，并引入 OSPF 路由。

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.1
[SwitchB-bgp] peer 192.168.2.2 as-number 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

在 SwitchC 上配置 EBGP 协议，并引入 OSPF 路由。

```
[SwitchC] bgp 200
[SwitchC-bgp] router-id 2.2.2.2
[SwitchC-bgp] peer 192.168.2.1 as-number 100
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

在 SwitchB 中的 OSPF 中引入 BGP。SwitchC 上的配置过程与 SwitchB 上的配置相似，配置过程略。

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

步骤 3 启动组播功能，在接口上启动 PIM-SM 功能，配置域边界，在主机侧接口上使能 IGMP 功能。

在 SwitchB 上启动组播功能，并在各接口上启动 PIM-SM 功能。其他 Switch 的配置过程与 SwitchB 上的配置相似，配置过程略。

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 100
```


版权所有 © 华为技术有限公司

```
[SwitchB-Vlanif100] pim sm
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] pim sm
```

在 SwitchB 的 VLANIF100 上配置域边界。

```
[SwitchB-Vlanif100] pim bsr-boundary
[SwitchB-Vlanif100] quit
```

在 SwitchC 的 VLANIF200 和 VLANIF400 上配置域边界。在 SwitchE 的 VLANIF400 上的配置 BSR 服务边界。配置过程与 SwitchB 上的配置相似，配置过程略。

在 SwitchD 连接末梢网络的接口上使能 IGMP 功能。

```
[SwitchD] interface vlanif 102
[SwitchD-Vlanif102] igmp enable
```

步骤 4 配置 CBSR、C-RP。

在 SwitchB 上创建 Loopback0 接口，配置 CBSR 和 C-RP。SwitchC 和 SwitchE 上的配置过程与 SwitchB 上的配置相似，配置过程略。

```
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] ip address 1.1.1.1 255.255.255.255
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

步骤 5 配置 MSDP 对等体。

在 SwitchB 上配置 MSDP 对等体。

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.2.2 connect-interface vlanif 200
[SwitchB-msdp] quit
```

在 SwitchC 上配置 MSDP 对等体。

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.2.1 connect-interface vlanif 200
[SwitchC-msdp] peer 192.168.4.2 connect-interface vlanif 400
[SwitchC-msdp] quit
```

在 SwitchE 上配置 MSDP 对等体。

```
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.4.1 connect-interface vlanif 400
[SwitchE-msdp] quit
```

步骤 6 验证配置结果。

通过使用 **display bgp peer** 命令可以查看 Switch 之间 BGP 对等体关系。例如 SwitchB、SwitchC 上 BGP 对等体关系的显示信息如下：

```
[SwitchB] display bgp peer

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 1                    Peers in established state : 1

  Peer          V    AS   MsgRcvd    MsgSent    OutQ    Up/Down     State          PrefRcv

  192.168.2.2   4    200   24         21          0      00:13:09    Established    6
```


版权所有 © 华为技术有限公司

```
[SwitchC] display bgp peer

BGP local router ID : 2.2.2.2
 Local AS number : 200
 Total number of peers : 1                    Peers in established state : 1

  Peer          V   AS    MsgRcvd    MsgSent     OutQ   Up/Down    State          PrefRcv

  192.168.2.1   4   100   18         16          0      00:12:04   Established    1
```

通过使用 **display bgp routing-table** 命令可以查看 Switch 上的 BGP 路由表。例如 SwitchC 上 BGP 路由表的显示信息如下：

```
[SwitchC] display bgp routing-table

 Total Number of Routes: 5
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop         MED        LocPrf    PrefVal Path/Ogn
 *>   1.1.1.1/32         192.168.2.1     0                    0       100?
 *>i  2.2.2.2/32         0.0.0.0         0                    0       ?
 *>   192.168.2.0        0.0.0.0         0                    0       ?
 *>   192.168.2.1/32     0.0.0.0         0                    0       ?
 *>   192.168.2.2/32     0.0.0.0         0                    0       ?
```

通过使用 **display msdp brief** 命令可以查看 Switch 之间 MSDP 对等体建立情况。SwitchB、SwitchC 和 SwitchE 上 MSDP 对等体建立情况的简要信息如下：

```
[SwitchB] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.2.2        UP        00:12:27        200    13         0

[SwitchC] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  2            2            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.2.1        UP        01:07:08        100    8          0
  192.168.4.2        UP        00:06:39        200    13         0

[SwitchE] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.4.1        UP        00:15:32        200    8          0
```

通过使用 **display msdp peer-status** 命令可以查看 Switch 上的 MSDP 对等体的详细信息。SwitchB 上 MSDP 对等体的详细信息如下：

```
[SwitchB] display msdp peer-status

  MSDP Peer 192.168.2.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: vlanif200 (192.168.2.1)
```


版权所有 © 华为技术有限公司

```
    Number of sent/received messages: 16/16
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:17:51
  Information about (Source, Group)Based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SACache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: unconfigured
    Peer authentication type: none
```

通过使用 **display pim routing-table** 命令可以查看 Switch 上的 PIM 路由表。当 PIM-SM1 内组播源 S1（10.110.1.2/24）和 PIM-SM3 内的 S3（10.110.3.2/24）向组播组 G（225.1.1.1）发送组播信息时，PIM-SM2 内的组成员 Receiver（10.110.2.2/24）能接收到相应的组播信息。SwitchB 和 SwitchC 上的 PIM 路由表显示信息如下：

```
[SwitchB] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.1.2, 225.1.1.1)
     RP: 1.1.1.1(local)
     Protocol: pim-sm, Flag: SPT EXT ACT
     UpTime: 00:00:42
     Upstream interface: vlanif200
         Upstream neighbor: 192.168.1.1
         RPF neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif100
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-

[SwitchC] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 2 (S, G) entries

(*, 225.1.1.1)
     RP: 2.2.2.2 (local)
     Protocol: pim-sm, Flag: WC RPT
     UpTime: 00:13:46
     Upstream interface: NULL,
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif300,
             Protocol: pim-sm, UpTime: 00:13:46, Expires:-
(10.110.1.2, 225.1.1.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT MSDP ACT
     UpTime: 00:00:42
     Upstream interface: vlanif200
         Upstream neighbor: 192.168.2.1
         RPF neighbor: 192.168.2.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif300
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-
(10.110.3.2, 225.1.1.1)
```


版权所有 © 华为技术有限公司

```
RP: 2.2.2.2
Protocol: pim-sm, Flag: SPT MSDP ACT
UpTime: 00:00:42
Upstream interface: vlanif400
    Upstream neighbor: 192.168.4.2
    RPF neighbor: 192.168.4.2
Downstream interface(s) information:
Total number of downstreams: 1
    1: vlanif300
        Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100 101
#
 multicast routing-enable
#
interface Vlanif100
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100 200
#
 multicast routing-enable
#
interface Vlanif100
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
bgp 100
 router-id 1.1.1.1
 peer 192.168.2.2 as-number 200
 import-route ospf 1
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.2.2 connect-interface vlanif200
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
 multicast routing-enable
#
interface Vlanif200
 ip address 192.168.2.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlanif300
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlanif400
 ip address 192.168.4.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
bgp 200
 router-id 2.2.2.2
 peer 192.168.2.1 as-number 100
 import-route ospf 1
#
```


版权所有 © 华为技术有限公司

```
ospf 1
 import-route bgp
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.2.1 connect-interface vlanif200
 peer 192.168.4.2 connect-interface vlanif400
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 102 300
#
 multicast routing-enable
#
interface Vlanif102
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif300
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
 vlan batch 400 500
#
 multicast routing-enable
#
interface Vlanif400
 ip address 192.168.4.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlanif500
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.4.1 connect-interface vlanif400
#
return
```

- SwitchF 的配置文件

```
#
 sysname SwitchF
#
 vlan batch 103 500
#
 multicast routing-enable
#
interface Vlanif103
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
#
ospf 1
 area 0.0.0.0
  network 192.168.5.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
#
return
```

6.9 IPv4 组播路由管理

系统可同时维护多个组播路由协议，通过控制平面与转发平面之间的信息交互，控制组播路由和转发。

6.9.1 IPv4 组播路由管理概述

组播路由与转发维护协议路由表、组播路由表和组播转发表。组播路由协议应用 RPF 机制创建组播路由表项。

AC6605 的组播实现中，组播路由与转发分为三个方面：

版权所有 © 华为技术有限公司

- 每个组播路由协议有一个协议自身的路由表，如 PIM Routing-Table。
- 各个组播路由协议的组播路由信息经过综合形成一个总的组播路由表，即 Multicast Routing-Table。

  Multicast Routing-Table 是组播路由管理模块中的路由表，由一组（S，G）表项组成。（S，G）表示由源 S 向组播组 G 发送的组播数据的路由信息。如果组播路由管理支持多种组播协议，则路由表中将包括由多种协议生成的组播路由。路由表项直接下发到转发表中。
- 组播转发表直接控制着组播数据包的转发，即 Multicast Forwarding-Table。

  Multicast Forwarding-Table 是真正指导组播数据转发的组播转发表。组播转发表与组播路由表保持一致。

组播路由协议运用 RPF（Reverse Path Forwarding）机制创建组播路由表项，以确保组播数据能够沿正确的路径传输。

系统根据以下几种路由执行 RPF 检查：

- 单播路由

  单播路由表中汇集了到达各个目的地址的最短路径。
- MBGP 路由

  MBGP 路由表直接提供组播路由信息。
- MIGP 路由

  MIGP 路由表提供根据 TE Tunnel 的物理接口计算出的路由信息，以指导组播报文转发。
- 组播静态路由

  组播静态路由表中列举了用户通过静态配置指定的 RPF 路由信息。

6.9.2 AC6605 支持的 IPv4 组播路由管理特性

系统支持的 IPv4 组播路由管理特性包括：组播静态路由、组播路由策略、控制组播转发的范围、控制组播转发表的规模、组播路由测试、以及组播负载分担。

组播静态路由

组播静态路由是 RPF 检查的重要依据。通过配置组播静态路由，用户可以在当前交换机上为特定“报文源”指定 RPF 接口和 RPF 邻居。

组播静态路由不能用于数据转发，它可以用来改变 RPF 路由或衔接 RPF 路由。

组播静态路由仅在所配置的组播交换机上生效，不会以任何方式被广播或者引入给其他交换机。

组播路由策略

运行组播的交换机选择上游接口时，若存在多条开销相同的单播路由，用户可以设置交换机选取 RPF 路由的方式，有以下三种：

- 缺省情况下，选择下一跳地址最大的路由。
- 按照最长匹配原则，选取目的地址与“报文源”地址匹配最长的路由。
- 各路由之间负载分担。根据不同的策略进行组播流量的负载分担，可以优化存在多个组播数据流时的网络流量。

版权所有 © 华为技术有限公司

组播负载分担策略共有 5 种：稳定优先、均衡优先、基于源地址、基于组地址、基于源/组地址。这 5 种负载分担策略是互斥的。在稳定优先和均衡优先负载分担方式中，还可以在接口上配置组播负载分担权值，实现组播不均衡负载分担。

控制组播转发的范围

网络中组播信息的转发不会是漫无边际的，每个组播组对应的组播信息都需要在一个确定的范围内传递。AC6605 允许用户通过以下方式定义组播转发范围：

- 在接口上配置组播转发边界，以形成一个封闭的组播转发区域。

控制组播转发表的规模

ISP 根据所提供的组播业务进行具体的网络规划时，可以进行如下的策略配置：

- 限制组播转发表中的表项数量

  交换机为每一个接收到的组播报文都维护有对应的转发表项。但是，过量的组播转发项将有可能会耗尽交换机内存。AC6605 允许用户自己定义交换机组播转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当的限制，可以避免由此引发的交换机故障。

- 限制单个转发表项的下行节点数量

  交换机为每一个下行节点复制一份组播报文，发送出去。每一个下行节点形成组播分发树的一路分支。下行节点数决定了组播分发树可能达到的最大规模和组播服务范围。AC6605 允许用户自己定义单个转发表项的下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当的限制，可以缓解交换机的处理压力，并控制组播服务范围。

组播路由测试

当组播网络出现故障时，可以首先使用 **ping multicast** 与 **mtrace** 命令测试网络连接是否正常工作。

ping multicast 命令主要用于检查组播组是否可达，实现以下功能：

- Ping 保留组地址：用来检测直连网段上是否存在保留组成员，不仅限于组播网络，还可以 Ping 其他使用组播地址的设备。
- Ping 普通组播组地址，有以下两个作用：
  - 构造组播流量，触发建立组播路由表项。用户通过查看组播路由信息来检查协议状态是否正常，判断网络是否具备承载组播业务的能力，或者测试转发性能。
  - 检查网络中存在的组成员。发起 Ping 的交换机通过统计目的主机反馈的 ICMP-Echo-Reply 报文来确定网络中存在的哪些组成员、计算从 Ping 发起者到组成员的 TTL、响应时间等。还可以按照一定时间间隔多次发起 Ping，以计算网络时延和路由抖动。

mtrace 能够追踪以下 4 种路径，并输出逐跳信息。

- 从组播源到查询者的 RPF 路径
- 从组播源到查询者的组播路径
- 从组播源到目的主机的 RPF 路径
- 从组播源到目的主机的组播路径

版权所有 © 华为技术有限公司

说明

使用 NQA 测试例或命令行都可以执行 Ping 组播地址的功能，NQA 测试例的配置方法请参见《AC6605 无线接入控制器 配置指南-网络管理》的“ NQA 配置”。

6.9.3 配置组播静态路由

组播静态路由实现的功能包括：改变 RPF 路由和衔接 RPF 路由。

建立配置任务

在配置组播静态路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

以具体应用环境区分，组播静态路由主要有两种功能：

- 改变 RPF 路由

  当网络中组播拓扑结构和单播拓扑结构相同时，组播数据的传输路径与单播相同。AC6605 允许用户配置组播静态路由，从而更改 RPF 路由，为组播数据创建一条与单播不同的传输路径。

- 衔接 RPF 路由

  在单播路由被阻断的网段，未配置组播静态路由时，由于没有 RPF 路由而无法进行报文转发。AC6605 允许用户配置组播静态路由，从而生成 RPF 路由、完成 RPF 检查，最终创建路由表项、指导报文转发。

前置任务

在配置组播静态路由之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播静态路由之前，需准备以下数据。

序号	数据
1	组播源地址、掩码/掩码长度
2	单播路由协议
3	过滤策略、优先级

配置组播静态路由

配置组播静态路由，可以在当前组播设备上指定 RPF 接口和 RPF 邻居。

版权所有 © 华为技术有限公司

背景信息

注意

配置组播静态路由时，若下一跳接口是点对点形式，则可在命令中配置出接口。若下一跳接口是非点对点形式，则必须使用下一跳地址形式。

在组播交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip rpf-route-static** *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] { *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]，配置组播静态路由。

- *source-address* {*mask* | *mask-length* }是组播源地址及掩码。
- 指定 **isis** *process-id*、**ospf** *process-id*、**rip** *process-id*、**bgp**、**static** 表示匹配的路由必须在指明的单播路由协议中出现。*process-id* 是进程号。
- **route-policy** *policy-name* 是静态组播路由的匹配规则。
- *interface-type interface-number* 是出接口类型及编号，作为 RPF 接口。
- **preference** *preference* 是路由优先级，优先级数值越大，优先级越低。
- **order** *order-num* 是同网段路由中的配置先后次序。

----结束

检查配置结果

配置组播静态路由成功后，查看组播静态路由表以及 RPF 路由信息，确保组播网络正常运行。

操作步骤

- 使用 **display multicast routing-table static** [**config**] [*source-address* { *mask* | *mask-length* }]命令查看组播静态路由表信息。
- 使用 **display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]命令查看指定组播源的 RPF 路由信息。

----结束

6.9.4 配置组播路由策略

组播路由策略包括：配置组播路由最长匹配、配置组播负载分担及权值。

建立配置任务

在配置组播路由策略前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

当组播交换机选择上游接口时，可能存在多个开销相同的单播路由。用户可以根据具体的网络需要，从以下三种方法中任选其一，设置 RPF 路由的选择方法。

- 缺省情况下，选择下一跳地址最大的路由。
- 配置按照最长匹配原则，选取目的地址与“报文源”地址匹配最长的路由。
- 配置各路由之间的负载分担。根据不同的策略配置组播负载分担，可以优化存在多个组播数据流时的网络流量。

前置任务

在配置组播路由策略之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播路由策略之前，需准备以下数据。

序号	数据
1	组播负载分担的策略
2	接口的组播负载分担权值

配置组播路由最长匹配

按照最长匹配选择路由时，组播设备会优先选取目的地址与报文源地址匹配“掩码”最长的路由。若存在多条路由掩码匹配长度相同，则按照组播静态路由、域间单播路由、域内单播路由的顺序选择一条路由作为组播数据的转发路径。

背景信息

缺省情况下，按照路由表项的顺序来选择路由。

在组播交换机上进行如下配置。

操作步骤

- 公网实例
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast longest-match**，配置按照最长匹配来选择路由。

----结束

配置组播负载分担

组播负载分担功能扩展了组播选路规则，不完全依赖 RPF 检查。根据不同的策略进行组播流量的负载分担，可以优化存在多个组播数据流时的网络流量。可选择使用均衡优先负载分担或稳定优先负载分担策略。

版权所有 © 华为技术有限公司

背景信息

组播负载分担功能扩展了组播选路规则，不完全依赖 RPF 检查。网络中存在多条等价的最优路由时，它们都可能用来转发组播数据，组播流量可以在多条等价路由间进行负载分担。

缺省情况下，没有配置组播负载分担。

在运行组播的交换机上进行如下配置。

操作步骤

- 公网实例
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast load-splitting** { **source** | **group** | **source-group** }，配置组播负载分担。
  3. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。

     这里的接口可以是 VLANIF 接口和 Loopback 接口。
  4. （可选）执行命令 **multicast load-splitting weight** *weight-value*，配置接口的组播负载分担权值。

     缺省情况下，接口的组播负载分担权值是 1。

     接口的组播负载分担权值越大，以此接口为上游接口的组播路由表项越多。当接口的组播负载分担权值为 0 时，以此接口为出接口的路由不参与组播负载分担。

----结束

配置组播负载分担权值

配置组播负载分担策略后，由于单播各等价路由的转发能力和实际负载情况不同，在一些场景下继续进行均衡负载分担不能满足网络要求。通过为接口配置组播负载分担权值，可以实现组播不均衡负载分担。

背景信息

配置了稳定优先或均衡优先组播负载分担策略时，由于单播各条等价路由的转发能力和实际负载情况不同，在一些场景下继续进行均衡负载分担不能满足网络要求。通过为接口配置组播负载分担权值，可以实现组播不均衡负载分担。

在运行组播的交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **multicast load-splitting weight** *weight-value*，配置接口的组播负载分担权值。

缺省情况下，接口的组播负载分担权值是 1。

版权所有 © 华为技术有限公司

接口的组播负载分担权值越大，以此接口为上游接口的组播路由表项越多。当接口的组播负载分担权值为 0 时，以此接口为出接口的路由不参与组播负载分担。

----结束

检查配置结果

配置组播路由策略成功后，查看组播路由表以及 RPF 路由信息，确保组播网络正常运行。

操作步骤

- 使用以下命令查看组播路由表信息：
  - **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]
- 使用 **display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]命令查看指定组播源的 RPF 路由信息。

----结束

6.9.5 配置组播转发范围

网络中每个组播组对应的组播信息都要在一个确定的范围内传递。通过配置组播转发边界限制组播数据转发范围。

建立配置任务

在配置组播转发范围前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

网络中每个组播组对应的组播信息都需要在一个确定的范围内传递。AC6605 允许用户通过以下方式定义组播转发范围：

- 在接口上配置组播转发边界，以形成一个封闭的组播转发区域。当交换机接口配置了针对某组播组的转发边界以后，将不能再发出或接收该组播组的报文。

前置任务

在配置组播转发范围之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播转发范围之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	组播转发边界的组地址、掩码/掩码长度

配置组播转发边界

当组播设备接口配置了针对某组播组的转发边界后，可以划定组播报文的转发范围。

背景信息

缺省情况下，接口未设置组播转发边界。

在组播交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 VLANIF 接口和 Loopback 接口。

步骤 3 执行命令 **multicast boundary** *group-address* { *mask* | *mask-length* }，配置组播转发边界。

----结束

检查配置结果

配置组播转发范围成功后，查看组播路由表信息、接口的组播边界信息，确保组播网络正常运行。

操作步骤

- 使用以下命令查看组播路由表信息：
  - **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]
- 使用 **display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]命令查看接口的组播边界信息。

----结束

6.9.6 配置组播转发表限制参数

在进行网络规划时，可限定组播设备的转发表容量，包括：组播转发表最大表项数和组播转发表项最大下行节点数。从而缓解组播设备的处理压力，避免因表项过多引发的设备故障。

版权所有 © 华为技术有限公司

建立配置任务

在配置组播转发表限制参数前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

ISP 根据所提供的组播业务进行具体的网络规划时，通常需要进行如下的策略配置：

- 限制组播转发表中的表项数量

  交换机为每一个接收到的组播报文都维护有对应的转发表项。但是，过量的组播转发项将有可能会耗尽交换机内存。AC6605 允许用户自己定义交换机组播转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当的限制，可以避免由此引发的交换机故障。
- 限制单个转发表项的下行节点数量

  交换机为每一个下行节点复制一份组播报文，发送出去。每一个下行节点形成组播分发树的一路分支。下行节点数决定了组播分发树可能达到的最大规模和组播服务范围。AC6605 允许用户自己定义单个转发表项的下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当的限制，可以缓解交换机的处理压力，并控制组播服务范围。

前置任务

在配置组播转发表限制参数之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播转发表限制参数之前，需准备以下数据。

序号	数据
1	组播源地址、组地址、掩码/掩码长度
2	组播路由的匹配策略、路由次序、路由优先级
3	组播转发表中最大路由数目
4	组播转发表中每条路由项的最大下行节点数目

配置组播转发表最大表项数

过量的组播转发项可能会耗尽设备内存。系统允许用户配置组播设备转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当限制，从而避免由此引发的设备故障。

背景信息

缺省情况下，采用交换机系统允许的最大值。

在组播交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **multicast forwarding-table route-limit** *limit*，配置组播转发表最大表项数。

----结束

配置组播转发表项最大下行节点数

组播设备为每一个下行节点复制一份组播报文。系统允许用户定义单个转发表项的最大下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当限制，从而缓解组播设备的处理压力。

背景信息

注意

该配置在执行命令 **reset multicast forwarding-table** 后才生效，执行 **reset multicast forwarding-table** 命令会导致组播业务中断，请谨慎使用。

在组播交换机上进行如下配置。

操作步骤

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **multicast forwarding-table downstream-limit** *limit*，配置组播转发表中单条路由项的最大下行节点数目。配置值小于系统缺省值时有效。

----结束

检查配置结果

配置组播转发表限制参数成功后，查看组播转发表信息，确保组播网络正常运行。

操作步骤

步骤 1 使用 **display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **statistics**] *命令查看组播转发表信息。

----结束

6.9.7 维护 IPv4 组播路由管理

IPv4 组播路由管理的维护包括：测试组播路由、检查 RPF 路径和组播路径、清除组播转发表项和路由表项、监控组播路由和转发状况。

版权所有 © 华为技术有限公司

测试组播路由

当组播数据传输出现故障时，选择执行 ping 命令查看 RPF 路径和组播路径。

背景信息

当组播数据传输出现故障时，可以通过执行以下命令查看 RPF 路径和组播路径。

操作步骤

- 使用 **ping multicast** [**-i** *interface-type interface-number* | **-c** *count* | **-h** *ttl-value* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packet（s）ize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host* 命令 Ping 保留组地址。
- 使用 **ping multicast** [**-c** *count* | **-h** *ttl-value* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packet（s）ize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host* 命令 Ping 普通组地址。

----结束

检查 RPF 路径和组播路径

当组播数据传输出现故障时，选择执行 mtrace 命令查看 RPF 路径和组播路径。

背景信息

说明

查看从组播源到目的主机的 RPF 路径或者组播路径时，需要在连接用户主机的交换机上执行命令 **mtrace query-policy** [*acl-number*]，配置查询者过滤策略。ACL 限定了可信任的查询者的地址范围，最后一跳交换机依据该 ACL 拒绝非法查询者发出的 IGMP-Tracert-Query 消息。使用该命令有以下注意事项：

- 该命令只在最后一跳交换机上生效，且查询者不是最后一跳交换机。
- 该命令只对使用单播 IP 报文封装的 IGMP-Tracert-Query 消息进行过滤。
- 该命令不适用于从查询者本地发起的追踪。

当组播数据传输出现故障时，可以通过执行以下命令查看 RPF 路径和组播路径。

操作步骤

- 使用 **mtrace** [**-ur** *resp-dest* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-name*] * **source** *source-address* 命令查看从组播源到查询者的 RPF 路径。
- 使用 **mtrace -g** *group* [{ **-mr** | **-ur** *resp-dest* } | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-name*] * **source** *source-address* 命令查看从组播源到查询者的组播路径。
- 使用 **mtrace** { **-gw** *last-hop-router* | **-d** } **-r** *receiver* [**-ur** *resp-dest* | **-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-name*] * **source** *source-address* 命令看从组播源到目的主机的 RPF 路径。
- 使用 **mtrace** { **-gw** *last-hop-router* | **-b** | **-d** } **-r** *receiver* **-g** *group* [{ **-mr** | **-ur** *resp-dest* } | **-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-name*] * **source** *source-address* 命令查看从组播源到目的主机的组播路径。

----结束

版权所有 © 华为技术有限公司

清除组播转发表项和路由表项

在确认需要清除组播转发表项和路由表项后，在用户视图下选择执行 reset 命令,清除组播转发表项和路由表项。执行 reset 命令将删除组播转发表或路由表中的信息，可能导致组播数据无法正常传输,请慎用。

背景信息

在确认需要清除组播转发表和路由表的运行信息后，请在用户视图下执行下面的 **reset** 命令。

操作步骤

- 请在用户视图下执行以下命令清除组播转发表中的转发项：
  - **reset multicast forwarding-table all**
  - **reset multicast forwarding-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *
- 请在用户视图下执行以下命令清除组播路由表的路由项：
  - **reset multicast routing-table all**
  - **reset multicast routing-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

----结束

监控组播路由和转发的状况

在 IPv4 组播路由管理日常维护中，在任意视图下选择执行 display 命令，了解组播转发表和路由表的运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解组播转发表和路由表的运行状况。

操作步骤

- 在任意视图下执行 **display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]命令，查看接口上配置的组播边界信息。
- 在任意视图下执行 **display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **statistics**] *命令，查看组播转发表信息。
- 在任意视图下执行以下命令，查看 IP 组播路由表信息：
  - **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface**

版权所有 © 华为技术有限公司

{ **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

- **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

- 在任意视图下执行 **display multicast routing-table static** [**config**] [*source-address* { *mask-length* | *mask* }]命令，查看组播静态路由信息。
- 在任意视图下执行 **display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]命令，查看 RPF（Reverse Path Forwarding）路由信息。

----结束

调试组播转发和路由

出现 IPv4 组播路由管理运行故障时，在用户视图下打开相应的 debugging 调试开关，查看调试信息，从而定位故障原因。打开调试开关将影响系统的性能。调试完毕后应及时关闭调试开关。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging** 命令关闭调试开关。

操作步骤

- 在用户视图下执行以下命令，打开组播转发的调试信息开关：
  - **debugging mfib all**
  - **debugging mfib** { **no-cache** | **module** | **packet** | **register** | **route** | **sync** | **upcall** | **wrong-iif** } [*advanced-acl-number*]
- 在用户视图下执行 **debugging mrm** { **all** | **event** | **packet** [*advanced-acl-number*] | **route** [*advanced-acl-number*] }命令，打开组播路由管理的调试信息开关。

----结束

6.9.8 配置举例

针对如何在组播网络中配置组播静态路由和组播负载分担，分别提供配置举例。

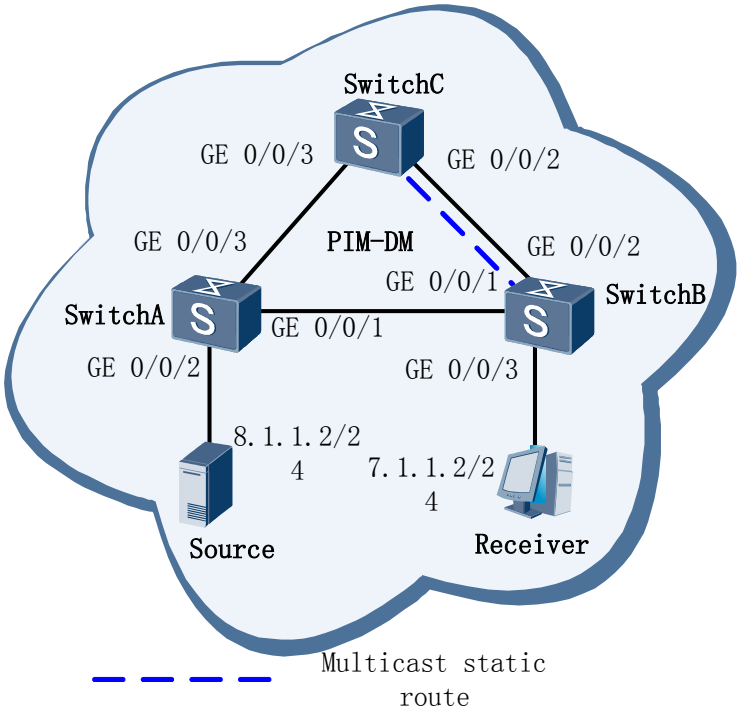
配置组播静态路由改变 RPF 示例

版权所有 © 华为技术有限公司

组网需求

如图 6-21 所示，网络中运行 PIM-DM，所有 Switch 支持组播，且 Receiver 能够正常接收组播源 Source 的信息。SwitchA、SwitchB 和 SwitchC 之间运行 OSPF 协议。要求：使用组播静态路由，使 Source 到 Receiver 的组播路径与单播路径不同。

图 6-21 配置组播静态路由改变 RPF 路由组网图



Switch	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF10	9.1.1.1/24
	GE0/0/2	VLANIF20	8.1.1.1/24
	GE0/0/3	VLANIF30	12.1.1.1/24
SwitchB	GE0/0/1	VLANIF10	9.1.1.2/24
	GE0/0/2	VLANIF40	13.1.1.1/24
	GE0/0/3	VLANIF50	7.1.1.1/24
SwitchC	GE0/0/2	VLANIF40	13.1.1.2/24
	GE0/0/3	VLANIF30	12.1.1.2/24

配置思路

采用如下的思路配置组播静态路由：

1. 配置各 Switch 接口 IP 地址和 OSPF 单播路由协议。
2. 使能组播功能，在各接口上使能 PIM-DM，在与主机相连的接口上使能 IGMP。
3. 在 SwitchB 上配置 RPF 组播静态路由，指定 RPF 邻居为 SwitchC。

数据准备

为完成此配置举例，需要准备如下数据：

版权所有 © 华为技术有限公司

- Source 的 IP 地址。
- SwitchB 上到 SwitchC 的出接口为 VLANIF40。

说明

配置用例中，只列出了与配置组播静态路由相关的命令。

操作步骤

步骤 1 配置各 Switch 接口 IP 地址和单播路由协议。

按照图 6-21 配置各 Switch 接口的 IP 地址和掩码。注意 SwitchIP 地址要在 VLANIF 接口上配置。SwitchA、SwitchB 和 SwitchC 之间运行 OSPF，能够借助单播路由协议实现动态路由更新。配置过程略。

步骤 2 使能组播功能，并在各接口上使能 PIM-DM 功能。

在所有 Switch 启动组播功能，并在各接口上使能 PIM-DM 功能，主机侧接口上使能 IGMP 功能。其他 Switch 的 PIM-DM 功能配置过程与 SwitchB 上的配置相似，配置过程略。

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] pim dm
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] pim dm
[SwitchB-Vlanif40] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] pim dm
[SwitchB-Vlanif50] igmp enable
[SwitchB-Vlanif50] quit
```

在 SwitchB 上执行 **display multicast rpf-info** 命令，查看 Source 的 RPF 路由信息。发现当前 RPF 路由来源于 unicast，RPF 邻居是 SwitchA。信息显示如下：

```
[SwitchB] display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source 8.1.1.2:
     RPF interface: vlanif10, RPF neighbor: 9.1.1.1
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

步骤 3 配置组播静态路由。

在 SwitchB 上配置 RPF 组播静态路由，到 Source 的 RPF 邻居为 SwitchC。

```
[SwitchB] ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
```

步骤 4 验证配置结果。

在 SwitchB 上执行 **display multicast rpf-info** 命令，查看 Source 的 RPF 信息。RPF 信息显示如下。与配置组播静态路由前比较，RPF 路由与 RPF 邻居已经依据静态路由更新。

```
[SwitchB] display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source 8.1.1.2:
     RPF interface: vlanif40, RPF neighbor: 13.1.1.2
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: mstatic
```


版权所有 © 华为技术有限公司

```
Route selection rule: preference-preferred
Load splitting rule: disable
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
interface Vlanif10
 ip address 9.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif20
 ip address 8.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif30
 ip address 12.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 8.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 40 50
#
 multicast routing-enable
#
interface Vlanif10
 ip address 9.1.1.2 255.255.255.0
 pim dm
#
interface Vlanif40
 ip address 13.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif50
 ip address 7.1.1.1 255.255.255.0
 pim dm
 igmp enable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
ospf 1
 area 0.0.0.0
  network 7.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 30 40
#
 multicast routing-enable
#
interface Vlanif30
 ip address 12.1.1.2 255.255.255.0
 pim dm
#
interface Vlanif40
 ip address 13.1.1.2 255.255.255.0
 pim dm
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
return
```

6.10 MLD Snooping 配置

介绍了 MLD（Multicast Listener Discovery）Snooping 在 AC6605 设备上的实现和配置方法。

6.10.1 MLD Snooping 概述

MLD Snooping 运行在 AC6605 设备上，通过侦听 MLD 消息建立组播数据报文的二层转发表，从而管理和控制组播数据报文的转发，只把组播数据报文转发给需要接收该数据的主机。

版权所有 © 华为技术有限公司

如果未启用 MLD Snooping 功能，IPv6 组播报文将会在 VLAN 内进行广播，造成网络带宽的浪费。启用 MLD Snooping 功能后，可带来以下优点：

- 减少了二层网络中的广播报文，节约了网络带宽。
- 提高了信息安全性。
- 便于实现对每个主机单独计费。

6.10.2 AC6605 支持的 MLD Snooping 特性

AC6605 支持的 MLD Snooping 特性有：MLD Snooping 基本特性、MLD Snooping 查询控制器、Router Alert 选项和接口快速离开。

MLD Snooping 基本特性

AC6605 支持的 MLD Snooping 基本特性有：

- 支持 MLDv1、MLDv2。
- 支持 VLAN 的组播策略和组播表项的配置，用以限制 VLAN 内的主机对 IP 组播组的访问。
- 支持将 VLAN 内的接口静态加入组播组。
- 支持将 VLAN 内的接口指定为静态路由器接口，由于静态路由器接口不会老化，有利于用户长期、稳定地接收数据。
- 响应二层网络拓扑变化，并能按照新的网络拓扑正确转发组播数据。

MLD Snooping 查询控制器特性

AC6605 支持的 MLD Snooping 查询控制器特性有：

- 可设置 VLAN 内路由器接口老化时间。

  缺省情况下，如果接口收到 MLD 查询消息，AC6605 将该接口的路由器接口老化时间的剩余值恢复为 180s。如果接口收到 PIM Hello 报文，AC6605 将该接口的路由器接口老化时间的剩余值恢复为 PIM Hello 报文携带的 Holdtime 值。
- 可设置报文最大响应时间，用于控制主机反馈组成员关系报告的最后期限。
- 可设置 VLAN 内的 MLD Snooping 健壮系数。发送 MLD 查询报文时，根据设置的健壮性系数调整 MLD 报文的重发次数。
- 可设置 MLD Snooping 发送通用查询报文的间隔时间，以适应网络的负载变化。
- 可设置 MLD Snooping 的最后成员查询时间间隔，以适应网络的负载变化。
- 可设置对相同内容的 Report 进行抑制的时间，节省网络带宽，减轻网络负担。

接口快速离开

接口快速离开是指当 AC6605 收到主机发送离开某个组播组的 MLD 离开消息时，不再发送查询报文，就将该主机对应组播组的转发项直接从转发表中删除。当接口下只有一个主机时，可以使能接口快速离开功能，及时释放带宽资源。

6.10.3 配置 MLD Snooping 基本功能

介绍启动 MLD Snooping、将接口静态加入组播组，以及将接口配置为静态路由器接口的操作步骤。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

缺省情况下 AC6605 的 MLD Snooping 功能处于关闭状态，因此需要使能 AC6605 的 MLD Snooping 功能。

在启动了 AC6605 的 MLD Snooping 功能后，VLAN 的 MLD Snooping 功能仍处于关闭状态，因此需要使能 VLAN 的 MLD Snooping 功能。

如果某个接口所连接的主机固定需要接收某个组播组的组播数据，可配置该接口静态加入该组播组，成为静态成员接口。静态成员接口不会老化。

在拓扑稳定的网络中，可将 AC6605 的路由器接口配置为静态路由器接口。静态配置的路由器接口永不超时，只能通过配置命令删除。

前置任务

在启动 MLD Snooping 之前，需完成以下任务：

- 创建 VLAN
- 接口加入 VLAN

数据准备

在启动 MLD Snooping 之前，需准备以下数据：

序号	数据
1	预备使能 MLD Snooping 功能的 VLAN 的编号。
2	静态加入组播组的接口编号及所属 VLAN 的编号、组播组 IPv6 地址。
3	配置静态路由器接口编号及所属 VLAN 的编号。

使能 AC6605 的 MLD Snooping 功能

背景信息

要启动 AC6605 的 MLD Snooping 功能，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mld-snooping enable**，启动 AC6605 的 MLD Snooping 功能。

缺省情况下，AC6605 的 MLD Snooping 功能处于禁止状态。

----结束

版权所有 © 华为技术有限公司

使能 VLAN 的 MLD Snooping 功能

背景信息

要启动 VLAN 的 MLD Snooping 功能，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping enable**，启动 VLAN 的 MLD Snooping 功能。

缺省情况下，VLAN 的 MLD Snooping 功能处于禁止状态。

----结束

（可选）配置接口静态加入组播组

背景信息

要配置接口静态加入组播组，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 和 Eth-trunk 接口。

步骤 3 执行命令 **mld-snooping static-group** { *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id* }，配置接口静态加入组播组。

说明

- 使用 **mld-snooping static-group** 命令前，当前接口必须已加入所指定的 VLAN，否则配置无效。
- 当 **mld-snooping static-group** 配置参数 *source-address* 时，需要 MLD 版本为 V2，否则命令可以正常配置，但不生效。

----结束

（可选）配置接口成为静态路由器接口

背景信息

要配置接口成为静态路由器接口，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图

版权所有 © 华为技术有限公司

这里的接口可以是 GigabitGE 和 Eth-trunk 接口。

步骤 3 执行命令 **mld-snooping static-router-port vlan** *vlan-id*，配置静态路由器接口。

说明

使用 **mld-snooping static-router-port vlan** *vlan-id* 命令前，当前接口必须已加入所指定的 VLAN，否则配置无效。

----结束

（可选）配置接口加入最大组播组数量

背景信息

如果限制用户点播组播节目的数量，可配置接口加入的组播组最大数量，控制接口上的数据流量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

这里的接口可以是 GE 接口、Eth-Trunk 接口。

步骤 3 执行命令 **mld-snooping table limit** *limit-num* **vlan** *vlan-id*，配置接口加入的组播组最大数量。

----结束

（可选）配置 MLD 版本

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping version** *version*，配置 MLD Snooping 可以处理的 MLD 协议报文版本。

参数 *version* 只能配置为 1 和 2。

缺省情况下，AC6605 可以处理 MLDv1 的报文。

----结束

检查配置结果

操作步骤

步骤 1 使用 **display mld-snooping configuration** 命令查看 MLD Snooping 配置信息。

版权所有 © 华为技术有限公司

步骤 2 使用 **display mld-snooping** [**vlan** *vlan-id*]命令查看 MLD Snooping 功能的使能状态。

步骤 3 使用 **display mld-snooping port-info** [**vlan** *vlan-id* [**group** *group-ipv6﹣address* [**source-address** *source-ipv6﹣address*] | **verbose**]]命令查看组播组成员接口和路由器接口的信息。

步骤 4 使用 **display mld-snooping router-port** [**vlan** *vlan-id*]命令查看路由器接口的信息。

----结束

6.10.4 配置 VLAN 的组播策略

介绍 VLAN 组播策略的配置方法及步骤。

建立配置任务

应用环境

如果需要限制 VLAN 内主机只能访问某些组播组时，可以通过配置 VLAN 的组播策略来实现。

前置任务

在配置 VLAN 的组播策略之前，需完成以下任务：

- **6.10.3 配置 MLD Snooping 基本功能**

数据准备

在配置 VLAN 的组播策略之前，需准备以下数据：

序号	数据
1	预备配置组播策略的 VLAN 的编号，及该 VLAN 内的组播源接口的编号。
2	（可选）应用组播策略的 MLD 的版本。

配置组播策略

背景信息

要配置组播策略，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping group-policy** *acl-number* [*mld-version*]，配置组播策略。

缺省状况下，VLAN 无组播策略，即 VLAN 内的主机可以加入任何组播组，MLD 协议版本为 V1/V2。

版权所有 © 华为技术有限公司

对应的 ACL6 只能是基本 ACL6 和高级 ACL6，配置组播策略前，首先保证 ACL6 已经创建，并配置了相应的规则，详细配置过程请参见**配置 ACL6**

说明

- 在配置 VLAN 的组播策略时，如果所使用的 ACL 编号对应的 ACL6 未被创建，则该组播策略不生效，VLAN 内的主机可以加入任何组播组。
- 在配置了 VLAN 的组播策略后，如果执行 **undo acl ipv6** 命令删除了该组播策略所使用的 ACL6，则该 VLAN 内的主机可以加入任何组播组。
- 组播策略对静态组播表项无效。

----结束

检查配置结果

操作步骤

步骤 1 使用 **display mld-snooping** [**vlan** *vlan-id*] [**configuration**]命令查看 VLAN 的 MLD Snooping 配置信息。

步骤 2 使用 **display mld-snooping port-info** [**vlan** *vlan-id* [**group** *group-ipv6-address* [**source-address** *source-ipv6-address*] | **verbose**]]命令参看 MLD Snooping 当前表项情。

----结束

6.10.5 配置接口快速离开功能

介绍如何配置 VLAN 内的接口快速离开功能。

建立配置任务

应用环境

当某个 VLAN 内的所有接口下都只可能有一个接收者主机时，可以使能该 VLAN 的接口快速离开功能，以节约网络带宽。

前置任务

需完成的前置任务有两个：

- 在配置 VLAN 内的接口快速离开之前，已完成 **6.10.3 配置 MLD Snooping 基本功能**。
- 已完成 ACL6 的创建。

数据准备

在配置 VLAN 内的接口快速离开之前，需准备以下数据：

序号	数据
1	预备配置接口快速离开的 VLAN 的编号。

版权所有 © 华为技术有限公司

配置接口快速离开

背景信息

要配置接口快速离开，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping prompt-leave** [**group-policy** *acl-number*]，配置接口快速离开功能。

说明

缺省状况下，不允许接口快速离开。

执行步骤 3 时，如果不给出 **group-policy** *acl-number* 参数，则 AC6605 只要从该 VLAN 内的成员接口收到 Done 消息，就将此接口上的转发表项立即删除。

----结束

检查配置结果

操作步骤

步骤 1 使用 **display mld-snooping** [**vlan** *vlan-id*] [**configuration**]命令查看 VLAN 的 MLD Snooping 配置信息。

在配置成功时，执行上面的命令，查看 VLAN 的 MLD Snooping 配置信息，VLAN 内的接口快速离开功能应配置正确。

----结束

6.10.6 配置 MLD Snooping 查询器

介绍如何配置 MLD Snooping 查询器功能。

建立配置任务

应用环境

在没有三层组播设备的网络中，由于二层设备不支持 MLD，因此无法实现 MLD 查询器的相关功能。为了解决这个问题，可以在二层设备上使能 MLD Snooping 查询器，使二层设备能够在数据链路层建立并维护 IPv6 组播转发表项，从而在数据链路层正常转发 IPv6 组播数据。

前置任务

在 VLAN 内配置 MLD Snooping 查询器功能之前，需要先使能 VLAN 的 MLD Snooping 功能。

版权所有 © 华为技术有限公司

数据准备

在 VLAN 内配置 MLD Snooping 查询器功能之前，需准备以下数据：

序号	数据
1	发送 MLD 普遍组查询报文的时间间隔
2	发送 MLD 特定组查询报文的时间间隔
3	MLD 普遍组查询的最大响应时间
4	MLD 普遍组查询报文的 IPv6 源地址
5	MLD 特定组查询报文的 IPv6 源地址

使能 MLD Snooping 查询器

背景信息

要配置 MLD Snooping 查询器，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping querier enable**，使能 MLD Snooping 查询器。

说明

缺省状况下，MLD Snooping 查询器处于关闭状态。

虽然 MLD Snooping 查询器并不参与 MLD 查询器的选举，但是在运行了 MLD 的 IPv6 组播网络中，配置 MLD Snooping 查询器功能不仅没有实际意义，反而可能因为查询器发送的 MLD 查询报文源 IPv6 地址较小而影响 MLD 查询器的选举。

----结束

配置 MLD Snooping 查询和响应

背景信息

AC6605 发出 MLD Snooping 查询报文（包括普遍组查询和特定组查询），会将最大响应时间（max-reponse-time）字段通过命令配置。交换机的下游用户在收到查询报文后，会启动一个定时器，当定时器的值减为 0 时，用户会向该定时器对应的 IPv6 组播组发送 MLD Snooping 成员关系报告报文。

合理配置 MLD Snooping 查询的最大响应时间（max-reponse-time），既可以使交换机对 MLD Snooping 查询报文做出快速响应，又可以减少由于定时器同时超时，造成大量交换机同时发送报告而引起网络拥塞。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping query-interval** *query-interval*，配置发送 MLD Snooping 普遍组查询报文的时间间隔。

步骤 4 执行命令 **mld-snooping max-response-time** *max-response-time*，配置 MLD Snooping 普遍组查询的最大响应时间。

步骤 5 执行命令 **mld-snooping last-listener-query-interval** *time-value*，配置发送 MLD Snooping 特定组查询的时间间隔。

----结束

配置 MLD 查询报文源 IPv6 地址

背景信息

通过下面步骤，配置 MLD 查询报文的源 IPv6 地址：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mld-snooping send-query source-address** *ipv6-address*，配置 MLD 查询报文的源 IPv6 地址。

说明

源地址必须是前缀为 FE80::/64 的 Link-local 地址。

----结束

检查配置结果

操作步骤

步骤 1 使用 **display mld-snooping** [**vlan** *vlan-id*] [**configuration**]命令查看 VLAN 的 MLD Snooping 配置信息。

```
[Quidway] display mld-snooping vlan 95 configuration
 MLD Snooping Configuration for VLAN 95
     mld-snooping enable
     mld-snooping version 2
```

步骤 2 使用 **display mld-snooping configuration** 命令查看全局配置。

```
[Quidway] display mld-snooping configuration
 MLD Snooping Configuration for VLAN 11
     mld-snooping enable
     mld-snooping group-policy 2000 2
 MLD Snooping Configuration for VLAN 12
     mld-snooping enable
```

----结束

版权所有 © 华为技术有限公司

6.10.7 （可选）调整 MLD Snooping 的性能

介绍如何调整 MLD Snooping 的性能，包括路由器接口的老化时间、最后成员查询时间间隔、发送通用查询报文的间隔时间、报文最大响应时间、MLD 健壮系数、响应二层网络拓扑变化、MLD 版本、报文抑制时间、MLD Snooping 表项最大值、Router Alert 字段。

建立配置任务

应用环境

根据网络的实际情况，调整 MLD Snooping 的参数可以优化 AC6605 的组播性能。

前置任务

在调整 MLD Snooping 的性能之前，需完成以下任务：

- **6.10.3 配置 MLD Snooping 基本功能**

数据准备

在调整 MLD Snooping 的性能之前，需准备以下数据：

序号	过程
1	预备调整 MLD Snooping 性能的 VLAN 编号
2	（可选）路由器接口老化时间
3	（可选）最后成员查询时间间隔
4	（可选）通用查询时间间隔
5	（可选）最大响应时间
6	（可选）MLD 健壮系数
7	（可选）MLD Snooping 模块响应二层网络拓扑变化事件时发送的 MLD 通用查询消息的源 IPv6 地址
8	（可选）MLD Snooping 在当前 VLAN 内可以处理的 MLD 报文的版本
9	（可选）对相同内容报文的抑制时间
10	（可选）接口上能够被配置或学习到的 MLD Snooping 表项的数量。

版权所有 © 华为技术有限公司

（可选）配置路由器接口的老化时间

背景信息

要配置路由器接口的老化时间，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping router-aging-time** *router-aging-time*，配置路由器接口老化时间。

缺省情况下，如果接口收到 MLD 查询消息，AC6605 将该接口的剩余路由器接口老化时间恢复为 180s。

----结束

（可选）配置计算成员接口老化时间相关参数

背景信息

要配置计算成员接口老化时间相关参数，需执行以下步骤（以下步骤是并列关系，无先后顺序）：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mld-snooping query-interval** *query-interval*，配置通用查询报文的间隔时间。缺省值为 60s。

步骤 4 执行命令 **mld-snooping max-response-time** *max-response-time*，配置最大响应时间。缺省值为 10s。

步骤 5 执行命令 **mld-snooping robust-count** *robust-count*，配置 MLD 健壮系数。缺省值为 2。

----结束

（可选）配置 MLD 报文的 Router Alert

背景信息

要配置 MLD 报文的 Router Alert，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **mld-snooping require-router-alert**，配置 AC6605 只接收 IP 头带有 Router Alert 的 MLD 报文。

步骤 4 执行命令 **mld-snooping send-router-alert**，配置 AC6605 只发送 IP 头带有 Router Alert 的 MLD 报文。

缺省状况下，AC6605 可以接收 IP 头中不带有 Router Alert 的 MLD 报文。AC6605 向 VLAN 内发送的 MLD 报文的 IP 头带有 Router Alert。

配置步骤 3、步骤 4 是可选配置，配置时没有先后顺序要求。

----结束

（可选）配置 MLD Snooping 响应二层网络拓扑变化事件

背景信息

要配置 MLD Snooping 响应二层网络拓扑变化事件，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mld-snooping send-query enable**，配置 AC6605 的 MLD Snooping 模块响应二层网络拓扑变化事件。

步骤 3 执行命令 **mld-snooping send-query source-address** *ipv6-address*，配置 MLD Snooping 模块响应二层网络拓扑变化事件时发送 MLD 通用查询消息的源 IPv6 地址。

缺省情况下，AC6605 发送 MLD 通用查询消息的源 IPv6 地址为 FE80::。

步骤 3 是可选配置。当配置 AC6605 的 MLD Snooping 模块响应二层网络拓扑变化事件后，如果 AC6605 收到拓扑变化消息，它将发送 MLD 通用查询消息，使得该 AC6605 下游的 AC6605 学习到新的路由器接口。当组播组成员接收到查询消息后，发送 MLD 报告消息进行响应，使得该 AC6605 和它下游的 AC6605 学习到新的组播转发表项。本功能可以使 AC6605 在二层网络拓扑变化后，继续正确转发组播数据。

----结束

（可选）配置 MLD Snooping 对相同内容报文抑制的时间

背景信息

要配置 MLD Snooping 对相同内容的 report 报文进行抑制的时间，需执行以下步骤：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mld-snooping suppression-time** *time-value*，配置 AC6605 的 MLD Snooping 在转发 report 报文时，对相同内容的 report 报文进行抑制的时间。

版权所有 © 华为技术有限公司

说明

- 缺省情况下，对相同 MLD Report 报文的抑制时间为 10s。
- MLD Snooping 对报文的抑制功能，只针对 MLD v1 报文，对 MLD v2 报文无效。

----结束

检查配置结果

操作步骤

步骤 1 使用 **display mld-snooping [vlan** *vlan-id* **]**命令查看 VLAN 的 MLD Snooping 信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

```
<Quidway> display mld-snooping vlan 10
 MLD Snooping Vlan Information for VLAN 10
     MLD Snooping is Enable
     MLD Version is Set to default 1
     MLD Query Interval is Set to default 125
     MLD Max Response Interval is Set to default 10
     MLD Robustness is Set to default 2
     MLD Last Member Query Interval is Set to default 1
     MLD Router Port Aging Interval is Set to 180s or holdtime in hello
     MLD Filter Group-Policy is Set to default : Permit All
     MLD Prompt Leave Disable
     MLD Router Alert is Not Required
     MLD Send Router Alert Enable
     MLD Snooping Querier Disable
```

6.10.8 维护

介绍如何调试 MLD Snooping。

清除 MLD Snooping 表项信息

背景信息

注意

本命令应慎用！使用本命令清除组播转发表中某 VLAN 的转发表项，会引起该 VLAN 内的主机接收组播流暂时性中断，直到主机再次发出 MLD 成员报告消息，AC6605 重新生成转发表项后，主机才能再收到组播流。

在确认需要清除组播转发表中的动态表项后，请在用户视图下执行以下命令。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **reset mld-snooping group** { **vlan** { *vlan-id* | **all** } | **all** }，清楚组播转发表中的动态转发表项。

----结束

清除 MLD Snooping 的统计信息

背景信息

注意

清除 MLD Snooping 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。 在确认需要清除 MLD Snooping 统计信息后，请在用户视图下执行以下命令。

操作步骤

步骤 1 执行 **reset mld-snooping statistics** [**vlan** *vlan-id*]命令，清除 VLAN 的 MLD Snooping 统计信息。

----结束

调试 MLD Snooping

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging mld-snooping all** 命令关闭所有调试开关。

在出现 MLD Snooping 运行故障时，请在用户视图下执行下面的 debugging 命令对 MLD Snooping 进行调试，查看调试信息，并定位故障的原因。

操作步骤

步骤 1 执行 **debugging mld-snooping** [**all** | **event** | **done** [*basic-acl-number*] | **packet** [*advance-acl-number*] | **query** [*advance-acl-number*] | **report** [*advance-acl-number*] | **timer** | **general**]命令，打开 MLD Snooping 的调试开关。

----结束

6.10.9 配置举例

介绍 MLD Snooping 的配置示例。

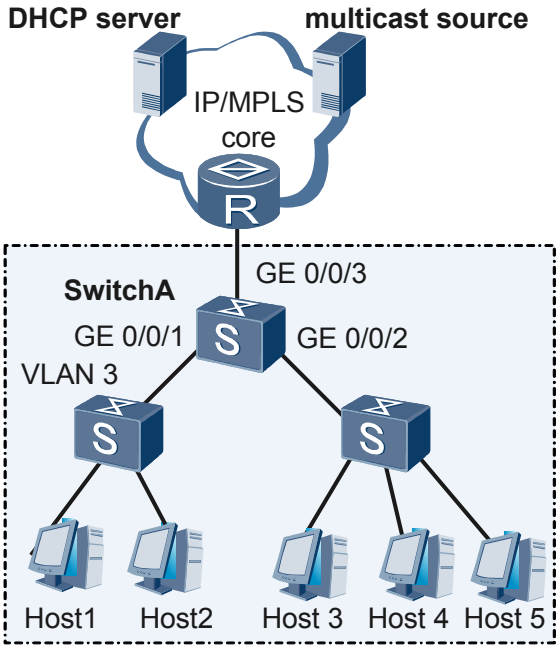
版权所有 © 华为技术有限公司

配置 VLAN 内的接口快速离开示例

组网需求

在如图 6-22 所示的网络中，SwitchA 的接口 GE0/0/1 和接口 GE0/0/2 分别只连接一台接收者主机，它们连接的其它主机都永远不需要接收组播数据报文。因此，当 SwitchA 从这两个接口收到主机发送的 MLD 离开消息后，不需要等到接口的老化定时器超时，就可以直接将这些接口对应主机要离开的组播组的转发表项从转发表中删除，以节约带宽和系统资源。

图 6-22 配置 VLAN 内的接口快速离开组网图



配置思路

采用如下的思路配置接口快速离开：

- 首先在 SwitchA 上创建 VLAN3，并将 SwitchA 上的以太网接口 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN3。
- 在 SwitchA 上使能 MLD Snooping 功能。
- 在 SwitchA 上使能 VLAN3 内的接口快速离开功能。
- 在 SwitchA 上使能 VLAN3 的 MLD Snooping 功能。

数据准备

为完成此配置例，需准备的数据：

- 配置接口快速离开的 VLAN 的编号为 3。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 VLAN3，并将 SwitchA 的 GE0/0/1、GE0/0/2 和 GE0/0/3 加入 VLAN3。配置过程略。

步骤 2 使能 SwitchA 的 MLD Snooping 功能。

```
[SwitchA] mld-snooping enable
```

步骤 3 配置 VLAN 内的接口快速离开。

```
[SwitchA] vlan 3
[SwitchA-vlan3] mld-snooping prompt-leave
```

步骤 4 使能 VLAN3 的 MLD Snooping 功能。

```
[SwitchA-vlan3] mld-snooping enable
```

步骤 5 验证配置结果。在 SwitchA 上执行 **display mld-snooping** 命令。

```
[SwitchA] display mld-snooping vlan 3
 MLD Snooping Vlan Information for VLAN 3
     MLD Snooping is Enable
     MLD Version is Set to default 1
     MLD Query Interval is Set to default 125
     MLD Max Response Interval is Set to default 10
     MLD Robustness is Set to default 2
     MLD Last Member Query Interval is Set to default 1
     MLD Router Port Aging Interval is Set to 180s or holdtime in hello
     MLD Filter Group-Policy is Set to default : Permit All
     MLD Prompt Leave Enable
     MLD Router Alert is Not Required
     MLD Send Router Alert Enable
     MLD Snooping Querier Disable
```

其中“MLD Prompt Leave enable”表示 VLAN 3 内的接口快速离开功能配置成功。

----结束

配置文件

```
#
 sysname SwitchA
#
 mld-snooping enable
#
 vlan batch 3
#
vlan 3
 mld-snooping enable
 mld-snooping prompt-leave
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 3
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 3
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 3
#
return
```


版权所有 © 华为技术有限公司

7 QoS 配置

关于本章

本文档从功能简介、配置方法、维护和配置举例方面介绍了 AC6605 的 QoS 特性，包括基于类的 QoS、流量监管、流量整形、拥塞避免和拥塞管理等功能点。阅读本文档能帮助读者掌握 QoS 的配置方法、应用场景和典型配置案例。

7.1 基于类的 QoS 配置
基于类的 QoS 配置介绍了流分类、流行为、流策略、优先级映射等基本概念，并介绍基于复杂流分类的流策略、基于简单流分类的优先级映射等的配置方法和配置示例。

7.2 流量监管和流量整形配置
流量监管和流量整形配置介绍了流量监管和流量整形基本概念，并介绍了基于类的流量监管、配置流量整形的配置方法和配置示例。

7.3 拥塞避免和拥塞管理配置
拥塞避免和拥塞管理配置介绍了拥塞避免和拥塞管理的基本概念、配置方法和配置示例。

版权所有 © 华为技术有限公司

7.1 基于类的 QoS 配置

基于类的 QoS 配置介绍了流分类、流行为、流策略、优先级映射等基本概念，并介绍基于复杂流分类的流策略、基于简单流分类的优先级映射等的配置方法和配置示例。

7.1.1 基于类的 QoS 概述

基于类的 QoS 是指通过对报文的信息与一定的规则进行匹配，把具有某类共同特征的报文划分为一类，为相同类型的流量提供同等的 QoS 服务，从而针对业务类型的差别提供差分服务。

7.1.2 AC6605 支持的基于类的 QoS 特性

AC6605 支持简单流分类、复杂流分类和优先级映射。

简单流分类

在 AC6605 中，用户可以根据 DiffServ（Differentiated Services）域中定义的报文优先级与 PHB（Per-Hop Behavior）行为之间的映射关系对报文进行简单流分类。对于来自上游设备的报文，在报文的入接口上绑定 DiffServ 域，在 DiffServ 域中将报文携带的优先级信息映射到相应的 PHB 行为、颜色，在设备内部，根据报文的 PHB 行为进行拥塞管理，根据报文的颜色进行拥塞避免；对于流向下游设备的报文，在报文的出接口上绑定 DiffServ 域，在 DiffServ 域中将报文的 PHB 行为、颜色映射为相应的优先级，下游设备根据报文的优先级提供相应的 QoS 服务。

简单流分类的分类依据有：

- VLAN 报文中的 802.1p 优先级
- IP 报文中的 DSCP 优先级

复杂流分类

除了借助 DiffServ 域进行分类外，用户也可以根据报文中携带的二三层信息或者借助 ACL（Access Control List）进行复杂流分类，然后将复杂流分类与某种流行为关联，对符合流分类的报文进行相应处理。

具体采取何种流行为，与报文所处的阶段以及网络当前的负载状况有关。例如，当报文流入节点时依据承诺速率对它进行流量监管、访问控制；流出节点之前进行流量整形、重标记等。

复杂流分类的分类依据有：

- VLAN 报文中的 802.1p 优先级
- VLAN 报文中的 VLAN ID
- CVLAN 报文中的 802.1p 优先级
- CVLAN 报文中的 CVLAN ID
- VLAN 报文中的双层 Tag
- 出/入接口
- IP 报文中的 IP 优先级

版权所有 © 华为技术有限公司

- IP 报文中的 DSCP 优先级
- TCP 报文中的 SYN Flag
- 源 MAC 地址
- 目的 MAC 地址
- 基于二层封装的协议字段
- 三层协议类型
- ACL
- 丢弃报文

优先级映射

不同的报文使用不同的 QoS 优先级，例如 VLAN 报文使用 802.1p 优先级，IP 报文使用 DSCP 优先级或 IP 优先级。当报文经过不同网络时，为了保持报文的优先级，需要在连接不同网络的网关处配置这些优先级标记的映射关系。

为了保证不同报文的服务质量，对于进入设备的报文，AC6605 可以根据配置将报文携带的优先级或端口缺省的 802.1p 优先级映射为内部优先级，然后根据内部优先级与队列之间的映射关系确定报文进入的队列，从而针对队列进行流量整形、拥塞避免、队列调度等处理，并可以根据配置修改报文发送出去时所携带的优先级，以便其他设备根据报文的优先级提供相应的 QoS 服务。

内部优先级与各队列之间的对应关系如表 7-1 所述。

表 7-1 内部优先级与各队列之间的对应关系表

内部优先级	队列索引
BE	0
AF1	1
AF2	2
AF3	3
AF4	4
EF	5
CS6	6
CS7	7

说明

颜色仅用在流量控制时识别是否丢包，对内部优先级与队列的映射关系没有影响。

流行为

进行复杂流分类是为了有区别地提供服务，它必须与某种流量控制或资源分配行为关联起来才有意义。

版权所有 © 华为技术有限公司

在 AC6605 中针对复杂流分类可实施的流行为包括以下几类（这些流行为可以组合使用）：

- 禁止/允许

  禁止/允许是最简单的流行为。AC6605 通过对报文的通过或丢弃处理，来达到控制网络流量的目的。

- 重标记

  重标记是对报文的优先级字段进行设置。在不同的网络中报文使用不同的优先级字段，例如 VLAN 网络使用 802.1p，IP 网络使用 DSCP。因此需要设备可以针对不同的网络对报文的优先级进行重新标记。

  通常网络的边界节点设备需要对进入的报文进行优先级标记。网络内部的节点设备只需按照边界节点所标记的优先级提供相应等级的 QoS 服务即可，或者按自己的标准重新进行标记。

- 重定向

  重定向是指将不按报文原始的目的地址进行路由转发，而是将报文重定向到接 CPU、指定接口或指定的下一跳地址。AC6605 支持指定多个下一跳，最多可指定 4 个下一跳。

  通过重定向可以实现策略路由。这种策略路由是静态的，当配置中的下一跳均不可用时，设备按报文原来的目的地址转发。

  AC6605 仅支持入方向的报文重定向。

- 流量监管

  流量监管就是一种通过对流量规格的监督，来限制流量及其资源使用的流控行为。通过流量监管，可以控制某个流的规格，对于超过规格的流量，可以采取丢弃、重标记颜色、重标记服务级别。

  这里实现的是基于类的流量监管，有关基于类的流量监管及相应配置请参见“**7.2 流量监管和流量整形配置**”。

- 流镜像

  流镜像，即将指定的报文复制到用户指定的目的地，以进行网络检测和故障排除。

  有关流镜像的具体描述及配置请参见《AC6605 无线接入控制器 配置指南-设备管理》中的**使用镜像监控设备**。

- 流量统计

  流量统计用于统计指定业务流的报文，它统计的是设备中转发的报文中匹配已定义的复杂流分类规则的数据信息。

- 禁止 MAC 地址学习

  禁止 MAC 地址学习，即让 AC6605 不再学习满足流分类的报文的 MAC 地址。

  在网络比较稳定、报文的 MAC 地址相对固定的情况下，禁止 MAC 地址学习既可以节省 MAC 地址表项开支，也可以提高设备的运行效率；且当非法用户通过频繁变换 MAC 地址的方式对网络进行攻击时，禁止 MAC 地址学习可以避免此类攻击所造成的设备 MAC 地址表项溢出，保护设备性能不受影响。

流策略

流策略是将流分类和流行为关联后形成的完整的 QoS 策略。用户可以通过流策略将指定的类和流行为绑定起来，方便的进行 QoS 控制。

版权所有 © 华为技术有限公司

7.1.3 配置基于简单流分类的优先级映射

配置基于简单流分类的优先级映射后，设备将报文携带的优先级信息映射到相应的 PHB 行为、颜色，从而提供差异化的服务。

建立配置任务

在配置基于简单流分类的优先级映射前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

对于来自上游设备的报文，用户可以根据报文携带的优先级进行分类，分类依据可以是 802.1p 优先级、DSCP 优先级。在 DiffServ 域中定义优先级到 PHB 行为、颜色的映射关系，作为分类依据。将 DiffServ 域绑定到报文的入接口后，QoS 将能够在报文的出接口上根据报文的 PHB 行为和颜色进行拥塞管理和拥塞避免。

对于流向下游设备的报文，用户可以根据报文的 PHB 行为、颜色进行分类。在 DiffServ 域中定义 PHB 行为、颜色到优先级的映射关系，作为分类依据。将 DiffServ 域绑定到报文的出接口后，下游设备将能够根据报文的优先级提供相应的 QoS 服务。

前置任务

在配置基于简单流分类的优先级映射之前，需完成以下任务：

- 将报文流经的接口加入指定 VLAN

数据准备

在配置基于简单流分类的优先级映射之前，需要准备以下数据。

序号	数据
1	DiffServ 域名
2	上行/下行 VLAN 报文的 802.1p 优先级、上行/下行 IP 报文的 DSCP 优先级、PHB 行为、报文颜色
3	绑定 DiffServ 域的接口类型和编号

配置端口信任的报文优先级

配置端口信任的报文优先级后，AC6605 将根据指定的优先级进行 PHB 映射。

背景信息

AC6605 提供两种优先级信任模式：

- 信任报文的 802.1p 优先级

  对于带 VLAN Tag 的报文，根据报文的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级；对于不带 VLAN Tag 的报文，AC6605

版权所有 © 华为技术有限公司

将使用端口的缺省 802.1p 优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

- 信任报文的 DSCP 优先级

  根据报文的 DSCP 优先级，查找 DSCP 优先级到内部优先级映射表，为报文标记内部优先级。

如果多个接口需要配置相同的信任报文优先级，可通过端口组进行配置，以减少重复配置工作。

说明

内部优先级以 DiffServ 模型的服务等级和颜色表示。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

- *interface-type* 可以是 GE 接口或 Eth-Trunk 接口。
- 端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **trust** { **8021p** { **inner** | **outer** } | **dscp** }，配置端口信任的报文优先级。

缺省情况下，端口信任外层 802.1p 优先级。

----结束

（可选）配置端口的缺省 802.1p 优先级

配置端口的缺省 802.1p 优先级后，如果端口配置的是信任报文的 802.1p 优先级，当端口收到不带 VLAN Tag 的报文时，AC6605 将根据端口的缺省 802.1p 优先级进行 PHB 映射。

背景信息

如果端口收到了不带 VLAN Tag 的报文，则在设备内部转发时需要为其添加缺省的 VLAN 和 802.1p 优先级。

如果端口配置的是信任报文的 802.1p 优先级，端口收到不带 VLAN Tag 的报文时，使用端口的缺省 802.1p 优先级。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port priority** *priority-value*，配置端口的缺省 802.1p 优先级。

缺省情况下，端口的缺省 802.1p 优先级为 0。

----结束

版权所有 © 华为技术有限公司

创建 DiffServ 域并配置优先级映射关系

当 AC6605 作为 DiffServ 域和其他网络的边界节点时，需要配置内部优先级（以 DiffServ 服务等级和颜色表示）和外部优先级（如 802.1p、DSCP、EXP）的相互映射关系。

背景信息

DiffServ 域由一组相连的 DiffServ 节点组成，这些相连的 DiffServ 节点采用相同的服务提供策略并实现相同 PHB 组集合。

当业务流流入设备时，AC6605 将报文携带的优先级信息映射到相应的 PHB 行为、颜色，在设备内部，根据报文的 PHB 行为进行拥塞管理，根据报文的颜色进行拥塞避免；当业务流流出设备时，AC6605 将报文的 PHB 行为、颜色映射为相应的优先级，对端设备根据报文的优先级提供相应的 QoS 服务。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **diffserv domain** { **default** | *ds-domain-name* }，创建 DiffServ 域并进入 DiffServ 域视图。

default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 **default** 域中定义的映射关系，但不能删除 **default** 域。

除了 **default** 域外，AC6605 最多可创建 7 个域。

步骤 3 请根据实际情况对设备的流策略进行定义。

- 在报文的入接口，将 VLAN 报文的 802.1p 优先级映射为 PHB 行为，并为报文着色，执行命令 **8021p-inbound** *8021p-value* **phb** *service-class* [*color*]。
- 在报文的出接口，将 PHB 行为、颜色映射为 VLAN 报文的 802.1p 优先级，执行命令 **8021p-outbound** *service-class color* **map** *8021p-value*。
- 在报文的入接口，将 IP 报文的 DSCP 优先级映射为 PHB 行为，并为报文着色，执行命令 **ip-dscp-inbound** *dscp-value* **phb** *service-class* [*color*]。
- 在报文的出接口，将 PHB 行为、颜色映射为 IP 报文的 DSCP 优先级，执行命令 **ip-dscp-outbound** *service-class color* **map** *dscp-value*。

缺省的 802.1p 优先级到 PHB 行为/颜色、PHB 行为/颜色到 802.1p 优先级、DSCP 到 PHB 行为/颜色、PHB 行为/颜色到 DSCP、EXP 到 PHB 行为/颜色、PHB 行为/颜色到 EXP 的映射关系请分别参见命令 8021p-inbound、8021p-outbound、ip-dscp-inbound、ip-dscp-outbound。

----结束

应用 DiffServ 域

将 DiffServ 域应用到指定的接口后，AC6605 将对通过接口的报文进行 PHB 映射。

背景信息

当需要根据 DiffServ 域中定义的映射关系，对流入设备的报文进行优先级到 PHB 行为和颜色之间的映射操作时，可以将 DiffServ 域绑定到报文的入接口，系统会根据 DiffServ 域中的映射关系将报文的优先级映射为相应的 PHB 行为和颜色。

版权所有 © 华为技术有限公司

当需要根据 DiffServ 域中定义的映射关系，对流出设备的报文进行 PHB 行为到优先级之间的映射操作时，可以将 DiffServ 域绑定到报文的出接口，系统会根据 DiffServ 域中的映射关系将报文的 PHB行为和颜色映射为优先级。

如果多个接口需要应用相同的 DiffServ 域，可通过端口组进行配置，以减少重复配置工作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入报文入接口的接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

- *interface-type* 可以是 GE 接口或 Eth-Trunk 接口。
- 端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **trust upstream** { *ds-domain-name* | **default** | **none** }，在接口上绑定 DiffServ 域。

如果接口上配置了 **trust upstream none** 命令，系统对出/入该接口的报文不做优先级映射。

如果要修改接口下绑定的 DiffServ 域，必须先执行 **undo trust upstream** 命令删除已绑定的 DiffServ 域，再执行 **trust upstream** 命令重新配置新的 DiffServ 域。

缺省情况下，端口上不绑定 DiffServ 域，系统采用缺省的优先级映射关系对出入接口的报文进行优先级映射。缺省的 802.1p 优先级到 PHB 行为/颜色、PHB 行为/颜色到 802.1p 优先级、DSCP 到 PHB 行为/颜色、PHB 行为/颜色到 DSCP 的映射关系请分别参见命令 8021p-inbound、8021p-outbound、ip-dscp-inbound、ip-dscp-outbound。

步骤 4 （可选）执行命令 **undo qos phb marking enable**，取消对接口出方向的报文进行 PHB 映射。

缺省情况下，对接口出方向的报文进行 PHB 映射。

----结束

检查配置结果

配置基于简单流分类的优先级映射完成后，可以查看报文优先级与 PHB 之间的映射关系，以及本地优先级到队列的映射关系。

前提条件

已经完成基于简单流分类的优先级映射配置。

操作步骤

- 执行命令 **display diffserv domain** [**all** | **name** *ds-domain-name*]，查看 DiffServ 域的配置信息。
- 执行命令 **display qos local-precedence-queue-map**，查看本地优先级到队列的映射关系。

----结束

版权所有 © 华为技术有限公司

7.1.4 配置基于复杂流分类的流策略

配置基于复杂流分类的流策略后，AC6605 将根据报文中的优先级、五元组信息等对报文进行流分类，然后对符合不同分类条件的报文执行不同的流动作，如执行禁止/允许、重标记、重定向等。

建立配置任务

在配置基于复杂流分类的流策略前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在网络的入口处，AC6605 作为边界节点。如果需要对进入网络的流量进行限制，则可以根据报文的 DSCP 值、协议类型、IP 地址、端口号、分片报文的类型以及时间段等参数对不同的业务提供差别服务，此时需要配置基于复杂流分类的流策略。

通常是在相对边界的节点上配置复杂流分类，在相对核心的节点上配置简单流分类。

前置任务

在配置基于复杂流分类的流策略之前，需要完成以下任务。

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关路由协议，使网络能够互通
- 如果使用 ACL 作为流分类规则，配置相应的 ACL

数据准备

在配置基于复杂流分类的流策略之前，请根据网络规划，准备好以下数据。

序号	数据
1	定义的流分类名和流分类规则
2	定义的流行为名及相关的参数
3	流策略名
4	应用流策略的接口、VLAN ID

配置复杂流分类

AC6605 支持根据 ACL、报文中的二层信息和三层信息进行流分类。

配置基于二层信息的流分类

配置基于二层信息的流分类后，AC6605 将根据报文中的 802.1p 值，VLAN ID，源/目的 MAC 地址，出/入接口，二层协议类型等二层信息进行流分类。

版权所有 © 华为技术有限公司

背景信息

请在需要配置基于二层信息进行流分类的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个二层流分类，进入流分类视图。

and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则以及其中一条 ACL 规则才能命中；**or** 表示流分类各规则之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

缺省情况下，流分类中各规则之间的关系为“逻辑与”。

步骤 3 定义流分类中的匹配规则。能定义的匹配规则如下：

- 定义基于 QinQ 报文内层 VLAN 的 802.1p 优先级的匹配规则，执行命令 **if-match cvlan-8021p** { *8021p-value* } &<1-8>。
- 定义基于 VLAN 报文 802.1p 优先级的匹配规则，执行命令 **if-match 8021p** { *8021p-value* } &<1-8>。
- 定义基于外层 VLAN ID 或基于 QinQ 报文内外两层 Tag 的 VLAN ID 的匹配规则，执行命令 **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]。
- 定义基于丢弃报文的匹配规则，执行命令 **if-match discard**。
- 定义基于 QinQ 报文双层 Tag 的匹配规则，执行命令 **if-match double-tag**。
- 定义基于目的 MAC 地址匹配规则，执行命令 **if-match destination-mac** *mac-address* [*mac-address-mask*]。
- 定义基于源 MAC 地址的匹配规则，执行命令 **if-match source-mac** *mac-address* [*mac-address-mask*]。
- 定义基于入接口的匹配规则，执行命令 **if-match inbound-interface** *interface-type interface-number*
- 定义基于出接口的匹配规则，执行命令 **if-match outbound-interface** *interface-type interface-number*
- 定义基于以太网帧头中协议类型字段的匹配规则，执行命令 **if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }。
- 定义基于所有报文的匹配规则，执行命令 **if-match any**。

----结束

配置基于三层信息的流分类

配置基于三层信息的流分类后，AC6605 将根据报文中指定的三层信息进行流分类。

背景信息

请在需要配置基于三层信息进行流分类的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个三层流分类，进入流分类视图。

and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中；**or** 表示流分类之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

缺省情况下，流分类中各规则之间的关系为“逻辑与”。

步骤 3 定义流分类中的匹配规则。能定义的匹配规则如下：

- 定义基于 IP 报文 DSCP 优先级的匹配规则，执行命令 **if-match dscp** *dscp-value* &<1-8>。
- 定义基于 IP 报文 IP 优先级的匹配规则，执行命令 **if-match ip-precedence** *ip-precedence-value* &<1-8>。

  说明

  不能在一个逻辑关系为“与”的流分类中同时配置 **if-match dscp** 和 **if-match ip-precedence**。
- 定义基于报文三层协议类型的匹配规则，执行命令 **if-match protocol** { **ip** | **ipv6** }。
- 定义基于 TCP 报文 SYN Flag 的匹配规则，执行命令 **if-match tcp syn-flag syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }。

----结束

配置基于 ACL 的流分类

配置基于 ACL 的流分类后，AC6605 将根据已经定义的 ACL 规则进行流分类。

背景信息

AC6605 可以借助 ACL 实现根据 IP 五元组对报文进行流分类。

AC6605 支持基本 ACL、高级 ACL、二层 ACL、用户自定义 ACL：

- 基本 ACL 主要基于源 IP 地址、分片标志、时间段对数据包进行分类定义。
- 高级 ACL 可以基于源 IP 地址、目的 IP 地址、源端口号、目的端口号、分片标志、时间段、协议类型等对数据包进行更为细致的分类定义。
- 二层 ACL 主要基于源 MAC 地址、目的 MAC 地址对数据包进行分类定义。
- 用户自定义 ACL 主要根据用户自定义的规则对数据报文做出相应的处理。

请根据实际需要选择一种 ACL 配置基于 ACL 的复杂流分类。

操作步骤

- 配置基于基本 ACL 的流分类
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *basic-acl-number*，创建一个基本 ACL，进入 ACL 视图。
  3. （可选）执行命令 **step** *step-value*，配置规则的步长。

版权所有 © 华为技术有限公司

4. 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*]*，定义基本 ACLv4 规则。
5. 执行命令 **quit**，返回系统视图。
6. 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

   and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中；**or** 表示流分类之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

   缺省情况下，流分类中各规则之间的关系为“逻辑与”。
7. 执行命令 **if-match acl** *basic-acl-number*，配置基于基本 ACL 的流分类。

- 配置基于高级 ACL 的流分类
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *advanced-acl-number*，创建一个高级 ACL，进入 ACL 视图。

     说明

     advanced-acl-number 用来指定高级 ACL 的编号，整数形式，取值范围是 3000 ~ 3999。
  3. 请根据实际需求定义规则：
     - 定义针对 GRE、IGMP、IP、IPinIP、OSPF 协议的高级 ACL 规则，执行命令 **rule** [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**tos** *tos*] [**destination** { *destination-address destination-wildcard* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** {*source-address source-wildcard* | **any** } | **time-range** *time-name*] *。
     - 定义针对 TCP 协议的高级 ACL 规则，执行命令 **rule** [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**tos** *tos*] [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **tcp-flag** { *tcp-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }* | **time-range** *time-name*] *。
     - 定义针对 UDP 协议的高级 ACL 规则，执行命令 **rule** [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**tos** *tos*] [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **time-range** *time-name*] *。
     - 定义针对 ICMP 协议的高级 ACL 规则，执行命令 **rule** [*rule-id*] { **deny** | **permit** }{ *protocol-number* | **icmp** } [**tos** *tos*] [**destination** { *destination-address destination-wildcard* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*]*。
  4. 执行命令 **quit**，返回系统视图。
  5. 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

     and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中；**or** 表示流分类之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

版权所有 © 华为技术有限公司

缺省情况下，流分类中各规则之间的关系为“逻辑与”。

6. 执行命令 **if-match acl** *advanced-acl-number*，配置基于高级 ACL 的流分类。

- 配置基于二层 ACL 的流分类
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *mac-acl-number*，创建一个二层 ACL，进入 ACL 视图。

     说明

     mac-acl-number 用来指定二层 ACL 的编号，整数形式，取值范围是 4000 ~ 4999。
  3. （可选）执行命令 **step** *step-value*，配置规则的步长。
  4. 执行命令 **rule** [*rule-id*] { **permit** | **deny** } [{ **ether-ii** | **802.3** | **snap** } | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag**] * [**time-range** *time-range-name*]，配置 ACL 规则。
  5. 执行命令 **quit**，返回系统视图。
  6. 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

     and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中；**or** 表示流分类之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

     缺省情况下，流分类中各规则之间的关系为“逻辑与”。
  7. 执行命令 **if-match acl** *l2-acl-number*，配置基于二层 ACL 的流分类。
- 配置基于用户自定义 ACL 的流分类
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *user-defined-acl-number*，创建一个用户自定义 ACL，进入 ACL 视图。

     说明

     user-defined-acl-number 用来指定用户自定义 ACL 的编号，整数形式，取值范围是 5000 ~ 5999。
  3. （可选）执行命令 **step** *step-value*，配置规则的步长。
  4. 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head**] { *rule-string rule-mask offset* }] [**time-range** *time-range-name*]，定义用户自定义 ACL 规则。
  5. 执行命令 **quit**，返回系统视图。
  6. 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

     and 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中；**or** 表示流分类之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

     缺省情况下，流分类中各规则之间的关系为“逻辑与”。
  7. 执行命令 **if-match acl** *user-defined-acl-number*，配置基于用户自定义 ACL 的流分类。

     用户可以在逻辑关系为“与”的流分类中只配置 **if-match acl** *user-defined-acl-number*，也可以同时配置其他匹配规则。但是在同时 **if-match acl** *user-defined-*

版权所有 © 华为技术有限公司

acl-number 和其他匹配规则时，**if-match acl** *user-defined-acl-number* 只能和 **if-match vlan-id** 或**if-match l2-protocol** 同时配置，否则会导致包含该流分类的流策略应用失败。

----结束

配置流行为

AC6605 支持禁止/允许、重标记、重定向、流量监管、流镜像、流量统计等流行为，请根据实际需要选择配置。

配置禁止或允许动作

通过配置禁止或允许动作，AC6605 将禁止或允许符合流分类规则的报文通过，从而控制网络流量。

操作步骤

步骤 1 请在执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 请根据实际需要进行如下配置：

- 执行命令 **permit**，配置允许动作。
- 执行命令 **deny**，配置禁止动作。

说明

- 如果配置了 **deny** 动作，则符合流分类规则的报文都会丢弃，即使配置其它动作也不会生效（流量统计除外）。
- 如果配置了 **permit** 动作，则对符合流分类规则的报文采取的动作进行逐条匹配。

----结束

配置重标记

通过配置重标记，AC6605 对符合流分类规则的报文的优先级字段进行设置，如 VLAN 报文中的 802.1p、IP 报文中的 DSCP 等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 请根据实际需要进行如下配置：

- 执行命令 **remark 8021p** [*8021p-value* | **inner-8021p**]，将符合流分类的报文重新标记 802.1p 优先级。

  说明

  选择 **inner-8021p** 参数，系统将内层 802.1p 优先级值拷贝到外层。

- 执行命令 **remark vlan-id** *vlan-id*，将符合流分类的 VLAN 报文重新标记外层 VLAN ID。
- 执行命令 **remark destination-mac** *mac-address*，将符合流分类的报文重新标记报文中的目的 MAC 地址。

版权所有 © 华为技术有限公司

说明

不能在同一流行为中既配置 **remark destination-mac** 又配置以下命令:

- **redirect ip-nexthop**
- **redirect ip-multihop**

- 执行命令 **remark dscp** { *dscp-name* | *dscp-value* }，将符合流分类的报文重新标记 DSCP 值。
- 执行命令 **remark local-precedence** { *local-precedence-name* | *local-precedence-value* } [*color*]，将符合流分类的重新标记本地优先级。

  不能在同一个流行为中同时配置 **remark 8021p** 和 **remark local-precedence**。
- 执行命令 **remark ip-precedence** *ip-precedence*，将符合流分类的的报文重新标记 IP 优先级。

  说明

  不能同时重新标记报文的 DSCP 值和它的 IP 优先级。

----结束

配置重定向

通过配置重定向，AC6605 将符合流分类规则的报文重定向到 CPU、指定接口、指定的下一跳地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 请根据实际需要进行如下配置：

- 执行命令 **redirect cpu**，将符合流分类的报文重定向到 CPU。

  注意

  应用包含 **redirect cpu** 的流策略后，会将符合流分类规则的报文重定向到 CPU，对 CPU 造成影响。请谨慎使用此命令。

- 执行命令 **redirect ip-nexthop** *ip-address* &<1-4>，将符合流分类的报文重定向到下一跳。

  当存在多个下一跳时，设备按照主备方式对报文进行重定向转发。一个流行为中最多可以配置 4 个下一跳，设备根据下一跳的配置顺序确定主备链路，配置在前面的下一跳 IP 地址优先级高，配置的第一个下一跳 IP 地址作为主用链路，其它链路作为备用链路。当主用链路 Down 掉之后，则自动选取优先级高的下一跳作为新的主链路。

  说明

  通过配置报文重定向功能可以实现策略路由。

- 执行命令 **redirect ip-multihop** { **nexthop** *ip-address* } &<2-4>，将符合流分类的报文重定向到配置的多个下一跳中的一个。

  如果配置了多个下一跳，设备按照等价路由负载分担方式对报文进行重定向转发，即：设备按照报文的源 IP 地址（不管流量大小）并根据 HASH 算法在多个下一跳中

版权所有 © 华为技术有限公司

选择一个进行转发。源 IP 地址相同的流量，则不管流量多大都是选择同一个下一跳转发。

使用重定向到多下一跳的正常转发过程中，如果当前下一跳对应的出接口状态突然为 Down，或路由突然发生了改变，设备可将链路快速切换到当前可用的某个下一跳对应的出接口上。

如果设备上没有命令中下一跳 IP 地址对应的 ARP 表项，使用此命令能配置成功，但重定向不能生效，设备仍按报文原来的目的地址转发，直到设备上有对应的 ARP 表项。

- 执行命令 **redirect interface** *interface-type interface-number*，将符合流分类的报文重定向到指定接口。

说明

不能在同一流行为中既配置 **remark destination-mac** 又配置以下命令:

- **redirect ip-nexthop**
- **redirect ip-multihop**

----结束

配置流量监管

通过配置流量监管，AC6605 对符合流分类规则的报文的流量进行监督，对于超过规格的流量，可以采取丢弃、重标记颜色、重标记服务级别。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **car cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }]，配置 CAR 动作。

步骤 4 （可选）执行命令 **car** *car-name* **share**，配置共享 CAR 动作。

说明

配置共享 CAR 之前，需要执行 **qos car** 命令配置 CAR 模板。

----结束

配置流镜像

通过配置流镜像，AC6605 将符合流分类规则的所有报文镜像到观察端口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **mirroring to observe-port** *index* 满足流分类规则的所有流镜像到观察端口。

版权所有 © 华为技术有限公司

说明

有关流镜像的详细描述及配置请参见《AC6605 无线接入控制器 配置指南-设备管理》中的**建立基于流的本地流镜像**。

----结束

配置流量统计

通过配置流量统计，AC6605 将对符合流分类规则的报文进行流量统计。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **statistic enable**，使能流量统计功能。

说明

如果需要查看流量统计信息，需要首先在流行为视图下使能流量统计功能。

----结束

配置禁止 MAC 地址学习

通过配置禁止 MAC 地址学习，符合流分类规则的报文的 MAC 地址不再被学习，有助于提高设备运行效率，保护设备安全。

背景信息

在网络比较稳定、报文的 MAC 地址相对固定的情况下，设备没有必要继续学习其他所有报文的 MAC 地址。此时通过对流策略下所有流分类禁止 MAC 地址学习功能，既可以节省 MAC 地址表项开支，也可以提高设备的运行效率。

某些非法用户有时会采用频繁变换 MAC 地址的方式对网络进行攻击，此时通过对流策略下所有流分类禁止 MAC 地址学习功能，可以避免此类攻击所造成的设备 MAC 地址表项溢出的问题，保护设备性能不受影响。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **mac-address learning disable**，配置禁止 MAC 地址学习功能。

配置后，与该流行为绑定的流分类所匹配的报文的 MAC 地址将不再被学习，而没有绑定该流行为的流分类所匹配的报文的 MAC 地址仍然默认被学习。

版权所有 © 华为技术有限公司

说明

用户可根据实际需要灵活选择配置禁止 MAC 地址学习：

- 如果需要设备在接口、端口组或 VLAN 范围内禁止学习 MAC 地址，应选择在接口视图、端口组视图和 VLAN 视图下配置 **mac-address learning disable**。
- 如果仅需要禁止学习特定流的 MAC 地址，应选择在流行为视图配置 mac-address learning disable。

----结束

配置流策略

通过配置流策略，关联流分类和动作。

背景信息

AC6605 支持在创建流策略时指定流策略中流分类的匹配顺序，包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类优先级决定，该优先级由高到底依次为：基于二层和三层信息流分类 > 基于三层信息流分类 > 基于二层信息流分类。 规则优先匹配优先级高的流分类。
- 如果选择配置顺序，匹配顺序由流分类在流策略中绑定的先后顺序决定。规则优先匹配绑定在先的流分类。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 请根据设备类型进行如下配置：

- AC6605 执行命令 **traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建流策略并进入流策略视图。

应用流量监管策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

步骤 3 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在策略中关联流分类和流行为。

----结束

应用流策略

配置的流策略只有在全局/槽位、接口或 VLAN 下应用后才能生效。

背景信息

说明

全局或 VLAN 下应用流策略时，可能由于某槽位不支持该流策略，而使该流策略在该槽位应用失败，可使用 **display traffic-policy applied-record** [*policy-name*]命令查看实际有效的槽位。

操作步骤

- 在全局应用流策略

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 请根据设备类型选择配置：
   - AC6605 执行命令 **traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或槽位的入方向或出方向应用流策略。

     全局的每个方向上能且只能应用一个流策略。

     槽位的每个方向上能且只能应用一个流策略。如果全局某方向应用流策略后，不能再指定槽位在该方向应用流策略；指定槽位在某方向应用流策略后，也不能再全局在该方向应用流策略。

     - 全局应用的流策略在本交换机的所有接口和 VLAN 生效，系统对进入本交换机的所有匹配流分类规则的入方向或出方向报文流实施策略控制。槽位应用等同于全局应用。

- 在接口上应用流策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 请根据设备类型选择配置：

     AC6605，执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口入方向或出方向应用流策略。

     每个接口的每个方向上能且只能应用一个流策略。

     应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。
- 在 VLAN 下应用流策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 请根据设备类型选择配置：

     AC6605，执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，在 VLAN 入方向或出方向应用流策略。

     每个 VLAN 的每个方向能且只能应用一个流策略。

     应用后，系统对属于该 VLAN 并匹配流分类中规则的入方向或出方向报文实施策略控制。

----结束

检查配置结果

配置基于复杂流分类的流策略后，可以查看流分类、流行为、流策略的配置信息。

前提条件

已经完成基于复杂流分类的流策略的配置。

操作步骤

- 执行命令 **display acl** { *acl-number* | **all** }，查看用户定义的 ACL 规则。

版权所有 © 华为技术有限公司

- 执行命令 **display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** *vlan-id*] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN 或接口上关联的 ACL 规则和流动作信息。
- 执行命令 **display traffic classifier user-defined** [*classifier-name*]，查看设备上的流分类信息。
- 执行命令 **display traffic behavior user-defined** [*behavior-name*]，查看流行为的配置信息。
- 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令 **display traffic policy** { **interface** [*interface-type interface-number*] | **vlan** [*vlan-id*] | **global** } [**inbound** | **outbound**]，查看流策略应用信息及基于流的流量统计信息。
- 执行命令 **display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录信息。

----结束

7.1.5 配置基于简化 QoS 命令的流策略

通过简化 QoS 配置命令，可以配置流量监控、流量统计、重定向、重标记、镜像等功能。与普通的 QoS 命令相比，通过简化 QoS 配置命令配置 QoS 功能，不需要单独创建流分类、流行为、流策略等步骤，配置步骤更加简洁。

建立配置任务

在配置基于简化 QoS 命令的流策略前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在网络的入口处，AC6605 作为边界节点。如果需要对进入网络的流量进行限制，则可以根据报文的 DSCP 值、协议类型、IP 地址、端口号、分片报文的类型以及时间段等参数对不同的业务提供差别服务，此时可以通过简化 QoS 命令配置流策略。

通过简化 QoS 配置命令，可以配置流量监控、流量统计、重定向、重标记、镜像等功能。与普通的 QoS 命令相比，通过简化 QoS 配置命令配置 QoS 功能，不需要单独创建流分类、流行为、流策略等步骤，配置步骤更加简洁。

前置任务

在配置基于简化 QoS 命令的流策略之前，需要完成以下任务。

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关路由协议，使网络能够互通
- 如果使用 ACL 作为流分类规则，配置相应的 ACL

数据准备

在基于简化 QoS 命令的流策略之前，请根据网络规划，准备好以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	ACL 规则
2	（可选）CIR、CBS

配置对匹配 ACL 规则的流量进行监管

背景信息

通过配置流量监管行为，设置 CIR、CBS 等 CAR 参数对报文的流量进行限制，并设置对具有不同颜色的保文采取的动作。

操作步骤

- 在全局下配置流量监管
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **traffic-limit** [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，根据 ACL 中设置的 rule 规则对交换机入方向的报文进行监管。

     或者执行命令 **traffic-limit** [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，根据 ACL 中设置的 rule 规则对交换机出方向报文进行监管。

版权所有 © 华为技术有限公司

说明

当指定 **vlan** *vlan-id* 参数时，表示基于 VLAN 配置流量监管，此时 VLAN 中的所有接口都按此配置执行。

当不指定 **vlan** *vlan-id* 参数时，表示设备上的所有接口都按此配置执行。

报文的颜色可以在流量监管中定义：

- 报文的突发尺寸<*cbs-value* 时，报文被标记为绿色；
- *cbs-value*<=报文的突发尺寸<*pbs-value* 时，报文被标记为黄色；
- 报文的突发尺寸>=*pbs-value* 时，报文被标记为红色。

缺省情况下，绿色、黄色报文被允许通过，红色报文被丢弃。

当配置了 **traffic-limit** 命令的同时也配置了 **traffic-filter（接口视图）**命令或 **traffic-filter（系统视图）**命令，且与 **traffic-limit** 命令关联了相同的 ACL 规则：

- 如果 ACL 规则中的动作为 deny 时，**traffic-limit** 命令不生效。
- 如果 ACL 规则中的动作为 permit 时，**traffic-limit** 命令正常生效。

traffic-limit 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机的入方向应用时，命令格式为：

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]

同时配置二层 ACL 与三层 ACL 且在交换机接口的出方向应用时，命令格式为：**traffic-limit** [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]

- 在接口下配置流量监管
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。或执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-trunk 接口视图。
  3. 执行命令 **traffic-limit inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，根据 ACL 中设置的 rule 规则对接口入方向的报文进行监管。

     或者执行命令 **traffic-limit outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* { *bas-acl* | *adv-acl* } } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，根据 ACL 中设置的 rule 规则对接口出方向报文进行监管。

版权所有 © 华为技术有限公司

说明

报文的颜色可以在流量监管中定义：

- 报文的突发尺寸<*cbs-value* 时，报文被标记为绿色；
- *cbs-value*<=报文的突发尺寸<*pbs-value* 时，报文被标记为黄色；
- 报文的突发尺寸>=*pbs-value* 时，报文被标记为红色。

缺省情况下，绿色、黄色报文被允许通过，红色报文被丢弃。

当配置了 **traffic-limit** 命令的同时也配置了 **traffic-filter（接口视图）**命令或 **traffic-filter（系统视图）**命令，且与 **traffic-limit** 命令关联了相同的 ACL 规则：

- 如果 ACL 规则中的动作为 deny 时，**traffic-limit** 命令不生效。
- 如果 ACL 规则中的动作为 permit 时，**traffic-limit** 命令正常生效。

traffic-limit 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口的入方向应用时，命令格式为：

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]

同时配置二层 ACL 与三层 ACL 且在交换机接口的出方向应用时，命令格式为：**traffic-limit outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]

----结束

配置对匹配 ACL 规则的流量进行过滤

背景信息

通过配置对匹配 ACL 规则的流量进行过滤，AC6605 将禁止或允许符合流分类规则的报文通过，从而控制网络流量。

操作步骤

- 在全局下配置流量过滤
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **traffic-filter** [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] }，根据 ACL 中设置的 rule 规则对接口入方向的报文进行过滤。

     说明

     当指定 **vlan** *vlan-id* 参数时，表示基于 VLAN 配置流量过滤，此时 VLAN 中的所有接口都按此配置执行。

     当不指定 **vlan** *vlan-id* 参数时，表示设备上的所有接口都按此配置执行。

     traffic-filter 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口上应用时，命令格式为：

     traffic-filter [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]
- 在接口下配置流量过滤

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。或执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-trunk 接口视图。
3. 执行命令 **traffic-filter inbound** { **acl** { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*]，根据 ACL 中设置的 rule 规则对接口入方向的报文进行过滤。

   说明

   traffic-filter 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口上应用时，命令格式为：

   traffic-filter inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

----结束

配置对匹配 ACL 规则的流量进行重标记

背景信息

通过配置重标记，AC6605 对符合流分类规则的报文的优先级字段进行设置，如 VLAN 报文中的 802.1p、IP 报文中的 DSCP 等。

操作步骤

- 在全局下配置重标记
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **traffic-remark** [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **ip-precedence** *ip-precedence-value* | **vlan-id** *vlan-id* }，根据 ACL 中设置的 rule 规则对接口入方向的报文进行重标记。

     说明

     当指定 **vlan** *vlan-id* 参数时，表示基于 VLAN 配置流量过滤，此时 VLAN 中的所有接口都按此配置执行。

     当不指定 **vlan** *vlan-id* 参数时，表示设备上的所有接口都按此配置执行。

     当配置了 **traffic-remark** 命令的同时也配置了 **traffic-filter（接口视图）**命令或 **traffic-filter（系统视图）**命令，且与 **traffic-remark** 命令关联了相同的 ACL 规则：

     - 如果 ACL 规则中的动作为 deny 时，**traffic-remark** 命令不生效。
     - 如果 ACL 规则中的动作为 permit 时，**traffic-remark** 命令正常生效。

     traffic-remark 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口的入方向应用时，命令格式为：

     traffic-remark [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **ip-precedence** *ip-precedence-value* | **vlan-id** *vlan-id* }
- 在接口下配置重标记
  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。或执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-trunk 接口视图。
3. 执行命令 **traffic-remark inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **ip-precedence** *ip-precedence-value* | **vlan-id** *vlan-id* }，根据 ACL 中设置的 rule 规则对接口入方向的报文进行重标记。

   说明

   当配置了 **traffic-remark** 命令的同时也配置了 **traffic-filter（接口视图）**命令或 **traffic-filter（系统视图）**命令，且与 **traffic-remark** 命令关联了相同的 ACL 规则：

   - 如果 ACL 规则中的动作为 deny 时，**traffic-remark** 命令不生效。
   - 如果 ACL 规则中的动作为 permit 时，**traffic-remark** 命令正常生效。

   traffic-remark 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口的入方向应用时，命令格式为：

   traffic-remark inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **ip-precedence** *ip-precedence-value* | **vlan-id** *vlan-id* }

----结束

配置对匹配 ACL 规则的流量进行统计

背景信息

通过配置流量统计，AC6605 将对符合流分类规则的报文进行流量统计。

操作步骤

- 在全局下配置流量统计
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **traffic-statistic** [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] [**by-bytes**]，根据 ACL 中设置的 rule 规则对接口入方向的报文进行流量统计。

     说明

     当指定 **vlan** *vlan-id* 参数时，表示基于 VLAN 配置流量过滤，此时 VLAN 中的所有接口都按此配置执行。

     当不指定 **vlan** *vlan-id* 参数时，表示设备上的所有接口都按此配置执行。

     traffic-statistic 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口应用时，命令格式为：

     traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]
- 在接口下配置流量统计
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。或执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-trunk 接口视图。

版权所有 © 华为技术有限公司

3. 执行命令 **traffic-statistic inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] [**by-bytes**]，根据 ACL 中设置的 rule 规则对接口入方向的报文进行流量统计。

   说明

   traffic-statistic 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口应用时，命令格式为：

   traffic-statistic inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

----结束

配置对匹配 ACL 规则的流量进行重定向

背景信息

通过配置重定向，AC6605 将符合流分类规则的报文重定向到 CPU、指定接口、指定的下一跳地址。

操作步骤

- 在全局下配置流量重定向
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **traffic-redirect** [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* }，根据 ACL 中设置的 rule 规则对接口的报文进行重定向。

     说明

     当指定 **vlan** *vlan-id* 参数时，表示基于 VLAN 配置流量重定向，此时 VLAN 中的所有接口都按此配置执行。

     当不指定 **vlan** *vlan-id* 参数时，表示设备上的所有接口都按此配置执行。

     当配置了 **traffic-redirect** 命令的同时也配置了 **traffic-filter（接口视图）**命令或 **traffic-filter（系统视图）**命令，且与 **traffic-redirect** 命令关联了相同的 ACL 规则：

     - 如果 ACL 规则中的动作为 deny 时，**traffic-redirect** 命令不生效。
     - 如果 ACL 规则中的动作为 permit 时，**traffic-redirect** 命令正常生效。

     traffic-redirect 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层 ACL 与三层 ACL 且在交换机接口应用时，命令格式为：

     traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* }
- 在接口下配置流量重定向
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **traffic-redirect inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* }，根据 ACL 中设置的 rule 规则对接口的报文进行重定向。

版权所有 © 华为技术有限公司

说明

traffic-redirect 命令支持同时匹配二层 ACL 与三层 ACL，只有先配置二层 ACL（4000 ~ 4999）及 rule 后，才能继续配置三层 ACL（2000 ~ 2999、3000 ~ 3999）及 rule。同时配置二层ACL 与三层 ACL 且在交换机接口的入方向应用时，命令格式为：

traffic-redirect inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* }

----结束

7.1.6 维护基于类的 QoS

如果已经使能了流量统计功能，可以查看和清除基于流的流量统计信息。

查看基于流的流量统计信息

通过 **display** 命令查看符合指定流分类规则的流量的统计信息。

背景信息

查看基于流的流量统计信息时，策略必须存在且已经包含流量统计动作。

操作步骤

- (AC6605)执行命令 **display traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看基于流的流量统计信息。

----结束

清除基于流的流量统计信息

通过 **reset** 命令清除基于流的流量统计信息。

背景信息

注意

清除基于流的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- (AC6605)用户视图下执行命令 **reset traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } { **inbound** | **outbound** }，清除基于流的流量统计信息。

----结束

版权所有 © 华为技术有限公司

7.1.7 配置举例

通过示例介绍如何应用基于类的 QoS。配置示例中包括组网需求、配置注意事项、配置思路等。

配置基于简单流分类的优先级映射示例

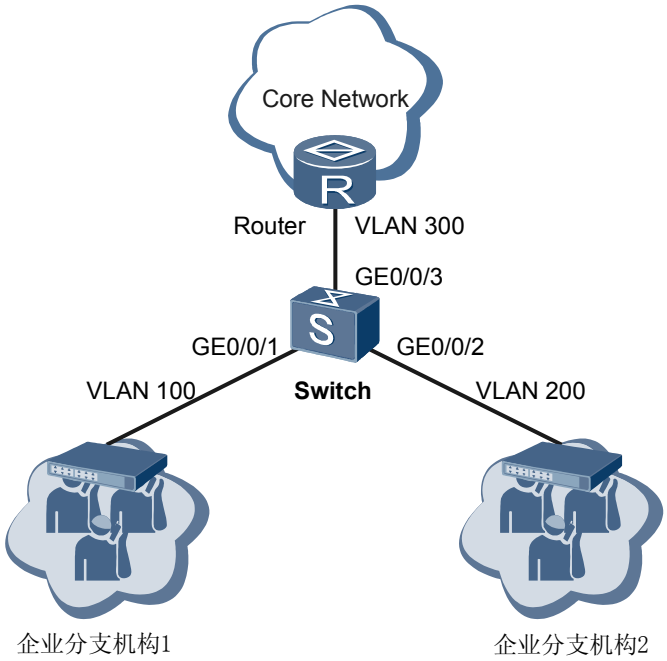
通过配置基于简单流分类的优先级映射，AC6605 将来自不同用户的报文中的 802.1p 优先级映射成不同的服务等级，从而提供差异化的服务。

组网需求

如图 7-1 所示，Switch 通过接口 GE0/0/3 与路由器互连，企业分支机构 1 和企业分支机构 2 可经由 Switch 和路由器访问网络。企业分支机构 1 和企业分支机构 2 的 VLAN ID 分别为 100、200。

企业分支机构 1 需要得到更好的 QoS 保证，因此将来自企业用户的数据报文优先级映射为 4，将来自企业分支机构 2 的数据报文优先级映射为 2，以提供差分服务。

图 7-1 基于简单流分类的优先级映射配置组网图



配置思路

采用如下的思路配置基于简单流分类的优先级映射：

1. 创建 VLAN，并配置各接口，企业分支机构 1 和企业分支机构 2 都能够通过 Switch 访问网络。
2. 创建 DiffServ 域，将 802.1p 优先级映射为 PHB 行为和颜色。
3. 在 Switch 入接口 GE0/0/1 和 GE0/0/2 上绑定 DiffServ 域。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- DiffServ 域的名称。
- 企业分支机构 1 和企业分支机构 2 的报文的 802.1p 优先级。
- 企业分支机构 1 和企业分支机构 2 的服务等级。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN 100、200、300。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
```

将接口 GE0/0/1、GE0/0/2、GE0/0/3 的接入类型分别配置为 trunk，并分别将接口 GE0/0/1、GE0/0/2 加入 VLAN 100、VLAN 200；接口 GE0/0/3 加入 VLAN 100、VLAN 200 和 VLAN 300。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200 300
[Switch-GigabitEthernet0/0/3] quit
```

创建 VLANIF300，并配置接口 IP 地址 192.168.1.1/24。

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
```

说明

请在 Router 上的与 Switch 对接的接口上配置 IP 地址 192.168.1.2/24。

步骤 2 创建并配置 DiffServ 域

在 Switch 上创建 DiffServ 域 ds1、ds2，并配置将企业分支机构 1 和企业分支机构 2 的 802.1p 优先级映射到服务等级。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 0 phb af4 green
[Switch-dsdomain-ds1] quit
[Switch] diffserv domain ds2
[Switch-dsdomain-ds2] 8021p-inbound 0 phb af2 green
[Switch-dsdomain-ds2] quit
```

步骤 3 将 DiffServ 域绑定到接口

将 DiffServ 域 ds1 和 ds2 分别绑定到接口 GE0/0/1、GE0/0/2。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] trust upstream ds1
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
```


版权所有 © 华为技术有限公司

```
[Switch-GigabitEthernet0/0/2] trust upstream ds2
[Switch-GigabitEthernet0/0/2] quit
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 100 200 300
#
diffserv domain ds1
  8021p-inbound 0 phb af4 green
#
diffserv domain ds2
  8021p-inbound 0 phb af2 green
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 trust upstream ds1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 trust upstream ds2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200 300
#
return
```

配置基于复杂流分类的优先级重标记示例

通过配置基于复杂流分类的优先级重标记，AC6605 对具有不同 VLAN ID 的报文添加相同的外层 VLAN ID，以便统一标识为业务数据；同时，对具有不同 VLAN ID 的报文重标记不同的 802.1p 优先级，以提供差分服务。

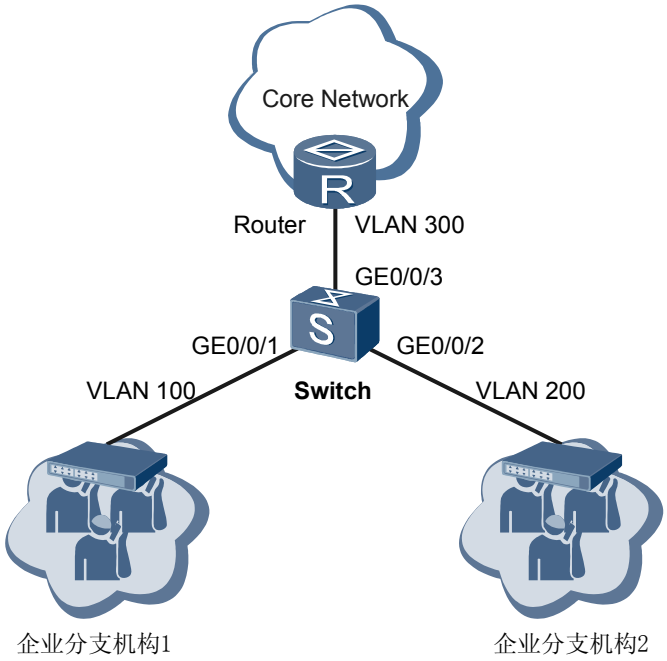
组网需求

Switch 通过接口 GE0/0/3 与路由器互连，企业分支机构 1 和企业分支机构 2 可经由 Switch 和路由器访问网络，如图 7-2 所示。

企业分支机构 1 和企业分支机构 2 的数据业务对应的 VLAN ID 分别为 100、200。当这两个用户的数据业务报文经过 Switch 时，需添加 VLAN ID 为 300 的外层 VLAN TAG，以便在网络侧统一将其标识为数据业务。此外，由于企业分支机构 1 需要得到更好的 QoS 保证，因此将发往分支机构 1 的数据报文优先级重标记为 4，将发往分支机构 2 用户的数据报文优先级重标记为 2，提供差分服务。

版权所有 © 华为技术有限公司

图 7-2 基于复杂流分类的优先级重标记组网图



配置思路

采用如下的思路配置基于复杂流分类的优先级重标记：

1. 创建 VLAN，并配置各接口，使企业用户和住宅用户能通过 Switch 访问网络。
2. 在 Switch 上配置基于内层 VLAN ID 进行流分类的匹配规则。
3. 在 Switch 上配置流行为，重标记报文的 802.1p 优先级。
4. 在 Switch 上配置流策略，绑定已经配置好的流行为和流分类，并应用到报文的接口入方向上。

数据准备

为完成此配置例，需准备如下的数据：

- 对不同内层 VLAN ID 的报文进行重标记后的优先级值。
- 需要应用流策略的接口类型、方向和编号。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 Switch 上创建 VLAN 100、200、300，并配置接口，使从接口 GE0/0/1、GE0/0/2 转发出去的报文封装上外层 VLAN 300，并使接口 GE0/0/3 能转发 VLAN 300 的报文。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port hybrid pivd vlan 100
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 100 300
[Switch-GigabitEthernet0/0/1] qinq vlan-translation enable
```


版权所有 © 华为技术有限公司

```
[Switch-GigabitEthernet0/0/1] port vlan-stacking vlan 100 stack-vlan 300
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port hybrid pivd vlan 200
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 200 300
[Switch-GigabitEthernet0/0/2] qinq vlan-translation enable
[Switch-GigabitEthernet0/0/2] port vlan-stacking vlan 200 stack-vlan 300
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 300
[Switch-GigabitEthernet0/0/3] quit
```

创建 VLANIF 300，并为该 VLANIF 接口配置 IP 地址 192.168.1.1/24。

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
[Switch-Vlanif300] quit
```

步骤 2 配置流分类

在 Switch 上创建并配置流分类 c1、c2，对来自用户的报文按照其内层 VLAN ID 进行分类。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match cvlan-id 100
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match cvlan-id 200
[Switch-classifier-c2] quit
```

步骤 3 配置流行为

在 Switch 上创建并配置流行为 b1、b2，重标记用户报文的优先级。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] remark 8021p 4
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] remark 8021p 2
[Switch-behavior-b2] quit
```

步骤 4 配置流策略并应用到接口上

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定并将流策略应用到 GE0/0/1 和 GE0/0/2 接口的入方向上，对来网络侧的报文进行重标记。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/2] quit
```

步骤 5 验证配置结果

查看流分类的配置信息。

```
<Switch> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match cvlan-id 200
```


版权所有 © 华为技术有限公司

```
   Classifier: c1
    Operator: AND
    Rule(s) : if-match cvlan-id 100
Total classifier number is 2
```

查看流策略的配置信息。

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Marking:
        Remark 8021p 4
   Classifier: c2
    Operator: AND
     Behavior: b2
      Marking:
        Remark 8021p 2
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 100 200 300
#
traffic classifier c1 operator and
 if-match cvlan-id 100
traffic classifier c2 operator and
 if-match cvlan-id 200
#
traffic behavior b1
 remark 8021p 4
traffic behavior b2
 remark 8021p 2
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100 300
 port vlan-stacking vlan 100 stack-vlan 300
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
 qinq vlan-translation enable
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200 300
 port vlan-stacking vlan 200 stack-vlan 300
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
return
```


版权所有 © 华为技术有限公司

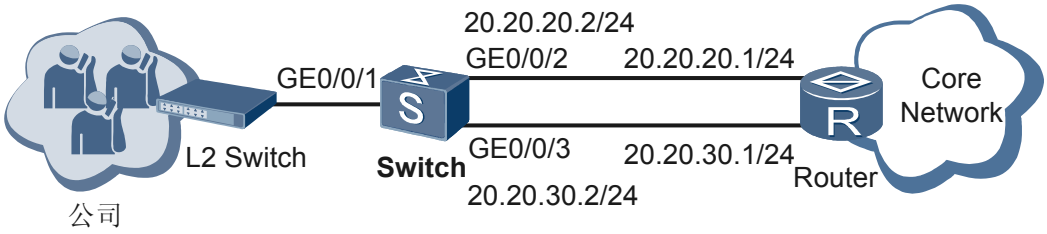
配置策略路由示例

通过配置基于复杂流分类的报文重定向，AC6605 将具有不同 IP 优先级的报文重定向到不同的接口，以提供不同的带宽服务。

组网需求

公司交换机通过 Switch 连接到服务提供商设备，一条是 1G 链路，网关为 20.20.20.1/24；另外一条是 10G 链路，网关为 20.20.30.1/24。公司要求 10G 链路只传送 IP 优先级为 4、5、6、7 的高优先级报文，而其它低优先级报文则使用 1G 链路连接到服务提供商。如图 7-3 所示。

图 7-3 策略路由配置组网图



配置思路

采用如下的思路配置基于复杂流分类的报文重定向：

1. 创建 VLAN 并配置各接口，使 Switch 能 Ping 通服务提供商。
2. 配置 ACL 规则，分别匹配 IP 优先级 4、5、6、7，以及 IP 优先级 0、1、2、3。
3. 配置流分类，匹配规则为上述 ACL 规则。
4. 配置流行为，使满足不同规则的报文分别被重定向到 20.20.20.1/24 和 20.20.30.1/24。
5. 配置流策略，绑定上述流分类和流行为，并应用到相应的接口。

数据准备

为完成此配置示例，需准备如下的数据：

- VLAN 编号为 20、30，GE0/0/1、GE0/0/2 和 GE0/0/3 同时加入 VLAN20 和 VLAN30。
- ACL 规则编号为 3001、3002。
- 流分类的名称为 c1、c2
- 流行为的名称为 b1、b2。
- 流策略的名称为 p1。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN20、VLAN30。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 20 30
```

#配置接口 GE0/0/1、GE0/0/2 和 GE0/0/3 为 trunk 类型端口，并将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 都加入 VLAN20 和 VLAN30。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 30
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 20 30
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 20 30
[Switch-GigabitEthernet0/0/3] quit
```

创建 VLANIF20、VLANIF30，并配置各虚拟接口 IP 地址。

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 20.20.20.2 24
[Switch-Vlanif20] quit
[Switch] interface vlanif 30
[Switch-Vlanif30] ip address 20.20.30.2 24
[Switch-Vlanif30] quit
```

说明

请在 Router 与 Switch 对接的接口上分别配置网段地址 20.20.20.1/24 和 20.20.30.1/24，本文不再描述。

步骤 2 配置 ACL 规则

在 Switch 上创建编码为 3001、3002 的高级 ACL，规则分别为允许 IP 优先级 4、5、6、7 和允许 IP 优先级 0、1、2、3 的报文通过。

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule permit ip precedence 0
[Switch-acl-adv-3001] rule permit ip precedence 1
[Switch-acl-adv-3001] rule permit ip precedence 2
[Switch-acl-adv-3001] rule permit ip precedence 3
[Switch-acl-adv-3001] quit
[Switch] acl 3002
[Switch-acl-adv-3002] rule permit ip precedence 4
[Switch-acl-adv-3002] rule permit ip precedence 5
[Switch-acl-adv-3002] rule permit ip precedence 6
[Switch-acl-adv-3002] rule permit ip precedence 7
[Switch-acl-adv-3002] quit
```

步骤 3 配置流分类

在 Switch 上创建流分类 c1、c2，匹配规则分别为 ACL 3001 和 ACL 3002。

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3001
[Switch-classifier-c1] quit
[Switch] traffic classifier c2
[Switch-classifier-c2] if-match acl 3002
[Switch-classifier-c2] quit
```

步骤 4 配置流行为

在 Switch 上创建流行为 b1、b2，并分别指定重定向到网段 20.20.20.1/24 和 20.20.30.1/24 的动作。

版权所有 © 华为技术有限公司

```
[Switch] traffic behavior b1
[Switch-behavior-b1] redirect ip-nexthop 20.20.20.1
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] redirect ip-nexthop 20.20.30.1
[Switch-behavior-b2] quit
```

步骤 5 配置流策略并应用到接口上

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 0/0/1。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] quit
[Switch] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息。

```
[Switch] display acl 3001
Advanced ACL 3001, 4 rules
Acl's step is 5
 rule 5 permit ip precedence routine
 rule 10 permit ip precedence priority
 rule 15 permit ip precedence immediate
 rule 20 permit ip precedence flash
[Switch] display acl 3002
Advanced ACL 3002, 4 rules
Acl's step is 5
 rule 5 permit ip precedence flash-override
 rule 10 permit ip precedence critical
 rule 15 permit ip precedence internet
 rule 20 permit ip precedence network
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match acl 3002

   Classifier: c1
    Operator: AND
    Rule(s) : if-match  acl 3001


Total classifier number is 2
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Redirect:
        Redirect ip-nexthop
        20.20.20.1
   Classifier: c2
    Operator: AND
```


版权所有 © 华为技术有限公司

```
Behavior: b2
 Redirect:
   Redirect ip-nexthop
   20.20.30.1
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 20 30
#
acl number 3001
 rule 5 permit ip precedence routine
 rule 10 permit ip precedence priority
 rule 15 permit ip precedence immediate
 rule 20 permit ip precedence flash
#
acl number 3002
 rule 5 permit ip precedence flash-override
 rule 10 permit ip precedence critical
 rule 15 permit ip precedence internet
 rule 20 permit ip precedence network
#
traffic classifier c1 operator and
 if-match acl 3001
traffic classifier c2 operator and
 if-match acl 3002
#
traffic behavior b1
 redirect ip-nexthop 20.20.20.1
traffic behavior b2
 redirect ip-nexthop 20.20.30.1
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
#
interface Vlanif20
 ip address 20.20.20.2 255.255.255.0
#
interface Vlanif30
 ip address 20.20.30.2 255.255.255.0
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 30
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 30
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20 30
#
return
```

配置基于复杂流分类的流量统计示例

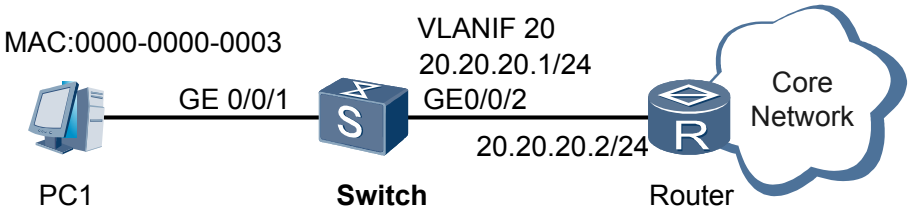
通过配置基于复杂流分类的流量统计，AC6605 对具有特定源 MAC 地址的报文进行流量统计。

版权所有 © 华为技术有限公司

组网需求

PC1 的 MAC 地址为 0000-0000-0003，它连接在 Switch 的 GE0/0/1 端口上，实现与其他设备的互连。现要求 Switch 对源 MAC 为 0000-0000-0003 的报文进行流量统计。如图 7-4 所示。

图 7-4 基于复杂流分类的流量统计组网图



配置思路

采用如下的思路配置基于复杂流分类的流量统计：

1. 配置各接口，实现 Switch 与 PC1、Router 互联。
2. 配置 ACL 规则，匹配源 MAC 为 0000-0000-0003 的报文。
3. 配置流分类，匹配规则为上述 ACL 规则。
4. 配置流行为，对满足规则的报文进行流量统计。
5. 配置流策略，绑定上述流分类和流行为，并应用到 GE 0/0/1 接口入方向。

数据准备

为完成此配置示例，需准备如下的数据：

- VLAN 编号为 20。
- ACL 规则编号为 4000。
- 流分类的名称为 c1
- 流行为的名称为 b1。
- 流策略的名称为 p1。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN20。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 20
[Switch-vlan20] quit
```

配置接口 GE0/0/1 为 Access 类型端口、GigabitEthernet0/0/2 为 trunk 类型端口，并将 GE 0/0/1、GigabitEthernet0/0/2 加入 VLAN20。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 20
```


版权所有 © 华为技术有限公司

```
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet0/0/2] quit
```

创建 VLANIF20，并配置接口 IP 地址为 20.20.20.1/24。

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 20.20.20.1 24
[Switch-Vlanif20] quit
```

说明

请在 Router 与 Switch 对接的接口上配置网段地址 20.20.20.2/24，本文不再描述。

步骤 2 配置 ACL 规则

在 Switch 上创建编码为 4000 的二层 ACL，匹配源 MAC 为 0000-0000-0003 的报文。

```
[Switch] acl 4000
[Switch-acl-L2-4000] rule permit source-mac 0000-0000-0003 ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

步骤 3 配置流分类

在 Switch 上创建流分类 c1，匹配规则为 ACL 4000。

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 4000
[Switch-classifier-c1] quit
```

步骤 4 配置流行为

在 Switch 上创建流行为 b1，并配置流量统计动作。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
```

步骤 5 配置流策略并应用到接口上

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/1。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] quit
[Switch] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息。

```
<Switch> display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 permit source-mac 0000-0000-0003
```

查看流分类的配置信息。

```
<Switch> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: AND
```


版权所有 © 华为技术有限公司

```
    Rule(s) : if-match  acl 4000
Total classifier number is 1
```

查看流策略的配置信息。

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      statistic: enable
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 20
#
acl number 4000
 rule 5 permit source-mac 0000-0000-0003
#
traffic classifier c1 operator and
 if-match acl 4000
#
traffic behavior b1
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

7.2 流量监管和流量整形配置

流量监管和流量整形配置介绍了流量监管和流量整形基本概念，并介绍了基于类的流量监管、配置流量整形的配置方法和配置示例。

7.2.1 流量监管和流量整形概述

流量监管和流量整形概述介绍了流量监管和流量整形基本概念，以及两者的区别。

流量监管

为了使有限的网络资源可以更好地为用户服务，可以对特定用户的业务流进行监管，使其适应分配给它的那部分网络资源。

版权所有 © 华为技术有限公司

流量监管（Traffic Policing）是通过对流量规格的监督，来限制流量及其资源使用的流控策略。

流量监管的典型应用是监督进入网络的某一流量的规格，把它限制在一个合理的范围之内，或对超出的部分流量进行“惩罚”，以保护网络资源和运营商的利益。

流量监管广泛的用于监管进入因特网服务提供商（ISP）的网络流量。

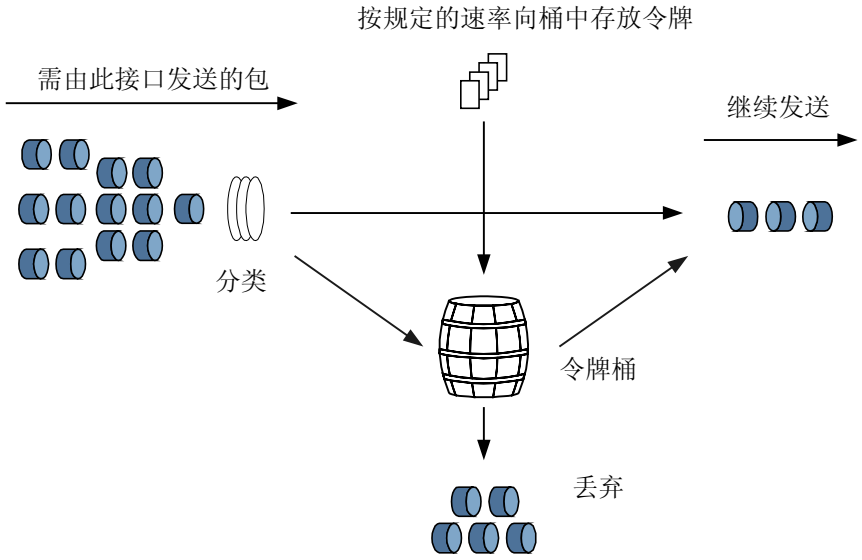
令牌桶与流量评估

进行流量监管有一个前提条件，就是要判断流量是否超出了规格，然后才能根据评估结果实施调控策略。一般采用令牌桶（Token Bucket）对流量的规格进行评估。

令牌桶可以看作是一个存放一定数量令牌的容器。系统按设定的速度向桶中放置令牌（1 令牌=1bit），当桶中令牌满时，多出的令牌溢出，桶中令牌不再增加。

在使用令牌桶对流量进行评估时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文，称流量遵守或符合约定值，否则称为不符合或超标。

图 7-5 用令牌桶评估流量



AC6605 支持单令牌桶和双令牌桶两种令牌桶技术：

- 单令牌桶

  单令牌桶技术中，令牌桶参数包括：

  - 承诺突发尺寸 CBS（Committed Burst Size）：即所谓的 C 桶，表示每次突发所允许的最大的流量尺寸，单位为 byte。
  - 承诺信息速率 CIR（Committed Information Rate）：表示向 C 桶中放置令牌的速率，即 C 桶允许的流的平均速度，单位为 kbps。

  单令牌桶技术中，当令牌桶中有足够的令牌可以用来发送报文时，则报文可以通过并被继续发送下去，同时令牌桶中的令牌量按报文的长度做相应的减少；当令牌桶空时，报文被丢弃。

版权所有 © 华为技术有限公司

- 双令牌桶

  双令牌桶技术中，令牌桶参数除了 CIR 和 CBS 外，还包括：

  - 过度突发尺寸 PBS（Peak Burst Size）：即所谓的 P 桶，表示每次突发所允许的超出 CBS 的最大的流量尺寸，单位为 byte。
  - 峰值信息速率 PIR（Peak Information Rate）：表示向 P 桶中放置令牌的速率，即 P 桶允许的流的平均速度，单位为 kbps。

  双令牌桶技术中，用户业务流量小于 CIR 的部分报文被标记为绿色，全部通过；用户流量超出 PIR 的部分报文被标记为红色，全部丢弃；超出 CIR 但小于 PIR 的部分报文被标记为黄色，这部分流量将在网络发生拥塞时被丢弃。

AC6605 支持的流量监管特性

AC6605 支持以下流量监管功能：

- 基于接口的流量监管

  基于接口的流量监管是指对进入该接口的所有流量进行控制，而不区分具体报文的类型，丢弃超出速率限制的部分，使进入设备的该类流量被限制在一个合理的范围之内，从而保护网络资源和运营商的利益。

- 基于类的流量监管

  基于类的流量监管是指在设备上经过流分类后，对符合流分类的流量进行速率限制。通过监督进入设备的该类流量速率，丢弃超出速率限制的部分，使进入设备的该类流量被限制在一个合理的范围之内，从而保护网络资源和运营商的利益。基于类的流量监管采用双令牌桶技术。

  基于类的流量监管中，AC6605 支持对上行流作两次 CAR，即在对符合流分类的上行流作完一次 CAR 后，将所有的上行流聚合在一起再作一次共享 CAR，这里所有的上行流是指满足同一流策略中绑定了配置共享 CAR 的流行为的流分类的入方向业务流。

  说明

  - 共享 CAR 仅支持单速单桶技术。
  - AC6605 支持的基于类的流量监管可实现出入两个方向的端口限速（匹配规则配置为 if-match any）和流限速。

流量整形

流量整形是对报文的速率进行控制，使报文以均匀的速率发送出去。流量整形通常是为了使报文速率与下游设备相匹配，以避免不必要的报文丢弃和拥塞。

流量整形（Traffic Shaping）也是通过对流量规格的监督，来限制流量及其资源使用的流控策略。流量整形的流量评估也是通过令牌桶技术。

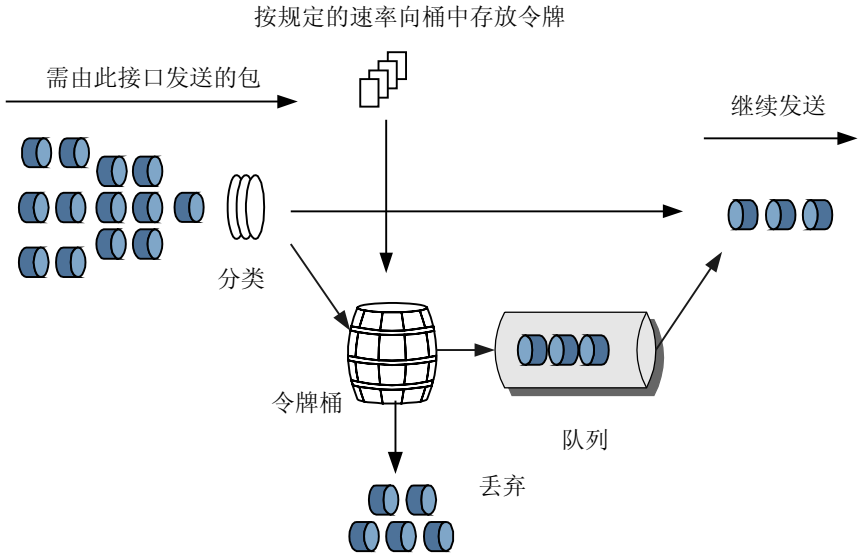
流量整形是一种主动调整流量输出速率的措施，一个典型应用是基于下游网络结点的流量监管指标来控制本地流量的输出。

流量整形与流量监管的区别

流量整形与流量监管的主要区别在于，流量监管对不符合流量特性的报文直接丢弃，而流量整形对不符合流量特性的报文则是进行缓存——通常是将它们放入缓冲区或队列内，减少了报文的丢弃，如图 7-6 所示。在图 1 中，当令牌桶有足够令牌时，均匀地发送被缓存的报文，令牌不够时就继续缓存。当需要缓存的报文个数大于队列长度时报文因无法缓存而被丢弃。

版权所有 © 华为技术有限公司

图 7-6 流量整形示意图



正是由于流量整形将报文入缓存或队列，所以流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

AC6605 支持的流量整形特性

AC6605 支持如下流量整形功能：

- 基于端口的流量整形

  对端口上所有通过的报文进行流量整形。

- 基于队列的流量整形

  对端口上通过的某类报文（基于简单流分类）分别进行流量整形，从而可实现针对业务（如语音、数据、视频）的流量整形。

  说明

  AC6605 不支持通过用户自定义流策略实现流量整形的功能。

7.2.2 配置基于接口的流量监管

配置基于接口的流量监管后，AC6605 将对通过该接口的报文进行流量监管。

建立配置任务

在配置基于接口的流量监管前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果不限制用户发送的业务流量，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的业务流量加以限制。在接口上应用基于接口的流量监管后，对流入接口的所有的用户业务流量进行限速。

版权所有 © 华为技术有限公司

前置任务

在配置接口限速之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性，保证接口的正常工作
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置基于接口的流量监管之前，需要准备以下数据。

序号	数据
1	流量监管的 CIR 和 CBS
2	应用流量监管的接口或队列索引

配置接口的流量限速

在接口配置流量监管，限制由该接口进出 AC6605 的流量速率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

可以在 GE 等类型接口上配置基于接口的流量监管。

如果多个接口需要配置相同的 CAR 参数，也可以通过端口组配置基于接口的流量监管，以减少重复配置工作。

端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **qos lr**{ **inbound** | **outbound** } **cir** *cir-value* [**cbs** *cbs-value*]，配置接口的流量监管。

----结束

配置管理网口的流量限速

通过在管理网口上配置流量监管，限制由管理网口进入 AC6605 的流量速率，提高系统正常运行率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface meth 0/0/1**，进入管理网口视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **qos lr pps** *packets*，配置管理网口的流量限速。

说明

管理网口的流量限速值不宜小于 100，否则可能会影响正常的 FTP 和 Telnet 功能。

----结束

检查配置结果

配置基于接口的速率限制后，可以查看接口上的速率限制信息。

前提条件

已经完成基于接口的速率限制的配置。

操作步骤

- 执行命令 **display qos lr** { **inbound** | **outbound** } **interface** *interface-type interface-number*，查看接口的速率限制信息。
- 执行命令 **display qos configuration interface** [*interface-type interface-number*]，查看接口上所有的 QoS 配置信息。

----结束

7.2.3 配置基于类的流量监管

配置基于类的流量监管后，AC6605 将对符合流分类规则的报文进行流量监管。

建立配置任务

在配置基于类的流量监管前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果不限制用户发送的业务流量，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的业务流量加以限制。

基于类的流量监管可用来针对用户的某类业务流量进行流量控制。

前置任务

在配置基于类的流量监管之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性，保证接口的正常工作
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置基于类的流量监管之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	流分类名称及相关参数
2	流量监管行为名称及 CAR 参数，包括承诺信息速率、（可选）承诺突发尺寸、（可选）峰值信息速率、（可选）峰值突发尺寸、（可选）颜色
3	流策略名称及应用基于类的流量监管策略的对象和方向（入方向或出方向）

配置复杂流分类

AC6605 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。

请根据实际应用，选择合适的流分类规则，配置复杂流分类，具体配置请参见配置复杂流分类。

配置流量监管行为

通过配置流量监管行为，设置 CIR、PIR、CBS、PBS 等 CAR 参数，并设置对具有不同 PHB 颜色的报文采取的动作。

背景信息

AC6605 支持二级 CAR，即系统对满足规则的业务流做一次 CAR 后，可以将同一流策略中满足绑定特定流行为（指配置了共享 CAR 的流行为）的流分类的所有业务流聚合在一起再做一次 CAR，称为层次化流量监管。

层次化流量监管可以实现用户流量的统计复用和精细业务的控制，如可以对第一级用户、第二级用户内的业务进行层次化监管，或者对第一级用户组、第二级用户进行层次化监管。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **car cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-precedence*] }]，配置 CAR 动作

可以在 CAR 动作中定义报文的颜色:

- 报文的突发尺寸<*cbs-value* 时，报文被着为绿色。
- *cbs-value*<=报文的突发尺寸<*pbs-value* 时，报文被着为黄色。
- 报文的突发尺寸>=*pbs-value* 时，报文被着为红色。

步骤 4 执行命令 **quit**，退出流行为视图。

步骤 5 （可选）请执行如下步骤配置共享 CAR

1. 请在执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **qos car** *car-name* **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]，配置 CAR 模板。

   说明

   共享 CAR 只支持单速单桶技术。

3. 执行命令 **traffic behavior** *behavior-name*，进入步骤 2 创建的流行为视图。
4. 执行命令 **car** *car-name* **share**，配置共享 CAR 动作。

   说明

   共享 CAR 只对 inbound 方向报文有效，对 outbound 方向报文无效。

   配置共享 CAR 后，绑定同一流行为的分类器的规则共用一个 CAR 索引，系统将这些流聚合在一起做 CAR。如果这些流分类中既有基于二层信息的流分类又有基于三层信息的流分类，那么 car share 配置将不会生效。

----结束

配置流量监管策略

通过配置流策略，关联流分类和动作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 请根据设备类型进行如下配置：

AC6605 应用流量监管策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先取消该策略应用，再重新创建并指定所需的匹配顺序。

步骤 3 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在流量监管策略中关联流分类和动作。

----结束

应用流量监管策略

配置的流策略只有在全局、接口或 VLAN 下应用后才能生效。

操作步骤

- 在全局或槽位应用流量监管策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 请根据设备类型选择配置：
     - 如果是 AC6605，执行命令 **traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或槽位的入方向或出方向应用流量监管策略。

       全局的每个方向上能且只能应用一个流量监管策略。

       槽位的每个方向上能且只能应用一个流量监管策略。如果全局某方向应用流量监管策略后，不能再指定槽位在该方向应用流量监管策略；指定槽位在某方向应用流量监管策略后，也不能再全局在该方向应用流量监管策略。

版权所有 © 华为技术有限公司

全局应用的流量监管策略在本交换机的所有接口和 VLAN 生效，系统对进入本交换机的所有匹配流分类规则的入方向或出方向报文流实施流量监管。槽位应用等同于全局应用。

- 在接口上应用流量监管策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口入方向或出方向应用流量监管策略。

     每个接口的每个方向上能且只能应用一个流量监管策略。

     应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施流量监管。
- 在 VLAN 下应用流量监管策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，在 VLAN 入方向或出方向应用流量监管策略。

     每个 VLAN 的每个方向能且只能应用一个流量监管策略。

     应用后，系统对属于该 VLAN 并匹配流分类中规则的入方向或出方向报文实施流量监管。

----结束

检查配置结果

配置基于类的流量监管后，可以查看流量统计信息或 CAR 统计信息。

前提条件

已经完成基于复杂流分类的流量监管的配置。

操作步骤

- 执行命令 **display traffic behavior user-defined** [*behavior-name*]，查看流行为的配置信息。
- 执行命令 **display traffic classifier user-defined** [*classifier-name*]，查看流分类的配置信息。
- 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令 **display traffic policy** { **interface** [*interface-type interface-number*] | **vlan** [*vlan-id*] | **global** } [**inbound** | **outbound**]，查看流策略应用信息及基于流的流量统计信息。
- 执行命令 **display qos car** { **all** | *car-name* }，查看 CAR 模板的配置信息。
- 执行命令 **display qos configuration interface** [*interface-type interface-number*]，查看接口上所有的 QoS 配置信息。

----结束

版权所有 © 华为技术有限公司

7.2.4 配置流量整形

配置流量整形后，AC6605 将对符合流分类规则的报文进行流量整形，使报文以均匀的速率发送出去。

建立配置任务

在配置流量整形前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果上下游网络的带宽不匹配，可在上游网络连接下游网络的出接口上配置流量整形功能，使流向下游网络的报文的速率满足下游网络的带宽要求，从而在一定程度上避免网络产生拥塞、丢包现象。

AC6605 支持端口整形、端口队列整形两种流量整形，可根据需要选择配置。两种流量整形共存时，需要保证端口整形承诺信息速率（CIR）大于等于端口队列整形 CIR 之和；否则，流量整形会出现异常现象（如低优先级队列抢占高优先级队列的带宽）。

前置任务

在配置流量整形之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置流量整形之前，需准备以下数据。

序号	数据
1	端口整形速率
2	（可选）端口队列整形速率，包括承诺信息速率和峰值信息速率。
3	应用流量整形的接口，或队列索引

配置端口整形

通过配置端口流量整形，限制接口向外发送数据的速率。

背景信息

如果需要对端口上的所有下行报文进行流量整形，请选择此步骤配置。

如果多个接口需要配置相同的端口整形速率，可通过端口组进行配置，以减少重复配置工作。

请在需要配置端口整形的 AC6605 上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **qos lr** { **inbound** | **outbound** } **cir** *cir-value* [**cbs** *cbs-value*]，配置端口整形速率。

缺省情况下，端口整形速率为端口的最大带宽（如 GigabitEhternet 端口为 100000kbit/s，GE 端口为 1000000kbit/s，）。

说明

- 在同一接口多次配置流量整形参数后，按最后一次配置生效。
- 如果该端口上同时配置端口队列整形，则端口整形的 CIR 必须大于等于端口队列整形的 CIR 之和；否则，流量整形会出现异常现象（如低优先级队列抢占高优先级队列的带宽）。

----结束

（可选）配置端口队列长度

通过配置端口队列长度，设置接口指定队列可以缓存报文的最大报文个数。

背景信息

配置端口队列长度前，应先执行 shutdown（接口视图）命令关闭接口，否则将导致流量中断，且系统提示告警信息。

操作步骤

- 在 AC6605 交换机上配置端口队列长度
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **qos queue** *queue-index* **length** *length-value*，配置接口优先级队列的长度。

----结束

配置端口队列整形

通过配置端口队列整形，启动指定端口队列的队列整形功能并设置整形参数。

背景信息

如果需要对接口上某类业务的报文进行流量整形，请选择此步骤配置。

配置端口队列整形前，需要配置基于简单流分类的优先级映射，将报文的优先级映射为 PHB 行为，或配置基于复杂流分类的内部优先级重标记，从而使不同业务进入不同的端口队列。

版权所有 © 华为技术有限公司

如果多个接口需要配置相同的队列整形速率，可通过端口组进行配置，以减少重复配置工作。

说明

基于简单流分类的优先级映射的配置请参见**配置基于简单流分类的优先级映射**。

基于复杂流分类的内部优先级重标记配置请参见**配置基于复杂流分类的流策略**。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **qos queue** *queue-index* **shaping cir** *cir-value* **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]，配置端口队列整形速率。

缺省情况下，端口队列的整形速率是端口的最大带宽。

----结束

检查配置结果

配置流量整形后，可以查看端口或端口队列的速率限制信息。

操作步骤

- 执行命令 **display qos lr** { **inbound** | **outbound** } **interface** *interface-type interface-number*，查看指定接口上的速率限制信息。
- 执行命令 **display qos queue statistics interface** *interface-type interface-number*，查看端口队列的速率限制信息。
- 执行命令 **display qos configuration interface** [*interface-type interface-number*]，查看接口上所有的 QoS 配置信息。

----结束

7.2.5 维护流量监管和流量整形

通过维护流量监管和流量整形，可以查看和清除流量监管和流量整形的统计信息。

查看流量统计信息

通过 **display** 命令，查看流量统计信息，如通过和丢弃的报文数。

背景信息

查看基于流的流量统计信息时，策略必须存在且已经包含流量统计动作。

版权所有 © 华为技术有限公司

操作步骤

- 执行命令 **display traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看基于流的流量统计信息。
- 执行命令 **display qos queue statistics interface** *interface-type interface-number*，查看接口上基于队列的流量统计信息。

----结束

查看队列使用情况

通过 **display** 命令查看接口优先级队列的使用情况。

背景信息

如果要了解队列的使用情况，可在任意视图下执行以下命令。

操作步骤

- 执行命令 **display qos queue length** *interface-type interface-number*，查看接口优先级队列的使用情况。

----结束

清除流量统计信息

通过 **reset** 命令清除流量统计信息。

背景信息



注意

清除基于流的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行命令 **reset traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } { **inbound** | **outbound** }，清除基于流的流量统计信息。
- 执行命令 **reset qos queue statistics interface** *interface-type interface-number*，清除接口上基于队列的流量统计信息。

----结束

7.2.6 配置举例

通过示例介绍如何应用流量监管和流量整形。配置示例中包括组网需求、配置注意事项、配置思路等。

版权所有 © 华为技术有限公司

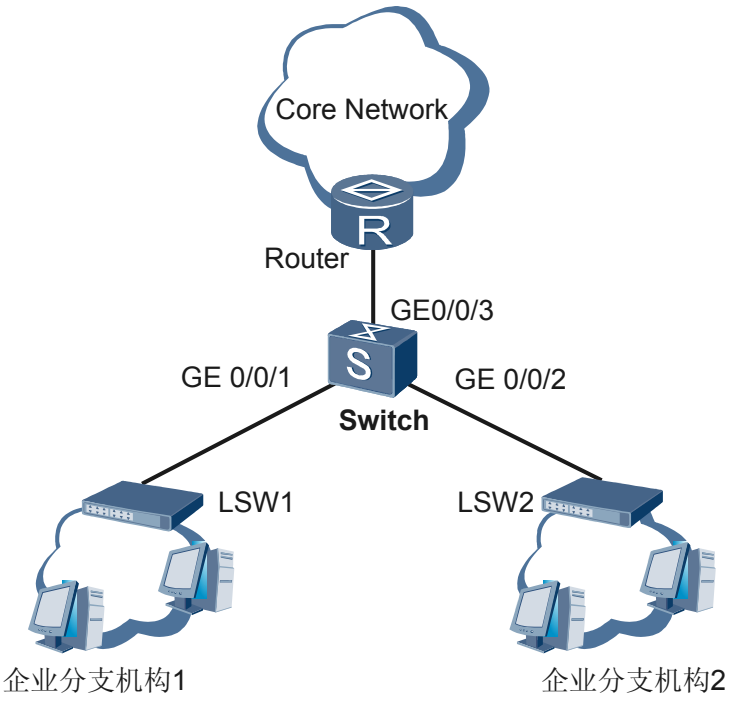
配置基于接口的流量监管示例

通过配置基于接口的流量监管示例，对不同用户提供不同的带宽服务。

组网需求

如图 7-7 所示，Switch 通过接口 GE0/0/3 与路由器互连，企业分支机构 1 和企业分支结构 2 通过接口 GE0/0/1 和 GE0/0/2 接入 Switch，经由 Switch 和路由器访问网络。企业分支机构 1 要求带宽为 8M，企业分支机构 2 要求带宽为 5M。

图 7-7 流量监管配置组网图



配置思路

采用如下的思路配置基于流量监管：

1. 配置 Switch 的各接口，使用户能够访问网络。
2. 在 Switch 接口 GE0/0/1 和 GE0/0/2 的上行方向上配置流量监管。

数据准备

为完成此配置例，需准备如下的数据：

- Switch 上行接口地址为 192.168.1.1/24。
- 企业分支机构 1 和企业分支机构 2 所属 VLAN 分别为 VLAN 100、VLAN 200。
- 企业分支机构 1 的带宽参数 CIR 为 8192kbit/s；企业分支机构 2 的带宽参数 CIR 为 5120kbit/s。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 VLAN 并配置 Switch 各接口

创建 VLAN 100、200、300，并将接口 GE0/0/1、GE0/0/2、GE0/0/3 分别加入 VLAN 100、200、300。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
```

将接口 GE0/0/1、GE0/0/2、GE0/0/3 的接入类型分别配置为 trunk，并分别允许 VLAN 100、200、300 通过。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 200 300
[Switch-GigabitEthernet0/0/1] quit
```

创建 VLANIF300，并配置网段地址 192.168.1.1/24。

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
[Switch-Vlanif300] quit
```

说明

请在 Router 上的与 Switch 对接的接口上配置 IP 地址 192.168.1.2/24。

步骤 2 配置基于接口的流量监管

在 Switch 接口 GE0/0/1 和 GE0/0/2 的上行方向上配置流量监管。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] qos lr inbound cir 8192
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] qos lr inbound cir 5120
[Switch-GigabitEthernet0/0/2] quit
[Switch] quit
```

步骤 3 验证配置结果

查看流量监管的配置信息。

```
[Switch] display qos lr inbound interface gigabitethernet0/0/1
 GigabitEthernet0/0/1 lr inbound:
  cir: 8192 Kbps, cbs: 1024000 Byte
[Switch] display qos lr inbound interface gigabitethernet0/0/2
 GigabitEthernet0/0/2 lr inbound:
  cir: 5120 Kbps, cbs: 640000 Byte
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 100 200 300
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 qos lr inbound cir 8192 cbs 1024000
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 qos lr inbound cir 5120 cbs 640000
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200 300
#

return
```

配置基于类的流量监管示例

通过配置基于类的流量监管，对不同的业务设置不同的 CAR 参数，提供不同的带宽服务。

组网需求

Switch 通过接口 GE0/0/2 与路由器互连，企业可经由 Switch 和路由器访问网络，如表 7-2 所示。

企业的语音业务对应的 VLAN ID 为 120，视频业务对应的 VLAN ID 分别为 110，数据业务对应的 VLAN ID 为 100。

在 Switch 上需要对不同业务的报文分别进行流量监管，以将流量限制在一个合理的范围之内，并保证各业务的带宽需求。

此外，由于来自用户侧的业务报文携带的 DSCP 优先级并不可靠，在实际应用中，不同业务对于服务质量的需求是不同的，所以在 Switch 中还需要重标记不同业务报文的 DSCP 优先级，以利于下游路由器按照报文的不同优先级分别进行处理。

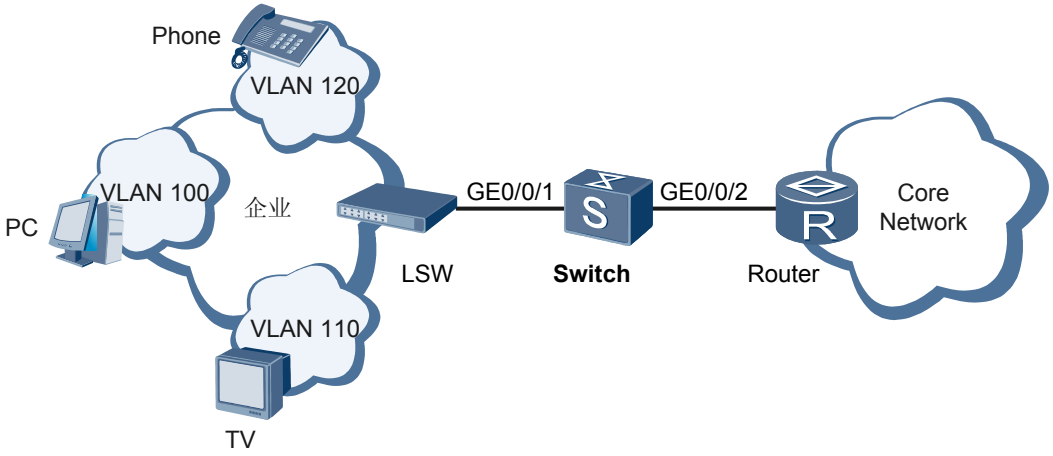
具体配置需求如下：

表 7-2 Switch 为上行流量提供的 QoS 保障

流量类型	CIR(Mbit/s)	PIR(Mbit/s)	DSCP 优先级
语音	2	10	46
视频	4	10	30
数据	4	10	14

版权所有 © 华为技术有限公司

图 7-8 基于复杂流分类的流量监管配置组网图



配置思路

采用如下的思路配置基于复杂流分类的流量监管：

1. 创建 VLAN，并配置各接口，使企业能够通过 Switch 访问网络。
2. 在 Switch 上配置基于 VLAN ID 进行流分类的匹配规则。
3. 在 Switch 上配置流行为，对来自企业的报文进行流量监管并且重标记报文的 DSCP 优先级。
4. 在 Switch 上配置流量监管策略，绑定已配置的流行为和流分类，并应用到企业与 Switch 连接的接口上。

数据准备

为完成此配置示例，需准备如下的数据：

- 匹配不同业务流的流分类名称。
- 对不同 VLAN ID 的报文进行重标记后的优先级值。
- 对不同 VLAN ID 的报文进行流量监管的参数：承诺信息速率、峰值信息速率。
- 需要应用流量监管策略的接口类型和编号。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 Switch 上创建 VLAN 100、110、120。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 110 120
```

将接口 GE0/0/1、GE0/0/2 的接入类型分别配置为 trunk，并分别将接口 GE0/0/1 和 GE0/0/2 加入 VLAN 100、VLAN 110、VLAN 120。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet0/0/2] quit
```

步骤 2 配置流分类

在 Switch 上创建流分类 c1 ～ c3，对来自企业的不同业务流按照其 VLAN ID 进行分类。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match vlan-id 120
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match vlan-id 110
[Switch-classifier-c2] quit
[Switch] traffic classifier c3 operator and
[Switch-classifier-c3] if-match vlan-id 100
[Switch-classifier-c3] quit
```

步骤 3 配置流量监管行为

在 Switch 上创建流行为 b1 ～ b3，对不同业务流进行流量监管以及重标记优先级。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 2000 pir 10000 green pass
[Switch-behavior-b1] remark dscp 46
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] car cir 4000 pir 10000 green pass
[Switch-behavior-b2] remark dscp 30
[Switch-behavior-b2] statistic enable
[Switch-behavior-b2] quit
[Switch] traffic behavior b3
[Switch-behavior-b3] car cir 4000 pir 10000 green pass
[Switch-behavior-b3] remark dscp 14
[Switch-behavior-b3] statistic enable
[Switch-behavior-b3] quit
```

步骤 4 配置流量监管策略并应用到接口上

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定并将流策略应用到接口 GE0/0/1 入方向上，对来自企业的报文进行流量监管和重标记。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] classifier c3 behavior b3
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] quit
```

步骤 5 验证配置结果

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: AND
    Rule(s) : if-match vlan-id 120

   Classifier: c2
    Operator: AND
    Rule(s) : if-match vlan-id 110

   Classifier: c3
```


版权所有 © 华为技术有限公司

```
    Operator: AND
    Rule(s) : if-match vlan-id 100

Total classifier number is 3
```

查看流策略的配置信息，以流策略 p1 为例。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
        Committed Access Rate:
        CIR 2000 (Kbps), CBS 250000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP ef
      statistic: enable
   Classifier: c2
    Operator: AND
     Behavior: b2
        Committed Access Rate:
        CIR 4000 (Kbps), CBS 500000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP af33
      statistic: enable
   Classifier: c3
    Operator: AND
     Behavior: b3
        Committed Access Rate:
        CIR 4000 (Kbps), CBS 500000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP af13
      statistic: enable
```

查看在接口上应用的流策略信息，以接口 GE0/0/1 为例。

```
[Switch] display traffic policy statistics interface gigabitethernet 0/0/1 inbound

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 3
 Current status: OK!
-----------------------------------------------------------------------
 Board : 0
Item                                Packets                       Bytes
-----------------------------------------------------------------------
Matched                                  10                       10000
  +--Passed                              8                        8000
  +--Dropped                             2                        2000
    +--Filter                            2                        2000
    +--URPF                              0                        0
    +--CAR                               2                        2000
```

----结束

版权所有 © 华为技术有限公司

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 100 110 120
#
traffic classifier c1 operator and
 if-match vlan-id 120
traffic classifier c2 operator and
 if-match vlan-id 110
traffic classifier c3 operator and
 if-match vlan-id 100
#
traffic behavior b1
 car cir 2000 pir 10000 cbs 250000 pbs 1250000 green pass yellow pass red discard
 remark dscp ef
 statistic enable
traffic behavior b2
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 green pass yellow pass red discard
 remark dscp af33
 statistic enable
traffic behavior b3
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 green pass yellow pass red discard
 remark dscp af13
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
#
return
```

配置层次化流量监管示例

通过配置层次化流量监管，对不同用户及其业务分别设置不同的 CAR 参数，提供不同的带宽服务。

组网需求

如图 7-9 所示，省中心与 A 市和 B 市之间的数据交换通过租用运营商网络实现，运营商给每个地市分配 2M 带宽，各城市中。省中心通过 Switch 连接运营商网络，需要在 Switch 上实现流量控制，确保：

- 省中心发往每个城市的流量严格限定在 2M 以内。
- 实现发往各城市的语音、视频、数据等类型流量根据优先级进行差别服务，高优先级的流量尽可能通过，低优先级的流量也有一定的带宽。
- 各流量在保证带宽的前提下，带宽随机分配。

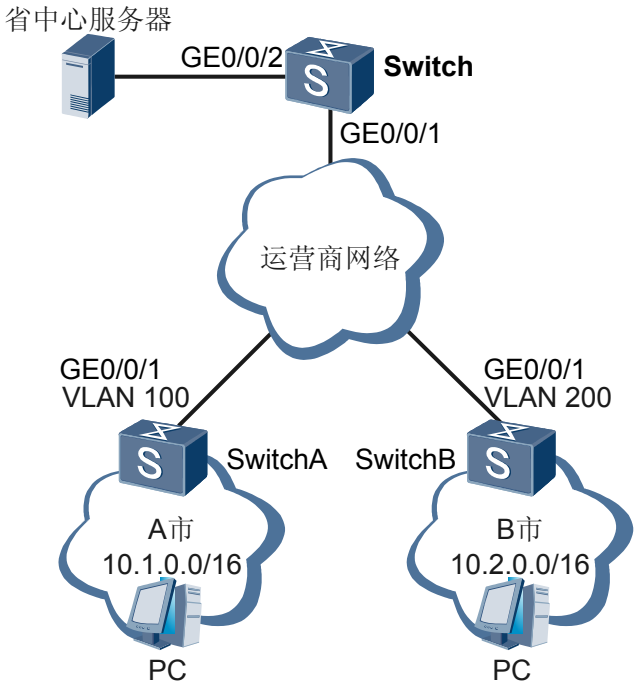
具体配置需求如下：

版权所有 © 华为技术有限公司

表 7-3 Switch 对下行流量的控制

城市	EF 流量	AF31 流量	AF11 流量	BE 流量
A 市	700k	400k	500k	200k
B 市	800k	500k	300k	100k

图 7-9 基于层次化流量监管配置组网图



配置思路

采用如下的思路配置基于复杂流分类的流量监管：

1. 配置 CAR 模板，将 A 市、B 市流量分别限制在 2M 内。
2. 配置 ACL，允许前往 A 市、B 市的流量通过。
3. 配置流分类，匹配规则为匹配各流量的优先级以及 ACL。
4. 配置流行为，对各类流量分配保证带宽，并限制各城市总流量。
5. 配置流策略，绑定已配置的流行为和流分类，并应用到省中心服务器与 Switch 连接的接口上。

数据准备

为完成此配置案例，需准备如下的数据：

- A 市、B 市的流量总带宽、CAR 模板名称。
- A 市、B 市的 ACL 编号、网段 IP 地址。

版权所有 © 华为技术有限公司

- 各类流量的优先级。
- 各类流量的保证带宽（承诺信息速率）。
- 流策略名称，以及应用此流策略的接口类型和编号。

操作步骤

步骤 1 配置 CAR 模板

创建并配置 A 市的 CAR 模板，将其总流量限制在 2M 内。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] qos car city_a cir 2000
```

创建并配置 B 市的 CAR 模板，将其总流量限制在 2M 内。

```
[Switch] qos car city_b cir 2000
```

步骤 2 配置 ACL

配置 ACL 3000，允许前往网段 IP 地址为 10.1.0.0/16 的 A 市的 TCP 报文通过。

```
[Switch] acl 3000
[Switch-acl-adv-3000] rule 5 permit tcp destination 10.1.0.0 0.0.255.255
```

配置 ACL 3001，允许前往网段 IP 地址为 10.2.0.0/16 的 B 市的 TCP 报文通过。

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule 5 permit tcp destination 10.2.0.0 0.0.255.255
```

步骤 3 配置流分类

创建 A 市各流量的流分类 city_a_ef、city_a_af31、city_a_af11、city_a_be，匹配规则分别为匹配 DSCP 优先级为 EF、AF31、AF11、0 的流量以及 ACL 3000；创建其他流量的流分类 city_a_default，匹配规则为匹配 ACL 3000。

```
[Switch] traffic classifier city_a_ef operator and
[Switch-classifier-city_a_ef] if-match dscp ef
[Switch-classifier-city_a_ef] if-match acl 3000
[Switch-classifier-city_a_ef] quit
[Switch] traffic classifier city_a_af31 operator and
[Switch-classifier-city_a_af31] if-match dscp af31
[Switch-classifier-city_a_af31] if-match acl 3000
[Switch-classifier-city_a_af31] quit
[Switch] traffic classifier city_a_af11 operator and
[Switch-classifier-city_a_af11] if-match dscp af11
[Switch-classifier-city_a_af11] if-match acl 3000
[Switch-classifier-city_a_af11] quit
[Switch] traffic classifier city_a_be operator and
[Switch-classifier-city_a_be] if-match dscp 0
[Switch-classifier-city_a_be] if-match acl 3000
[Switch-classifier-city_a_be] quit
[Switch] traffic classifier city_a_default operator and
[Switch-classifier-city_a_default] if-match acl 3000
[Switch-classifier-city_a_default] quit
```

创建 B 市各流量的流分类 city_b_ef、city_b_af31、city_b_af11、city_b_be，匹配规则分别为匹配 DSCP 优先级为 EF、AF31、AF11、0 的流量以及 ACL 3001；创建其他流量的流分类 city_b_default，匹配规则为匹配 ACL 3001。

```
[Switch] traffic classifier city_b_ef operator and
[Switch-classifier-city_b_ef] if-match dscp ef
[Switch-classifier-city_b_ef] if-match acl 3001
[Switch-classifier-city_b_ef] quit
[Switch] traffic classifier city_b_af31 operator and
```


版权所有 © 华为技术有限公司

```
[Switch-classifier-city_b_af31] if-match dscp af31
[Switch-classifier-city_b_af31] if-match acl 3001
[Switch-classifier-city_b_af31] quit
[Switch] traffic classifier city_b_af11 operator and
[Switch-classifier-city_b_af11] if-match dscp af11
[Switch-classifier-city_b_af11] if-match acl 3001
[Switch-classifier-city_b_af11] quit
[Switch] traffic classifier city_b_be operator and
[Switch-classifier-city_b_be] if-match dscp 0
[Switch-classifier-city_b_be] if-match acl 3001
[Switch-classifier-city_b_be] quit
[Switch] traffic classifier city_b_default operator and
[Switch-classifier-city_b_default] if-match acl 3001
[Switch-classifier-city_b_default] quit
```

步骤 4 配置流行为

创建并配置 A 市各流量的流行为 city_a_ef、city_a_af31、city_a_af11、city_a_be，使 DSCP 优先级为 EF、AF31、AF11、0 的流量的保证带宽分别为 700kbit/s、400kbit/s、500kbit/s 和 200kbit/s；创建其他流量的流行为 city_a_default，保证其他流量也有一定的带宽。

```
[Switch] traffic behavior city_a_ef
[Switch-behavior-city_a_ef] car cir 700 pir 2000
[Switch-behavior-city_a_ef] car city_a share
[Switch-behavior-city_a_ef] statistic enable
[Switch-behavior-city_a_ef] quit
[Switch] traffic behavior city_a_af31
[Switch-behavior-city_a_af31] car cir 400 pir 2000
[Switch-behavior-city_a_af31] car city_a share
[Switch-behavior-city_a_af31] statistic enable
[Switch-behavior-city_a_af31] quit
[Switch] traffic behavior city_a_af11
[Switch-behavior-city_a_af11] car cir 500 pir 2000
[Switch-behavior-city_a_af11] car city_a share
[Switch-behavior-city_a_af11] statistic enable
[Switch-behavior-city_a_af11] quit
[Switch] traffic behavior city_a_be
[Switch-behavior-city_a_be] car cir 200 pir 2000
[Switch-behavior-city_a_be] car city_a share
[Switch-behavior-city_a_be] statistic enable
[Switch-behavior-city_a_be] quit
[Switch] traffic behavior city_a_default
[Switch-behavior-city_a_default] car cir 64 pir 2000
[Switch-behavior-city_a_default] car city_a share
[Switch-behavior-city_a_default] statistic enable
[Switch-behavior-city_a_default] quit
```

创建并配置 B 市各流量的流行为 city_b_ef、city_b_af31、city_b_af11、city_b_be，使 DSCP 优先级为 EF、AF31、AF11、0 的流量的保证带宽分别为 800kbit/s、500kbit/s、300kbit/s 和 100kbit/s；创建其他流量的流行为 city_b_default，保证其他流量也有一定的带宽。

```
[Switch] traffic behavior city_b_ef
[Switch-behavior-city_b_ef] car cir 800 pir 2000
[Switch-behavior-city_b_ef] car city_b share
[Switch-behavior-city_b_ef] statistic enable
[Switch-behavior-city_b_ef] quit
[Switch] traffic behavior city_b_af31
[Switch-behavior-city_b_af31] car cir 500 pir 2000
[Switch-behavior-city_b_af31] car city_b share
[Switch-behavior-city_b_af31] statistic enable
[Switch-behavior-city_b_af31] quit
[Switch] traffic behavior city_b_af11
[Switch-behavior-city_b_af11] car cir 300 pir 2000
[Switch-behavior-city_b_af11] car city_b share
[Switch-behavior-city_b_af11] statistic enable
[Switch-behavior-city_b_af11] quit
```


版权所有 © 华为技术有限公司

```
[Switch] traffic behavior city_b_be
[Switch-behavior-city_b_be] car cir 100 pir 2000
[Switch-behavior-city_b_be] car city_b share
[Switch-behavior-city_b_be] statistic enable
[Switch-behavior-city_b_be] quit
[Switch] traffic behavior city_b_default
[Switch-behavior-city_b_default] car cir 64 pir 2000
[Switch-behavior-city_b_default] car city_b share
[Switch-behavior-city_b_default] statistic enable
[Switch-behavior-city_b_default] quit
```

步骤 5 配置流策略

创建并配置流策略 city_control，绑定流分类和对应的流行为，并将此流策略应用到省中心服务器与 S9300 连接的接口上。

```
[Switch] traffic policy city_control
[Switch-trafficpolicy-city_control] classifier city_a_ef behavior city_a_ef
[Switch-trafficpolicy-city_control] classifier city_a_af31 behavior city_a_af31
[Switch-trafficpolicy-city_control] classifier city_a_af11 behavior city_a_af11
[Switch-trafficpolicy-city_control] classifier city_a_be behavior city_a_be
[Switch-trafficpolicy-city_control] classifier city_a_default behavior city_a_default
[Switch-trafficpolicy-city_control] classifier city_b_ef behavior city_b_ef
[Switch-trafficpolicy-city_control] classifier city_b_af31 behavior city_b_af31
[Switch-trafficpolicy-city_control] classifier city_b_af11 behavior city_b_af11
[Switch-trafficpolicy-city_control] classifier city_b_be behavior city_b_be
[Switch-trafficpolicy-city_control] classifier city_b_default behavior city_b_default
[Switch-trafficpolicy-city_control] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy city_control inbound
[Switch-GigabitEthernet0/0/2] quit
```

步骤 6 验证配置结果

- 验证从 Switch 发往各城市的流量均被限定在 2M 内。

  使用测试仪模拟 EF、AF31、AF11、BE 以及其他优先级的流量，每种流量按照 100Mbit/s 同时从 Switch 的 GE 0/0/2 接口发往 A 市和 B 市，分别在 SwitchA 和 SwitchB 的接口 GE0/0/1 使用测试仪观察从运营商网络接收的流量，流量为 2Mbit/s。

- 验证其他优先级的流量也有一定的带宽

  使用测试仪模拟 DSCP 优先级为 EF 和为 AF21 的流量，每种流量按照 100Mbit/s 同时从 Switch 的 GE 0/0/2 发往 A 市，在 SwitchA 的接口 GE0/0/1 使用测试仪观察从运营商网络接收的两种流量，EF 流量带宽大于 700kbit/s，AF21 流量大于 64kbit/s，但两者流量总和为 2Mbit/s。

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 qos car city_a cir 2000 cbs 376000
 qos car city_b cir 2000 cbs 376000
#
acl number 3000
 rule 5 permit tcp destination 10.1.0.0 0.0.255.255
acl number 3001
 rule 5 permit tcp destination 10.2.0.0 0.0.255.255
#
traffic classifier city_a_af11 operator and
 if-match acl 3000
 if-match dscp af11
traffic classifier city_a_af31 operator and
```


版权所有 © 华为技术有限公司

```
 if-match dscp af31
 if-match acl 3000
traffic classifier city_a_be operator and
 if-match dscp default
 if-match acl 3000
traffic classifier city_a_default operator and
 if-match acl 3000
traffic classifier city_a_ef operator and
 if-match dscp ef
 if-match acl 3000
traffic classifier city_b_af11 operator and
 if-match dscp af11
 if-match acl 3001
traffic classifier city_b_af31 operator and
 if-match dscp af31
 if-match acl 3001
traffic classifier city_b_be operator and
 if-match dscp default
 if-match acl 3001
traffic classifier city_b_default operator and
 if-match acl 3001
traffic classifier city_b_ef operator and
 if-match dscp ef
 if-match acl 3001
#
traffic behavior city_a_af11
 car cir 500 pir 2000 cbs 62500 pbs 250000 green pass yellow pass red discard
 car city_a share
traffic behavior city_a_af31
 car cir 400 pir 2000 cbs 50000 pbs 250000 green pass yellow pass red discard
 car city_a share
traffic behavior city_a_be
 car cir 200 pir 2000 cbs 25000 pbs 250000 green pass yellow pass red discard
 car city_a share
traffic behavior city_a_default
 car cir 64 pir 2000 cbs 8000 pbs 250000 green pass yellow pass red discard
traffic behavior city_a_ef
 car cir 700 pir 2000 cbs 87500 pbs 250000 green pass yellow pass red discard
 car city_a share
traffic behavior city_b_af11
 car cir 300 pir 2000 cbs 37500 pbs 250000 green pass yellow pass red discard
 car city_b share
traffic behavior city_b_af31
 car cir 500 pir 2000 cbs 62500 pbs 250000 green pass yellow pass red discard
 car city_b share
traffic behavior city_b_be
 car cir 100 pir 2000 cbs 12500 pbs 250000 green pass yellow pass red discard
 car city_b share
traffic behavior city_b_default
 car cir 64 pir 2000 cbs 8000 pbs 250000 green pass yellow pass red discard
traffic behavior city_b_ef
 car cir 800 pir 2000 cbs 100000 pbs 250000 green pass yellow pass red discard
 car city_b share
#
traffic policy city_control
 classifier city_a_ef behavior city_a_ef
 classifier city_a_af31 behavior city_a_af31
 classifier city_a_af11 behavior city_a_af11
 classifier city_a_be behavior city_a_be
 classifier city_a_default behavior city_a_default
 classifier city_b_ef behavior city_b_ef
 classifier city_b_af31 behavior city_b_af31
 classifier city_b_af11 behavior city_b_af11
 classifier city_b_be behavior city_b_be
 classifier city_b_default behavior city_b_default
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 200
 traffic-policy city_control inbound
#
return
```

配置流量整形示例

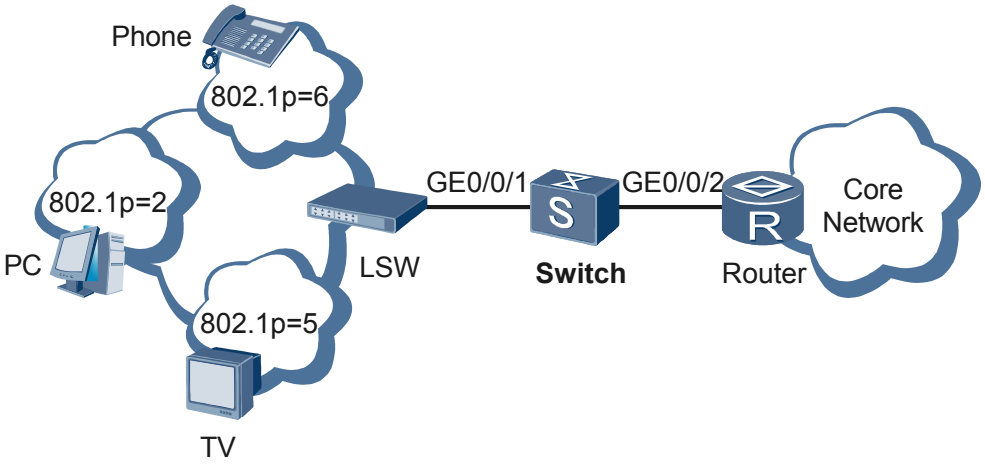
通过配置流量整形，对不同类型的业务报文设置不同的整形速率，以减少抖动，同时保证各类业务带宽要求。

组网需求

Switch 通过接口 GE0/0/2 与路由器互连，来自 Internet 的业务有语音、视频、数据，携带的 802.1p 优先级分别为 6、5、2，这些业务可经由路由器和 Switch 到达用户，如图 7-10 所示。由于来自网络侧的流量速率大于 LSW 接口的速率，出接口 GE0/0/1 处可能会发生带宽抖动。为减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

- 端口保证带宽为 20000kbit/s。
- 语音保证带宽为 3000kbit/s，峰值带宽为 5000kbit/s。
- 视频保证带宽为 5000kbit/s，峰值带宽为 8000kbit/s。
- 数据保证带宽为 2000kbit/s，峰值带宽为 3000kbit/s。

图 7-10 流量整形配置组网图



配置思路

采用如下的思路配置流量整形：

1. 创建 VLAN，并配置各接口，使用户能够通过 Switch 访问网络。
2. 配置接口信任报文的 802.1p 优先级。
3. 配置端口整形功能，限制端口带宽。
4. 配置端口队列整形功能，限制语音、视频、数据三类业务的带宽。

版权所有 © 华为技术有限公司

数据准备

为完成此配置示例，需准备如下的数据：

- 802.1p 优先级。
- 端口整形速率。
- 端口各队列整形速率。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN 10。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 10
```

将接口 GE0/0/1、GE0/0/2 的接入类型分别配置为 trunk，并分别将接口 GE0/0/1、GE0/0/2 加入 VLAN 10。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/2] quit
```

创建 VLANIF10，并配置网段地址 10.10.10.1/24。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.10.10.1 255.255.255.0
[Switch-Vlanif10] quit
```

说明

请在 Router 上的与 Switch 对接的接口上配置 IP 地址 10.10.10.2/24。

步骤 2 配置接口信任报文的类型

配置接口信任报文的 802.1p 优先级。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] trust 8021p
[Switch-GigabitEthernet0/0/2] quit
```

步骤 3 配置端口整形

在 Switch 上配置端口整形，将端口速率限制在 20000kbit/s。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 2500000
```

步骤 4 配置端口队列整形

配置调度模式为 WRR 调度，队列 6、5、2 的 WRR 权重分别为 60、40、20，其它队列采用缺省权重。

```
[Switch-GigabitEthernet0/0/1] qos wrr
[Switch-GigabitEthernet0/0/1] qos queue 6 wrr weight 60
[Switch-GigabitEthernet0/0/1] qos queue 5 wrr weight 40
[Switch-GigabitEthernet0/0/1] qos queue 2 wrr weight 20
```


版权所有 © 华为技术有限公司

在 Switch 上配置端口队列整形，使语音、视频、数据业务的保证带宽分别为 3000kbit/s、5000kbit/s、2000kbit/s，峰值带宽分别为 5000kbit/s、8000kbit/s、3000kbit/s。

```
[Switch-GigabitEthernet0/0/1] qos queue 6 shaping cir 3000 pir 5000
[Switch-GigabitEthernet0/0/1] qos queue 5 shaping cir 5000 pir 8000
[Switch-GigabitEthernet0/0/1] qos queue 2 shaping cir 2000 pir 3000
[Switch-GigabitEthernet0/0/1] quit
[Switch] quit
```

步骤 5 验证配置结果

配置成功后，从接口 GE0/0/1 发出的报文保证速率为 20000kbit/s；语音业务保证速率为 3000kbit/s，不超过 5000kbit/s；视频业务保证速率为 5000kbit/s，不超过 8000kbit/s；数据业务保证速率为 2000kbit/s，不超过 3000kbit/s。

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 qos lr outbound cir 20000 cbs 2500000
 qos wrr
 qos queue 2 wrr weight 20
 qos queue 5 wrr weight 40
 qos queue 6 wrr weight 60
 qos queue 2 shaping cir 2000 pir 3000
 qos queue 5 shaping cir 5000 pir 8000
 qos queue 6 shaping cir 3000 pir 5000
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 trust 8021p
#
return
```

7.3 拥塞避免和拥塞管理配置

拥塞避免和拥塞管理配置介绍了拥塞避免和拥塞管理的基本概念、配置方法和配置示例。

7.3.1 拥塞避免和拥塞管理概述

拥塞避免和拥塞管理概述介绍了拥塞避免和拥塞管理基本概念。

版权所有 © 华为技术有限公司

拥塞避免

拥塞避免是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种流量控制机制。

先后出现过尾部丢弃（Tail-Drop）、随机早期检测 RED（Random Early Detection）、加权随机早期检测 WRED（Weighted Random Early Detection）等拥塞避免策略。AC6605 基于 WRED 实现拥塞避免。

尾部丢弃

传统的丢包策略采用尾部丢弃的方法，同等的对待所有的报文，不对服务等级进行区分。在拥塞发生期间，队列尾部的数据报文将被丢弃，直到拥塞解决。

这种丢弃策略会引发 TCP 全局同步现象。所谓 TCP 全局同步现象，是指当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量；而后这几个 TCP 连接又会在某个时刻同时出现流量高峰。如此反复，使网络流量忽大忽小，影响链路利用率。

RED

RED 技术通过随机地丢弃报文，让多个 TCP 连接不同时降低发送速度，从而避免了 TCP 的全局同步现象。

在 RED 技术的算法中，为每个队列的长度都设定了阈值上下限，并规定：

- 当队列的长度小于阈值下限时，不丢弃报文。
- 当队列的长度大于阈值上限时，丢弃所有收到的报文。
- 当队列的长度在阈值上限和阈值下限之间时，开始随机丢弃到来的报文。方法是为每个到来的报文赋予一个随机数，并用该随机数与当前队列的丢弃概率比较，如果大于丢弃概率则报文被丢弃。队列越长，报文被丢弃的概率越高。

WRED

WRED 技术也是通过随机丢弃报文来避免 TCP 的全局同步现象，但该技术生成的随机丢弃参数是基于优先级的，它通过报文的不同颜色来区别丢弃策略，考虑了高优先级报文的利益并使其被丢弃的概率相对较小。

SRED

基于 RED 技术，AC6605 设备上实现了 SRED（Simple Random Early Detection）。在接口出队列上，SRED 根据报文的优先级将其区分为红色、黄色，并分别为红色和黄色的报文设定起始丢包点和丢包率。

根据 SRED，AC6605 按照一定的丢弃概率主动丢弃队列中的报文，从而调整从接口输出的流量速率。

拥塞管理

当网络中间歇性的出现拥塞，时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务时，需要进行拥塞管理；如果任何时候都出现拥塞，则需要增加带宽。

拥塞管理一般采用队列调度技术，目前 AC6605 采用的队列调度技术有：

版权所有 © 华为技术有限公司

- PQ 调度
- WRR 调度
- DRR 调度
- PQ+WRR/PQ+DRR 调度

PQ 调度

PQ（Priority Queuing）调度，就是严格按照队列优先级的高低顺序进行调度。只有高优先级队列中的报文全部调度完毕后，低优先级队列才有调度机会。

采用 PQ 调度方式，将延迟敏感的关键业务放入高优先级队列，将非关键业务放入低优先级队列，从而确保关键业务被优先发送。

PQ 调度的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

WRR 调度

WRR（Weighted Round Robin）调度即加权轮询调度。WRR 在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。

以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），加权值表示获取资源的比重。例如：一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 50、50、30、30、10、10、10、10（依次对应 w7、w6、w5、w4、w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 5Mbit/s 带宽，避免了采用 PQ 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

WRR 还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

WRR 调度有两个缺点：

- WRR 调度按照报文个数进行调度，而用户一般关心的是带宽。当每个队列的平均报文长度相等或已知时，通过配置 WRR 权重，用户能够获得想要的带宽；但是，当队列的平均报文长度变化时，用户就不能通过配置 WRR 权重获取想要的带宽。
- 低延时需求业务（如语音）得不到及时调度。

DRR 调度

DRR（Deficit Round Robin）调度实现原理与 WRR 调度基本相同。

DRR 与 WRR 的区别是：WRR 调度是按照报文个数进行调度，而 DRR 是按照报文长度进行调度。如果报文长度超过了队列的调度能力，DRR 调度允许出现负权重，以保证长报文也能够得到调度。但下次轮循调度时该队列将不会被调度，直到权重为正，该队列才会参与 DRR 调度。

DRR 调度避免了采用 PQ 调度时低优先级队列中的报文可能长时间得不到服务的缺点，也避免了各队列报文长度不等或变化较大时，WRR 调度不能按配置比例分配带宽资源的缺点。

但是，DRR 调度也具有低延时需求业务（如语音）得不到及时调度的缺点。

版权所有 © 华为技术有限公司

PQ+WRR/PQ+DRR 调度

PQ 调度和 WRR/DRR 调度各有优缺点。单纯采用 PQ 调度时，低优先级队列中的报文长期得不到带宽，而单纯采用 WRR/DRR 调度时低延时需求业务得不到优先调度，“PQ+WRR/PQ+DRR”调度方式则将前两种调度方式结合起来，不仅能发挥两种调度的优势，而且能克服两种调度各自的缺点。

用户可以借助“PQ+WRR/PQ+DRR”调度方式，将重要的协议报文和有低延时需求的业务报文放入 PQ 队列中进行调度，并为该队列分配指定带宽；而将其他报文按各自的优先级放入采用 WRR/DRR 调度的各队列中，按照权值对各队列进行循环调度。

7.3.2 配置拥塞避免

配置拥塞避免后，AC6605 将根据 WRED 的配置信息对不同颜色的报文进行相应的处理。

建立配置任务

在配置拥塞避免前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

为避免网络拥塞的发生，解决 TCP 全局同步的问题，可以通过配置 WRED，调整网络流量，解除网络过载。

前置任务

在配置拥塞避免之前，需在报文的入接口上完成以下任务：

- 配置基于简单流分类的优先级映射，将报文的优先级映射为 PHB 行为并着色
- 配置基于复杂流分类的流量监管和重标记

说明

在配置拥塞避免任务之前，需要通过这两条前置任务中的任意一条为报文着色，作为拥塞避免操作的依据。

数据准备

在配置拥塞避免之前，需要准备以下数据。

序号	数据
1	WRED 的高低阈值与最大丢弃概率

（可选）配置端口队列长度

通过配置端口队列长度，设置接口指定队列可以缓存报文的最大报文个数。

版权所有 © 华为技术有限公司

背景信息

配置端口队列长度前，应先执行 shutdown（接口视图）命令关闭接口，否则将导致流量中断，且系统提示告警信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **qos queue** *queue-index* **length** *length-value*，配置接口优先级队列的长度。

----结束

（可选）配置 CFI 作为内部丢弃优先级

配置 CFI 作为内部丢弃优先级后，在报文超出 CIR（承诺信息速率）时 AC6605 会将报文的 DEI 位置 1。当发生拥塞的时候，AC6605 将优先丢弃 DEI 位置 1 的报文。

背景信息

VLAN Tag 中的 CFI（Canonical Format Indicator）字段又称为 DEI（Drop Eligible Indicator），在某些情况下用来标识报文的丢弃优先级，某些设备在报文超出 CIR（承诺信息速率）时会将报文的 DEI 位置 1，标识该报文的丢弃优先级为高，后续设备在拥塞的时候优先丢弃 DEI 位置 1 的报文。

如果多个接口需要配置 CFI 作为内部丢弃优先级，可通过端口组进行配置，以减少重复配置工作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

- *interface-type* 可以是 GE 接口或 Eth-Trunk 接口。
- 端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **dei enable**，配置 CFI 作为内部丢弃优先级。

缺省情况下，未设置 CFI 字段为内部丢弃优先级。

----结束

配置 WRED 模板

通过配置 WRED 模板，设置对具有不同 PHB 颜色的报文的丢弃高低门限以及最大丢弃概率。

背景信息

在需要配置拥塞避免的 AC6605 上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **drop-profile** *drop-profile-name*，创建丢弃模板，并进入丢弃模板视图。

系统存在一个缺省 WRED 模板 default，只能修改其参数，不能删除。

步骤 3 执行命令 **color** { **green** | **non-tcp** | **red** | **yellow** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置 WRED 参数。

缺省情况下，WRED 模板的高低门限以及最大丢弃概率的取值均为 100。

----结束

应用 WRED 模板

配置的 WRED 模板必须应用后才能生效。可以将 WRED 模板应用在全局、接口或队列上。

背景信息

AC6605 支持在全局、端口、端口队列上应用 WRED 模板，可根据需要配置其中一种或多种。

- 如果同时在全局、端口上应用了 WRED 模板，以端口上应用的模板为准。全局应用等效于在所有端口应用。
- 如果同时在端口、端口队列应用了 WRED 模板，系统按照“端口队列 > 端口”的顺序依次匹配报文流，然后依次对报文流进行拥塞避免控制（不匹配的不作）。

如果多个接口需要配置相同的 WRED 模板，可通过端口组进行配置，以减少重复配置工作。

应用 WRED 模板前，必须先通过 **drop-profile** 命令创建丢弃模板。

操作步骤

- 在全局应用 WRED 模板
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **qos queue** *queue-index* **wred** *drop-profile-name*，将 WRED 模板应用于全局。
- 在接口上应用 WRED 模板
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **qos wred** *drop-profile-name*，将 WRED 模板应用于接口。
- 在端口组应用 WRED 模板
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **port-group** *port-group-name*，进入端口组视图。

     说明

     端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。
  3. 执行命令 **qos wred** *drop-profile-name*，将 WRED 模板应用于端口组。

版权所有 © 华为技术有限公司

- 在端口队列上应用 WRED 模板
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **qos queue** *queue-index* **wred** *drop-profile-name*，将 WRED 模板应用于端口队列。

  drop-profile-name 为 WRED 模板名，必须与**配置 WRED 模板**中配置的 WRED 模板名相同。

----结束

检查配置结果

配置拥塞避免后，可以查看模板的名称、模板的索引、模板的参数等信息。

前提条件

已经完成 WRED 模板的配置。

操作步骤

- 执行命令 **display drop-profile** [**all** | **name** *drop-profile-name*]，查看 WRED 模板的配置结果。
- 执行命令 **display qos configuration interface** [*interface-type interface-number*]，查看接口上所有的 QoS 配置信息。

----结束

7.3.3 配置拥塞管理

配置拥塞管理后，当网络中发生拥塞时，AC6605 将按照制定的调度策略决定报文转发时的处理次序。

建立配置任务

在配置拥塞管理前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当网络发生拥塞时，若用户希望能均衡各类报文的延迟和延迟抖动，关键业务（如视频业务、语音业务）的报文能够得到优先处理；同时对于非关键业务（如 E-Mail）的报文，保证相同优先级业务得到公平处理，不同优先级业务按照各自权值处理。可以通过配置拥塞管理来实现。

前置任务

在配置拥塞管理之前，需在报文的入接口上完成以下任务：

- 基于简单流分类的优先级映射
- 配置基于复杂流分类的内部优先级重标记

版权所有 © 华为技术有限公司

说明

在配置拥塞管理任务之前，需要通过这两条前置任务中的任意一条将报文映射进不同的队列，从而进行队列调度。

数据准备

在配置拥塞管理之前，需要准备以下数据。

序号	数据
1	本地优先级和队列之间的映射关系
2	队列的调度模式
3	DRR 调度中各队列的权值
4	WRR 调度中各队列的权值
5	（可选）最小静态缓冲区大小
6	（可选）队列的最大长度

（可选）配置端口队列长度

通过配置端口队列长度，设置接口指定队列可以缓存报文的最大报文个数。

背景信息

配置端口队列长度前，应先执行 shutdown（接口视图）命令关闭接口，否则将导致流量中断，且系统提示告警信息。

操作步骤

- 在 AC6605 交换机上配置端口队列长度
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **qos queue** *queue-index* **length** *length-value*，配置接口优先级队列的长度。

----结束

配置端口队列调度

AC6605 支持的端口对列调度方式包括：PQ、DRR、WRR、PQ+DRR、PQ+WRR。

背景信息

AC6605 支持 8 个端口队列，不同的队列可以采用不同的队列调度算法。队列调度时，先调度 PQ 队列，多个 PQ 队列按优先级高低顺序进行调度。PQ 队列调度完成后，再对 WRR 或 DRR 队列进行加权轮循调度。

如果多个接口需要配置相同的队列调度参数，可通过端口组进行配置，以减少重复配置工作。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

或执行命令 **port-group** *port-group-name*，进入端口组视图。

说明

端口组必须事先创建并配置，有关端口组的描述及配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的**配置端口组**。

步骤 3 执行命令 **qos** { **pq** | **wrr** | **drr** }，配置端口队列调度方式为 PQ、WRR 或 DRR。

缺省情况下，端口队列的调度方式为 WRR。

步骤 4 （可选）执行命令 **qos queue** *queue-index* **wrr weight** *weight*，指定端口队列 WRR 调度的权值。

缺省情况下，WRR 调度方式的队列权重为 1。

只有端口队列调度方式为 WRR 或 PQ+WRR 时，才需要使用此步骤配置。

说明

在采用 WRR 调度方式的前提下，如果设置某队列权值为 0，说明该队列以 PQ 方式调度，此时对应的整体调度方式为 PQ+WRR。

步骤 5 （可选）执行命令 **qos queue** *queue-index* **drr weight** *weight*，指定端口队列 WRR 调度的权值。

缺省情况下，DRR 调度方式的队列权重为 1。

只有端口队列调度方式为 DRR 或 PQ+DRR 时，才需要使用此步骤配置。

说明

在采用 DRR 调度方式的前提下，如果设置某队列权值为 0，说明该队列以 PQ 方式调度，此时整体调度方式为 PQ+DRR。

----结束

检查配置结果

配置拥塞管理后，可以查看指定接口上基于队列的流量统计信息和各队列的调度参数。

前提条件

已经完成拥塞管理的配置。

操作步骤

- 执行命令 **display qos local-precedence-queue-map**，查看本地优先级和队列之间的映射关系。
- 执行命令 **display qos configuration interface** [*interface-type interface-number*]，查看接口上所有的 QoS 配置信息。

----结束

版权所有 © 华为技术有限公司

7.3.4 维护拥塞避免和拥塞管理

通过维护流量监管和流量整形，可以查看和清除基于队列的流量的统计信息。

查看队列统计信息

通过 **display** 命令，查看基于队列的流量统计信息，如通过和丢弃的报文数量。

背景信息

执行以下步骤查看基于队列的统计信息。

操作步骤

- 执行命令 **display qos queue statistics interface** *interface-type interface-number*

----结束

清除队列统计信息

通过 **reset** 命令，清除基于队列的流量统计信息。

背景信息

当需要对接口上基于队列的流量信息重新进行统计时，可以在用户视图下执行以下命令，清除之前的统计信息。



注意

清除接口上基于队列的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行命令 **reset qos queue statistics interface** *interface-type interface-number*，清除接口上基于队列的流量统计信息。

----结束

7.3.5 配置举例

通过示例介绍拥塞避免和拥塞管理。

配置拥塞避免和拥塞管理综合示例

通过配置拥塞避免和拥塞管理，AC6605 为不同优先级的报文提供不同的服务，保证用户对于高优先级、低延迟业务的服务要求。

版权所有 © 华为技术有限公司

组网需求

Switch 通过接口 GE0/0/3 与路由器互连，来自 Internet 的业务有语音、视频、数据，携带的 802.1p 优先级分别为 6、5、2，这些业务可经由路由器和 Switch 到达用户，如图 7-11 所示。由于 Switch 入接口 GE0/0/3 的速率大于出接口 GE0/0/1、GE0/0/2 的速率，在这两个出接口处可能会发生拥塞。为了减轻网络拥塞造成的影响，保证用户对于高优先级、低延迟业务的服务要求，配置需求如下表所述。

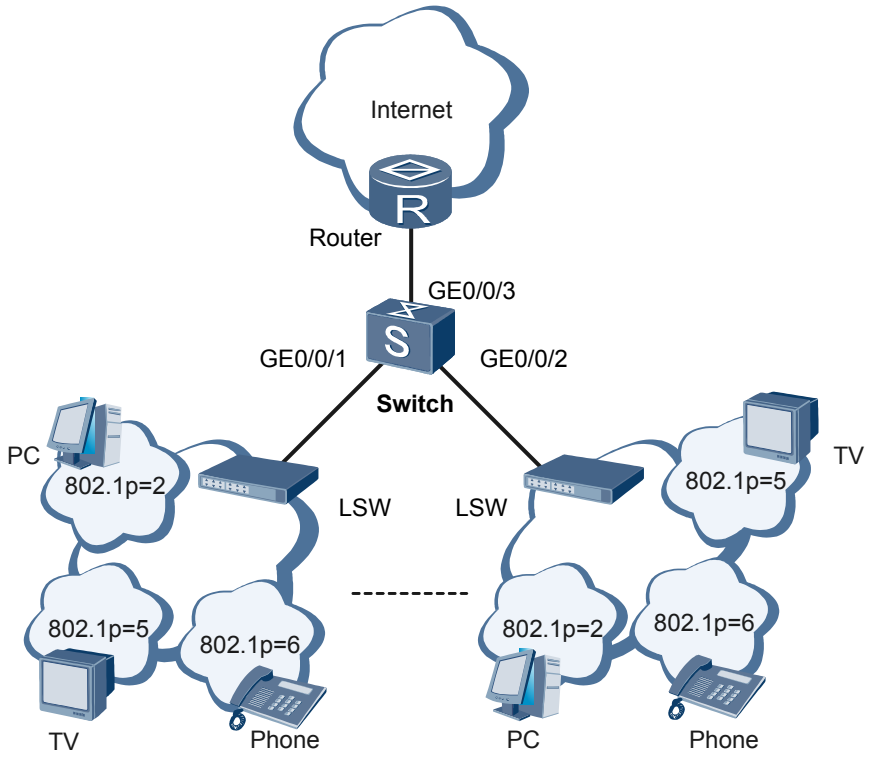
表 7-4 拥塞避免配置参数

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率
语音	绿	80	100	10
视频	黄	60	80	20
数据	红	40	60	40

表 7-5 拥塞管理配置参数

业务类型	服务等级
语音	EF
视频	AF3
数据	AF1

图 7-11 拥塞避免和拥塞管理配置组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置：

1. 配置各接口所属的 VLAN，使各设备间链路互通。
2. 在 Switch 上创建并配置 DiffServ 域，将 802.1p 优先级映射为 PHB 行为并着色，并在 Switch 入接口上绑定 DiffServ 域。
3. 在 Switch 上配置 WRED 模板，并在出接口应用 WRED 模板。
4. 在 Switch 出接口上配置各服务等级队列的调度参数。

数据准备

为完成此配置示例，需准备如下的数据：

- 数据、视频、语音业务报文所带 VLAN 分别为 2、5、6。
- 802.1p 优先级 6、5、2 分别映射的 PHB 行为及颜色。
- WRED 模板名及 WRED 参数。
- 各服务等级队列的调度参数。

操作步骤

步骤 1 配置各接口所属的 VLAN，使各设备间链路互通。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 2 5 6
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet0/0/3] quit
```

步骤 2 配置基于简单流分类的优先级映射

创建 DiffServ 域 ds1，将 802.1p 优先级 6、5、2 分别映射为 PHB 行为 EF、AF3、AF1，并分别将颜色标记为绿色、黄色、红色。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 6 phb ef green
[Switch-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[Switch-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[Switch-dsdomain-ds1] quit
```

在 Switch 入接口 GE0/0/3 上绑定 DiffServ 域。

```
[Switch] interface gigabitethernet0/0/3
[Switch-GigabitEthernet0/0/3] trust upstream ds1
[Switch-GigabitEthernet0/0/3] trust 8021p inner
[Switch-GigabitEthernet0/0/3] quit
```

步骤 3 配置拥塞避免

版权所有 © 华为技术有限公司

在 Switch 上创建 WRED 模板 wred1，并配置 wred1 的三色报文参数。

```
[Switch] drop-profile wred1
[Switch-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[Switch-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[Switch-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[Switch-drop-wred1] quit
```

在 Switch 出接口 GE0/0/1、GE0/0/2 上应用 WRED 模板 wred1。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] qos wred wred1
[Switch-GigabitEthernet0/0/1] qos queue 5 wred wred1
[Switch-GigabitEthernet0/0/1] qos queue 3 wred wred1
[Switch-GigabitEthernet0/0/1] qos queue 1 wred wred1
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] qos wred wred1
[Switch-GigabitEthernet0/0/2] qos queue 5 wred wred1
[Switch-GigabitEthernet0/0/2] qos queue 3 wred wred1
[Switch-GigabitEthernet0/0/2] qos queue 1 wred wred1
[Switch-GigabitEthernet0/0/2] quit
```

步骤 4 配置拥塞管理

在 Switch 的报文出接口 GE0/0/1、GE0/0/2 上配置各服务等级队列的调度参数。

```
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] qos drr
[Switch-GigabitEthernet0/0/1] qos queue 5 drr weight 0
[Switch-GigabitEthernet0/0/1] qos queue 3 drr weight 100
[Switch-GigabitEthernet0/0/1] qos queue 1 drr weight 50
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet0/0/2
[Switch-GigabitEthernet0/0/2] qos drr
[Switch-GigabitEthernet0/0/2] qos queue 5 drr weight 0
[Switch-GigabitEthernet0/0/2] qos queue 3 drr weight 100
[Switch-GigabitEthernet0/0/2] qos queue 1 drr weight 50
[Switch-GigabitEthernet0/0/2] quit
[Switch] quit
```

步骤 5 验证配置结果

查看 DiffServ 域 ds1 的配置信息。

```
<Switch> display diffserv domain name ds1
Diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 red
 8021p-inbound 2 phb af2 red
 8021p-inbound 3 phb af3 yellow
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs7 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 ......
```

查看 WRED 模板配置信息。

```
<Switch> display drop-profile name wred1
Drop-profile[3]: wred1
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
```


版权所有 © 华为技术有限公司

```
Non-tcp    100          100          100
------------------------------------------------------------
```

----结束

配置文件

- Switch 的配置文件

```
#
 sysname Switch
#
 vlan batch 2 5 6
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
 drop-profile wred1
  color green low-limit 80 high-limit 100 discard-percentage 10
  color yellow low-limit 60 high-limit 80 discard-percentage 20
  color red low-limit 40 high-limit 60 discard-percentage 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 qos drr
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 5 drr weight 0
 qos wred wred1
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 qos drr
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 5 drr weight 0
 qos wred wred1
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 trust upstream ds1
 trust 8021p inner
#
return
```


版权所有 © 华为技术有限公司

8 安全配置

关于本章

本文档针对 AC6605 应用中的安全方面的要求，从基本原理、配置步骤和配置举例方面介绍了 AAA 及用户管理、网络接入控制（NAC）、DHCP Snooping、ARP 安全、IP Source Guard、IP Source Trail、本机防攻击、PPPoE+、MAC 强制转发（MFF）、流量抑制以及访问控制列表（ACL）的配置方法。

本文档提供了 AC6605 安全特性的原理和配置方法。

8.1 AAA 及用户管理配置
介绍 AAA、本地用户管理、RADIUS、HWTACACS、域的原理和配置。

8.2 NAC 配置
介绍 NAC 的原理和配置。

8.3 DHCP Snooping 配置
介绍 DHCP Snooping 的原理和配置方法，并给出配置举例。

8.4 ARP 安全配置
ARP 安全通过过滤不信任的 ARP 报文以及对某些 ARP 报文进行时间戳抑制来保证网络设备的安全性和健壮性。

8.5 IP 源防攻击配置
介绍防止针对 IP 源进行攻击的原理和配置方法。

8.6 本机防攻击配置
介绍本机防攻击的原理和配置。

8.7 MFF 配置
介绍 MFF（MAC-Forced Forwarding，MAC 强制转发）的原理和配置。

8.8 流量抑制配置
介绍流量抑制的原理和配置。

8.9 ACL 配置
ACL 通过一系列规则对数据包进行分类，这些规则应用到 AC6605 接口上，AC6605 根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

8.10 ND Snooping 配置

版权所有 © 华为技术有限公司

介绍 ND Snooping 的原理和配置方法，并给出配置举例。

版权所有 © 华为技术有限公司

8.1 AAA 及用户管理配置

介绍 AAA、本地用户管理、RADIUS、HWTACACS、域的原理和配置。

8.1.1 AAA 及用户管理概述

简要介绍 AAA 及用户管理的知识。

AAA

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称。它提供对用户进行认证、授权和计费三种功能。

- 认证：验证用户是否可以获得访问权。
- 授权：授权用户可以使用哪些服务。
- 计费：记录用户使用网络资源的情况。

AAA 一般采用“客户端—服务器”结构。这种结构既具有良好的可扩展性，又便于用户信息的集中管理。

基于域的用户管理

用户的认证、授权、计费都需要在域下执行。通过域来进行用户管理，域下可以进行授权配置、认证和计费方案的配置、RADIUS/HWTACACS 服务器模板配置等。

本地用户管理

本地用户管理是指在本地 AC6605 上建立本地用户数据库，维护用户信息，并对用户进行管理。

8.1.2 AC6605 支持的 AAA 及用户管理特性

介绍 AAA 及用户管理特性在 AC6605 中的支持情况。

AAA

AC6605 支持的认证方案包括：

- 无需认证（None 认证方式）：当对用户非常信任时，不对其进行合法性检查，其他情况下一般不采用这种方式。
- 本地认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在 AC6605 上，并使用这些用户信息对本地用户进行认证。本地认证的优点是速度快；缺点是存储信息量受设备硬件条件限制。
- 远端认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在认证服务器上。AC6605 作为客户端，与认证服务器通信，通过 RADIUS（Remote Authentication Dial In User Service）协议或 HWTACACS（HUAWEI Terminal Access Controller Access Control System）协议进行远端认证。

说明

如果在一个认证方案中采用多种认证方式，将按照认证方式的配置先后顺序依次进行认证，None 认证必须作为最后一种认证方式。

版权所有 © 华为技术有限公司

AC6605 支持的授权方案包括：

- 无需授权：对用户非常信任，直接授权通过。
- 本地授权：根据 AC6605 上为本地用户帐号配置的相关属性进行授权。
- 远端授权：AC6605 作为客户端，与授权服务器通信，通过 HWTACACS 协议进行远端授权。
- If Authenticated 授权：如果用户通过了认证，并且使用了本地认证或远端认证模式，则用户授权通过。

AC6605 支持的计费方案包括：

- 不计费：不对用户进行计费。
- RADIUS 计费：AC6605 将计费报文送往 RADIUS 服务器，由 RADIUS 服务器完成对用户的计费。
- HWTACACS 计费：AC6605 将计费报文送往 HWTACACS 服务器，由 HWTACACS 服务器完成对用户的计费。

在 RADIUS/HWTACACS 计费模式中，正常情况下 AC6605 在用户上线和下线时各生成一份计费报文传送给服务器，服务器根据计费报文中的信息（上下线时间）对用户进行计费。

AC6605 支持实时计费功能。实时计费功能是指用户在线过程中，AC6605 定时生成计费报文传送给服务器。通过实时计费功能，AC6605 可以在其和服务器通信中断时，最大程度的减少计费异常的时间。

本地用户管理

本地用户管理是指在本地 AC6605 上建立本地用户数据库，维护用户信息，并对用户进行管理。

如果认证方案采用本地认证模式，或者授权方案采用本地授权模式，则需要 **8.1.8 配置本地用户管理**。

基于域的用户管理

AC6605 通过域来进行用户管理，域下可以配置认证、授权和计费方案。属于该域的用户通过指定的方案进行认证和授权。

AC6605 的所有用户都属于某个域。用户所属的域是由域分隔符后的字符串来决定的。域分隔符可以是“@”、“|”、“%”等符号，比如：用户名“user@huawei”，就属于 huawei 域。如果用户名中没有带@，就属于系统缺省的 default 域。

缺省情况下，AC6605 存在配置名为 default 和 default_admin 两个域，不能删除，只能修改。当无法确认接入用户的域时使用缺省域。

- default 用于接入用户的缺省域，缺省为本地认证。
- default_admin 用于管理员的缺省域，缺省为本地认证。

AC6605 总共可以配置 32 个域，包括缺省的两个域。

域下配置的授权信息较 AAA 服务器的授权信息优先级低，即，优先使用 AAA 服务器下发的授权属性，在 AAA 服务器无该项授权或不支持该项授权时，域的授权属性生效。这样处理可以凭借域管理灵活增加业务，而不必受限于 AAA 服务器提供的属性。

版权所有 © 华为技术有限公司

RADIUS 模板和 HWTACACS 模板

如果认证方案或授权方案指定通过 RADIUS 协议或 HWTACACS 协议与服务器通信，则需要在域下配置 RADIUS 或 HWTACACS 模板。

- RADIUS 模板中，可以指定认证和计费服务器的 IP 地址、端口号、密钥等属性。
- HWTACACS 模板中，可以指定认证服务器的 IP 地址、计费服务器的 IP 地址、授权服务器的 IP 地址、端口号、密钥等属性。

说明

仅 RADIUS 协议的认证和授权是绑定在一起的，且不能使用 RADIUS 协议单独进行授权。

8.1.3 配置 AAA 方案

介绍 AC6605 上认证方案、授权方案和记录方案的配置方法。

建立配置任务

应用环境

AC6605 中的 AAA 方案包括认证方案、授权方案、计费方案、记录方案。AAA 方案规定了 AC6605 对用户进行认证、授权、计费、记录的模式（本地处理、远端处理或者不处理），以及相关的其他参数。

当配置了 AAA 方案后，可以在配置域时引用已配置的 AAA 方案，AC6605 根据 AAA 方案的配置对该域的用户进行认证、授权、计费。对于记录方案，可以在 AAA 视图下配置对不同事件所使用的记录方案。

前置任务

无

数据准备

在配置 AAA 之前，需要准备以下数据。

序号	数据
1	认证方案名称、认证模式
2	授权方案名称、授权模式、（可选）HWTACACS 按命令行授权的用户级别、（可选）命令行授权超时时间
3	计费方案名称、计费模式
4	（可选）记录方案名称、（可选）与记录方案关联的 HWTACACS 服务器模板的名称、（可选）记录策略，即对哪些事件进行记录

版权所有 © 华为技术有限公司

配置认证方案

背景信息

说明

缺省情况下，AC6605 对用户进行本地认证。

如果不对用户进行认证，必须创建一个认证方案或者修改“default”认证方案，在该方案下配置认证模式为无需认证，然后在用户相应的域下应用此认证方案。

用户登录 AC6605 的认证模式和用户级别提升的认证模式需要分别配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authentication-scheme** *authentication-scheme-name*，创建认证方案，并进入认证方案视图。

缺省情况下，AC6605 中有一个认证方案，认证方案名称是 default，不能删除，只能修改。

步骤 4 执行命令 **authentication-mode** { **hwtacacs** | **radius** | **local** }* [**none**]配置认证模式。

none 表示无需认证。缺省情况下，认证模式为本地认证。

如果在一个认证方案中使用多种认证模式，**none** 必须作为最后一种认证模式。

如果采用 RADIUS 或 HWTACACS 认证模式，必须配置 **RADIUS** 或 **HWTACACS** 服务器模板，然后在用户所属域的视图下应用该服务器模板。

说明

如果在一个认证方案中使用多种认证模式，则认证模式的执行顺序为配置的先后顺序。只有在当前认证模式没有响应的情况下，才会采用下一种认证模式；如果当前认证模式认证失败，则不会跳转到下一个认证方案进行认证。

步骤 5 执行命令 **authentication-super** { **hwtacacs** | **super** }* [**none**]或者 **authentication-super none** 配置用户级别提升认证方案。

none 表示无需认证，直接让用户更改用户级别。缺省情况下，用户级别提升时采用 **super** 即本地认证模式。

如果采用本地认证模式对用户级别提升进行认证，需要在系统视图下执行 **super password** 命令，配置用户级别提升时的密码。

----结束

配置授权方案

背景信息

只有在使用 HWTACACS 协议时，才可以配置用户按命令行授权功能。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authorization-scheme** *authorization-scheme-name*，创建授权方案，并进入授权方案视图。

缺省情况下，AC6605 有一个授权方案，授权方案配置名称是 default，不能删除，只能修改。

步骤 4 执行命令 **authorization-mode** [**hwtacacs**] { **if-authenticated** | **local** | **none** }，配置授权模式。

缺省情况下，授权模式为本地授权模式。

如果在一个授权方案中使用多种授权模式，**if-authenticated**、**none** 必须作为最后一种授权模式。

如果采用 HWTACACS 授权模式，必须**配置 HWTACACS 服务器模板**，然后在用户所属域的视图下应用该服务器模板。

说明

如果在一个授权方案中使用多种授权模式，则授权模式的执行顺序为配置的先后顺序。只有在当前授权模式没有响应的情况下，才会采用下一种授权模式；如果当前授权模式失败，则不会采用下一种授权模式进行授权。

步骤 5 （可选）执行命令 **authorization-cmd** *privilege-level* **hwtacacs** [**local**]，配置某级别的用户按命令行授权。

缺省情况下，0 ～ 15 级用户都没有配置按命令行授权。

如果使能按命令行授权功能，必须配置 HWTACACS 服务器模板，然后在用户所属域的视图下应用该服务器模板。

----结束

配置计费方案

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **accounting-scheme** *accounting-scheme-name*，创建计费方案，并进入计费方案视图。

缺省情况下，AC6605 中有一个计费方案，计费方案配置名称是 default，不能删除，只能修改。

步骤 4 执行命令 **accounting-mode** { **hwtacacs** | **radius** | **none** }，配置计费模式。

缺省情况下，计费方案采用不计费模式（none）。

如果采用 RADIUS 或 HWTACACS 计费模式，必须配置 **RADIUS** 或 **HWTACACS** 服务器模板，然后在用户所属域下应用该服务器模板。

版权所有 © 华为技术有限公司

步骤 5 执行命令 **accounting realtime** *interval*，使能实时计费并设置计费间隔。

缺省情况下，实时计费功能未使能。

实时计费的时间间隔应当根据网络情况来确定。间隔时间过小，会增大网络中的数据流量，同时使接收实时计费报文的设备负载加大。如果间隔过大，当计费服务器和 AC6605 发生通讯故障后，计费误差越大。

步骤 6 （可选）执行命令 **accounting start-fail** { **online** | **offline** }，配置远端计费开始失败策略。

在用户接入时，如果初始计费失败，就可以根据初始计费失败策略对用户进行相应的处理。

缺省情况下，如果初始计费失败，不允许用户上线。

步骤 7 （可选）执行命令 **accounting interim-fail** [**max-times** *times*] { **online** | **offline** }，配置远端实时计费失败策略。

用户上线后，如果出现实时计费失败的情况，可以根据实时计费失败策略对用户进行相应的处理。

缺省情况下，实时计费功能未使能。

----结束

（可选）配置记录方案

背景信息

配置记录方案可以帮助用户进行设备监控和故障处理。记录内容可以包括用户在 AC6605 上执行过的命令、连接信息、系统级事件。

说明

只有在使用 HWTACACS 协议时，才可以配置记录功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，创建 HWTACACS 模板。

步骤 3 执行命令 **aaa**，进入 AAA 视图。

步骤 4 执行命令 **recording-scheme** *recording-scheme-name*，创建记录方案，并进入记录方案视图。

缺省情况下，AC6605 中没有记录方案。

步骤 5 执行命令 **recording-mode hwtacacs** *template-name*，配置与记录方案相关联的 HWTACACS 服务器模板。

缺省情况下，记录方案不与 HWTACACS 服务器模板相关联。

步骤 6 执行命令 **quit**，退回至 AAA 视图。

步骤 7 执行命令 **cmd recording-scheme** *recording-scheme-name*，记录用户在 AC6605 上执行过的命令。

版权所有 © 华为技术有限公司

缺省情况下，不记录用户在 AC6605 上执行过的命令。

步骤 8 执行命令 **outbound recording-scheme** *recording-scheme-name*，记录连接信息。

缺省情况下，不记录连接信息。

步骤 9 执行命令 **system recording-scheme** *recording-scheme-name*，记录系统级事件。

缺省情况下，不记录系统级事件。

----结束

检查配置结果

前提条件

已完成 AAA 方案的配置。

操作步骤

- 使用命令 **display aaa configuration** 查看 AAA 的概要信息。
- 使用命令 **display authentication-scheme** [*authentication-scheme-name*]查看认证方案的配置信息。
- 使用命令 **display authorization-scheme** [*authorization-scheme-name*]查看授权方案的配置信息。
- 使用命令 **display accounting-scheme** [*accounting-scheme-name*]查看计费方案的配置信息。
- 使用命令 **display recording-scheme** [*recording-scheme-name*]查看记录方案的配置信息。
- 使用命令 **display access-user** [**domain** *domain-name* | **ip-address** *ip-address* [**vpn-instance** *instance-name*] | **mac-address** *mac-address* | **slot** *slot-id* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **user-id** *user-number*]查看所有在线用户的概要信息。

----结束

8.1.4 配置 RADIUS 服务器模板

介绍 AC6605 上 RADIUS 服务器模板的配置方法。

建立配置任务

应用环境

在采用远端认证、授权时需要配置服务器模板。用户可以根据需要选择服务器模板。如果认证方案采用 RADIUS 模式，则需要配置 RADIUS 模板。

说明

RADIUS 服务器模板的各项参数都有缺省配置，可以根据实际组网需求进行调整。只有当该 RADIUS 服务器模板没有被使用时，才能改变 RADIUS 配置。

版权所有 © 华为技术有限公司

前置任务

无

数据准备

在配置 RADIUS 服务器模板之前，需要准备以下数据。

序号	数据
1	RADIUS 认证服务器的 IP 地址
2	RADIUS 计费服务器的 IP 地址
3	（可选）RADIUS 共享密钥
4	（可选）RADIUS 用户名格式
5	（可选）RADIUS 流量单位
6	（可选）RADIUS 超时重传时间，超时重传次数
7	（可选）RADIUS 的 NAS 端口形式

创建 RADIUS 模板

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，创建 RADIUS 服务器模板，并进入 RADIUS 服务器模板视图。

----结束

配置 RADIUS 认证服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server authentication** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 主用认证服务器。

缺省情况下，RADIUS 主用认证服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 4 （可选）执行命令 **radius-server authentication** *ip-address port* [**source loopback** *interface-number*] **secondary**，配置 RADIUS 备份认证服务器。

版权所有 © 华为技术有限公司

缺省情况下，RADIUS 备用认证服务器的 IP 地址为 0.0.0.0，端口号为 0。

----结束

配置 RADIUS 计费服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server accounting** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 主用计费服务器。

缺省情况下，RADIUS 主用计费服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 4 （可选）执行命令 **radius-server accounting** *ip-address port* [**source loopback** *interface-number*] **secondary**，配置 RADIUS 备份计费服务器。

缺省情况下，RADIUS 备份计费服务器的 IP 地址为 0.0.0.0，端口号为 0。

----结束

配置 RADIUS 授权服务器

背景信息

RADIUS 授权服务器主要用于用户进行动态业务选择时的业务授权。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server authorization** *ip-address* { **server-group** *group-name* | **shared-key** { **cipher** | **simple** } *key-string* } * [**ack-reserved-interval** *interval*]，配置 RADIUS 授权服务器。

缺省情况下，AC6605 中未配置 RADIUS 授权服务器。

----结束

（可选）配置 RADIUS 密钥

背景信息

AC6605 和 RADIUS 服务器在发送认证报文时，对口令等重要信息使用 MD5 加密，确保认证信息在网络中传输的安全性。为了确保认证双方身份的合法性，要求 AC6605 上的密钥与 RADIUS 服务器的密钥必须相同。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server shared-key** [**cipher** | **simple**] *key-string*，配置 RADIUS 密钥。

缺省情况下，RADIUS 共享密钥是 huawei。

----结束

（可选）配置 RADIUS 用户名格式

背景信息

说明

用户名通常采用“纯用户名@域名”格式，@后面的部分为域名。这里@表示域名分隔符，域名分隔符也可以是 \ / : < > | ' % 中的一种。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server user-name domain-included**，配置 RADIUS 用户名格式。

缺省情况下，RADIUS 用户名中包含域名，即 AC6605 会把用户名和域名及域名分割符一起发送给 RADIUS 服务器进行认证。

如果 RADIUS 服务器不接受带域名的用户名，可以执行命令 **undo radius-server user-name domain-included** 将用户名中的域名去掉，再发送给 RADIUS 服务器。

----结束

（可选）配置 RADIUS 流量单位

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }，配置 RADIUS 流量单位。

缺省情况下，AC6605 以字节（byte）作为 RADIUS 流量单位。

----结束

（可选）配置 RADIUS 重传参数

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server timeout** *timeout*，配置 RADIUS 服务器的应答超时时间。

缺省情况下，RADIUS 服务器的应答超时时间为 5 秒。

为判断某个 RADIUS 服务器是否失效，AC6605 会向 RADIUS 服务器周期性地发送请求报文，如果在超时重传时间内未得到 RADIUS 服务器的应答，需重传请求报文。

步骤 4 执行命令 **radius-server retransmit** *retry-times*，配置 RADIUS 服务器超时重传次数。

缺省情况下，超时重传次数为 3。

AC6605 向 RADIUS 服务器重传请求报文的次数超出超时重传次数后，AC6605 认为该 RADIUS 服务器已不可用。

----结束

（可选）配置 RADIUS 的 NAS 端口

背景信息

NAS 端口形式和 NAS 端口 ID 形式都属于华为公司内部扩展的属性，用于华为公司设备之间的互通和业务配合。NAS 端口和 NAS 端口 ID 都有新、旧两种形式，配置不同的形式，接入用户所在的物理端口形式不一样。

对于以太网接入用户:

- NAS 端口
  - 选择新形式，端口形式为：槽位号（8 位）＋子槽位号（4 位）＋端口号（8 位）＋ VLAN ID（12 位）。
  - 选择旧形式，端口形式为：槽位号（12 位）＋端口号（8 位）＋ VLAN ID（12 位）。
- NAS 端口 ID
  - 选择新形式，NAS 端口 ID 形式为：“slot ＝ XX；subslot ＝ XX；port ＝ XXX；VLANID ＝ XXXX；”，其中，Slot 取值范围是 0 ～ 15，Subslot 取值范围是 0 ～ 15，Port 取值范围是 0 ～ 255，VLANID 取值范围是 1 ～ 4094。
  - 选择旧形式，NAS 端口 ID 形式为：端口号（两个字符）＋子槽号（两个字节）＋卡号（三个字节）＋ VLANID（9 个字符）

对于 ADSL 接入用户:

- NAS 端口形式都是：槽位号（4 位）＋子槽位号（2 位）＋端口号（2 位）＋ VPI（8 位）＋ VCI（16 位）。
- NAS 端口 ID
  - 选择新形式，NAS 端口 ID 形式为“slot ＝ XX；subslot ＝ X；port ＝ X；VPI ＝ XXX；VCI ＝ XXXXX；”其中，Slot 取值范围是 0 ～ 15，Subslot 取值范围是 0 ～ 9，Port 取值范围是 0 ～ 9，VPI 取值范围是 0 ～ 255，VCI 取值范围是 0 ～ 65535。

版权所有 © 华为技术有限公司

- 选择旧形式，NAS 端口 ID 形式为：端口号（两个字符）＋子槽号（两个字节）＋卡号（三个字节）＋ VPI（8 个字符）＋ VCI（16 个字符），字节数不够的，在前面补零。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server nas-port-format** { **new** | **old** }，配置 RADIUS 服务器的 NAS 端口形式。

缺省情况下，采用新的 NAS 端口形式（**new**）。

步骤 4 执行命令 **radius-server nas-port-id-format** { **new** | **old** }，配置 RADIUS 服务器的 NAS 端口 ID 形式。

缺省情况下，采用新的 NAS 端口 ID 形式（**new**）。

----结束

（可选）配置 RADIUS 报文中 MAC 地址的封装格式

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **calling-station-id mac-format** { **dot-split** | **hyphen-split** } [**mode1** | **mode2**] [**lowercase** | **uppercase**] *timeout*，或者 **calling-station-id mac-format unformatted** [**lowercase** | **uppercase**]命令配置 RADIUS 报文中 calling-station-id（Type 31）属性字段中 MAC 地址的封装格式。

缺省情况下，calling-station-id 属性字段中 MAC 地址的格式为 xxxx-xxxx-xxxx，小写形式。

----结束

检查配置结果

前提条件

已完成 RADIUS 服务器模板的配置。

操作步骤

- 使用命令 **display radius-server configuration** [**template** *template-name*]查看 RADIUS 服务器模板的配置信息。
- 使用命令 **display radius-attribute** [**template** *template-name*] **disable** 查看设备禁用的 RADIUS 属性。

版权所有 © 华为技术有限公司

- 使用命令 **display radius-attribute** [**template** *template-name*] **translate** 查看 RADIUS 属性转换的配置信息。

----结束

任务示例

配置完 RADIUS 服务器模板后，执行命令 **display radius-server configuration** 可以查看所有模板的配置信息。

```
<Quidway> display radius-server configuration
------------------------------------------------------------------

  Server-template-name             :  rrr
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  huawei
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  0.0.0.0;    0;  LoopBack:NULL
  Primary-accounting-server        :  100.1.1.1;    90;  LoopBack:20
  Secondary-authentication-server  :  0.0.0.0;    0;  LoopBack:NULL
  Secondary-accounting-server      :  0.0.0.0;    0;  LoopBack:NULL
  Retransmission                   :  3
  Domain-included                  :  YES
  Calling-station-id MAC-format    :  xxxx-xxxx-xxxx
  ------------------------------------------------------------------
  ------------------------------------------------------------------

  Server-template-name             :  trl
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  huawei
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  0.0.0.0;    0;  LoopBack:NULL
  Primary-accounting-server        :  0.0.0.0;    0;  LoopBack:NULL
  Secondary-authentication-server  :  0.0.0.0;    0;  LoopBack:NULL
  Secondary-accounting-server      :  0.0.0.0;    0;  LoopBack:NULL
  Retransmission                   :  3
  Domain-included                  :  YES
  Calling-station-id MAC-format    :  XX.XX.XX.XX.XX.XX
  ------------------------------------------------------------------
  Total of radius template :2
```

执行命令 **display radius-attribute** [**template** *template-name*] **disable** 查看设备禁用的 RADIUS 属性。

```
<Quidway> display radius-attribute disable
Server-templet-name: rs
-------------------------------------------------------------------------------
Source-attr                                 Dest-attr          Direct
-------------------------------------------------------------------------------
NAS-IP-Address                              Disable            send
-------------------------------------------------------------------------------
```

执行命令 **display radius-attribute** [**template** *template-name*] **translate** 查看 RADIUS 属性转换的配置信息。

```
<Quidway> display radius-attribute translate
Server-templet-name: rs
-------------------------------------------------------------------------------
Source-attr                                 Dest-attr          Direct
-------------------------------------------------------------------------------
NAS-Identifier                              NAS-Port-Id        send
-------------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

8.1.5 配置 HWTACACS 服务器模板

介绍 AC6605 上 HWTACACS 服务器模板的配置方法。

建立配置任务

应用环境

在采用远端认证、授权时需要配置服务器模板。用户可以根据需要选择服务器模板。如果认证方案或授权方式采用 HWTACACS 模式，则需要配置 HWTACACS 模板。

说明

除删除服务器外，HWTACACS 的大部分属性在改变配置时都不检查当前是否有用户在使用此模板。

前置任务

无

数据准备

在配置 HWTACACS 服务器模板之前，需要准备以下数据。

序号	数据
1	HWTACACS 模板名称
2	HWTACACS 认证服务器、授权服务器、计费服务器 IP 地址
3	（可选）HWTACACS 源 IP 地址
4	（可选）HWTACACS 共享密钥
5	（可选）HWTACACS 用户名格式
6	（可选）HWTACACS 流量单位
7	（可选）HWTACACS 应答超时时间、主用服务器恢复激活时间

创建 HWTACACS 模板

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，创建 HWTACACS 服务器模板，并进入 HWTACACS 服务器模板视图。

----结束

版权所有 © 华为技术有限公司

配置 HWTACACS 认证服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主用认证服务器 IP 地址。

缺省情况下，HWTACACS 主用认证服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 4 （可选）执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备用认证服务器 IP 地址。

缺省情况下，HWTACACS 备用认证服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

----结束

配置 HWTACACS 授权服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主用授权服务器 IP 地址。

缺省情况下，HWTACACS 主用授权服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 4 （可选）执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备用授权服务器 IP 地址。

缺省情况下，HWTACACS 备用授权服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

----结束

配置 HWTACACS 计费服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 主用计费服务器。

版权所有 © 华为技术有限公司

缺省情况下，HWTACACS 主用计费服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 4 （可选）执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 备用计费服务器。

缺省情况下，HWTACACS 备用计费服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

----结束

（可选）配置 HWTACACS 的源 IP 地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server source-ip** *ip-address*，配置 HWTACACS 的源 IP 地址。

缺省情况下，HWTACACS 的源 IP 地址是 0.0.0.0，此时 AC6605 使用实际出方向的 VLANIF 接口的 IP 地址作为 HWTACACS 报文的源 IP 地址。

指定 HWTACACS 的源 IP 地址后，使用该 HWTACACS 模板与服务器通信时，报文的源 IP 地址为指定的 IP 地址。此时，服务器也将使用指定的 IP 地址与 AC6605 通信。

----结束

（可选）配置 HWTACACS 密钥

背景信息

设置密钥可以提高 AC6605 与 HWTACACS 服务器通信的安全性。为了确保认证双方的身份合法性，要求 AC6605 上的密钥与 HWTACACS 服务器的密钥必须相同。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server shared-key** [**cipher** | **simple**] *key-string*，配置 HWTACACS 的密钥。

缺省情况下，无密钥。

----结束

（可选）配置 HWTACACS 用户名格式

版权所有 © 华为技术有限公司

背景信息

说明

用户名通常采用“纯用户名@域名”格式，@后面的部分为域名。这里@表示域名分隔符，域名分隔符也可以是 \ / : < > | ' % 中的一种。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server user-name domain-included**，配置 HWTACACS 用户名格式。

缺省情况下，HWTACACS 用户名中包含域名，即 AC6605 会把用户名和域名及域名分割符一起发送给 HWTACACS 服务器进行认证。

如果 HWTACACS 服务器不接受带域名的用户名，可以执行命令 **undo hwtacacs-server user-name domain-included** 将用户名中的域名去掉，再发送给 HWTACACS 服务器。

----结束

（可选）配置 HWTACACS 流量单位

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }，配置 HWTACACS 流量单位。

缺省情况下，AC6605 使用字节（byte）作为 HWTACACS 流量单位。

----结束

（可选）配置 HWTACACS 定时器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 3 执行命令 **hwtacacs-server timer response-timeout** *value*，配置 HWTACACS 服务器应答超时时间。

缺省情况下，HWTACACS 应答超时时间为 5 秒。

如果 AC6605 在应答超时时间内没有收到 HWTACACS 服务器的回复，则认为服务器不可用。此时 AC6605 将尝试使用其他方式进行认证、授权。

步骤 4 执行命令 **hwtacacs-server timer quiet** *value*，配置 HWTACACS 主服务器恢复激活时间。

版权所有 © 华为技术有限公司

缺省情况下，主用服务器恢复激活状态前需要等待 5 分钟。

----结束

（可选）配置计费结束报文的重传功能

背景信息

使用 HWTACACS 计费模式时，用户下线后，AC6605 会生成计费结束报文传送给 HWTACACS 服务器。如果网络状况不是非常理想，可以配置计费结束报文的重传功能，以保证计费信息不会丢失。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server accounting-stop-packet resend** { **disable** | **enable** *number* }，配置计费结束报文的重传功能。

可以配置是否启用计费结束报文的重传功能以及报文的重传次数。缺省情况下，AC6605 启用计费结束报文的重传功能，报文的重传次数为 100。

----结束

检查配置结果

前提条件

已完成 HWTACACS 服务器模板的配置。

操作步骤

- 使用命令 **display hwtacacs-server template** [*template-name*]查看 HWTACACS 服务器模板的配置信息。

----结束

任务示例

配置完 HWTACACS 服务器模板后，执行命令 **display hwtacacs-server template** [*template-name*]可以查看模板的配置信息。

```
<Quidway> display hwtacacs-server template huawei
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : huawei
  Primary-authentication-server   : 0.0.0.0:0:-
  Primary-authorization-server    : 0.0.0.0:0:-
  Primary-accounting-server       : 0.0.0.0:0:-
  Secondary-authentication-server : 0.0.0.0:0:-
  Secondary-authorization-server  : 0.0.0.0:0:-
  Secondary-accounting-server     : 0.0.0.0:0:-
  Current-authentication-server   : 0.0.0.0:0:-
  Current-authorization-server    : 0.0.0.0:0:-
  Current-accounting-server       : 0.0.0.0:0:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : -
  Quiet-interval(min)             : 5
```


版权所有 © 华为技术有限公司

```
Response-timeout-Interval(sec)  : 5
Domain-included                 : Yes
Traffic-unit                    : B
------------------------------------------------------------------------------
```

8.1.6 配置业务方案

在 AC6605 上配置业务方案，存放用户的授权信息。

建立配置任务

应用环境

接入用户需要获取授权信息才能上线，可以通过配置业务方案管理用户的授权信息。

前置任务

在配置业务方案之前，需要完成以下任务：

- 创建 DHCP 服务器组
- 创建 IP 地址池

数据准备

在配置业务方案之前，需要准备以下数据。

序号	数据
1	业务方案名称
2	管理员用户级别
3	用户优先级
4	DHCP 服务器组名
5	地址池名、地址池位置信息
6	DNS 主备服务器地址

创建业务方案

背景信息

业务方案是用户授权信息的集合，创建业务方案后，可以在业务方案视图下配置用户的各项属性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **service-scheme** *service-scheme-name*，创建一个业务方案。

业务方案名 *service-scheme-name* 为字符串形式，长度范围是 1 ～ 32，且不能包括/ \ : * ? " < > | @ ' %字符。

缺省情况下，AC6605 中没有创建业务方案。

----结束

配置管理员用户级别

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **service-scheme** *service-scheme-name*，进入业务方案视图。

步骤 4 执行命令 **admin-user privilege level** *level*，配置用户可以作为管理员登录 AC6605，同时指定登录时的管理员级别。

level 参数的取值范围是 0 ～ 15。如果没有配置这条命令，则显示为 16，表示是一个无效值。

----结束

配置 DNS 主备服务器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **service-scheme** *service-scheme-name*，进入业务方案视图。

步骤 4 执行命令 **dns** *ip-address*，配置 DNS 主用服务器地址。

步骤 5 （可选）执行命令 **dns** *ip-address* **secondary**，配置 DNS 备用服务器地址。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display service-scheme** [**name** *name*]查看业务方案配置信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display service-scheme** 可以查看所有业务方案信息。

```
<Quidway> display service-scheme
  ------------------------------------------------------------------
  service-scheme-name                   scheme-index
  ------------------------------------------------------------------
  huwei1                                0
  ------------------------------------------------------------------
  Total of service scheme: 1
```

执行命令 **display service-scheme name** *name* 可以查看名为 svcscheme1 的业务方案配置信息。

```
<Quidway> display service-scheme name svcscheme1

  service-scheme-name          : svcscheme1
  service-scheme-primary-dns   : -
  service-scheme-secondry-dns  : -
  service-scheme-adminlevel    : 16
```

8.1.7 配置域

介绍 AC6605 上域的配置方法。

建立配置任务

应用环境

对登录 AC6605 的用户进行认证、授权管理时需要配置域。

说明

修改域的配置，将在用户下一次登录时生效。

前置任务

在配置域之前，需要完成以下任务：

- 配置认证方案和授权方案。
- 如果认证方案采用 RADIUS 模式，需要配置 RADIUS 模板。
- 如果认证方案或授权方案采用 HWTACACS 模式，需要配置 HWTACACS 模板。
- 如果认证方案或授权方案采用本地模式，需要配置本地用户管理。

数据准备

在配置域之前，需要准备以下数据。

序号	数据
1	域的名称
2	域的认证方案、授权方案名称

版权所有 © 华为技术有限公司

序号	数据
3	（可选）域的 RADIUS 模板或 HWTACACS 模板名称
4	（可选）域的状态

创建域

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域，并进入域视图。

缺省情况下，AC6605 中存在两个域：“default”和“default_admin”。“default”用于普通接入用户的域，“default_admin”用于管理员的域。

AC6605 一共可以配置 32 个域，包括缺省的两个域。

----结束

后续处理

创建域以后，可以在系统视图下执行命令 **domain** *domain-name* [**admin**]，配置全局默认域，以管理无法确认所属域名的接入用户。

如果不执行该命令，则当接入 AC6605 的用户不带域名时，使用缺省的“default”和“default_admin”域分别管理普通接入用户和管理员用户。

配置域的认证方案、授权方案和计费方案

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域的认证方案。

缺省情况下，域使用配置名为 default 的认证方案。

步骤 5 执行命令 **authorization-scheme** *authorization-scheme-name*，配置域的授权方案。

缺省情况下，域下没有绑定授权方案。

步骤 6 执行命令 **accounting-scheme** *accounting-scheme-name*，配置域的计费方案。

版权所有 © 华为技术有限公司

缺省情况下，域使用配置名为 default 的计费方案。

----结束

配置域的 RAIDUS 服务器模板

背景信息

如果域采用的认证方案为 RADIUS 远端认证，需要配置域的 RADIUS 模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入用户域视图。

步骤 4 执行命令 **radius-server** *template-name*，配置域的 RADIUS 模板。

缺省情况下，域下没有配置 RADIUS 模板。

----结束

配置域的 HWTACACS 服务器模板

背景信息

如果域采用的认证方案或授权方案为 HWTACACS 远端认证或授权，需要配置域的 HWTACACS 模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入用户域视图。

步骤 4 执行命令 **hwtacacs-server** *template-name*，配置域的 HWTACACS 模板。

缺省情况下，域下没有配置 HWTACACS 模板。

----结束

（可选）配置域的业务方案

背景信息

配置域的业务方案，即在域下绑定一个业务方案，该域下的用户从此业务方案里获取相应的业务信息，如 IP 地址、DNS 服务器等。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **service-scheme** *service-scheme-name*，配置域的业务方案。

缺省情况下，域下没有绑定任何业务方案。

配置域的业务方案前，业务方案必须已经创建完成。

----结束

（可选）配置域的状态

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入用户域视图。

步骤 4 执行命令 **state** { **active** | **block** }，配置域的状态。

当域处于阻塞态时，属于该域的用户不能登录。缺省情况下，域创建后处于激活状态。

----结束

（可选）配置域名分隔符

背景信息

AC6605 中用户名包含纯用户名与域名，纯用户名与域名之间由域名分隔符分隔。比如，如果定义域名分隔符为@，则 dom1 域的 user1 用户名表达为 user1@dom1。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain-name-delimiter** *delimiter*，配置域名分隔符。

域名分隔符可以是 \ / : < > | @ ' % 中的某一个。

缺省情况下，域名分隔符为@。

----结束

检查配置结果

版权所有 © 华为技术有限公司

前提条件

已完成域的配置。

操作步骤

- 使用命令 **display domain** [**name** *domain-name*]查看域的配置信息。

----结束

任务示例

配置完成后，执行命令 **display domain**，可以查看所有域的简要信息。

```
<Quidway> display domain
  ------------------------------------------------------------------------------
  DomainName                      index
  ------------------------------------------------------------------------------
  default                         0
  default_admin                   1
  huawei                          2
  ------------------------------------------------------------------------------

  Total: 3
```

执行命令 **display domain name** *domain-name*，可以查看指定域的配置信息。

```
<Quidway> display domain name huawei
  Domain-name                   : huawei
  Domain-state                  : Active
  Authentication-scheme-name    : scheme0
  Accounting-scheme-name        : default
  Authorization-scheme-name     : -
  Service-scheme-name           : -
  RADIUS-server-template        : -
  HWTACACS-server-template      : -
```

8.1.8 配置本地用户管理

介绍 AC6605 上本地用户的配置方法。

建立配置任务

应用环境

可以在 AC6605 上创建本地用户帐号，并配置本地用户的相关属性，根据本地用户信息，对登录 AC6605 的用户进行认证、授权。

前置任务

无

数据准备

在配置本地用户管理之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	用户名、用户口令
2	本地用户的接入类型
3	本地用户的 FTP 目录名
4	本地用户的状态
5	本地用户的优先级别
6	本地用户的接入限制数量

创建本地用户帐号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* { **password** { **simple** | **cipher** } *password* | **access-limit** *max-number* | **ftp-directory** *directory* | **privilege level** *level* | **state** { **block** | **active** } } *，创建本地用户帐号，并配置本地用户的各项参数。

如果用户名中带域名分割符（如“@”、“|”、“%”等符号），则认为分割符前面的部分是用户名，后面部分是域名。如果没有分割符，则整个字符串为用户名，默认到 **default** 域认证。

local-user 命令不仅可以创建本地用户，而且可以配置本地用户的各项参数。如果用户使用 **local-user** 命令配置本地用户的各项参数之后需要修改配置，可以使用 **local-user access-limit** 命令、**local-user ftp-directory** 命令、**local-user service-type** 命令、**local-user privilege level** 命令或 **local-user state** 命令单独配置各项参数。

----结束

（可选）配置本地用户的接入类型

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **service-type** { **8021x** | **bind** | **ftp** | **http** | **ppp** | **ssh** | **telnet** | **terminal** | **web** | **x25-pad** } *，配置本地用户的接入类型。

缺省情况下，本地用户可以使用所有的接入类型。

对用户配置接入类型后，只有用户的实际接入方式匹配该用户的接入类型，用户才能登录。

----结束

版权所有 © 华为技术有限公司

（可选）配置本地用户的 FTP 目录

背景信息

说明

若本地用户以 FTP 方式接入，则必须配置这个用户的 FTP 目录，否则该用户无法登录。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置本地用户的 FTP 目录权限。

缺省情况下，本地用户的 FTP 目录为空。

----结束

（可选）配置本地用户的状态

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **state** { **active** | **block** }，配置本地用户的状态。

缺省情况下，本地用户的状态为激活态。

AC6605 对处于激活态和阻塞态用户的处理方式如下：

- 若用户状态为激活态，将接收该用户的认证请求并做进一步处理。
- 若用户状态为阻塞态，将拒绝该用户的认证请求。

----结束

（可选）配置本地用户的优先级

背景信息

通过配置用户的优先级，用户成功登录后，只有用户的优先级等于或者高于命令的级别，用户才能使用该命令。

与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越大则优先级越高。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **privilege level** *level*，配置本地用户的优先级。

缺省情况下，本地用户的优先级由管理模块来决定，例如在用户界面视图下有用户级别的配置，如果没有配置，则为 0 级用户。

----结束

（可选）配置本地用户的接入限制

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **access-limit** *max-number*，配置本地用户的接入限制。

缺省情况下，不限制指定用户名在 AC6605 上的接入数目。

----结束

检查配置结果

前提条件

已完成本地用户的配置。

操作步骤

- 使用命令 **display local-user** [**username** *user-name*]，查看本地用户的属性。

----结束

任务示例

完成本地用户管理的配置后，执行命令 **display local-user** 可以查看本地用户简要属性。

```
<Quidway> display local-user
  ------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  lsj                            A      A         -
  ------------------------------------------------------------------------------
  Total 1 user(s)
```

执行命令 **display local-user** [**username** *user-name*]，可以查看指定用户的详细信息。

```
<Quidway> display local-user username user-a
  The contents of local user(s):
  Password         : admin
  State            : active
  Service-type-mask : H
  Privilege level   : -
  Ftp-directory     : -
  Access-limit      : -
  Accessed-num      : 0
```


版权所有 © 华为技术有限公司

8.1.9 维护 AAA 及用户管理

清除 HWTACACS 统计信息，调试 RADIUS 或者 HWTACACS。

清除统计信息

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除统计信息后,请在用户视图下执行以下命令。

操作步骤

- 使用 **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** }命令清除 HWTACACS 的统计信息。
- 使用 **reset hwtacacs-server accounting-stop-packet** { **all** | **ip** *ip-address* }命令清除计费停止报文的统计信息。

----结束

监控 AAA 运行状况

操作步骤

步骤 1 使用命令 **display aaa configuration** 查看 AAA 运行信息。

----结束

任务示例

执行命令 **display aaa configuration** 可以查看 AAA 的运行信息。

```
<Quidway> display aaa configuration

  Domain Name Delimiter           : @
  Domainname parse direction      : Left to right
  Domainname location             : After-delimiter
  Domain                          : total: 32     used: 5
  Authentication-scheme           : total: 16     used: 1
  Accounting-scheme               : total: 16     used: 3
  Authorization-scheme            : total: 16     used: 1
  Service-scheme                  : total: 16     used: 0
```

调试

版权所有 © 华为技术有限公司

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 RADIUS 或者 HWTACACS 运行故障时，请在用户视图下执行以下 **debugging** 命令对其进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

- 使用 **debugging radius packet** 命令打开 RADIUS 的报文调试信息开关。
- 使用 **debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }打开 HWTACACS 的调试信息开关。

----结束

8.1.10 配置举例

介绍 AAA 及用户管理的举例。

配置采用 RADIUS 协议进行认证、计费示例

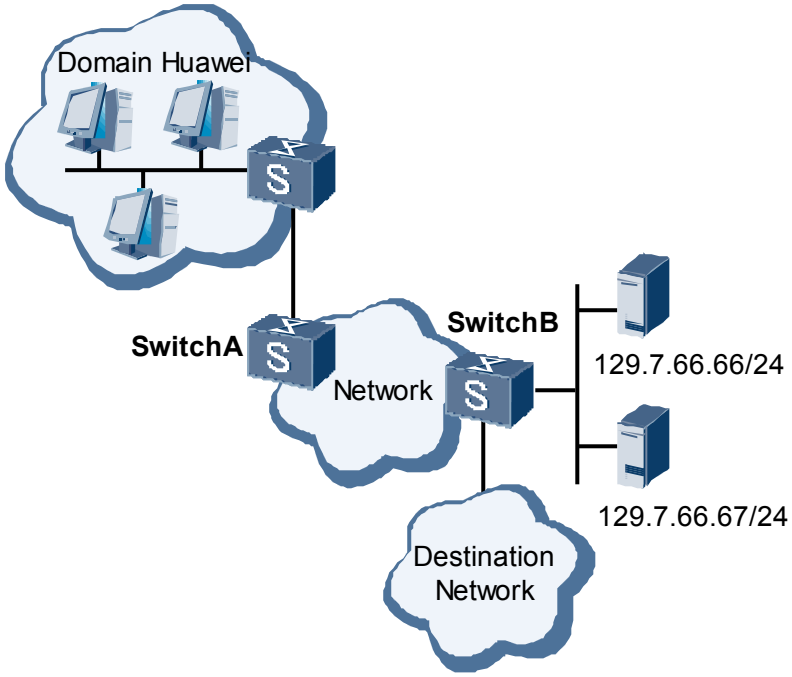
组网需求

如图 8-1 所示，用户通过 SwitchA 访问网络，用户同处于 huawei 域。SwitchB 作为目的网络的网络接入服务器。用户首先需要穿越 SwitchA 和 SwitchB 所在的网络，然后通过服务器的远端认证才能通过 SwitchB 访问目的网络。在 SwitchB 上的远端认证方式如下：

- 用 RADIUS 服务器对接入用户进行认证、计费。
- RADIUS 服务器 129.7.66.66/24 作为主用认证服务器和计费服务器，RADIUS 服务器 129.7.66.67/24 作为备用认证服务器和计费服务器，认证端口号缺省为 1812，计费端口号缺省为 1813。

版权所有 © 华为技术有限公司

图 8-1 采用 RADIUS 协议对用户进行认证和计费组网图



配置思路

用如下的思路配置采用 RADIUS 协议对用户进行认证和计费。

1. 配置 RADIUS 服务器模板。
2. 配置认证方案、计费方案
3. 在域下应用 RADIUS 服务器模板、认证方案和计费方案。

数据准备

为完成此配置举例，需要准备如下数据：

- 用户所属的域名
- RADIUS 服务器模板名
- 认证方案名、认证模式、计费方案名、计费模式
- 主用和备用 RADIUS 服务器的 IP 地址、认证端口号、计费端口号
- RADIUS 服务器密钥和重传次数

说明

以下配置均在 SwitchB 上进行。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 shiva。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] radius-server template shiva
```

配置 RADIUS 主用认证服务器和计费服务器的 IP 地址、端口。

```
[Quidway-radius-shiva] radius-server authentication 129.7.66.66 1812
[Quidway-radius-shiva] radius-server accounting 129.7.66.66 1813
```

配置 RADIUS 备用认证服务器和计费服务器的 IP 地址、端口。

```
[Quidway-radius-shiva] radius-server authentication 129.7.66.67 1812 secondary
[Quidway-radius-shiva] radius-server accounting 129.7.66.67 1813 secondary
```

配置 RADIUS 服务器密钥、重传次数。

```
[Quidway-radius-shiva] radius-server shared-key cipher hello
[Quidway-radius-shiva] radius-server retransmit 2
[Quidway-radius-shiva] quit
```

步骤 2 配置认证方案、计费方案

配置认证方案 1，认证模式为 RADIUS。

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme 1
Info: Create a new authentication scheme
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

配置计费方案 1，计费模式为 RADIUS。

```
[Quidway-aaa] accounting-scheme 1
Info: Create a new accounting scheme
[Quidway-aaa-accounting-1] accounting-mode radius
[Quidway-aaa-accounting-1] quit
```

步骤 3 配置 huawei 域，在域下应用认证方案 1、计费方案 1、RADIUS 模板 shiva

```
[Quidway-aaa] domain huawei
[Quidway-aaa-domain-huawei] authentication-scheme 1
[Quidway-aaa-domain-huawei] accounting-scheme 1
[Quidway-aaa-domain-huawei] radius-server shiva
```

步骤 4 检查配置结果

在 SwitchB 上执行命令 **display radius-server configuration template**，可以观察到该 RADIUS 服务器模板的配置与要求一致。

```
<Quidway> display radius-server configuration template shiva
 ------------------------------------------------------------------------
  Server-template-name             :  shiva
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  3MQ*TZ,O3KCQ=^Q`MAF4<1!!
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  129.7.66.66    :1812   LoopBack:NULL
  Primary-accounting-server        :  129.7.66.66    :1813   LoopBack:NULL
  Secondary-authentication-server  :  129.7.66.67    :1812   LoopBack:NULL
  Secondary-accounting-server      :  129.7.66.67    :1813   LoopBack:NULL
  Retransmission                   :  2
  Domain-included                  :  YES
  Calling-station-id MAC-format    :  XX.XX.XX.XX.XX.XX
 ------------------------------------------------------------------------
```

----结束

配置文件

```
#
```


版权所有 © 华为技术有限公司

```
sysname Quidway
#
radius-server template shiva
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 129.7.66.66 1812
 radius-server authentication 129.7.66.67 1812 secondary
 radius-server accounting 129.7.66.66 1813
 radius-server accounting 129.7.66.67 1813 secondary
 radius-server retransmit 2
#
aaa
 authentication-scheme default
 authentication-scheme 1
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 accounting-scheme 1
  accounting-mode radius
 domain default
 domain default_admin
 domain huawei
  authentication-scheme 1
  accounting-scheme 1
  radius-server shiva
#
return
```

配置采用 HWTACACS 协议进行认证、计费和授权示例

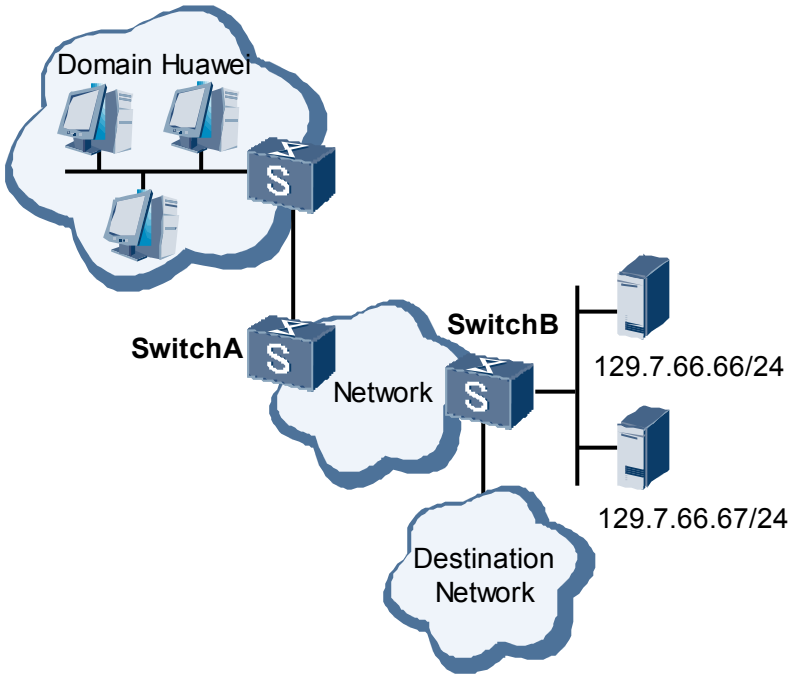
组网需求

如图 8-2 所示，

- 对接入用户先用 HWTACACS 服务器进行认证，如果认证没有响应，再使用本地认证。
- 接入的用户进行用户等级提升时，要求先使用 HWTACACS 对其进行认证，如果 HWTACACS 认证没有响应，再使用本地认证。
- 对接入用户采用 HWTACACS 授权。
- 对所有用户都需要计费。
- 对用户进行实时计费，计费间隔为 3 分钟。
- 记录用户执行过的命令、连接信息、系统级事件。
- HWTACACS 主用服务器为 129.7.66.66/24，备用服务器为 129.7.66.67/24，服务器的认证、授权和计费端口号均为 49。

版权所有 © 华为技术有限公司

图 8-2 采用 HWTACACS 协议对用户进行认证、计费和授权组网图



配置思路

采用如下的思路配置对用户使用本地和 HWTACACS 认证、HWTACACS 授权和进行实时计费。

1. 配置 HWTACACS 服务器模板。
2. 配置认证方案、授权方案、计费方案、记录方案。
3. 在域下应用 HWTACACS 服务器模板、认证方案、授权方案、计费方案。

数据准备

为完成此配置举例，需要准备如下数据：

- 用户所属的域名
- HWTACACS 服务器模板名
- 认证方案名、认证模式、授权方案名、授权模式、计费方案名、计费模式、记录方案名
- 主用和备用 HWTACACS 服务器的 IP 地址、认证端口号、授权端口号、计费端口号
- HWTACACS 服务器密钥

说明

以下配置均在 SwitchB 上进行。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 HWTACACS 服务器模板

配置 HWTACACS 服务器模板 ht。

```
<Quidway> system-view
[Quidway] hwtacacs-server template ht
```

配置 HWTACACS 主用认证、授权、计费服务器的 IP 地址和端口。

```
[Quidway-hwtacacs-ht] hwtacacs-server authentication 129.7.66.66 49
[Quidway-hwtacacs-ht] hwtacacs-server authorization 129.7.66.66 49
[Quidway-hwtacacs-ht] hwtacacs-server accounting 129.7.66.66 49
```

配置 HWTACACS 备用认证、授权、计费服务器的 IP 地址和端口。

```
[Quidway-hwtacacs-ht] hwtacacs-server authentication 129.7.66.67 49 secondary
[Quidway-hwtacacs-ht] hwtacacs-server authorization 129.7.66.67 49 secondary
[Quidway-hwtacacs-ht] hwtacacs-server accounting 129.7.66.67 49 secondary
```

配置 TACACS 服务器密钥。

```
[Quidway-hwtacacs-ht] hwtacacs-server shared-key cipher hello
[Quidway-hwtacacs-ht] quit
```

步骤 2 配置认证方案、授权方案、计费方案、记录方案

配置认证方案 l-h，认证方法为先进行本地认证，后进行 HWTACACS 认证。用户级别提升方为先进行 HWTACACS 认证，后进行本地认证。

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme l-h
[Quidway-aaa-authen-l-h] authentication-mode hwtacacs local
[Quidway-aaa-authen-l-h] authentication-super hwtacacs super
[Quidway-aaa-authen-l-h] quit
```

配置授权方案 hwtacacs，授权方法为 HWTACACS。

```
[Quidway-aaa] authorization-scheme hwtacacs
[Quidway-aaa-author-hwtacacs] authorization-mode hwtacacs
[Quidway-aaa-author-hwtacacs] quit
```

配置计费方案 hwtacacs，计费方法为 HWTACACS。

```
[Quidway-aaa] accounting-scheme hwtacacs
[Quidway-aaa-accounting-hwtacacs] accounting-mode hwtacacs
[Quidway-aaa-accounting-hwtacacs] accounting start-fail online
```

配置实时计费间隔为 3 分钟。

```
[Quidway-aaa-accounting-hwtacacs] accounting realtime 3
[Quidway-aaa-accounting-hwtacacs] quit
```

配置记录方案 scheme0，并与 HWTACACS 服务器模板 ht 相关联。

```
[Quidway-aaa] recording-scheme scheme0
[Quidway-aaa-recording-scheme0] recording-mode hwtacacs ht
[Quidway-aaa-recording-scheme0] quit
```

配置记录方案 scheme0 的记录策略为记录用户在 SwitchB 上执行过的命令、记录连接信息以及记录系统级事件。

```
[Quidway-aaa] cmd recording-scheme scheme0
[Quidway-aaa] outbound recording-scheme scheme0
[Quidway-aaa] system recording-scheme scheme0
```

步骤 3 配置 huawei 域，在域下采用 l-h 认证方案、HWTACACS 授权方案、HWTACACS 计费方案、ht 的 HWTACACS 模板

版权所有 © 华为技术有限公司

```
[Quidway-aaa] domain huawei
[Quidway-aaa-domain-huawei] authentication-scheme l-h
[Quidway-aaa-domain-huawei] authorization-scheme hwtacacs
[Quidway-aaa-domain-huawei] accounting-scheme hwtacacs
[Quidway-aaa-domain-huawei] hwtacacs-server ht
[Quidway-aaa-domain-huawei] quit
[Quidway-aaa] quit
```

步骤 4 检查配置结果

在 SwitchB 上执行命令 **display hwtacacs-server template**，可以观察到该 HWTACACS 服务器模板的配置与要求一致。

```
<Quidway> display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 129.7.66.66:49:-
  Primary-authorization-server    : 129.7.66.66:49:-
  Primary-accounting-server       : 129.7.66.66:49:-
  Secondary-authentication-server : 129.7.66.67:49:-
  Secondary-authorization-server  : 129.7.66.67:49:-
  Secondary-accounting-server     : 129.7.66.67:49:-
  Current-authentication-server   : 129.7.66.66:49:-
  Current-authorization-server    : 129.7.66.66:49:-
  Current-accounting-server       : 129.7.66.66:49:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
  ------------------------------------------------------------------------------
```

同时在 SwitchB 上执行命令 **display domain**，可以观察到该域的配置与要求一致。

```
<Quidway> display domain name huawei

  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : l-h
  Accounting-scheme-name          : hwtacacs
  Authorization-scheme-name       : hwtacacs
  Service-scheme-name             : -
  RADIUS-server-group             : -
  HWTACACS-server-template        : ht
```

----结束

配置文件

```
#
sysname Quidway
#
hwtacacs-server template ht
 hwtacacs-server authentication 129.7.66.66
 hwtacacs-server authentication 129.7.66.67 secondary
 hwtacacs-server authorization 129.7.66.66
 hwtacacs-server authorization 129.7.66.67 secondary
 hwtacacs-server accounting 129.7.66.66
 hwtacacs-server accounting 129.7.66.67 secondary
 hwtacacs-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode hwtacacs local
  authentication-super hwtacacs super
 authorization-scheme default
 authorization-scheme hwtacacs
```


版权所有 © 华为技术有限公司

```
  authorization-mode  hwtacacs
 accounting-scheme default
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
  accounting start-fail online
  accounting realtime 3
 recording-scheme scheme0
  recording-mode hwtacacs ht
 cmd recording-scheme scheme0
 outbound recording-scheme scheme0
 system recording-scheme scheme0
 domain default
 domain default_admin
 domain huawei
  authentication-scheme l-h
  accounting-scheme hwtacacs
  authorization-scheme hwtacacs
  hwtacacs-server ht
#
return
```

8.2 NAC 配置

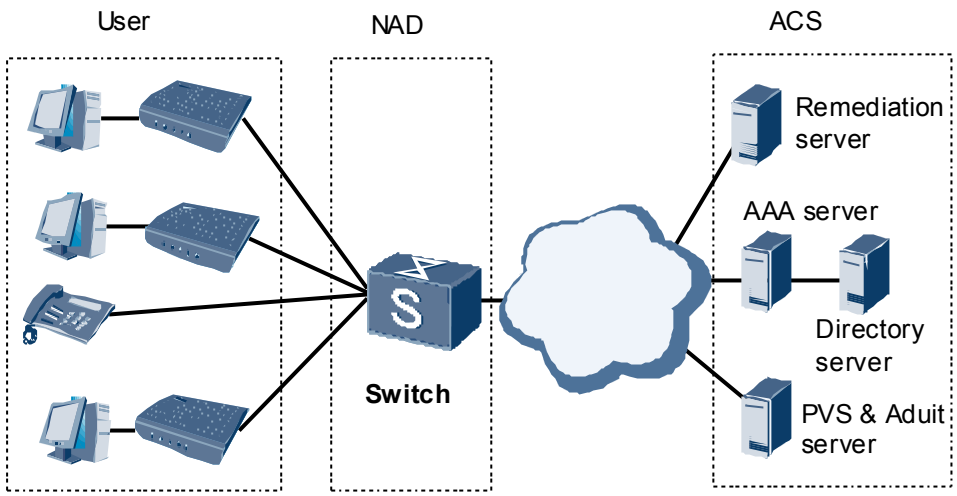
介绍 NAC 的原理和配置。

8.2.1 NAC 概述

简要介绍 NAC 的原理。

传统的网络安全技术只考虑了外部计算机对网络的威胁，而没有考虑到内部计算机对网络的威胁，而且现有的网络设备难以有效防止内部设备对网络的威胁。NAC（Network Admission Control）称为网络接入控制，是一种安全接入的框架，其理念是安全“端到端”的概念。NAC 从用户终端考虑内部网络安全，而不是从网络设备层面考虑安全。

图 8-3 NAC 典型组网图



如图 8-3 所示，NAC 作为网络安全接入的一种控制方案，主要包括以下几部分：

- User：接入用户，需要对其进行认证。如果采用 802.1x 认证，用户需要安装客户端软件。

版权所有 © 华为技术有限公司

- NAD：网络接入设备，包括路由器、交换机等（这里是 AC6605），对接入用户进行认证和授权。一般需要和 AAA 服务器配合使用，防止非法终端接入，降低不安全终端的威胁；防止合法终端越权访问，保护核心资源。
- ACS：安全策略服务器，主要进行终端安全健康性检查与策略管理；用户行为管理与违规审计，强化行为审计，防止恶意终端破坏。

Web 认证

Web 认证也称 Portal 认证，其基本原理是：用户首次打开浏览器，输入任何网址，都被强制重定向到 Web 服务器的认证页面，只有在认证通过后，用户才能访问网络资源。未认证用户只能访问特定的站点服务器。Web 认证通过 Web 页面输入用户名和密码，使用 Portal 协议完成认证过程。

Portal 协议主要用于 Web 服务器和其他设备之间的信息交互。Portal 协议基于客户端/服务器结构，采用 UDP 作为传输协议。在 Web 认证中，Web 认证服务器和 AC6605 之间的通信使用 Portal 协议，AC6605 为客户端。Web 认证服务器从认证页面中将用户输入的用户名和密码提取后，通过 Portal 协议传送给 AC6605。

802.1x 认证

IEEE 802.1x 标准（以下简称 802.1x）的主要内容是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1x 协议仅关注接入端口的状态。当合法用户（根据帐号和密码）接入时，该端口打开；当非法用户接入或没有用户接入时，该端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题，是各种认证技术中最简化的实现方案。

802.1x 不仅支持基于端口的认证模式，还支持基于 MAC 的认证模式。

- 基于端口模式：当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源。但是当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 模式：当采用基于 MAC 地址方式时，该端口下的所有接入用户均需要单独认证。

802.1x 支持两种认证方式：

- EAP 终结认证：由网络接入设备终结用户的 EAP 报文，解析出用户名和密码，并对密码进行加密，再发送到 RADIUS 服务器进行认证。
- EAP 透传认证：也叫 EAP 中继认证，由网络接入设备直接把 802.1x 用户的认证信息以及 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证。

MAC 认证

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件，用户名和密码都是用户设备的 MAC 地址。网络接入设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证。

版权所有 © 华为技术有限公司

MAC 旁路认证

MAC 旁路认证，AC6605 首先触发用户采用 802.1x 认证方式，如果 30 秒钟内用户不响应 AC6605 发出 802.1x 认证请求，则 AC6605 以用户的 MAC 地址为认证信息，把 MAC 地址作为用户名和密码上送 RADIUS 服务器进行认证。

8.2.2 AC6605 支持的 NAC 特性

介绍 NAC 特性在 AC6605 中的支持情况。

AC6605 作为 NAC 方案中的 NAD（Network Access Device），支持以下特性：

- 基于端口的 802.1X 认证
- 基于 MAC 的 802.1X 认证
- EAPOL 终结认证
- EAPOL 透传认证
- MAC 认证
- MAC 旁路认证
- 802.1x、MAC 认证或 MAC 旁路认证通过后自动给用户指定 VLAN

  当 802.1x、MAC 认证或 MAC 旁路认证用户认证通过后，系统根据认证服务器应答报文中携带的 VLAN 信息将用户下发一个 VLAN。共有两种方式将用户自动下发 VLAN。
  - 认证服务器应答报文中携带的 VLAN 信息是范围为 1 ～ 4094 的整数时，系统将其按照 VLAN ID 进行下发。
  - 认证服务器应答报文中携带的 VLAN 信息不是范围为 1 ～ 4094 的整数时，系统将其按照 VLAN 描述信息进行下发。
- 802.1x、MAC 认证或 MAC 旁路认证未通过将用户加入 Guest VLAN
- 802.1x、MAC 认证或 MAC 旁路认证通过后自动将用户下发 ACL 默认允许通过
- RADIUS 服务器动态授权 ACL

  如果在 RADIUS 服务器上配置了授权 ACL，在 AC6605 的相应端口配置 RADIUS 方案，则 AC6605 会根据 RADIUS 服务器下发的授权 ACL 对用户进行控制。网络管理员可以通过改变 RADIUS 服务器上的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限，提供了相对灵活的配置方式。

8.2.3 配置 Web 认证

配置 Web 认证。

建立配置任务

应用环境

对无法安装客户端软件的用户，可以配置 Web 认证，通过在网络浏览器（Internet Web Browser）上输入用户名和密码进行认证。

版权所有 © 华为技术有限公司

前置任务

Web 认证只提供了一个用户身份认证的实现方案，为了完成用户的身份认证还需要选择使用 RADIUS 或本地认证方法。因此，需要首先完成以下配置任务：

- 配置用户所属的 ISP 认证域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。
- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在网络接入设备上手动添加认证的用户名和密码。

数据准备

在配置 Web 认证之前，需要准备以下数据。

序号	数据
1	Web 服务器名称、IP 地址、URL
2	Portal 协议版本号、端口号
3	免认证规则 ID

配置 Web 认证服务器

背景信息

要对用户进行 Web 认证，必须配置 Web 认证服务器。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **web-auth-server** *server-name*，配置 Web 认证服务器，进入 Web 认证服务器视图。

最多可以配置 8 个 Web 认证服务器。

步骤 3 执行命令 **server-ip** *ip-address*，配置 Web 认证服务器的 IP 地址。

AC6605 支持一个 Web 服务器可以配置 4 个 IP 地址。

步骤 4 执行命令 **url** *url-string*，配置 Web 认证服务器对应的 URL（Uniform Resource Locator，统一资源定位符）。

步骤 5 执行命令 **port** *port-number* [**all**]，配置 Web 认证服务器接收 AC6605 发送的通知报文的端口号。

步骤 6 执行命令 **shared-key** { **cipher** | **simple** }*key-string*，配置 Web 认证服务器交互信息的共享密钥。

----结束

版权所有 © 华为技术有限公司

接口下绑定 Web 认证服务器

背景信息

在 VLANIF 接口下绑定 Web 认证服务器后，此 VLANIF 接口下接入的用户可以进行 Web 认证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

只能是 VLANIF 接口，目前 AC6605 只能通过 VLANIF 接口完成对接入用户的 Web 认证。

步骤 3 执行命令 **web-auth-server** *server-name*，在 VLANIF 接口下绑定 Web 认证服务器。

该 Web 认证服务器必须已经在系统视图下配置完成，才能在接口视图下通过服务器名进行绑定。

----结束

（可选）配置 Web 认证 Free Rule

背景信息

当某些特殊用户在未通过认证的情况下需要访问特定资源，可以配置 Free Rule。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **portal free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* }* } }*，配置免认证规则。

为 Web 认证用户配置免认证规则，符合配置规则的用户报文在用户未认证前即可被转发，使得用户在认证前具有一定的访问权限。

----结束

（可选）配置 Web 认证策略

背景信息

在使用 RADIUS 服务器对用户进行认证时，如果需要将 RADIUS 服务器返回的用户认证信息发给 Web 认证服务器，则需要进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **web-auth-server reply-message**，配置将用户的认证回应信息发给 Web 认证服务器。

缺省情况下，AC6605 会将用户的认证回应信息发给 Web 认证服务器。

----结束

（可选）配置侦听 Portal 协议报文的端口号

背景信息

本任务用于配置 AC6605 与 Web 服务器报文交互时，AC6605 接收 Portal 报文的端口号。这个端口号需要和 Web 认证服务器发送 Portal 报文的目的端口号相同，并且全局唯一。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **web-auth-server listening-port** *port-number*，配置侦听 Portal 协议报文的端口号。

缺省情况下，AC6605 接收 Portal 报文的端口号为 2000。

----结束

（可选）配置 Portal 协议版本

背景信息

AC6605 和 Web 认证服务器使用 Portal 协议进行交互时，要求支持的 Portal 协议版号必须一致。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **web-auth-server version v2** [**v1**]，配置 Portal 协议版本号。

缺省情况下，两种版本同时存在。如果不选择 v1，则只使用 v2 版本。

----结束

检查配置结果

背景信息

完成配置 Web 认证。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display web-auth-server configuration** 命令查看 Web 认证配置信息。

----结束

任务示例

查看 Web 认证服务器的配置信息。

```
<Quidway> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  ------------------------------------------------------------------------
  Web-auth-server Name : hw1
  IP-address           : 192.168.1.100
  Shared-key           : huawei
  Port / PortFlag      : 50100 / NO
  URL                  :
  ------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

8.2.4 配置 802.1x 认证

配置 802.1x 认证。

建立配置任务

应用环境

通过配置 802.1x 接入控制可以实现基于接口的网络接入控制，即在局域网接入控制设备的接口这一级对所接入的设备进行认证和控制。

前置任务

802.1x 认证只提供了一个用户身份认证的实现方案，为了完成用户的身份认证还需要选择使用 RADIUS 或本地认证方法。因此，需要首先完成以下配置任务：

- 配置用户所属的 ISP 认证域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。
- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在网络接入设备上手动添加认证的用户名和密码。

数据准备

在配置 802.1x 之前，需要准备以下数据。

序号	数据
1	使能 802.1x 地址认证的接口的接口号

版权所有 © 华为技术有限公司

使能全局 802.1x 认证功能

背景信息

配置 802.1x 认证功能前，需要首先使能全局 802.1x 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x enable**，使能全局 802.1x 认证功能。

执行本命令相当于打开全局 802.1x 认证的开关，802.1x 认证的其他相关配置在打开开关后才会生效。

缺省情况下，全局未使能 802.1x 认证功能。

----结束

使能接口 802.1x 认证功能

背景信息

注意

如果接口使能了 802.1x 功能，则禁止在该接口上使能 MAC 地址认证功能；反之，如果接口使能了 MAC 地址认证功能，则不能使能该接口的 802.1x 功能。

接口下使能 802.1x 认证，有以下两种配置方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x enable interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口的 802.1x 认证功能。

     系统视图下执行 **dot1x enable** 命令时指定接口列表，可以批量配置接口 802.1x 功能。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x enable**，在接口下使能 802.1x 认证功能。

  说明

  如果当前有 802.1x 在线用户，不允许去使能 802.1x 认证功能。

----结束

版权所有 © 华为技术有限公司

（可选）使能 MAC 旁路认证功能

背景信息

MAC 旁路认证，指当终端进行 802.1x 认证失败后，把它的 MAC 地址作为用户名和密码上送 RADIUS 服务器进行认证。对于某些特殊终端，例如打印机等，无法使用和安装 802.1x 终端软件，可以通过基于 MAC 的旁路认证方式进行认证。

配置 MAC 旁路认证，有以下两种配置方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x mac-bypass interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口 MAC 旁路认证功能。

     系统视图下执行 **dot1x mac-bypass** 命令时指定接口列表，可以批量配置接口 MAC 旁路认证功能。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x mac-bypass**，在接口下使能 MAC 旁路认证功能。

  执行本命令将包含并覆盖该接口下的 802.1x 使能命令，即
  - 如果接口下原来没有使能 802.1x，执行 **dot1x mac-bypass** 命令后，802.1x 使能了。
  - 如果接口下原来已经使能 802.1x，执行 **dot1x mac-bypass** 命令后，覆盖原来的配置，即接口的认证方式为 MAC 旁路认证。

  去使能 MAC 旁路认证功能，使用 **undo dot1x enable** 命令。注意同时也将去使能 802.1x 功能。

----结束

配置 802.1x 用户的认证方法

背景信息

根据实际组网环境和安全需要，可以配置对 802.1x 用户的认证方式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x authentication-method** { **chap** | **eap** | **pap** }，配置 802.1x 用户的认证方法。

缺省情况下，802.1x 用户认证方式为 CHAP 认证。 本命令为覆盖式命令，多次执行后保存最后一次配置。

版权所有 © 华为技术有限公司

- PAP（Password Authentication Protocol）是一种两次握手认证协议，它采用明文方式传送口令 。
- CHAP（Challenge Handshake Authentication Protocol）是一种三次握手认证协议，它只在网络上传输用户名，而并不传输口令。相比之下，CHAP 认证保密性较好，更为安全可靠。
- EAP 认证功能，意味着交换机直接把 802.1x 用户的认证信息以 EAP 报文发送给 RADIUS 服务器完成认证，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证。如果要采用 PEAP、EAP-TLS、EAP-TTLS 或者 EAP-MD5 这四种认证方法之一，只需启动 EAP 认证即可。

其中 PAP 和 CHAP 认证属于终结认证，EAP 方式属于中继认证方式。

注意

只有采用 RADIUS 认证时，802.1x 用户的认证方式才可以配置为 EAP 方式。

----结束

（可选）配置接口接入模式

背景信息

802.1x 可以工作在两种模式下：

- 基于端口模式：只要连接在该端口的第一个 MAC 设备通过认证，该端口连接的其他 MAC 设备不用认证都允许接入。
- 基于 MAC 模式：端口下每个 MAC 设备接入时都需要通过认证。

配置接口的接入模式，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x port-method** { **mac** | **port** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的接入模式。

     系统视图下执行 **dot1x port-method** 命令时指定接口列表，可以批量配置接口的接入模式。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x port-method** { **mac** | **port** }，配置接口的接入模式。

  缺省情况下，接口的接入模式为基于 MAC 地址。

版权所有 © 华为技术有限公司

注意

当有 802.1x 用户在线时，不允许执行本命令更改接口接入控制方式。

----结束

（可选）配置接口授权状态

背景信息

用户通过认证以后，可以对用户进行授权，控制用户能够访问哪些网络资源。

配置接口的授权状态，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x port-control** { **auto** | **authorized-force** | **unauthorized-force** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的授权状态。

     系统视图下执行 **dot1x port-control** 命令时指定接口列表，可以批量配置接口的授权状态。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x port-control** { **auto** | **authorized-force** | **unauthorized-force** }，配置接口的授权状态。

  缺省情况下，接口的授权状态为 **auto**，即自动识别模式。

  - 自动识别模式（**auto**）：接口初始状态为非授权状态，仅允许收发 EAPoL 报文，不允许用户访问网络资源；如果认证通过，则接口切换到授权状态，允许用户访问网络资源。
  - 强制授权模式（**authorized-force**）：接口始终处于授权状态，允许用户不经认证授权即可访问网络资源。
  - 强制非授权模式（**unauthorized-force**）：接口始终处于非授权状态，不允许用户访问网络资源。

----结束

（可选）配置接口接入的最大用户数量

背景信息

当接口接入的用户数达到最大数量时，AC6605 将不会再对之后接入的用户触发认证动作，这些用户也就无法正常访问网络。

版权所有 © 华为技术有限公司

配置接口接入的最大用户数量，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x max-user** *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口可以同时接入的最大用户数量。

     系统视图下执行 **dot1x max-user** 命令时指定接口列表，可以批量配置接口的最大接入用户数。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x max-user** *user-number*，配置接口可以同时接入的最大用户数量。

  缺省情况下，每个接口可以同时接入用户的最大数为 256。

  此命令只针对配置为 MAC 接入模式的接口生效。如果接口的配置为 **port** 模式，接口接入的最大用户数自动设置为 1，因为接口只需要一个用户认证成功，其他用户都可以上线。

  说明

  当设备上有用户在线时可配置该命令，该命令对已经在线的用户无效，对配置后进行认证的用户有效。

  AC6605 整机允许接入的 NAC 用户的最大数为 256。

----结束

（可选）配置允许 DHCP 报文触发认证

背景信息

配置允许 DHCP 报文触发认证后，802.1x 允许 AC6605 在接入用户运行 DHCP、申请动态 IP 地址时就触发对其身份的认证。接入用户可以不经过客户端软件拨号就开始 802.1x 认证，这种方式有助于快速部署网络。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x dhcp-trigger**，配置允许 DHCP 报文触发认证。

缺省情况下，DHCP 不触发接入用户的身份认证。

在执行此命令后，若用户未通过认证，则无法从 DHCP Server 获得动态 IP 地址。

----结束

版权所有 © 华为技术有限公司

（可选）配置 802.1x 定时器

背景信息

802.1x 在运行时会启动很多定时器以控制接入用户（Supplicant）、接入认证设备（Authenticator）以及认证服务器（Authentication Server）之间进行合理、有序的交互。

可以使用命令改变部分定时器值（另外部分定时器是不可调节的），以调节交互进程。这在较为特殊或比较恶劣的网络环境下可能是必需的措施。一般情况下，建议保持这些定时器的缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令，**dot1x timer** { **client-timeout** *client-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **tx-period** *tx-period-value* }，配置 802.1x 认证的各项定时器参数。

- **client-timeout**：客户端认证超时定时器。缺省值是 30 秒。
- **handshake-period**：AC6605 与 802.1x 客户端握手时间间隔。缺省值是 15 秒。
- **quiet-period**：静默定时器时长。缺省值是 60 秒。
- **server-timeout**：认证服务器超时定时器。缺省值是 30 秒。
- **tx-period**：发送认证请求的时间间隔。缺省值是 30 秒。

这里只是配置定时器的时长，具体到每个定时器是否使能，要进行相应配置或采取系统默认配置。

----结束

（可选）配置定时静默功能

背景信息

开启静默定时器功能后，当 802.1x 用户认证失败以后，AC6605 会将该用户静默一段时间，在这段时间内不对用户的认证请求进行处理。这样可以防止频繁认证对系统造成冲击。

为了避免静默功能使能后，用户认证失败 1 次就被静默，在 AC6605 上用户可以配置静默前允许认证失败的次数大于 1 次。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x quiet-period**，使能静默定时器功能。

缺省情况下，未使能静默定时器功能。

在静默期间，AC6605 丢弃该用户的 802.1x 认证请求。静默定时器的时长通过命令 **dot1x timer** 配置，配置过程请参见**（可选）配置 802.1x 定时器**。

步骤 3 执行命令 **dot1x quiet-times** *fail-times*，配置 802.1x 用户被静默前 60 秒内允许认证失败的次数。

版权所有 © 华为技术有限公司

缺省情况下，802.1x 用户在 60 秒内认证失败 3 次被静默。

----结束

（可选）配置 802.1x 认证的 Guest VLAN

背景信息

当用户的接入方式为 **mac** 方式时，Guest VLAN 功能开启后，AC6605 向所有开启 802.1x 功能的端口广播主动认证报文，如果达到最大重认证次数后，仍有端口上未返回响应报文，则 AC6605 将该端口加入到 Guest VLAN 中。之后属于该 Guest VLAN 中的用户访问该 Guest VLAN 中的资源时，不需要进行 802.1x 认证，但访问外部的资源时仍需要进行认证。从而满足了允许未认证通过的用户访问某些资源的需求。

当用户的接入方式为 **port** 方式时，Guest VLAN 功能开启后，如果系统和接口下的 802.1x 功能已经配置，并且接口的接入控制模式为默认的 **auto** 模式，AC6605 直接将端口加入 Guest VLAN，该端口下的用户无需任何认证即可访问 Guest VLAN 中网络资源。

配置 Guest VLAN，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x guest-vlan** *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的 Guest VLAN。

     系统视图下执行 **dot1x guest-vlan** 命令时指定接口列表，可以批量配置接口的 Guest VLAN。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x guest-vlan** *vlan-id*，配置接口的 Guest VLAN。

  缺省情况下，接口下未配置 Guest VLAN。

----结束

（可选）配置在线用户握手功能

背景信息

握手报文的发送需要华为客户端的支持，用以探测用户是否在线。

对于不支持握手功能的客户端，在握手周期内 AC6605 不会收到握手回应报文。因此为了防止 AC6605 错误地认为用户下线，需要将在线用户握手功能关闭。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **dot1x handshake**，配置 dot1x 的握手功能。

缺省情况下，AC6605 不使能与在线用户握手功能。

握手周期需要使用 **dot1x timer** 命令配置。

步骤 3 （可选）执行命令 **dot1x handshake packet-type** { **request-identity** | **srp-sha1-part2** }，配置 802.1x 认证握手报文的类型。

缺省情况下，802.1x 认证握手报文的类型是 request-identity。

----结束

（可选）配置向用户发送认证请求的最大次数

背景信息

AC6605 初次向用户发送认证请求帧后，在规定的时间里没有收到用户的响应，AC6605 将再次向用户发送该认证请求。当发送次数达到最大次数后仍没有收到响应，AC6605 不再重复向用户发送该认证请求。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x retry** *max-retry-value*，配置向用户发送认证请求的最大次数。

缺省情况下，AC6605 可以重复向接入用户发送认证请求帧的最大次数为 2 次。

----结束

检查配置结果

前提条件

已完成 802.1x 的配置。

操作步骤

- 使用命令 **display dot1x** [**statistics**] [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] 查看 802.1x 的配置信息。
- 使用命令 **display mac-address** { **authen** | **guest** } [**vlan** *vlan-id*]查看通过 802.1x 认证、MAC 认证或者加入 Guest VLAN 的 MAC 地址信息。

----结束

任务示例

查看 GE0/0/1 接口 802.1x 认证信息。

```
<Quidway> display dot1x interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1 status: UP  802.1x protocol is Enabled[mac-bypass]
  Port control type is Auto
  Authentication method is MAC-based
  Reauthentication is disabled
  Maximum users: 256
```


版权所有 © 华为技术有限公司

```
  Current users: 2

  Authentication Success: 1          Failure: 11
  EAPOL Packets: TX     : 24         RX     : 4
  Sent      EAPOL Request/Identity Packets  : 11
            EAPOL Request/Challenge Packets : 1
            Multicast Trigger Packets       : 0
            DHCP Trigger Packets            : 0
            EAPOL Success Packets           : 1
            EAPOL Failure Packets           : 11
  Received  EAPOL Start Packets             : 2
            EAPOL LogOff Packets            : 0
            EAPOL Response/Identity Packets : 1
            EAPOL Response/Challenge Packets: 1
```

查看通过 802.1x 认证或 MAC 认证的 MAC 地址信息。

```
<Quidway> display mac-address authen
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
0000-0000-0100 3000        -      -      GE0/0/1         authen    -
0000-0000-0200 3000        -      -      GE0/0/1         authen    -
0000-0000-0600 3000        -      -      GE0/0/1         authen    -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 64
```

查看加入 Guest VLAN 的 MAC 地址信息。

```
<Quidway> display mac-address guest
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
0000-0000-0404 3010        -      -      GE0/0/1         guest     -
0000-0000-0407 3010        -      -      GE0/0/1         guest     -
0000-0000-0410 3010        -      -      GE0/0/1         guest     -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 67
```

8.2.5 配置 MAC 认证

配置 MAC 认证。

建立配置任务

应用环境

对无法安装客户端软件的终端，如传真机、打印机等设备，当需要对其进行认证时，可以配置 MAC 地址认证。

前置任务

MAC 认证只提供了一个用户身份认证的实现方案，为了完成用户的身份认证还需要选择使用 RADIUS 或本地认证方法。因此，需要首先完成以下配置任务：

- 配置用户所属的 ISP 认证域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。

版权所有 © 华为技术有限公司

- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在网络接入设备上手动添加认证的用户名和密码。

数据准备

在配置 MAC 地址认证前，需要准备以下数据。

序号	数据
1	使能 MAC 地址认证的接口的接口号

使能全局 MAC 认证功能

背景信息

配置 MAC 认证功能前，需要首先使能全局 MAC 认证功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen**，使能全局 MAC 认证功能。

执行本命令相当于打开全局 MAC 认证的开关，MAC 认证的其他相关配置在打开开关后才会生效。

缺省情况下，全局未使能 MAC 认证功能。

----结束

使能接口 MAC 认证功能

背景信息



注意

如果接口使能了 MAC 地址认证功能，则禁止在该接口上使能 802.1x 功能；反之，如果接口使能了 802.1x 功能，则不能使能该接口的 MAC 地址认证功能。

接口下使能 MAC 地址认证，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **mac-authen interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口的 MAC 地址认证功能。

   系统视图下执行 **mac-authen** 命令时指定接口列表，可以批量配置接口 MAC 地址认证功能。

- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen**，在接口下使能 MAC 地址认证功能。

  如果当前有 MAC 认证在线用户，不允许去使能 MAC 认证功能。

----结束

配置 MAC 认证的用户名

MAC 认证的用户名形式可以采用固定用户名形式或 MAC 地址形式。

背景信息

当 MAC 认证的用户名形式为固定用户名形式时，用户可以设置密码也可以不设置密码。当 MAC 认证的用户名形式为 MAC 地址形式时，用户使用 MAC 地址作为用户名进行认证，同时该 MAC 地址也作为认证密码。

操作步骤

- 系统视图下配置用户名形式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen username** { **fixed** *username* [**password** { **cipher** | **simple** } *password*] | **macaddress** [**format** { **with-hyphen** | **without-hyphen** }] }，配置 MAC 认证用户名的形式。

     MAC 地址用户名形式有两种，带“-”（如 0010-8300-0011）和不带“-”（001083000011）。缺省情况下，使用不带有分隔符“-”的 MAC 地址形式。

----结束

（可选）配置 MAC 认证的域

背景信息

当用户采用 MAC 地址认证用户名形式，或者固定用户名形式时不带域名，如果没有配置认证域，用户使用 **default** 认证。当采用固定格式用户名时在用户名中指定了域，则采用用户自带的认证域。

说明

配置 MAC 地址认证用户所使用的认证域，配置前应确定已有可用的域，否则配置时会提示出错。

操作步骤

- 系统视图下

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mac-authen domain** *isp-name* [**mac-address** *mac-address* **mask** *mask*]，配置 MAC 地址认证用户所使用的认证域的域名。

----结束

（可选）配置 MAC 认证定时器

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen timer** { **guest-vlan reauthenticate-period** *interval* | **offline-detect** *offline-detect-value* | **quiet-period** *quiet-value* | **reauthenticate-period** *interval* | **server-timeout** *server-timeout-value* }，配置 MAC 地址认证的各项定时器参数。

- **guest-vlan reauthenticate-period**：Guest VLAN 内的用户进行重认证的时间间隔。缺省值是 60 秒。
- **offline-detect**：下线检测定时器，用来设置 AC6605 检查用户是否已经下线的时间间隔。缺省值是 300 秒。
- **quiet-period**：静默定时器，对用户认证失败以后，AC6605 需要静默一段时间后再处理用户认证请求，在静默期间，AC6605 不处理该用户的认证请求。缺省值是 60 秒。
- **server-timeout**：服务器超时定时器，在用户的认证过程中，如果 AC6605 同 RADIUS 服务器的连接超时，则此次认证失败。缺省值是 30 秒。

----结束

（可选）配置 MAC 认证的 Guest VLAN

背景信息

当 Guest VLAN 功能开启后，如果用户 MAC 认证失败，则 AC6605 将该用户加入到 Guest VLAN 中。之后属于该 Guest VLAN 中的用户访问该 Guest VLAN 中的资源时，不需要进行 MAC 认证，但访问外部的资源时仍需要进行认证。从而满足了允许未认证用户访问某些资源的需求。

说明

配置的 Guest VLAN 必须已经创建，且不能是接口的缺省 VLAN。

Guest VLAN 功能只能在 Hybrid 端口和 Trunk 端口生效。

配置 Guest VLAN，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen guest-vlan** *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的 Guest VLAN。

     系统视图下执行 **mac-authen guest-vlan** 命令时指定接口列表，可以批量配置接口的 Guest VLAN。

版权所有 © 华为技术有限公司

- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen guest-vlan** *vlan-id*，配置接口的 Guest VLAN。

  缺省情况下，接口下未配置 Guest VLAN。

----结束

（可选）配置 MAC 认证用户的最大数量

背景信息

当接入用户到达配置的限制数量时，AC6605 将不会再对之后接入的用户进行认证触发动作，这些用户也就无法正常访问网络。

配置 MAC 认证用户的最大数量，有以下两种方法：

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen max-user** *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口可以接入的 MAC 地址认证用户的最大数量。

     系统视图下执行 **mac-authen max-user** 命令时指定接口列表，可以批量配置接口的最大接入用户数。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen max-user** *user-number*，配置接口可以接入的 MAC 地址认证用户的最大数量。

  缺省情况下，AC6605 接口允许接入的 MAC 地址认证用户的最大数量为 256 个。

  AC6605 整机允许接入的 NAC 用户的最大数量为：512。

----结束

（可选）对指定 MAC 地址进行重认证

背景信息

系统可以对某个已经通过 MAC 认证的用户进行一次重认证，如果重认证成功则对用户重新进行授权，否则使该用户下线。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **mac-authen reauthenticate mac-address** *mac-address*，配置对某个已经通过认证的 MAC 地址进行重认证。

对指定 MAC 地址进行重认证，如果该 MAC 地址处于认证不通过状态，则忽略此操作。

步骤 3 执行命令 **mac-authen reauthenticate interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能指定接口的 MAC 认证功能。

步骤 4 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 5 执行命令 **mac-authen reauthenticate**，使能指定接口的 MAC 认证功能。

----结束

检查配置结果

前提条件

已完成 MAC 认证的配置。

操作步骤

- 使用命令 **display mac-authen** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] 查看 MAC 认证的配置信息。
- 使用命令 **display mac-address** { **authen** | **guest** } [**vlan** *vlan-id*]查看通过 802.1x 认证、MAC 认证或者加入 Guest VLAN 的 MAC 地址信息。

----结束

8.2.6 维护 NAC

清除认证统计信息、调试 NAC。

清除 802.1x 统计信息

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除统计信息后，请在用户视图下执行以下命令。

操作步骤

- 使用 **reset dot1x statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] }]命令清除 802.1x 的统计信息。

----结束

版权所有 © 华为技术有限公司

清除 MAC 认证统计信息

背景信息



注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除统计信息后，请在用户视图下执行以下命令。

操作步骤

- 使用 **reset mac-authen statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] }]命令清除 MAC 地址认证的统计信息。

----结束

8.2.7 配置举例

介绍各种认证方式的应用举例。

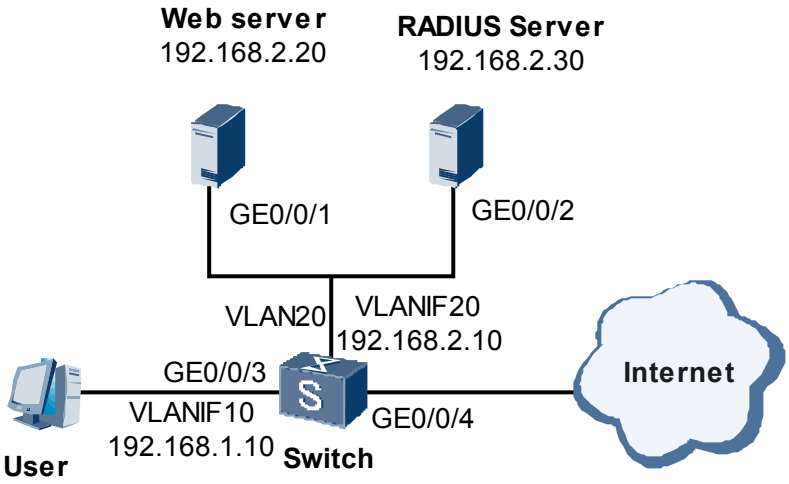
配置 Web 认证示例

组网需求

如图 8-4 所示，要求如下：

- 用户通过 Switch 完成 Web 认证。
- 使用 RADIUS 服务器完成认证。
- 用户在未通过 Web 认证前，只能访问 Web 服务器。
- 用户通过 Web 认证后，可以访问外部网络。

图 8-4 配置 Web 认证组网图



版权所有 © 华为技术有限公司

配置思路

用如下的思路配置 Web 认证。

1. 配置用户接入三层接口 IP 地址。
2. 配置 RADIUS 服务器模板。
3. 配置 AAA 认证模板。
4. 配置域。
5. 配置 Web 认证。

数据准备

为完成此配置举例，需要准备如下数据：

- Web 认证服务器 IP 地址，URL。
- 连接认证终端上行三层口的 IP 地址。
- RADIUS 服务器 IP 地址，认证端口号。
- RADIUS 服务器密钥为 hello，重传次数为 2。
- AAA 认证方案 web1。
- RADIUS 服务器模版 rd1。
- 域 isp1。

说明

本案例只包括 Switch 的配置，Web 服务器、RADIUS 服务器的配置这里不做相关说明。

操作步骤

步骤 1 配置用户接入的三层接口 IP 地址

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type access
[Quidway-GigabitEthernet0/0/3] port default vlan 10
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.10 24
[Quidway-Vlanif10] quit
```

步骤 2 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 rd1。

```
[Quidway] radius-server template rd1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

配置 RADIUS 服务器密钥、重传次数。

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```


版权所有 © 华为技术有限公司

步骤 3 配置认证方案,认证方案 web1，认证方法为 RADIUS

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

步骤 4 配置 isp1 域，绑定认证方式和 RADIUS 服务器模板

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

步骤 5 配置 Web 认证

配置 Web 认证服务器 IP 地址和 URL。

```
[Quidway] web-auth-serer isp1
[Quidway-web-auth-server-isp1] server-ip 192.168.2.20
[Quidway-web-auth-server-isp1] url http：//www.isp1.com
```

在接口下绑定 Web 认证服务器。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] web-auth-server isp1
[Quidway-Vlanif10] quit
```

步骤 6 检查配置结果

在 Switch 上执行命令 **display web-auth-server configuration**，可以看到 Web 服务器的详细配置信息。

```
<Quidway> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  ------------------------------------------------------------------------
  Web-auth-server Name : isp1
  IP-address           : 192.168.1.20
  Shared-key           : huawei
  Port / PortFlag      : 50100 / NO
  URL                  : http：//www.isp1.com
   ------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

----结束

配置文件

```
#
sysname Quidway
#
vlan batch 1 10
#
web-auth-server isp1
 server-ip 10.1.1.1
 port 50100
 url http//www.isp1.com
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
```


版权所有 © 华为技术有限公司

```
  authentication-scheme web1
  radius-server  rd1
#
interface Vlanif10
 ip address 192.168.1.10 255.255.255.0
 web-auth-server web
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
#
return
```

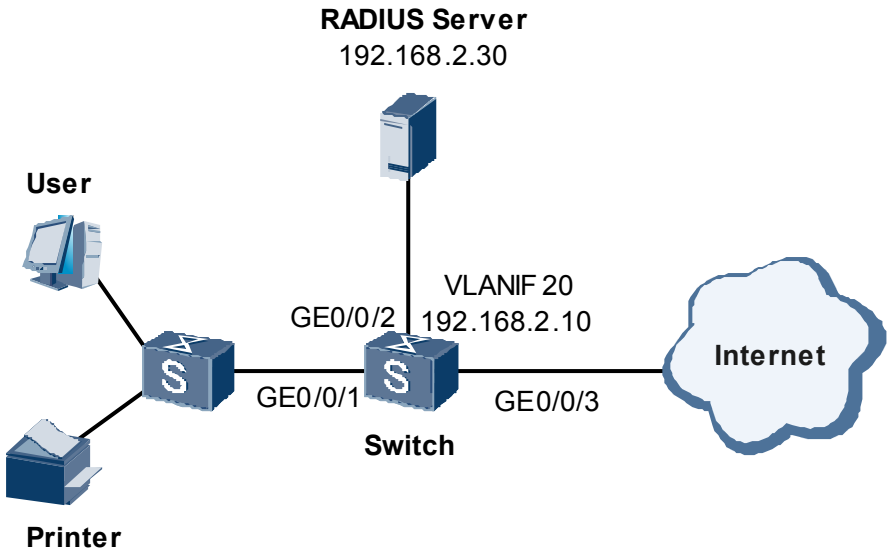
配置 802.1x 认证示例

组网需求

如图 8-5 所示，要求如下：

- 对 GE0/0/1 接口上的接入用户进行 802.1x 认证，以控制其访问 Internet，接入控制方式采用缺省方式，即基于 MAC 的接入控制方式。
- 使用 RADIUS 服务器完成认证。
- GE0/0/1 接口最大接入用户数为 100。
- 对 GE0/0/1 接口下的打印机采用 MAC 旁路认证。

图 8-5 配置 802.1x 认证组网图



配置思路

用如下的思路配置 802.1x 认证。

1. 配置 RADIUS 服务器模板。
2. 配置 AAA 认证模板。
3. 配置域。

版权所有 © 华为技术有限公司

4. 配置 802.1x 认证。

数据准备

为完成此配置举例，需要准备如下数据：

- RADIUS 服务器 IP 地址，认证端口号。
- RADIUS 服务器密钥为 hello，重传次数为 2。
- AAA 认证方案 web1。
- RADIUS 服务器模版 rd1。
- 域 isp1。

说明

本案例只包括 Switch 的配置，RADIUS 服务器的配置这里不做相关说明。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 rd1。

```
[Quidway] radius-server template rd1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

配置 RADIUS 服务器密钥、重传次数。

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

步骤 2 配置认证方案，认证方案 web1，认证方法为 RADIUS

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

步骤 3 配置 isp1 域，绑定认证方式和 RADIUS 服务器模板

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

步骤 4 配置 802.1x 认证

在全局和接口下使能 802.1x 认证。

```
[Quidway] dot1x enable
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dot1x enable
```

配置允许接入的最大用户数。

```
[Quidway-GigabitEthernet0/0/1] dot1x max-user 100
```

配置 MAC 旁路认证。

```
[Quidway-GigabitEthernet0/0/1] dot1x mac-bypass
```

步骤 5 检查配置结果

在 Switch 执行命令 **display dot1x interface**，可以看到 802.1x 配置信息和统计信息。

版权所有 © 华为技术有限公司

```
<Quidway> display dot1x interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1 status: UP  802.1x protocol is Enabled[mac-bypass]
  Port control type is Auto
  Authentication method is MAC-based
  Reauthentication is disabled
  Maximum users: 100
  Current users: 1

  Authentication Success: 4          Failure: 0
  EAPOL Packets: TX     : 8          RX     : 16
  Sent      EAPOL Request/Identity Packets  : 4
            EAPOL Request/Challenge Packets : 4
            Multicast Trigger Packets       : 0
            EAPOL Success Packets           : 4
            EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets             : 4
            EAPOL LogOff Packets            : 3
            EAPOL Response/Identity Packets : 4
            EAPOL Response/Challenge Packets: 4
```

----结束

配置文件

```
#
sysname Quidway
#
dot1x enable
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  radius-server rd1
#
interface GigabitEthernet0/0/1
 dot1x mac-bypass
 dot1x max-user 100
#
return
```

配置 MAC 认证示例

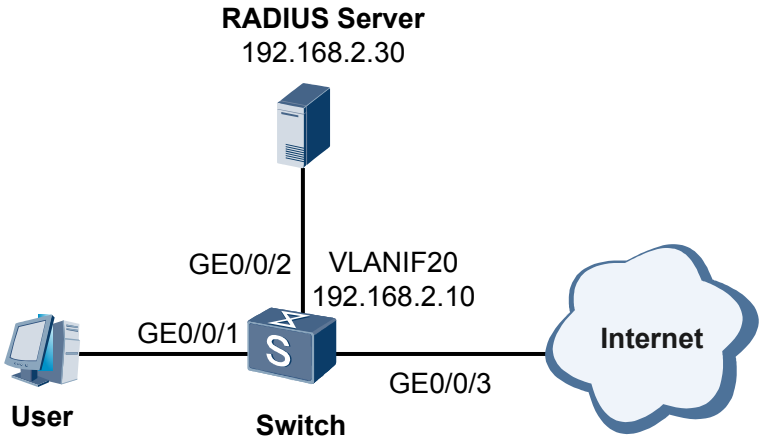
组网需求

如图 8-6 所示，要求如下：

- 在接口 GE0/0/1 上的设备上对接入用户进行认证，以控制其访问 Internet。
- 使用 RADIUS 服务器完成认证。
- 对接口下的所有认证用户名采用缺省方式，MAC 地址不带“-”用户名方式认证。
- GE0/0/1 接口下允许接入的最大用户数为 100。

版权所有 © 华为技术有限公司

图 8-6 配置 MAC 地址认证组网图



配置思路

用如下的思路配置 MAC 认证。

1. 配置 RADIUS 服务器模板。
2. 配置 AAA 认证模板。
3. 配置域和 MAC 认证用户使用的域。
4. 配置 MAC 认证。

数据准备

为完成此配置举例，需要准备如下数据：

- RADIUS 服务器 IP 地址，认证端口号。
- RADIUS 服务器密钥为 hello，重传次数为 2。
- AAA 认证方案 web1。
- RADIUS 服务器模版 rd1。
- 域 isp1。

说明

本案例只包括 Switch 的配置，RADIUS 服务器的配置这里不做相关说明。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 rd1。

```
[Quidway] radius-server template rd1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

配置 RADIUS 服务器密钥、重传次数。

版权所有 © 华为技术有限公司

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

步骤 2 配置认证方案，认证方案 web1，认证方法为 RADIUS

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

步骤 3 配置 isp1 域，绑定认证方式和 RADIUS 服务器模板

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

步骤 4 配置 MAC 认证

在全局和接口下使能 MAC 认证。

```
[Quidway] mac-authen
[Quidway] interface gigabitethernet0/0/1
[Quidway-GigabitEthernet0/0/1] mac-authen
```

配置允许接入的最大用户数。

```
[Quidway-GigabitEthernet0/0/1] mac-authen max-user 100
[Quidway-GigabitEthernet0/0/1] quit
```

配置 MAC 认证用户所属的域。

```
[Quidway] mac-authen domain isp1
```

步骤 5 检查配置结果

在 Switch 执行命令 **display mac-authen interface**，可以看到 MAC 认证配置信息。

```
<Quidway> display mac-authen interface gigabitethernet 0/0/1
  GigabitEthernet0/0/1 state: UP  MAC address authentication is enabled
  Maximum users: 100
  Current users: 2
  Guest VLAN is disabled
```

----结束

配置文件

```
#
sysname Quidway
#
mac-authen
mac-authen domain isp
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  radius-server rd1
#
interface GigabitEthernet0/0/1
 mac-authen
 mac-authen max-user 100
```


版权所有 © 华为技术有限公司

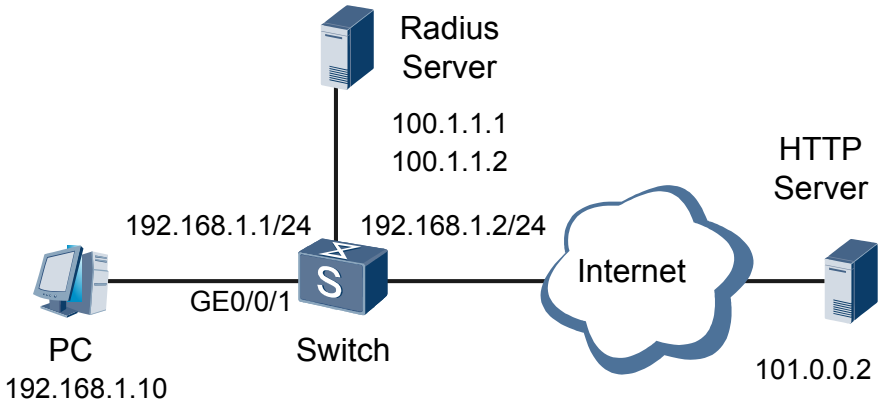
```
#
return
```

配置 RADIUS 服务器动态授权 ACL 示例

组网需求

如图 8-7 所示，PC 通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器。Internet 网络中有一台 HTTP 服务器。要求当用户认证成功上线后，通过 RADIUS 服务器下发 ACL，来控制 PC 能够访问 Internet，但是不能访问 HTTP 服务器。

图 8-7 配置 802.1x 认证组网图



配置思路

用如下的思路配置 RADIUS 服务器动态授权 ACL。

1. 在认证服务器上配置授权下发 ACL。
2. 配置 RADIUS 服务器模板。
3. 配置 AAA 认证模板。
4. 配置域。
5. 在 Switch 上配置和 RADIUS 服务器上一样的 ACL，并配置相应的规则。
6. 配置 802.1x 认证。

数据准备

为完成此配置举例，需要准备如下数据：

- RADIUS 认证服务器的 IP 地址为 100.1.1.1，认证端口号为 1812。
- RADIUS 服务器模板为 rd1。
- RADIUS 服务器的共享密钥为 hello。
- AAA 认证方案 web1。
- 域 isp1。

版权所有 © 华为技术有限公司

- ACL 编号为 3000。

说明

本案例只包括 Switch 的配置，RADIUS 服务器的配置这里不做相关说明。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 rd1。

```
[Quidway] radius-server template rd1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Quidway-radius-rd1] radius-server authentication 100.1.1.1 1812
```

配置 RADIUS 服务器密钥。

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] quit
```

步骤 2 配置认证方案，认证方案 web1，认证方法为 RADIUS

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

步骤 3 配置 isp1 域，绑定认证方式和 RADIUS 服务器模板

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] accounting-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

步骤 4 配置 ACL 3000，拒绝目的 IP 地址为 101.0.0.2 的报文通过。

```
[Quidway] acl 3000
[Quidway-acl-adv-3000] rule 0 deny ip destination 101.0.0.2 0
[Quidway-acl-adv-3000] quit
```

步骤 5 配置 802.1x 认证

在全局使能 802.1x 认证。

```
[Quidway] dot1x enable
```

步骤 6 检查配置结果

当 PC 用户认证成功上线后，通过命令 ping 可以验证认证服务器下发的 ACL 3000 是否生效。

```
[Quidway] ping 101.0.0.2
PING 101.0.0.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- 101.0.0.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

----结束

版权所有 © 华为技术有限公司

配置文件

```
#
sysname Quidway
#
dot1x enable
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 100.1.1.1 1812
 radius-server accounting 100.1.1.2 1813
#
acl number 3000
 rule 0 deny ip destination 101.0.0.2 0
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  accounting-scheme web1
  radius-server rd1
#
return
```

8.3 DHCP Snooping 配置

介绍 DHCP Snooping 的原理和配置方法，并给出配置举例。

8.3.1 DHCP Snooping 概述

简要介绍 DHCP Snooping 的原理。

DHCP Snooping 是 DHCP（Dynamic Host Configuration Protocol）的一种安全特性，通过截获 DHCP Client 和 DHCP Server 之间的 DHCP 报文并进行分析处理，可以过滤不信任的 DHCP 报文并建立和维护一个 DHCP Snooping 绑定表。该绑定表包括 MAC 地址、IP 地址、租约时间、绑定类型、VLAN ID、接口等信息。

DHCP Snooping 通过记录 DHCP Client 的 IP 地址与 MAC 地址的对应关系，保证合法用户能访问网络，作用相当于在 DHCP Client 和 DHCP Server 之间建立一道防火墙。

DHCP Snooping 可以解决设备应用 DHCP 时遇到 DHCP DoS（Denial of Service）攻击、DHCP Server 仿冒攻击、DHCP 仿冒续租报文攻击等问题。

说明

本手册中，DHCP Snooping 包括 DHCPv4 Snooping 和 DHCPv6 Snooping。

8.3.2 AC6605 支持的 DHCP Snooping 特性

介绍 DHCP Snooping 特性在 AC6605 中的支持情况。

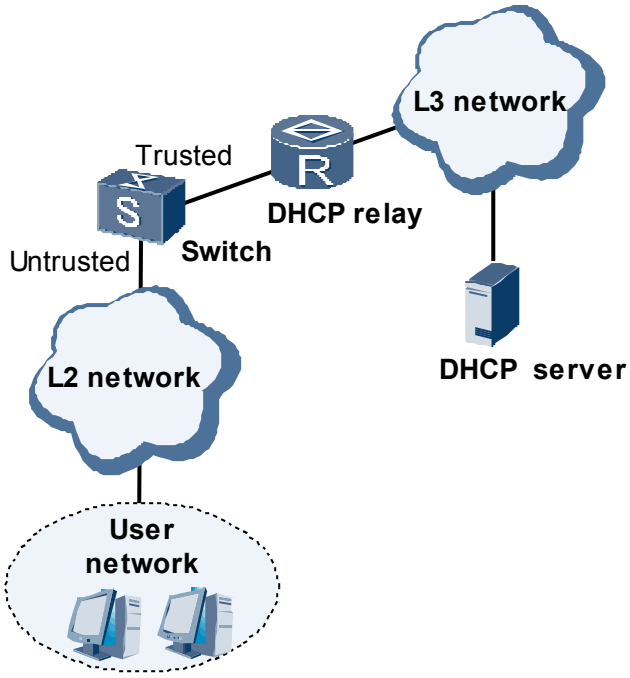
AC6605 支持 Trusted 接口、DHCP Snooping 安全绑定、IP + MAC + 接口 + VLANID 组合绑定、Option82 字段等安全方面的功能，为 DHCP 功能在网络中的应用提供更高的安全性。

版权所有 © 华为技术有限公司

AC6605 在二层网络中应用 DHCP Snooping

AC6605 部署在二层网络中时，处于 DHCP Relay 和用户网络之间。DHCP Snooping 在 AC6605 上的应用如图 8-8 所示，图中 AC6605 使能了 DHCP Snooping 功能。

图 8-8 AC6605 在二层网络中应用 DHCP Snooping 典型组网图

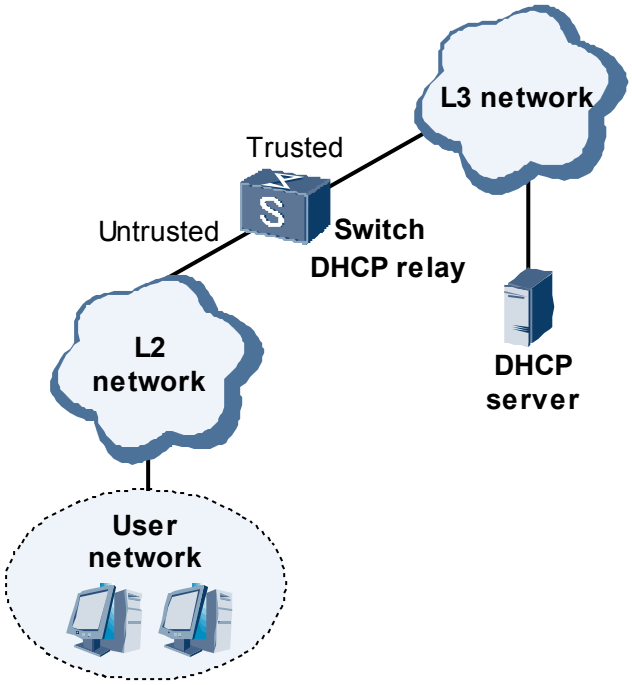


AC6605 作为 DHCP Relay 应用 DHCP Snooping

AC6605 具有三层路由功能，也可以作为 DHCP Relay 应用在组网中。如图 8-9 所示，AC6605 作为 DHCP Relay，使能了 DHCP Snooping 功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 8-9 AC6605 作为 DHCP Relay 应用 DHCP Snooping 典型组网图



说明

AC6605 应用在二层网络中或作为 DHCP Relay 应用时使能 DHCP Snooping，都可以防止如表 8-1 所示的几种攻击类型。在配置上的区别仅是：作为 DHCP Relay 时支持 ARP 与 DHCP 的联动功能。在二层网络中应用时不支持该功能。通过执行 **arp dhcp-snooping-detect enable** 命令可以使能 ARP 与 DHCP Snooping 的联动功能。

DHCPv6 Snooping

AC6605 支持 DHCPv6 Snooping，在使能 DHCP Snooping 功能后，对 IPv6 地址的用户也会生成绑定表。绑定表的内容包括 IPv6 地址、MAC 地址、接口、VLAN 等信息。

DHCP Snooping 能对抗的攻击类型

根据不同的攻击类型，DHCP Snooping 提供不同的工作模式，见表 8-1。

说明

建议开启所有 DHCP Snooping 安全功能。

表 8-1 攻击类型与 DHCP Snooping 工作模式对应表

攻击类型	DHCP Snooping 工作模式
DHCP Server 仿冒者攻击	配置接口状态为信任（Trusted）/不信任（Untrusted）
改变 CHADDR 值的 DoS 攻击	检查 DHCP 报文的 CHADDR 字段
仿冒 DHCP 续租报文攻击	检查 DHCP Request 报文是否匹配 DHCP Snooping 绑定表

版权所有 © 华为技术有限公司

攻击类型	DHCP Snooping 工作模式
DHCP 报文洪泛攻击	限制 DHCP 报文的上送速率

8.3.3 配置防止 DHCP Server 仿冒者攻击

为防止 DHCP 服务器仿冒者攻击，可使用 DHCP Snooping 的“信任（Trusted）/不信任（Untrusted）”工作模式。

建立配置任务

建立配置防止 DHCP Server 仿冒者攻击的配置任务。

应用环境

当网络中存在 DHCP Server 仿冒者时，DHCP Server 仿冒者回应给 DHCP Client 仿冒信息，如错误的网关地址、错误的 DNS 服务器、错误的 IP 等，从而使 Client 无法访问网络或访问到不正确的网络。

为了避免受到 DHCP Server 仿冒者的攻击，可以在 AC6605 上配置 DHCP Snooping 功能，把网络侧的接口配置为 Trusted 模式，把用户侧的接口配置为 Untrusted 模式，凡是从 Untrusted 接口收到的 DHCP Reply 报文全部丢弃。

同时为定位 DHCP Server 仿冒者，可以在 AC6605 上配置伪 DHCP Server 探测功能，通过检查 DHCP Reply 报文，获取 DHCP Server 相关信息，记入日志中，便于网络管理员进行网络维护。

前置任务

在配置防止 DHCP Server 仿冒者攻击之前，需要完成以下任务：

- 配置 DHCP Server。

数据准备

在配置防止 DHCP Server 仿冒者攻击之前，需要准备以下数据。

序号	数据
1	需要配置为 Trusted 模式的接口类型和编号

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

版权所有 © 华为技术有限公司

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

     如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。
- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

配置接口为信任状态

一般把通向 DHCP Server 的接口设成“信任（Trusted）”，其他接口都设为“不信任（Untrusted）”。配置接口状态后，从“不信任”接口收到的 DHCP Reply 报文被直接丢弃。

背景信息

使能接口的 DHCP Snooping 功能后，缺省情况下，接口为“不信任”状态。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

该接口为连接 DHCP Server 的网络侧接口。

步骤 3 接口视图下执行命令 **dhcp snooping trusted**，或者 VLAN 视图下执行命令 **dhcp snooping trusted interface** *interface-type interface-number*，配置接口为“信任”状态。

版权所有 © 华为技术有限公司

如果在 VLAN 视图下指定接口为“信任”状态，该接口必须已经加入了该 VLAN。

----结束

（可选）使能 DHCP Server 探测功能

为了定位 DHCP Server 仿冒者，可以在 AC6605 上配置伪 DHCP Server 探测功能，通过检查 DHCP Reply 报文，获取 DHCP Server 相关信息，记入日志中，便于网络管理员进行网络维护。使能 DHCP Server 探测功能前，必须使能 AC6605 全局和接口下的 DHCP Snooping 功能，否则 DHCP Server 探测功能不生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server detect**，使能 DHCP Server 探测功能。

缺省情况下，AC6605 没有使能 DHCP Server 探测功能。

----结束

检查配置结果

检查配置防止 DHCP Server 仿冒者攻击的结果。

前提条件

已完成防止 DHCP Server 仿冒者攻击的配置。

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。
- 使用命令 **display dhcp snooping interface** *interface-type interface-number* 查看接口下的 DHCP Snooping 信息。
- 使用命令 **display dhcp** { **snooping** | **static** } **user-bind** { **dai-status** | **interface** *interface-type interface-number* | **ip-address** *ip-address* | **ipsg-status** | **mac-address** *mac-address* | **vlan** *vlan-id* [**interface** *interface-type interface-number*] | **all** [**verbose**] }查看 DHCP 绑定表信息。
- 使用命令 **display dhcpv6** { **snooping** | **static** } **user-bind** { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **ipsg-status** | **mac-address** *mac-address* | **vlan** *vlan-id* [**interface** *interface-type interface-number*] | **all** [**verbose**] }查看 DHCPv6 绑定表信息。

----结束

8.3.4 配置防止改变 CHADDR 值的 DoS 攻击

防止攻击者通过改变 CHADDR 值攻击 DHCP Server。

建立配置任务

建立配置防止改变 CHADDR 值的 DoS 攻击的配置任务。

版权所有 © 华为技术有限公司

应用环境

如果攻击者改变的不是数据帧头部的源 MAC，而是通过改变 DHCP 报文中的 CHADDR（Client Hardware Address）值来不断申请 IP 地址，而 AC6605 仅根据数据帧头部的源 MAC 来判断该报文是否合法，那么 MAC 地址限制不能完全起作用，这样的攻击报文还是可以被正常转发。

为了避免受到攻击者改变 CHADDR 值的攻击，可以在 AC6605 上配置 DHCP Snooping 功能，检查 DHCP Request 报文中 CHADDR 字段。如果该字段跟数据帧头部的源 MAC 相匹配，转发报文；否则，丢弃报文。

前置任务

在配置防止改变 CHADDR 值的 DoS 攻击之前，需要完成以下任务：

- 配置 DHCP Server。

数据准备

在配置防止改变 CHADDR 值的 DoS 攻击之前，需要准备以下数据。

序号	数据
1	使能报文检查的接口类型和接口编号

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

版权所有 © 华为技术有限公司

如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。

- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

使能对报文的 CHADDR 值检查功能

把 DHCP Request 报文中携带的 CHADDR 字段与以太帧中的源 MAC 值相比较，如果不相同则认为是攻击报文，直接丢弃该报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

该接口为用户侧接口。

步骤 3 执行命令 **dhcp snooping check dhcp-chaddr enable** [**alarm dhcp-chaddr** { **enable** [**threshold** *threshold-value*] | **threshold** *threshold-value* }]，使能在接口下检查 DHCP 报文的 CHADDR 值与源 MAC 是否一致。

缺省情况下，AC6605 没有使能 CHADDR 值检查功能，丢弃 DHCP Request 报文告警的阈值为 100。

----结束

检查配置结果

检查配置防止改变 CHADDR 值的 DoS 攻击的结果。

前提条件

已完成防止改变 CHADDR 值的 DoS 攻击配置。

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。
- 使用命令 **display dhcp snooping interface** *interface-type interface-number* 查看接口下的 DHCP Snooping 信息。

----结束

8.3.5 配置防止仿冒 DHCP 续租报文攻击

防止攻击者通过仿冒 DHCP 续租报文攻击 DHCP Server。

版权所有 © 华为技术有限公司

建立配置任务

建立配置防止仿冒 DHCP 续租报文攻击的配置任务。

应用环境

如果攻击者通过不断发送 DHCP Request 报文来冒充用户续租 IP 地址，会导致一些到期的 IP 地址无法正常回收。

为了避免攻击者仿冒 DHCP 续租报文进行攻击，可以在 AC6605 上配置绑定表，检查 DHCP Request 报文的源 IP 地址、源 MAC 地址、VLAN 及接口是否与绑定表中的匹配，如果找到匹配的表项，则 DHCP Request 报文被正常转发。否则，报文被丢弃。

说明

IP 地址包括 IPv4 地址和 IPv6 地址，AC6605 对 DHCP Request 报文的源 IPv4 地址和源 IPv6 地址都会进行检查。

对 DHCP Request 报文的检查规则如下：

1. 首先检查报文的目的 MAC 是否是全 f，如果是则认为是第一次上线的 DHCP Request 广播报文，直接通过；如果报文的目的 MAC 不是全 f，则认为是续租报文，根据绑定表进行检查；
2. 检查报文中的 CHADDR 是否命中绑定表，如果没有命中，则认为是第一次上线，直接通过；如果 CHADDR 命中绑定表，则继续检查报文中的 VLAN、IP、接口信息是否均和绑定表匹配，完全匹配通过，否则丢弃。

前置任务

在配置防止仿冒 DHCP 续租报文攻击之前，需要完成以下任务：

- 配置 DHCP Server。
- 配置 DHCP Relay。

数据准备

在配置防止仿冒 DHCP 续租报文攻击之前，需要准备以下数据。

序号	数据
1	使能报文检查的接口类型和接口编号

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

版权所有 © 华为技术有限公司

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

     如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。
- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

使能 DHCP Request 报文检查功能

为了防止非法用户不断发送 DHCP Request 报文冒充合法用户续租 IP 地址，可以通过检查 DHCP 续租报文是否匹配绑定表，来决定是否转发该报文。

背景信息

对 DHCP 用户，使能 DHCP Snooping 功能后会自动生成绑定表；对静态分配 IP 地址的用户，需要手工配置静态绑定表。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

该接口应为用户侧接口。

步骤 3 执行命令 **dhcp snooping check dhcp-request enable** [**alarm dhcp-request** { **enable** [**threshold** *threshold-value*] | **threshold** *threshold-value* }]，使能接口对 DHCP Request 报文的检查功能，对接口接收到的报文进行检查。

缺省情况下，接口下没有使能 DHCP Request 报文检查功能，丢弃 DHCP Request 报文告警的阈值为 100。

----结束

版权所有 © 华为技术有限公司

（可选）配置 Option82 功能

使能 Option82 功能，可以根据 Option82 信息建立精确到接口的绑定表。从而避免 DHCP Server 仿冒者回应给 DHCP Client 仿冒信息。

操作步骤

- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     该接口为用户侧接口。
  3. 执行命令 **dhcp option82 insert enable**，使能 Option82 功能；或者执行命令 **dhcp option82 rebuild enable**，使能强制插入 Option82 功能。
     - 配置 **dhcp option82 insert enable** 后，如果原来的 DHCP 报文中没有 Option82 选项，则在 DHCP 报文中插入 Option82 选项；如果原来的 DHCP 报文中有 Option82 选项，则判断原选项是否有 Remote-id，如果有则不处理；如果没有，则插入 Remote-id，Remote-id 的内容默认为本设备的 MAC 地址。
     - 配置 **dhcp option82 rebuild enable** 后，如果原来的 DHCP 报文中没有 Option82 选项，则在 DHCP 报文中插入 Option82 选项；如果原来的 DHCP 报文中有 Option82 选项，则删除 DHCP 报文中原来的 Option82 选项，插入新的 Option82 选项。
- VLAN 视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 执行命令 **dhcp option82 insert enable interface** { *interface-name* | *interface-type interface-number* } [**to** *interface-number*]，使能 Option82 功能；或者执行命令 **dhcp option82 rebuild enable interface** { *interface-name* | *interface-type interface-number* } [**to** *interface-number*]，使能强制插入 Option82 功能。

     如果需要指定接口，需要保证该接口在步骤 2 的 VLAN 中。
     - 配置 **dhcp option82 insert enable interface** 后，如果原来的 DHCP 报文中没有 Option82 选项，则在 DHCP 报文中插入 Option82 选项；如果原来的 DHCP 报文中有 Option82 选项，则判断原选项是否有 Remote-id，如果有则不处理；如果没有，则插入 Remote-id，Remote-id 的内容默认为本设备的 MAC 地址。
     - 配置 **dhcp option82 rebuild enable interface** *interface-type interface-number* [**to** *interface-number*]后，如果原来的 DHCP 报文中没有 Option82 选项，则在 DHCP 报文中插入 Option82 选项；如果原来的 DHCP 报文中有 Option82 选项，则删除 DHCP 报文中原来的 Option82 选项，插入新的 Option82 选项。

----结束

（可选）配置 Option82 选项格式

用户可以在全局或接口下配置 Option82 的选项格式，如果接口下配置了 Option82 选项格式，以接口的配置为准；如果接口下没有配置 Option82 选项格式，以全局的配置为准。

版权所有 © 华为技术有限公司

操作步骤

- 系统视图下配置 Option82 选项格式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp option82** [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }，构造 Option82 的格式。

     缺省情况下，使用 **default** 格式上送 Option82。

     说明

     如果选择自定义 Option82 的格式（**user-defined**），建议在 *text* 中包含接口类型、槽号、端口号等必要的接口信息。
- 接口视图下配置 Option82 选项格式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dhcp option82** [**vlan** *vlanid*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }，构造 Option82 的格式。

     缺省情况下，使用 **default** 格式上送 Option82。

     说明

     如果选择自定义 Option82 的格式（**user-defined**），建议在 *text* 中包含接口类型、槽号、端口号等必要的接口信息。

----结束

（可选）配置在 DHCPv6 报文中插入 option18 或 option37 字段

当 DHCPv6 服务器需要获取客户端的接口或 MAC 地址信息时，AC6605 在客户端发送给 DHCPv6 服务器的 DHCPv6 Request 报文中可以插入 option18 或 option37 字段。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **dhcpv6** { **option18** | **option37** } **insert enable**，配置在 DHCPv6 报文中插入 option18 或 option37 字段。

其中，option18 字段包含了客户端的接口信息，option37 字段包含了客户端的 MAC 地址信息。

----结束

检查配置结果

检查配置防止仿冒 DHCP 续租报文攻击的结果。

前提条件

已完成防止仿冒 DHCP 续租报文攻击的配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。
- 使用命令 **display dhcp snooping interface** *interface-type interface-number* 查看接口下的 DHCP Snooping 信息。
- 使用命令 **display dhcp** { **snooping** | **static** } **user-bind** { **dai-status** | **interface** *interface-type interface-number* | **ip-address** *ip-address* | **ipsg-status** | **mac-address** *mac-address* | **vlan** *vlan-id* [**interface** *interface-type interface-number*] | **all** [**verbose**] }查看 DHCP 绑定表信息。
- 使用命令 **display dhcpv6** { **snooping** | **static** } **user-bind** { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **ipsg-status** | **mac-address** *mac-address* | **vlan** *vlan-id* [**interface** *interface-type interface-number*] | **all** [**verbose**] }查看 DHCPv6 绑定表信息。
- 使用命令 **display dhcp option82** { **interface** *interface-type interface-number* | **vlan** *vlan-id* }查看 Option82 的使能标记。

----结束

8.3.6 配置 DHCP Snooping 用户数限制

防止攻击者通过不断申请 IP 地址造成合法用户无法上线。

建立配置任务

建立配置 DHCP Snooping 用户数限制的配置任务。

应用环境

为了抑制用户恶意申请 IP 地址，可配置限制用户数的功能。

当用户数达到配置的最大用户数限制数量，任何用户将无法成功申请到 IP 地址。

前置任务

在配置用户数限制之前，需要完成以下任务：

- 全局使能 DHCP Snoopin 功能。
- 配置检查 DHCP Snooping 绑定表的功能。

数据准备

在配置用户数限制之前，需要准备以下数据。

序号	数据
1	接口类型和接口编号、VLAN 编号、限制的用户数数量

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

版权所有 © 华为技术有限公司

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

     如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。
- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

配置接入用户数限制

为了防止非法用户恶意申请 IP 地址，造成合法用户无法接入，可以配置接入用户数限制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp snooping global max-user-number** *max-user-number*，配置全局允许接入的最大用户总数。

缺省情况下，AC6605 所有接口允许接入的最大用户总数为 512。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 4 执行命令 **dhcp snooping max-user-number** *max-user-number*，配置接口或 VLAN 下允许接入的最大用户数。

版权所有 © 华为技术有限公司

缺省情况下，AC6605 接口或 VLAN 下允许接入的最大用户数为 1024。

如果同时在接口、VLAN 或全局配置了允许接入用户的最大数，它们共同生效。

----结束

（可选）配置接口下 MAC 安全功能

对于 DHCP 用户，用户上线后生成动态绑定表可转化为静态 MAC，报文可以被正常转发。对于静态用户，静态绑定表无法转化为静态 MAC，必须配置静态 MAC，报文才能正常转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

该接口为用户侧接口。

步骤 3 执行命令 **dhcp snooping sticky-mac**，配置接口下 DHCP Snooping 功能的 MAC 安全。

缺省情况下，AC6605 未使能 DHCP Snooping 功能的 MAC 安全。

本命令生效的前提是全局使能 DHCP Snooping 功能。

执行本命令后，接口接收到的 IP 报文首先被上送到主控板 CPU，在主控板 CPU 生成动态绑定表。生成动态绑定表后，在对应接口上下发静态 MAC，即将动态 MAC 转换成静态 MAC。静态 MAC 表项中包含用户的 MAC、VLAN 信息。后续只有源 MAC 与静态 MAC 匹配的报文才可以通过接口，否则报文会被丢弃。

说明

对于静态用户，静态绑定表不会下发静态 MAC，必须为静态用户**配置静态 MAC**。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 （可选）执行命令 **undo mac-address snooping** [*interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [*interface-type interface-number*]]，删除 **dhcp snooping sticky-mac** 命令转换的静态 MAC 信息。

----结束

检查配置结果

检查配置 DHCP Snooping 用户数限制的配置结果。

前提条件

已完成接入用户数限制配置。

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。
- 使用命令 **display dhcp snooping interface** *interface-type interface-number* 查看接口下的 DHCP Snooping 信息。

版权所有 © 华为技术有限公司

- 使用命令 **display mac-address snooping** [*interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [*interface-type interface-number*]] [**verbose**]查看通过执行 **dhcp snooping sticky-mac** 后 DHCP Snooping 表项转换成的静态 MAC 表项信息。

----结束

8.3.7 配置限制 DHCP 报文上送速率

防止攻击者发送大量的 DHCP Request 报文攻击 AC6605。

建立配置任务

建立配置限制 DHCP 报文上送速率的配置任务。

应用环境

如果网络中有攻击者不断地发送 DHCP 报文，会对 AC6605 的 DHCP 协议栈造成影响。

为了避免受到攻击者发送大量 DHCP 报文攻击，可以在 AC6605 上配置 DHCP Snooping 功能，检查 DHCP 报文，并限制报文的上送速率，在一定的时间内只允许规定数目的报文上送协议栈，多余的报文将被丢弃。

前置任务

在配置限制报文上送速率之前，需要完成以下任务：

- 配置 DHCP Server。
- 配置 DHCP Relay。

数据准备

在配置限制报文上送速率之前，需要准备以下数据。

序号	数据
1	DHCP 报文的上送速率限值

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

版权所有 © 华为技术有限公司

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

     如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。
- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

配置限制 DHCP 报文上送速率

用户可以在全局、VLAN 或接口下配置限制 DHCP 报文上送速率，如果在全局、VLAN 或接口下同时配置，有效的顺序为接口优先，VLAN 其次，最后为全局。

操作步骤

- 系统视图下配置限制 DHCP 报文上送速率
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp snooping check dhcp-rate enable**，全局使能 DHCP 报文的速率检查功能。

     缺省情况下，全局没有使能 DHCP 报文速率检查功能。
  3. 执行命令 **dhcp snooping check dhcp-rate** *rate*，全局配置 DHCP 报文的上送速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps（报文/秒）以内。超过此速率限制的 DHCP 报文会被丢弃。
  4. （可选）执行命令 **dhcp snooping check dhcp-rate alarm enable**，全局使能 DHCP 报文的速率检查告警功能。

     缺省情况下，不对 DHCP 报文上送到 DHCP 协议栈的速率检查产生告警。
  5. （可选）执行命令 **dhcp snooping check dhcp-rate alarm threshold** *threshold*，全局配置 DHCP 报文的速率检查告警阈值。

版权所有 © 华为技术有限公司

缺省情况下，DHCP 报文速率检查告警阈值为 100。当 DHCP 报文超过速率限制被丢弃的数目超过此阈值时，发出告警信息。

- VLAN 视图下配置限制 DHCP 报文上送速率
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 执行命令 **dhcp snooping check dhcp-rate enable**，在 VLAN 视图下使能 DHCP 报文的速率检查功能。

     缺省情况下，VLAN 视图下没有使能 DHCP 报文速率检查功能。
  4. 执行命令 **dhcp snooping check dhcp-rate** *rate*，在 VLAN 视图下配置 DHCP 报文的上送速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps（报文/秒）以内。超过此速率限制的 DHCP 报文会被丢弃。
- 接口视图下配置限制 DHCP 报文上送速率
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dhcp snooping check dhcp-rate** { **enable** | **enable** *rate* | *rate* } [**alarm dhcp-rate** [**enable**] [**threshold** *threshold-value*]]，可以在接口下同时配置以下功能。
     - 使能 DHCP 报文上送到 DHCP 协议栈的速率检查功能。
     - 配置 DHCP 报文上送到 DHCP 协议栈的检查速率。
     - 使能 DHCP 报文上送到 DHCP 协议栈的速率检查告警功能。
     - 配置 DHCP 报文上送到 DHCP 协议栈的速率检查的告警阈值。

     缺省情况下，在接口下 DHCP 报文上送到 DHCP 协议栈的速率检查功能未使能，检查速率为 100pps；DHCP 报文上送到 DHCP 协议栈的速率检查告警功能未使能，告警阈值为 100。

----结束

检查配置结果

检查配置限制 DHCP 报文上送速率的结果。

前提条件

已完成 DHCP Request 报文速率限制配置。

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。

----结束

任务示例

执行命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。

```
<Quidway> display dhcp snooping global
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
```


版权所有 © 华为技术有限公司

```
Dhcp snooping enable is configured at vlan :NULL

Dhcp snooping enable is configured at interface :
GigabitEthernet0/0/1

Dhcp snooping trusted is configured at interface :NULL

Dhcp option82 insert is configured at interface :
GigabitEthernet0/0/2

Dhcp option82 rebuild is configured at interface :NULL

Dhcp option82 insert is configured at vlan :NULL,,
Dhcp option82 rebuild is configured at vlan :NULL

dhcp packet drop count within alarm range : 0
dhcp packet drop count total : 0
```

8.3.8 配置丢弃报文告警功能

丢弃的报文数超过指定阈值时发出告警。

建立配置任务

建立配置丢弃报文告警功能的配置任务。

应用环境

配置 DHCP Snooping 功能后，AC6605 将丢弃攻击者发送的报文，其中攻击类型和丢弃报文种类的对应关系如表 8-2 所示：

表 8-2 攻击类型和丢弃报文种类的对应关系

攻击类型	丢弃报文类型
仿冒者攻击	Untrusted 接口收到的 DHCP Reply 报文
改变 CHADDR 值攻击	CHADDR 字段与源 MAC 地址不一致的 DHCP Request 报文
仿冒 DHCP 续租报文攻击	与绑定表不匹配的 DHCP Request 报文
发送大量 DHCP Request 报文	超出速率限制的报文

使能丢弃报文告警功能后，AC6605 丢弃报文的数量达到告警阈值后会产生告警信息。

前置任务

在配置报文相关告警功能之前，需要完成以下任务：

- 配置 DHCP Server。
- 配置 DHCP Relay。
- 配置丢弃用户侧 Untrusted 接口的 DHCP Reply 报文。
- 配置 DHCP Request 报文检查功能。

版权所有 © 华为技术有限公司

- 配置检查 DHCP Request 报文中的 CHADDR 字段功能。
- 配置检查 DHCP 报文的上送速率。

数据准备

在配置报文相关告警功能之前，需要准备以下数据。

序号	数据
1	丢弃报文后产生告警的阈值

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

     如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。
- 接口视图下使能 DHCP Snooping 功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **dhcp snooping enable**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

----结束

版权所有 © 华为技术有限公司

配置丢弃报文告警

使能告警功能后如果有对应的攻击，并且丢弃的攻击报文超过阈值，会有相应的告警信息出现。

背景信息

丢弃报文告警可以在全局和接口下配置。

- 全局的配置对所有接口都有效。
- 接口的配置只在指定接口下有效。如果接口下没有配置，则继承全局的配置值。

操作步骤

- 配置全局丢弃报文告警
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp snooping alarm threshold** *threshold*，配置全局丢弃报文的告警阈值。

     缺省情况下，全局丢弃报文数量的告警阈值为 100。
- 配置接口丢弃报文告警
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dhcp snooping check dhcp-chaddr enable** [**alarm dhcp-chaddr** [**enable** [**threshold** *threshold-value*] | **threshold** *threshold-value*]]，使能根据 DHCP Request 报文里的 CHADDR 字段检查 DHCP Request 报文的功能和丢弃 DHCP Request 报文的告警功能，配置接口下丢弃 DHCP Request 报文的告警阈值。

     缺省情况下，根据 DHCP Request 报文里的 CHADDR 字段检查 DHCP Request 报文的功能和 DHCP Request 报文丢弃告警功能均未使能。丢弃 DHCP Request 报文告警的阈值为 100。
  4. 执行命令 **dhcp snooping check dhcp-request enable** [**alarm dhcp-request** [**enable** [**threshold** *threshold-value*] | **threshold** *threshold-value*]]，使能检查 DHCP Request 报文功能和丢弃 DHCP Request 报文告警功能，配置接口下丢弃 DHCP Request 报文的告警阈值。

     缺省情况下，DHCP Request 报文检查功能和 DHCP Request 报文丢弃告警功能均未使能。丢弃 DHCP Request 报文告警的阈值为 100。
  5. （可选）执行命令 **dhcp snooping alarm** { **dhcp-chaddr** | **dhcp-reply** | **dhcp-request** } { **enable** [**threshold** *threshold*] | **threshold** *threshold* }，使能从非信任接口接收到 DHCP 报文的丢弃告警功能。

     缺省情况下，从非信任接口丢弃 DHCP 报文的告警功能未使能，丢弃 DHCP 报文告警阈值为 100。

     配置该命令后，AC6605 会丢弃以下类型的报文：
     - 与 DHCP Snooping 绑定表不匹配的 DHCP Request 报文
     - Untrusted 接口接收到的 DHCP Reply 报文。
     - 源 MAC 地址与 CHADDR 字段不匹配的 DHCP Request 报文。

----结束

版权所有 © 华为技术有限公司

检查配置结果

检查配置丢弃报文告警功能的结果。

前提条件

已完成报文丢弃告警配置。

操作步骤

- 使用命令 **display dhcp snooping global** 查看全局 DHCP Snooping 的信息。
- 使用命令 **display dhcp snooping interface** *interface-type interface-number* 查看接口下的 DHCP Snooping 配置信息。

----结束

8.3.9 维护 DHCP Snooping

复位、调试 DHCP Snooping。

清除 DHCP 的统计信息

清除 DHCP 统计信息包括清除全局和接口下的 DHCP 统计信息。

背景信息

清除统计信息后，以前的统计信息将无法恢复。

在确认需要 DHCP Snooping 报文丢弃计数后，请在用户视图下执行以下命令。

操作步骤

- 使用命令 **reset dhcp snooping statistics global** 清除全局的报文丢弃统计计数。
- 使用命令 **reset dhcp snooping statistics interface** *interface-type interface-number* 清除接口下的报文丢弃统计计数。
- 使用命令 **reset dhcp snooping statistics vlan** *vlan-id* 清除 VLAN 下的报文丢弃统计计数。

----结束

清除 DHCP Snooping 绑定表

配置了 DHCP Snooping 功能，DHCP 用户上线后会生成 DHCP Snooping 绑定表。用户可以根据 VLAN ID、接口、IP 地址批量删除动态绑定表项。

版权所有 © 华为技术有限公司

背景信息

说明

由于组网环境变化之后，DHCP Snooping 绑定表不会立即老化，而 DHCP Snooping 绑定表匹配的如下信息可能会发生变化，导致匹配出错。

- VLAN 信息在报文中的位置。
- 接口信息。

所以，请在变更组网环境之前手动清除所有 DHCP Snooping 绑定表项，使得设备根据新的网络环境生成新的 DHCP Snooping 绑定表。

在确认需要清除 DHCP Snooping 绑定表中的表项时，请在用户视图或系统视图下执行以下命令。

操作步骤

- 使用命令 **reset dhcp snooping user-bind** [[**vlan** *vlan-id* | **interface** *interface-type interface-number*]* | **ip-address** *ip-address* | **ipv6-address** *ipv6-address*]复位 DHCP Snooping 绑定表。

----结束

8.3.10 配置举例

介绍 DHCP Snooping 的配置举例。

配置防止 DHCP Server 仿冒者攻击示例

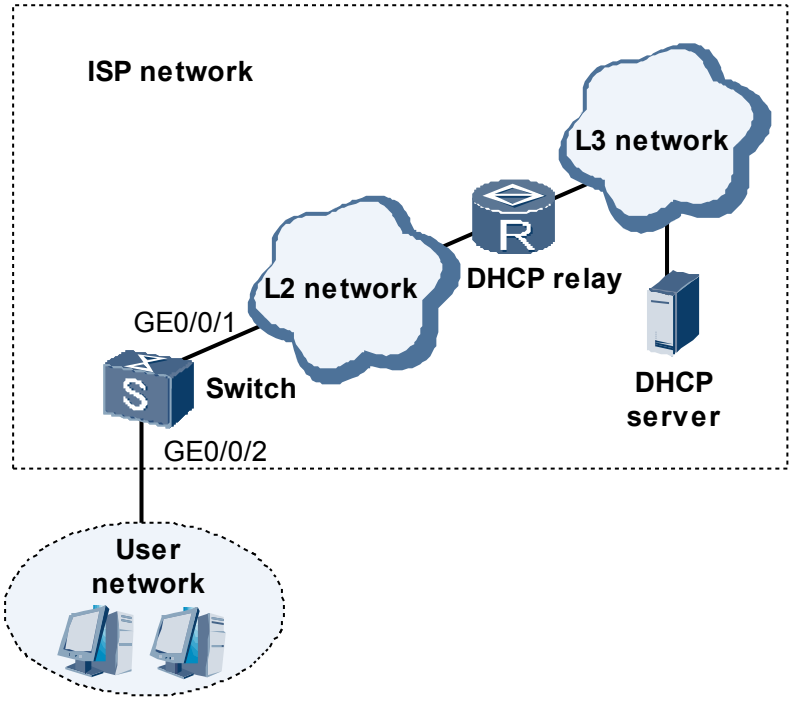
介绍防止 DHCP Server 仿冒者攻击的基本配置过程，包括配置信任接口、配置 DHCP Reply 报文丢弃告警功能。

组网需求

如图 8-10 所示，Switch 应用在用户网络和 ISP 的二层网络之间，为防止 DHCP Server 仿冒者攻击，要求在 Switch 上应用 DHCP Snooping 功能，把用户侧的接口配置为 Untrusted 模式，把运营商网络侧的接口配置为 Trusted 模式。同时配置 DHCP Reply 报文丢弃告警功能。

版权所有 © 华为技术有限公司

图 8-10 配置防止 DHCP Server 仿冒者攻击组网图



配置思路

采用如下的思路配置 DHCP Server 仿冒者攻击（假设 DHCP Server 已经配置完成）：

1. 使能全局和接口下的 DHCP Snooping 功能。
2. 使能伪 DHCP Server 探测功能。
3. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
4. 配置 DHCP Reply 报文丢弃告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 Trusted/Untrusted 模式：GE0/0/1 接口 Trusted，GE0/0/2 接口 Untrusted 模式。
- 发出告警的阈值：120。

说明

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

步骤 1 配置 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```


版权所有 © 华为技术有限公司

使能伪 DHCP Server 探测功能。

```
[Quidway] dhcp server detect
```

使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

配置用户侧的接口为 Untrusted 模式。

GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

步骤 3 配置 DHCP Reply 报文丢弃告警功能

使能对不信任端口收到的 DHCP Reply 报文丢弃告警功能，并配置告警阈值。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping alarm dhcp-reply enable threshold 120
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 4 验证配置结果

在 Switch 上执行 **display dhcp snooping global** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 GigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :
 GigabitEthernet0/0/1

 Dhcp option82 insert is configured at interface :NULL

 Dhcp option82 rebuild is configured at interface :NULL

 Dhcp option82 insert is configured at vlan :NULL

 Dhcp option82 rebuild is configured at vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 60


<Quidway> display dhcp snooping interface gigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0

<Quidway> display dhcp snooping interface gigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp packet dropped by untrust-reply checking = 10
```

----结束

版权所有 © 华为技术有限公司

配置文件

```
#
 dhcp enable
 dhcp snooping enable
 dhcp server detect
#
interface GigabitEthernet0/0/1
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
#
return
```

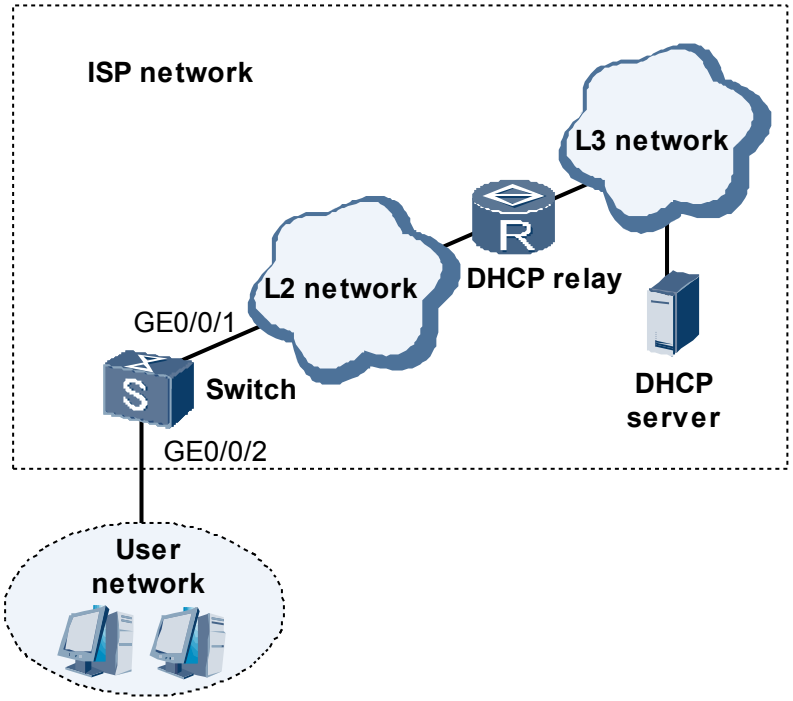
配置防止改变 CHADDR 值的 DoS 攻击示例

介绍防止改变 CHADDR 值的 DoS 攻击的基本配置过程，包括配置用户侧接口的 CHADDR 检查功能和告警功能。

组网需求

如图 8-11 所示，Switch 应用在用户网络和 ISP 的二层网络之间，为防止攻击者通过改变 CHADDR 值进行 DoS 攻击，要求在 Switch 上应用 DHCP Snooping 功能。检查 DHCP Request 报文中 CHADDR 字段，如果该字段跟数据帧头部的源 MAC 相匹配，便转发报文；否则丢弃报文。同时使能丢弃报文告警功能。

图 8-11 配置防止改变 CHADDR 值的 DoS 攻击组网图



配置思路

采用如下的思路配置防止攻击者通过改变 CHADDR 值攻击：

版权所有 © 华为技术有限公司

1. 使能全局和接口下的 DHCP Snooping 功能。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 在用户侧接口配置 CHADDR 值检查。
4. 配置告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 发出告警的阈值

说明

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

步骤 1 配置 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

配置用户侧的接口为 Untrusted 模式。

GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

步骤 3 配置用户侧接口的 CHADDR 检查功能，并配置告警功能和告警阈值。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable
threshold 120
```

步骤 4 验证配置结果

在 Switch 上执行 **display dhcp snooping global** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 GigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :
 GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 Dhcp option82 insert is configured at interface :NULL

 Dhcp option82 rebuild is configured at interface :NULL

 Dhcp option82 insert is configured at vlan :NULL

 Dhcp option82 rebuild is configured at vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 25

<Quidway> display dhcp snooping interface gigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
<Quidway> display dhcp snooping interface gigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp packet dropped by dhcp-chaddr checking = 25
 dhcp packet dropped by untrust-reply checking = 0
```

----结束

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
#
return
```

配置防止仿冒 DHCP 续租报文攻击示例

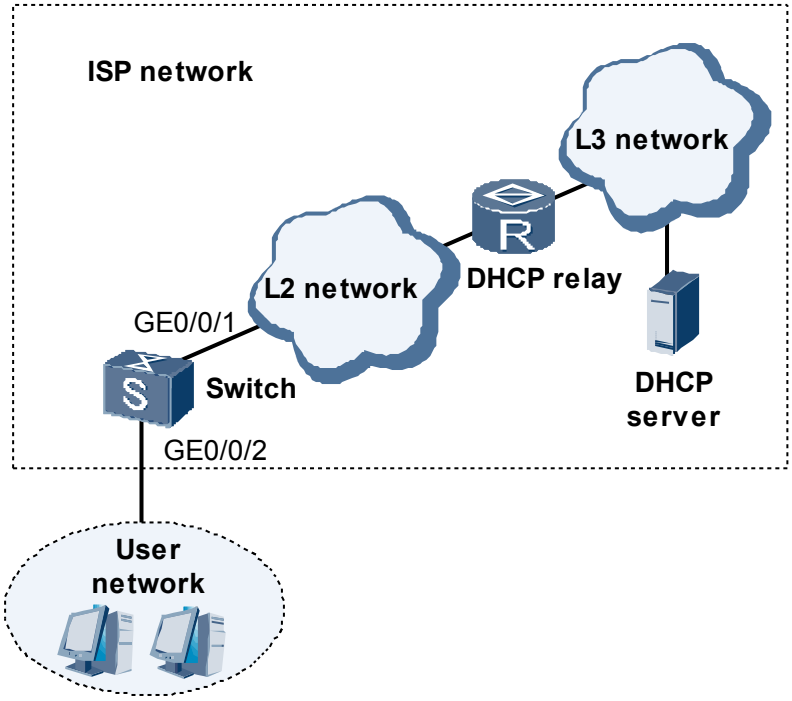
介绍防止仿冒 DHCP 续租报文攻击的基本配置过程，包括配置用户侧接口的 DHCP Request 报文检查功能和告警功能。

组网需求

如图 8-12 所示，Switch 应用在用户网络和 ISP 的二层网络之间。为防止攻击者仿冒 DHCP 续租报文，要求在 Switch 上应用 DHCP Snooping 功能，建立 DHCP Snooping 绑定表，检查接收到的 DHCP Request 报文，只有和绑定表中的内容一致的报文才被转发，否则将被丢弃。同时使能丢弃报文告警功能。

版权所有 © 华为技术有限公司

图 8-12 配置防止仿冒 DHCP 续租攻击组网图



配置思路

采用如下的思路配置防止攻击者仿冒 DHCP 续租报文攻击的示例：

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 使用 DHCP Snooping 绑定表工作模式，对 DHCP Request 报文进行匹配绑定检查。
4. 配置丢弃报文告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 各接口所属的 VLAN。
- 允许转发的静态 IP 地址。
- 发出告警的阈值。

说明

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

步骤 1 配置 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

配置用户侧的接口为 Untrusted 模式。

GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

步骤 3 配置报文检查功能，并配置告警功能和告警阈值

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping check dhcp-request enable alarm dhcp-request enable
threshold 120
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 4 查看动态绑定表

执行 **display dhcp snooping user-bind all** 命令可以看到所有 DHCP snooping 用户绑定表项。

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
-------------------------------------------------------------------------------
10.1.1.3         0000-005e-008a   3 /--  /--      GigabitEthernet0/0/2        2010.08.14-12:58
-------------------------------------------------------------------------------
print count:           1         total count:           1
```

步骤 5 验证配置结果

在 Switch 上执行 **display dhcp snooping global** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 GigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :NULL
 GigabitEthernet0/0/1
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 45

<Quidway> display dhcp snooping interface gigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
<Quidway> display dhcp snooping interface gigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
```


版权所有 © 华为技术有限公司

```
 dhcp packet dropped by dhcp-request checking = 45
 dhcp packet dropped by untrust-reply checking = 0
```

----结束

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
#
return
```

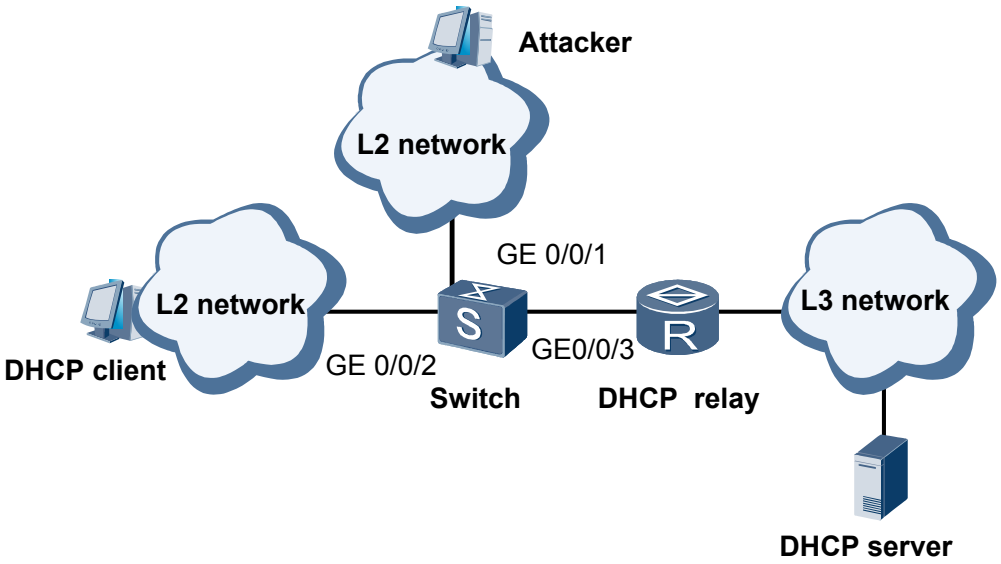
配置限制 DHCP 报文上送速率示例

介绍限制 DHCP 报文上送速率的基本配置过程，包括配置 DHCP 报文上送协议栈的速率和配置报文限速告警功能。

组网需求

当网络中存在攻击者通过大量发送 DHCP Request 或 Reply 报文进行攻击时，会造成 Switch 处理资源紧张，合法用户的请求得不到及时处理。如图 8-13 所示，为了防止大量发送 DHCP 报文的攻击，需要在 Switch 上配置 DHCP Snooping 功能，控制 DHCP 报文的上送速率，同时使能报文限速告警功能。

图 8-13 配置限制 DHCP 报文的上送速率组网图



配置思路

采用如下的思路配置防止攻击者发送大量 DHCP 报文攻击的示例：

版权所有 © 华为技术有限公司

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 在接口下配置 DHCP 报文上送协议栈的速率。
4. 在接口下配置报文限速告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- DHCP 报文的上送速率
- 发出告警的阈值

说明

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

步骤 1 配置 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

使能用户侧接口的 DHCP Snooping 功能。GigabitEthernet0/0/2、GE0/0/1 和 GigabitEthernet0/0/1 的配置步骤一样，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernetGigabitEthernet0/0/1] dhcp snooping enable
```

步骤 2 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet x0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

配置用户侧的接口为 Untrusted 模式。

GigabitEthernet0/0/1 接口和 GigabitEthernetGigabitEthernet0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

步骤 3 配置 DHCP 报文上送速率限制以及报文限速告警功能。

配置接口下 DHCP 报文上送速率限制以及报文限速告警功能。GigabitEthernet0/0/2、GE0/0/1 和 GigabitEthernet0/0/1 的配置步骤一样，此处省略。

```
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable
threshold 50
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 4 验证配置结果

在 Switch 上执行 **display dhcp snooping global** 命令，可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
[Quidway] display dhcp snooping global
 dhcp snooping enable
```


版权所有 © 华为技术有限公司

```
 Dhcp snooping enable is configured at these vlan :NULL

 Dhcp snooping enable is configured at these interface :
 GigabitEthernet0/0/1 GigabitEthernet0/0/2 GigabitEthernet0/0/1

 Dhcp snooping trusted is configured at these interface :
 GigabitEthernet0/0/1
 Dhcp option82 insert is configured at these interface :NULL

 Dhcp option82 rebuild is configured at these interface :NULL

 Dhcp option82 insert is configured at these vlan :NULL

 Dhcp option82 rebuild is configured at these vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
```

在 Switch 上执行 **display dhcp snooping interface** 命令，可以看到接口视图下 DHCP Snooping 的配置信息。

```
[Quidway] display dhcp snooping interface GigabitEthernet0/0/1
 dhcp snooping trusted
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
[Quidway] display dhcp snooping interface GigabitEthernet 0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
[Quidway] display dhcp snooping interface GigabitEthernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
```

----结束

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
return
```

配置在二层网络中应用 DHCP Snooping 示例

介绍二层网络中应用 DHCP Snooping 的基本配置过程，包括配置信任接口、配置对 DHCP 报文的检查功能、配置 DHCP 报文上送速率限制和配置 Option82 功能等。

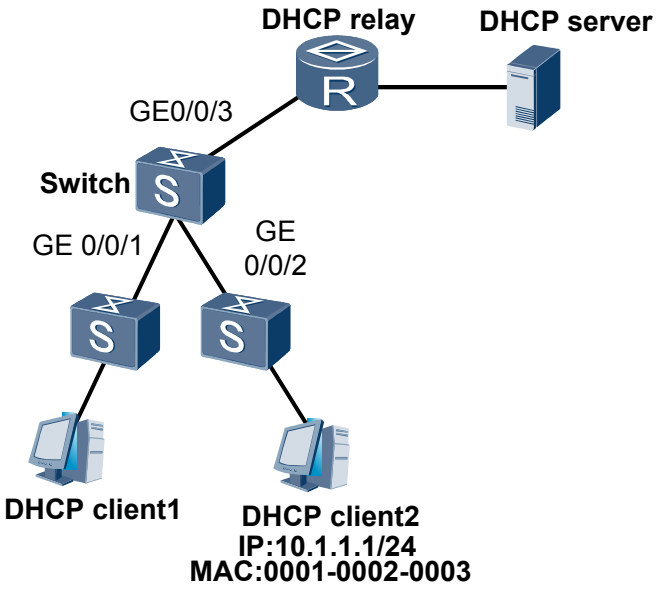
版权所有 © 华为技术有限公司

组网需求

如图 8-14 所示，DHCP Client 通过 VLAN10 接入 Switch。其中 DHCP Client1 使用动态分配的 IP 地址；DHCP Client2 使用静态分配的 IP 地址。要求在 Switch 的用户侧接口 GigabitEthernet0/0/1 和 GigabitEthernet0/0/2 上配置 DHCP Snooping 功能，以防止以下类型的攻击：

- DHCP Server 仿冒者攻击
- 改变 CHADDR 值的 DoS 攻击
- 仿冒 DHCP 续租报文攻击
- 大量发送 DHCP 请求报文

图 8-14 配置 DHCP Snooping 功能组网图



配置思路

采用如下的思路配置 DHCP Snooping 的基本功能：

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 配置 Trusted/Untrusted 接口，防止 DHCP Server 仿冒者攻击。
3. 配置 DHCP Snooping 绑定表，对 DHCP 请求报文进行匹配绑定检查，防止仿冒 DHCP 续租报文攻击。
4. 配置 CHADDR 值检查，防止改变 CHADDR 值的 DoS 攻击。
5. 配置 DHCP 报文上送协议栈的速率，防止 DHCP Reply 报文攻击。
6. 配置 Option82 功能。
7. 配置丢弃报文告警。

数据准备

为完成此配置举例，需要准备如下数据：

版权所有 © 华为技术有限公司

- 接口所属的 VLAN：VLAN 10。
- 接口的 Trusted/Untrusted 模式：GigabitEthernet0/0/2 为 Untrusted 模式，GE0/0/1 为 Trusted 模式。
- 允许转发的静态 IP 地址：10.1.1.1/24，对应的 MAC 地址：0001-0002-0003。
- DHCP 报文上送协议栈的速率：90。
- Option82 功能的模式：**insert**。
- 丢弃报文告警阈值：120。

说明

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

步骤 1 使能 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

使能用户侧接口的 DHCP Snooping 功能。以 GigabitEthernet0/0/1 接口为例，GigabitEthernet0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 2 配置 Trusted 接口

将连接 DHCP Server 侧的接口配置为“Trusted”，将连接 DHCP Clinet 侧的所有接口使能 DHCP Snooping（如果用户侧接口没有配置“Trusted”模式，那么使能了接口的 Snooping 特性后，接口模式默认为“Untrusted”），这样可以防止 DHCP Server 仿冒者攻击。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 3 配置对 DHCP 报文的检查，并配置告警功能。

在 DHCP Clinet 侧的接口配置进行 DHCP Request 报文检查和告警功能，这样可以防止仿冒 DHCP 续租报文的攻击。以 GigabitEthernet0/0/1 接口为例，GigabitEthernet0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-request enable alarm dhcp-request enable
threshold 120
```

在 DHCP Clinet 侧的接口配置进行 CHADDR 检查和告警功能，这样可以防止改变 CHADDR 值的 DoS 攻击。以 GigabitEthernet0/0/1 接口为例，GigabitEthernet0/0/2 的配置相同，此处省略。

```
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable
threshold 120
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 4 确认 DHCP 动态绑定表信息

在 Switch 上执行 **display dhcp snooping user-bind all** 命令可以看到 DHCP 动态绑定表信息。

版权所有 © 华为技术有限公司

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
-------------------------------------------------------------------------------
10.1.1.1         0001-0002-0003   10 /--  /--     GigabitEthernet0/0/2        2010.08.14-12:58
-------------------------------------------------------------------------------
print count:           1         total count:           1
```

步骤 5 配置 DHCP 报文上送速率限制

配置 DHCP 上送速率检查，这样可以防止 DHCP Request 报文攻击。

```
[Quidway] dhcp snooping check dhcp-rate enable
[Quidway] dhcp snooping check dhcp-rate 90
```

步骤 6 配置 Option82 功能

在 DHCP Client 侧接口配置 Option82 功能。以 GigabitEthernet0/0/1 接口为例，GigabitEthernet0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp option82 insert enable
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 7 配置告警功能

配置 DHCP Reply 报文丢弃告警功能。以 GigabitEthernet0/0/1 接口为例，GigabitEthernet0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-reply enable threshold 120
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 8 验证配置结果

在 Switch 上执行 **display dhcp snooping global** 命令可以看到全局已经使能 DHCP Snooping 功能，并查看告警的统计信息。

```
[Quidway] display dhcp snooping global
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90

 Dhcp snooping enable is configured at these vlan :NULL

 Dhcp snooping enable is configured at these interface :
 gigabitethernet0/0/1 gigabitethernet0/0/2

 Dhcp snooping trusted is configured at these interface :
 GigabitEthernet0/0/1

 Dhcp option82 insert is configured at these interface :
 gigabitethernet0/0/1 gigabitethernet0/0/2

 Dhcp option82 rebuild is configured at these interface :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
```

执行 **display dhcp snooping interface** 命令可以看到接口下的 DHCP Snooping 信息。

```
[Quidway] display dhcp snooping interface gigabitethernet 0/0/1
 dhcp snooping enable
 dhcp option82 insert enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
 dhcp packet dropped by dhcp-request checking = 0
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
```


版权所有 © 华为技术有限公司

```
 dhcp packet dropped by dhcp-chaddr checking = 0
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp packet dropped by untrust-reply checking = 0

[Quidway] display dhcp snooping interface gigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
```

执行 **display dhcp option82 interface** 命令可以查看接口下 Option82 的配置。

```
[Quidway] display dhcp option82 interface gigabitethernet 0/0/1
 dhcp option82 insert enable
```

----结束

配置文件

```
#
 dhcp enable
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90
#
 user-bind static ip-address 10.1.1.1 mac-address 0001-0002-0003 interface GigabitEthernet 0/0/2
vlan 10
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120
 dhcp option82 insert enable
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120
 dhcp option82 insert enable
#
interface GigabitEthernet0/0/1
 dhcp snooping trusted
#
return
```

8.4 ARP 安全配置

ARP 安全通过过滤不信任的 ARP 报文以及对某些 ARP 报文进行时间戳抑制来保证网络设备的安全性和健壮性。

8.4.1 ARP 安全概述

ARP 攻击是网络中最常见同时影响比较大的攻击方式，作为交换机的 AC6605 在离攻击源最近的位置，从设备级安全的角度提供 ARP 的防攻击方法。

在现今的网络中，Ethernet 是最常用的接入手段，而 ARP 协议作为 Ethernet 网络上的开放协议，由于本身过于简单和开放，没有任何的安全手段，为恶意用户的攻击提供了可能。

ARP 攻击类型

ARP 的攻击方式多种多样。

版权所有 © 华为技术有限公司

- 按照攻击对象可以分为针对主机的攻击和针对设备的攻击。
- 按照攻击触发源可以分为来自病毒的攻击或者来自非法软件的人为攻击。
- 按照攻击影响可以分为：
  - 地址欺骗型的攻击

    地址欺骗攻击主要包括：
    - 用错误的主机 MAC 地址刷新网关的 ARP 缓存，导致主机无法上线。
    - 向主机发送错误的 ARP 应答，使主机得到错误的网关地址，导致主机无法上线。
  - DOS（Denial of Service）攻击
    - 从空间方面，攻击主要利用设备 ARP 缓存的有限性，通过发送大量伪造的 ARP 请求、应答报文，造成设备的 ARP 缓存溢出，从而无法缓存正常的 ARP 表项，进而阻碍正常转发。
    - 从时间方面，攻击主要利用设备计算能力的有限性，通过发送大量伪造的 ARP 请求、应答报文或其他能够触发设备 ARP 处理的报文（比如攻击者利用工具扫描本网段主机或者跨网段进行扫描时，设备在发送回应报文前，会查找 ARP 表项，如果目的 IP 地址对应的 MAC 地址不存在，会导致设备的 ARP 模块向上层软件发送 ARP Miss 消息，要求上层软件发送 ARP 请求报文以获得目的端的 MAC 地址，大量的扫描报文会导致大量的 ARP Miss 消息。），造成设备的计算资源长期忙于 ARP 报文处理，影响其他业务的处理，进而阻碍正常转发。

  欺骗攻击的防范措施往往只能针对非法用户，仿造合法用户报文造成的大量的 DOS 攻击是当前影响比较大的攻击方式。

ARP 攻击影响

如果是主机遭受 ARP 攻击，该主机无法上线，网关信息被篡改或者被窃取。

如果接入交换机遭受 ARP 攻击，可能导致局域网内多用户甚至大量用户无法上线。

如果路由器遭受 ARP 攻击，由于路由器一般下接多个交换机，结果是更多的用户无法上线。

ARP 防攻击策略

从造成的影响看，防攻击越靠近攻击源进行防范，代价越小，效果越佳。

- 对于主机的防攻击，由于造成的影响比较小，可以通过在主机上安装守护程序的方法来解决，如果守护程序发现网关 MAC 地址被欺骗就清除本机 ARP 缓存，并重发 ARP 请求。
- 对于路由器的防攻击，目前双向绑定、主动防御等大部分的 ARP 防攻击的技术都可以在路由器上实施 ARP 防攻击。但是由于路由器是整个局域网的出口，而 ARP 攻击是以整个局域网为目标，当 ARP 攻击包已经达到路由器的时候，影响已经造成。所以由路由器来承担防御 ARP 攻击的任务并不能很好的解决问题。
- 对于交换机的防攻击，由于任何 ARP 包，都必须经由交换机转发，才能达到被攻击目标，只要交换机不接受非法的 ARP 报文，非法报文的攻击就不可能产生。

双向绑定等防 ARP 攻击方法可以防范非法用户的上线，属于防欺骗攻击的范畴，相关的措施一般在攻击发生前进行，但是伪造合法用户的 DOS 攻击往往会造成大量用户下线，影响范围更大。而且在攻击发生后才能发现，所以在大部分的网络中会默认使能限速或者 CAR 等用于预防此类攻击的产生。如果攻击仍然产生，根据具体的情况，可以通过网络监控等方式发现后通过指定目标限速、隔离等方法来解决。

版权所有 © 华为技术有限公司

作为交换机的 AC6605 可以起到良好的 ARP 防攻击的作用。

AC6605 的 ARP 防攻击定位

层次化网络安全分为业务级安全、网络级安全和设备级安全。业务级安全依赖于业务本身的安全机制、无阻塞可靠网络的建设；网络级的安全依赖于网络流量区分隔离，配合客户终端和安全控制服务器，精细监控；设备级安全依赖于基本的设备高可靠性。在 ARP 防攻击领域，AC6605 聚焦于设备级的网络安全。

8.4.2 AC6605 支持的 ARP 安全特性

AC6605 支持的 ARP 安全特性包括 ARP 表项限制、防止 ARP 地址欺骗、防止 ARP 网关冲突、ARP 报文源抑制、ARP Miss 消息源抑制、防止 ARP 中间人攻击、ARP 报文速率限制。

ARP 表项限制

可以配置严格学习 ARP 表项，使 AC6605 只学习自己发送的 ARP 请求的回应报文。

可以配置接口可以学习到的最大动态 ARP 表项数目，以防止恶意用户占用 ARP 表项资源造成 AC6605 无法学习合法用户的 ARP 表项。

防止 ARP 地址欺骗

ARP 地址欺骗指的是攻击者通过伪造其他用户发出的 ARP 报文，篡改设备上的用户 ARP 表项，造成其它合法用户的网络中断。

AC6605 可以通过以下两种方法防御此类攻击。

- 固定 MAC 地址：AC6605 第一次学习到 ARP 表项之后不再允许通过 ARP 学习来修改 MAC 地址，直到此 ARP 表项老化之后才允许更新，以保护合法用户的 ARP 表项不被修改。

  固定 MAC 地址有两种方式：Fixed-mac 和 Fixed-all。Fixed-mac 方式下，不允许修改 MAC 地址，但是允许修改 VLAN 和接口信息；Fixed-all 方式下，MAC、VLAN 和接口信息都不允许修改。
- 主动确认：AC6605 收到一个涉及表项中 MAC 地址信息修改的 ARP 报文时，不会立即修改 ARP 表项，而是先对原 ARP 表中与此 MAC 地址对应的用户发一个单播确认，根据确认结果再决定是否修改。

防止 ARP 网关冲突

ARP 网关冲突指攻击者仿冒网关地址，在局域网内部发送源 IP 地址是网关地址的免费 ARP 报文。主机接收到该报文后，会修改自己原来的网关地址为攻击者的地址，最终导致局域网内部所有主机无法访问网络。

AC6605 收到与网关地址冲突的 ARP 报文时，如果存在下列情况之一：

- ARP 报文的源 IP 与报文入接口的 IP 地址相同；
- VRRP（Virtual Router Redundancy Protocol）虚 MAC 方式时，ARP 报文的源 IP 是入接口的虚拟 IP 地址，但 ARP 报文源 MAC 不是 VRRP 虚 MAC。

则系统生成 ARP 防攻击表项，在后续一段时间（默认 3 分钟）内直接丢弃该报文，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

版权所有 © 华为技术有限公司

为了防止网络中主机的报文不能被正常转发到网关或者被恶意攻击者窃听，AC6605 支持主动发送免费 ARP 报文的功能，定时更新主机 ARP 表项中的网关地址为正确的网关地址。

ARP 报文源抑制

某个源 IP 地址、MAC 地址发送大量 ARP 报文，浪费设备的 CPU 资源和给 ARP 报文上送预留的有限带宽。

AC6605 具有针对源 IP 地址和源 MAC 地址的 ARP 报文速率抑制的功能。在一段时间内，如果 AC6605 收到某一源 IP 地址或者源 MAC 的 ARP 报文数目超过设定阈值，则不处理超出阈值部分的 ARP 请求报文。

AC6605 支持基于源 MAC 地址的 ARP 抑制。

ARP Miss 消息源抑制

主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备。

对此类攻击，AC6605 提供对 ARP Miss 消息基于源 IP 地址的抑制。如果一个源 IP 地址向 AC6605 发送了目标 IP 地址不能解析的 IP 报文，就会触发 ARP Miss 消息，AC6605 对上报的 ARP Miss 消息进行统计。如果一个源 IP 地址在一定时间内不断触发 ARP Miss，而且其触发速率超过了设定的阈值，则认为此 IP 地址在进行攻击。对于前 16 个攻击源，AC6605 将下发 ACL 规则，在后续的一段时间内（默认为 50 秒）把这个地址发出的 IP 报文丢弃；对于之后的攻击源，AC6605 使用设定的阈值对 IP 报文进行抑制。

防止 ARP 中间人攻击

当网络中存在中间人攻击时，中间人仿冒服务器，向客户端发送带有自己的 MAC 和服务器 IP 的报文，让客户端学到中间人的 IP 和 MAC，达到仿冒服务器的目的。然后，中间人向服务器发送带有自己的 MAC 和客户端 IP 的报文，让服务器学到中间人的 IP 和 MAC，达到仿冒客户端的目的。这样攻击者就可以获得服务器和客户端的数据。

为了避免受到中间人攻击，可以在 AC6605 上配置 ARP 报文的检查功能(EAI,Egress ARP Inspection)，对接收到的 ARP 报文进行绑定表匹配检查，只有报文的信息和绑定表中的内容一致才会被转发，否则报文将被丢弃。

ARP 报文和 ARP Miss 消息速率限制

基于全局、接口或 VLAN 对 ARP 报文或 ARP Miss 消息进行限速，防止上送安全模块检查的 ARP 报文或 ARP Miss 消息过多，对系统性能造成影响。

8.4.3 配置 ARP 报文源 MAC 地址检查功能

ARP 头源 MAC 和以太头源 MAC 地址不一致的 ARP 报文大多数情况下都是攻击报文，配置对这类报文的检查和丢弃功能可以防范这类的攻击。

应用环境

ARP 报文进入 AC6605 后，系统会首先自动对 ARP 报文的有效性进行检查，包括但不限于：

- 报文长度检查

版权所有 © 华为技术有限公司

- 以太头的源 MAC 合法性检查
- ARP 请求、回应类型检查
- 硬件地址长度检查
- 协议地址长度检查
- ARP 帧格式是否为以太类型检查

这些检查是用来判断是否与协议一致，过滤无效报文。其中 ARP 头源 MAC 和以太头源 MAC 地址不匹配的 ARP 报文是协议允许的 ARP 报文，但是在现网应用中，该类报文很可能是攻击报文，配置了 **arp anti-attack packet-check sender-mac** 命令后，系统会检查 ARP 头源 MAC 和以太头源 MAC 地址是否匹配，如果不匹配，则丢弃该报文，可以防止此类报文的攻击产生。

ARP 头源 MAC 和以太头源 MAC 地址不一致的 ARP 报文在协议里面定义的是有效报文，但是在实际的组网中这种报文很多情况下都是攻击报文。AC6605 提供了命令行控制是否进行该类报文的检查，如果满足条件就删除该报文，配置灵活。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack packet-check sender-mac**，启动对 ARP 头源 MAC 和以太头源 MAC 地址不匹配的 ARP 报文的检查功能，如果不匹配，丢弃该报文。

----结束

8.4.4 配置防 ARP DOS 攻击

大量 ARP 攻击报文会造成 MAC 地址表项溢出或者 CPU 资源占用过高，AC6605 可以针对不同的报文类型进行丢弃、限速等操作防范 ARP DOS 攻击。

建立配置任务

建立配置任务主要介绍了防 ARP DOS 攻击的应用场景、前置条件和数据准备，为后期的配置提供整体背景和相关准备。

应用环境

产生 ARP DOS 攻击的报文包括 ARP 请求应答报文、ARP Miss 报文、免费 ARP 报文，表 8-3 分析了不同报文类型的产生过程、子场景和 AC6605 对应的处理措施，提供了不同的解决方法，增强网络抗击 ARP DOS 攻击的能力。

版权所有 © 华为技术有限公司

表 8-3 ARP 防 DoS 攻击的场景和处理方法

报文类型	攻击产生场景	AC6605 的处理方法
ARP 请求应答报文	● 攻击者发送大量的 ARP 请求应答报文，造成 AC6605 设备 CPU 资源占用过高和 ARP 表项溢出。	整体的思路是抑制此类报文，具体措施包括： ● 基于源 MAC 地址、源 IP 地址对 ARP 报文进行限速。 ● 在全局、VLAN 下或者接口下进行 ARP 限速。 ● 限制接口能够学习到的最大动态 ARP 表项数目，抑制攻击端口接收的 ARP 请求应答报文更新 ARP 表项。
ARP Miss 报文	攻击者使用大量的找不到目的 MAC 地址扫描 IP 报文攻击 AC6605，造成 AC6605 产生大量的 ARP Miss 报文，生成 ARP 临时表项。	AC6605 针对该类攻击的处理方法包括： ● 基于源 MAC 地址、源 IP 地址对 ARP Miss 报文进行限速。 ● 基于不同的视图进行 ARP Miss 限速。
免费 ARP 报文	免费 ARP 是用于帮助作为网关的 AC6605 及时向 VLAN 内的主机更新 MAC 地址信息，防止对主机网关 MAC 地址的恶意篡改。 但是，如果攻击者伪造大量的免费 ARP 报文可能造成 AC6605 设备 CPU 资源占用过高	AC6605 针对该类攻击的处理方法是当判断出该类攻击后，配置 AC6605 丢弃免费 ARP 报文。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 防 DoS 攻击攻击功能之前，需要准备以下数据。

序号	数据
1	ARP 请求应答报文的源抑制地址、限速值
2	（可选）ARP 报文限速丢弃告警阈值
3	ARP Miss 报文的源抑制地址、限速值
4	（可选）ARP Miss 消息限速丢弃告警阈值

版权所有 © 华为技术有限公司

配置 ARP 报文的源 MAC 地址抑制

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp speed-limit source-mac maximum** *maximum*，配置基于源 MAC 地址的 ARP 报文源抑制速率。

步骤 3 执行命令 **arp speed-limit source-mac** [*mac_addr*] **maximum** *maximum*，配置指定 MAC 地址用户的 ARP 报文源抑制速率。

对指定了 MAC 地址的用户，ARP 报文源抑制速率为步骤 3 中配置的 *maximum* 值；其它 MAC 地址的 ARP 报文源抑制速率为步骤 2 中配置的 *maximum* 值。

缺省情况下，所有 MAC 地址的 ARP 报文源抑制速率为 0pps，即不对 ARP 报文进行源抑制。

----结束

配置 ARP 报文源 IP 地址抑制

背景信息

考虑到某些特定的用户有特别的需求，在对 ARP 报文进行源 IP 地址抑制时，可以针对该用户的 IP 地址配置不同于其他 IP 地址的 ARP 报文抑制速率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp speed-limit source-ip maximum** *maximum*，配置 ARP 报文源 IP 地址抑制速率。

步骤 3 执行命令 **arp speed-limit source-ip** *ip-address* **maximum** *maximum*，配置指定 **source-ip** 用户的 ARP 报文源 IP 地址抑制速率。

对指定了 **source-ip** 的用户，ARP 报文源 IP 地址抑制速率为步骤 3 中配置的 *maximum* 值；其它 IP 地址的 ARP 报文源抑制速率为步骤 2 中配置的 *maximum* 值。

缺省情况下，所有 IP 地址的 ARP 报文抑制速率为 500pps。

----结束

配置 ARP Miss 消息源抑制

背景信息

考虑到某些特定的用户有特别的需求，对于该用户的 IP 地址可以配置不同于其他 IP 地址的 ARP Miss 抑制速率。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp-miss speed-limit source-ip maximum** *maximum*，配置 ARP Miss 消息源抑制速率。

步骤 3 （可选）执行命令 **arp-miss speed-limit source-ip** [*ip-address* [**mask** *mask*]] **maximum** *maximum* [**none-block** | **block timer** *timer*]，配置指定 **source-ip** 用户的 ARP Miss 源抑制速率。

完成上述配置后，对指定了 **source-ip** 的用户，ARP Miss 源抑制速率为步骤 3 中配置的 *maximum* 值；其它 IP 地址的 ARP Miss 源抑制速率为步骤 2 中配置的 *maximum* 值。

如果将速率配置为 0，则表示不作 ARP Miss 源抑制。缺省情况下，所有 IP 地址的 ARP Miss 源抑制速率为 500pps。

如果该端口指定 IP 地址的 ARP Miss 达到速率后 AC6605 会下发一条 ACL 丢弃触发 ARP Miss 的 IP 报文，50 秒的老化时间后撤销该 ACL。

----结束

配置 ARP Miss 消息速率抑制

背景信息

如果全局、VLAN 或接口在一定时间内不断上报 ARP Miss 消息，使得设备由于忙于发送广播 ARP 请求而性能下降。ARP Miss 消息的抑制功能是对上报的 ARP Miss 消息进行统计，并将超过限速值的 ARP Miss 消息丢弃的过程。

操作步骤

- 系统视图下配置 ARP Miss 消息速率抑制功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp-miss anti-attack rate-limit enable**，全局使能 ARP Miss 消息速率抑制功能。

     缺省情况下，全局未使能 ARP Miss 消息速率抑制功能。
  3. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在系统视图下配置 ARP Miss 消息的限速时间和限速值。

     配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。
  4. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，全局使能 ARP Miss 消息限速丢弃告警功能。

     缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。
  5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在系统视图下配置 ARP Miss 消息限速丢弃告警阈值。

     缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。
- VLAN 视图下配置 ARP Miss 消息速率抑制功能

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
3. 执行命令 **arp-miss anti-attack rate-limit enable**，在 VLAN 视图下使能 ARP Miss 消息速率抑制功能。

   缺省情况下，VLAN 视图下未使能 ARP Miss 消息速率抑制功能。
4. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在 VLAN 视图下配置 ARP Miss 消息的限速时间和限速值。

   配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。
5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，在 VLAN 视图下使能 ARP Miss 消息限速丢弃告警功能。

   缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。
6. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在 VLAN 视图下配置 ARP Miss 消息限速丢弃告警阈值。

   缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

- 接口视图下配置 ARP Miss 消息速率抑制功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **arp-miss anti-attack rate-limit enable**，在接口视图下使能 ARP Miss 消息速率抑制功能。

     缺省情况下，接口视图下未使能 ARP Miss 消息速率抑制功能。
  4. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在接口视图下配置 ARP Miss 消息的限速时间和限速值。

     配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。
  5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，在接口视图下使能 ARP Miss 消息限速丢弃告警功能。

     缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。
  6. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在接口视图下配置 ARP Miss 消息限速丢弃告警阈值。

     缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

----结束

配置 ARP 报文速率抑制

操作步骤

- 系统视图下配置 ARP 报文速率抑制功能
  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **arp anti-attack rate-limit enable**，全局使能 ARP 报文速率抑制功能。

   缺省情况下，全局未使能 ARP 报文速率抑制功能。

3. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在系统视图下配置 ARP 报文的限速时间和限速值。

   配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。

4. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，全局使能 ARP 报文限速丢弃告警功能。

   缺省情况下，未使能 ARP 报文限速丢弃告警功能。

5. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在系统视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

- VLAN 视图下配置 ARP 报文速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
3. 执行命令 **arp anti-attack rate-limit enable**，在 VLAN 视图下使能 ARP 报文速率抑制功能。

   缺省情况下，VLAN 视图下未使能 ARP 报文速率抑制功能。

4. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在 VLAN 视图下配置 ARP 报文的限速时间和限速值。

   配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。

5. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，在 VLAN 视图下使能 ARP 报文限速丢弃告警功能。

   缺省情况下，未使能 ARP 报文限速丢弃告警功能。

6. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在 VLAN 视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

- 接口视图下配置 ARP 报文速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **arp anti-attack rate-limit enable**，在接口视图下使能 ARP 报文速率抑制功能。

   缺省情况下，接口视图下未使能 ARP 报文速率抑制功能。

4. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在接口视图下配置 ARP 报文的限速时间和限速值。

   配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。

5. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，在接口视图下使能 ARP 报文限速丢弃告警功能。

版权所有 © 华为技术有限公司

缺省情况下，未使能 ARP 报文限速丢弃告警功能。

6. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在接口视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

----结束

配置发送 ARP 免费报文

通过配置发送免费 ARP 报文，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

背景信息

该报文使用网关的 IP 地址作为目标地址发送 ARP 请求，定时更新用户 ARP 表项的网关 MAC 地址，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

当 AC6605 作为网关时，可以在全局或 VLANIF 接口下发送免费 ARP 报文。当全局和 VLANIF 接口下都使能发送免费 ARP 功能时，VLANIF 接口下的配置优先生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **arp gratuitous-arp send enable**，使能发送免费 ARP 报文的功能。

缺省情况下，发送免费 ARP 报文的功能未使能。

步骤 4 （可选）执行命令 **arp gratuitous-arp send interval** *interval-time*，配置发送免费 ARP 报文的时间间隔。

缺省情况下，系统发送免费 ARP 报文的时间间隔为 60 秒。

----结束

检查配置结果

前提条件

已完成 ARP 防攻击的配置。

操作步骤

- 使用命令 **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **log-trap-timer** | **packet-check** | **all** }和 **display arp anti-attack configuration check user-bind interface** *interface-type interface-number* 查看当前 ARP 防攻击配置。

----结束

任务示例

执行命令 **display arp anti-attack configuration all**，可以查看当前所有 ARP 防攻击配置。

版权所有 © 华为技术有限公司

```
<Quidway> display arp anti-attack configuration all
 ARP anti-attack packet-check function: disable

 ARP gateway-duplicate anti-attack function: disabled

 ARP anti-attack log-trap-timer: 0 seconds
 (The log and trap timer of speed-limit, default is 0 and means disabled.)

 ARP anti-attack entry-check mode:
 Vlanif      Mode
-------------------------------------------------------------------------------
 All         disabled
-------------------------------------------------------------------------------

 ARP rate-limit configuration:
-------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
 Vlan configuration:
-------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
-------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
 Vlan configuration:
-------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 All                 0
-------------------------------------------------------------------------------
 0 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 All                 5
-------------------------------------------------------------------------------
 0 specified IP addresses are configured, spec is 256 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 All                 5
-------------------------------------------------------------------------------
 0 specified IP addresses are configured, spec is 256 items.
```

执行命令 **display arp anti-attack configuration arp-speed-limit**，可以查看 ARP 报文源抑制的抑制速率。

```
<Quidway> display arp anti-attack configuration arp-speed-limit
 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 10.0.0.20           400
 Others              0
 ------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 256 items.
```

执行命令 **display arp anti-attack configuration arpmiss-speed-limit**，可以查看 ARP Miss 消息源抑制的抑制速率。

```
<Quidway> display arp anti-attack configuration arpmiss-speed-limit
 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 10.0.0.30           400
```


版权所有 © 华为技术有限公司

```
Others              0
------------------------------------------------------------------------------
1 specified IP addresses are configured, spec is 256 items.
```

8.4.5 配置防 ARP 欺骗攻击

ARP 表项攻击、网关攻击、中间人攻击是 ARP 欺骗攻击的主要应用场景，AC6605 针对这三个场景可以进行针对性的防攻击。

建立配置任务

建立配置任务主要介绍了防 ARP 欺骗攻击的应用场景、前置条件和数据准备，为后期的配置提供整体背景和相关准备。

应用环境

如表 8-4 所示，AC6605 针对不同 ARP 欺骗攻击的场景，提供了不同的解决方法，增强网络抗击 ARP 欺骗攻击的能力。

表 8-4 ARP 防欺骗攻击的场景和处理方法

场景名称	场景产生过程	AC6605 的处理方法
ARP 表项自我保护	ARP 欺骗攻击一般都是通过修改 ARP 表项来完成的。	增强 ARP 表项的自我保护功能，AC6605 提供了如下的处理方法： ● 严格地址学习：AC6605 只学习自己发送的 ARP 请求报文的应答报文 ● 防地址欺骗：通过固定 ARP 表项的 MAC 地址、接口、VLAN 等信息，或者确认机制，保证 ARP 表项的相对稳定。 ● DHCP 触发 ARP 学习：当 DHCP 服务器给用户分配 IP 地址时，AC6605 回应用户 DHCP ACK 报文成功后，会取用户的 MAC 地址，生成该 IP 地址对应的 ARP 表项。这样可以省掉 AC6605 学习用户主机 ARP 的过程,避免攻击者通过 ARP 报文对 ARP 表项的攻击。
网关冲突	攻击者仿冒网关地址，发送 ARP 报文头的源 IP 地址是网关地址的 ARP 报文，从而使主机修改网关的 MAC 地址为攻击者的 MAC 地址，需要发送给原来网关的报文就发送给攻击者了。	配置作为网关的 AC6605 丢弃 ARP 报文头的源 IP 地址是自己 IP 地址的 ARP 报文。 但是这种防攻击策略只能适用于所有主机的 ARP 报文必须通过网关转发的场景。

版权所有 © 华为技术有限公司

场景名称	场景产生过程	AC6605 的处理方法
防中间人攻击	中间人攻击会同时修改主机和网关的信息。 ● 修改主机上的网关信息：攻击者仿冒网关地址，发送 ARP 报文头的源 IP 地址是网关地址的 ARP 报文，使主机修改网关的 MAC 地址为攻击者的MAC 地址 ● 修改网关上的主机信息：攻击者仿冒主机地址，发送 ARP 报文头的源 IP 地址是主机地址的 ARP 报文，使网关修改主机的 MAC 地址为攻击者的 MAC 地址	在 AC6605 上配置绑定表，将 ARP 报文与绑定表进行对比，不符合的丢弃该报文。目前 AC6605 只支持 DHCP Snooping 的绑定表。 但是这种防攻击策略只能适用于所有主机的 ARP 报文必须通过网关转发的场景。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 防欺骗攻击功能之前，需要准备以下数据。

序号	数据
1	ARP 地址防欺骗的方式
2	防中间人攻击中与 DHCP Snooping 绑定表匹配检查方式
3	（可选）ARP 报文检查不匹配丢弃报文告警阈值

配置严格学习 ARP 表项

背景信息

严格学习 ARP 表项指的是 AC6605 只学习自己发送的 ARP 请求报文的应答报文。

操作步骤

- 配置全局严格学习 ARP 表项
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp learning strict**，配置严格学习 ARP 表项。

版权所有 © 华为技术有限公司

缺省情况下，严格学习 ARP 表项功能处于使能状态。

- 配置 VLANIF 接口严格学习 ARP 表项功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入 VLANIF 接口视图。
  3. 执行命令 **arp learning strict** { **force-enable** | **force-disable** | **trust** }，配置 VLANIF 接口的 ARP 严格学习功能。
     - **force-enable** 表示使能 VLANIF 接口的 ARP 严格学习功能。
     - **force-disable** 表示去使能 VLANIF 接口的 ARP 严格学习功能。
     - **trust** 表示 VLANIF 接口的 ARP 严格学习功能与全局配置保持一致。

     缺省情况下，VLANIF 接口的 ARP 严格学习功能和全局配置保持一致。

----结束

配置基于接口的 ARP 表项限制

背景信息

为了防止攻击者占用大量 ARP 表项资源，造成 AC6605 学习不到合法用户的 ARP 表项，可以配置接口能够学习到的最大动态 ARP 表项数目。

操作步骤

- 配置接口的 ARP 表项限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 在非 VLANIF 接口下，执行命令 **arp-limit** [**vlan** *vlan-id1* [**to** *vlan-id2*]] **maximum** *maximum*，在 VLANIF 接口视图下，执行命令 **arp-limit maximum** *maximum* 配置基于接口的 ARP 表项限制。

     当在非 VLANIF 接口下配置时，必须指定 **vlan** *vlan-id1*。

----结束

配置防止 ARP 地址欺骗

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，使能 ARP 地址防欺骗功能。

只能同时使能一种 ARP 地址防欺骗方式。如果原来使能了某一种方式，则新配置的方式将覆盖原来配置的方式。

缺省情况下，AC6605 未使能 ARP 地址防欺骗功能。

----结束

版权所有 © 华为技术有限公司

配置防止 ARP 网关冲突

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack gateway-duplicate enable**，使能 ARP 网关冲突防攻击功能。

ARP 网关冲突防攻击功能使能后，系统生成 ARP 防攻击表项，在后续一段时间内对收到具有相同源 MAC 地址的报文直接丢弃，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

说明

防止 ARP 网关冲突功能仅仅在攻击所在单板生效。

----结束

配置防止 ARP 中间人攻击

背景信息

防止 ARP 中间人攻击，可以配置 ARP 报文检查功能，对接口或 VLAN 下收到的 ARP 报文和绑定表进行匹配检查，当报文的检查项和绑定表中的特征项一致时，转发该报文，否则丢弃报文。

同时可以配置告警功能，当丢弃的报文数超过限制的阈值时，发出告警信息。

说明

对 DHCP 用户，使能 DHCP Snooping 功能后会自动生成绑定表；对静态分配 IP 地址的用户，需要手工配置静态绑定表。绑定表的内容包括用户的 IP 地址、MAC 地址、VLAN、接口等信息。

DHCP Snooping 的配置，请参见使能 DHCP Snooping 功能；静态绑定表的配置，请参见**（可选）配置静态用户绑定表**。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **arp anti-attack check user-bind enable**，使能 ARP 报文检查功能。

缺省情况下，接口或 VLAN 未使能对 ARP 报文的检查功能。

步骤 4 接口视图下执行命令 **arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **vlan** }*，或者 VLAN 视图下执行命令 **arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **interface** }*，配置 ARP 报文检查方式。

缺省情况下，对 IP 地址、MAC 地址、VLAN 和接口都进行检查。对检查项不匹配绑定表的报文做丢弃处理。

说明

ARP 报文检查方式对配置了静态绑定表的用户不起作用，该用户依然按照静态绑定表检查报文。

版权所有 © 华为技术有限公司

步骤 5 （可选）接口视图下执行命令 **arp anti-attack check user-bind alarm enable**，使能 ARP 报文检查丢弃报文告警功能。

缺省情况下，接口未使能丢弃 ARP 报文告警功能。

注意

请不要在 VLAN 和接口下同时配置 **arp anti-attack check user-bind enable**，否则将导致 ARP 报文检查丢弃报文告警功能失效。

步骤 6 （可选）接口视图下执行命令 **arp anti-attack check user-bind alarm threshold** *threshold*，配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

缺省情况下，ARP 报文不匹配绑定表而丢弃的告警阈值为 100。

----结束

配置 DHCP 触发 ARP 学习

背景信息

配置 DHCP 触发 ARP 学习，当 DHCP 服务器给用户分配 IP 地址，AC6605 回应用户 DHCP ACK 报文成功后，会取用户的 MAC 地址，生成该 IP 地址对应的 ARP 表项。这样可以省掉设备学习用户主机 ARP 的过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*，进入 Vlanif 接口视图。

步骤 3 执行命令 **arp learning dhcp-trigger**，配置 AC6605 根据 Vlanif 接口上收到的 DHCP ACK 报文生成 ARP 表项，同时丢弃查询该接口网段目的主机的 ARP 请求报文。

缺省情况下，AC6605 收到 DHCP ACK 报文不生成 ARP 表项。当有流量通过时，才触发学习 ARP。

说明

- 本命令生效的前提是使能 DHCP Snooping 功能和 Vlanif 接口下使能 DHCP Relay 功能。
- 如果 DHCP 用户与 DHCP 服务器在相同网段，不能配置本命令。
- 在 VRRP 和 DHCP Relay 组合场景下，VRRP 主备设备上都不能再配置 DHCP Snooping 功能和 **arp learning dhcp-trigger** 命令。

----结束

检查配置结果

前提条件

已完成 ARP 防攻击配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **log-trap-timer** | **packet-check** | **all** }和 **display arp anti-attack configuration check user-bind interface** *interface-type interface-number* 查看当前 ARP 防攻击配置。
- 使用命令 **display arp anti-attack gateway-duplicate item** 查看当前网络中存在的网关地址冲突攻击信息。

----结束

任务示例

执行命令 **display arp anti-attack configuration all**，可以查看当前所有 ARP 防攻击配置。

```
<Quidway> display arp anti-attack configuration all
 ARP anti-attack packet-check function: disable

 ARP gateway-duplicate anti-attack function: disabled

 ARP anti-attack log-trap-timer: 0 seconds
 (The log and trap timer of speed-limit, default is 0 and means disabled.)

 ARP anti-attack entry-check mode:
 Vlanif      Mode
------------------------------------------------------------------------------
 All         disabled
------------------------------------------------------------------------------

 ARP rate-limit configuration:
------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
 Vlan configuration:
------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
 Vlan configuration:
------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 All                 0
------------------------------------------------------------------------------
 0 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 All                 5
------------------------------------------------------------------------------
 0 specified IP addresses are configured, spec is 256 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 All                 5
------------------------------------------------------------------------------
 0 specified IP addresses are configured, spec is 256 items.
```

执行命令 **display arp anti-attack gateway-duplicate item**，可以查看当前网络中存在的网关地址冲突攻击信息。

版权所有 © 华为技术有限公司

```
<Quidway> display arp anti-attack gateway-duplicate item
 interface                  IP address       MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 GigabitEthernet0/0/1    2.1.1.1          0000-0000-0002  2        150
 GigabitEthernet0/0/1    2.1.1.1          0000-0000-0004  2        160
--------------------------------------------------------------------------------
There are 2 records in gateway conflict table
```

8.4.6 维护 ARP 安全

查看、清除 ARP 报文的统计信息，清除 ARP 丢弃报文计数以及调试 ARP 报文。

查看 ARP 报文统计信息

通过 **display** 命令查看 ARP 报文的统计信息。

操作步骤

- 使用命令 **display arp packet statistics** 查看 ARP 报文的统计信息。

----结束

任务示例

执行命令 **display arp packet statistics**，可以查看 ARP 报文的统计信息。

```
<Quidway> display arp packet statistics
ARP Pkt Received:   sum  199992
ARP-Miss Msg Received:   sum      0
ARP Learnt Count:   sum      4
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum      0
ARP Pkt Discard For Proxy Suppress:   sum      0
ARP Pkt Discard For Other:   sum  18220
ARP-Miss Msg Discard For SpeedLimit:   sum      0
ARP-Miss Msg Discard For Other:   sum      0
```

清除 ARP 报文统计信息

通过 **reset** 命令清除 ARP 报文统计信息。

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 使用命令 **reset arp packet statistics** 清除 ARP 报文的统计信息。

----结束

版权所有 © 华为技术有限公司

清除 ARP 丢弃报文计数

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 使用命令 **reset arp anti-attack statistics rate-limit** 清除由于 ARP 报文速率超过限制阈值造成的丢弃计数。

----结束

调试 ARP 报文信息

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现运行故障时，请在用户视图下执行下面的 debugging 命令进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

- 使用命令 **debugging arp packet** [**slot** *slot-id* | **interface** *interface-type interface-number*]调试 ARP 报文。
- 使用命令 **debugging arp process** [**slot** *slot-id* | **interface** *interface-type interface-number*]调试报文的处理过程。

----结束

配置对潜在的 ARP 攻击行为发送告警

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack log-trap-timer** *time*，配置对潜在的攻击行为发送告警的时间间隔。

版权所有 © 华为技术有限公司

对潜在的攻击行为发送告警功能针对所有的 IP 地址。

time 为发送告警时间间隔。缺省情况下该值为 0，表示未使能发送告警功能。

----结束

8.4.7 配置举例

介绍 ARP 安全功能的配置举例。

配置 ARP 安全功能示例

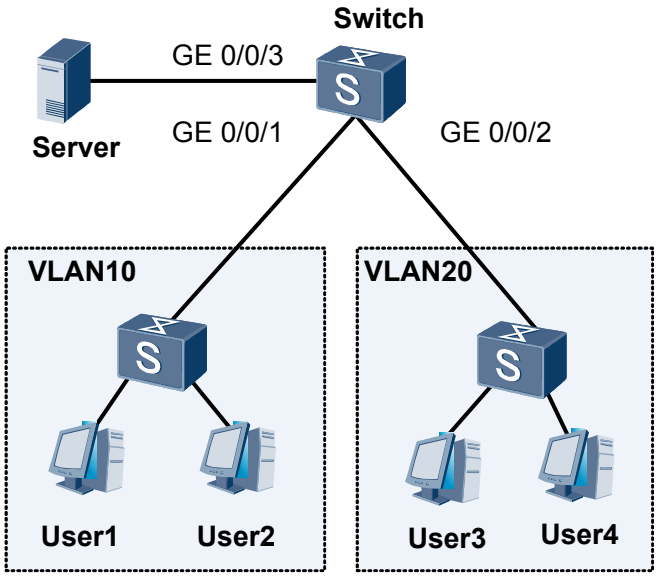
组网需求

如图 8-15 所示，Switch 通过 GE0/0/3 接口连接一台服务器，通过 GE0/0/1 和 GE0/0/2 接口连接 VLAN10 和 VLAN20 下的四个用户。网络中存在的 ARP 威胁是：

- 服务器可能会发出一些目的 IP 地址不可达的报文，而且这种报文相对其他普通用户的报文要多。
- 用户 User1 中病毒后，会发出大量 ARP 攻击报文，部分 ARP 报文的源 IP 地址在本网段内不停变化，部分 ARP 报文的源 IP 地址和网关 IP 地址相同。
- 用户 User3 构造大量源 IP 地址固定的 ARP 报文对网络进行攻击。
- 用户 User4 发送大量目的 IP 不可达的 IP 报文对网络进行攻击。

要求在 Switch 配置 ARP 的安全功能，能够防止以上的攻击。对 Server，需要配置其 ARP Miss 源抑制的速率比其他用户大。

图 8-15 配置 ARP 安全功能组网图



配置思路

采用如下思路配置 ARP 的安全功能：

版权所有 © 华为技术有限公司

1. 配置严格学习 ARP 表项。
2. 配置基于接口的 ARP 表项限制。
3. 配置防止 ARP 地址欺骗攻击。
4. 配置防止 ARP 网关冲突攻击。
5. 配置 ARP 报文源抑制。
6. 配置 ARP Miss 源抑制。
7. 配置对潜在的攻击行为写日志和发送告警。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 ARP 表项限制：20 个。
- 防止 User1 发起的 ARP 地址欺骗攻击方式为 **fixed-mac**。
- 服务器 IP 地址：2.2.2.2/24。
- 发出大量 ARP 报文的 User4 的地址：2.2.4.2/24。
- ARP 报文速率源抑制阈值：User4 为 10pps，其他用户为 15pps。
- ARP Miss 源抑制阈值：普通用户为 20pps，对 Server 为 50pps。
- 对潜在的攻击行为写日志和发送告警的时间间隔为 300 秒。

操作步骤

步骤 1 配置严格学习 ARP 表项

```
<Quidway> system-view
[Quidway] arp learning strict
```

步骤 2 配置基于接口的 ARP 表项限制

各个接口的 ARP 表项限制为 20，以 GE0/0/1 为例，其他接口配置步骤相似。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] arp-limit vlan 10 maximum 20
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 3 配置防止 ARP 地址欺骗攻击

配置 ARP 地址欺骗防攻击方式为 **fixed-mac** 方式，防止 User1 发起的 ARP 地址欺骗攻击。

```
[Quidway] arp anti-attack entry-check fixed-mac enable
```

步骤 4 配置防止 ARP 网关冲突攻击

使能 ARP 网关冲突防攻击功能，防止 User1 发起的伪造网关地址攻击。

```
[Quidway] arp anti-attack gateway-duplicate enable
```

步骤 5 配置 ARP 报文源抑制

配置 User4 发送的 ARP 报文速率抑制阈值为 10pps。为防止所有用户误发过多 ARP 报文，配置系统的 ARP 报文速率抑制阈值为 15pps。

```
[Quidway] arp speed-limit source-ip maximum 15
[Quidway] arp speed-limit source-ip 2.2.4.2 maximum 10
```


版权所有 © 华为技术有限公司

步骤 6 配置 ARP Miss 源抑制

配置系统的 ARP Miss 源抑制阈值为 20pps，以防止较大流量目的 IP 地址不可达的 IP 报文的攻击。

```
[Quidway] arp-miss speed-limit source-ip maximum 20
```

配置 Server 的 ARP Miss 源抑制阈值为 50pps，这样既防止 Server 无意发起大流量目的 IP 地址不可达的 IP 报文的攻击；又防止在其发送的目的 IP 地址不可达的 IP 报文速率并非特别大的时候，就阻止了它的网络通信。

```
[Quidway] arp-miss speed-limit source-ip 2.2.2.2 maximum 50
```

步骤 7 配置对潜在的攻击行为写日志和发送告警

```
[Quidway] arp anti-attack log-trap-timer 300
```

步骤 8 验证配置结果

配置完成后，可以使用命令 **display arp learning strict**，查看 ARP 严格学习情况。

```
<Quidway> display arp learning strict
 The global configuration:arp learning strict
 interface                          LearningStrictState
--------------------------------------------------------------
--------------------------------------------------------------
 Total:0
 force-enable:0
 force-disable:0
```

可以使用命令 **display arp-limit** 查看接口可以学习 ARP 数目的最大值。

```
<Quidway> display arp-limit interface gigabitethernet 0/0/1
 interface                    LimitNum   VlanID     LearnedNum(Mainboard)
------------------------------------------------------------------------------
 GigabitEthernet0/0/1         20         10         0
------------------------------------------------------------------------------
 Total:1
```

可以使用命令 **display arp anti-attack configuration all** 查看当前 ARP 防攻击配置情况。

```
<Quidway> display arp anti-attack configuration all
 ARP anti-attack entry-check mode: fixed-MAC

 ARP gateway-duplicate anti-attack function: enabled

 ARP anti-attack log-trap-timer: 15seconds
 (The log and trap timer of speed-limit, default is 0 and means disabled.)

ARP rate-limit configuration:
------------------------------------------------------------------------------
 Globle configuration:
 Interface configuration:
 Vlan configuration:
------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
------------------------------------------------------------------------------
 Globle configuration:
 Interface configuration:
 Vlan configuration:
------------------------------------------------------------------------------

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 2.2.4.2             10
 Others              15
 ------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
 1 specified IP addresses are configured, spec is 1024 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 2.2.2.2             50
 Others              20
 ------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 1024 items.
```

可以使用命令 **display arp packet statistics** 查看丢弃的 ARP 报文数目和学习到的 ARP 表项。同时，还可以通过 **display arp anti-attack gateway-duplicate item** 命令查看当前网络中存在的网关地址冲突攻击信息。

```
<Quidway> display arp packet statistics
ARP Pkt Received:   sum    167
ARP Learnt Count:   sum      8
ARP Pkt Discard For Limit:   sum      5
ARP Pkt Discard For SpeedLimit:   sum      0
ARP Pkt Discard For Other:   sum      3
<Quidway> display arp anti-attack gateway-duplicate item
 interface               IP address       MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 GigabitEthernet0/0/1    2.1.1.1          0000-0000-0002  2        153
 GigabitEthernet0/0/2    2.1.1.2          0000-0000-0004  2        179
--------------------------------------------------------------------------------
There are 2 records in gateway conflict table
```

----结束

配置文件

```
#
 sysname Quidway
#
vlan batch 10 20 30
#
 arp speed-limit source-ip maximum 15
 arp-miss speed-limit source-ip maximum 20
 arp learning strict
 arp anti-attack log-trap-timer 300
#
 arp anti-attack entry-check fixed-mac enable
 arp anti-attack gateway-duplicate enable
 arp-miss speed-limit source-ip 2.2.2.2 maximum 50
 arp speed-limit source-ip 2.2.4.2 maximum 10
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid tagged vlan 10
 arp-limit vlan 10 maximum 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid tagged vlan 20
 arp-limit vlan 20 maximum 20
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
 arp-limit vlan 30 maximum 20
#
return
```

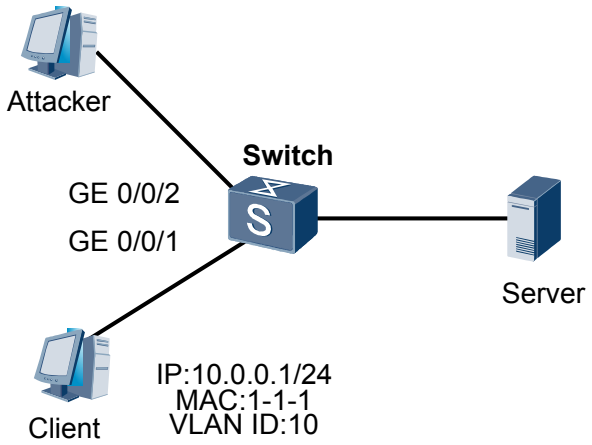
配置防止 ARP 中间人攻击示例

版权所有 © 华为技术有限公司

组网需求

如图 8-16 所示，Switch 的 GE0/0/1 和 GE0/0/2 接口连接了两个用户。假设 GE0/0/2 接口连接的用户是一个攻击者。为了防止 ARP 中间人攻击，要求在 Switch 上配置 ARP 报文检查功能，只有接收到的 ARP 报文信息和绑定表中的内容一致才会被转发，否则报文将被丢弃。同时使能丢弃报文告警功能。

图 8-16 配置防止 ARP 中间人攻击组网图



配置思路

采用如下的思路配置防止 ARP 中间人攻击：

1. 使能 ARP 报文检查功能。
2. 配置对 ARP 报文匹配检查。
3. 配置静态绑定表。
4. 使能丢弃报文告警功能。

数据准备

为完成此配置举例，需要准备以下数据：

- 使能报文检查的接口：GE0/0/1、GE0/0/2。
- 匹配检查项：“IP 地址+MAC 地址+VLAN”。
- ARP 报文检查丢弃告警阈值：80。
- 静态绑定表绑定 Client 的的 IP 地址：10.0.0.1/24，MAC 地址：1-1-1，VLAN ID：10。

操作步骤

步骤 1 配置 ARP 报文检查功能

在连接 Client 的 GE0/0/1 接口使能 ARP 报文检查功能。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind check-item ip-address mac-address
```


版权所有 © 华为技术有限公司

```
vlan
[Quidway-GigabitEthernet0/0/1] quit
```

在连接 Attacker 的 GE0/0/2 接口使能 ARP 报文检查功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind enable
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind check-item ip-address mac-address
vlan
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置报文丢弃告警功能

在连接 Client 的 GE0/0/1 接口配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm threshold 80
[Quidway-GigabitEthernet0/0/1] quit
```

在连接 Attacker 的 GE0/0/2 接口配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind alarm enable
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind alarm threshold 80
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 3 配置静态绑定表项

配置 Client 为静态绑定表项。

```
[Quidway] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
GigabitEthernet 0/0/1 vlan 10
```

步骤 4 验证配置结果

执行 **display arp anti-attack configuration check user-bind interface** 命令可以查看接口下 ARP 报文检查配置信息。

```
<Quidway> display arp anti-attack configuration check user-bind interface gigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
 arp anti-attack check user-bind check-item ip-address mac-address vlan
ARP packet drop count = 0
 <Quidway> display arp anti-attack configuration check user-bind interface gigabitethernet 0/0/2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 ARP packet drop count = 2442
```

由显示信息可知，GE0/0/1 接口下没有丢弃 ARP 报文，GE0/0/2 接口下产生了 ARP 报文丢弃计数。针对 Attacker 的防攻击功能已经生效。

----结束

配置文件

```
#
vlan batch 10
#
  user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface GigabitEthernet 0/0/1
vlan 10
#
interface GigabitEthernet0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address vlan
```


版权所有 © 华为技术有限公司

```
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
#
interface GigabitEthernet0/0/2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
#
return
```

8.5 IP 源防攻击配置

介绍防止针对 IP 源进行攻击的原理和配置方法。

8.5.1 IP 源防攻击概述

简要介绍 IP 源防攻击的原理。

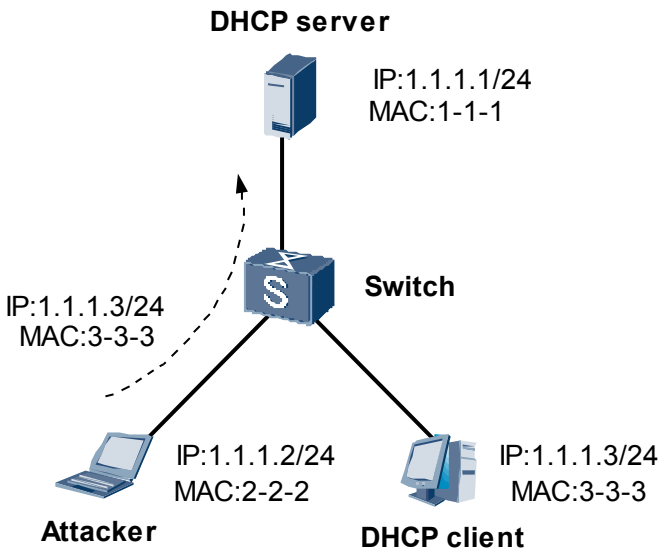
网络中常常存在针对 IP 源地址进行欺骗的攻击行为，如攻击者仿冒合法用户发送 IP 报文给服务器，或者伪造其他用户的源 IP 地址进行通信，从而导致合法用户不能正常获得网络服务。针对此类攻击，AC6605 提供了 IP Source Guard 的功能。

IP Source Guard

IP Source Guard 用于对接口转发的 IP 报文进行过滤，防止非法报文通过接口，提高了接口的安全性。

当网络中存在攻击者向服务器发送带有合法用户 IP 和 MAC 的报文，令服务器误以为已经学到这个合法用户的 IP 和 MAC，但真正的合法用户不能从服务器获得服务。如图 8-17 所示。

图 8-17 IP/MAC 欺骗攻击示意图



为了防止此类攻击，可以在 AC6605 上配置 IP Source Guard 功能，对进入接口的 IP 报文进行绑定表匹配检查，报文的信息和绑定表一致，允许其通过，否则丢弃报文。

版权所有 © 华为技术有限公司

8.5.2 AC6605 支持的 IP 源防攻击特性

介绍 IP 源防攻击特性在 AC6605 中的支持情况。

IP Source Guard

IP Source Guard 的主要功能是对用户的 IP 报文进行绑定表匹配检查，报文的检查项可以是：源 IP 地址、源 MAC 地址、VLAN 和接口。并且 AC6605 支持这几项的任意组合作为检查项，如在接口视图下支持：

- IP+MAC
- IP+VLAN
- IP+MAC+VLAN
- ……

在 VLAN 视图下支持：

- IP+MAC
- IP+Interface
- IP+MAC+Interface
- ……

AC6605 提供两种绑定机制：

- 对 DHCP 用户，使能 DHCP Snooping 功能后会动态生成绑定表。
- 对静态分配 IP 地址的用户，通过命令行配置静态绑定表。

DHCP Snooping 的相关配置，请参见 **8.3 DHCP Snooping 配置**。

8.5.3 配置 IP Source Guard

介绍 IP Source Guard 的原理和配置方法，并给出配置举例。

建立配置任务

应用环境

通过在 AC6605 上配置 IP Source Guard 功能，对接收到的 IP 报文进行绑定表匹配检查，只有 IP 报文的信息和绑定表中的内容一致才会被转发，否则报文将被丢弃。

数据准备

在配置 IP Source Guard 功能之前，需要准备以下数据。

序号	数据
1	（可选）需要配置静态绑定表的用户信息：IPv4 地址或 IPv6 地址、MAC 地址、VLAN、接口

版权所有 © 华为技术有限公司

序号	数据
2	使能 IP Source Guard 功能的接口类型和接口编号
3	IP 报文检查告警阈值。

（可选）配置静态用户绑定表

背景信息

对于静态分配 IP 地址的用户，在转发数据前 AC6605 不会自动学习用户的 MAC 地址，也不能建立绑定关系表，所以需要手动建立绑定关系表。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-bind static** { { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]，配置静态用户绑定表项。

----结束

使能 IP Source Guard 功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

该接口为用户侧接口。

步骤 3 执行命令 **ip source check user-bind enable** 使能 IP 报文检查功能。

缺省情况下，AC6605 接口下没有使能 IP 报文检查功能。

----结束

配置 IP 报文检查选项

背景信息

使能 IP 报文检查功能后，AC6605 对进入接口或 VLAN 的 IP 报文进行绑定表匹配检查，检查项目可以是源 IPv4 地址、源 IPv6 地址、MAC 地址、VLAN 或接口。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

该接口为用户侧接口。

步骤 3 接口视图下执行命令 **ip source check user-bind check-item** { **ip-address** | **mac-address** | **vlan** }*，或者 VLAN 视图下执行命令 **ip source check user-bind check-item** { **ip-address** | **mac-address** | **interface** }*，配置 IP 报文检查项。

如果接口收到 IP 报文，根据配置的检查项，用报文中的源 IPv4 地址、源 MAC 地址、VLAN 或其组合去匹配绑定表，如果匹配则报文被正常转发，不匹配则该报文就被丢弃。

缺省情况下，IP 报文检查选项包括 IPv4 地址、IPv6 地址、MAC 地址、VLAN 和接口信息。

说明

本命令只对动态绑定表生效，对静态绑定表不生效。

----结束

（可选）配置 IP 报文检查告警功能

配置了 IP 报文检查告警功能之后，AC6605 会将单位时间超过阈值的 IP 报文的个数进行累加，当总数超过 IP 报文检查告警阈值后，AC6605 会向网管发送告警信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip source check user-bind alarm enable**，使能 IP 报文检查告警功能。

缺省情况下，IP 报文检查告警功能未使能。

注意

请不要在 VLAN 和接口下同时配置 IP 报文检查功能，否则将导致 IP 报文检查告警功能失效。

步骤 4 执行命令 **ip source check user-bind alarm threshold** *threshold*，配置 IP 报文检查告警阈值。

缺省情况下，IP 报文检查告警阈值为 100。

----结束

版权所有 © 华为技术有限公司

（可选）配置丢弃源 IP 地址与目的 IP 地址相同的 IP 报文

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip anti-attack source-ip equals destination-ip drop**，开启丢弃源 IP 地址与目的 IP 地址相同的 IP 报文的功能。

缺省情况下，源 IP 地址与目的 IP 地址相同的 IP 报文不被丢弃。

----结束

检查配置结果

前提条件

已完成 IP Source Guard 配置。

操作步骤

步骤 1 使用命令 **display dhcp static user-bind** { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **ipsg-status** | **mac-address** *mac-address* | **vlan** *vlan-id* [**interface** *interface-type interface-number*] | **all** [**verbose**] } 查看静态绑定表信息。

步骤 2 使用命令 **display ip source check user-bind interface** *interface-type interface-number* 查看接口下 IP Source Guard 相关的配置信息。

----结束

8.5.4 配置 URPF

配置 URPF 功能。

建立配置任务

应用环境

为了防止基于源地址欺骗的网络攻击行为，可以通过配置 URPF，检查报文的源地址和入接口是否匹配。如果匹配，认为源地址合法，允许报文通过；否则，认为源地址是伪装的，丢弃报文。

前置任务

在配置 URPF 功能之前，需完成以下任务：

- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。

数据准备

在配置 URPF 功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

配置接口的 URPF 检查模式

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

说明

URPF 检查功能要在物理接口下配置，这是因为 URPF 功能是按照物理接口配置实现的。

步骤 3 执行命令 **urpf** { **loose** | **strict** } [**allow-default-route**]，配置接口的 URPF 检查功能。

URPF 通过选择是否配置参数 **allow-default-route** 来确定对缺省路由的处理方式。

- 配置参数 **allow-default-route** 时，不管是严格检查还是松散检查，如果报文的源地址在 FIB 表中不存在，即使找到缺省路由作为其相应的路由，该报文都将被丢弃。
- 不配置参数 **allow-default-route** 时，如果报文的源地址在 FIB 表中不存在，
  - 严格检查模式下，如果缺省路由的出接口与报文的入接口一致，报文将通过 URPF 检查，进行正常的转发。如果缺省路由的出接口与报文的入接口不一致，则报文将被丢弃。
  - 松散检查模式下，不管缺省路由的出接口和报文的入接口是否一致，都将通过 URPF 检查，进行正常的转发。

说明

针对符合流策略重定向规则的报文将不支持 URPF 检测。

----结束

检查配置结果

前提条件

已完成 URPF 功能的配置。

操作步骤

- 在接口视图下使用命令 **display this** 查看当前接口下是否配置了 URPF 功能。

----结束

8.5.5 配置举例

介绍 IP Source Guard 配置举例。

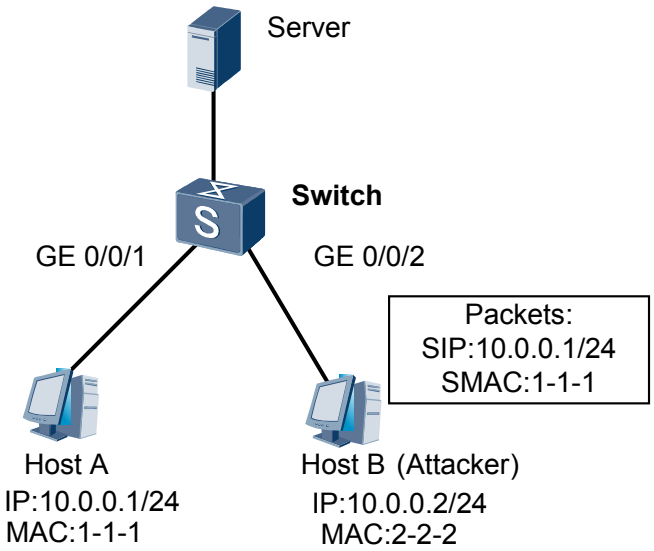
配置 IP Source Guard 示例

组网需求

如图 8-18 所示，HostA 与 HostB 分别与 Switch 的 GE0/0/1 和 GE0/0/2 接口相连。要求在 Switch 上配置 IP Source Guard 功能，使 HostB 不能仿冒 HostA 的 IP 和 MAC 欺骗服务器，保证 HostA 的 IP 报文能正常上送。

版权所有 © 华为技术有限公司

图 8-18 配置 IP Source Guard 组网图



配置思路

采用如下的思路配置 IP Source Guard 功能（假设用户的 IP 地址是静态分配的）：

1. 接口使能 IP 报文检查功能。连接 HostA 和 HostB 的接口都需要使能该功能。
2. 配置对 IP 报文匹配检查。
3. 配置静态绑定表。

数据准备

为完成此配置举例，需要准备以下数据：

- 连接 HostA 的接口：GE0/0/1；连接 HostB 的接口：GE0/0/2。
- HostA 的 IP 地址：10.0.0.1/24，MAC 地址：1-1-1
- HostA 所在 VLAN：VLAN10

说明

以下配置步骤中，只列出了和 IP Source Guard 配置相关的命令。

操作步骤

步骤 1 配置 IP 报文检查功能

在连接 HostA 的 GE0/0/1 接口使能 IP 报文检查功能。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] ip source check user-bind enable
```

在连接 HostA 的 GE0/0/1 接口配置 IP 报文检查告警功能。

```
[Quidway-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[Quidway-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 200
[Quidway-GigabitEthernet0/0/1] quit
```

在连接 HostB 的 GE0/0/2 接口使能 IP 报文检查功能。

版权所有 © 华为技术有限公司

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] ip source check user-bind enable

[Quidway-GigabitEthernet0/0/2] quit
```

在连接 HostB 的 GE0/0/2 接口配置 IP 报文检查告警功能。

```
[Quidway-GigabitEthernet0/0/2] ip source check user-bind alarm enable
[Quidway-GigabitEthernet0/0/2] ip source check user-bind alarm threshold 200
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置静态绑定表项

配置 HostA 为静态绑定表项。

```
[Quidway] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
gigabitethernet 1/0/1 vlan 10
```

步骤 3 验证配置结果

在 Switch 上执行 **display dhcp snooping user-bind all** 命令可以查看绑定表信息。

```
<Quidway> display dhcp snooping user-bind all
DHCP static Bind-table:,Flags:O - outer vlan ,I - inner vlan ,P - map vlan,
IP Address                      MAC Address     VSI/VLAN (O/I/P)  Interface,
-------------------------------------------------------------------------------,
 10.0.0.1                        0001-0001-0001  10  /--  /--    GE0/0/1,
-------------------------------------------------------------------------------,
print count:           1          total count:           1,
```

从显示信息可知，HostA 已经配置为静态绑定表项，HostB 不在绑定表中。

----结束

配置文件

```
#
  user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface GigabitEthernet 0/0/1
vlan 10
#
interface GigabitEthernet 0/0/1
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
interface GigabitEthernet 0/0/2
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
return
```

8.6 本机防攻击配置

介绍本机防攻击的原理和配置。

8.6.1 本机防攻击概述

AC6605 通过对上送 CPU 的报文进行限制来实现本机防攻击。

随着网络的规模逐渐增大和应用日益普及，对网络安全和网络设备的安全的要求也越来越高。在网络中，存在大量需要上送 CPU 的各类报文和针对 CPU 的恶意攻击报文。上送 CPU 的报文过多，导致 CPU 占用率过高，性能下降，影响正常的业务。针对 CPU

版权所有 © 华为技术有限公司

的恶意攻击报文则会导致 CPU 长时间繁忙的处理攻击报文，从而引发其它业务的断续，甚至系统中断。

为保护 CPU，保持 CPU 对正常业务的处理和响应，需要对上送 CPU 的报文进行限制。比如过滤上送报文、分类上送报文、限制上送报文的数量、限制上送速率、设定上送的优先级等，对不符合上送规则的报文直接丢弃，保证 CPU 对正常业务的处理。

AC6605 的本机防攻击特性针对的是上送 CPU 的报文，主要用于保护交换机设备自身安全，保证已有业务在发生攻击时的正常运转。

8.6.2 AC6605 支持的本机防攻击特性

AC6605 通过黑名单、CAR 实现本机防攻击。

AC6605 主要通过以下几种方式实现本机防攻击功能：

- 黑名单

  黑名单指非法用户的集合。通过 ACL 可以设置自定义黑名单，后续匹配黑名单特征的报文会被丢弃。可以将确定为攻击者的非法用户设置到黑名单中。

- CAR（committed access rate）

  CAR 用来设置上送 CPU 的报文的分类限速上送规则，针对每类报文可设置承诺信息速率（CIR，Committed Information Rate）和承诺突发尺寸（CBS，Committed Burst Size）。通过对不同的报文设置不同的 CAR 规则，可以降低报文的相互影响，达到保护 CPU 的目的。CAR 还可以设置上送 CPU 报文的整体速率，当整体上送速率超过阈值后，报文将被丢弃，避免 CPU 过载。

8.6.3 配置防攻击策略

配置防攻击策略。

建立配置任务

建立防攻击策略的配置任务。

应用环境

当 AC6605 接入大量用户时，容易遭受针对 CPU 的报文攻击或需要处理大量上送 CPU 的报文，可以配置防攻击策略。

前置任务

在配置防攻击策略之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置防攻击策略之前，需要准备以下数据。

序号	数据
1	防攻击策略名称、防攻击策略的描述信息

版权所有 © 华为技术有限公司

序号	数据
2	黑名单的 ACL 规则及编号
3	上送 CPU 报文的 CIR（承诺信息速率）、CBS（承诺突发尺寸）

创建防攻击策略

用户可以使用名称创建防攻击策略。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

AC6605 最多支持 13 个防攻击策略。其中名称为 default 的策略为系统自动生成的缺省策略，default 策略默认应用到所有单板，不允许删除，也不允许修改参数；其余 12 个允许用户创建和删除。

步骤 3 （可选）执行命令 **description** *text*，配置防攻击策略的描述信息。

----结束

配置黑名单

黑名单指非法用户的集合，匹配黑名单特征的报文会被丢弃。

背景信息

可以创建黑名单，把符合特定特征的用户纳入到黑名单中，系统直接丢弃黑名单用户上送的报文。AC6605 支持通过 ACL 灵活设置黑名单。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **blacklist** *blacklist-id* **acl** *acl-number*，创建自定义黑名单。

AC6605 上最多可以配置 8 条黑名单。

黑名单应用的 ACL 可以是基本 ACL、高级 ACL 或以太帧头 ACL。ACL 的配置方法，请参见 **8.9.3 配置 ACL**。

缺省情况下，AC6605 中没有配置黑名单。

----结束

配置协议报文区分端口类型上送

如果端口类型设置合理，区分端口类型上送 CPU 不同的协议报文可以一定程度的防止攻击产生后所有报文无法上送或者 CPU 来不及处理的情况发生。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port type** [**uni** | **eni** | **nni**]，配置端口的类型，包括 NNI、UNI、ENI 三种端口类型。

缺省情况下，端口不区分 NNI、UNI、ENI 类型。

步骤 4 执行命令 **quit**，返回到系统视图。

步骤 5 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 6 执行命令 **port-type** { **uni** | **eni** | **nni** } **packet-type** *type*，指定协议能够生效的端口类型，包括 UNI、ENI 和 NNI 类型。

缺省情况下，各协议的默认端口类型如在未做任何配置的情况下的 display cpu-defend configuration 查询的显示所示。

----结束

（可选）配置报文上送 CPU 的上送规则

报文上送 CPU 的上送规则包括 car。

背景信息

说明

对上送 CPU 的同一个报文既可以配置 **car** 也可以配置 **deny**，当先后配置同一报文类型的 **deny** 命令和 **car** 命令时，最后配置的命令生效。

当 FTP、BGP 和 OSPF 协议连接建立后，如果用户没有配置 **linkup-car** 的承诺信息速率和承诺突发尺寸，那么 FTP、BGP 和 OSPF 协议报文使用默认的 **linkup-car** 的承诺信息速率和承诺突发尺寸上送。

建议在 AC6605 上使用默认的 **car** 值。

动态协议联动、协议报文限速（包括基于报文数的协议报文上送速率限制、基于比特的报文上送速率限制）、端口限速（随所有报文的限速）和队列限速这几者之间的限速优先级关系如下:

- 动态协议联动的速率限制优先级最高。
- 协议报文限速次之，其中基于包的协议报文上送速率限制、基于比特的报文上送速率限制两者都有限制值的情况下，系统选择实际速率最小的速率。
- 队列限速优先级再次之。
- 端口限速最后。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **linkup-car packet-type** { **bgp** | **ftp** | **ospf** } **cir** *cir-value* [**cbs** *cbs-value*]，配置建立连接后的 BGP、FTP 或者 OSPF 报文的 CAR 限速，并设置速率阈值。

步骤 4 执行命令 **car packet-type** *packet-type* **cir** *cir-value* [**cbs** *cbs-value*]，配置对上送 CPU 的报文进行 CAR 限速，并设置速率阈值。

版权所有 © 华为技术有限公司

步骤 5 执行命令 **deny packet-type** *packet-type*，配置对上送 CPU 的报文动作为丢弃。

缺省情况下，AC6605 对上送 CPU 的报文进行 CAR 限速。AC6605 对各种报文的 CAR 限速值可通过 **display cpu-defend configuration** 命令查看，当 AC6605 不应用任何防攻击策略时，**display cpu-defend configuration** 命令查看的是限速的缺省值。

步骤 6 执行命令 **quit**，返回系统视图。

步骤 7 执行命令 **cp-car** { **total** | **queue** *queue-index* } **speed** *speed-value*，配置报文上送到 CPU 的最大速率。

步骤 8 执行命令 **cp-car total pps** *packets*，配置对上送 CPU 的报文根据报文数进行速率限制。

----结束

（可选）配置协议报文上送 CPU 的队列号

系统根据协议报文上送 CPU 的队列号进行轮流调度，可以保证每个队列都得到一定的服务时间。

背景信息

在报文上送 CPU 时，会先由 ACL 将报文送到 CPU 队列，在该队列做一次调度，然后再由 CPU 处理报文。该队列的调度方式采用 WRR 调度，具体请参见《拥塞管理》。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **queue packet-type** *packet-type queue-value*，配置协议报文上送 CPU 的队列号。

缺省情况下，协议报文上送 CPU 的队列号可以通过 **display cpu-defend configuration all** 查看。

----结束

应用防攻击策略

创建防攻击策略之后，必须将策略在系统视图下应用，否则不会生效。

操作步骤

- 系统视图下应用防攻击策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cpu-defend-policy** *policy-name* **global**，应用防攻击策略。

----结束

检查配置结果

检查防攻击策略的配置结果。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display cpu-defend policy** *policy-name*，查看防攻击策略信息。
- 使用命令 **display cpu-defend statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看上送 CPU 报文的统计信息。
- 使用命令 **display cpu-defend configuration** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看上送 CPU 报文的 CAR 的配置信息。

----结束

任务示例

执行命令 **display cpu-defend policy test** 查看防攻击策略 test 的信息。

```
<Quidway> display cpu-defend policy test
Related slot : <>,
Configuration :,
Car packet-type arp-request : CIR (256)   CBS (48128),
Car all-packets pps : 500  (default)
```

执行命令 **display cpu-defend configuration all**，查看交换机的 CAR 配置信息。

```
<Quidway> display cpu-defend configuration all
Car Configurations On Slot 0.
------------------------------------------------------------------------
Packet Name           Status   Cir(Kbps)   Cbs(Byte)  Queue  Port-Type
------------------------------------------------------------------------
8021x              Disabled          64       10000      2         NA
arp-mff            Disabled          64       10000      4         NA
arp-miss            Enabled          64       10000      0         NA
arp-reply           Enabled          64       10000      1        UNI
arp-request         Enabled          64       10000      4        UNI
bfd                Disabled      100000    18800000      3        NNI
bgp                 Enabled         256       32000      2        NNI
bpdu-tunnel        Disabled          64       10000      2         NA
dhcp-client        Disabled         256       32000      5        UNI
dhcp-server        Disabled         256       32000      2        NNI
dhcpv6-reply       Disabled         256       32000      2        NNI
dhcpv6-request     Disabled         256       32000      5        UNI
dns                 Enabled          64       10000      2         NA
eoam-lag            Enabled      100000    18800000      3         NA
eoam-lag-lblt       Enabled          64       10000      3         NA
eoam-3ah           Disabled         256       32000      4         NA
fib-hit             Enabled          64       10000      2         NA
ftp                 Enabled          64       10000      2        NNI
hotlimit            Enabled         128       16000      6        NNI
http               Disabled          64       10000      2         NA
hw-tacacs           Enabled          64       10000      2        NNI
icmp                Enabled         128       10000      2        UNI
icmpv6              Enabled          64       10000      2        NNI
igmp                Enabled         192       64000      2         NA
isis                Enabled         256       16000      2        NNI
mld                Disabled         128       16000      2        NNI
mpls-ldp            Enabled         256       32000      4         NA
mpls-ping           Enabled          64       10000      4         NA
mpls-ttl-expired    Enabled         128       16000      4         NA
nd                  Enabled          64       10000      2        UNI
ntp                 Enabled          64       10000      2        NNI
ospf                Enabled         256       32000      2        NNI
ospfv3              Enabled          64       10000      2        NNI
pim                 Enabled         256       32000      3        NNI
pppoe              Disabled         128       16000      2         NA
radius              Enabled          64       10000      2        NNI
reserved-multicast  Enabled          64       10000      2         NA
rip                Disabled         128       16000      2        NNI
ripng               Enabled         256       32000      2        NNI
```


版权所有 © 华为技术有限公司

```
rrpp                Disabled          64        10000       3          NA
smart-link          Disabled          64        10000       2          NA
snmp                 Enabled         128        10000       2         NNI
ssh                  Enabled          64        10000       3         NNI
tcp                  Enabled          64        10000       2          NA
telnet               Enabled          64        10000       3          NA
ttl-expired          Enabled          64        10000       2          NA
vrrp                Disabled          64        10000       2          NA
vrrp6               Disabled          64        10000       2          NA
------------------------------------------------------------------------
Linkup Information:
------------------------------------------------------------------------
Packet Name  Cir(Kbps)/Cbs(Byte)  SIP(SMAC)         DIP(DMAC)         Port(C/S)
------------------------------------------------------------------------
bgp          512/64000           6.6.6.6           9.9.9.9           53706/179
------------------------------------------------------------------------
```

8.6.4 配置攻击溯源

配置攻击溯源，分析上送 CPU 的报文是否会对 CPU 造成攻击，对可能造成攻击的报文进行写日志或告警提醒用户。

建立配置任务

建立攻击溯源的配置任务。

应用环境

网络上可能会出现大量攻击报文攻击网络节点设备的 CPU。攻击溯源可以通过分析上送 CPU 的报文是否会对 CPU 造成攻击，对可能造成攻击的报文进行写日志或告警提醒用户。

前置任务

在配置攻击溯源之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置攻击溯源之前，需要准备以下数据。

序号	数据
1	防攻击策略名称、防攻击策略的描述信息
2	攻击溯源速率检查阈值
3	攻击溯源速率告警阈值

创建防攻击策略

用户可以使用名称创建防攻击策略。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

AC6605 最多支持 13 个防攻击策略。其中名称为 default 的策略为系统自动生成的缺省策略，default 策略默认应用到所有单板，不允许删除，也不允许修改参数；其余 12 个允许用户创建和删除。

步骤 3 （可选）执行命令 **description** *text*，配置防攻击策略的描述信息。

----结束

配置自动攻击溯源功能

配置自动攻击溯源功能包括配置攻击溯源检查功能和配置攻击溯源告警功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 执行命令 **auto-defend threshold** *threshold*，配置攻击溯源检查阈值。

缺省情况下，攻击溯源检查阈值为 128pps。

步骤 5 （可选）执行命令 **auto-defend alarm enable**，使能攻击溯源告警功能。

缺省情况下，攻击溯源告警功能未使能。

步骤 6 （可选）执行命令 **auto-defend alarm threshold** *threshold*，配置攻击溯源告警阈值。

缺省情况下，攻击溯源告警阈值为 128pps。

----结束

（可选）配置攻击溯源的方式

AC6605 提供了灵活的攻击溯源方式，具体的方式根据实际需求，可以通过命令行控制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 （可选）执行命令 **auto-defend trace-type** { **source-mac** | **source-ip** | **source-portvlan** } *，配置攻击溯源的方式，包括基于源 MAC 地址、基于源 IP 地址、基于源端口+VLAN 三种。

版权所有 © 华为技术有限公司

缺省情况下，基于源 MAC 地址、基于源 IP 地址、基于源端口+VLAN 这三种攻击溯源方式都开启。

----结束

（可选）配置攻击溯源的白名单

配置攻击溯源的白名单后，可以对白名单用户不做溯源。

前提条件

需要定义合适的 ACL 和对应的规则。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 （可选）执行命令 **auto-defend trace-type** { **source-mac** | **source-ip** | **source-portvlan** } *，配置攻击溯源的方式，包括基于源 MAC 地址、基于源 IP 地址、基于源端口+VLAN 三种。

缺省情况下，基于源 MAC 地址、基于源 IP 地址、基于源端口+VLAN 这三种攻击溯源方式都开启。

如果定义源 IP 地址或者 MAC 地址作为白名单的过滤规则，需要同时使用此命令配置攻击溯源的方式。

步骤 5 执行命令 **auto-defend whitelist** *whitelist-num* { **acl** *acl_number* | **interface** *interface-type interface-number* }，配置攻击溯源的白名单。

缺省情况下，没有攻击溯源的白名单。

----结束

（可选）配置攻击溯源支持的协议类型

配置攻击溯源支持的协议类型可以针对性地取消或者开启某些协议的攻击溯源功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 （可选）执行命令 **auto-defend protocol** { { **arp** | **icmp** | **dhcp** | **igmp** | **ttl-expired** | **tcp** | **telnet** } * | **all** }，配置攻击溯源支持的协议类型。

版权所有 © 华为技术有限公司

缺省情况下，ARP、ICMP、DHCP、IGMP、TCP、Telnet 协议报文，TTL 为 1 的报文都支持攻击溯源 。

----结束

（可选）配置攻击溯源的自动防御措施

攻击溯源明确了攻击源后，AC6605 提供对攻击源的适当处理，可以由命令控制处理的方式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 （可选）执行命令 **auto-defend action deny** [**timer** *second*]，配置攻击溯源的自动防御措施为丢弃。

缺省情况下，攻击溯源的防御功能关闭，定时器的缺省值是 300 秒。

----结束

（可选）配置攻击溯源的采样比

采样比的大小会影响攻击溯源的精度，配置合适的采样比可以在满足精度要求的同时又可以保证不过多增加 CPU 的占用率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **auto-defend enable**，使能自动攻击溯源功能。

缺省情况下，自动攻击溯源功能未使能。

步骤 4 （可选）执行命令 **auto-defend attack-packet sample** *sample-value*，配置攻击溯源的采样比。

缺省情况下，攻击溯源的采样比为 16。

当采样比小于 5 的时候，精度不完全取决于采样比，有可能受报文的发送速率的影响。

----结束

应用防攻击策略

创建防攻击策略之后，必须将策略在系统视图下应用，否则不会生效。

版权所有 © 华为技术有限公司

操作步骤

- 系统视图下应用防攻击策略
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cpu-defend-policy** *policy-name* **global**，应用防攻击策略。

----结束

检查配置结果

检查攻击溯源的配置结果。

操作步骤

- 使用命令 **display cpu-defend policy** *policy-name*，查看防攻击策略信息。
- 使用命令 **display auto-defend attack-source [detail]** 查看全局的攻击源列表。

----结束

任务示例

执行命令 **display cpu-defend policy test** 可以查看 test 号防攻击策略的信息。

```
<Quidway> display cpu-defend policy test
Related slot : <>,
Configuration :,
Car packet-type arp-request : CIR (256)   CBS (48128),
Car all-packets pps : 500  (default)
```

执行命令 **display auto-defend attack-source** 可以查看攻击源信息。

```
<Quidway> display auto-defend attack-source
  Attack Source User Table (MPU):
  ------------------------------------------------------------------------------
      MacAddress       InterfaceName      Vlan:Outer/Inner      TOTAL
  ------------------------------------------------------------------------------
      0003-5556-3244   GigabitEthernet0/0/1  199/299            156464
  ------------------------------------------------------------------------------

  Attack Source Port Table (MPU)
  ----------------------------------------------
  InterfaceName     Vlan:Outer/Inner  TOTAL
  ----------------------------------------------
  GigabitEthernet0/0/1     199/299    156464
  ----------------------------------------------
  ----------------------------------------------
  Attack Source IP Table  (MPU) :
  -------------------------------------
   IPAddress        TOTAL Packets
  -------------------------------------
   10.1.1.1         12652
  -------------------------------------
```

8.6.5 维护防攻击策略

清除上送 CPU 报文统计信息、清除攻击源信息。

清除上送 CPU 报文统计信息

清除统计信息后，以前的统计信息将无法恢复。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **reset cpu-defend statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，清除上送 CPU 报文统计信息。

----结束

清除攻击源信息

清除统计信息后，以前的统计信息将无法恢复。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 在 AC6605 上执行命令 **reset auto-defend attack-source** { **source-mac** [*mac-address*] | **source-ip** [*ip-address*] | **source-portvlan** [**interface** { *ifname* | *iftype ifnum* } **vlan-id** *vlan-id* [**cvlan-id** *vlan-id*]] } *，基于源 MAC 地址、基于源 IP 地址、基于源端口+VLAN 三种方式清除攻击溯源计数。

----结束

8.6.6 配置举例

介绍防攻击策略的应用举例。

配置防攻击策略示例

介绍防攻击策略的基本配置过程，包括配置 ACL、配置防攻击策略、配置上送 CPU 报文的上送规则和应用防攻击策略。

组网需求

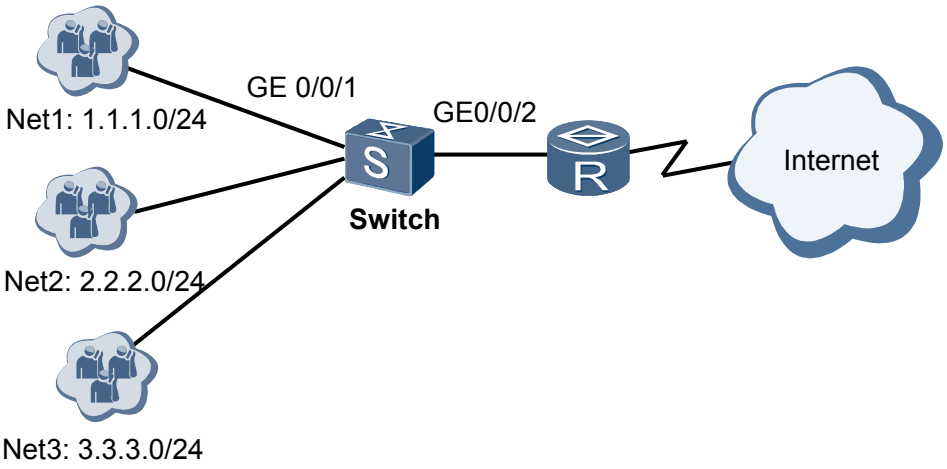
如图 8-19 所示，本地网用户通过 Switch 连接到路由器访问 Internet，Switch 接入大量的用户，会接收到大量需要上送 CPU 的报文，容易遭受针对 CPU 的报文攻击。为保护 CPU，使 Switch 能够正常处理其它业务，需要配置本机防攻击特性。

在 Switch 配置以下防攻击特性：

- Net1 网段中的用户经常会发生攻击行为，所以将 Net1 加入黑名单，阻止其接入网络。
- 配置 ARP Request 报文上送 CPU 的 CAR 值。
- 配置 FTP 协议建立连接时 FTP 报文上送 CPU 的速率限制规则。

版权所有 © 华为技术有限公司

图 8-19 配置防攻击策略组网图



配置思路

采用如下的思路配置本机防攻击：

1. 配置 ACL，定义上送 CPU 报文的过滤规则。
2. 创建防攻击策略，配置黑名单。
3. 配置上送 CPU 报文的上送规则。
4. 应用防攻击策略。

数据准备

为完成此配置举例，需要准备如下数据：

- 防攻击策略名称。
- 黑名单的编号。
- 应用的 ACL 规则和编号。
- ARP Request 报文上送 CPU 报文的速率限制值。
- FTP 协议建立连接时 FTP 报文上送 CPU 的速率限制值。

操作步骤

步骤 1 配置上送 CPU 报文的过滤规则

定义 ACL 规则。

```
<Quidway> system-view
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 1.1.1.0 0.0.0.255
[Quidway-acl-basic-2001] quit
```

步骤 2 创建防攻击策略

创建防攻击策略，配置黑名单。

版权所有 © 华为技术有限公司

```
[Quidway] cpu-defend policy test1
[Quidway-cpu-defend-policy-test1] blacklist 1 acl 2001
```

步骤 3 配置上送 CPU 报文的上送规则

配置 ARP Request 报文的速率限制规则。

```
[Quidway-cpu-defend-policy-test1] car packet-type arp-request cir 128
```

配置 FTP 协议建立连接时 FTP 报文上送 CPU 的速率限制规则。

```
[Quidway-cpu-defend-policy-test1] linkup-car packet-type ftp cir 128
[Quidway-cpu-defend-policy-test1] quit
```

步骤 4 应用防攻击策略

```
[Quidway] cpu-defend-policy test1 global
```

步骤 5 验证配置结果

查看配置的防攻击策略的信息。

```
<Quidway> display cpu-defend policy test1
 Related slot : <0>
 Configuration :
   Blacklist 1 ACL number : 2001
   Car packet-type arp-request : CIR(128)  CBS(24064)
   Car all-packets pps : 500 (default)
```

查看配置的 CAR 的信息。

```
<Quidway> display cpu-defend arp-request configuration all
Car Configurations On Slot 0.
------------------------------------------------------------------------------
Packet Name           Status   Cir(Kbps)   Cbs(Byte)  Queue  Port-Type
------------------------------------------------------------------------------
arp-request           Enabled    128       24064        2    UNI
------------------------------------------------------------------------------
```

----结束

配置文件

```
#
acl number 2001
 rule 5 permit source 1.1.1.0 0.0.0.255
#
cpu-defend policy test1
 blacklist 1 acl 2001
 car packet-type arp-request cir 128 cbs 24064
 link-car packet-type ftp cir 128 cbs 24064
#
 cpu-defend-policy test1 global
#
return
```

8.7 MFF 配置

介绍 MFF（MAC-Forced Forwarding，MAC 强制转发）的原理和配置。

8.7.1 MFF 概述

简要介绍 MFF 的原理。

版权所有 © 华为技术有限公司

背景

在传统的以太网组网方案中，为了实现不同客户端主机之间的二层隔离和三层互通，通常采用在交换机上划分 VLAN 的方法。但是当彼此间需要二层隔离的用户较多时，这种方式会占用大量的 VLAN 资源；同时，为实现客户端之间三层互通，需要为每个 VLAN 规划不同的 IP 网段，并配置 VLAN 接口的 IP 地址，因此划分过多的 VLAN 会降低 IP 地址的分配效率。

为了改善这种现状，MFF（MAC-Forced Forwarding）为同一广播域内实现客户端主机间的二层隔离和三层互通，提供了一种解决方案。MFF 截获用户的 ARP 请求报文，通过 ARP 代答机制，回复网关 MAC 地址的 ARP 应答报文。通过这种方式，可以强制用户将所有流量（包括同一子网内的流量）发送到网关，使网关可以监控数据流量，防止用户之间的恶意攻击，能更好的保障网络部署的安全性。

MFF 接口角色

MFF 特性包括两种接口角色：用户接口和网络接口。

- 用户接口

  MFF 的用户接口是指直接接入网络终端用户的接口。

  用户接口上对于不同的报文处理如下：

  - 对于 ARP 和 DHCP 报文上送 CPU 进行处理；
  - 允许 ARP 报文、DHCP 协议报文、IGMP 协议报文和 EAPOL 报文通过；
  - 对于普通数据报文，若已经学习到网关 MAC 地址，则仅允许目的 MAC 地址为网关 MAC 地址的单播报文通过，其他报文都将被丢弃；若没有学习到网关 MAC 地址，所有报文被丢弃；
  - 组播数据和广播报文都不允许通过。

- 网络接口

  MFF 的网络接口是指连接其他网络设备如接入交换机、汇聚交换机或网关的接口。

  网络接口上对于不同的报文处理如下：

  - 允许组播报文和 DHCP 报文通过；
  - 对于 ARP 报文则上送 CPU 进行处理；
  - 不处理，正常转发。

说明

- 在启动 MFF 功能的 AC6605 上，能接收到网关发来的报文的接口需要配置为网络接口。
- 网络接口只是一种接口角色，它和该接口在网络拓扑中的位置没有关系。
- 在使能 MFF 的 VLAN 中，只有网络接口和用户接口，不存在二者之外的接口角色。

8.7.2 AC6605 支持的 MFF 特性

介绍 MFF 特性在 AC6605 中的支持情况。

静态网关

应用于静态配置 IP 地址的场景中。在静态配置用户 IP 地址时，用户无法通过 DHCP 报文来获取网关信息，此时，一个 VLAN 下需要维护一个静态网关地址。如果不配置静态网关地址，那么除了 DHCP 动态分配的合法用户以外，其他用户都不能正常通信。

版权所有 © 华为技术有限公司

网关地址探测及维护

如果配置了定时探测网关的功能，则 MFF 定时发送报文对网关进行探测，以检查是否需要更新动态网关。

探测使用伪造的 ARP 报文，报文的源 IP 地址和源 MAC 地址来自于 MFF 记录的用户列表，其原则是选择 MFF 记录的第一个用户的 IP 和 MAC 地址。若该用户表项被删除，则重新选择伪造侦听报文的用户信息。若用户表项删除之后网关没有对应用户，则清空网关探测信息。

ARP 代答

用户之间的三层互通通过类似代理 ARP 的 ARP 代答机制保证，这种代答机制在一定程度上减少了用户侧的广播报文数量。

针对 ARP 报文，MFF 具体进行以下处理：

- 代答用户 ARP 请求

  代替网关给用户回应 ARP 报文，使用户之间的报文交互都通过网关进行三层转发。这里，用户的 ARP 请求既包含对网关的请求，也包含对其他用户 IP 地址的 ARP 请求。
- 网关和 Server 对用户的 ARP 请求，设备用用户的 IP 地址和 MAC 信息进行代答。

部署网络中的服务器

这里的服务器 IP 地址可以是 DHCP 服务器的 IP 地址，也可以是其他业务的服务器的 IP 地址或者是 VRRP 的虚拟 IP 地址。

如果 MFF 的网络侧接口收到了源 IP 地址为服务器 IP 地址的 ARP 请求，按照对待网关的方式代答服务器的请求。即，用户发送给服务器的报文，都会通过网关进行转发；而服务器发送给用户的报文，则不需经过网关转发。

与 VLAN Mapping 和 VLAN Stacking 相结合的应用

当前 AC6605 仅支持在 1：1 映射的 VLAN Mapping 和 VLAN Stacking 上应用 MFF 功能。

IPv6 报文隔离

在与用户相连接的 MFF 设备 AC6605 的入端口侧，AC6605 可以将用户发送的 IPv6 报文丢弃，防止 IPv6 报文在 VLAN 下广播，引起用户之间互相学习到对方的 MAC，从而导致 MFF 的用户隔离功能失效。

网关探测用户状态报文透传

在网关有计费功能的场景中，网关需要及时知道用户的在线状态，作为 MFF 设备的 AC6605 可以透传网关探测用户在线的报文，不再采用 AC6605 代答，当用户在线状态发生改变，网关可以及时感知变化。

8.7.3 配置 MFF

配置 MFF 可实现接入用户之间二层隔离，而流量可以通过网关进行转发。

版权所有 © 华为技术有限公司

建立配置任务

应用环境

在城域以太网的接入层网络中，可以配置 MFF 特性，实现多个接入用户之间的二层隔离，而用户之间的流量通过网关进行三层转发，从而实现用户流量的安全过滤、策略调度和计费。

下面的配置组合必须二选一：

- 配置静态网关地址
- 探测功能和服务器地址

前置任务

在配置 MFF 的基本功能之前，需要完成以下任务：

如果存在动态分配 IP 的用户，则需要

- 使能 DHCP Snooping 功能。
- 配置 DHCP Snooping 信任接口。

数据准备

在配置 MFF 功能之前，需要准备以下数据。

序号	数据
1	需要配置 MFF 的 VLAN ID
2	需要配置为网络接口的接口类型和接口编号
3	（可选）需要配置的静态网关 IP 地址
4	（可选）需要配置的服务器 IP 地址

使能全局 MFF 功能

背景信息

使能全局 MFF 功能后，才能进行其他 MFF 的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-forced-forwarding enable**，使能全局 MFF 功能。

缺省情况下，全局没有使能 MFF 功能。

----结束

版权所有 © 华为技术有限公司

配置 MFF 网络接口

背景信息

至少要在 VLAN 内配置一个网络接口，VLAN 内的 MFF 功能才会生效。

说明

此配置任务可以在没有使能全局 MFF 功能前执行，但是只有使能了全局 MFF 功能后才能起作用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **mac-forced-forwarding network-port**，配置接口为网络接口。

缺省情况下，接口为用户接口。

----结束

使能 VLAN 内 MFF 功能

背景信息

在有多台 AC6605 并使能了 MFF 功能的网络中，至少保证一个网络侧接口在 MFF 功能所属的 VLAN 中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-forced-forwarding enable**，使能 VLAN 内的 MFF 功能。

缺省情况下，VLAN 没有使能 MFF 功能。

----结束

（可选）配置静态网关地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VlAN 视图。

步骤 3 执行命令 **mac-forced-forwarding static-gateway** *ip-address*，配置静态网关 IP 地址。

----结束

版权所有 © 华为技术有限公司

（可选）使能网关定时探测功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VlAN 视图。

步骤 3 执行命令 **mac-forced-forwarding gateway-detect**，使能网关定时探测功能。

使能网关定时探测功能后，AC6605 定时发送 ARP 报文对网关进行探测。

缺省情况下，未使能网关定时探测功能。

----结束

（可选）配置服务器地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-forced-forwarding server** *server-ip* &<1-10>，配置网络中部署的服务器 IP 地址。

----结束

（可选）配置透传网关探测用户状态的报文

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-forced-forwarding user-detect_transparent**，允许网关通过 ARP 请求探测用户是否在线。

----结束

（可选）配置 IPv6 报文隔离功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-forced-forwarding ipv6-isolate**，配置在连接用户的 MFF 设备的入端口上丢弃用户的 IPv6 报文，隔离用户的 IPv6 报文，防止 IPv6 报文在 VLAN 内广播。

----结束

版权所有 © 华为技术有限公司

检查配置结果

操作步骤

- 使用命令 **display mac-forced-forwarding network-port** 查看 MFF 网络接口。
- 使用命令 **display mac-forced-forwarding vlan** *vlan-id*，查看 VLAN 下 MFF 用户和网关信息。

----结束

任务示例

执行命令 **display mac-forced-forwarding network-port**，可以看到使能了 MFF 功能的 VLAN 对应的网络侧接口信息。

```
<Quidway> display mac-forced-forwarding network-port
--------------------------------------------------------------------------------
VLAN ID                 Network-ports
--------------------------------------------------------------------------------
VLAN 10                 GigabitEthernet0/0/1
                        GigabitEthernet0/0/2
                        GigabitEthernet0/0/3
VLAN 100                GigabitEthernet0/0/4
                        GigabitEthernet0/0/5
```

执行命令 **display mac-forced-forwarding vlan** *vlan-id*，可以看到 VLAN 内 MFF 用户信息和网关信息。

```
<Quidway> display mac-forced-forwarding vlan 100
Servers:          192.168.1.2
                  192.168.1.3
------------------------------------------------------------------------
User IP         User MAC              Gateway IP      Gateway MAC
------------------------------------------------------------------------
192.168.1.10    00-01-00-01-00-01     192.168.1.254   00-02-00-02-00-01
192.168.1.11    00-01-00-01-00-02     192.168.1.254   00-02-00-02-00-01
192.168.1.12    00-01-00-01-00-03     192.168.1.252   00-02-00-02-00-03
------------------------------------------------------------------------
[Vlan 100] MFF host total count = 3
```

8.7.4 配置举例

介绍 MFF 的应用举例。

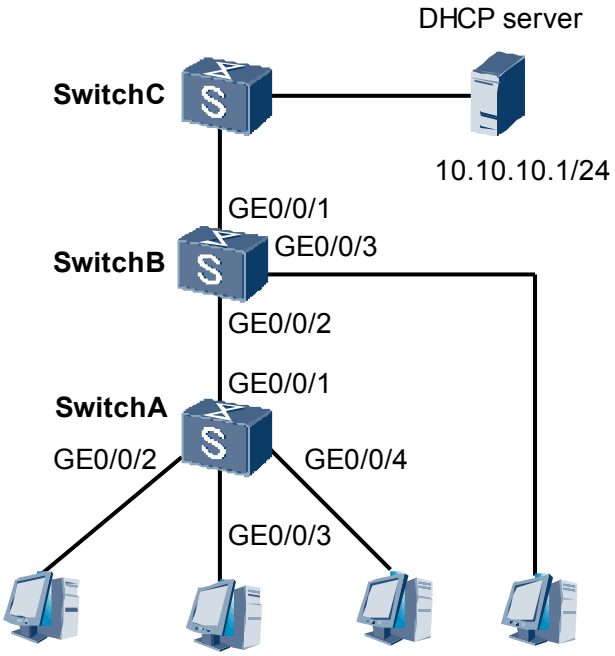
配置 MFF 功能示例

组网需求

如图 8-20 所示，所有用户主机通过 DHCP 服务器获取 IP 地址，所有设备在同一个 VLAN 10 内。为了实现主机之间二层隔离，同时又可以通过网关进行三层互通，在 SwitchA 和 SwitchB 上配置 MFF 功能。

版权所有 © 华为技术有限公司

图 8-20 配置 MFF 功能组网图



配置思路

采用如下的思路配置 MFF：

1. 配置 DHCP Snooping。
2. 全局使能 MFF 功能。
3. 配置 MFF 的网络接口。
4. 使能 VLAN 的 MFF 功能。
5. （可选）配置定时探测网关功能。
6. （可选）配置服务器。

数据准备

为完成此配置举例，需要准备如下数据：

- 需要配置 MFF 的 VLAN ID
- 配置为网络接口的接口类型和接口编号
- （可选）配置的服务器 IP 地址

操作步骤

步骤 1 配置 DHCP Snooping

在 SwitchA 上使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchA
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

在 SwitchA 上使能接口的 DHCP Snooping 功能。以 GE0/0/1 的配置为例，GE0/0/2、GE0/0/3 和 GE0/0/4 的配置与此相同，不再列举。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] dhcp snooping enable
[SwitchA-GigabitEthernet0/0/1] quit
```

在 SwitchA 上配置 GE0/0/1 接口为“信任”状态。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] dhcp snooping trusted
[SwitchA-GigabitEthernet0/0/1] quit
```

在 SwitchB 上使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] dhcp enable
[SwitchB] dhcp snooping enable
```

在 SwitchB 上使能接口的 DHCP Snooping 功能。以 GE0/0/1 的配置为例，GE0/0/2 的配置与此相同，不再列举。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] dhcp snooping enable
[SwitchB-GigabitEthernet0/0/1] quit
```

在 SwitchB 上配置 GE0/0/1 接口为“信任”状态。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] dhcp snooping trusted
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 2 使能全局 MFF 功能

使能 SwitchA 的全局 MFF 功能。

```
[SwitchA] mac-forced-forwarding enable
```

使能 SwitchB 的全局 MFF 功能。

```
[SwitchB] mac-forced-forwarding enable
```

步骤 3 配置 MFF 网络接口

配置 SwitchA 的 GE0/0/1 为网络接口。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] mac-forced-forwarding network-port
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB 的 GE0/0/2 为网络接口。

```
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] mac-forced-forwarding network-port
[SwitchB-GigabitEthernet0/0/2] quit
```

步骤 4 使能 VLAN 的 MFF 功能

在 SwitchA 上使能 VLAN10 的 MFF 功能。

```
[SwitchA] vlan 10
[SwitchA-vlan10] mac-forced-forwarding enable
```

在 SwitchB 上使能 VLAN10 的 MFF 功能。

版权所有 © 华为技术有限公司

```
[SwitchB] vlan 10
[SwitchB-vlan10] mac-forced-forwarding enable
```

步骤 5 （可选）配置定时探测网关功能

在 SwitchA 上配置定时探测网关功能。

```
[SwitchA-vlan10] mac-forced-forwarding gateway-detect
```

在 SwitchB 上配置定时探测网关功能。

```
[SwitchB-vlan10] mac-forced-forwarding gateway-detect
```

步骤 6 （可选）配置服务器

在 SwitchA 上配置服务器。

```
[SwitchA-vlan10] mac-forced-forwarding server 10.10.10.1
```

在 SwitchB 上配置服务器。

```
[SwitchB-vlan10] mac-forced-forwarding server 10.10.10.1
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan 10
#
dhcp enable
dhcp snooping enable
mac-forced-forwarding enable
#
vlan 10
 mac-forced-forwarding enable
 mac-forced-forwarding gateway-detect
 mac-forced-forwarding server 10.10.10.1
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 dhcp snooping enable
 dhcp snooping trusted
 mac-forced-forwarding network-port
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping enable
 #
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
```


版权所有 © 华为技术有限公司

```
#
 vlan 10
#
dhcp enable
dhcp snooping enable
mac-forced-forwarding enable
#
vlan 10
 mac-forced-forwarding enable
 mac-forced-forwarding gateway-detect
 mac-forced-forwarding server 10.10.10.1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
 mac-forced-forwarding network-port
#
return
```

8.8 流量抑制配置

介绍流量抑制的原理和配置。

8.8.1 流量抑制概述

简要介绍流量抑制原理。

进入 AC6605 的广播报文、组播报文和未知单播报文会在该 VLAN 的所有端口被转发。可以看到，这三类报文会消耗系统数倍的带宽，降低系统的可用带宽，影响正常的转发能力和处理能力。

流量抑制功能可以限制进入端口的这些类型的流量。保障 AC6605 免受这三种流量的冲击，在网络流量异常的情况下，保证设备的可用带宽和处理能力。

8.8.2 AC6605 支持的流量抑制特性

介绍流量抑制特性在 AC6605 的支持情况。

AC6605 支持在以太接口和 VLAN 下配置流量抑制功能。

AC6605 支持对广播、组播、单播报文的流量抑制和广播风暴控制。

8.8.3 配置流量抑制

在指定接口下配置流量抑制功能。

建立配置任务

版权所有 © 华为技术有限公司

应用环境

要限制进入接口的广播、组播或未知单播类型报文的速率，避免设备受到大的流量冲击，可以在该接口上配置对应类型的流量抑制功能。

前置任务

无

数据准备

在配置流量抑制之前，需要准备以下数据。

序号	数据
1	需要配置流量抑制的接口类型和编号
2	需要抑制的流量类型（广播、组播或未知单播）
3	基于何种方式来抑制流量（包速率、实际物理端口速率百分比）
4	限制的速率值(包速率值、百分比值)

配置接口的流量抑制

背景信息

在需要进行流量抑制的 AC6605 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令{ **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } { *percent-value* | **packets** *packets-per-second* }配置流量抑制。

AC6605 支持在一个接口下同时配置三种流量类型的流量抑制。接口下流量类型的抑制方式包括以下两种。

- 如果需要配置按包速率进行流量抑制，请选择参数 **packets**。
- 如果需要配置按百分比进行流量抑制，请选择参数 *percent-value*。

说明

- 在接口下，如果已经配置某一种流量类型的流量抑制，再次下发不同速率的该流量类型的流量抑制配置时，新的配置将覆盖原有配置。

步骤 4 执行命令{ **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **block outbound**，配置在接口出方向上阻断报文。

----结束

版权所有 © 华为技术有限公司

（可选）配置 VLAN 的广播抑制

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **broadcast-suppression** *threshold-value*，配置 VLAN 的广播抑制速率。

缺省情况下，不对 VLAN 下的广播报文进行抑制。

----结束

（可选）配置接口 ICMP 报文流量抑制

用户可以通过配置 ICMP 报文流量抑制来防止接口 ICMP 报文攻击。

背景信息

网络中经常存在 ICMP 报文攻击。如果 AC6605 用户侧有大量的 ICMP 请求广播报文攻击，这些报文都会上送 CPU 处理，使 CPU 占用率大大提高，导致其他业务功能异常。

因此，在设备上新增了防止接口 ICMP 报文攻击的功能。

接口 ICMP 报文流量抑制功能生效需要去使能 ICMP-Reply fast 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **icmp rate-limit enable**，使能 ICMP 接口流量抑制功能。

缺省情况下，设备接口的 ICMP 报文流量抑制功能使能。

步骤 3 执行命令 **icmp rate-limit** { **total** | **interface** *interface-type interface-number* [**to** *interface-number*] } **threshold** *threshold-value*，配置接口 ICMP 报文限速阈值。

缺省情况下，接口和全局 ICMP 报文接口流量抑制的阈值为 100pps。

----结束

检查配置结果

前提条件

已完成流量抑制配置。

操作步骤

- 使用命令 **display flow-suppression interface** *interface-type interface-number* 查看流量抑制配置信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display flow-suppression interface** *interface-type interface-number* 可以查看指定接口下的流量抑制配置。

```
<Quidway> display flow-suppression interface gigabitethernet 0/0/1
 storm type         rate mode   set rate value
------------------------------------------------------------------------------
 unknown-unicast    percent     percent: 80%
 multicast          percent     percent: 80%
 broadcast          percent     percent: 80%
------------------------------------------------------------------------------
```

8.8.4 配置风暴控制功能

介绍风暴控制功能的配置方法。

建立配置任务

建立风暴控制的配置任务。

应用环境

当 AC6605 收到未知单播、组播或广播报文时，由于根据报文的目的 MAC 地址并不能明确指定出接口，AC6605 会向 VLAN 内除了接收接口之外的所有接口转发这些流量，这样可能导致广播风暴，降低 AC6605 的转发性能。因此需要对风暴进行控制，使得流量激增时可以保证 AC6605 依然能进行正常的单播转发。

前置任务

在配置风暴控制之前，需完成以下任务：

- 配置接口的链路属性。
- 配置接口的物理参数。

数据准备

在配置风暴控制之前，需要准备以下数据。

序号	数据
1	报文类型、速率上下限。
2	风暴控制的动作。
3	风暴控制的检测时间间隔。
4	记录日志和上报告警是否使能。

配置风暴控制功能

风暴控制功能是对接口上的广播、组播或未知单播报文进行风暴控制。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **storm-control** { **broadcast** | **multicast** | **unicast** } **min-rate** *min-rate-value* **max-rate** *max-rate-value*，对接口上的广播、组播或未知单播报文进行风暴控制。

步骤 4 执行命令 **storm-control action** { **block** | **shutdown** }，配置风暴控制的动作。

缺省情况下，当接口接收报文的平均速度大于高阈值时，不执行风暴控制动作。

步骤 5 （可选）执行命令 **storm-control enable** { **log** | **trap** }，打开风暴控制时记录日志或者上报告警的开关。

缺省情况下，记录日志和上报告警的开关处于关闭状态。

步骤 6 （可选）执行命令 **storm-control interval** *interval-value*，配置风暴控制的检测时间间隔。

缺省情况下，风暴控制的检测时间间隔是 5 秒。

----结束

检查配置结果

检查风暴控制的配置结果。

前提条件

已经完成风暴控制功能的所有配置。

操作步骤

- 使用命令 **display storm-control** [**interface** *interface-type interface-number*]，查看接口的风暴控制信息。

----结束

任务示例

执行命令 **display storm-control**，可以查看接口名称、报文类型、速率上下限、风暴控制动作、当前接口的报文状态、日志告警开关状态以及风暴控制的检测时间间隔是否配置正确。例如：

```
<Quidway> display storm-control interface gigabitethernet 0/0/1
PortName     Type  Rate      Action    Punish-   Trap Log Interval Last-
                   (Min/Max)           Status                      Punish-Time
-------------------------------------------------------------------------------
GE0/0/1Broadcast    14881000  shutdown  shutdown  off  off 180      2010-12-12
                   /14881000                                       14:30:00
```

8.8.5 配置举例

介绍流量抑制配置举例。

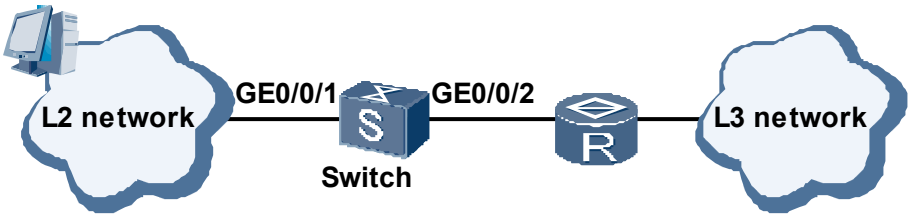
配置流量抑制示例

版权所有 © 华为技术有限公司

组网需求

如图 8-21 所示，Switch 作为二层网络到三层路由器的衔接点，当需要限制二层网络转发的广播、组播或者未知单播报文时，可以通过在 GE0/0/1 接口上配置流量抑制来实现。

图 8-21 配置流量抑制组网图



配置思路

直接在 GE0/0/1 接口视图下配置流量抑制功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 配置流量抑制的接口名称为 GE0/0/1。
- 广播、未知单播和组播的流量抑制方式选择按百分比进行流量抑制。
- 流量抑制后的广播、未知单播和组播报文的速率为接口速率的 80%。

操作步骤

步骤 1 进入接口视图

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
```

步骤 2 配置广播流量抑制

```
[Quidway-GigabitEthernet0/0/1] broadcast-suppression 80
```

步骤 3 配置组播流量抑制

```
[Quidway-GigabitEthernet0/0/1] multicast-suppression 80
```

步骤 4 配置未知单播流量抑制

```
[Quidway-GigabitEthernet0/0/1] unicast-suppression 80
```

步骤 5 验证配置结果

执行命令 **display flow-suppression interface** 查看 GE0/0/1 接口下的流量抑制配置情况。

```
<Quidway> display flow-suppression interface gigabitethernet 0/0/1
 storm type         rate mode    set rate value
--------------------------------------------------------------------------------
 unknown-unicast    percent         percent: 80%
 multicast          percent         percent: 80%
 broadcast          percent         percent: 80%
--------------------------------------------------------------------------------
```

----结束

版权所有 © 华为技术有限公司

配置文件

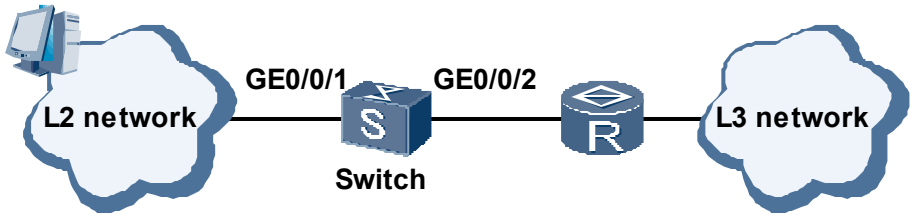
```
#
 sysname Quidway
#
interface GigabitEthernet0/0/1
 unicast-suppression 80
 multicast-suppression 80
 broadcast-suppression 80
#
return
```

配置风暴控制示例

组网需求

如图 8-22 所示，当 Switch 收到未知单播、组播或广播报文时，由于根据报文的目的 MAC 地址并不能明确指定出接口，Switch 会向 VLAN 内除了接收接口之外的所有接口转发这些流量，这样可能导致广播风暴，降低 Switch 的转发性能。Switch 作为二层网络到三层路由器的衔接点，需要对 VLAN 内广播、组播或者未知单播报文进行风暴控制时，可以通过在 GE0/0/1 接口上的配置来实现。

图 8-22 配置风暴控制组网图



配置思路

直接在 GE0/0/1 接口视图下配置风暴控制功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 配置风暴控制的接口名称为 GE0/0/1。
- 对广播、组播或未知单播报文进行风暴控制的低阈值和高阈值。
- 风暴控制的动作。
- 风暴控制的检测时间间隔。

操作步骤

步骤 1 进入接口视图

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
```

步骤 2 配置广播风暴控制

版权所有 © 华为技术有限公司

```
[Quidway-GigabitEthernet0/0/1] storm-control broadcast min-rate 1000 max-rate 2000
```

步骤 3 配置组播风暴控制

```
[Quidway-GigabitEthernet0/0/1] storm-control multicast min-rate 1000 max-rate 2000
```

步骤 4 配置未知单播风暴控制

```
[Quidway-GigabitEthernet0/0/1] storm-control unicast min-rate 1000 max-rate 2000
```

步骤 5 配置风暴控制的动作为阻塞报文

```
[Quidway-GigabitEthernet0/0/1] storm-control action block
```

步骤 6 配置打开风暴控制时记录日志的功能

```
[Quidway-GigabitEthernet0/0/1] storm-control enable log
```

步骤 7 配置风暴控制的检测时间间隔

```
[Quidway-GigabitEthernet0/0/1] storm-control interval 90
```

步骤 8 验证配置结果

执行命令 **display storm-control interface gigabitethernet 0/0/1** 查看 GE0/0/1 接口下的风暴控制配置情况。

```
<Quidway> display storm-control interface gigabitethernet 0/0/1
PortName     Type  Rate      Action    Punish-   Trap Log Interval Last-
                   (Min/Max)           Status                      Punish-Time
-------------------------------------------------------------------------------
GE0/0/1  Multicast  1000     Block      shutdown   off  off 90      2010-12-12
                   /2000                                          14:34:00
GE0/0/1  Broadcast  1000     Block      shutdown   off  off 90      2010-12-12
                   /2000                                          14:30:00
GE0/0/1  Unicast    1000     Block      shutdown   off  off 90      2010-12-12
                   /2000                                          14:36:00
```

----结束

配置文件

```
#
interface GigabitEthernet0/0/1
 storm-control broadcast min-rate 1000 max-rate 2000
 storm-control multicast min-rate 1000 max-rate 2000
 storm-control unicast min-rate 1000 max-rate 2000
 storm-control interval 90
 storm-control action block
 storm-control enable log
#
return
```

8.9 ACL 配置

ACL 通过一系列规则对数据包进行分类，这些规则应用到 AC6605 接口上，AC6605 根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

8.9.1 ACL 概述

介绍 ACL 的基本概念和相关参数。

AC6605 为了过滤数据包，需要配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过访问控制列表 ACL（Access Control List）定义的。

访问控制列表是由 **permit** | **deny** 语句组成的一系列有顺序的规则，这些规则根据数据包的源地址、目的地址、端口号等来对数据包进行过滤。ACL 通过这些规则对数据包进行

版权所有 © 华为技术有限公司

分类，这些规则应用到 AC6605 上，AC6605 根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

8.9.2 AC6605 支持的 ACL 分类

介绍 AC6605 支持的 ACL 分类。

说明

本手册中，ACL 指用于过滤 IPv4 报文的访问控制列表，ACL6 指用于过滤 IPv6 报文的访问控制列表。

ACL 的分类

对用于过滤 IPv4 报文的 ACL，AC6605 支持基本 ACL、高级 ACL、二层 ACL 和用户自定义 ACL。

- 基本 ACL 主要基于源地址、分片标记和时间段信息对数据包进行分类定义。
- 高级 ACL 可以基于源地址、目的地址、源端口号、目的端口号、协议类型、优先级、时间段等信息对数据包进行更为细致的分类定义。
- 二层 ACL 主要基于源 MAC 地址、目的 MAC 地址和报文类型等信息对数据包进行分类定义。
- 用户自定义 ACL 主要根据用户自定义的规则对数据报文做出相应的处理。

对用于过滤 IPv6 报文的 ACL6，AC6605 支持基本 ACL6 和高级 ACL6。

- 基本 ACL6 使用源地址、分片标记和时间段信息作为定义 ACL6 的规则的元素。
- 高级 ACL6 可以使用数据包的源地址、目的地址、IP 承载的协议类型、针对协议的特性（例如 TCP 的源端口、目的端口、ICMPv6 协议的类型、ICMPv6 Code）等内容定义规则。

ACL 的应用

AC6605 上定义的 ACL 支持以下两种应用方式：

- 基于硬件的应用：ACL 被下发到硬件，例如配置 QoS 功能时引用 ACL，对报文进行流分类。需要注意的是，当 ACL 被 QoS 功能引用时，如果 ACL 规则中定义的动作为 **deny**，则匹配此 ACL 的报文就被丢弃。如果 ACL 规则中定义的动作为 **permit**，则 AC6605 对匹配此 ACL 的报文采取的动作由 QoS 中流行为定义的动作决定。关于流行为的详细介绍请参见《AC6605 无线接入控制器 配置指南-QoS》。
- 基于软件的应用：ACL 被上层软件引用，例如配置登录用户控制功能时引用 ACL，可以对 FTP、Telnet 和 SSH 用户进行控制。或者当 AC6605 作为 TFTP 客户端时，可以在 AC6605 上配置 ACL，控制本设备以 TFTP 方式登录到哪些 TFTP 服务器。

  需要注意的是，当 ACL 被上层软件引用时，AC6605 对匹配此 ACL 的报文采取的动作由 ACL 规则中定义的动作（**deny** 或 **permit**）决定。关于登录用户控制的详细介绍请参见《AC6605 无线接入控制器 配置指南-基础配置》。

说明

- 当 ACL 下发到硬件，被 QoS 策略引用进行流分类时，如果报文没有与 ACL 中的规则匹配，此时 AC6605 不会使用流行为中定义的动作对此类报文进行处理。
- 当 ACL 被上层软件引用，对 FTP、Telnet 或者 SSH 登录用户进行控制时，如果报文没有与 ACL 中的规则匹配，此时 AC6605 对此类报文采取的动作为 deny，即拒绝报文通过。

版权所有 © 华为技术有限公司

8.9.3 配置 ACL

介绍创建 ACL、创建 ACL 生效时间、配置 ACL 描述信息、配置各种 ACL 规则和配置 ACL 步长的方法。

建立配置任务

建立配置 ACL 的配置任务。

应用环境

访问控制列表（ACL）可以用于很多业务中，比如路由策略、包过滤等，主要是为了区分不同类别的报文，从而进行不同的处理。

前置任务

无

数据准备

在配置 ACL 之前，需准备以下数据。

序号	数据
1	ACL 的编号或 ACL 的名称
2	（可选）ACL 起作用的时间段名，以及起始时间和结束时间
3	（可选）ACL 的描述内容
4	ACL 规则的编号，以及确定报文类型的规则，具体包括协议、源地址和源端口、目的地址和目的端口、ICMP 类型和编码、IP 优先级、tos 值
5	（可选）ACL 的步长

创建 ACL

用户可以使用编号或名称来创建 ACL。

背景信息

一个 ACL 是由若干 **permit** 或 **deny** 语句组成的一系列规则的列表，若干个规则列表构成一个 ACL。配置 ACL 的规则之前，首先需要创建一个 ACL。

创建一个 ACL，需要指定如下参数：

- 当使用编号创建 ACL 时，指定 ACL 的编号，该编号为 ACL 种类的标示。例如 2000 ～ 2999 为基本 ACL，3000 ～ 3999 为高级 ACL。
- 当使用名称创建 ACL 时，指定 ACL 的名称。用户可以为命名型 ACL 指定编号或类型。如果没有为命名型 ACL 指定编号，那么系统为其自动分配编号。

版权所有 © 华为技术有限公司

操作步骤

- 以编号创建 ACL
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *acl-number*，以编号创建一个 ACL。
     - 要创建基本 ACL，*acl-number* 的取值范围是 2000 ～ 2999。
     - 要创建高级 ACL，*acl-number* 的取值范围是 3000 ～ 3999。
     - 要创建二层 ACL，*acl-number* 的取值范围是 4000 ～ 4999。
     - 要创建用户自定义 ACL，*acl-number* 的取值范围是 5000 ～ 5999。
- 以名称创建 ACL
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl name** *acl-name* [**advance** | **basic** | **link** | **user** | *acl-number*]，以名称创建一个 ACL。

     如果没有指定命名 ACL 的编号，AC6605 会为其自动分配编号。主要包括以下两种情况。
     - 如果只为命名型 ACL 指定了类型，AC6605 为其分配的编号是该类型 ACL 编号取值范围内的最大值。
     - 如果既没有指定命名型 ACL 的编号，也没有指定命名型 ACL 的类型，AC6605 认为该 ACL 为高级 ACL，为其分配高级 ACL 编号取值范围内的最大值。

     AC6605 不会为命名型 ACL 重复分配编号。

----结束

（可选）创建 ACL 生效时间段

创建 ACL 生效时间段以后，当配置 ACL 规则时引用该时间段，该 ACL 规则才会在这个时间段内生效；如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该规则或删除该 ACL。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **time-range** *time-range-name* { *starting-time* **to** *ending-time days* | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

可以为多个时间段范围配置相同的 *time-name*，共同来描述某个特殊时间。例如：时间段“test”配置了三个生效时段

- 从 2009 年 1 月 1 日 00:00 起到 2009 年 12 月 31 日 23:59 生效，这是一个绝对时间段。
- 在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
- 在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则“test”最终将在以下时间内生效：2009 年的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00。

----结束

版权所有 © 华为技术有限公司

（可选）配置 ACL 描述信息

配置 ACL 的描述信息，用来描述该 ACL 的功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，或执行命令 **acl name** *acl-name*，进入 ACL 视图。

步骤 3 执行命令 **description** *description*，配置 ACL 描述信息。

ACL 的描述信息可以用来表示该 ACL 的用途，长度不能超过 127 个字符。

缺省情况下，ACL 没有配置描述信息。

----结束

配置基本 ACL

基本 ACL 可以根据源地址对数据包进行分类定义。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number*，以编号创建一个基本 ACL；或者执行命令 **acl name** *acl-name* [**basic** | *acl-number*]，以名称创建一个基本 ACL。

要创建基本 ACL，*acl-number* 的取值范围是 2000 ～ 2999。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*]*，配置 ACL 规则。

----结束

配置高级 ACL

高级 ACL 可以根据源地址、目的地址、源端口号、目的端口号、协议类型等对数据包进行更为细致的分类定义。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number*，以编号创建一个高级 ACLe；或者执行命令 **acl name** *acl-name* [**advance** | *acl-number*]，以名称创建一个高级 ACL。

要创建高级 ACL，*acl-number* 的取值范围是 3000 ～ 3999。

步骤 3 请根据不同情况进行以下配置 ACL 规则。

根据 IP 承载的协议类型不同，在 AC6605 上配置不同的高级 ACL。对于不同的协议类型，有不同的参数组合。

- 当参数 *protocol* 为 TCP 时，创建 ACL 规则

  rule [*rule-id*] { **deny** | **permit** } **tcp** [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** |

版权所有 © 华为技术有限公司

logging | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **tcp-flag** { *tcp-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为 UDP 时，创建 ACL 规则

  rule [*rule-id*] { **deny** | **permit** } **udp** [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为 ICMP 时，创建 ACL 规则

  rule [*rule-id*] { **deny** | **permit** } **icmp** [**destination** { *destination-address destination-wildcard* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为除 TCP、UDP 或 ICMP 之外的协议时，创建 ACL 规则

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **tos** *tos*]*

说明

参数 **dscp** *dscp* 和 **precedence** *precedence* 不能同时配置。

----结束

配置二层 ACL

二层 ACL 可以根据源 MAC 地址、源 VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定规则，对数据进行相应处理。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number*，以编号创建一个二层 ACL；或者执行命令 **acl name** *acl-name* [**link** | *acl-number*]，以名称创建一个二层 ACL。

要创建二层 ACL，*acl-number* 的取值范围是 4000 ～ 4999。

步骤 3 执行命令 **rule** [*rule-id*] { **permit** | **deny** } [{ **ether-ii** | **802.3** | **snap** } | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag**] * [**time-range** *time-range-name*]，配置 ACL 规则。

----结束

配置用户自定义 ACL

用户自定义 ACL 可以根据用户自定义的规则对数据报文做出相应的处理。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number* ，以编号创建一个用户自定义 ACL。或者执行命令 **acl name** *acl-name* [**user** | *acl-number*]，以名称创建一个用户自定义 ACL。

要创建用户自定义 ACL，*acl-number* 的取值范围是 5000 ～ 5999。

说明

用户自定义 ACL 只能应用于上行策略。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head**] { *rule-string rule-mask offset* } &<1-8>] [**time-range** *time-range-name*]，配置用户自定义 ACL 规则。

----结束

（可选）配置 ACL 的步长

AC6605 可以根据 ACL 的步长自动为 ACL 规则分配编号。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，或执行命令 **acl name** *acl-name*，进入 ACL 视图。

步骤 3 执行命令 **step** *step-value*，配置 ACL 步长。

缺省情况下，ACL 规则步长（*step-value*）值为 5。

调整 ACL 的配置时，请注意 **undo step** 命令将把 ACL 步长恢复为缺省值，同时对规则编号进行重新排列。

----结束

检查配置结果

检查配置 ACL 的结果。

前提条件

已经完成了 ACL 的配置。

操作步骤

- 使用命令 **display acl** { *acl-number* | **all** }，查看以编号创建的 ACL 规则。
- 使用命令 **display acl name** *acl-name* ，查看以名称创建的 ACL 规则。
- 使用命令 **display time-range** { **all** | *time-name* }，查看时间段信息。
- 使用命令 **display acl resource** [**slot** *slot-id*]，查看 ACL 的资源信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行命令 **display acl**，可以看到 ACL 的编号、规则数量、步长和规则的具体内容。

```
<Quidway> display acl 3000
Advanced ACL  3000, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.1.1 0
```

执行命令 **display acl name**，可以看到 ACL 的名称、编号、规则数量、步长和规则的具体内容。

```
<Quidway> display acl name test
Advanced ACL test 3999, 1 rule
Acl's step is 5
 rule 5 permit tcp
```

执行命令 **display time-range**，可以看到当前时间段的配置和状态。

```
<Quidway> display time-range all
Current time is 14:19:16 12-4-2008 Tuesday
Time-range : time1 ( Inactive )
 10:00 to 12:00 daily
from 09:09 2008/9/9 to 23:59 2099/12/31
```

执行命令 **display acl resource** 命令，可以看到当前 ACL 资源的使用情况。

```
<Quidway> display acl resource slot 0
 Slot  0  Unit 0: GE0/0/25 to GE0/0/48
          Unit 1: GE0/0/1 to GE0/0/24
   Unit  0 :        Pre-Ingress       Ingress      Egress
------------------------------------------------------------------------------
  Rule Used               0             4             0
  Rule Free            1024          2812           512
  Rule Total           1024          2816           512

  Meter Used              0             0             0
  Meter Free            512          1408           256
  Meter Total           512          1408           256

  Counter Used            0             1             0
  Counter Free          512          1407           512
  Counter Total         512          1408           512
------------------------------------------------------------------------------
       Unit  1 :       Pre-Ingress       Ingress      Egress
------------------------------------------------------------------------------
  Rule Used               0             6             0
  Rule Free            1024          2810           512
  Rule Total           1024          2816           512

  Meter Used              0             1             0
  Meter Free            512          1407           256
  Meter Total           512          1408           256

  Counter Used            0             2             0
  Counter Free          512          1406           512
  Counter Total         512          1408           512
------------------------------------------------------------------------------
```

8.9.4 配置 ACL6

配置基本 ACL6 和高级 ACL6。

版权所有 © 华为技术有限公司

建立配置任务

建立配置 ACL6 的配置任务。

应用环境

ACL6 可用于以下业务：

- 配置包过滤策略
- 配置策略路由
- 配置路由策略

前置任务

无

数据准备

在配置 ACL6 之前，需要准备以下数据。

序号	数据
1	ACL6 的编号或 ACL6 的名称
2	（可选）ACL6 起作用的时间段名，以及起始时间和结束时间
3	ACL6 规则的编号，以及确定报文类型的规则，具体包括协议、源地址和源端口、目的地址和目的端口、ICMPv6 类型和编码、优先级、tos 值

创建 ACL6

用户可以使用编号或名称来创建 ACL6。

背景信息

创建一个访问控制列表，需要指定一个数字，该数字为 ACL6 种类的标示。例如 2000 ～ 2999 为基本 ACL6，3000 ～ 3999 为高级 ACL6。

操作步骤

- 以编号创建 ACL6
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl ipv6** [**number**] *acl6-number*，以编号创建一个 ACL6。
     - 要创建基本 ACL6，*acl-number* 的取值范围是 2000 ～ 2999。
     - 要创建高级 ACL6，*acl-number* 的取值范围是 3000 ～ 3999。
- 以名称创建 ACL6
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl ipv6 name** *acl6-name* [**advance** | **basic** | *acl6-number*]，以名称创建一个 ACL6。

版权所有 © 华为技术有限公司

如果没有指定命名 ACL6 的编号，AC6605 会为其自动分配编号。主要包括以下两中情况。

- 如果只为命名型 ACL6 指定了类型，那么 AC6605 为其分配的编号是该类型 ACL6 编号取值范围内的最大值。
- 如果即没有指定命名型 ACL6 的编号，也没有指定命名型 ACL6 的类型，AC6605 认为该 ACL6 为高级 ACL6，为其分配高级 ACL6 编号取值范围内的最大值。

AC6605 不会为命名型 ACL6 重复分配编号。

----结束

（可选）创建 ACL6 生效时间段

创建 ACL6 生效时间段以后，当配置 ACL6 规则时引用该时间段，该 ACL6 规则才会在这个时间段内生效；如果配置规则时不指定时间段，则该规则不受时间范围限制，将一直生效，除非删除该规则或删除该 ACL6。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **time-range** *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

可以为多个时间段范围配置相同的 *time-name*，共同来描述某个特殊时间。例如：时间段“test”配置了三个生效时段

- 从 2009 年 1 月 1 日 00:00 起到 2009 年 12 月 31 日 23:59 生效，这是一个时间范围。
- 在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
- 在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则“test”最终将在以下时间内生效：2009 年 1 月 1 日起到 2009 年 12 月 31 日 23:59 内的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00。

----结束

配置基本 ACL6

基本 ACL6 可以根据源地址对数据包进行分类定义。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl ipv6** [**number**] *acl6-number*，以编号创建一个基本 ACL6；或者执行命令 **acl ipv6 name** *acl6-name* [**advance** | **basic** | *acl6-number*]，以名称创建一个基本 ACL6。

要创建基本 ACL6，*acl6-number* 的取值范围是 2000 ～ 2999。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name*] *，配置 ACL6 规则。

----结束

版权所有 © 华为技术有限公司

配置高级 ACL6

高级 ACL6 可以根据源地址、目的地址、源端口号、目的端口号、协议类型等对数据包进行更为细致的分类定义。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl ipv6** [**number**] *acl6-number*，创建一个高级 ACL6；或者执行命令 **acl ipv6 name** *acl6-name* [**advance** | **basic** | *acl6-number*]，以名称创建一个高级 ACL6。

要创建高级 ACL6，*acl6-number* 的取值范围是 3000 ～ 3999。

步骤 3 请根据不同情况进行以下配置 ACL6 规则。

根据 IP 承载的协议类型不同，在 AC6605 上配置不同的高级 ACL6。对于不同的协议类型，有不同的参数组合。

- 当参数 *protocol* 为 TCP 时，创建 ACL6 规则使用如下命令：

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **tcp-flag** {*tcp-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为 UDP 时，创建 ACL6 规则使用如下命令：

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为 ICMPv6 时，创建 ACL6 规则使用如下命令：

  rule [*rule-id*] { **deny** | **permit** } { **icmpv6** | *protocol* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **dscp** *dscp* | **fragment** | **icmp6-type** { *icmp6-type-name* | *icmp6-type icmp6-code* } | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **tos** *tos*]*

- 当参数 *protocol* 为除 TCP、UDP 或 ICMPv6 之外的协议时，创建 ACL6 规则使用如下命令：

  rule [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **tos** *tos*]*

----结束

版权所有 © 华为技术有限公司

检查配置结果

检查 ACL6 的配置结果。

前提条件

已经完成了 ACL6 的配置。

操作步骤

- 使用命令 **display acl ipv6** { *acl6-number* | **all** }，查看以编号创建的 ACL6 规则。
- 使用命令 **display acl ipv6 name** *acl6-name*，查看以名称创建的 ACL6 规则。
- 使用命令 **display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

任务示例

执行命令 **display acl ipv6**，可以看到 ACL6 的编号、规则数量和规则的具体内容。

```
<Quidway> display acl ipv6 2002
Basic IPv6 ACL 2002, 2 rules
 rule 0 permit time-range time1
 rule 1 permit
```

执行命令 **display acl ipv6 name**，可以看到 ACL6 的名称、编号、规则数量和规则的具体内容。

```
<Quidway> display acl ipv6 name test
Advanced IPv6 ACL 3999 name test, 1 rule
 rule 0 permit udp
```

执行命令 **display time-range**，可以看到当前时间段的配置和状态。

```
<Quidway> display time-range all
Current time is 09:33:31 5-21-2009 Thursday

Time-range : time1 ( Inactive )
 12:00 to 23:00 working-day
```

8.9.5 配置举例

介绍 ACL 的配置举例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置思路、操作步骤等。

配置基本 ACL 示例

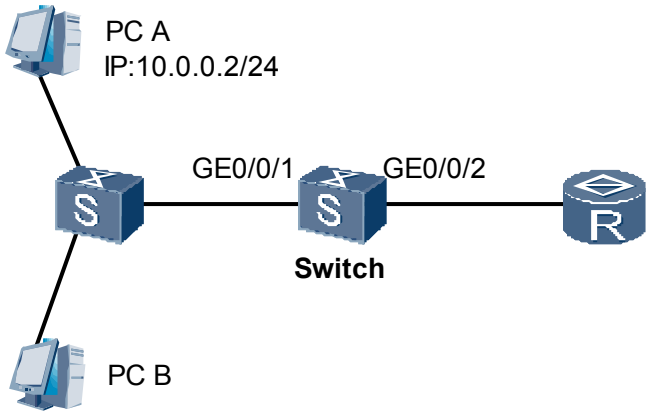
介绍基本 ACL 的配置过程，包括配置基本 ACL 规则、配置流行为、流分类和流策略等。

组网需求

如图 8-23 所示，Switch 的 GE0/0/1 接口连接用户，GE0/0/2 接口连接上层路由器。要求拒绝 IP 地址为 10.0.0.2/24 的用户 A 的流通过。

版权所有 © 华为技术有限公司

图 8-23 配置基本 ACL 功能组网图



配置思路

采用如下的思路配置基本 ACL 功能：

1. 配置 ACL。
2. 配置流分类。
3. 配置流行为。
4. 配置流策略。
5. 在接口上应用流策略。

数据准备

为完成此配置举例，需要准备如下数据：

- ACL 编号。
- 用户 A 的 IP 地址。
- 流分类、流行为、流量策略的名字。
- 应用流策略的接口。

操作步骤

步骤 1 配置基于 ACL 的流分类

定义 ACL 规则。

```
[Quidway] acl 2000
[Quidway-acl-basic-2000] rule permit source 10.0.0.2 0.0.0.255
[Quidway-acl-basic-2000] quit
```

配置流分类，定义基于 ACL 的匹配规则。

```
[Quidway] traffic classifier tcl
[Quidway-classifier-tcl] if-match acl 2000
[Quidway-classifier-tcl] quit
```

步骤 2 配置流行为

版权所有 © 华为技术有限公司

```
[Quidway] traffic behavior tb1
[Quidway-behavior-tb1] deny
[Quidway-behavior-tb1] quit
```

步骤 3 配置流策略

定义流策略，将流分类与流行为关联。

```
[Quidway] traffic policy tp1
[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1
[Quidway-trafficpolicy-tp1] quit
```

应用流策略到 GE0/0/1 接口。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] traffic-policy tp1 inbound
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 4 验证配置结果

查看 ACL 规则的配置信息

```
<Quidway> display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 permit source 10.0.0.0 0.0.0.255
```

查看流分类的配置信息

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 2000
```

查看流策略的配置信息

```
<Quidway> display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
     Classifier: tc1
      Operator: AND
       Behavior: tb1
        Deny
```

----结束

配置文件

```
#
acl number 2000
 rule 5 permit source 10.0.0.0 0.0.0.255
#
traffic classifier tc1 operator and
 if-match acl 2000
#
traffic behavior tb1
  deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet0/0/1
 traffic-policy tp1 inbound
#
return
```


版权所有 © 华为技术有限公司

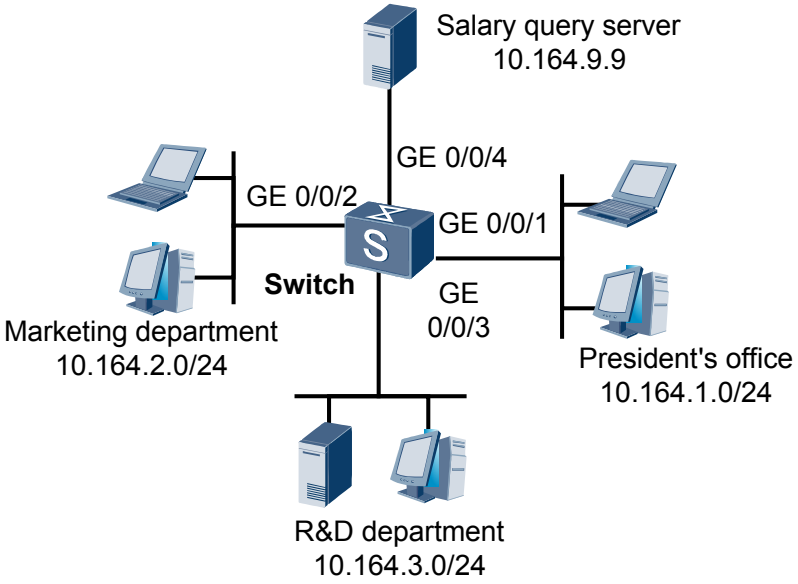
配置高级 ACL 示例

介绍高级 ACL 的配置过程，包括配置生效时间段、配置高级 ACL 规则、配置流行为、流分类和流策略等。

组网需求

如图 8-24 所示，公司企业网通过 Switch 实现各部门之间的互连。要求正确配置 IPv4 ACL，禁止研发部门和市场部门在上班时间（8:00 至 17:30）访问工资查询服务器（IP 地址为 10.164.9.9），而总裁办公室不受限制，可以随时访问。

图 8-24 配置 IPv4 ACL 组网图



配置思路

采用如下的思路配置 IPv4 ACL：

1. 配置接口 IP 地址。
2. 配置时间段。
3. 配置 ACL。
4. 配置流分类。
5. 配置流行为。
6. 配置流策略。
7. 在接口上应用流策略。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口所属 VLAN

版权所有 © 华为技术有限公司

- 时间段名称
- ACL 编号及规则
- 流分类名称及分类规则
- 流行为名称及动作
- 流策略名称及关联的流分类和流行为
- 应用流策略的接口

操作步骤

步骤 1 配置接口 IP 地址

配置接口加入 VLAN，并配置 VLANIF 接口的 IP 地址。

规划 GE0/0/1 ～ GE0/0/3 分别加入 VLAN10、20、30，GE0/0/4 加入 VLAN100。VLANIF 接口的地址取所在网段的第一个 IP 地址。下面配置以 GE0/0/1 接口为例，其他接口的配置与此类似，不再赘述。

```
<Quidway> system-view
[Quidway] vlan batch 10 20 30 100
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Quidway-Vlanif10] quit
```

步骤 2 配置时间段

配置 8:00 至 17:30 的周期时间段。

```
<Quidway> system-view
[Quidway] time-range satime 8:00 to 17:30 working-day
```

步骤 3 配置 ACL

配置市场部门到工资查询服务器的访问规则。

```
[Quidway] acl 3002
[Quidway-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Quidway-acl-adv-3002] quit
```

配置研发部门到工资查询服务器的访问规则。

```
[Quidway] acl 3003
[Quidway-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Quidway-acl-adv-3003] quit
```

步骤 4 配置基于 ACL 的流分类

配置流分类 c_market，对匹配 ACL 3002 的报文进行分类。

```
[Quidway] traffic classifier c_market
[Quidway-classifier-c_market] if-match acl 3002
[Quidway-classifier-c_market] quit
```

配置流分类 c_rd，对匹配 ACL 3003 的报文进行分类。

```
[Quidway] traffic classifier c_rd
[Quidway-classifier-c_rd] if-match acl 3003
[Quidway-classifier-c_rd] quit
```


版权所有 © 华为技术有限公司

步骤 5 配置流行为

配置流行为 b_market，动作为拒绝报文通过。

```
[Quidway] traffic behavior b_market
[Quidway-behavior-b_market] deny
[Quidway-behavior-b_market] quit
```

配置流行为 b_rd，动作为拒绝报文通过。

```
[Quidway] traffic behavior b_rd
[Quidway-behavior-b_rd] deny
[Quidway-behavior-b_rd] quit
```

步骤 6 配置流策略

配置流策略 p_market，将流分类 c_market 与流行为 b_market 关联。

```
[Quidway] traffic policy p_market
[Quidway-trafficpolicy-p_market] classifier c_market behavior b_market
[Quidway-trafficpolicy-p_market] quit
```

配置流策略 p_rd，将流分类 c_rd 与流行为 b_rd 关联。

```
[Quidway] traffic policy p_rd
[Quidway-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Quidway-trafficpolicy-p_rd] quit
```

步骤 7 应用流策略

将流策略 p_market 应用到 GE0/0/2 接口。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] traffic-policy p_market inbound
[Quidway-GigabitEthernet0/0/2] quit
```

将流策略 p_rd 应用到 GE/0/3 接口。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] traffic-policy p_rd inbound
[Quidway-GigabitEthernet0/0/3] quit
```

步骤 8 验证配置结果

查看 ACL 规则的配置信息。

```
<Quidway> display acl all
 Total nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Inactive)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Inactive)
```

查看流分类的配置信息。

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: AND
    Rule(s) : if-match acl 3002

   Classifier: c_rd
    Operator: AND
    Rule(s) : if-match acl 3003
```


版权所有 © 华为技术有限公司

查看流策略的配置信息。

```
<Quidway>  display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
    Classifier: c_market
     Operator: AND
      Behavior: b_market
       Deny

  Policy: p_rd
   Classifier: c_rd
    Operator: AND
     Behavior: b_rd
      Deny
```

----结束

配置文件

```
#
 vlan batch 10 20 30 40 100
#
 time-range satime 08:00 to 17:30 working-day
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
#
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
traffic policy p_market
 classifier c_market behavior b_market
traffic policy p_rd
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 20
 traffic-policy p_market inbound
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 30
 traffic-policy p_rd inbound
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 100
#
return
```

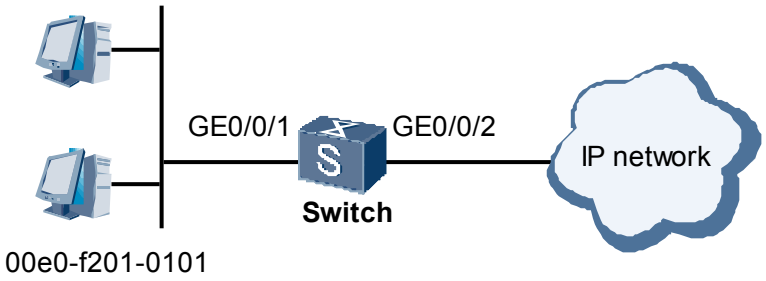
配置二层 ACL 示例

介绍二层 ACL 的配置过程，包括配置二层 ACL 规则、配置流行为、流分类和流策略等。

组网需求

如图 8-25 所示，Switch 作为网关设备，下挂用户 PC。要求配置 ACL，禁止源 MAC 地址为 00e0-f201-0101、目的 MAC 地址为 0260-e207-0002 的报文通过。

图 8-25 配置二层 ACL 组网图



配置思路

采用如下的思路配置二层 ACL：

1. 配置 ACL。
2. 配置流分类。
3. 配置流行为。
4. 配置流策略。
5. 在接口上应用流策略。

数据准备

为完成此配置举例，需要准备如下数据：

- ACL 编号及规则
- 流分类名称及分类规则
- 流行为名称及动作
- 流策略名称及关联的流分类和流行为

版权所有 © 华为技术有限公司

- 应用流策略的接口

操作步骤

步骤 1 配置 ACL

配置符合要求的二层 ACL。

```
[Quidway] acl 4000
[Quidway-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff destination-mac 0260-e207-0002 ffff-ffff-ffff
[Quidway-acl-L2-4000] quit
```

步骤 2 配置基于 ACL 的流分类

配置流分类 tc1，对匹配 ACL 4000 的报文进行分类。

```
[Quidway] traffic classifier tc1
[Quidway-classifier-tc1] if-match acl 4000
[Quidway-classifier-tc1] quit
```

步骤 3 配置流行为

配置流行为 tb1，动作为拒绝报文通过。

```
[Quidway] traffic behavior tb1
[Quidway-behavior-tb1] deny
[Quidway-behavior-tb1] quit
```

步骤 4 配置流策略

配置流策略 tp1，将流分类 tc1 与流行为 tb1 关联。

```
[Quidway] traffic policy tp1
[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1
[Quidway-trafficpolicy-tp1] quit
```

步骤 5 应用流策略

将流策略 tp1 应用到 GE0/0/1 接口。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] traffic-policy tp1 inbound
[Quidway-GigabitEthernet0/0/1] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息。

```
<Quidway> display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 deny destination-mac 0260-e207-0002 source-mac 00e0-f201-0101
```

查看流分类的配置信息。

```
<Quidway> display traffic classifier user-defined
   User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 4000
```

查看流策略的配置信息。

```
<Quidway>  display traffic policy user-defined tp1
 User Defined Traffic Policy Information:
  Policy: tp1
```


版权所有 © 华为技术有限公司

```
  Classifier: tc1
   Operator: AND
    Behavior: tb1
     Deny
```

----结束

配置文件

```
#
acl number 4000
 rule 5 deny destination-mac 0260-e207-0002 source-mac 00e0-f201-0101
#
traffic classifier tc1 operator and
 if-match acl 4000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet0/0/1
  traffic-policy tp1 inbound
#
return
```

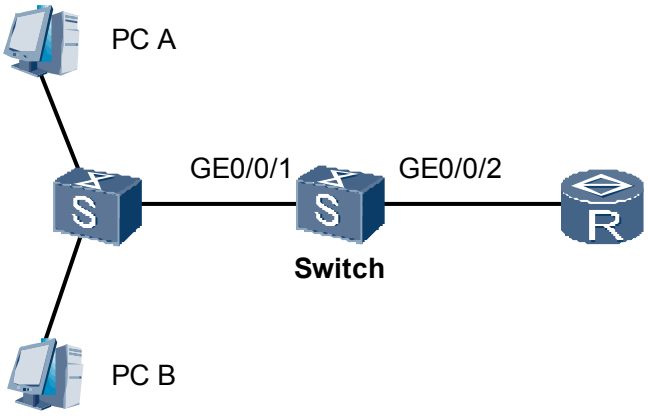
配置用户自定义 ACL 示例

介绍用户自定义 ACL 的配置过程，包括配置用户自定义 ACL 规则、配置流行为、流分类和流策略等。

组网需求

如图 8-26 所示，Switch 的 GE0/0/1 接口连接用户，GE0/0/2 接口连接上层路由器。要求在上行接口 GE0/0/2 下绑定用户自定义 ACL，从二层报文头偏移 14 个字节开始匹配，拒绝匹配成功的报文通过，匹配的字符串内容为 0x0180C200。

图 8-26 配置用户自定义 ACL 组网图



配置思路

采用如下的思路配置用户自定义 ACL：

版权所有 © 华为技术有限公司

1. 配置 ACL。
2. 配置流分类。
3. 配置流行为。
4. 配置流策略。
5. 在接口下应用流策略。

数据准备

为完成此配置举例，需要准备如下数据：

- ACL 编号。
- ACL 规则。
- 流分类、流行为、流量策略的名称。
- 应用流策略的接口。

操作步骤

步骤 1 配置 ACL

配置符合要求的用户自定义 ACL。

```
[Quidway] acl 5000
[Quidway-acl-user-5000] rule deny l2-head 0x0180C200 0xFFFFFFFF 14
[Quidway-acl-user-5000] quit
```

步骤 2 配置基于用户自定义 ACL 的流分类

配置流分类 tc1，对匹配 ACL 5000 的报文进行分类。

```
[Quidway] traffic classifier tc1
[Quidway-classifier-tc1] if-match acl 5000
[Quidway-classifier-tc1] quit
```

步骤 3 配置流行为

配置流行为 tb1，动作为拒绝报文通过。

```
[Quidway] traffic behavior tb1
[Quidway-behavior-tb1] deny
[Quidway-behavior-tb1] quit
```

步骤 4 配置流策略

定义流策略，将流分类与流行为关联。

```
[Quidway] traffic policy tp1
[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1
[Quidway-trafficpolicy-tp1] quit
```

步骤 5 在接口下应用流策略

在接口 GE0/0/2 下应用流策略。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] traffic-policy tp1 inbound
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息

版权所有 © 华为技术有限公司

```
<Quidway> display acl 5000
User ACL 5000, 1 rule
Acl's step is 5
 rule 5 permit 0x0180c200 0xffffffff 14
```

查看流分类的配置信息

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 5000
```

查看流策略的配置信息

```
<Quidway>  display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: AND
     Behavior: tb1
      Deny
```

----结束

配置文件

```
#
acl number 5000
 rule 5 permit 0x0180c200 0xffffffff 14
#
traffic classifier tc1 operator and
 if-match acl 5000
#
traffic behavior tb1
  deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet0/0/2
 traffic-policy tp1 inbound
#
return
```

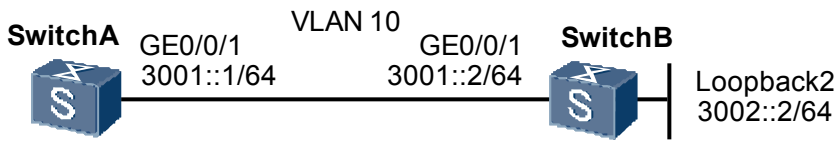
配置 ACL6 控制 FTP 用户访问示例

组网需求

如图 8-27 所示，FTP 服务器 IP 地址为 3002::1/64。

客户端 PC1，PC2 和 FTP 服务器路由可达，在作为 FTP 服务器的 Switch 中，配置 ACL6 后，实现 FTP 服务器禁止主机地址为 3001::2/64 的 PC2 通过 FTP 方式下载和上传文件。

图 8-27 配置 ACL6 控制 FTP 用户访问组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 ACL6 控制 FTP 用户访问：

1. 在 FTP 服务器端进行基础配置
2. 配置基本 ACL6
3. 在 FTP 服务器端绑定基本 ACL6

数据准备

为完成此配置举例，需要准备如下数据：

- 在 FTP 服务器端设置 FTP 用户名和密码
- 基本 ACL6 编号

操作步骤

步骤 1 配置 FTP 基本功能

请参见**配置 FTP 服务器端示例**。

步骤 2 配置基本 ACL6

```
<Quidway> system-view
[Quidway] acl ipv6 number 2001
[Quidway-acl-basic-2001] rule deny source 3001::2/128
[Quidway-acl-basic-2001] quit
```

步骤 3 配置 FTP 支持的 ACL6 列表

```
[Quidway] ftp ipv6 acl 2001
```

步骤 4 验证配置结果

从 PC1 连接 FTP Server

```
c:\ ftp 3002::1
Connected to 3002::1
220 FTP service ready.
User (3003::5:(none)):u1
331 Password required for u1
Password:
230 User logged in.
ftp>
```

从 PC2 连接 FTP Server

```
c:\ ftp 3002::1
Connected to 3002::1
Info:ACL6 was denied by remote host!
Connection closed by remote host.
```

----结束

配置文件

```
#
acl ipv6 number 2001
 rule 0 deny source 3001::2/128
#
ftp ipv6 acl 2001
```


版权所有 © 华为技术有限公司

```
#
return
```

8.10 ND Snooping 配置

介绍 ND Snooping 的原理和配置方法，并给出配置举例。

8.10.1 ND Snooping 概述

简要介绍 ND Snooping 的原理。

邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了 IPv4 的 ARP（Address Resolution Protocol）、ICMP 路由器发现（Router Discovery）和 ICMP 重定向（Redirect）消息，并提供了地址冲突检测、邻居地址解析、确定邻居可达性以及进行主机地址配置等功能。

IPv6 邻居发现机制提供了 5 种不同类型的 ICMPv6 报文。

- 路由器请求报文 RS（Router Solicitation）：主机启动后，通过 RS 报文向路由设备发出请求，路由设备则会以 RA 报文响应。
- 路由器通告报文 RA（Router Advertisement）：路由设备周期性的发布 RA 报文，其中包括前缀和一些标志位的信息。
- 邻居请求报文 NS（Neighbor Solicitation）：IPv6 节点通过 NS 报文可以得到邻居的链路层地址，检查邻居是否可达，也可以进行重复地址检测。
- 邻居通告报文 NA（Neighbor Advertisement）：NA 报文是 IPv6 节点对 NS 报文的响应，同时 IPv6 节点在链路层变化时也可以主动发送 NA 报文。
- 重定向报文（Redirect）：路由设备发现报文的入接口和出接口相同时，可以通过重定向报文通知主机选择另外一个更好的下一跳地址。

ND Snooping 是 ND 的一种安全特性，通过截获以上 5 种类型的报文并进行分析处理，可以过滤不信任的报文并建立和维护前缀管理表和 ND 动态绑定表。前缀管理表中包括前缀、前缀老化租期等信息。ND 动态绑定表中包括 IPv6 地址、MAC 地址、端口和 VLAN 等信息。

ND Snooping 通过维护前缀管理表和 ND 动态绑定表，能够保证合法用户访问网络，防止非法用户对网络设备和合法用户造成攻击。

8.10.2 AC6605 支持的 ND Snooping 特性

介绍 ND Snooping 特性在 AC6605 中的支持情况。

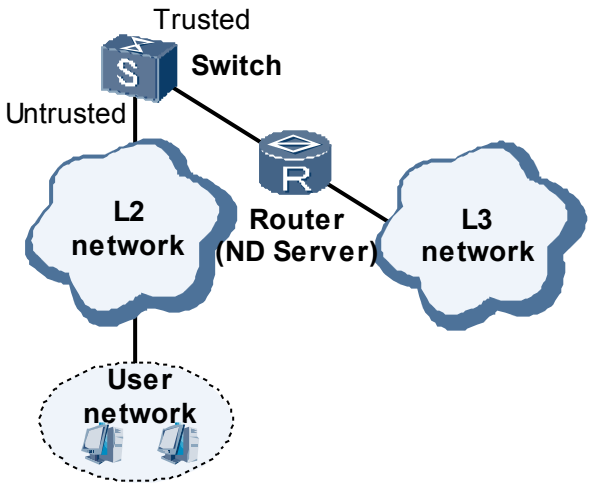
AC6605 部署在二层网络中时，处于 ND Server（通常是路由器）和用户网络之间。AC6605 通过配置接口状态为信任（Trusted）或非信任（Untrusted），可以防止非法用户仿冒 ND Server。

AC6605 中建立和维护前缀管理表和 ND 动态绑定表，能够保证合法用户访问网络，防止非法用户对网络设备和合法用户造成攻击。

ND Snooping 在 AC6605 上的应用如**图 8-28** 所示，图中 AC6605 使能了 ND Snooping 功能。

版权所有 © 华为技术有限公司

图 8-28 AC6605 在二层网络中应用 ND Snooping 典型组网图



8.10.3 配置 ND Snooping

介绍了 ND Snooping 的基本概念、配置步骤以及配置举例。

建立配置任务

在提高 IPv6 网络的安全性前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当网络中存在 ND Server（通常是路由器）仿冒者时，ND Server 仿冒者回应给 ND 客户端的仿冒信息，如错误的网关地址、错误的 DNS 服务器、错误的 IP 等，从而使客户端无法访问网络或访问到不正确的网络。

为了避免受到 ND Server 仿冒者的攻击，可以在 AC6605 上配置 ND Snooping 功能，把网络侧的接口配置为信任状态，把用户侧的接口配置为不信任状态，凡是从不信任接口收到的 RA（Router Advertisement）报文全部丢弃。

根据信任接口接收到的 RA 报文，AC6605 会建立前缀管理表。该表保存 ND Server 分配给 AC6605 的前缀信息，用来管理客户端的地址。

根据前缀管理表中的前缀信息，客户端自动生成 IPv6 地址，然后发送 NS（Neighbor Solicitation）探测报文在网络中检查地址是否重复。在这过程中，AC6605 据 NS 报文的信息生成 ND 动态绑定表，用来保存客户端的 IPv6 地址、MAC 地址和 VLAN 编号等信息，并将该表项中的内容下发到 ACL 中默认允许通过。

前置任务

在配置 ND Snooping 功能之前，需要完成以下任务：

版权所有 © 华为技术有限公司

- 配置 ND Server

数据准备

在配置 ND Snooping 功能之前，需要准备以下数据。

序号	数据
1	需要配置为信任状态的接口类型和编号
2	（可选）ND 动态绑定表的老化探测次数
3	（可选）ND 动态绑定表的老化探测时间

使能 ND Snooping 功能

全局使能 ND Snooping 功能后，必须在接口或 VLAN 下使能，否则 ND Snooping 功能无法生效。

背景信息

使能 ND Snooping 功能的顺序是先使能全局的 ND Snooping 功能，再使能接口或 VLAN 的 ND Snooping 功能。缺省情况下，全局、接口和 VLAN 的 ND Snooping 功能都未使能。

操作步骤

- 在接口视图下配置
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **nd snooping enable**，全局使能 ND Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **nd snooping enable**，使能接口下的 ND Snooping 功能。
- 在 VLAN 视图下配置
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，全局使能 DHCP 功能。
  3. 执行命令 **nd snooping enable**，全局使能 ND Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **nd snooping enable**，使能 VLAN 的 ND Snooping 功能。

----结束

配置接口为信任状态

一般把 AC6605 网络侧的接口配置为信任状态，把 AC6605 用户侧的接口配置为不信任状态。

版权所有 © 华为技术有限公司

背景信息

当 ND Server 发送的 RA 报文流经 AC6605 的信任接口时，AC6605 根据 RA 报文建立前缀管理表。该表保存 RA 报文中分配给 AC6605 的前缀信息。AC6605 将直接丢弃从不信任接口接收到的 ND Server回应的 RA 报文。

一般把连接 ND Server 的接口设成信任状态，其他接口都设为不信任状态。

操作步骤

- 在接口视图下配置
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 在接口视图下，执行命令 **nd snooping trusted**，配置接口为信任状态。

     缺省情况下，接口为不信任状态。
- 在 VLAN 视图下配置
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 在 VLAN 视图下，执行命令 **nd snooping trusted interface** *interface-type interface-number*，配置 VLAN 内的接口为信任状态。

     缺省情况下，VLAN 内的接口为不信任状态。

     说明

     在 VLAN 视图下执行命令时，指定的接口必须属于该 VLAN。和接口视图下的命令相比，在 VLAN 视图下的命令精度更高一些，因为它可以配置指定 VLAN 下指定接口的信任状态。

----结束

（可选）配置 ND 动态绑定表老化功能

通过配置老化功能，AC6605 可以自动管理 ND 动态绑定表。

背景信息

使能 ND Snooping 功能后，AC6605 会根据用户的信息建立 ND 动态绑定表。

当用户 ND 动态绑定表项的租期到期后，如果配置了 ND 动态绑定表老化功能，AC6605 会根据设备配置的老化探测次数和探测时间发送 NS 探测报文。如果在配置的老化探测次数内用户没有回应 NA（Neighbor Advertisement）报文，AC6605 认为用户不在线，删除用户的 ND 动态绑定表项，使得 AC6605 不能将报文转发给该用户。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nd user-bind detect enable**，使能 ND 动态绑定表的老化功能。

缺省情况下，ND 动态绑定表的老化功能未使能。

步骤 3 执行命令 **nd user-bind detect retransmit** *retransmit-times* **interval** *retransmit-interval*，配置 ND 动态绑定表的老化探测时间间隔和探测次数。

版权所有 © 华为技术有限公司

缺省情况下，ND 动态绑定表的老化探测时间间隔为 1000 毫秒，老化探测次数为 2 次。

----结束

检查配置结果

通过配置 ND Snooping 的各种性能，提高 IPv6 网络的安全性后，您可以查看配置的概要统计信息。

前提条件

已完成 ND Snooping 功能的配置。

操作步骤

- 使用命令 **display nd snooping prefix** 查看 ND 用户的前缀管理表项。
- 使用命令 **display nd snooping user-bind** { **all** | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* | **vlan** *vlan-id* **interface** *interface-type interface-number* }查看 ND 动态绑定表项。
- 系统视图下使用命令 **display this** 查看 ND Snooping 功能的配置信息。

  display this 命令可以查看是否使能了 ND Snooping 功能,以及 ND 动态绑定表的老化功能信息。

----结束

任务示例

配置成功后，执行命令 **display nd snooping prefix** 可以查看 ND 用户的前缀管理表。

```
<Quidway> display nd snooping prefix
prefix-table:
Prefix                              Length   Valid-Time  Preferred-Time
------------------------------------------------------------------------------
3001::                              64       100000      100000
------------------------------------------------------------------------------
Prefix table total count:      1
```

执行命令 **display nd snooping user-bind all** 可以查看 ND 动态绑定表中的所有信息。

```
<Quidway> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                      MAC Address     VSI/VLAN(O/I/P) Lease
------------------------------------------------------------------------------
3001::E58C:A2E7:AA4C:8E59       00e0-4c7c-af8f  30  /--  /--    2011.05.06-20:09
------------------------------------------------------------------------------
print count:           1          total count:           1
```

在系统视图下执行命令 **display this**，可以查看 ND Snooping 功能的配置信息。

```
[Quidway] display this
 nd snooping enable
 nd user-bind detect enable
 nd user-bind detect retransmit 10 interval 1000
```

8.10.4 维护 ND Snooping

复位 ND Snooping 前缀管理表和 ND 动态绑定表。

版权所有 © 华为技术有限公司

清除前缀管理表

AC6605 支持手动删除前缀管理表项。

背景信息

ND Server 会定时发送 RA 前缀公告报文，通知客户端更新前缀信息。AC6605 为客户的接入设备会维护该前缀信息，对前缀信息进行更新和老化。

一般情况下，不建议手工删除前缀管理表项。当同时具备以下两种情况时需要手动删除。

- 用户的租期未到期，前缀管理表还不能自动老化。
- 确认用户不再连接网络。

在确认需要手动清除前缀管理表项时，请在用户视图或系统视图下执行以下命令。

操作步骤

- 使用命令 **reset nd snooping prefix** [*ipv6-address*/*prefix-length*]，复位前缀管理表。

----结束

清除 ND 动态绑定表

AC6605 支持手动删除 ND 动态绑定表项。

背景信息

当同时具备以下几种情况时需要手动删除 ND 动态绑定表项。

- ND 动态绑定表未到老化周期，还不能自动老化。
- 确认用户不再连接网络。
- 用户的 VLAN 或接口信息发生变化。

说明

由于组网环境变化之后，ND 动态绑定表不会立即老化，而 ND 动态绑定表匹配的如下信息可能会发生变化，导致匹配出错。

- VLAN 信息在报文中的位置。
- 接口信息。

所以，请在变更组网环境之前手动清除所有 ND 动态绑定表项，使得设备根据新的网络环境生成新的 ND 动态绑定表。

在确认需要手动清除 ND 动态绑定表项时，请在用户视图或系统视图下执行以下命令。

操作步骤

- 使用命令 **reset nd snooping user-bind** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id*]，复位 ND 动态绑定表。

----结束

8.10.5 配置举例

介绍 ND Snooping 的配置举例。

版权所有 © 华为技术有限公司

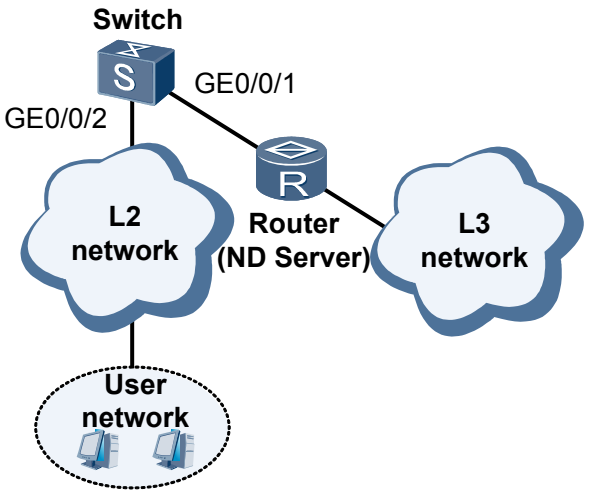
配置在二层网络上应用 ND Snooping 示例

介绍 ND Snooping 的基本配置过程，包括配置信任接口、配置 ND 动态绑定表的老化功能。

组网需求

如图 8-29 所示，Switch 应用在用户网络和 ND Server（通常是路由器）之间的二层网络。为防止 ND Server 仿冒者攻击，要求在 Switch 上应用 ND Snooping 功能，把运营商网络侧的接口配置为 Trusted 模式。Switch 通过维护前缀管理表和 ND 动态绑定表，能够保证合法用户访问网络，防止非法用户对网络设备和合法用户造成攻击。

图 8-29 配置在二层网络上应用 ND Snooping 组网图



配置思路

采用如下的思路在二层网络中配置 ND Snooping 功能：（假设 ND Server 已经配置完成）

1. 使能全局和接口下的 ND Snooping 功能。
2. 把连接 ND Server 的接口设置为“信任（Trusted）”。
3. 配置 ND 动态绑定表的老化功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 Trusted/Untrusted 模式：GE0/0/1 接口 Trusted 模式，GE0/0/2 接口 Untrusted 模式。
- ND 动态绑定表的老化时间。
- ND 动态绑定表的老化探测次数。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 ND Snooping 功能

使能全局 ND Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] nd snooping enable
```

使能接口的 ND Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] nd snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

步骤 2 配置接口 GE0/0/1 为 Trusted 模式

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] nd snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

GE0/0/2 接口使能了 ND Snooping 功能后，接口模式默认为“Untrusted”。

步骤 3 配置 ND 动态绑定表的老化功能

配置 ND 动态绑定表的老化探测时间和老化探测次数。

```
[Quidway] nd user-bind detect enable
[Quidway] nd user-bind detect retransmit 5 interval 600
```

步骤 4 验证配置结果

在系统视图下执行 **display this** 命令可以看到全局和接口视图下已经使能 ND Snooping 功能。

```
[Quidway] display this
 nd snooping enable
 nd user-bind detect enable
 nd user-bind detect retransmit 5 interval 600
```

执行 **display nd snooping prefix** 命令可以查看 ND 用户的前缀管理表。

```
<Quidway> display nd snooping prefix
prefix-table:
Prefix                          Length   Valid-Time  Preferred-Time
-------------------------------------------------------------------------------
2001::                          64       600         600
Info: Prefix table total count:1
```

执行命令 **display nd snooping user-bind all** 可以查看 ND 动态绑定表中的所有信息。

```
<Quidway> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                  MAC Address     VSI/VLAN(O/I/P) Lease
-------------------------------------------------------------------------------
3001::E58C:A2E7:AA4C:8E59       00e0-4c7c-af8f  30  /--  /--    2011.05.06-20:09
3001::E58C:A2E7:AA4C:8D54       00e0-4c7c-afae  30  /--  /--    2011.05.06-20:09
-------------------------------------------------------------------------------
Dynamic binditem count:        2         Dynamic binditem total count:  2
```

----结束

配置文件

```
#
 dhcp enable
```


版权所有 © 华为技术有限公司

```
#
 nd snooping enable
#
 nd user-bind detect enable
#
 nd user-bind detect retransmit 5 interval 600
#
interface GigabitEthernet0/0/1
 nd snooping enable
 nd snooping trusted
#
interface GigabitEthernet0/0/2
 nd snooping enable
#
return
```


版权所有 © 华为技术有限公司

9 可靠性配置

关于本章

本文档针对 AC6605 的可靠性业务，主要包括 DLDP 配置、Smart Link 配置、RRPP 配置、EFM 配置、BFD 配置、VRRP 配置和 VRRP6 配置、以太网 OAM 配置、Y.1731 配置、MAC SWAP 环回测试。

本文档从配置过程和配置举例两大方面介绍了此业务的配置方法和应用场景。

9.1 DLDP 配置
介绍 DLDP 的基本知识、配置方法和配置实例。

9.2 Smart Link 和 Monitor Link 配置
介绍 Smart Link 和 Monitor Link 的基本知识、配置方法和配置实例。

9.3 RRPP 配置
RRPP(Rapid Ring Protection Protocol)具有收敛速度快，收敛时间与环网上节点数无关及 RRPP 多实例支持不同业务流量负载均衡等特点。

9.4 以太网 OAM 配置
通过对以太网 OAM 的介绍和各种配置，实现链路级以太网 OAM 和网络级以太网 OAM 链路的检测，提高网络可靠性。

9.5 Y.1731 配置
Y.1731 对 MEP 之间进行基于业务的丢包检测、时延统计，实现与 IEEE 802.1ag 类似的故障检测功能。

9.6 BFD 配置
通过创建 BFD 会话，可以实现快速检测网络中链路故障。

9.7 VRRP 和 VRRP6 配置
通过创建 VRRP 或 VRRP6 备份组，实现当主用设备出现故障时，由备用设备承担网路流量。

9.8 联动配置举例集
汇总提供以太网 OAM 与接口、以太网 OAM 与其他协议联动的配置举例，便于工程师能方便的找到需要的内容。

9.9 MAC SWAP 环回测试配置
介绍 MAC SWAP 环回测试的原理和配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

9.1 DLDP 配置

介绍 DLDP 的基本知识、配置方法和配置实例。

9.1.1 DLDP 概述

简要介绍 DLDP 的基本概念。

在实际组网中，经常会出现单向链路的现象。所谓单向链路是指本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。

以光纤为例，单向链路分为两种类型：一种是光纤交叉相连，另一种是一条光纤断路。

图 9-1 光纤交叉相连

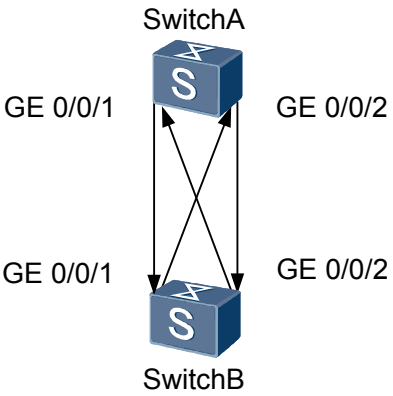
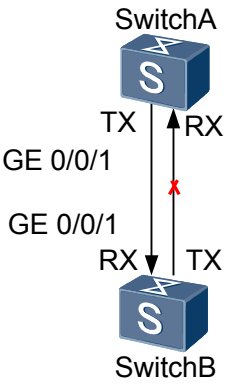


图 9-2 一条光纤断路



设备链路检测协议 DLDP（Device Link Detection Protocol）可以监控光纤/铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络故障发生。目前 AC6605 最多可以支持对 256 个邻居进行 DLDP 检测。

版权所有 © 华为技术有限公司

DLDP 是链路层协议，它与物理层协议协同工作来监控设备的链路状态。物理层的自动协商机制进行物理信号和故障的检测；DLDP 进行对端设备的识别、单向链路的识别和关闭不可达端口等工作。二者协同工作，可以检测和关闭物理和逻辑的单向连接。

如果链路两端在物理层都能独立正常工作，DLDP 会在链路层检测这些链路是否正确连接、两端是否可以正确的交互报文。

说明

DLDP 主要针对两端接口工作在非自动协商模式的情况。

9.1.2 配置 DLDP 功能

介绍配置 DLDP 功能的过程与步骤。

建立配置任务

应用环境

在实际组网中，经常会出现单向链路的情况导致网络故障。在两端设备接口配置 DLDP，可以监控光纤/铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会自动关闭或通知用户手工关闭配置 DLDP 的端口，以防止网络故障发生。

光纤/铜质双绞线两端的设备必须都支持 DLDP 功能才可以实现单向链路检测。

前置任务

在配置 DLDP 之前，需完成以下任务：

- 两端接口工作在非自协商模式下。

数据准备

在配置 DLDP 功能之前，需要准备以下数据。

序号	数据
1	需要配置的接口类型和编号
2	（可选）需要配置的端口组名称
3	（可选）通告报文的时间间隔
4	（可选）DelayDown 定时器的超时时间

使能 DLDP 功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **dldp enable**，使能全局的 DLDP 功能。

步骤 3 执行命令 **interface** *interface-type interface-number* 进入接口视图，或执行命令 **port-group** *port-group-name* 进入端口组视图。

步骤 4 执行命令 **dldp enable**，使能端口的 DLDP 功能。

缺省情况下，全局 DLDP 功能和端口 DLDP 功能都处于关闭状态。

----结束

（可选）配置 DLDP 的工作模式

背景信息

当 DLDP 协议工作在普通模式下，系统只能识别一种类型的单向链路：光纤交叉连接。普通模式下不能检测由双通变成单通的情况，因为没有启动加强定时器功能。

当 DLDP 协议工作在加强模式下，系统能识别两种类型的单向链路：一种是光纤交叉连接，另一种是一条光纤未连接或一条光纤断路。在探测后一种类型的单向链路时，需要将端口配置为强制速率和强制全双工模式，否则即使启用了 DLDP 协议，该协议也不起作用。当出现后一种单向链路时，收端有光信号的一端的端口处于 Disable 状态，收端没有光信号的一端的端口处于 Inactive 状态。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp work-mode** { **enhance** | **normal** }，配置 DLDP 的工作模式。

缺省情况下，DLDP 的工作模式为 **enhance**，即加强模式。

----结束

（可选）使能 DLDP 兼容模式

背景信息

如果需要 AC6605 需要和以下型号华为交换机进行 DLDP 互通时，需要进行以下配置，否则会导致 DLDP 不能互通。以下交换机软件版本必须是支持 DLDP 功能的版本。

- S8500 交换机
- S7800 交换机
- S6500 交换机
- S5600 系列交换机
- S5100－EI 交换机
- S3900 交换机
- S3500 系列交换机
- S3100 系列交换机

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bpdu mac-address** *mac-address* [*mac-address-mask*]，配置指定 MAC 地址为 BPDU MAC 为 010F-E200-0001。

由于 AC6605 和老式华为交换机发送 DLDP 报文所用的 MAC 地址不相同，如果需要和上述交换机实现 DLDP 互通，必须把 BPDU MAC 地址配置为 10F-E200-0001。

步骤 3 执行命令 **interface** *interface-type interface-number* 进入接口视图，或执行命令 **port-group** *port-group-name* 进入端口组视图。

步骤 4 执行命令 **dldp compatible-mode enable**，使能 DLDP 兼容模式。

对于检测交叉链路的情况下，两个接口的 DLDP 兼容模式必须一致，要么同时使能 DLDP 兼容模式，要么同时去使能 DLDP 兼容模式。

如果两端都是 AC6605，两端接口的 DLDP 兼容模式必须一致，要么同时使能兼容模式，要么同时去使能 DLDP 兼容模式。

步骤 5 执行命令 **dldp compatible-mode local-mac**，配置 DLDP 兼容模式下发送 DLDP 报文的 MAC 地址。

在 AC6605 上使能兼容模式之后，使用此命令配置 DLDP 兼容模式发送 DLDP 报文 MAC 地址，可以防止对端设备由于发现多个邻居而出现 DLDP 振荡的问题。

说明

配置的 MAC 地址必须有一个字节为 0，并且不能为组播 MAC 地址。

----结束

（可选）配置发送 Advertisement 报文的时间间隔

背景信息

请在需要配置 DLDP 的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp interval** *time*，配置发送通告（Advertisement）报文的时间间隔。

缺省情况下，发送通告（Advertisement）报文的时间间隔为 5 秒。

配置的通告（Advertisement）报文时间间隔应该小于 STP 收敛时间的三分之一。如果设定的时间太长，DLDP 在没有关闭单向链路的情况下已出现 STP 环路；如果设定的时间太短，会增加网络的流量。

说明

如果用户配置了发送通告（Advertisement）报文的时间间隔，要确保通过光纤/铜质双绞线连接的对端设备也配置了相同的发送 Advertisement 报文的时间间隔，否则 DLDP 不能正常工作。

----结束

版权所有 © 华为技术有限公司

（可选）配置 DelayDown 定时器的超时时间

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp delaydown-timer** *time*，配置 DelayDown 定时器的超时时间。

缺省情况下，DelayDown 定时器的超时时间为 1 秒。

当 DLDP 处于 Active、Advertisement 或 Probe 状态时，如果收到端口 down 事件，比如有些端口在 Tx 线发生故障时会引起 Rx 线的光信号抖动即端口先 down 随即又 up。为了避免在这种情况下 DLDP 直接进入 Inactive 状态清除邻居信息，故 DLDP 先进入 DelayDown 状态，同时启动 DelayDown 定时器（此时仍保留 DLDP 邻居信息，且只响应端口 up 事件）。

- 若该定时器超时后仍未收到端口 up 事件，则删除 DLDP 邻居信息并进入 Inactive 状态。
- 若该定时器超时前收到了端口 up 事件，则返回到原来的 DLDP 状态。

此定时器配置后应用于所有配置了 DLDP 的接口。

----结束

（可选）配置发现单向链路后端口的堵塞模式

背景信息

当 DLDP 检测到单向链路时，可以采用两种方式堵塞单通的端口：

- 手动模式：手动模式的目的是避免网络性能差时，DLDP 协议检测到单通就立即自动堵塞端口，造成业务报文不能收发。该模式是针对这种误判较多的情形采取的一种折中方案。它仅依靠 DLDP 协议检测单向链路，关闭端口由网络管理员手动完成。DLDP 状态机在检测到单通后，只输出 Log 和 Trap 信息，建议用户 Shutdown 此端口，然后迁移到 Disable 状态。
- 自动模式：如果不配置手动模式，默认的堵塞模式是自动模式，这种模式下在发现单通时，除了 DLDP 状态机迁移到 Disable 状态，输出 Log 和 Trap 信息外，还会自动将端口设为堵塞状态。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp unidirectional-shutdown** { **auto** | **manual** }，配置发现单向链路后端口的堵塞模式。

缺省情况下，发现单向链路后端口的堵塞模式为 **auto**。

DLDP Down 状态下的端口仍然会周期性的发送链路恢复探测报文，一旦收到正确的恢复回应报文，则说明单向链路已经变为双向链路，DLDP 会将此端口重新 Up。

----结束

版权所有 © 华为技术有限公司

（可选）配置 DLDP 报文的认证方式

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp authentication-mode** { **md5** *md5-password* | **none** | **simple** *simple-password* }，配置当前设备上的端口与邻居设备上的端口间的 DLDP 认证方式。

缺省情况下，当前设备上的端口与邻居设备上的端口间的 DLDP 认证方式为 **none**。

说明

如果用户配置了 DLDP 认证方式和认证口令，要确保通过光纤/铜质双绞线连接的对端设备也配置了相同的 DLDP 认证方式和认证口令，否则不能通过认证，只有通过认证后 DLDP 才能正常工作。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display dldp** [**interface** *interface-type interface-number*]查看 DLDP 的配置信息和邻居信息表项。

----结束

任务示例

执行命令 **display dldp** 可以查看到 DLDP 的工作模式、发送通告报文的时间间隔、DelayDown 定时器的超时时间、发现单向链路后端口的关闭模式以及报文的认证方式。

```
<Quidway> display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : simple, password is 123
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 2s
 The number of enabled ports is 2.
 The number of global neighbors is: 2.

Interface GigabitEthernet0/0/1
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-0100
    Neighbor port index : 21
    Neighbor state : two way
    Neighbor aged time : 13

Interface GigabitEthernet0/0/2
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-1100
    Neighbor port index : 22
    Neighbor state : two way
    Neighbor aged time : 12
```


版权所有 © 华为技术有限公司

9.1.3 重置 DLDP 状态

介绍重置 DLDP 状态的过程与步骤。

建立配置任务

应用环境

DLDP 协议发现单向链路后，端口进入 Disable 状态。此时需要根据用户选择的端口关闭模式，提示用户关闭端口或自动将端口设为 DLDP Down 状态。如果用户需要该端口重新探测，可以重置端口的 DLDP 状态。恢复后的端口状态与端口的物理状态有关，如果端口的物理状态为 Down，则端口的 DLDP 状态变为 inactive；如果端口的物理状态为 Up，则端口的 DLDP 状态变为 active。

前置任务

无

数据准备

在重置 DLDP 之前，需要准备以下数据。

序号	数据
1	需要重置的接口类型和编号
2	需要重置的端口组名称

全局重置 DLDP 状态

背景信息

在全局重置 DLDP 状态，对设备上所有被 Disable 的端口生效。

dldp reset 是覆盖式命令，只有全局和接口都使能 DLDP 功能后，该配置命令才能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dldp reset**，全局重置 DLDP 状态。

----结束

端口重置 DLDP 状态

版权所有 © 华为技术有限公司

背景信息

在端口重置 DLDP 状态，对单个被 Disable 的端口或者端口组中所有被 Disable 的端口生效。

dldp reset 是覆盖式命令，只有全局和接口都使能 DLDP 功能后，该配置命令才能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* 或 **port-group** *port-group-name* 进入以太网接口视图或端口组视图。

步骤 3 执行命令 **dldp reset**，端口重置 DLDP 状态。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display dldp** [**interface** *interface-type interface-number*]查看 DLDP 的配置信息和邻居信息表项。

----结束

任务示例

执行命令 **display dldp** 可以查看到重置 DLDP 后的接口状态。

```
<Quidway> display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : simple, password is 123
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 2s
 The number of enabled ports is 2.
 The number of global neighbors is: 2.

Interface GigabitEthernet0/0/1 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-0100
    Neighbor port index : 21
    Neighbor state : two way
    Neighbor aged time : 13

Interface GigabitEthernet0/0/2
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-1100
    Neighbor port index : 22
    Neighbor state : two way
    Neighbor aged time : 12
```

9.1.4 维护

介绍维护 DLDP 的相关命令和方法。

版权所有 © 华为技术有限公司

清除 DLDP 的统计信息

背景信息

> **注意**
>
> 清除 DLDP 的统计信息后，DLDP 的统计信息将被清零，已删除的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在用户视图下执行命令 **reset dldp statistics** [**interface** *interface-type interface-number*]，清除端口的 DLDP 报文统计信息。

----结束

9.1.5 配置举例

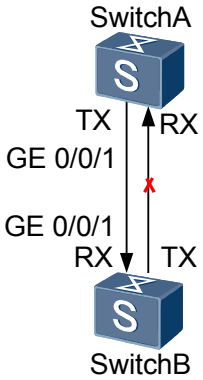
介绍 DLDP 的组网举例。

DLDP 配置举例

组网需求

如图 9-3 所示，两台 AC6605 对接时有一对光纤相连，其中 RX 表示光纤接收端，TX 表示光纤发送端。在两端接口配置 DLDP 功能，如果 SwitchA 的 RX 线突然发生故障，SwitchA 则无法收到信号，SwitchA 的 GE0/0/1 接口物理 Down，不再收发任何报文。但是 SwitchB 的 TX 线还能发送信号，SwitchB 也能收到信号，因此 SwitchB 的链路状态还是 Up 状态。若 SwitchB 在邻居老化定时器超时前收不到邻居 SwitchA 发送的 DLDP 报文，SwitchB 的 GE0/0/1 变为单通状态。为了防止网络故障，DLDP 会自动抑制 SwitchB 处于单通状态的 GE0/0/1 接口。

图 9-3 一条光纤断路示例



版权所有 © 华为技术有限公司

配置思路

采用如下思路配置 DLDP 功能：

1. 配置两端接口工作在非自协商模式下。
2. 使能 DLDP 功能。
3. 配置 DLDP 的工作模式。
4. 配置发送 Advertisement 报文的时间间隔。
5. 配置 DelayDown 定时器的超时时间。
6. 配置发现单向链路后端口的关闭模式。
7. 配置 DLDP 报文的认证方式。

数据准备

为完成此配置例，需准备如下的数据：

- 需要配置的接口类型和编号
- 通告报文的时间间隔
- DelayDown 定时器的超时时间

操作步骤

步骤 1 配置接口处于非自协商状态

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] undo negotiation auto
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤 2 使能全局的 DLDP 功能

```
[SwitchA] dldp enable
```

步骤 3 使能端口的 DLDP 功能

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] dldp enable
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤 4 配置 DLDP 的工作模式为增强模式

```
[SwitchA] dldp work-mode enhance
```

步骤 5 配置发送 Advertisement 报文的时间间隔为 80 秒

```
[SwitchA] dldp interval 80
```

步骤 6 配置 DelayDown 定时器的超时时间为 4 秒

```
[SwitchA] dldp delaydown-timer 4
```

步骤 7 配置发现单向链路后端口的关闭模式为自动模式

```
[SwitchA] dldp unidirectional-shutdown auto
```

步骤 8 配置 DLDP 报文的认证方式 simple 方式，密码为 12345

```
[SwitchA] dldp authentication-mode simple 12345
```


版权所有 © 华为技术有限公司

对 SwitchB 重复上述步骤配置。

步骤 9 检查配置结果

配置完成后，**display dldp** 命令可以看到接口下 DLDP 状态为 **advertisement**

```
[SwitchA] display dldp interface gigabitethernet 0/0/1

Interface GigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:0018-2000-0083
   Neighbor port index:27
   Neighbor state:two way
   Neighbor aged time:185
```

如图 9-3 所示，如果拔掉 SwitchA 上的接收端光纤，SwitchA 和 SwitchB 的接口 GE0/0/1 出现单向链路时，DLDP 会自动阻塞 SwitchB 的 GE0/0/1 接口。

#使用 **display dldp** 命令查看 SwitchA 的 GE0/0/1 接口的 DLDP 状态为 inactive。SwitchB 的 GE0/0/1 接口的 DLDP 状态为 disable。

```
[SwitchA] display dldp interface gigabitethernet 0/0/1

Interface GigabitEthernet0/0/1
 DLDP port state: inactive
 DLDP link state: down
 The neighbor number of the port is: 0
[SwitchB] display dldp interface gigabitethernet 0/0/1

Interface GigabitEthernet0/0/1
 DLDP port state: disable
 DLDP link state: up
 The neighbor number of the port is: 0
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 dldp enable
 dldp interval 80
 dldp delaydown-timer 4
 dldp authentication-mode simple 12345
#
interface GigabitEthernet0/0/1
 dldp enable
 undo negotiation auto
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 dldp enable
 dldp interval 80
 dldp delaydown-timer 4
 dldp authentication-mode simple 12345
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 dldp enable
 undo negotiation auto
#
return
```

9.2 Smart Link 和 Monitor Link 配置

介绍 Smart Link 和 Monitor Link 的基本知识、配置方法和配置实例。

9.2.1 Smart Link 和 Monitor Link 概述

介绍 Smart Link 和 Monitor Link 的基本概念。

双上行组网是目前常用应用组网之一，该组网下通过生成树协议阻塞冗余链路，起备份作用。当主用链路故障时，将流量切换到备用链路。虽然这种方案从功能上可以实现客户冗余备份的需求，但是在性能上却不能达到很多用户的要求，因为即使采用快速生成树协议的快速迁移，也只能是秒级的收敛速度。这对于应用于电信级网络核心的高端以太网交换机，是非常不利的一个性能参数。

基于上述原因，我们提出了 Smart Link 解决方案，针对双上行组网，实现主备链路冗余备份及快速迁移。该方案为双上行组网量身定做，既保证了性能，又简化了配置。

Monitor Link 是为了对 Smart Link 进行补充而引入的，是一种接口联动的方案。Monitor Link 组中包括一个上行链路接口和若干个下行链路接口，当上行链路接口出现故障后，Monitor Link 组会自动 shutdown 下行链路接口。当上行链路接口恢复后也会将下行链路接口恢复。

9.2.2 配置 Smart Link 组基本功能

介绍如何配置 Smart Link 基本功能，包括绑定 VLAN 与实例、创建 Smart Link 组、使能组功能、配置主从接口、使能回切功能以及配置 Flush 报文等。

建立配置任务

应用环境

如图 9-4 所示，位于接入汇聚层的 SwitchD 和 SwitchE 设备以双归属方式连接到上行设备，这样可以提供更好的安全性，也能够缩短由于链路故障造成的业务中断时间。

版权所有 © 华为技术有限公司

图 9-4 Smart Link 应用环境

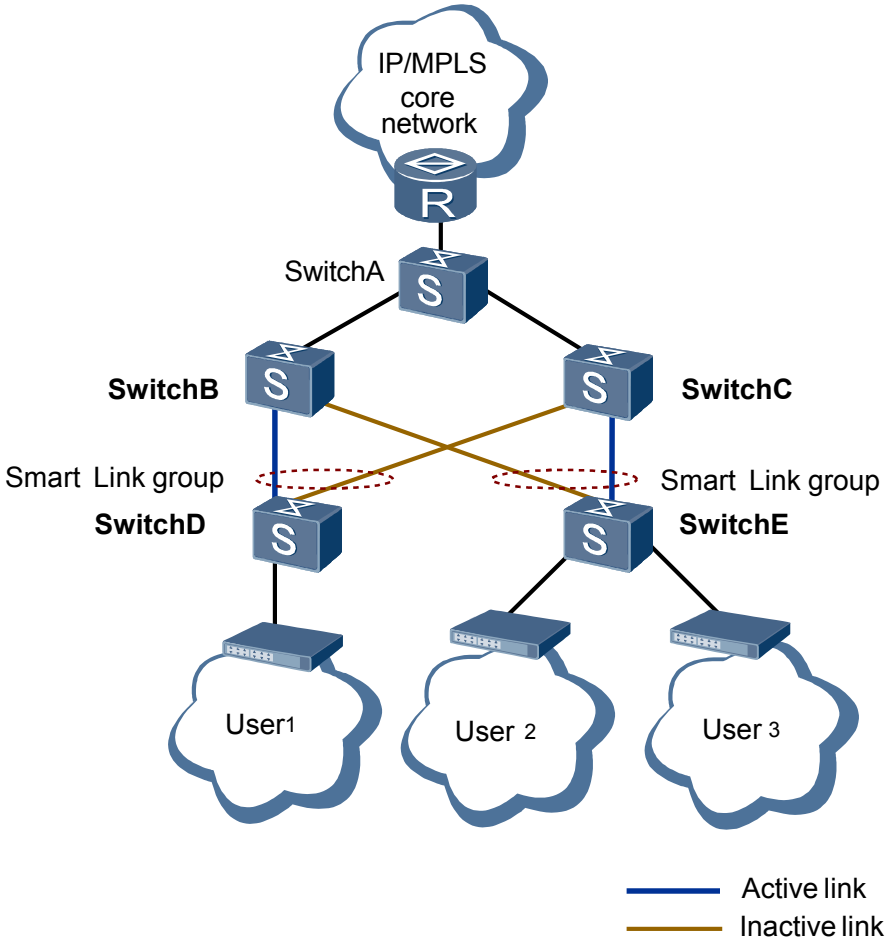


图 9-4 中，SwitchD 和 SwitchE 连接用户设备，再通过双归属连接到 SwitchB 和 SwitchC 上。在 SwitchD 和 SwitchE 上分别配置 Smart Link，将两个上行接口加入 Smart Link 组，可以避免出现环路，同时能够保证由于链路故障造成的业务中断时间为毫秒级。

前置任务

在配置 Smart Link 组基本功能之前，需完成以下任务：

- 确保加入 Smart link 组的主接口和从接口没有使能 MSTP、RRPP 功能。

数据准备

在配置 Smart Link 组基本功能之前，需要准备以下数据。

序号	数据
1	加入 Smart Link 组接口的编号。
2	创建 Smart Link 组的 ID。
3	与实例绑定的 VLAN 编号。

版权所有 © 华为技术有限公司

序号	数据
4	发送 Flush 报文携带的控制 VLAN 编号。
5	（可选）发送 Flush 报文携带的密码。

创建 Smart Link 组

背景信息

请在需要配置 Smart Link 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，创建 Smart Link 组并进入 Smart Link 组视图。

AC6605 设备最多支持创建 16 个 Smart Link 组。

步骤 3 （可选）执行命令 **protected-vlan reference-instance** { *instance-id1* [**to** *instance-id2*] } &<1-10>，配置 Smart Link 组绑定的保护实例。

Smart Link 组功能只在绑定保护实例映射的 VLAN 上生效。STP Instance 的配置方法请参见**配置 MST 域并激活**。

----结束

配置 Smart Link 组主接口和从接口

背景信息

Smart Link 组中的从接口在组启动后会被阻塞。

下面几种情况，接口不能加入到 Smart Link 组中。

- 该接口是 RRPP 接口
- 该接口已经使能 STP 功能
- 该接口已经加入 Eth-Trunk
- 该接口已经加入 Monitor Link 组
- 该接口已经加入其它 Smart Link 组

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **stp disable**，去使能接口的 STP 功能。

步骤 4 执行命令 **quit**，退出接口视图。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 5 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 6 执行命令 **port** *interface-type interface-number* **master**，将接口加入 Smart Link 组，并指定为主接口。

步骤 7 执行命令 **port** *interface-type interface-number* **slave**，将另外一个接口加入 Smart Link 组，并指定为从接口。

一个 Smart Link 组包括一个主接口和一个从接口。缺省情况下，Smart Link 组中不存在接口。

----结束

使能 Flush 报文发送功能

背景信息

当 Smart Link 组发生链路倒换时，原有的转发表项将不适用于新的拓扑网络，需要整个网络进行 MAC 表项和 ARP 表项的更新。这时，Smart Link 组通过发送 Flush 报文通知其他设备进行 MAC 表和 ARP 表项的刷新操作。

由于 Flush 报文格式的定义根据厂商不同会有所区别，因此这里配置的 Flush 报文只用于华为 S 系列交换机设备之间的通信。且对端设备必须使能 Flush 报文接收功能。

在 Smart Link 组视图下配置 **flush send control-vlan** *vlan-id* [**password simple** *password*] 命令，将允许本 Smart Link 组发送 Flush 报文，并且携带指定的控制 VLAN 编号和密码。其中 *vlan-id* 必须是 AC6605 设备上已经存在的 VLAN 的编号，如果 AC6605 设备上不存在指定的 VLAN，Flush 报文将会发送失败。

请在图 9-4 中 SwitchD 和 SwitchE 上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **flush send control-vlan** *vlan-id* [**password simple** *password*]，使能 Flush 报文发送功能，并配置 Flush 报文携带的控制 VLAN 编号和密码。

控制 VLAN 不能是负载分担实例映射的 VLAN。

两端设备配置的 Flush 报文的控制 VLAN ID 和密码要相同。即发送 Flush 报文的设备配置的控制 VLAN ID 和密码与接收 Flush 报文的设备配置的控制 VLAN ID 和密码要相同。

说明

配置此命令并不能把端口加入到控制 VLAN，需要在端口下配置允许此控制 VLAN 通过。

----结束

（可选）配置 Smart Link 组负载分担功能

背景信息

在 AC6605 上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行命令 **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，配置实例和 VLAN 的映射关系。

一个域中最多可创建 49 个实例，其中 Instance 0 为缺省配置，不需要创建。

缺省情况下，所有的 VLAN 都映射到 Instance 0。

步骤 4 执行命令 **active region-configuration**，激活 MST 域的配置。

配置 MST 域的域名、VLAN 映射表和 MSTP 修订级别时，必须执行命令 **active region-configuration** 才可以使配置生效。

步骤 5 执行命令 **quit**，返回系统视图。

步骤 6 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 7 执行命令 **load-balance instance** { *instance-id1* [**to** *instance-id2*] } &<1-10> **slave**，用来配置该实例绑定的 VLAN 报文从备用端口发送，实现负载分担方式。

----结束

（可选）使能 Smart Link 组回切功能并设置回切时间

背景信息

当 Smart Link 组中主链路出现故障时，会自动倒换到从链路。当原主链路故障恢复后，为了保持流量稳定，它将维持在阻塞状态，不进行抢占。如果需要将其恢复为主链路，可以通过如下两种方法实现：

- 使能 Smart Link 组回切功能。在回切定时器超时后会自动倒换主链路。
- 使用 **smart-link manual switch** 命令强制执行链路倒换。

说明

组内两成员接口都处于 Up 状态才能完成链路倒换。

请在需要配置 Smart Link 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **restore enable**，使能 Smart Link 组的回切功能。

缺省情况下，Smart Link 组回切功能处于关闭状态。

步骤 4（可选）执行命令 **timer wtr** *wtr-time*，设置 Smart Link 组回切时间。

缺省情况下，Smart Link 组回切时间为 60 秒。

----结束

版权所有 © 华为技术有限公司

（可选）使能 Flush 报文接收功能

背景信息

只有为接口配置了控制 VLAN 编号并将接口加入该 VLAN，接口才能接收到 Flush 报文。

请在图 9-4 中的 SwitchA、SwitchB 和 SwitchC 上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，分别进入 SwitchA、SwitchB 和 SwitchC 三台设备下行接口的接口视图。

步骤 3 执行命令 **smart-link flush receive control-vlan** *vlan-id* [**password simple** *password*]，使能 Flush 报文接收功能，并配置接口接收 Flush 报文携带的控制 VLAN 编号和密码。

密码是可选项，若不配置表示不使用密码验证。如果重新配置控制 VLAN 编号，密码也需要重新配置。

两端设备配置的 Flush 报文的控制 VLAN ID 和密码要相同。即发送 Flush 报文的设备配置的控制 VLANID 和密码与接收 Flush 报文的设备配置的控制 VLANID 和密码要相同。

----结束

（可选）配置 Smart Link 倒换的延时时间

背景信息

如果由于链路闪断导致的 Smart link 倒换，会影响报文转发和系统性能，可以通过配置 Smart Link 倒换的延时解决此问题。如果 Smart Link 组的接口有 up/down 动作，Smart Link 组的状态不会立刻倒换，而是等待延时时间到达后，根据 Smart Link 组的接口最后获得的 up/down 状态处理 Smart Link 组的状态，从而抑制了由于链路闪断导致的 Smart link 倒换。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart-link 组视图。

步骤 3 执行命令 **smart-link hold-time** *hold-time*，配置 Smart Link 倒换的延时时间。

----结束

使能 Smart Link 组

背景信息

Smart Link 组功能使能后，会阻塞组中的从接口。Smart Link 组功能关闭后，会将被阻塞的从接口恢复正常。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **smart-link enable**，使能 Smart Link 组功能。

----结束

检查配置结果

操作步骤

- 使用命令 **display smart-link group** { **all** | *group-id* }查看 Smart Link 组状态信息。
- 使用命令 **display smart-link flush** 查看接收到的 Flush 报文信息。

----结束

任务示例

使用命令 **display smart-link group** { **all** | *group-id* }查看 Smart Link 组的状态信息。显示如下：

```
<Quidway> display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 1 to 2
    There is no protected-vlan reference-instance
    DeviceID: 0018-2000-0083  Control-vlan ID: 20
      Member            Role    State     Flush Count  Last-Flush-Time
  ------------------------------------------------------------------------
  GigabitEthernet0/0/1  Master  Active    1            2008/11/21 16:37:20 UTC+05:00
  GigabitEthernet0/0/2  Slave   Inactive  2            2008/11/21 17:45:20 UTC+05:00
```

如果配置正确将能得到如下信息：

- Smart Link 组功能已经使能，显示为“Smart link group was enabled.”。
- Smart Link 组中接口状态，包括接口在组中的角色、发送 Flush 报文的数量、发送最后一个 Flush 报文的时间等。如上面显示信息中，接口 GE0/0/1 是 Smart Link 组中的主接口，当前处于转发状态，发送过 1 个 Flush 报文且发送时间是 2008 年 11 月 21 日 16 时 37 分 20 秒。
- 发送 Flush 报文携带的控制 VLAN 编号是用户配置的编号，这里是 20。

执行命令 **display smart-link flush**，可以看到接收到 Flush 报文的信息。

```
<Quidway> display smart-link flush
Receive flush packets count:                1191
Receive last flush interface:               GigabitEthernet0/0/1
Receive last flush packet time:             16:48:53 UTC+05:00 2009/02/23
Receive last flush packet source mac:       0018-0202-0088
Receive last flush packet control vlan ID:  20
```

9.2.3 配置 Smart Link 组数据流策略

介绍如何配置 Smart Link 组高级功能，包括数据流锁定和手动切换链路。

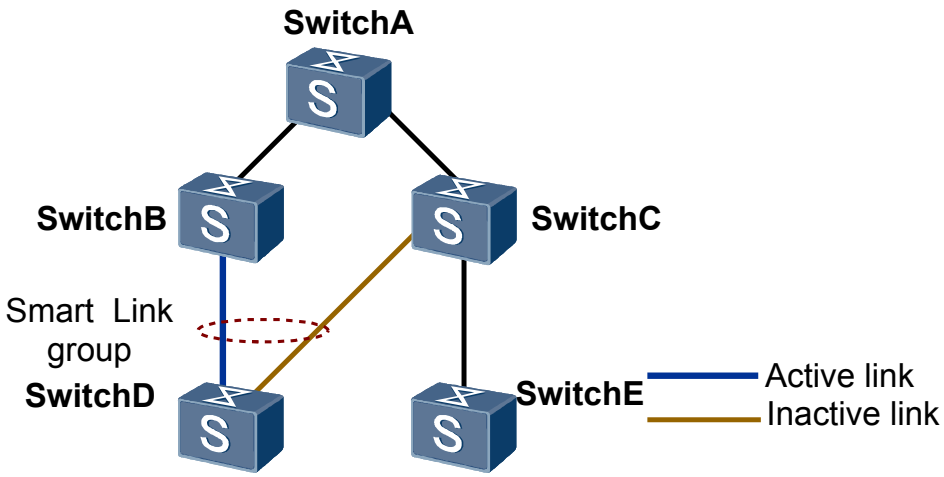
版权所有 © 华为技术有限公司

建立配置任务

应用环境

如图 9-5 所示，在设备 SwitchD 上配置了 Smart Link 组基本功能，并使能了回切功能。维护中需要对 Smart Link 组的主链路进行检修，为了不影响正常的业务，需对 Smart Link 组进行数据流策略的配置，将数据流强制锁定到从链路上，检修完毕后再将数据流倒换到主链路上。

图 9-5 配置数据流策略



前置任务

在配置 Smart Link 组数据流策略之前，需完成以下任务：

- 9.2.2 配置 Smart Link 组基本功能

数据准备

无

配置将数据流锁定在主接口

背景信息

注意

将数据流锁定在主接口后，如果主接口发生故障，此时不会自动切换到从接口，从而会导致流量中断。

在图 9-5 中 SwitchD 上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **smart-link lock**，将数据流锁定在主接口上。

----结束

配置将数据流锁定在从接口

背景信息

注意

将数据流锁定在从接口后，如果从接口发生故障，此时不会自动切换到主接口，从而会导致流量中断。

在图 9-5 中 SwitchD 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **smart-link force**，将数据流锁定在从接口上。

----结束

配置数据流手工倒换

背景信息

在图 9-5 中 SwitchD 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-link group** *group-id*，进入 Smart Link 组视图。

步骤 3 执行命令 **smart-link manual switch** 执行链路倒换。

成功实现主备链路倒换需要满足如下条件：

- 两个成员接口必须都存在，且均处于 Up 状态。
- 没有使用 **smart-link** 命令启动数据流锁定功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

在 Smart Link 组视图下可以重复使用本命令，每配置一次执行一次链路倒换。链路倒换会出现暂时的丢包，持续时间为毫秒级。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display smart-link group** { **all** | *group-id* }查看 Smart Link 组状态信息。

----结束

任务示例

在配置成功时，执行命令 **display smart-link group** { **all** | *group-id* }，应能正确显示是否配置数据流锁定功能以及锁定的位置，这里显示“lock”表示锁定在主接口。如果显示“force”则表示数据流锁定在从接口。

```
<Quidway> display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Link status:lock
  Wtr-time is: 30 sec.
  Load-Balance Instance: 1 to 2
  There is no protected-vlan reference-instance
  DeviceID: 0018-2000-0083  Control-vlan ID: 20
      Member            Role    State     Flush Count  Last-Flush-Time
  ------------------------------------------------------------------------------
  GigabitEthernet0/0/1  Master  Active    1            2008/11/21 16:37:20 UTC+05:00
  GigabitEthernet0/0/2  Slave   Inactive  2            2008/11/21 17:45:20 UTC+05:00
```

9.2.4 配置 Monitor Link 组功能

介绍如何配置 Monitor Link 功能，包括创建 Monitor Link 组、配置上/下行链路接口以及使能回切功能。

建立配置任务

应用环境

如图 9-6 所示，配置了 Smart Link 功能的 AC6605 设备能够对主接口的故障快速响应，将流量倒换到从接口，从而减少业务中断时间。但如果与主接口相连设备的上行链路发生故障，同样会造成业务的中断，这就要求通过一定的方式对上行链路进行监控，在其出现故障后能够让下行链路感知，并做出反应。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 9-6 Monitor Link 应用环境

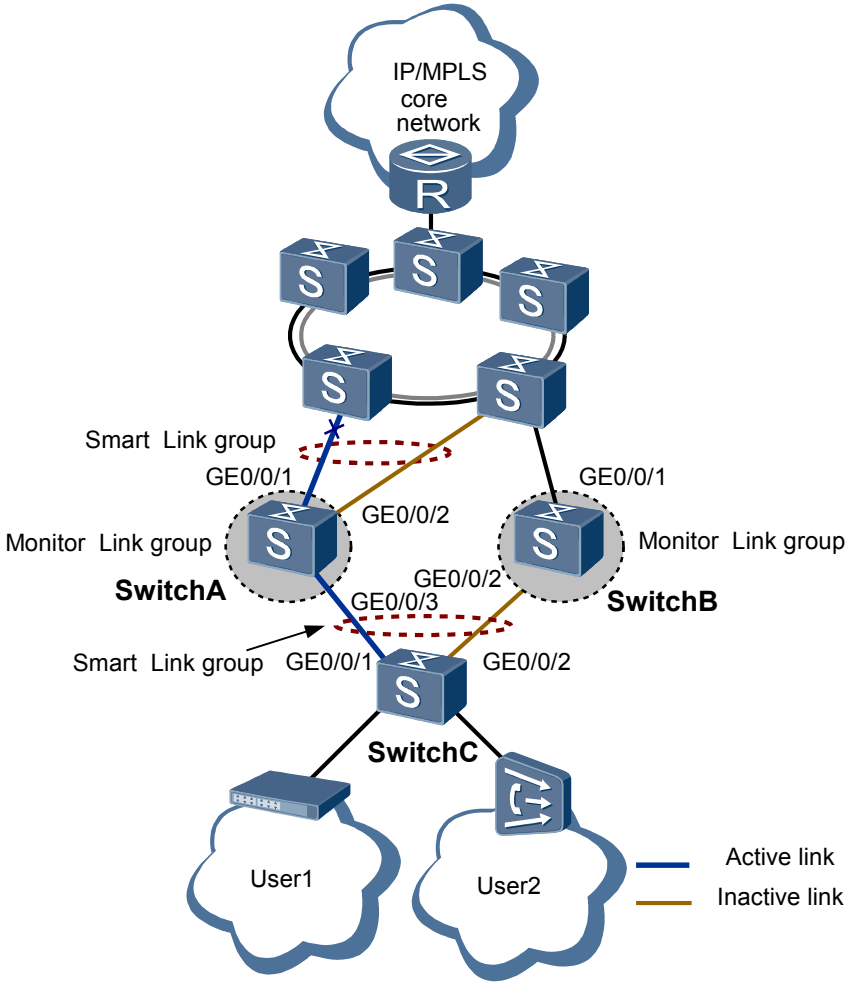


图 9-6 中，如果 SwitchA 的上行链路出现故障，对于 SwitchC 设备，虽然使能了 Smart Link 功能，但由于主链路并没有出现故障因此不会进行链路倒换。此时，会造成业务中断。为了使 Smart Link 组能够更快的对上行链路故障做出响应，在其主链路连接的设备上配置 Monitor Link 功能，对上行链路进行监控。一旦发生故障，迅速将 Smart Link 组的主链路阻塞，这样 Smart Link 组就能感知到故障，从而进行链路倒换，减少业务中断时间。

当上行端口是 Smart Link 组时，只有当 Smart Link 组的两个端口都处于 inactive 状态（包括 DOWN）时，才能认为该上行端口故障。

前置任务

在配置 Monitor Link 组功能之前，需完成以下任务：

- **9.2.2 配置 Smart Link 组基本功能**
- 确保将要加入 Monitor Link 组的接口没有加入 Eth-Trunk、Smart Link 组和其他 Monitor Link 组。

华为专有和保密信息
版权所有 © 华为技术有限公司

数据准备

在配置 Monitor Link 组功能之前，需要准备以下数据。

序号	数据
1	创建 Monitor Link 组的 ID。
2	加入 Monitor Link 组接口的类型和编号。
3	Monitor Link 组回切时间。
4	已创建 Smart Link 组的 ID。

创建 Monitor Link 组

背景信息

在 SwitchA 和 SwitchB 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor-link group** *group-id*，进入 Monitor Link 组视图。

----结束

配置 Monitor Link 组的上行接口和下行接口

背景信息

在 SwitchA 和 SwitchB 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor-link group** *group-id*，进入 Monitor Link 组视图。AC6605 设备最多支持创建 16 个 Monitor Link 组。

步骤 3 执行命令 **port** *interface-type interface-number* { **downlink** [*downlink-id*] | **uplink** }，配置单接口为 Monitor link 组的上行接口或下行接口。或者执行命令 **smart-link group** *group-id* **uplink**，配置 Smart Link 组为 Monitor Link 组的上行链路。

下面三种情况，接口不能加入到 Monitor Link 组中：

- 该接口已经加入 Eth-Trunk
- 该接口已经加入 Smart Link 组
- 该接口已经加入其它 Monitor Link 组

版权所有 © 华为技术有限公司

说明

上行接口的状态决定 Monitor Link 组的状态。因此在下行接口加入到 Monitor Link 组后，虽然可以通过命令 **shutdown** 或 **undo shutdown** 对其进行操作，但操作效果只能维持到 Monitor Link 组中上行接口状态发生改变之前。当上行接口状态发生改变后，下行接口状态会被重新配置，即：

- 若 Monitor Link 组添加 Up 状态的上行接口或组中已存在 Down 状态的上行接口变为 Up 状态，则所有下行接口均被 **undo shutdown**。
- 若从 Monitor Link 组中删除上行接口或者组中已存在 Up 状态的上行接口变为 Down 状态，则所有下行接口均被 **shutdown**。

如果要将 Smart Link 组加入到 Monitor Link 组中，需要先将 Monitor Link 组中已经存在的上行链路接口删除。

----结束

配置 Monitor Link 组的回切时间

背景信息

在 SwitchA 和 SwitchB 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **monitor-link group** *group-id*，进入 Monitor Link 组视图。

步骤 3 执行命令 **timer recover-time** *recover-time*，配置自动回切时间。

缺省情况下，Monitor Link 组的回切功能处于使能状态，且默认回切时间为 3 秒。

----结束

检查配置结果

操作步骤

步骤 1 使用命令 **display monitor-link group** { **all** | *group-id* }查看 Monitor Link 组的基本配置信息。

----结束

任务示例

在配置成功时，执行命令 **display monitor-link group** { **all** | *group-id* }，应能看到加入组接口的基本信息，包括接口角色、状态以及最后一次变为 Up 或 Down 状态的时间。

```
<Quidway> display monitor-link group 1
  Monitor Link group 1 information :
  Recover-timer is 5 sec.
    Member             Role      State Last-up-time                    Last-down-time
 GigabitEthernet0/0/1   UpLk      UP    0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
 GigabitEthernet0/0/2   DwLk[1]   DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
```


版权所有 © 华为技术有限公司

9.2.5 维护

介绍如何调试 Smart Link。

调试 Smart Link

背景信息

说明

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

- 使用命令 **debugging smart-link** { **all** | **error** | **event** | **fsm-machine** } [**group** *group-id*] 打开 Smart link 的调试开关。
- 使用命令 **debugging smart-link flush** { **all** | **receive** |**send** } 打开 Flush 报文的调试开关。

----结束

9.2.6 配置举例

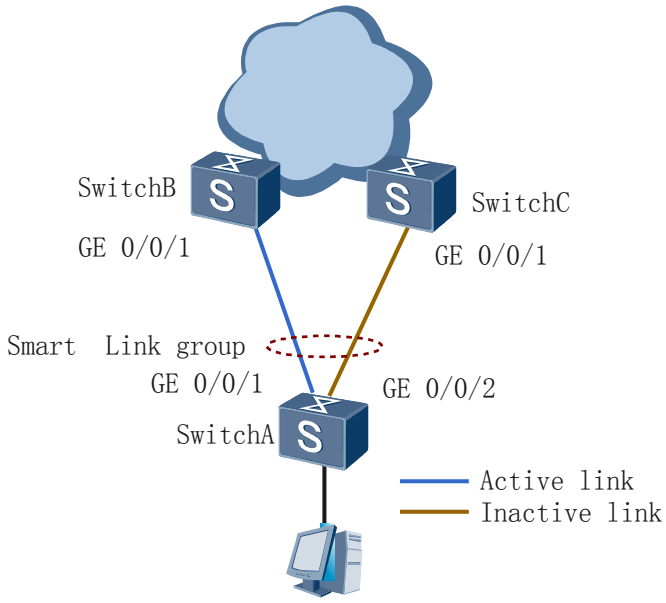
介绍 Smart Link 的组网举例。

配置 Smart Link 基本功能示例

组网需求

如图 9-7 所示，为了保证网络的可靠性，用户侧网络采用双归属上行方式连接到城域网。同时，要保证在主链路发生故障时，主链路报文能够快速切换到从链路，并且使业务中断时间控制在毫秒级。

图 9-7 配置 Smart Link 基本功能示例组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 Smart Link 基本功能：

1. SwitchA 上配置 Smart Link 组，并将上行链路加入组中。
2. SwitchA 上使能回切功能。
3. SwitchA 上使能发送 Flush 报文功能。
4. SwitchB 和 SwitchC 两台设备上使能 Flush 报文接收功能。
5. SwitchA 上使能 Smart Link 组功能。

数据准备

为完成此配置示例，需准备如下的数据：

- 创建 Smart Link 组的 ID。
- SwitchA 上行链路接口编号。
- 发送 Flush 报文携带的控制 VLAN 编号和密码。

操作步骤

步骤 1 在 SwitchA 上配置控制 VLAN，并将接口加入该 VLAN 中

```
<SwitchA> system-view
[SwitchA] vlan batch 10
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
```

SwitchB 和 SwitchC 配置同 SwitchA 相似。

步骤 2 将去使能 STP 功能的上行接口加入 Smart Link 组并指定为主接口或从接口

配置 SwitchA。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] port gigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port gigabitethernet 0/0/2 slave
```

步骤 3 使能回切功能并设置回切时间

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

步骤 4 使能发送 Flush 报文功能

配置 SwitchA。

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
```


版权所有 © 华为技术有限公司

步骤 5 在 SwitchA 使能 Smart Link 组功能

```
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

步骤 6 使能接收 Flush 报文功能

配置 SwitchB。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password simple 123
[SwitchB-GigabitEthernet0/0/1] quit
```

配置 SwitchC。

```
<SwitchC> system-view
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password simple 123
[SwitchC-GigabitEthernet0/0/1] quit
```

步骤 7 验证配置结果

使用 **display smart-link group** 命令查看 SwitchA 上的 Smart Link 组信息。如果显示如下信息，则表示配置成功。

- Smart Link 组功能已经使能
- 控制 VLAN 编号为 10
- 接口 GE0/0/1 为主接口且处于 Active 状态，接口 GE0/0/2 为从接口且处于 Inactive。

```
<SwitchA> display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Active   1           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2         Slave  Inactive 0           0000/00/00 00:00:00 UTC+00
:00
```

使用 **shutdown** 命令关闭接口 GE0/0/1，可以看到接口 GE0/0/1 已经处于 Inactive 状态，接口 GE0/0/2 为 Active 状态。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] shutdown
[SwitchA-GigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494  Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Inactive 1           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2          Slave  Active   1           0000/00/00 00:00:00 UTC+00
:00
```


版权所有 © 华为技术有限公司

使用 **undo shutdown** 命令开启接口 GE0/0/1，等待 30 秒后，可以看到接口 GE0/0/1 处于 Active 状态，接口 GE0/0/2 为 Inactive 状态。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] undo shutdown
[SwitchA-GigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Active   2           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2          Slave  Inactive 1           0000/00/00 00:00:00 UTC+00
:00
```

----结束

配置文件

- 设备 SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
smart-link group 1
 restore enable
 smart-link enable
 port GigabitEthernet0/0/1 master
 port GigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

- 设备 SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

- 设备 SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10
```


版权所有 © 华为技术有限公司

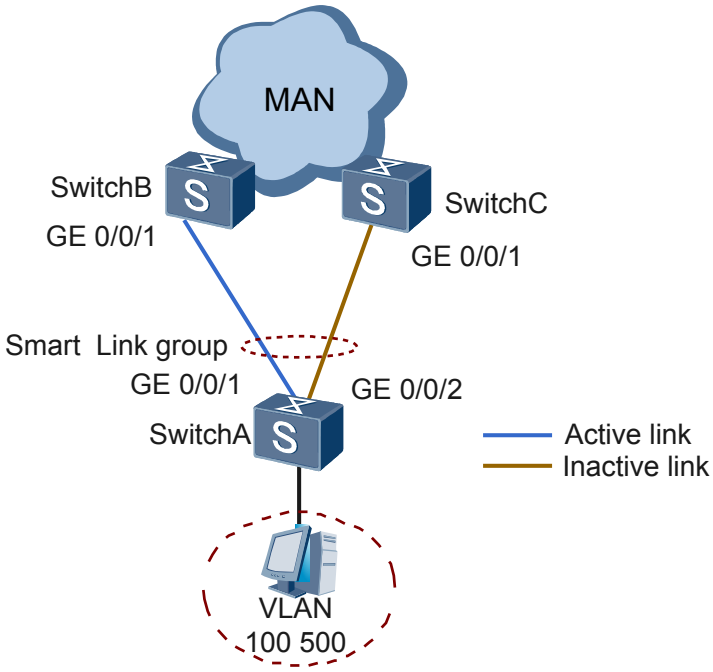
```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

配置 Smart Link 主备链路负载分担示例

组网需求

如图 9-8 所示，VLAN 100 和 VLAN 500 报文走备份链路，其他报文走主链路。为了保证网络的可靠性，用户侧网络采用双归属上行方式连接到城域网，VLAN 100 和 VLAN 500 报文走备份链路，其他报文走主链路。在主链路发生故障时，主链路报文能够快速切换到从链路；备份链路发生故障后，VLAN 100 和 VLAN 500 的报文能够快速切换到主链路，并且使业务中断时间控制在毫秒级。

图 9-8 配置 Smart Link 主备链路冗余备份示例组网图



配置思路

采用如下的思路配置 Smart Link 基本功能：

1. SwitchA 上配置 Smart Link 组多实例，并将上行链路加入组中。
2. 在 SwitchA 上配置负载分担功能。
3. SwitchA 上使能回切功能。
4. SwitchA 上使能发送 Flush 报文功能。
5. SwitchB 和 SwitchC 两台设备上使能 Flush 报文接收功能。
6. SwitchA 上使能 Smart Link 组功能。

版权所有 © 华为技术有限公司

数据准备

为完成此配置示例，需准备如下的数据：

- SwitchA 实例编号和要绑定的 VLAN 编号。
- 创建 Smart Link 组的 ID。
- SwitchA 上行链路接口编号。
- 发送 Flush 报文携带的控制 VLAN 编号和密码。

操作步骤

步骤 1 在 SwitchA 上配置控制 VLAN，并将上行链路接口加入该 VLAN 中

```
<SwitchA> system-view
[SwitchA] vlan batch 10 100 500
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 100 500
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 100 500
[SwitchA-GigabitEthernet0/0/2] quit
```

SwitchB 和 SwitchC 配置同 SwitchA 相似。

步骤 2 在 SwitchA 上配置 VLAN 映射。

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 10 vlan 100 500
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

步骤 3 将去使能 STP 功能的上行接口加入 Smart Link 组并指定为主接口或从接口

配置 SwitchA

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] port gigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port gigabitethernet 0/0/2 slave
```

步骤 4 在 SwitchA 上配置负载分担功能。

```
[SwitchA-smlk-group1] load-balance instance 10 slave
```

步骤 5 使能回切功能并设置回切时间

配置 SwitchA

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

步骤 6 使能发送 Flush 报文功能

配置 SwitchA

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
```

步骤 7 在 SwitchA 使能 Smart Link 组功能

版权所有 © 华为技术有限公司

```
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

步骤 8 使能接收 Flush 报文功能

配置 SwitchB

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password simple 123
[SwitchB-GigabitEthernet0/0/1] quit
```

配置 SwitchC。

```
<SwitchC> system-view
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password simple 123
[SwitchC-GigabitEthernet0/0/1] quit
```

步骤 9 验证配置结果

使用 **display smart-link group** 命令查看 SwitchA 上的 Smart Link 组信息。如果显示如下信息，则表示配置成功。

- Smart Link 组功能已经使能
- 控制 VLAN 编号为 10
- 接口 GE0/0/1 为主接口且处于 Active 状态，接口 GE0/0/2 为从接口且处于 Inactive。并且配置了负载分担功能。

```
[SwitchA] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
     Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Active   1           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2          Slave  Inactive 0           0000/00/00 00:00:00 UTC+00
:00
```

使用 **shutdown** 命令关闭接口 GE0/0/1，可以看到接口 0GE0/0/1 已经处于 Inactive 状态，接口 GE0/0/2 为 Active 状态。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] shutdown
[SwitchA-GigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
     Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Inactive 1           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2          Slave  Active   1           0000/00/00 00:00:00 UTC+00
:00
```

使用 **undo shutdown** 命令开启接口 0GigabitEthernet/0/1，等待 30 秒后，可以看到接口 0GigabitEthernet/0/1 处于 Active 状态，接口 GigabitEthernet0/0/2 为 Inactive 状态。

版权所有 © 华为技术有限公司

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] shutdown
[SwitchA-GigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------------

  GigabitEthernet0/0/1          Master Active   2           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2          Slave  Inactive 1           0000/00/00 00:00:00 UTC+00
:00
```

----结束

配置文件

- 设备 SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 100 500
#
stp region-configuration
 instance 10 vlan 10 100 500
 active region-configuration
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 stp disable
#
smart-link group 1
 load-balance instance 10 slave
 restore enable
 smart-link enable
 port GigabitEthernet0/0/1 master
 port GigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

- 设备 SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 100 500
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

- 设备 SwitchC 的配置文件

```
#
 sysname SwitchC
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 10 100 500
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

配置 Smart Link 综合应用示例

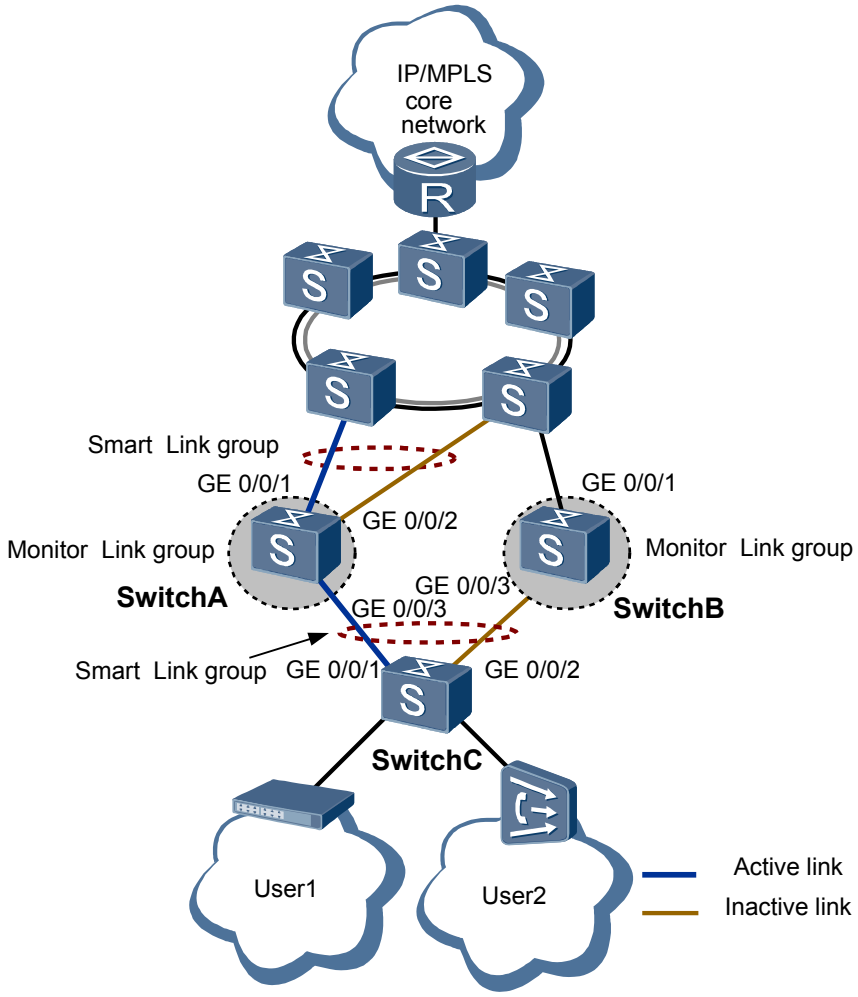
组网需求

如图 9-9 所示，城域网中设备 SwitchC 向下连接用户网络，通过双归属上行连接到 SwitchA 和 SwitchB 两台设备上，最后向上连接到骨干网。

SwitchA 和 SwitchC 两台设备都是通过双归属方式连接到上行设备，为了避免出现环路需要阻塞其中一条链路。同时，在主链路出现故障时，能够将数据流迅速切换到从链路上，保证业务正常。

另外，为了防止上行链路出现故障导致下游业务中断，需要引入一种监控机制。即在上行链路出现故障时，能够使下行链路迅速感知。以便能够及时进行链路切换，缩短业务中断时间。

图 9-9 配置 Smart Link 综合应用示例组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 Smart Link 特性：

1. SwitchA 和 SwitchC 两台设备上配置 Smart Link 组，并将上行链路加入组中。
2. SwitchA 和 SwitchB 两台设备上配置 Monitor Link 组。
3. SwitchA 和 SwitchC 两台设备上使能发送 Flush 报文功能。
4. SwitchA 和 SwitchB 两台设备上使能接收 Flush 报文功能。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA、SwitchB 和 SwitchC 三台设备的接口编号。
- 创建 Smart Link 组的 ID。
- 发送 Flush 报文携带的控制 VLAN 编号和密码。
- 创建 Monitor Link 组的 ID 以及下行链路编号。

操作步骤

步骤 1 在 SwitchA、SwitchB 和 SwitchC 三台设备上配置相同控制 VLAN，并将加入 Smart Link 组或 Monitor Link 组的接口加入该 VLAN 中

略。具体配置方法请参见：《AC6605 无线接入控制器 配置指南-以太网》中的 **VLAN 配置**。

步骤 2 创建 Smart Link 组功能

配置 SwitchA

```
<SwitchA> system-view
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] quit
```

配置 SwitchC

```
<SwitchC> system-view
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] quit
```

步骤 3 将接口加入 Smart Link 组并指定为主接口或从接口

配置 SwitchA

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA]smart-link group 1
[SwitchA-smlk-group1] port gigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port gigabitethernet 0/0/2 slave
```

配置 SwitchC。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] stp disable
```


版权所有 © 华为技术有限公司

```
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] stp disable
[SwitchC-GigabitEthernet0/0/2] quit
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] port gigabitethernet 0/0/1 master
[SwitchC-smlk-group2] port gigabitethernet 0/0/2 slave
```

步骤 4 使能回切功能并设置回切时间

配置 SwitchA

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

配置 SwitchC

```
[SwitchC-smlk-group2] restore enable
[SwitchC-smlk-group2] timer wtr 30
```

步骤 5 使能发送/接收 Flush 报文功能

配置 SwitchA

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
[SwitchA-smlk-group1] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] smart-link flush receive control-vlan 10 password simple 123
[SwitchA-GigabitEthernet0/0/3] quit
```

配置 SwitchB

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] smart-link flush receive control-vlan 10 password simple 123
[SwitchB-GigabitEthernet0/0/3] quit
```

配置 SwitchC

```
[SwitchC-smlk-group2] flush send control-vlan 10 password simple 123
[SwitchC-smlk-group2] quit
```

步骤 6 使能 Smart Link 组

配置 SwitchA。

```
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

配置 SwitchC

```
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] smart-link enable
[SwitchC-smlk-group2] quit
```

步骤 7 创建 Monitor Link 组，并添加上行/下行链路接口

配置 SwitchA

```
[SwitchA] monitor-link group 1
[SwitchA-mtlk-group1] smart-link group 1 uplink
[SwitchA-mtlk-group1] port gigabitethernet 0/0/3 downlink 1
```

配置 SwitchB

```
[SwitchB] monitor-link group 2
[SwitchB-mtlk-group2] port gigabitethernet 0/0/1 uplink
[SwitchB-mtlk-group2] port gigabitethernet 0/0/3 downlink 1
```


版权所有 © 华为技术有限公司

步骤 8 配置 Monitor Link 组的回切时间

配置 SwitchA

```
[SwitchA-mtlk-group1] timer recover-time 10
[SwitchA-mtlk-group1] quit
```

配置 SwitchB

```
[SwitchB-mtlk-group2] timer recover-time 10
[SwitchB-mtlk-group2] quit
```

步骤 9 查看配置结果

```
[SwitchA] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494  Control-vlan ID: 10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  GigabitEthernet0/0/1           Master  Active    1           0000/00/00 00:00:00 UTC+00
:00
  GigabitEthernet0/0/2           Slave   Inactive  0           0000/00/00 00:00:00 UTC+00
:00
[SwitchA] display monitor-link group 1
Monitor Link group 1 information :
  Recover-timer is 10 sec.
    Member              Role     State Last-up-time               Last-down-tim
e
 Smart-link1            UpLk     UP    0000/00/00 00:00:00 UTC+00:00      0000/0
0/00 00:00:00 UTC+00:00
 GigabitEthernet0/0/3          DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00      0000/0
0/00 00:00:00 UTC+00:00
```

----结束

配置文件

- 设备 SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
smart-link group 1
 restore enable
 smart-link enable
 port GigabitEthernet0/0/1 master
 port GigabitEthernet0/0/2 slave
 timer wtr 30
```


版权所有 © 华为技术有限公司

```
 flush send control-vlan 10 password simple 123
#
monitor-link group 1
 smart-link group 1 uplink
 port GigabitEthernet0/0/3 downlink 1
 timer recover-time 10
#
return
```

- 设备 SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
monitor-link group 2
 port GigabitEthernet0/0/1 uplink
 port GigabitEthernet0/0/3 downlink 1
 timer recover-time 10
#
return
```

- 设备 SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
smart-link group 2
 restore enable
 smart-link enable
 port GigabitEthernet0/0/1 master
 port GigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

9.3 RRPP 配置

RRPP(Rapid Ring Protection Protocol)具有收敛速度快，收敛时间与环网上节点数无关及RRPP 多实例支持不同业务流量负载均衡等特点。

版权所有 © 华为技术有限公司

9.3.1 RRPP 概述

RRPP（快速环保护协议），是一个专门应用于以太网环的链路层协议。具有拓扑收敛速度快，防止数据环路引起的广播风暴等优点。

城域网和企业网大多采用环网来构建以提供高可靠性，但环上任意一个节点发生故障都会影响业务。环网采用的技术一般是 RPR 或以太网环。RPR 需要专用硬件，因此成本较高。而随着以太网环的日趋成熟，成本低廉，城域网和企业网采用以太网环的趋势越来越明显。

目前，解决二层网络环路问题的技术有 RSTP/MSTP 和 RRPP（Rapid Ring Protection Protocol）。RSTP/MSTP 应用比较成熟，但收敛时间在秒级。

RRPP 是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速启用备份链路恢复环网上各个节点之间的通信通路。

RRPP 是一个专门应用于以太网环的链路层协议。相比其他以太环网技术，RRPP 具有以下优势。

- 收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
- 在以太网环完整时能够防止数据环路引起的广播风暴。
- 当以太网环上一条链路断开时能迅速启用备份链路以恢复环网上各个节点之间的通信通路。
- 成本低。

9.3.2 AC6605 支持的 RRPP 特性

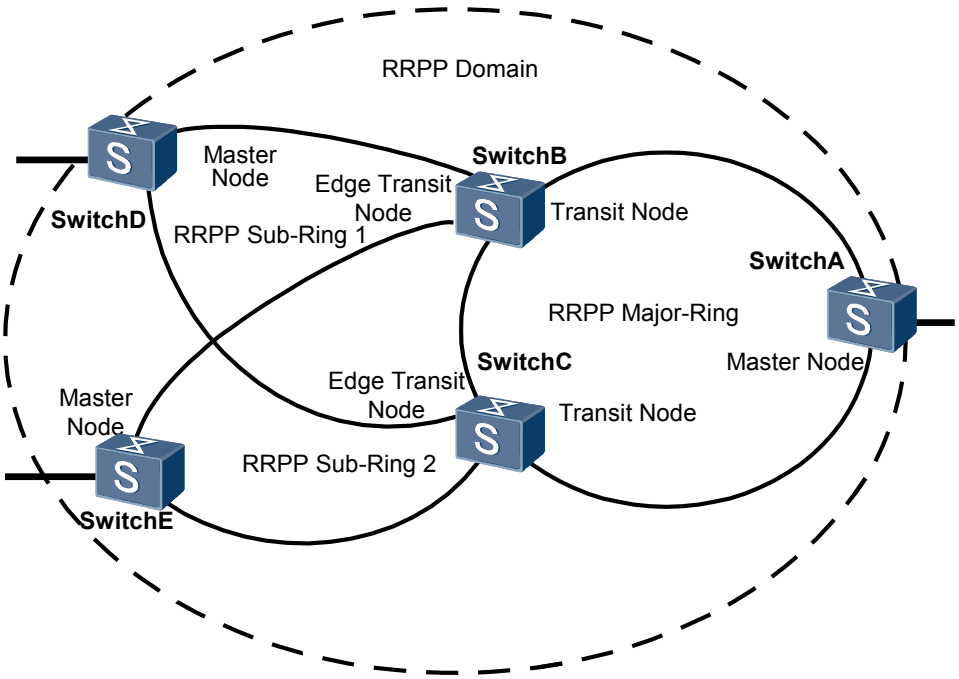
介绍 RRPP 的在 AC6605 上的支持情况。

RRPP 的基本功能

结合图 9-10，介绍 RRPP 的基本概念。

版权所有 © 华为技术有限公司

图 9-10 RRPP 相交环应用场景图



- RRPP 域

  RRPP 域（RRPP Domain）由一组配置了相同的域 ID 和控制 VLAN，且相互连通的交换机群体构成。一个 RRPP 域具有 RRPP 主环和子环、控制 VLAN、主节点、传输节点、主端口和副端口等要素。

  用整数表示的 ID 来唯一标识一个 RRPP 域。

- RRPP 环

  一个 RRPP 环物理上对应一个环形连接的以太网拓扑。每个 RRPP 环都是其所在的 RRPP 域的一个局部单元，一个 RRPP 域可以由一个 RRPP 环或多个彼此相交的 RRPP 环构成。

- RRPP 主环和子环

  如果一个 RRPP 域由彼此相交的 RRPP 环组成，可以通过指定 RRPP 环的级别来设定其中任何一个环是主环，而另外的环就是子环。

  一个 RRPP 域中，只能有一个 RRPP 主环。

  子环的协议报文在主环中作为数据报文传送；主环协议报文只在主环中传送。

- 控制 VLAN

  在 RRPP 域中，控制 VLAN 用来传递 RRPP 协议报文。控制 VLAN 中只能包含 RRPP 端口。

  每个 RRPP 域配有两个控制 VLAN，分别为主控制 VLAN 和子控制 VLAN。配置时只需要指定主控制 VLAN，而把比主控制 VLAN ID 值大 1 的 VLAN 作为子控制 VLAN。

  与控制 VLAN 相对，数据 VLAN 用来传输数据报文。数据 VLAN 中可以包含 RRPP 端口，也可以包含非 RRPP 端口。

- 主节点

版权所有 © 华为技术有限公司

以太网环上每一台交换机都称为一个节点，每个 RRPP 环上必须有一个主节点，而且只能有一个。

- 传输节点

  在 RRPP 环中，除了主节点外的其他节点都是传输节点。

  传输节点负责监测自己直连的 RRPP 链路状态，并把链路变化通知主节点，然后由主节点来决策如何处理传输节点上报的链路变化。

- 边缘节点和辅助边缘节点。

  边缘节点或辅助边缘节点是交换机在子环上的角色，其在主环上的角色为传输节点。

  在 RRPP 子环中，和主环相交的两个节点中，可以任选一个作为边缘节点。一个子环中，有且只能有一个边缘节点。

  在 RRPP 子环中，和主环相交的两个节点中，如果一个被指定为边缘节点，另外一个节点就是辅助边缘节点。

- 主端口和副端口

  主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为副端口，端口的角色由用户的配置决定。

- 公共端口和边缘端口。

  在边缘或辅助边缘节点中，子环和主环公共的端口称为公共端口，只在子环中的端口称为边缘端口。

Hello 和 Fail 定时器

RRPP 检测以太网环的链路状况时，主节点根据 Hello 定时器发送 Hello 报文，根据 Fail 定时器判断副端口是否收到 Hello 报文。

- Hello 定时器值规定了主节点从主端口发送 Hello 报文的周期。
- Fail 定时器值规定了从副端口上接收到 2 次 Hello 报文的最大时间间隔。

RRPP 多实例

- 多实例

  在 RRPP 组网中，一个环上只能有一个主节点。当主节点处于 Complete 状态时，被阻塞的副端口会阻止所有用户报文通过。这样，所有用户报文在 RRPP 环上通过一条路径传输。主节点副端口侧的链路空闲，造成带宽浪费。

  RRPP 多实例基于域实现。在一个域中，所有端口、节点角色、拓扑都遵循基本的 RRPP 原则。与 RRPP 不同的是，RRPP 多实例在一个 RRPP 环上可以存在多个域。

  一个域内可以包含一个或多个实例，每个实例代表一个 VLAN 范围。这些包含在域中的 VLAN，称为 RRPP 域的保护 VLAN。保护 VLAN 包括属于该域的数据 VLAN、主环控制 VLAN 和子环控制 VLAN。

  在 RRPP 多实例组网中，在同一个环路上存在多个主节点。根据主节点的 Secondary Port 阻塞属性即可实现业务流量的负载分担和链路备份。

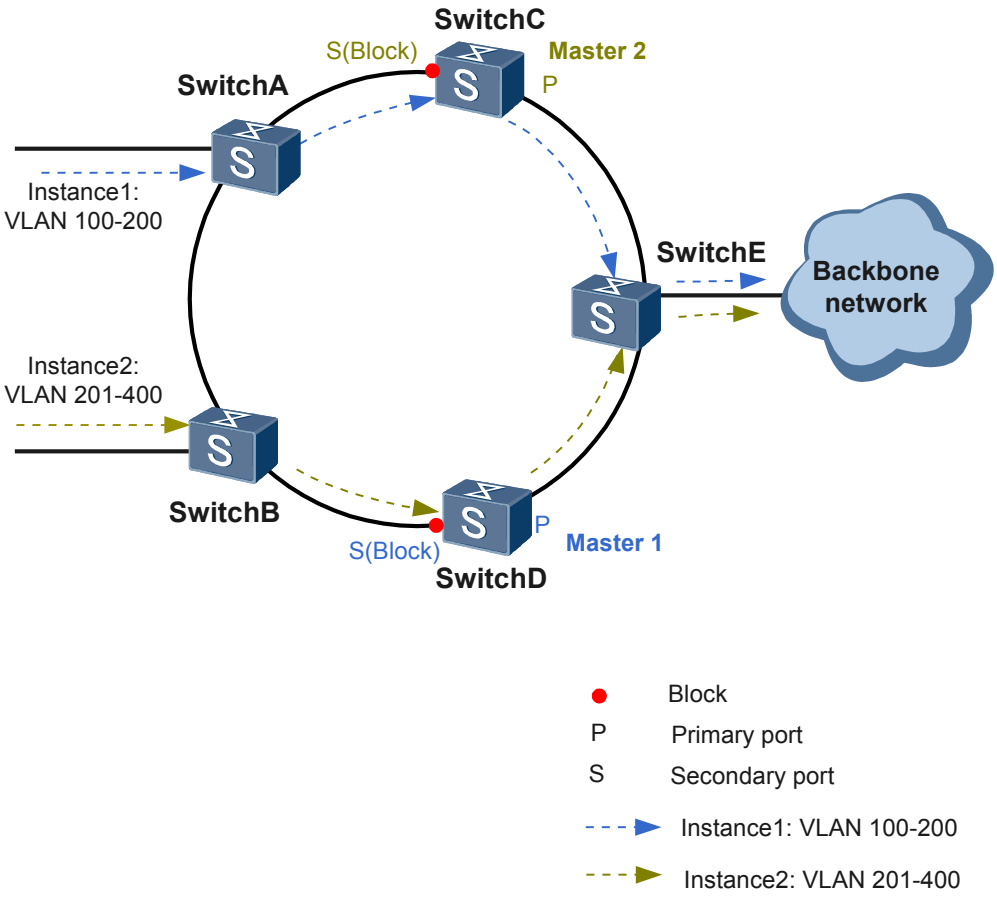
  如图 9-11 所示。在由 SwitchA、B、C、D、E 组成的 RRPP 多实例环上，有两个域。SwitchC 为域 2 的主节点，SwitchD 为域 1 的主节点。主节点的主端口和副端口如图 9-11 所示。

  域 1 包含实例 1，VLAN 范围为 100 ～ 200。当主节点 SwitchD 为 Complete 状态时，副端口被阻塞，因此 VLAN100 ～ VLAN200 的报文上传路径为 SwitchA->SwitchC->SwitchE。

版权所有 © 华为技术有限公司

域 2 包含实例 2，VLAN 范围为 201 ～ 400。当主节点 SwitchC 为 Complete 状态时，副端口被阻塞，因此 VLAN201 ～ VLAN400 的报文上传路径为 SwitchB->SwitchD->SwitchE。

图 9-11 RRPP 多实例组网图



- 环组

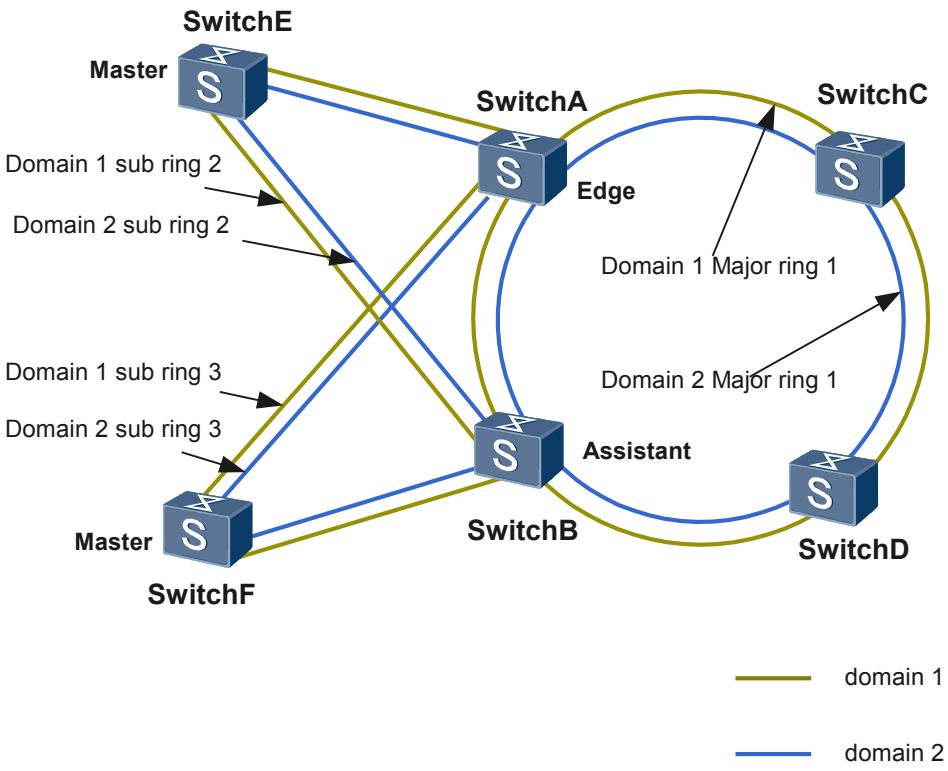
  环组是 RRPP 多实例相交环组网中子环的特性。

  在 RRPP 多实例相交环组网中，如果有多个子环，会出现以下情况：

  多个子环的边缘节点是同一台设备，辅助边缘节点也是同一台设备。并且，边缘节点和辅助边缘节点所对应的主环链路相同。即，这些子环边缘节点的 Edge-Hello 报文沿相同的路径到达辅助边缘节点。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 9-12 RRPP 多实例中的环组



为减少 Edge-Hello 报文的收发数量，提高系统性能。将具有相同边缘节点和辅助边缘节点的一组子环加入环组。选择环组内的一个成员子环发送 Edge-Hello 报文，进行主环上子环协议报文通道的检测。

图 9-12 中的 4 个子环：域 1 环 2、域 1 环 3、域 2 环 2、域 2 环 3 由于有相同的主环链路，因此可以加入一个环组。加入环组后，4 个子环只发送一个 Edge-Hello 报文，减少了 Edge-Hello 报文的收发。

- 链路 Up 时延定时器

  在主节点上启动链路 Up 时延定时器，可避免频繁地改变流量传输路径，造成环路振荡。

  主节点在 Failed 定时器超时时间内收到自身的 Hello 报文后，不会立刻状态迁移至 Complete 状态，而是要经过延时时间后状态迁移至 Complete，从而减小链路状态的振荡。

  定时器超时后，才会处理副端口收到的 Hello 报文。

9.3.3 配置 RRPP 基本功能

RRPP 通过将以太环网上的设备配置为 RRPP 环上不同角色的节点。各个节点之间通过收发和处理 RRPP 协议报文来检测环网状态，传递环网拓扑变化信息，由环上的决策节点即主节点来根据环网状态适时的阻塞或放开其副端口。这样在环网上设备或链路发生故障时，能达到迅速启用备份链路并消除环路的目的。

建立配置任务

同一端口上使能了 RRPP 协议，不能再使能 STP 协议。即，两种协议不能同时配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

应用环境

RRPP 主要应用于单环或多环相交的组网环境。配置 RRPP 时，需要为 RRPP 环上的每个节点配置角色。

说明

同一端口上只能配置 RRPP 协议或者 STP 协议中的一种，不能两种协议同时配置。

RRPP 没有自动选举机制，因此只有为环网上的每个节点进行正确配置，才能让协议真正实现环网的检测和保护。请注意保证配置的正确性。

前置任务

在配置 RRPP 的特性功能之前，需完成以下任务：

- 在物理上搭建环形拓扑的组网环境
- 配置接口的链路属性

数据准备

在配置 RRPP 的基本功能之前，需准备以下数据。

序号	数据
1	RRPP 域的 ID
2	RRPP 域控制 VLAN 的 ID
3	RRPP 域中各个 RRPP 环的 ID
4	RRPP 域的 Hello 定时器、Fail 定时器的值
5	RRPP 环的端口名

创建实例

背景信息

请在需要加入 RRPP 多实例域的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行以下步骤，配置多生成树实例与 VLAN 的映射关系。

- 执行命令 **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，配置实例和 VLAN 的映射关系。
- 执行命令 **vlan-mapping modulo** *modulo*，配置实例和 VLAN 按照缺省算法自动分配映射关系。

版权所有 © 华为技术有限公司

vlan-mapping modulo 命令将 VLAN 映射到编号为（VLAN ID-1）%*modulo*+1 的生成树实例上。例如，模值为 16，则 VLAN1 映射到 MSTI1、VLAN2 映射到 MSTI2…… VLAN16 映射到 MSTI16，依次类推。

主环控制 VLAN 和子环控制 VLAN 必须包含在 VLAN 列表中。

一个域中最多可创建 49 个实例，其中 Instance 0 为缺省配置，不需要创建。

缺省情况下，所有的 VLAN 都映射到 Instance 0。

步骤 4 执行命令 **active region-configuration**，激活 MST 域的配置。

----结束

配置 RRPP 环上的接口

背景信息

请在需要加入 RRPP 环的端口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

RRPP 支持的二层端口有 GigabitEthernet 和 Eth-Trunk。

不能把已启用 SmartLink、LDT、MUXVLAN、MSTP 的端口配置成 RRPP 端口。

步骤 3（可选）执行命令 **port link-type trunk**，设置端口为 Trunk 端口。

缺省情况下端口为 Hybrid 端口。

由于 RRPP 端口既要允许控制 VLAN 中的报文通过，又要允许数据 VLAN 中的报文通过，所以应为 Trunk 类型或 Hybrid 类型。

步骤 4 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，或执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置 RRPP 端口允许通过的数据 VLAN。

控制 VLAN 由 RRPP 域视图下的 **control-vlan** 命令指定，并配置了 **ring node-mode** 命令后，会自动成为 RRPP 环上各端口允许通过的控制 VLAN。因此，本步骤中仅需指定数据 VLAN 即可。

步骤 5 执行命令 **stp disable**，去使能端口上的 STP 功能。

缺省情况下，设备所有端口上都使能了 STP 协议。在创建 RRPP 环前，需要先去使能即将加入 RRPP 环中的端口的 STP 功能。

----结束

创建 RRPP 域

一组配置了相同域 ID 和控制 VLAN，并且相互联通的交换机群体构成一个 RRPP 域。一个 RRPP 域主要由 RRPP 环、RRPP 控制 VLAN、主节点等要素组成。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 RRPP 域内每台交换机上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，创建 RRPP 域。

AC6605 上最多可创建 8 个不同的域。

创建 RRPP 域时要指定域的 ID，如果该域已存在则直接进入域视图。

----结束

创建控制 VLAN

每个 RRPP 域具有两个控制 VLAN，主控制 VLAN 中传播的主要是主环的协议报文，子控制 VLAN 中传播的主要是子环的协议报文。

操作步骤

步骤 1 在 RRPP 域内每台交换机上执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **control-vlan** *vlan-id* 命令，创建控制 VLAN。

由参数 *vlan-id* 指定的控制 VLAN 和由 *vlan-id*+1 指定的子控制 VLAN 必须都是未被创建，并且未被 port trunk、mapping、stacking 等方式使用过的 VLAN。

每个 RRPP 域配有两个控制 VLAN，分别为主控制 VLAN 和子控制 VLAN。配置时只需要指定主控制 VLAN，而把比主控制 VLAN ID 值大 1 的 VLAN 作为子控制 VLAN。

控制 VLAN 创建后不能直接修改，只能通过先删除域，然后再重新配置的方式修改。子控制 VLAN 也在删除域时被连带删除。

说明

RRPP 控制 VLAN 不能配置 DHCP 业务。

----结束

配置保护 VLAN

背景信息

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，进入 RRPP 域视图。

步骤 3 执行命令 **protected-vlan reference-instance** { { *instance-id1* [**to** *instance-id2*] } &<1-10> | **all** }，配置 RRPP 域的保护 VLAN 列表。

RRPP 端口允许通过的 VLAN 都应该配置为保护 VLAN，包括数据 VLAN 和控制 VLAN。

版权所有 © 华为技术有限公司

说明

配置 RRPP 保护 VLAN 列表需要注意以下事项:

- 在配置 RRPP 环之前必须配置保护 VLAN。
- 在配置 RRPP 环之前可以删除、修改已经配置的保护 VLAN。在配置环之后不允许更改保护 VLAN。
- 在同一物理拓扑中，本域的控制 VLAN 不能做为其他域的保护 VLAN。
- 控制 VLAN 必须在保护 VLAN 范围内，否则不允许配置环。
- 控制 VLAN 在创建环前允许加入别的实例，在创建环后不允许更改，除非删除域。
- 实例和 VLAN 映射关系发生变化时，RRPP 域的保护 VLAN 随之变化。
- RRPP 端口允许通过的所有 VLAN 都应该被 RRPP 域保护。

----结束

创建 RRPP 环

背景信息

说明

缺省情况下，设备所有接口使能 STP 协议。同一端口上只能配置 RRPP 协议或者 STP 协议中的一种。所以，在创建 RRPP 环前，需要先执行 **stp disable** 命令去使能即将加入 RRPP 环中的接口的 STP 功能。

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，进入域视图。

步骤 3 执行命令 **ring** *ring-id* **node-mode** { **master** |**transit** } **primary-port** *interface-type interface-number* **secondary-port** *interface-type interface-number* **level** *level-value*，创建 RRPP 环。

RRPP 支持的二层端口有 GigabitEthernet 和 Eth-Trunk。

环级别为 0 表示主环，级别为 1 表示子环。

一个域中只能有一个主环，必须先创建主环再创建子环。

子环主节点不能作为边缘节点和辅助边缘节点。

一台 AC6605 上最多可以配置 16 个环。

步骤 4 执行命令 **ring** *ring-id* **node-mode** { **edge** | **assistant-edge** } **common-port** *interface-type interface-number* **edge-port** *interface-type interface-number*，配置 RRPP 子环上的边缘节点和辅助边缘节点。

边缘节点和辅助边缘节点的公共端口必须在主环上。

边缘节点和辅助边缘节点所在的环级别系统自动设置为 1，不需手动配置。

----结束

版权所有 © 华为技术有限公司

使能 RRPP 环

子环的协议报文在主环中作为数据报文传送，主环协议报文只在主环中传送。打开 RRPP 环开关，RRPP 环才能生效。

背景信息

说明

同时使能 RRPP 环和 RRPP 协议，才能激活 RRPP 环。

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **ring** *ring-id* **enable** 命令，使能 RRPP 环。

----结束

使能 RRPP 协议

只使能 RRPP 环还不能真正激活 RRPP 环，必须同时使能 RRPP 协议才能激活 RRPP 环。

背景信息

说明

同时使能 RRPP 环和 RRPP 协议，才能激活 RRPP 环。

请在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp enable** 命令，使能 RRPP 协议。

----结束

（可选）设置 RRPP 域定时器的值

主节点在发送和接收 RRPP 协议报文时用到两个定时器，分别是：Hello 定时器和 Fail 定时器。Hello 定时器用于主端口发送 Hello 报文；Fail 定时器用于副端口接收本节点发出的 Hello 报文的超时时间。

背景信息

请在 RRPP 域内的主节点上执行以下操作。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **timer hello-timer** *hello-value* **fail-timer** *fail-value* 命令，设置 RRPP 域定时器的值。

Fail timer 的值应大于等于 Hello timer 的值的三倍。

Edge-hello 定时器的值默认为主环主节点 Hello 定时器值的一半。

对于 Hello 定时器和 Fail 定时器，在同一个域内各个节点上的配置需要一致，否则，容易导致边缘节点的边缘端口不稳定。

----结束

检查配置结果

操作步骤

- 使用命令 **display stp region-configuration** 查看实例与 VLAN 的映射关系。
- 使用命令 **display rrpp brief** [**domain** *domain-id*]查看 RRPP 域的概要信息。
- 使用命令 **display rrpp verbose domain** *domain-id* [**ring** *ring-id*]查看 RRPP 域的详细信息。
- 使用命令 **display rrpp statistics domain** *domain-id* [**ring** *ring-id*]查看 RRPP 域的报文统计信息。

----结束

任务示例

执行 **display stp region-configuration** 命令，可以查看实例与 VLAN 之间的映射关系。例如：

```
<Quidway> display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0fc010203
   Revision level     :0

   Instance   Vlans Mapped
      0       3 to 9, 12 to 99, 301 to 4094
      1       1 to 2, 100 to 200
      2       10 to 11, 201 to 300
```

执行 **display rrpp brief** 命令，可以查看节点模式、RRPP 协议状态、控制 VLAN、保护 VLAN、定时器值、链路恢复时延、等信息。例如：

```
<Quidway> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common             Secondary/Edge        Is
 ID     Level   Mode     Port                       Port                  Enabled
```


版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------------------
1       0       M       GigabitEthernet0/0/2       GigabitEthernet0/0/3
```

执行 **display rrpp verbose** 命令，可以查看控制 VLAN、保护 VLAN、定时器、节点模式、端口状态等详细信息。例如：

```
<Quidway> display rrpp verbose domain 1 ring 1
Domain Index    : 1
Control VLAN    : major 400    sub 401
Protected VLAN : Reference Instance 30
Hello Timer     : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring       : 1
Ring Level      : 0
Node Mode       : Master
Ring State      : Complete
Is Enabled      : Enable                        Is Active : Yes
Primary port    : GigabitEthernet0/0/1         Port status: UP
Secondary port : GigabitEthernet0/0/2          Port status: BLOCKED
```

执行 **display rrpp statistics** 命令，可以查看各类报文的发送、接收统计信息。例如：

```
<Quidway> display rrpp statistics domain 1 ring 1
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Is Active  : Yes
Primary port   : GigabitEthernet0/0/1
 Packet            LINK      COMMON    COMPLETE  EDGE      MAJOR     Packet

 Direct  HEALTH    DOWN      FDB       FDB       HELLO     FAULT     Total

 --------------------------------------------------------------------------------
 Send    2934      0         1         1         0         0         2936
 Rcv     0         1         0         0         0         0         1
Secondary port: GigabitEthernet0/0/2
 Packet            LINK      COMMON    COMPLETE  EDGE      MAJOR     Packet

 Direct  HEALTH    DOWN      FDB       FDB       HELLO     FAULT     Total

 --------------------------------------------------------------------------------
Send    0         0         1         0         0         0         1
Rcv     2928      1         0         0         0         0         2929
```

9.3.4 配置 RRPP 多实例

RRPP 多实例以基于域的方式，允许在一个物理环路上配置多个 RRPP 域，每一个域中，所有端口、节点角色、拓扑都遵循基本的 RRPP 原则。相应的，一个物理环路上就有多个主节点，各个主节点分别检测物理环路的完整性，并相应的阻塞或放开自己的副端口，彼此互不影响。

建立配置任务

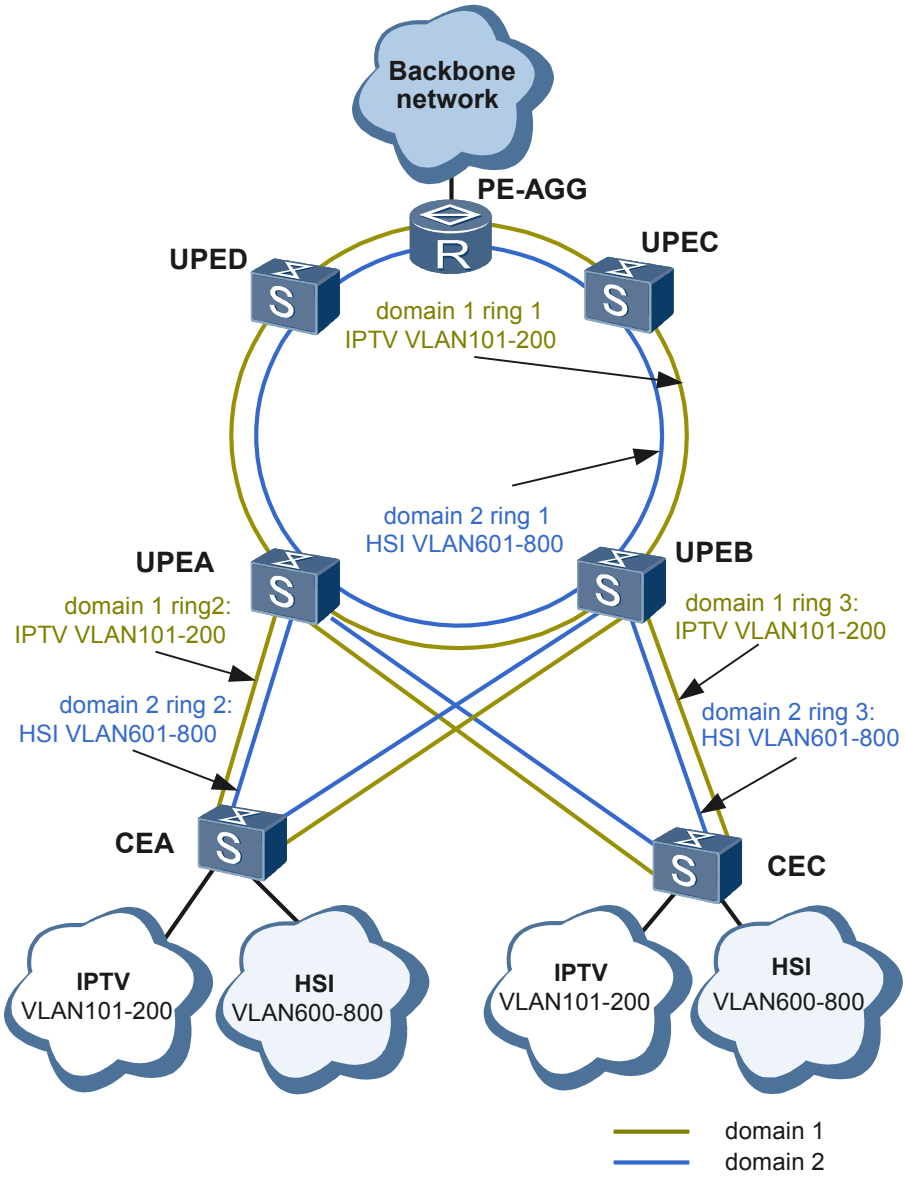
RRPP 没有自动选举机制，因此只有为环网上的每个节点进行正确配置，才能让协议真正实现环网的检测和保护。请注意保证配置的正确性。

应用环境

RRPP 多实例可以满足更复杂的组网需求，如图 9-13 所示。CE 连接 UPE 组成两个 RRPP 子环，CE 双归属接入 UPE。四台 UPE 设备与一台 PE 设备组成一个 RRPP 环路，由 PE 设备将用户数据接入骨干网络。

版权所有 © 华为技术有限公司

图 9-13 RRPP 多实例应用场景图



CE: Customer Edge

UPE: Underlayer Provider Edge

PE-AGG: PE-Aggregation

IPTV: Internet Protocol Television

HSI: High Speed Internet

图中 IPTV、HSI 业务分别对应两个不同的域，共享同一个 RRPP 环路。利用 RRPP 多实例，实现两种业务流量负载分担。IPTV 业务通过域 1 传输流量，HSI 业务通过域 2 传输业流量。

说明

同一端口上只能配置 RRPP 协议或者 STP 协议中的一种，不能两种协议同时配置。

RRPP 没有自动选举机制，因此只有为环网上的每个节点进行正确配置，才能让协议真正实现环网的检测和保护。请注意保证配置的正确性。

版权所有 © 华为技术有限公司

前置任务

在配置 RRPP 多实例之前，需完成以下任务：

- 搭建环形拓扑的组网环境。
- 配置接口的链路属性。

数据准备

在配置 RRPP 多实例之前，需要准备以下数据。

序号	数据
1	RRPP 域的 ID
2	RRPP 域控制 VLAN 的 ID
3	RRPP 域的保护 VLAN ID
4	RRPP 域中各个 RRPP 环的 ID
5	RRPP 环的端口名
6	（可选）环组 ID
7	（可选）链路恢复时延
8	（可选）RRPP 域的 Hello 定时器、Fail 定时器的值

创建实例

背景信息

请在需要加入 RRPP 多实例域的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行以下步骤，配置多生成树实例与 VLAN 的映射关系。

- 执行命令 **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，配置实例和 VLAN 的映射关系。
- 执行命令 **vlan-mapping modulo** *modulo*，配置实例和 VLAN 按照缺省算法自动分配映射关系。

vlan-mapping modulo 命令将 VLAN 映射到编号为（VLAN ID-1）%*modulo*+1 的生成树实例上。例如，模值为 16，则 VLAN1 映射到 MSTI1、VLAN2 映射到 MSTI2…… VLAN16 映射到 MSTI16，依次类推。

主环控制 VLAN 和子环控制 VLAN 必须包含在 VLAN 列表中。

一个域中最多可创建 49 个实例，其中 Instance 0 为缺省配置，不需要创建。

版权所有 © 华为技术有限公司

缺省情况下，所有的 VLAN 都映射到 Instance 0。

步骤 4 执行命令 **active region-configuration**，激活 MST 域的配置。

----结束

配置 RRPP 环上的接口

背景信息

请在需要加入 RRPP 环的端口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

RRPP 支持的二层端口有 GigabitEthernet 和 Eth-Trunk。

不能把已启用 SmartLink、LDT、MUXVLAN、MSTP 的端口配置成 RRPP 端口。

步骤 3 （可选）执行命令 **port link-type trunk**，设置端口为 Trunk 端口。

缺省情况下端口为 Hybrid 端口。

由于 RRPP 端口既要允许控制 VLAN 中的报文通过，又要允许数据 VLAN 中的报文通过，所以应为 Trunk 类型或 Hybrid 类型。

步骤 4 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，或执行命令 **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置 RRPP 端口允许通过的数据 VLAN。

控制 VLAN 由 RRPP 域视图下的 **control-vlan** 命令指定，并配置了 **ring node-mode** 命令后，会自动成为 RRPP 环上各端口允许通过的控制 VLAN。因此，本步骤中仅需指定数据 VLAN 即可。

步骤 5 执行命令 **stp disable**，去使能端口上的 STP 功能。

缺省情况下，设备所有端口上都使能了 STP 协议。在创建 RRPP 环前，需要先去使能即将加入 RRPP 环中的端口的 STP 功能。

----结束

创建 RRPP 域

一组配置了相同域 ID 和控制 VLAN，并且相互联通的交换机群体构成一个 RRPP 域。一个 RRPP 域主要由 RRPP 环、RRPP 控制 VLAN、主节点等要素组成。

操作步骤

步骤 1 在 RRPP 域内每台交换机上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，创建 RRPP 域。

AC6605 上最多可创建 8 个不同的域。

版权所有 © 华为技术有限公司

创建 RRPP 域时要指定域的 ID，如果该域已存在则直接进入域视图。

----结束

配置保护 VLAN

背景信息

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，进入 RRPP 域视图。

步骤 3 执行命令 **protected-vlan reference-instance** { { *instance-id1* [**to** *instance-id2*] } &<1-10> | **all** }，配置 RRPP 域的保护 VLAN 列表。

RRPP 端口允许通过的 VLAN 都应该配置为保护 VLAN，包括数据 VLAN 和控制 VLAN。

说明

配置 RRPP 保护 VLAN 列表需要注意以下事项:

- 在配置 RRPP 环之前必须配置保护 VLAN。
- 在配置 RRPP 环之前可以删除、修改已经配置的保护 VLAN。在配置环之后不允许更改保护 VLAN。
- 在同一物理拓扑中，本域的控制 VLAN 不能做为其他域的保护 VLAN。
- 控制 VLAN 必须在保护 VLAN 范围内，否则不允许配置环。
- 控制 VLAN 在创建环前允许加入别的实例，在创建环后不允许更改，除非删除域。
- 实例和 VLAN 映射关系发生变化时，RRPP 域的保护 VLAN 随之变化。
- RRPP 端口允许通过的所有 VLAN 都应该被 RRPP 域保护。

----结束

创建控制 VLAN

每个 RRPP 域具有两个控制 VLAN，主控制 VLAN 中传播的主要是主环的协议报文，子控制 VLAN 中传播的主要是子环的协议报文。

操作步骤

步骤 1 在 RRPP 域内每台交换机上执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **control-vlan** *vlan-id* 命令，创建控制 VLAN。

由参数 *vlan-id* 指定的控制 VLAN 和由 *vlan-id*+1 指定的子控制 VLAN 必须都是未被创建，并且未被 port trunk、mapping、stacking 等方式使用过的 VLAN。

每个 RRPP 域配有两个控制 VLAN，分别为主控制 VLAN 和子控制 VLAN。配置时只需要指定主控制 VLAN，而把比主控制 VLAN ID 值大 1 的 VLAN 作为子控制 VLAN。

版权所有 © 华为技术有限公司

控制 VLAN 创建后不能直接修改，只能通过先删除域，然后再重新配置的方式修改。子控制 VLAN 也在删除域时被连带删除。

说明

RRPP 控制 VLAN 不能配置 DHCP 业务。

----结束

创建 RRPP 环

背景信息

说明

缺省情况下，设备所有接口使能 STP 协议。同一端口上只能配置 RRPP 协议或者 STP 协议中的一种。所以，在创建 RRPP 环前，需要先执行 **stp disable** 命令去使能即将加入 RRPP 环中的接口的 STP 功能。

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rrpp domain** *domain-id*，进入域视图。

步骤 3 执行命令 **ring** *ring-id* **node-mode** { **master** |**transit** } **primary-port** *interface-type interface-number* **secondary-port** *interface-type interface-number* **level** *level-value*，创建 RRPP 环。

RRPP 支持的二层端口有 GigabitEthernet 和 Eth-Trunk。

环级别为 0 表示主环，级别为 1 表示子环。

一个域中只能有一个主环，必须先创建主环再创建子环。

子环主节点不能作为边缘节点和辅助边缘节点。

一台 AC6605 上最多可以配置 16 个环。

步骤 4 执行命令 **ring** *ring-id* **node-mode** { **edge** | **assistant-edge** } **common-port** *interface-type interface-number* **edge-port** *interface-type interface-number*，配置 RRPP 子环上的边缘节点和辅助边缘节点。

边缘节点和辅助边缘节点的公共端口必须在主环上。

边缘节点和辅助边缘节点所在的环级别系统自动设置为 1，不需手动配置。

----结束

使能 RRPP 环

子环的协议报文在主环中作为数据报文传送，主环协议报文只在主环中传送。打开 RRPP 环开关，RRPP 环才能生效。

背景信息

说明

同时使能 RRPP 环和 RRPP 协议，才能激活 RRPP 环。

版权所有 © 华为技术有限公司

在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **ring** *ring-id* **enable** 命令，使能 RRPP 环。

----结束

使能 RRPP 协议

只使能 RRPP 环还不能真正激活 RRPP 环，必须同时使能 RRPP 协议才能激活 RRPP 环。

背景信息

说明

同时使能 RRPP 环和 RRPP 协议，才能激活 RRPP 环。

请在 RRPP 域内每台交换机上进行如下配置。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp enable** 命令，使能 RRPP 协议。

----结束

（可选）创建环组

为了减少 Edge-Hello 报文的收发数量，用户可以采用环组机制，即将具有相同边缘节点/辅助边缘节点配置的一组子环加入环组。

操作步骤

步骤 1 在边缘节点或辅助边缘节点上执行命令 **system-view**，进入系统视图。

步骤 2 执行 **rrpp ring-group** *ring-group-id* 命令，创建环组。

只能在子环边缘节点或辅助边缘节点上创建环组。

一个环组内的所有子环所在节点应该具有相同的类型：都是边缘节点或者都是辅助边缘节点。

步骤 3 执行 **domain** *domain-id* **ring** { *ring-id1* [**to** *ring-id2*] } &<1-10>命令，在环组内增加子环。

加入同一环组的子环边缘节点是同一台设备。同样，辅助边缘节点也是同一台设备。

一个子环只能属于一个环组。

增加或删除环组时，需要注意：

- 如果需要将激活的子环加入环组中，必须先在辅助边缘节点将环加入环组，再在边缘节点将环加入环组。

版权所有 © 华为技术有限公司

- 如果需要将激活的子环从环组中删除，必须先在边缘节点将环从环组中删除，再在辅助边缘节点将环从环组中删除。

----结束

（可选）配置链路恢复时延

配置链路恢复时延后，RRPP 链路阻塞点不会立即完成切换，而是要经过配置的链路阻塞点切换的时延定时器超时后再切换，从而减小链路状态的震荡。

背景信息

本配置只有在主节点上配置生效。

操作步骤

步骤 1 在主节点上执行命令 **system-view**，进入系统视图。

步骤 2 执行 **rrpp linkup-delay-timer** *linkup-delay-timer-value* 命令，设置 RRPP 链路阻塞点切换的时延定时器。

linkup-delay-timer-value 的值必须小于等于任何 RRPP 域中 fail 定时器减 2 倍 HELLO 定时器的值。

----结束

（可选）设置 RRPP 域定时器的值

主节点在发送和接收 RRPP 协议报文时用到两个定时器，分别是：Hello 定时器和 Fail 定时器。Hello 定时器用于主端口发送 Hello 报文；Fail 定时器用于副端口接收本节点发出的 Hello 报文的超时时间。

背景信息

请在 RRPP 域内的主节点上执行以下操作。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **rrpp domain** *domain-id* 命令，进入域视图。

步骤 3 执行 **timer hello-timer** *hello-value* **fail-timer** *fail-value* 命令，设置 RRPP 域定时器的值。

Fail timer 的值应大于等于 Hello timer 的值的三倍。

Edge-hello 定时器的值默认为主环主节点 Hello 定时器值的一半。

对于 Hello 定时器和 Fail 定时器，在同一个域内各个节点上的配置需要一致，否则，容易导致边缘节点的边缘端口不稳定。

----结束

检查配置结果

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display stp region-configuration** 查看实例与 VLAN 的映射关系。
- 使用命令 **display rrpp brief** [**domain** *domain-id*]查看 RRPP 域的概要信息。
- 使用命令 **display rrpp verbose domain** *domain-id* [**ring** *ring-id*]查看 RRPP 域的详细信息。
- 使用命令 **display rrpp statistics domain** *domain-id* [**ring** *ring-id*]查看 RRPP 域的报文统计信息。

----结束

任务示例

执行 **display stp region-configuration** 命令，可以查看实例与 VLAN 之间的映射关系。例如：

```
<Quidway> display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0fc010203
   Revision level     :0

   Instance   Vlans Mapped
      0       3 to 9, 12 to 99, 301 to 4094
      1       1 to 2, 100 to 200
      2       10 to 11, 201 to 300
```

执行 **display rrpp brief** 命令，可以查看节点模式、RRPP 协议状态、控制 VLAN、保护 VLAN、定时器值、链路恢复时延、等信息。例如：

```
<Quidway> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common            Secondary/Edge        Is
 ID     Level   Mode     Port                      Port                  Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2      GigabitEthernet0/0/3
```

执行 **display rrpp verbose** 命令，可以查看控制 VLAN、保护 VLAN、定时器、节点模式、端口状态等详细信息。例如：

```
<Quidway> display rrpp verbose domain 1 ring 1
Domain Index   : 1
Control VLAN   : major 400    sub 401
Protected VLAN : Reference Instance 30
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                        Is Active : Yes
Primary port   : GigabitEthernet0/0/1         Port status: UP
Secondary port : GigabitEthernet0/0/2          Port status: BLOCKED
```

执行 **display rrpp statistics** 命令，可以查看各类报文的发送、接收统计信息。例如：

版权所有 © 华为技术有限公司

```
<Quidway> display rrpp statistics domain 1 ring 1
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Is Active  : Yes
Primary port   : GigabitEthernet0/0/1
 Packet            LINK      COMMON    COMPLETE  EDGE      MAJOR     Packet

 Direct  HEALTH    DOWN      FDB       FDB       HELLO     FAULT     Total

 ---------------------------------------------------------------------------
 Send    2934      0         1         1         0         0         2936
 Rcv     0         1         0         0         0         0         1
Secondary port: GigabitEthernet0/0/2
 Packet            LINK      COMMON    COMPLETE  EDGE      MAJOR     Packet

 Direct  HEALTH    DOWN      FDB       FDB       HELLO     FAULT     Total

 ---------------------------------------------------------------------------
Send    0         0         1         0         0         0         1
Rcv     2928      1         0         0         0         0         2929
```

9.3.5 维护 RRPP

清除 RRPP 的统计信息对定位 RRPP 的故障有帮助。

清除运行信息

通过 reset 命令可以将 RRPP 统计计数置 0，便于重新统计。

背景信息



注意

清除 RRPP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除 RRPP 的统计报文后，请在用户视图下执行下面的 **reset** 命令。

操作步骤

步骤 1 执行 **reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]命令，清除 RRPP 统计信息。

----结束

调试 RRPP

调试信息为故障定位提供了便利，主要包括：事件、报文等调试开关。

版权所有 © 华为技术有限公司

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 RRPP 运行故障时，请在用户视图下执行 debugging 命令对 RRPP 进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

步骤 1 请在用户视图下执行 **debugging rrpp** [**domain** *domain-id* [**ring** *ring-id*]] { **error** | **event** | **packet** | **all** }命令，调试 RRPP。

----结束

9.3.6 配置举例

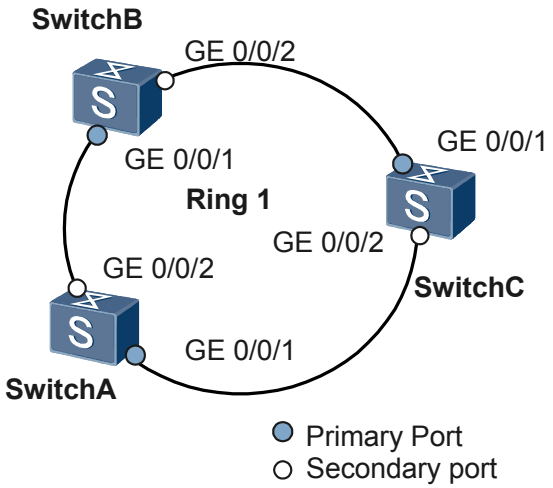
介绍 RRPP 多实例的各种组网举例。

配置 RRPP 单环示例

组网需求

如图 9-14 所示，SwitchA、SwitchB、SwitchC 都支持 RRPP 功能。将 SwitchA、SwitchB 和 SwitchC 配置为域 1 的环 1。要求对 VLAN100 ～ VLAN300 的数据进行保护。

图 9-14 配置 RRPP 单环组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 RRPP 单环示例：

1. 配置实例 1 映射 VLAN100 ～ VLAN300。
2. 将 SwitchA、SwitchB 和 SwitchC 配置为域为 1 的环 1。
3. 配置 SwitchA 为环 1 的主节点，SwitchB 和 SwitchC 为环 1 的传输节点。

数据准备

为完成此配置例，需准备如下的数据：

- RRPP 接口的接口编号
- 环 1 的控制 VLAN ID

操作步骤

步骤 1 配置实例 1 映射 VLAN100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 1 vlan 20 21 100 to 300
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

SwitchB 和 SwitchC 配置过程和 SwitchA 一样，此处不再赘述。

步骤 2 创建 RRPP 域，同时创建域的控制 VLAN

配置环 1 的主节点 SwitchA 的域为 1，主控制 VLAN 的 VLAN ID 为 20。

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] control-vlan 20
[SwitchA-rrpp-domain-region1] quit
```

配置环 1 的传输节点 SwitchB 的域为 1，主控制 VLAN 的 VLAN ID 为 20。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] control-vlan 20
[SwitchB-rrpp-domain-region1] quit
```

配置环 1 的传输节点 SwitchC 的域为 1，控制 VLAN 的 VLAN ID 为 20。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 20
[SwitchC-rrpp-domain-region1] quit
```

步骤 3 将即将加入 RRPP 环的接口配置为 Trunk 类型接口，允许 VLAN100 ～ VLAN300 通过，并去使能接口的 STP 功能

配置 SwitchA。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
```


版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
```

配置 SwitchB。

```
[SwitchB] interface gigabitehternet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchB-GigabitEthernet0/0/1] stp disable
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[SwitchB-GigabitEthernet0/0/2] stp disable
[SwitchB-GigabitEthernet0/0/2] quit
```

配置 SwitchC。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchC-GigabitEthernet0/0/1] stp disable
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[SwitchC-GigabitEthernet0/0/2] stp disable
[SwitchC-GigabitEthernet0/0/2] quit
```

步骤 4 配置保护 VLAN，并创建 RRPP 环

在 SwitchA 配置保护 VLAN，并配置 SwitchA 为 RRPP 主环 1 的主节点，并指定主副接口。

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchA-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchA-rrpp-domain-region1] ring 1 enable
[SwitchA-rrpp-domain-region1] quit
```

在 SwitchB 配置保护 VLAN，并配置 SwitchB 为 RRPP 主环 1 的传输节点，并指定主副接口。

```
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchB-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region1] ring 1 enable
[SwitchB-rrpp-domain-region1] quit
```

在 SwitchC 配置保护 VLAN，并配置 SwitchC 为 RRPP 主环 1 的传输节点，并指定主副接口。

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchC-rrpp-domain-region1] ring 1 enable
[SwitchC-rrpp-domain-region1] quit
```

步骤 5 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

配置 SwitchA 上 RRPP 协议使能。

版权所有 © 华为技术有限公司

```
[SwitchA] rrpp enable
```

配置 SwitchB 上 RRPP 协议使能。

```
[SwitchB] rrpp enable
```

配置 SwitchC 上 RRPP 协议使能。

```
[SwitchC] rrpp enable
```

步骤 6 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 SwitchA 为例。

- 在 SwitchA 上执行 **display rrpp brief** 命令，查看结果如下：

```
[SwitchA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common           Secondary/Edge          Is
 ID     Level   Mode     Port                     Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/1           GigabitEthernet0/0/2          Yes
```

可以看到 SwitchA 的 RRPP 协议状态使能了，在域 1 中的主控制 VLAN 为 20，子控制 VLAN 为 21，SwitchA 为主环 1 中的主节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

- 在 SwitchA 上执行 **display rrpp verbose domain** 命令，查看结果如下：

查看 SwitchA 上域 1 中的详细信息。

```
[SwitchA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                      Is Active : Yes
Primary port  : GigabitEthernet0/0/1        Port status: UP
Secondary port: GigabitEthernet0/0/2        Port status: BLOCKED
```

----结束

配置文件

- SwitchA 的配置文件

```
sysname SwitchA
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 20 to 21 100 to 300
```


版权所有 © 华为技术有限公司

```
  active region-configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
```

- SwitchB 的配置文件

```
#
sysname SwitchB
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 20 to 21 100 to 300
  active region-configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
#
```

- SwitchC 的配置文件

```
#
sysname SwitchC
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 20 to 21 100 to 300
  active region-configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

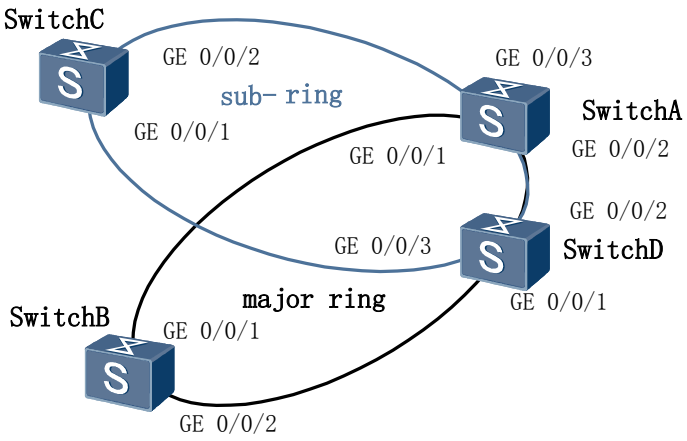
配置 RRPP 单实例相交环示例

组网需求

如图 9-15 所示，SwitchA、SwitchB、SwitchC 和 SwitchD 都支持 RRPP 功能，将 SwitchA、SwitchB 和 SwitchD 配置为域 1 的主环 1；将 SwitchA、SwitchC 和 SwitchD 配置为域 1 的子环 2。其中 SwitchA 为域 1 子环 2 的边缘节点，SwitchD 为域 1 子环 2 的辅助边缘节点。

主控制 VLAN ID 为 10。该 RRPP 环传送 VLAN2 ～ 9 的用户数据。

图 9-15 RRPP 单实例相交环示例



配置思路

采用如下的思路配置 RRPP 单实例相交环示例：

1. 将 SwitchA、SwitchB 和 SwitchD 配置为域 1 的主环 1。主控制 VLAN 为 10。主环和子环上允许通过的业务流量所属 VLAN ID 为 2 ～ 9。
2. 将 SwitchA、SwitchC 和 SwitchD 配置为域 1 的子环 2。
3. 配置 SwitchB 为主环主节点，SwitchA 和 SwitchD 为主环传输节点。
4. 配置 SwitchC 为子环主节点，SwitchA 为子环边缘节点，SwitchD 为子环辅助边缘节点。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- 加入 RRPP 环的接口编号
- 控制 VLAN ID 和数据 VLAN ID

操作步骤

步骤 1 配置 SwitchB 为主环主节点。

在 SwitchB 上创建数据 VLAN2 ～ VLAN9。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 2 to 9
```

配置实例 1，映射允许通过的 VLAN 和保护 VLAN。

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] instance 1 vlan 1 to 11
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

配置 SwitchB 的域 1，主控制 VLAN 为 10，保护 VLAN 实例为 1。

```
[SwitchB] rrpp enable
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] control-vlan 10
[SwitchB-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchB-rrpp-domain-region1] quit
```

去使能即将加入 RRPP 环中的接口的 STP 功能，并配置 RRPP 端口为 Trunk 口，并允许 VLAN2 ～ VLAN9 通过。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchB-GigabitEthernet0/0/1] stp disable
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchB-GigabitEthernet0/0/2] stp disable
[SwitchB-GigabitEthernet0/0/2] quit
```

配置 RRPP 主环主节点主副端口。

```
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region1] ring 1 enable
[SwitchB-rrpp-domain-region1] quit
```

步骤 2 配置 SwitchC 为子环主节点。

在 SwitchC 上创建数据 VLAN2 ～ VLAN9。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 2 to 9
```

配置实例 1，映射允许通过的 VLAN 和保护 VLAN。

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] instance 1 vlan 1 to 11
```


版权所有 © 华为技术有限公司

```
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

配置 SwitchC 域 1，主控制 VLAN 为 10，保护 VLAN 实例为 1。

```
[SwitchC] rrpp enable
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 10
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] quit
```

去使能即将加入 RRPP 环中的接口的 STP 功能，并将 RRPP 端口配置为 Trunk 类型，并允许 VLAN2 ～ VLAN9 通过。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchC-GigabitEthernet0/0/1] stp disable
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchC-GigabitEthernet0/0/2] stp disable
[SwitchC-GigabitEthernet0/0/2] quit
```

配置 RRPP 子环主节点主副端口。

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] ring 2 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 1
[SwitchC-rrpp-domain-region1] ring 2 enable
[SwitchC-rrpp-domain-region1] quit
```

步骤 3 配置 SwitchA 为主环传输节点，子环边缘传输节点。

在 SwitchA 上创建数据 VLAN2 ～ VLAN9。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 2 to 9
```

配置实例 1，映射允许通过的 VLAN 和保护 VLAN。

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 1 vlan 1 to 11
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

配置 SwitchA 域 1，主控制 VLAN 为 10，保护 VLAN 实例为 1。

```
[SwitchA] rrpp enable
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] control-vlan 10
[SwitchA-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchA-rrpp-domain-region1] quit
```

去使能即将加入 RRPP 环中的接口的 STP 功能，并将 RRPP 端口配置为 Trunk 类型，并允许 VLAN2 ～ VLAN9 通过。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 9
[SwitchA-GigabitEthernet0/0/3] stp disable
[SwitchA-GigabitEthernet0/0/3] quit
```

配置 RRPP 主环传输节点主副端口。

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 0
[SwitchA-rrpp-domain-region1] ring 1 enable
[SwitchA-rrpp-domain-region1] quit
```

配置 RRPP 子环边缘传输节点的公共端口和边缘端口。

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] ring 2 node-mode edge common-port gigabitethernet 0/0/2 edge-port gigabitethernet 0/0/3
[SwitchA-rrpp-domain-region1] ring 2 enable
[SwitchA-rrpp-domain-region1] quit
```

步骤 4 配置 SwitchD 为主环传输节点，子环辅助边缘节点。

在 SwitchD 上创建数据 VLAN2 ～ VLAN9。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan batch 2 to 9
```

配置实例 1，映射允许通过的 VLAN 和保护 VLAN。

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] instance 1 vlan 1 to 11
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

配置 SwitchD 域 1，主控制 VLAN 为 10，保护 VLAN 实例为 1。

```
[SwitchD] rrpp enable
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] control-vlan 10
[SwitchD-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchD-rrpp-domain-region1] quit
```

去使能即将加入 RRPP 环中的接口的 STP 功能，并将 RRPP 端口配置为 Trunk 类型。

```
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] port link-type trunk
[SwitchD-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchD-GigabitEthernet0/0/1] stp disable
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] port link-type trunk
[SwitchD-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchD-GigabitEthernet0/0/2] stp disable
[SwitchD-GigabitEthernet0/0/2] quit
[SwitchD] interface gigabitethernet 0/0/3
[SwitchD-GigabitEthernet0/0/3] port link-type trunk
[SwitchD-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 9
[SwitchD-GigabitEthernet0/0/3] stp disable
[SwitchD-GigabitEthernet0/0/3] quit
```

配置 RRPP 主环传输节点主副端口。

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 0
[SwitchD-rrpp-domain-region1] ring 1 enable
[SwitchD-rrpp-domain-region1] quit
```


版权所有 © 华为技术有限公司

配置 RRPP 子环辅助边缘节点的公共端口和边缘端口。

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port gigabitethernet 0/0/2
edge-port gigabitethernet 0/0/3
[SwitchD-rrpp-domain-region1] ring 2 enable
[SwitchD-rrpp-domain-region1] quit
```

步骤 5 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

- 在 SwitchB 上执行 **display rrpp brief** 命令，查看结果如下：

```
[SwitchB] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 1   0          M        GigabitEthernet0/0/1         GigabitEthernet0/0/2         Yes
```

可以看到 SwitchB 上的 RRPP 协议已经使能，主控制 VLAN 为 10，子控制 VLAN 为 11，SwitchB 为主环主节点，主端口为 GE0/0/1，副端口为 GE0/0/2。

- 在 SwitchB 上执行 **display rrpp verbose domain** 命令，查看结果如下：

```
[SwitchB] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Completed
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: BLOCKED
```

可以看到环为完整状态，主节点的副端口被阻塞。

- 在 SwitchC 上执行 **display rrpp brief** 命令，查看结果如下：

```
[SwitchC] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 2   1          M         GigabitEthernet0/0/1          GigabitEthernet0/0/2         Yes
```


版权所有 © 华为技术有限公司

可以看到 SwitchC 的 RRPP 协议状态使能了，主控制 VLAN 为 10，子控制 VLAN 为 11，SwitchC 子环主节点，主端口为 GE0/0/1，副端口为 GE0/0/2。

- 在 SwitchC 上执行 **display rrpp verbose domain** 命令，查看结果如下：

```
[SwitchC] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Master
Ring State    : Completed
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: BLOCKED
```

可以看到子环为完整状态，子环主节点的副端口被阻塞。

- 在 SwitchA 上执行 **display rrpp brief** 命令，查看结果如下：

```
[SwitchA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 1     0        T        GigabitEthernet0/0/2         GigabitEthernet0/0/1         Yes
 2     1        E        GigabitEthernet0/0/2         GigabitEthernet0/0/3         Yes
```

可以看到 SwitchA 的 RRPP 协议状态使能了，主控制 VLAN 为 10，子控制 VLAN 为 11，SwitchA 为主环 1 中的传输节点。主端口为 0GE0/0/2，副端口为 GE0/0/1。

同时，SwitchA 为子环 2 中的边缘节点，公共端口为 GE0/0/2，边缘端口为 GE0/0/3。

- 在 SwitchA 上执行 **display rrpp verbose domain** 命令，查看结果如下：

```
[SwitchA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/2         Port status: UP
Secondary port: GigabitEthernet0/0/1         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : Linkup
Is Enabled    : Disable                Is Active : No
Common port   : GigabitEthernet0/0/2         Port status: UP
Edge port     : GigabitEthernet0/0/3         Port status: UP
```

- 在 SwitchD 上执行 **display rrpp brief** 命令，查看结果如下：

版权所有 © 华为技术有限公司

```
[SwitchD] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 1      0       T        GigabitEthernet0/0/2        GigabitEthernet0/0/1        Yes
 2      1       A        GigabitEthernet0/0/2        GigabitEthernet0/0/3        Yes
```

可以看到 SwitchD 的 RRPP 协议状态使能了，主控制 VLAN 为 10，子控制 VLAN 为 11，SwitchD 为主环 1 中的传输节点，主端口为 GE0/0/2，副端口为 GE0/0/1；同时，SwitchD 为子环 2 中的辅助边缘节点，公共端口为 GE0/0/2，边缘端口为 GE0/0/3。

- 在 SwitchD 上执行 **display rrpp verbose domain** 命令，查看结果如下：

```
[SwitchD] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/2         Port status: UP
Secondary port: GigabitEthernet0/0/1         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Assistant-edge
Ring State    : Linkup
Is Enabled    : Disable               Is Active : No
Common port   : GigabitEthernet0/0/2         Port status: UP
Edge port     : GigabitEthernet0/0/3         Port status: UP
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
 vlan batch 1 to 11
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 1 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/2 secondary-port GigabitEthernet
```


版权所有 © 华为技术有限公司

```
0/0/1 level 0
 ring 1 enable
 ring 2 node-mode edge common-port GigabitEthernet 0/0/2 edge-port GigabitEthernet 0/0/3
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- SwitchB 的配置文件

```
#
sysname SwitchB
#
 vlan batch 1 to 11
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 1 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet
0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- SwitchC 的配置文件

```
#
sysname SwitchC
#
 vlan batch 1 to 11
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 1 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet
0/0/2 level 1
```


版权所有 © 华为技术有限公司

```
 ring 2 enable
#
interface GigabitEthernet 0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet 0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- SwitchD 的配置文件

```
#
sysname SwitchD
 vlan batch 1 to 11
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 1 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/2 secondary-port GigabitEthernet
0/0/1 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port GigabitEthernet 0/0/2 edge-port GigabitEthernet
0/0/3
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

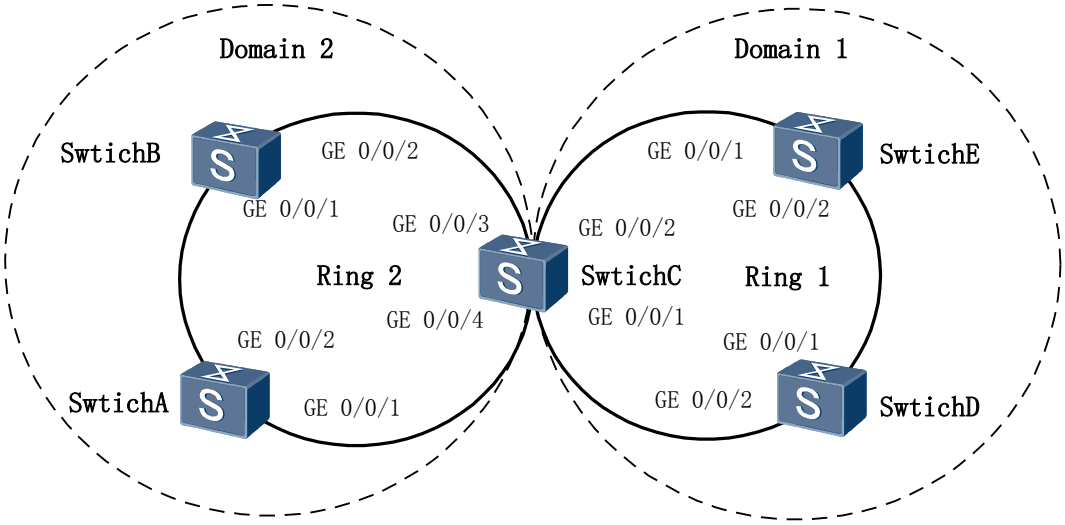
配置 RRPP 相切环示例

组网需求

如图 9-16 所示，SwitchA、SwitchB、SwitchC、SwitchE 和 SwitchD 都支持 RRPP 功能，将 SwitchA、SwitchB 和 SwitchC 配置为域 2 的环 2；将 SwitchC、SwitchE 和 SwitchD 配置为域 1 的环 1。两个环相切于节点 SwitchC。

版权所有 © 华为技术有限公司

图 9-16 配置 RRPP 相切环组网图



配置思路

采用如下的思路配置 RRPP 相切环示例：

1. 创建实例，将控制 VLAN 加入保护 VLAN 列表。
2. 将 SwitchA、SwitchB 和 SwitchC 配置为域为 2 的环 2。
3. 将 SwitchC、SwitchE 和 SwitchD 配置为域为 1 的环 1。
4. 配置 SwitchA 为环 2 的主节点，SwitchB 和 SwitchC 为环 2 的传输节点。
5. 配置 SwitchE 为环 1 的主节点，SwitchC 和 SwitchD 为环 1 的传输节点。

数据准备

为完成此配置例，需准备如下的数据：

- RRPP 接口的接口编号
- 环 1 和 2 的控制 VLAN ID

操作步骤

步骤 1 创建实例，将控制 VLAN 加入保护 VLAN 列表。

配置 SwitchA

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 2 vlan 20 to 21
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

配置 SwitchB

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] stp region-configuration
```


版权所有 © 华为技术有限公司

```
[SwitchB-mst-region] instance 2 vlan 20 to 21
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

配置 SwitchC

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] stp region-configuration
[SwitchC-mst-region] instance 1 vlan 10 to 11
[SwitchC-mst-region] instance 2 vlan 20 to 21
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

配置 SwitchD

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] stp region-configuration
[SwitchD-mst-region] instance 1 vlan 10 to 11
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

配置 SwitchE

```
<Quidway> system-view
[Quidway] sysname SwitchE
[SwitchE] stp region-configuration
[SwitchE-mst-region] instance 1 vlan 10 to 11
[SwitchE-mst-region] active region-configuration
[SwitchE-mst-region] quit
```

步骤 2 创建 RRPP 域，同时创建域的控制 VLAN 和保护 VLAN

配置环 1 的主节点 SwitchE 的域为 1，控制 VLAN 的 VLAN ID 为 10，保护实例 1 的 VLAN 列表。

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] control-vlan 10
[SwitchE-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchE-rrpp-domain-region1] quit
```

配置环 1 的传输节点 SwitchC 的域为 1，控制 VLAN 的 VLAN ID 为 10,保护实例 1 的 VLAN 列表。

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 10
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] quit
```

配置环 1 的传输节点 SwitchD 的域为 1，主控制 VLAN 的 VLAN ID 为 10,保护实例 1 的 VLAN 列表。

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] control-vlan 10
[SwitchD-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchD-rrpp-domain-region1] quit
```

配置环 2 的主节点 SwitchA 的域为 2，主控制 VLAN 的 VLAN ID 为 20,保护实例 2 的 VLAN 列表。

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] control-vlan 20
[SwitchA-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchA-rrpp-domain-region2] quit
```

配置环 2 的传输节点 SwitchB 的域为 2，主控制 VLAN 的 VLAN ID 为 20,保护实例 2 的 VLAN 列表。

版权所有 © 华为技术有限公司

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] control-vlan 20
[SwitchB-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchB-rrpp-domain-region2] quit
```

配置环 2 的传输节点 SwitchC 的域为 2，控制 VLAN 的 VLAN ID 为 20,保护实例 2 的 VLAN 列表。

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] control-vlan 20
[SwitchC-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchC-rrpp-domain-region2] quit
```

步骤 3 设置 RRPP 域定时器的值

说明

因为两个相切环处于不同的域内，所以相切点的定时器可以针对性地配置两个。

配置环 1 主节点 SwitchE 的定时器。

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchE-rrpp-domain-region1] quit
```

配置环 1 传输节点 SwitchD 的定时器。

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchD-rrpp-domain-region1] quit
```

配置环 1 传输节点 SwitchC 的定时器。

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchC-rrpp-domain-region1] quit
```

配置环 2 主节点 SwitchA 的定时器。

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchA-rrpp-domain-region2] quit
```

配置环 2 传输节点 SwitchB 的定时器。

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchB-rrpp-domain-region2] quit
```

配置环 2 传输节点 SwitchC 的定时器。

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchC-rrpp-domain-region2] quit
```

步骤 4 去使能即将加入 RRPP 环的接口的 STP 功能

去使能 SwitchA 上即将加入 RRPP 环的接口的 STP 功能。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] stp disable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] stp disable
[SwitchA-GigabitEthernet0/0/2] quit
```

去使能 SwitchB 上即将加入 RRPP 环的接口的 STP 功能。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] stp disable
```


版权所有 © 华为技术有限公司

```
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] stp disable
[SwitchB-GigabitEthernet0/0/2] quit
```

去使能 SwitchC 上即将加入 RRPP 环的接口的 STP 功能。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] stp disable
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] stp disable
[SwitchC-GigabitEthernet0/0/2] quit
[SwitchC] interface gigabitethernet 0/0/3
[SwitchC-GigabitEthernet0/0/3] stp disable
[SwitchC-GigabitEthernet0/0/3] quit
[SwitchC] interface gigabitethernet 0/0/4
[SwitchC-GigabitEthernet0/0/4] stp disable
[SwitchC-GigabitEthernet0/0/4] quit
```

去使能 SwitchE 上即将加入 RRPP 环的接口的 STP 功能。

```
[SwitchE] interface gigabitethernet 0/0/1
[SwitchE-GigabitEthernet0/0/1] stp disable
[SwitchE-GigabitEthernet0/0/1] quit
[SwitchE] interface gigabitethernet 0/0/2
[SwitchE-GigabitEthernet0/0/2] stp disable
[SwitchE-GigabitEthernet0/0/2] quit
```

去使能 SwitchD 上即将加入 RRPP 环的接口的 STP 功能。

```
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] stp disable
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] stp disable
[SwitchD-GigabitEthernet0/0/2] quit
```

步骤 5 创建 RRPP 环

配置环 2 上的节点，步骤如下：

配置 SwitchA 为 RRPP 环 2 的主节点，并指定主副接口。

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] ring 2 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchA-rrpp-domain-region2] ring 2 enable
[SwitchA-rrpp-domain-region2] quit
```

配置 SwitchB 为 RRPP 主环 2 的传输节点，并指定主副接口。

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] ring 2 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region2] ring 2 enable
[SwitchB-rrpp-domain-region2] quit
```

配置 SwitchC 为 RRPP 环 2 的传输节点，并指定主副接口。

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] ring 2 node-mode transit primary-port gigabitethernet 0/0/3 secondary-port gigabitethernet 0/0/4 level 0
[SwitchC-rrpp-domain-region2] ring 2 enable
[SwitchC-rrpp-domain-region2] quit
```

配置环 1 上的节点，步骤如下：

配置 SwitchE 为 RRPP 主环 1 的主节点，并指定主副接口。

版权所有 © 华为技术有限公司

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchE-rrpp-domain-region1] ring 1 enable
[SwitchE-rrpp-domain-region1] quit
```

配置 SwitchC 为 RRPP 环 1 的传输节点，并指定主副接口。

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchC-rrpp-domain-region1] ring 1 enable
[SwitchC-rrpp-domain-region1] quit
```

配置 SwitchD 为 RRPP 环 1 的传输节点，并指定主副接口。

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[SwitchD-rrpp-domain-region1] ring 1 enable
[SwitchD-rrpp-domain-region1] quit
```

步骤 6 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

使能 SwitchA 上 RRPP 协议。

```
[SwitchA] rrpp enable
```

使能 SwitchB 上 RRPP 协议。

```
[SwitchB] rrpp enable
```

使能 SwitchC 上 RRPP 协议。

```
[SwitchC] rrpp enable
```

使能 SwitchE 上 RRPP 协议。

```
[SwitchE] rrpp enable
```

使能 SwitchD 上 RRPP 协议。

```
[SwitchD] rrpp enable
```

步骤 7 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以相切点 SwitchC 为例。

- 在 SwitchC 上执行 **display rrpp brief** 命令，查看结果如下：

```
[SwitchC] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 2 sec(default is 1 sec)  Fail Timer : 7 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
```


版权所有 © 华为技术有限公司

```
 ------------------------------------------------------------------------------
 1      0       T        GigabitEthernet0/0/1         GigabitEthernet0/0/2         Yes
Domain Index  : 2
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 2
Hello Timer   : 3 sec(default is 1 sec)  Fail Timer : 10 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 2      0       T        GigabitEthernet0/0/3         GigabitEthernet0/0/4         Yes
```

可以看到 SwitchC 的 RRPP 协议状态使能了，在域 1 中的主控制 VLAN 为 10，子控制 Vlan 为 11，SwitchC 为主环 1 中的传输节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

同时，SwitchC 在域 2 中的主控制 Vlan 为 20，子控制 Vlan 为 21，SwitchC 为主环 2 中的传输节点。主端口为 GE0/0/3，副端口为 GE0/0/4。

- 在 SwitchC 上执行 **display rrpp verbose domain** 命令，查看结果如下：

  # 查看 SwitchC 上域 1 中的详细信息。

```
[SwitchC] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 2 sec(default is 1 sec)  Fail Timer : 7 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: UP
```

  # 查看 SwitchC 上域 2 中的详细信息。

```
[SwitchC] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 2
Hello Timer   : 3 sec(default is 1 sec)  Fail Timer : 10 sec(default is 6 sec)

RRPP Ring     : 2
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/3         Port status: UP
Secondary port: GigabitEthernet0/0/4         Port status: UP
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
vlan batch 20 to 21
#
rrpp enable
#
 stp region-configuration
  instance 2 vlan 20 to 21
  active region-configuration
#
rrpp domain 2
 control-vlan 20
```


版权所有 © 华为技术有限公司

```
 protected-vlan reference-instance 2
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode master primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernetGigabitEhternet0/0/2 level 0
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20 to 21
 stp disable
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 to 21
 stp disable
#
```

- SwitchB 的配置文件

```
#
sysname SwitchB
#
vlan batch 20 to 21
#
rrpp enable
#
 stp region-configuration
  instance 2 vlan 20 to 21
  active region-configuration
#
rrpp domain 2
 control-vlan 20
 protected-vlan reference-instance 2
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode transit primary-portGigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 20 to 21
 stp disable
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 20 to 21
 stp disable
#
return
#
```

- SwitchC 的配置文件

```
#
sysname SwitchC
#
vlan batch 10 to 11 20 to 21
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 10 to 11
  instance 2 vlan 20 to 21
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 20
 protected-vlan reference-instance 2
```


版权所有 © 华为技术有限公司

```
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode transit primary-port GigabitEthernet0/0/3 secondary-port
GigabitEthernet0/0/4 level 0
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 pport hybrid tagged vlan 10 to 11
 stp disable
#
interface GigabitEthernet0/0/3
 port hybrid tagged vlan 20 to 21
 stp disable
#
interface GigabitEthernet0/0/4
 port hybrid tagged vlan 20 to 21
 stp disable
#
return
```

- SwitchD 的配置文件

```
#
sysname SwitchD
#
vlan batch 10 to 11
#
 rrpp enable
#
 stp region-configuration
  instance 1 vlan 10 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 to 11
 stp disable
#
return
```

- SwitchE 的配置文件

```
#
sysname SwitchE
#
vlan batch 10 to 11
#
rrpp enable
#
 stp region-configuration
  instance 1 vlan 10 to 11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
```


版权所有 © 华为技术有限公司

```
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface GigabitEthernet0/0/2
 port hybrid tagged vlan 10 to 11
 stp disable
#
return
```

配置 RRPP 多实例单环示例

组网需求

如图 9-17 所示，UPE A、UPE B、UPE C 和 PE-AGG 组成 RRPP 多实例单环。

组网中有域 1 环 1 和域 2 环 1 两个环。

从 CE 处接入的 VLAN 范围是 VLAN100 ～ 300。域 1 和域 2 对 VLAN100 ～ 300 的报文进行负载分担。域 1 传输 VLAN100 ～ 200 的报文，域 2 传输 VLAN201 ～ 300 的报文。

域 1 和域 2 中的保护 VLAN 以及保护 VLAN 所属实例详见表 9-1。

表 9-1 实例与保护 VLAN 的映射关系表

Ring ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
域 1	VLAN 5、VLAN 6	Instance 1	VLAN 100 ～ 200	Instance 1
域 2	VLAN 10、VLAN 11	Instance 2	VLAN 201 ～ 300	Instance 2

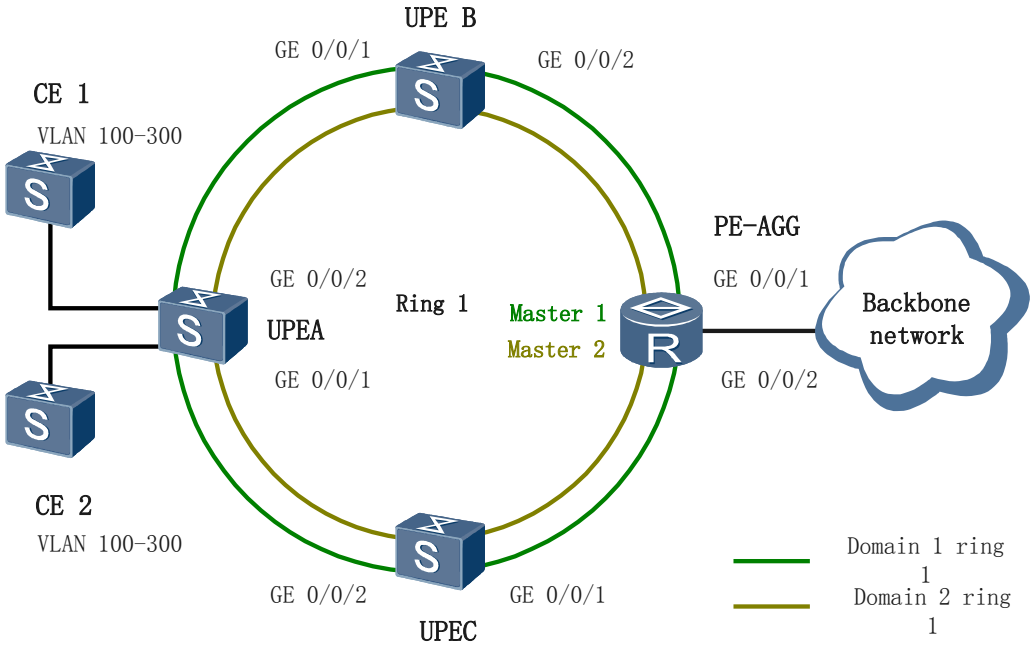
两个环中的主节点以及主节点上的主、副端口详见表 9-2。

表 9-2 主节点以及主、副端口信息表

Ring ID	Master Node	Primary Port	Secondary Port
域 1 环 1	PE-AGG	GE0/0/1	GE0/0/2
域 2 环 1	PE-AGG	GE0/0/2	GE0/0/1

版权所有 © 华为技术有限公司

图 9-17 配置 RRPP 多实例单环组网图



配置思路

采用如下的思路配置 RRPP 多实例单环示例：

1. 配置实例 1 映射 VLAN100 ～ 200。配置实例 2 映射 VLAN201 ～ 300。
2. 将 UPE A、UPE B、UPE C 和 PE-AGG 配置为域 1 的环 1。
3. 将 UPE A、UPE B、UPE C 和 PE-AGG 配置为域 2 的环 1。
4. 配置域 1 和域 2 的保护 VLAN。
5. 配置域 1 和域 2 的控制 VLAN。
6. 配置 PE-AGG 为域 1 环 1 的主节点，UPE A、UPE B、UPE C 为传输节点。
7. 配置 PE-AGG 为域 2 环 1 的主节点，UPE A、UPE B、UPE C 为传输节点。

数据准备

为完成此配置例，需准备如下的数据：

- 实例 ID
- 保护 VLAN 范围
- 控制 VLAN ID
- RRPP 接口的接口编号

操作步骤

步骤 1 创建实例

- 配置 UPE A

在 UPE A 上创建数据 VLAN 100 ～ 300。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- 配置 UPE B

在 UPE B 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- 配置 UPE C

在 UPE C 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- 配置 PE-AGG

在 PE-AGG 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname PE-AGG
[PE-AGG] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

版权所有 © 华为技术有限公司

```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[PE-AGG-mst-region] active region-configuration
[PE-AGG-mst-region] quit
```

- 检查配置结果

经过以上配置，执行以下操作查看实例与 VLAN 的映射关系，以 UPEA 为例。

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0cd568d00
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
      1       5 to 6, 100 to 200
      2       10 to 11, 201 to 300
```

步骤 2 配置加入 RRPP 环的端口

- 配置 UPE A

去使能 UPE A 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEA] interface gigabitethernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port link-type trunk
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface gigabitethernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port link-type trunk
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- 配置 UPE B

去使能 UPE B 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEB] interface gigabitethernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port link-type trunk
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface gigabitethernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port link-type trunk
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
```

- 配置 UPE C

去使能 UPE C 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEC] interface gigabitethernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port link-type trunk
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
```


版权所有 © 华为技术有限公司

```
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface gigabitethernet 0/0/2
[UPEC-GigabitEthernet0/0/2] port link-type trunk
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
```

- 配置 PE-AGG

去使能 PE-AGG 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[PE-AGG] interface gigabitethernet 0/0/1
[PE-AGG-GigabitEthernet0/0/1] port link-type trunk
[PE-AGG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/1] stp disable
[PE-AGG-GigabitEthernet0/0/1] quit
[PE-AGG] interface gigabitethernet 0/0/2
[PE-AGG-GigabitEthernet0/0/2] port link-type trunk
[PE-AGG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/2] stp disable
[PE-AGG-GigabitEthernet0/0/2] quit
```

步骤 3 创建 RRPP 域，配置保护 VLAN 和控制 VLAN。

- 配置 UPE A

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- 配置 UPE B

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
```


版权所有 © 华为技术有限公司

```
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- 配置 PE-AGG

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 5
[PE-AGG-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

步骤 4 创建 RRPP 环

- 配置 UPE A

配置 UPE A 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

配置 UPE A 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- 配置 UPE B

配置 UPE B 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

配置 UPE B 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置 UPE C 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

配置 UPE C 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-
```


版权所有 © 华为技术有限公司

```
port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- 配置 PE-AGG

配置 PE-AGG 为域 1 环 1 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

配置 PE-AGG 为域 2 环 1 的主节点，主接口为 GE0/0/2，副接口为 GE0/0/1。

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 0
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

步骤 5 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

- 配置 UPE A

使能 RRPP 协议。

```
[UPEA] rrpp enable
```

- 配置 UPE B

使能 RRPP 协议。

```
[UPEB] rrpp enable
```

- 配置 UPE C

使能 RRPP 协议。

```
[UPEC] rrpp enable
```

- 配置 PE-AGG

使能 RRPP 协议。

```
[PE-AGG] rrpp enable
```

步骤 6 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 UPE A 和 PE-AGG 为例。

- 在 UPE A 上执行 **display rrpp brief** 命令，查看结果如下：

```
[UPEA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
```


版权所有 © 华为技术有限公司

```
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      T     GigabitEthernet0/0/1           GigabitEthernet0/0/2           Yes

Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      T     GigabitEthernet0/0/1           GigabitEthernet0/0/2           Yes
```

可以看到 UPE A 的上已经使能了 RRPP 协议。

在域 1 中的主控制 VLAN 为 5，保护 VLAN 为 Instance 1，UPEA 为环 1 的传输节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

在域 2 中的主控制 VLAN 为 10，保护 VLAN 为 Instance 2，UPEA 为环 1 的传输节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

- 在 PE-AGG 上执行 **display rrpp brief** 命令，查看结果如下：

```
[PE-AGG] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       M         GigabitEthernet0/0/1          GigabitEthernet0/0/2          Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0        M         GigabitEthernet0/0/2          GigabitEthernet0/0/1          Yes
```

可以看到 PE-AGG 上已经使能了 RRPP 协议。

在域 1 中的主控制 VLAN 为 5，保护 VLAN 为 Instance 1，PE-AGG 为环 1 的主节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

在域 2 中的主控制 VLAN 为 10，保护 VLAN 为 Instance 2，PE-AGG 为环 1 的主节点。主端口为 GE0/0/2，副端口为 GE0/0/1。

- 在 UPE A 上执行 **display rrpp verbose domain** 命令，查看结果如下：

查看 UPE A 在域 1 中的详细信息。

```
[UPEA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
```


版权所有 © 华为技术有限公司

```
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                 Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: UP
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。UPE A 在域 1 中是传输节点，节点状态为 LinkUp。

查看 UPE A 在域 2 中的详细信息。

```
[UPEA] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                 Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: UP
```

可以看到域 2 的控制 VLAN 是 VLAN10，保护 VLAN 是 Instance 2。UPE A 在域 2 中是传输节点，节点状态为 LinkUp。

- 在 PE-AGG 上执行 **display rrpp verbose domain** 命令，查看结果如下：

查看 PE-AGG 在域 1 中的详细信息。

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable               Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: BLOCKED
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。

PE-AGG 在域 1 中是主节点，节点状态为 Complete。

主端口是 GE0/0/1，副端口是 GE0/0/2。

查看 PE-AGG 在域 2 中的详细信息。

```
[PE-AGG] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
```


版权所有 © 华为技术有限公司

```
Ring State    : Complete
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/2         Port status: UP
Secondary port: GigabitEthernet0/0/1         Port status: BLOCKED
```

可以看到域 2 的控制 VLAN 是 VLAN10，保护 VLAN 是 Instance 2。

PE-AGG 在域 2 中是主节点，节点状态为 Complete。

主端口是 GE0/0/2，副端口是 GE0/0/1。

----结束

配置文件

- UPE A 的配置文件

```
#
sysname UPEA
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- UPE B 的配置文件

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
```


版权所有 © 华为技术有限公司

```
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- UPE C 的配置文件

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- PE-AGG 的配置文件

```
#
sysname PE-AGG
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
```


版权所有 © 华为技术有限公司

```
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port GigabitEthernet0/0/1
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

配置 RRPP 多实例相交环示例

组网需求

如图 9-18 所示，UPEA、UPEB、UPEC、UPED 和 PE-AGG 组成 RRPP 多实例主环：域 1 环 1 和域 2 环 1。

CE1、UPEB 和 UPEC 组成 2 个子环：域 1 环 2、域 2 环 2。CE1 与主环相交于 UPEB 和 UPEC 的 GE0/0/3。UPEB 为边缘节点、UPEC 为辅助边缘节点。

CE2、UPEB 和 UPEC 组成 2 个子环：域 1 环 3、域 2 环 3。CE2 与主环相交于 UPEB 和 UPEC 的 GE0/0/4。UPEB 为边缘节点、UPEC 为辅助边缘节点。

从 CE 处接入的 VLAN 范围是 VLAN100 ～ 300。域 1 和域 2 对 VLAN100 ～ 300 的报文进行负载分担。域 1 传输 VLAN100 ～ 200 的报文，域 2 传输 VLAN201 ～ 300 的报文。

域 1 和域 2 中的保护 VLAN 以及保护 VLAN 所属实例详见表 9-3。

表 9-3 实例与保护 VLAN 的映射关系表

Domain ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
域 1	VLAN 5、VLAN 6	Instance 1	VLAN 100 ～ 200	Instance 1
域 2	VLAN 10、VLAN 11	Instance 2	VLAN 201 ～ 300	Instance 2

版权所有 © 华为技术有限公司

6 个环中的主节点以及主节点上的主、副端口详见表 9-4。

表 9-4 主节点以及主、副端口信息表

Ring ID	Master Node	Primary Port	Secondary Port	Ring Type
域 1 环 1	PE-AGG	GE0/0/1	GE0/0/2	Major ring
域 2 环 1	PE-AGG	GE0/0/2	GE0/0/1	Major ring
域 1 环 2	CE1	GE0/0/1	GE0/0/2	Sub ring
域 2 环 2	CE1	GE0/0/2	GE0/0/1	Sub ring
域 1 环 3	CE2	GE0/0/1	GE0/0/2	Sub ring
域 2 环 3	CE2	GE0/0/2	GE0/0/1	Sub ring

4 个子环中的边缘节点、辅助边缘节点、公共端口和边缘端口见表 9-5。

表 9-5 边缘节点、辅助边缘节点以及公共端口、边缘端口信息表

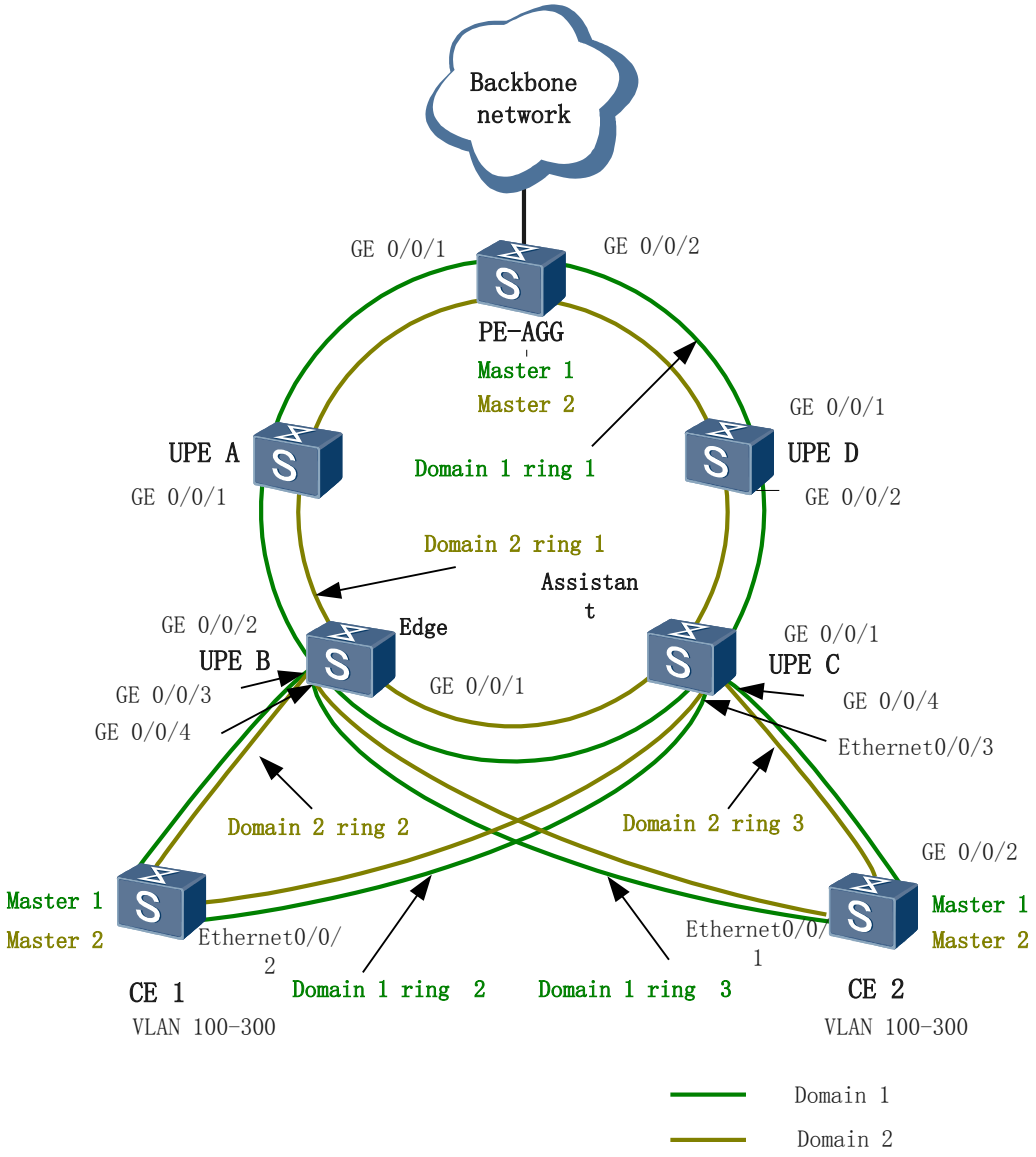
Ring ID	Edge Node	Common Port	Edge Port	Edge-Assistant Node	Common Port	Edge Port
域 1 环 2	UPE B	GE0/0/1	GE0/0/3	UPE C	GE0/0/2	GE0/0/3
域 1 环 3	UPE B	GE0/0/1	GE0/0/4	UPE C	GE0/0/2	GE0/0/4
域 2 环 2	UPE B	GE0/0/1	GE0/0/3	UPE C	GE0/0/2	GE0/0/3
域 2 环 3	UPE B	GE0/0/1	GE0/0/4	UPE C	GE0/0/2	GE0/0/4

为减少 4 个子环的 Edge-Hello 报文都在主环通道中发送，增加有效带宽，将所有子环加入环组。

为防止拓扑振荡，在主节点上配置链路 Up 时延定时器。

版权所有 © 华为技术有限公司

图 9-18 配置 RRPP 多实例相交环组网图



配置思路

采用如下的思路配置 RRPP 多实例相交环示例：

1. 配置实例 1 映射 VLAN100 ～ 200。配置实例 2 映射 VLAN201 ～ 300。
2. 将 UPEA、UPEB、UPEC、UPED 和 PE-AGG 配置为域 1 的环 1 和域 2 的环 1。
3. 将 CE1、UPEB、UPEC 配置为域 1 的环 2 和域 2 的环 2。
4. 将 CE2、UPEB、UPEC 配置为域 1 的环 3 和域 2 的环 3。
5. 配置域 1 和域 2 的保护 VLAN。
6. 配置域 1 和域 2 的控制 VLAN。
7. 配置 PE-AGG 为域 1 环 1 和域 2 环 1 的主节点，UPEA、UPEB、UPEC 为传输节点。

华为专有和保密信息
版权所有 © 华为技术有限公司

8. 配置 CE1 为域 1 环 2 和域 2 环 2 的主节点，UPEB 为边缘节点、UPEC 为辅助边缘节点。
9. 配置 CE2 为域 1 环 3 和域 2 环 3 的主节点，UPEB 为边缘节点、UPEC 为辅助边缘节点。
10. 配置环组。
11. 启动链路 Up 时延定时器。

数据准备

为完成此配置例，需准备如下的数据：

- 实例 ID
- 保护 VLAN 范围
- 控制 VLAN ID
- RRPP 接口的接口编号
- 环组 ID
- 链路 Up 时延定时器值

操作步骤

步骤 1 创建实例

- 配置 CE1

  # 在 CE1 上创建数据 VLAN 100 ～ 300。

  ```
  <Quidway> system-view
  [Quidway] sysname CE1
  [CE1] vlan batch 100 to 300
  ```

  # 创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

  ```
  [CE1] stp region-configuration
  [CE1-mst-region] instance 1 vlan 5 6 100 to 200
  ```

  # 创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

  ```
  [CE1-mst-region] instance 2 vlan 10 11 201 to 300
  ```

  # 激活配置。

  ```
  [CE1-mst-region] active region-configuration
  [CE1-mst-region] quit
  ```

- 配置 CE2

  # 在 CE21 上创建数据 VLAN 100 ～ 300。

  ```
  <Quidway> system-view
  [Quidway] sysname CE2
  [CE2] vlan batch 100 to 300
  ```

  # 创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

  ```
  [CE2] stp region-configuration
  [CE2-mst-region] instance 1 vlan 5 6 100 to 200
  ```

  # 创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

  ```
  [CE2-mst-region] instance 2 vlan 10 11 201 to 300
  ```

  # 激活配置。

  ```
  [CE2-mst-region] active region-configuration
  [CE2-mst-region] quit
  ```

- 配置 UPE A

版权所有 © 华为技术有限公司

在 UPE A 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- 配置 UPE B

在 UPE B 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- 配置 UPE C

在 UPE C 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- 配置 UPE D

在 UPE D 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPED
[UPED] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

```
[UPED-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

版权所有 © 华为技术有限公司

```
[UPED-mst-region] active region-configuration
[UPED-mst-region] quit
```

- 配置 PE-AGG

  # 在 PE-AGG 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname PE-AGG
[PE-AGG] vlan batch 100 to 300
```

  # 创建实例 1，对应域 1 的控制 VLAN5、6 和数据 VLAN100 ～ 200。

```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 5 6 100 to 200
```

  # 创建实例 2，对应域 2 的控制 VLAN10、11 和数据 VLAN201 ～ 300。

```
[PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
```

  # 激活配置。

```
[PE-AGG-mst-region] active region-configuration
[PE-AGG-mst-region] quit
```

- 检查配置结果

  经过以上配置，执行以下操作查看实例与 VLAN 的映射关系，以 UPEA 为例。

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0cd568d00
   Revision level     :0

   Instance   Vlans Mapped
   0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
   1       5 to 6, 100 to 200
   2       10 to 11, 201 to 300
```

步骤 2 配置加入 RRPP 环的端口

- 配置 CE1

  # 去使能 CE1 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[CE1] interface gigabitethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port link-type trunk
[CE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[CE1-GigabitEthernet0/0/1] stp disable
[CE1-GigabitEthernet0/0/1] quit
[CE1] interface gigabitethernet 0/0/2
[CE1-GigabitEthernet0/0/2] port link-type trunk
[CE1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[CE1-GigabitEthernet0/0/2] stp disable
[CE1-GigabitEthernet0/0/2] quit
```

- 配置 CE2

  # 去使能 CE2 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[CE2] interface gigabitethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port link-type trunk
[CE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[CE2-GigabitEthernet0/0/1] stp disable
[CE2-GigabitEthernet0/0/1] quit
[CE2] interface gigabitethernet 0/0/2
[CE2-GigabitEthernet0/0/2] port link-type trunk
[CE2-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[CE2-GigabitEthernet0/0/2] stp disable
[CE2-GigabitEthernet0/0/2] quit
```

- 配置 UPE A

版权所有 © 华为技术有限公司

去使能 UPE A 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEA] interface gigabitethernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port link-type trunk
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface gigabitethernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port link-type trunk
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- 配置 UPE B

  # 去使能 UPE B 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEB] interface gigabitethernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port link-type trunk
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface gigabitethernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port link-type trunk
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
[UPEB] interface gigabitethernet 0/0/3
[UPEB-GigabitEthernet0/0/3] port link-type trunk
[UPEB-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/3] stp disable
[UPEB-GigabitEthernet0/0/3] quit
[UPEB] interface gigabitethernet 0/0/4
[UPEB-GigabitEthernet0/0/4] port link-type trunk
[UPEB-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/4] stp disable
[UPEB-GigabitEthernet0/0/4] quit
```

- 配置 UPE C

  # 去使能 UPE C 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEC] interface gigabitethernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port link-type trunk
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface gigabitethernet 0/0/2
[UPEC-GigabitEthernet0/0/2] port link-type trunk
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
[UPEC] interface gigabitethernet 0/0/3
[UPEC-GigabitEthernet0/0/3] port link-type trunk
[UPEC-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/3] stp disable
[UPEC-GigabitEthernet0/0/3] quit
[UPEC] interface gigabitethernet 0/0/4
[UPEC-GigabitEthernet0/0/4] port link-type trunk
[UPEC-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/4] stp disable
[UPEC-GigabitEthernet0/0/4] quit
```

- 配置 UPE D

  # 去使能 UPE D 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPED] interface gigabitethernet 0/0/1
[UPED-GigabitEthernet0/0/1] port link-type trunk
```


版权所有 © 华为技术有限公司

```
[UPED-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/1] stp disable
[UPED-GigabitEthernet0/0/1] quit
[UPED] interface gigabitethernet 0/0/2
[UPED-GigabitEthernet0/0/2] port link-type trunk
[UPED-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/2] stp disable
[UPED-GigabitEthernet0/0/2] quit
```

- 配置 PE-AGG

  # 去使能 PE-AGG 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[PE-AGG] interface gigabitethernet 0/0/1
[PE-AGG-GigabitEthernet0/0/1] port link-type trunk
[PE-AGG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/1] stp disable
[PE-AGG-GigabitEthernet0/0/1] quit
[PE-AGG] interface gigabitethernet 0/0/2
[PE-AGG-GigabitEthernet0/0/2] port link-type trunk
[PE-AGG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/2] stp disable
[PE-AGG-GigabitEthernet0/0/2] quit
```

步骤 3 创建 RRPP 域，配置保护 VLAN 和控制 VLAN。

- 配置 CE1

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[CE1] rrpp domain 1
[CE1-rrpp-domain-region1] protected-vlan reference-instance 1
[CE1-rrpp-domain-region1] control-vlan 5
[CE1-rrpp-domain-region1] quit
```

  # 配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[CE1] rrpp domain 2
[CE1-rrpp-domain-region2] protected-vlan reference-instance 2
[CE1-rrpp-domain-region2] control-vlan 10
[CE1-rrpp-domain-region2] quit
```

- 配置 CE2

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[CE2] rrpp domain 1
[CE2-rrpp-domain-region1] protected-vlan reference-instance 1
[CE2-rrpp-domain-region1] control-vlan 5
[CE2-rrpp-domain-region1] quit
```

  # 配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[CE2] rrpp domain 2
[CE2-rrpp-domain-region2] protected-vlan reference-instance 2
[CE2-rrpp-domain-region2] control-vlan 10
[CE2-rrpp-domain-region2] quit
```

- 配置 UPE A

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

  # 配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- 配置 UPE B

版权所有 © 华为技术有限公司

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- 配置 UPE D

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] protected-vlan reference-instance 1
[UPED-rrpp-domain-region1] control-vlan 5
[UPED-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

- 配置 PE-AGG

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 5
[PE-AGG-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

步骤 4 创建 RRPP 环

- 配置 PE-AGG

配置 PE-AGG 为域 1 环 1 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1
secondary-port gigabitethernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

配置 PE-AGG 为域 2 环 1 的主节点，主接口为 GE0/0/2，副接口为 GE0/0/1。

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port gigabitethernet 0/0/2
secondary-port gigabitethernet 0/0/1 level 0
```


版权所有 © 华为技术有限公司

```
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

- 配置 UPE A

  # 配置 UPE A 为域 1 环 1 的传输节点，并指定主、副接口。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

  # 配置 UPE A 为域 2 环 1 的传输节点，并指定主、副接口。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- 配置 UPE D

  # 配置 UPE D 为域 1 环 1 的传输节点，并指定主、副接口。

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

  # 配置 UPE D 为域 2 环 1 的传输节点，并指定主、副接口。

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

- 配置 UPE B

  # 配置 UPE B 为域 1 环 1 的传输节点，并指定主、副接口。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port ggigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

  # 配置 UPE B 为域 2 环 1 的传输节点，并指定主、副接口。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

  # 配置 UPE B 为域 1 环 2 的边缘节点，公共端口为 GE0/0/1，边缘端口为 GE0/0/3。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 2 node-mode edge common-port gigabitethernet 0/0/1 edge-port gigabitethernet 0/0/3
[UPEB-rrpp-domain-region1] ring 2 enable
[UPEB-rrpp-domain-region1] quit
```

  # 配置 UPE B 为域 2 环 2 的边缘节点，公共端口为 GE0/0/1，边缘端口为 GE0/0/3。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 2 node-mode edge common-port gigabitethernet 0/0/1 edge-port gigabitethernet 0/0/3
[UPEB-rrpp-domain-region2] ring 2 enable
[UPEB-rrpp-domain-region2] quit
```

  # 配置 UPE B 为域 1 环 3 的边缘节点，公共端口为 GE0/0/1，边缘端口为 GE0/0/4。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 3 node-mode edge common-port gigabitethernet 0/0/1 edge-port gigabitethernet 0/0/4
```


版权所有 © 华为技术有限公司

```
[UPEB-rrpp-domain-region1] ring 3 enable
[UPEB-rrpp-domain-region1] quit
```

配置 UPE B 为域 2 环 3 的边缘节点，公共端口为 GE0/0/1，边缘端口为 GE0/0/4。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 3 node-mode edge common-port gigabitethernet 0/0/1 edge-port gigabitethernet 0/0/4
[UPEB-rrpp-domain-region2] ring 3 enable
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置 UPE C 为域 1 环 1 的传输节点，并指定主、副接口。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

配置 UPE C 为域 2 环 1 的传输节点，并指定主、副接口。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

配置 UPE C 为域 1 环 2 的辅助边缘节点，公共端口为 GE0/0/2，边缘端口为 GE0/0/3。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port gigabitethernet 0/0/2 edge-port gigabitethernet 0/0/3
[UPEC-rrpp-domain-region1] ring 2 enable
[UPEC-rrpp-domain-region1] quit
```

配置 UPE C 为域 2 环 2 的辅助边缘节点，公共端口为 GE0/0/2，边缘端口为 GE0/0/3。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 2 node-mode assistant-edge common-port gigabitethernet 0/0/2 edge-port gigabitethernet 0/0/3
[UPEC-rrpp-domain-region2] ring 2 enable
[UPEC-rrpp-domain-region2] quit
```

配置 UPE C 为域 1 环 3 的辅助边缘节点，公共端口为 GE0/0/1，边缘端口为 GE0/0/4。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 3 node-mode assistant-edge common-port gigabitethernet 0/0/2 edge-port gigabitethernet 0/0/4
[UPEC-rrpp-domain-region1] ring 3 enable
[UPEC-rrpp-domain-region1] quit
```

配置 UPE C 为域 2 环 3 的辅助边缘节点，公共端口为 GE0/0/2，边缘端口为 GE0/0/4。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 3 node-mode assistant-edge common-port gigabitethernet 0/0/2 edge-port gigabitethernet 0/0/4
[UPEC-rrpp-domain-region2] ring 3 enable
[UPEC-rrpp-domain-region2] quit
```

- 配置 CE1

配置 CE1 为域 1 环 2 的主节点，主接口为 0GE0/0/1，副接口为 GE0/0/2。

```
[CE1] rrpp domain 1
[CE1-rrpp-domain-region1] ring 2 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 1
[CE1-rrpp-domain-region1] ring 2 enable
[CE1-rrpp-domain-region1] quit
```

配置 CE1 为域 2 环 2 的主节点，主接口为 GE0/0/2，副接口为 GE0/0/1。

版权所有 © 华为技术有限公司

```
[CE1] rrpp domain 2
[CE1-rrpp-domain-region2] ring 2 node-mode master primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 1
[CE1-rrpp-domain-region2] ring 2 enable
[CE1-rrpp-domain-region2] quit
```

- 配置 CE2

  # 配置 CE2 为域 1 环 3 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[CE2] rrpp domain 1
[CE2-rrpp-domain-region1] ring 3 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 1
[CE2-rrpp-domain-region1] ring 3 enable
[CE2-rrpp-domain-region1] quit
```

  # 配置 CE2 为域 2 环 3 的主节点，主接口为 GE0/0/2，副接口为 GE0/0/1。

```
[CE2] rrpp domain 2
[CE2-rrpp-domain-region2] ring 3 node-mode master primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 1
[CE2-rrpp-domain-region2] ring 3 enable
[CE2-rrpp-domain-region2] quit
```

步骤 5 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

- 配置 PE-AGG

  # 使能 RRPP 协议。

```
[PE-AGG] rrpp enable
```

- 配置 UPE A

  # 使能 RRPP 协议。

```
[UPEA] rrpp enable
```

- 配置 UPE D

  # 使能 RRPP 协议。

```
[UPED] rrpp enable
```

- 配置 UPE B

  # 使能 RRPP 协议。

```
[UPEB] rrpp enable
```

- 配置 UPE C

  # 使能 RRPP 协议。

```
[UPEC] rrpp enable
```

- 配置 CE1

  # 使能 RRPP 协议。

```
[CE1] rrpp enable
```

- 配置 CE2

  # 使能 RRPP 协议。

```
[CE2] rrpp enable
```

步骤 6 配置环组

- 配置 UPE C（辅助边缘节点）

  # 创建环组 1，包含 4 个子环：域 1 环 2、域 1 环 3、域 2 环 2 和域 2 环 3。

```
[UPEC] rrpp ring-group 1
[UPEC-rrpp-ring-group1] domain 1 ring 2 to 3
```


版权所有 © 华为技术有限公司

```
[UPEC-rrpp-ring-group1] domain 2 ring 2 to 3
[UPEC-rrpp-ring-group1] quit
```

- 配置 UPE B（边缘节点）

  # 创建环组 1，包含 4 个子环：域 1 环 2、域 1 环 3、域 2 环 2 和域 2 环 3。

```
[UPEB] rrpp ring-group 1
[UPEB-rrpp-ring-group1] domain 1 ring 2 to 3
[UPEB-rrpp-ring-group1] domain 2 ring 2 to 3
[UPEB-rrpp-ring-group1] quit
```

步骤 7 配置链路 Up 时延定时器

- 配置 CE1

  # 设置链路恢复时延为 1 秒。

```
[CE1] rrpp linkup-delay-timer 1
```

- 配置 CE2

  # 设置链路恢复时延为 1 秒。

```
[CE2] rrpp linkup-delay-timer 1
```

- 配置 PE-AGG

  # 设置链路恢复时延为 1 秒。

```
[PE-AGG] rrpp linkup-delay-timer 1
```

步骤 8 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 UPE B 和 PE-AGG 为例。

- 在 UPE B 上执行 **display rrpp brief** 命令，查看结果如下：

```
[UPEB] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common         Secondary/Edge          Is
 ID     Level   Mode     Port                   Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       T        GigabitEthernet0/0/1          GigabitEthernet0/0/2          Yes
 2      1       E        GigabitEthernet0/0/1          GigabitEthernet0/0/3          Yes
 3      1       E        GigabitEthernet0/0/1          GigabitEthernet0/0/4          Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       T        GigabitEthernet0/0/1          GigabitEthernet0/0/2          Yes
 2      1       E        GigabitEthernet0/0/1          GigabitEthernet0/0/3          Yes
 3      1       E        GigabitEthernet0/0/1          GigabitEthernet0/0/4          Yes
```

可以看到 UPE B 上已经使能了 RRPP 协议。

在域 1 中：

主控制 VLAN 为 5，保护 VLAN 为 Instance 1。

版权所有 © 华为技术有限公司

UPEB 为环 1 的传输节点，主端口为 GE0/0/1，副端口为 GE0/0/2。

UPEB 为环 2 的边缘节点。公共端口为 GE0/0/1，边缘端口为 GE0/0/3。

UPEB 为环 3 的边缘节点。公共端口为 GE0/0/1，边缘端口为 GE0/0/4。

在域 2 中：

主控制 VLAN 为 10，保护 VLAN 为 Instance 2。

UPEB 为环 1 的传输节点。主端口为 0GE/0/1，副端口为 0GE/0/2。

UPEB 为环 2 的边缘节点。公共端口为 GE0/0/1，边缘端口为 GE0/0/3。

UPEB 为环 3 的边缘节点。公共端口为 GE0/0/1，边缘端口为 GE0/0/4。

- 在 PE-AGG 上执行 **display rrpp brief** 命令，查看结果如下：

```
[PE-AGG] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/1          GigabitEthernet0/0/2          Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2          GigabitEthernet0/0/1          Yes
```

可以看到 PE-AGG 上已经使能了 RRPP 协议，链路 Up 时延设置为 2 秒。

在域 1 中的主控制 VLAN 为 5，保护 VLAN 为 Instance 1，PE-AGG 为环 1 的主节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

在域 2 中的主控制 VLAN 为 10，保护 VLAN 为 Instance 2，PE-AGG 为环 1 的主节点。主端口为 GE0/0/2，副端口为 GE0/0/1。

- 在 UPE B 上执行 **display rrpp verbose domain** 命令，查看结果如下：

查看 UPE B 在域 1 中的详细信息。

```
[UPEB] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Primary port  :  GigabitEthernet0/0/2             Port status: UP
Secondary port:  GigabitEthernet0/0/2             Port status: UP

RRPP Ring     : 2
Ring Level    : 1
```


版权所有 © 华为技术有限公司

```
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Common port   : GigabitEthernet0/0/1             Port status: UP
Edge port     : GigabitEthernet0/0/3             Port status: UP

RRPP Ring     : 3
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Common port   : GigabitEthernet0/0/1             Port status: UP
Edge port     : GigabitEthernet0/0/4             Port status: UP
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。

UPE B 在域 1 环 1 中是传输节点，节点状态为 LinkUp。

UPE B 在域 1 环 2 中是边缘节点，节点状态为 LinkUp。公共端口是 GE0/0/1，边缘端口是 GE0/0/3。

UPE B 在域 1 环 3 中是边缘节点，节点状态为 LinkUp。公共端口是 GE0/0/1，边缘端口是 GE0/0/4。

查看 UPE B 在域 2 中的详细信息。

```
[UPEB] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Primary port  : GigabitEthernet0/0/1             Port status: UP
Secondary port: GigabitEthernet0/0/2             Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Common port   : GigabitEthernet0/0/1             Port status: UP
Edge port     : GigabitEthernet0/0/3             Port status: UP

RRPP Ring     : 3
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                          Is Active : Yes
Common port   : GigabitEthernet0/0/1             Port status: UP
Edge port     : GigabitEthernet0/0/4             Port status: UP
```

可以看到域 2 的控制 VLAN 是 VLAN10，保护 VLAN 是 Instance 2。

UPE B 在域 2 中是传输节点，节点状态为 LinkUp。

UPE B 在域 2 环 2 中是边缘节点，节点状态为 LinkUp。公共端口是 GE0/0/1，边缘端口是 GE0/0/3。

UPE B 在域 2 环 3 中是边缘节点，节点状态为 LinkUp。公共端口是 GE0/0/1，边缘端口是 GE0/0/4。

- 在 PE-AGG 上执行 **display rrpp verbose domain** 命令，查看结果如下：

  # 查看 PE-AGG 在域 1 中的详细信息。

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
```


版权所有 © 华为技术有限公司

```
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                              Is Active : Yes
Primary port  : GigabitEthernet0/0/1                 Port status: UP
Secondary port: GigabitEthernet0/0/2                 Port status: BLOCKED
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。

PE-AGG 在域 1 中是主节点，节点状态为 Complete。

主端口是 GE0/0/1，副端口是 GE0/0/2。

查看 PE-AGG 在域 2 中的详细信息。

```
[PE-AGG] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                              Is Active : Yes
Primary port  : GigabitEthernet0/0/2                 Port status: UP
Secondary port: GigabitEthernet0/0/1                 Port status: BLOCKED
```

可以看到域 2 的控制 VLAN 是 VLAN10，保护 VLAN 是 Instance 2。

PE-AGG 在域 2 中是主节点，节点状态为 Complete。

主端口是 GE0/0/2，副端口是 GE0/0/1。

- 在 UPEB 上执行 **display rrpp ring-group** 命令，查看环组设置结果。

  # 显示环组 1 的配置。

```
[UPEB] display rrpp ring-group 1
 Ring Group 1:

 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
```

----结束

配置文件

- CE1 的配置文件

```
#
sysname CE1
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 1
```


版权所有 © 华为技术有限公司

```
 ring 2 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 2 node-mode master primary-port GigabitEthernet0/0/2 secondary-port GigabitEthernet0/0/1
level 1
 ring 2 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- CE2 的配置文件

```
#
#
sysname CE2
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 3 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 1
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 3 node-mode master primary-port GigabitEthernet0/0/2 secondary-port GigabitEthernet0/0/1
level 1
 ring 3 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- UPE A 的配置文件

```
#
#
sysname UPEA
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
```


版权所有 © 华为技术有限公司

```
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- UPE B 的配置文件

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port GigabitEthernet0/0/1 edge-port GigabitEthernet0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port GigabitEthernet0/0/1 edge-port GigabitEthernet0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port GigabitEthernet0/0/1 edge-port GigabitEthernet0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port GigabitEthernet0/0/1 edge-port GigabitEthernet0/0/4
 ring 3 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
```


版权所有 © 华为技术有限公司

```
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- UPE C 的配置文件

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port GigabitEthernet0/0/2 edge-port
GigabitEthernet0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port GigabitEthernet0/0/2 edge-port
GigabitEthernet0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port GigabitEthernet0/0/2 edge-port
GigabitEthernet0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port GigabitEthernet0/0/2 edge-port
GigabitEthernet0/0/4
 ring 3 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan  6 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- UPE D 的配置文件

```
#
sysname UPED
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- PE-AGG 的配置文件

```
#
sysname PE-AGG
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
```


版权所有 © 华为技术有限公司

```
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet0/0/1 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

配置 RRPP 多实例相切环示例

组网需求

如图 9-19 所示，UPE A、UPE B、UPE C、UPE D 组成 RRPP 多实例环，环上包括域 1 环 1 和域 2 环 1。UPE D、UPE E、UPE F、UPE G 组成 RRPP 域 3 环 1。从 CE 处接入的数据 VLAN 通过两个相切环后从 UPE F 上送到骨干网。

两个物理环相切于 UPE D。

从 CE 处接入的 VLAN 范围是 VLAN100 ～ 300。域 1 和域 2 对 VLAN100 ～ 300 的报文进行负载分担。域 1 传输 VLAN100 ～ 200 的报文，域 2 传输 VLAN201 ～ 300 的报文。

域 1、域 2 和域 3 中的保护 VLAN 以及保护 VLAN 所属实例详见表 9-6。

表 9-6 实例与保护 VLAN 的映射关系表

Domain ID	Control VLAN	Instance ID	Protected VLAN	Instance ID
域 1	VLAN 5、6	Instance 1	VLAN 100 ～ 200	Instance 1
域 2	VLAN 10、11	Instance 2	VLAN 201 ～ 300	Instance 2
域 3（UPE D）	VLAN 20、21	Instance 3	VLAN 100 ～ 300	Instance 1、Instance 2
域 3	VLAN 20、21	Instance 1	VLAN 100 ～ 300	Instance 1

3 个环中的主节点以及主节点上的主、副端口详见表 9-7。

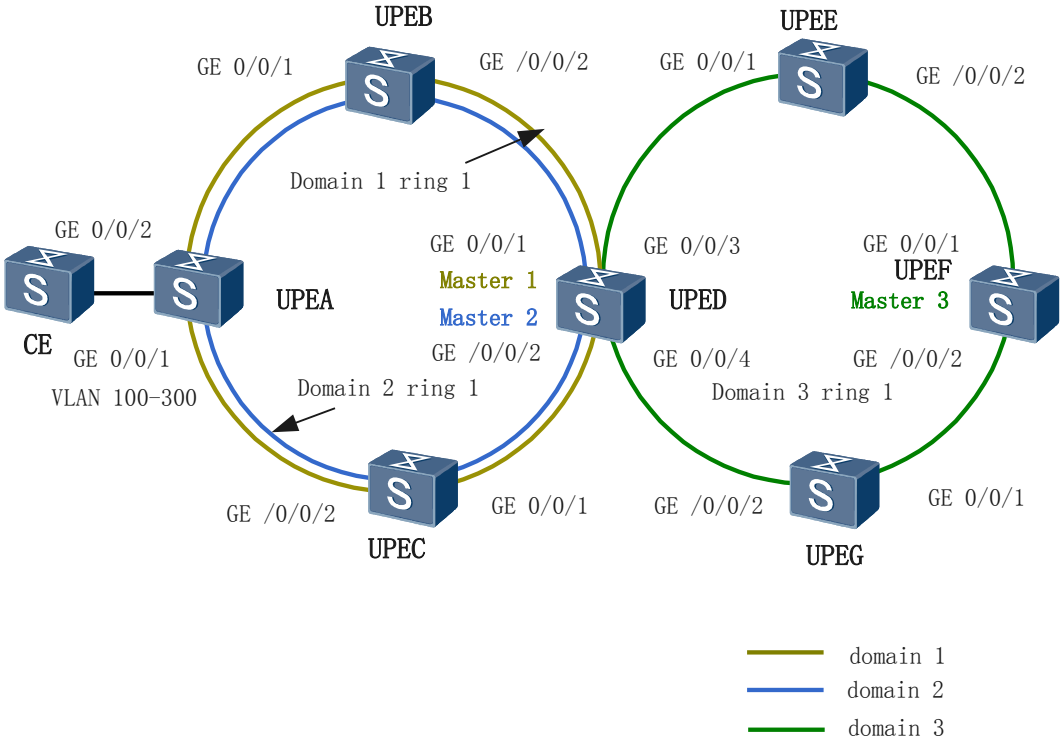
表 9-7 主节点以及主、副端口信息表

Ring ID	Master Node	Primary Port	Secondary Port
域 1 环 1	UPE D	GE0/0/1	GE0/0/2

华为专有和保密信息
版权所有 © 华为技术有限公司

Ring ID	Master Node	Primary Port	Secondary Port
域 2 环 1	UPE D	GE0/0/2	GE0/0/1
域 3 环 1	UPE F	GE0/0/1	GE0/0/2

图 9-19 配置 RRPP 多实例相切环组网图



配置思路

采用如下的思路配置 RRPP 多实例相交环示例：

1. 配置实例 1 映射 VLAN100 ～ 200。配置实例 2 映射 VLAN201 ～ 300。
2. 将 UPE A、UPE B、UPE C、UPE D 配置为域 1 的环 1 和域 2 的环 1。
3. 将 UPE D、UPE E、UPE F、UPE G 配置为域 3 的环 1。
4. 配置域 1 和域 2 的保护 VLAN。
5. 配置域 1 和域 2 的控制 VLAN。
6. 配置域 3 的控制 VLAN。
7. 配置 UPE D 为域 1 环 1 和域 2 环 1 的主节点，UPE A、UPE B、UPE C 为传输节点。
8. 配置 UPE F 为域 3 环 1 的主节点，UPE D、UPE E、UPE G 为传输节点。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- 实例 ID
- 保护 VLAN 范围
- 控制 VLAN ID
- RRPP 接口的接口编号

操作步骤

步骤 1 创建实例

- 配置 UPE A

在 UPE A 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- 配置 UPE B

在 UPE B 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- 配置 UPE C

在 UPE C 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

版权所有 © 华为技术有限公司

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

激活配置。

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- 配置 UPE D

在 UPE D 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPED
[UPED] vlan batch 100 to 300
```

创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 5 6 100 to 200
```

创建实例 2，对应域 2 的控制 VLAN10、VLAN11 和数据 VLAN201 ～ 300。

```
[UPED-mst-region] instance 2 vlan 10 11 201 to 300
```

创建实例 3，对应域 3 的控制 VLAN20、VLAN21。

```
[UPED-mst-region] instance 3 vlan 20 21
```

激活配置。

```
[UPED-mst-region] active region-configuration
[UPED-mst-region] quit
```

- 配置 UPE E

在 UPE 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEE
[UPEE] vlan batch 100 to 300
```

创建实例 1，对应域 3 的控制 VLAN20、VLAN21 和数据 VLAN100 ～ 300。

```
[UPEE] stp region-configuration
[UPEE-mst-region] instance 1 vlan 20 21 100 to 300
```

激活配置。

```
[UPEE-mst-region] active region-configuration
[UPEE-mst-region] quit
```

- 配置 UPE F

在 UPE F 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEF
[UPEF] vlan batch 100 to 300
```

创建实例 1，对应域 3 的控制 VLAN20、VLAN21 和数据 VLAN100 ～ 300。

```
[UPEF] stp region-configuration
[UPEF-mst-region] instance 1 vlan 20 21 100 to 300
```

激活配置。

版权所有 © 华为技术有限公司

```
[UPEF-mst-region] active region-configuration
[UPEF-mst-region] quit
```

- 配置 UPE G

在 UPE G 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname UPEG
[UPEG] vlan batch 100 to 300
```

创建实例 1，对应域 3 的控制 VLAN20、VLAN21 和数据 VLAN100 ～ 300。

```
[UPEG] stp region-configuration
[UPEG-mst-region] instance 1 vlan 20 21 100 to 300
```

激活配置。

```
[UPEG-mst-region] active region-configuration
[UPEG-mst-region] quit
```

- 检查配置结果

经过以上配置，执行以下操作查看实例与 VLAN 的映射关系，以 UPE A 为例。

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0cd568d00
   Revision level     :0

Instance   Vlans Mapped
   0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
   1       5 to 6, 100 to 200
   2       10 to 11, 201 to 300
```

步骤 2 配置加入 RRPP 环的端口

- 配置 UPE A

去使能 UPE A 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEA] interface gigabitethernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port link-type trunk
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface gigabitethernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port link-type trunk
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- 配置 UPE B

去使能 UPE B 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEB] interface gigabitethernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port link-type trunk
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface gigabitethernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port link-type trunk
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

- 配置 UPE C

去使能 UPE C 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEC] interface gigabitethernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port link-type trunk
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface gigabitethernet 0/0/2
[UPEC-GigabitEthernet0/0/2] port link-type trunk
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
```

- 配置 UPE D

去使能 UPE D 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPED] interface gigabitethernet 0/0/1
[UPED-GigabitEthernet0/0/1] port link-type trunk
[UPED-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/1] stp disable
[UPED-GigabitEthernet0/0/1] quit
[UPED] interface gigabitethernet 0/0/3
[UPED-GigabitEthernet0/0/3] port link-type trunk
[UPED-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/3] stp disable
[UPED-GigabitEthernet0/0/3] quit
[UPED] interface gigabitethernet 0/0/2
[UPED-GigabitEthernet0/0/2] port link-type trunk
[UPED-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/2] stp disable
[UPED-GigabitEthernet0/0/2] quit
[UPED] interface gigabitethernet 0/0/4
[UPED-GigabitEthernet0/0/4] port link-type trunk
[UPED-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/4] stp disable
[UPED-GigabitEthernet0/0/4] quit
```

- 配置 UPE E

去使能 UPE E 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEE] interface gigabitethernet 0/0/1
[UPEE-GigabitEthernet0/0/1] port link-type trunk
[UPEE-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEE-GigabitEthernet0/0/1] stp disable
[UPEE-GigabitEthernet0/0/1] quit
[UPEE] interface gigabitethernet 0/0/2
[UPEE-GigabitEthernet0/0/2] port link-type trunk
[UPEE-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEE-GigabitEthernet0/0/2] stp disable
[UPEE-GigabitEthernet0/0/2] quit
```

- 配置 UPE F

去使能 UPE F 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEF] interface gigabitethernet 0/0/1
[UPEF-GigabitEthernet0/0/1] port link-type trunk
[UPEF-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEF-GigabitEthernet0/0/1] stp disable
[UPEF-GigabitEthernet0/0/1] quit
[UPEF] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[UPEF-GigabitEthernet0/0/2] port link-type trunk
[UPEF-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEF-GigabitEthernet0/0/2] stp disable
[UPEF-GigabitEthernet0/0/2] quit
```

- 配置 UPE G

去使能 UPE G 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEG] interface gigabitethernet 0/0/1
[UPEG-GigabitEthernet0/0/1] port link-type trunk
[UPEG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEG-GigabitEthernet0/0/1] stp disable
[UPEG-GigabitEthernet0/0/1] quit
[UPEG] interface gigabitethernet 0/0/2
[UPEG-GigabitEthernet0/0/2] port link-type trunk
[UPEG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEG-GigabitEthernet0/0/2] stp disable
[UPEG-GigabitEthernet0/0/2] quit
```

步骤 3 创建 RRPP 域，配置保护 VLAN 和控制 VLAN。

- 配置 UPE A

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- 配置 UPE B

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```


版权所有 © 华为技术有限公司

- 配置 UPE D

配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] protected-vlan reference-instance 1
[UPED-rrpp-domain-region1] control-vlan 5
[UPED-rrpp-domain-region1] quit
```

配置域 2 的保护 VLAN 为 instance 2 映射的 VLAN。控制 VLAN 为 VLAN10。

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

配置域 3 的保护 VLAN 为 instance 1 ～ 3 映射的 VLAN。控制 VLAN 为 VLAN20。

```
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] protected-vlan reference-instance 1 2 3
[UPED-rrpp-domain-region3] control-vlan 20
[UPED-rrpp-domain-region3] quit
```

- 配置 UPE E

配置域 3 的控制 VLAN 为 VLAN20。

```
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEE-rrpp-domain-region3] control-vlan 20
[UPEE-rrpp-domain-region3] quit
```

- 配置 UPE F

配置域 3 的控制 VLAN 为 VLAN20。

```
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEF-rrpp-domain-region3] control-vlan 20
[UPEF-rrpp-domain-region3] quit
```

- 配置 UPE G

配置域 3 的控制 VLAN 为 VLAN20。

```
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEG-rrpp-domain-region3] control-vlan 20
[UPEG-rrpp-domain-region3] quit
```

步骤 4 创建 RRPP 环

- 配置 UPE A

配置 UPE A 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

配置 UPE A 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```


版权所有 © 华为技术有限公司

- 配置 UPE B

配置 UPE B 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

配置 UPE B 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

- 配置 UPE C

配置 UPE C 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

配置 UPE C 为域 2 环 1 的传输节点，并指定主副接口。

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- 配置 UPE D

配置 UPE D 为域 1 环 1 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

配置 UPE D 为域 2 环 1 的主节点，主接口为 GE0/0/2，副接口为 GE0/0/1。

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode master primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/1 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

配置 UPE D 为域 3 环 1 的传输节点，并指定主副接口。

```
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] ring 1 node-mode transit primary-port gigabitethernet 0/0/2 secondary-port gigabitethernet 0/0/4 level 0
[UPED-rrpp-domain-region3] ring 1 enable
[UPED-rrpp-domain-region3] quit
```

- 配置 UPE E

配置 UPE E 为域 3 环 1 的传输节点，并指定主副接口。

```
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEE-rrpp-domain-region3] ring 1 enable
[UPEE-rrpp-domain-region3] quit
```


版权所有 © 华为技术有限公司

- 配置 UPE F

配置 UPE F 为域 3 环 1 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEF-rrpp-domain-region3] ring 1 enable
[UPEF-rrpp-domain-region3] quit
```

- 配置 UPE G

配置 UPE G 为域 3 环 1 的传输节点，并指定主副接口。

```
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEG-rrpp-domain-region3] ring 1 enable
[UPEG-rrpp-domain-region3] quit
```

步骤 5 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

- 配置 UPE A

使能 RRPP 协议。

```
[UPEA] rrpp enable
```

- 配置 UPE B

使能 RRPP 协议。

```
[UPEB] rrpp enable
```

- 配置 UPE C

使能 RRPP 协议。

```
[UPEC] rrpp enable
```

- 配置 UPE D

使能 RRPP 协议。

```
[UPED] rrpp enable
```

- 配置 UPE E

使能 RRPP 协议。

```
[UPEE] rrpp enable
```

- 配置 UPE F

使能 RRPP 协议。

```
[UPEF] rrpp enable
```

- 配置 UPE G

使能 RRPP 协议。

```
[UPEG] rrpp enable
```

步骤 6 检查配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 UPE D 为例。

版权所有 © 华为技术有限公司

- 在 UPE D 上执行 **display rrpp brief** 命令，查看结果如下：

```
[UPED] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 3

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      M     GigabitEthernet0/0/1           GigabitEthernet0/0/2           Yes

Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary                  Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      M     GigabitEthernet0/0/2           GigabitEthernet0/0/1           Yes

Domain Index   : 3
Control VLAN   : major 20    sub 21
Protected VLAN : Reference Instance 1 to 3
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 ------------------------------------------------------------------------------
 1     0      T     GigabitEthernet0/0/3           GigabitEthernet0/0/4           Yes
```

可以看到 UPE D 的上已经使能了 RRPP 协议。

在域 1 中：

主控制 VLAN 为 1，保护 VLAN 为 Instance 1。

UPE D 为环 1 的主节点，主端口为 GE0/0/1，副端口为 GE0/0/2。

在域 2 中：

主控制 VLAN 为 10，保护 VLAN 为 Instance 2。

UPE D 为环 1 的主节点。主端口为 GE0/0/2，副端口为 GigabitEthernet0/0/1。

在域 3 中：

主控制 VLAN 为 20，保护 VLAN 为 Instance 1 to 3。

UPE D 为环 1 的传输节点。主端口为 GE0/0/3，副端口为 GE0/0/4。

- 在 UPE D 上执行 **display rrpp verbose domain** 命令，查看结果如下：

查看 UPE D 在域 1 中的详细信息。

```
[UPED] display rrpp verbose domain 1
Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
```


版权所有 © 华为技术有限公司

```
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                          Is Active: Yes
Primary port   : GigabitEthernet0/0/1            Port status: UP
Secondary port : GigabitEthernet0/0/2            Port status: BLOCKED
```

可以看到域 1 的控制 VLAN 是 VLAN1，保护 VLAN 是 Instance 1。

UPE D 在域 1 中是主节点，节点状态为 Complete。

主端口是 GE0/0/1，副端口是 GE0/0/2。

查看 UPE D 在域 2 中的详细信息。

```
[UPED] display rrpp verbose domain 2
Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                          Is Active: Yes
Primary port   : GigabitEthernet0/0/2            Port status: UP
Secondary port : GigabitEthernet0/0/1            Port status: BLOCKED
```

可以看到域 2 的控制 VLAN 是 VLAN10，保护 VLAN 是 Instance 2。

UPE D 在域 2 中是主节点，节点状态为 Complete。

主端口是 GE0/0/2，副端口是 GE0/0/1。

查看 UPE D 在域 3 中的详细信息。

```
[UPED] display rrpp verbose domain 3
Domain Index   : 3
Control VLAN   : major 20    sub 21
Protected VLAN : Reference Instance 1 to 3
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Transit
Ring State     : LinkUp
Is Enabled     : Enable                          Is Active: Yes
Primary port   : GigabitEthernet0/0/3            Port status: UP
Secondary port : GigabitEthernet0/0/4            Port status: UP
```

可以看到域 3 的控制 VLAN 是 VLAN20，保护 VLAN 是 Instance 1 to 3。

UPE D 在域 3 中是传输节点，节点状态为 LinkUp。

主端口是 GE0/0/3，副端口是 GE0/0/4。

----结束

配置文件

- UPE A 的配置文件

版权所有 © 华为技术有限公司

```
#
sysname UPEA
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- UPE B 的配置文件

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- UPE C 的配置文件

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 1
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
Return
```

- UPE D 的配置文件

```
#
sysname UPED
#
vlan batch 5 to 6 10 to 11 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 instance 3 vlan 20 to 21
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2 level
0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet0/0/2 secondary-port GigabitEthernet0/0/1 level
0
 ring 1 enable
rrpp domain 3
```


版权所有 © 华为技术有限公司

```
 control-vlan 20
 protected-vlan reference-instance 1 2 3
 ring 1 node-mode transit primary-port GigabitEthernet0/0/3 secondary-port GigabitEthernet0/0/4
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- UPE E 的配置文件

```
#
sysname UPEE
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- UPE F 的配置文件

```
#
sysname UPEF
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
```


版权所有 © 华为技术有限公司

```
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2 level
0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- UPE G 的配置文件

```
#
sysname UPEG
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet0/0/1 secondary-port GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

9.4 以太网 OAM 配置

通过对以太网 OAM 的介绍和各种配置，实现链路级以太网 OAM 和网络级以太网 OAM 链路的检测，提高网络可靠性。

9.4.1 以太网 OAM 概述

以太网 OAM 是能够有效提高以太网的网络管理能力和维护能力，保障网络的稳定运行。它主要应用在以太网中。

版权所有 © 华为技术有限公司

产生背景

以太网技术自诞生起，以其简单易用、价格低廉的特点逐步成为局域网的主导技术。近年来，随着千兆、万兆以太网技术的相继应用，以太网已经向城域网和广域网方向扩展。

由于以太网最初主要应用于局域网，相对于城域网和广域网，局域网对可靠性、稳定性要求都较低，因此以太网一直缺乏运行维护管理机制，这一点已成为以太网严重障碍。因此，在以太网上实现 OAM（Operations Administration and Maintenance）成为一个必然的发展趋势。

主要功能

以太网 OAM 主要功能可分为以下两部分：

- 故障管理
  - 通过定时或手动发送检测报文来探测网络的连通性。
  - 提供类似 IP 网络中的 Ping（Packet Internet Groper）和 Traceroute 的功能，对以太网进行故障确认和故障定位。
  - 和保护倒换协议配合，当检测到连通性故障后触发保护倒换，以实现网络业务中断小于等于 50 毫秒的可靠性目标。
- 性能管理

  性能管理主要是指对网络中的丢包、时延、抖动进行衡量，也包括对网络中各类流量进行统计。性能管理通常在用户接入点实施。有了性能管理工具，可通过网管监测网络运行情况、定位故障，确认网络转发能力是否符合与用户签订的 SLA（Service Level Agreement）。

以太网 OAM 能够有效提高以太网的网络管理和维护能力，保障网络的稳定运行。

9.4.2 AC6605 支持的以太网 OAM 特性

介绍以太网 OAM 特性在 AC6605 中的支持情况。

EFM OAM

802.3ah（Ethernet in the First Mile，简称 EFM）主要定义用于用户接入部分的以太网物理层规范，以及接入部分的以太网 OAM。主要用于最后一公里的链路检测。是链路级的 OAM。AC6605 设备的 EFM OAM 功能包括：

- 对端发现

  对端发现是指当 AC6605 的某个接口和对端接口使能了 EFM OAM 功能时，该接口和对端接口通过发送和响应慢速协议帧 OAMPDU（OAM Protocol Data Unit）来协商确定双方的 EFM OAM 配置是否匹配。如果双方的 EFM OAM 配置匹配，则双方进入 EFM OAM 握手阶段。在握手阶段，双方通过定时发送 OAMPDU 维持邻居关系。
- 链路监控

  链路监控是指如果接口检测到误帧越限事件或误帧秒越限事件，则该接口通过向对端设备发送事件通告 OAMPDU 来通告故障。其中：
  - 误帧越限事件是指在设定的观察时长内，接口检测到的误帧数量达到或超过设定的阈值。

版权所有 © 华为技术有限公司

- 误码越限事件是指在设定的观察时长内，接口检测到的误码数量达到或超过设定的阈值。
- 误帧秒越限事件是指在设定的观察时长内，接口检测到的误帧秒数量达到或超过设定的阈值。

其中，误帧秒是指将设定的观察时长划分为若干个以 1 秒为单位的时间段，如果在某个时间段内检测到了至少一个误帧，则该时间段称为一个误帧秒。

- 故障通告

  故障通告是指当本端发生报文错误越限事件或严重故障事件后，本端发送故障消息通告对端设备，同时将故障事件记入日志并上报给网管系统。

  - 系统重新启动
  - 物理链路故障
  - 协议报文超时
  - OAM 管理模块传递的故障

  对端设备接到通知消息后，将消息中携带的故障事件记入日志，并上报给网管系统。

每个具备 EFM OAM 功能的接口都有一个工作模式属性。EFM OAM 工作模式共包括两种：主动模式和被动模式。对端发现和远端环回都只能由主动模式的接口发起。

以太网 CFM

802.1ag（Connectivity Fault Management，简称 CFM）定义了基于以太网承载网络的连接检测的 OAM 功能，适用于大规模组网的端到端场景，是网络级的 OAM。

表 9-8 802.1 协议 draft7 版本和 standard2007 版本的区别

特性	draft7	standard2007	备注
MD（Maintenance Domain）	支持	支持	标准版本和草案实现的功能、配置一样
默认 MD（Default Maintenance Domain）	不支持	支持	-
MA（Maintenance Association）	支持	支持	标准版本和草案实现的功能、配置一样
MEP（Maintenance association End Point）	支持	支持	标准版本和草案实现的功能、配置一样
RMEP（Remote Maintenance association End Point）	支持	支持	标准版本和草案实现的功能、配置一样

华为专有和保密信息
版权所有 © 华为技术有限公司

特性	draft7	standard2007	备注
MIP（Maintenance association Intermediate Point）	支持	支持	标准版本和草案中 MIP 节点的生成规则是一样的，分为：default 型、explicit 型和 none 型。不同的是： ● 草案中，MIP 节点是基于端口创建。 ● 标准版本中，MIP 节点是基于 MD 或默认 MD 创建。
MP（Maintenance Point）	支持	支持	标准版本和草案实现的功能、配置一样

- 基本概念
  - MD

    维护域 MD（Maintenance Domain）是指对其实施以太网 CFM 管理的一个网络或一个网络的一部分。一个 MD 由一个统一的 ISP（Internet Service Provider）进行管理。
  - MA

    维护联盟 MA（Maintenance Association）是 MD 的一部分。一个 MD 可以划分成一个或多个 MA。在 AC6605 设备上，每个 MA 可以对应一个 VLAN。以太网 CFM 对每个 MA 分别进行连通性故障检测。
  - 默认 MD

    802.1ag2007 标准版本规定，每台设备上可配置一个默认 MD。默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。
  - MEP

    维护联盟边缘节点 MEP（Maintenance association End Point）是 MA 的边缘节点。

    对于运行以太网 CFM 的网络中的任意一台设备，该设备上的 MEP 称为本地 MEP，同一 MA 内其它设备上的 MEP 对本设备而言称为远端维护联盟边缘节点 RMEP（Remote Maintenance association End Point）。

    注意

    一个 Trunk 口上只支持配置一个 MEP。
  - MIP

    维护联盟内部节点 MIP（Maintenance association Intermediate Point）是 MA 的内部节点。

    MIP 位于设备的接口上，是设备按规则自动创建的。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 连通性故障检测

  以太网 CFM 将整个网络划分成一个或多个 MD，将每个 MD 又划分成一个或多个 MA，通过同一 MA 的 MEP 之间定时互发 CCM（Continuity Check Message）消息来检测该 MA 内以太网的连通性。

- 故障确认
  - 802.1ag MAC Ping

    802.1ag MAC Ping 与 Ping 类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。802.1ag MAC Ping 在同一个 MA 内进行，由 MEP 发起，目的节点可以是 RMEP 或 MIP。
  - 通用 Gmac ping

    通用 Gmac ping 和 802.1ag MAC Ping 原理相似，但是通用 Gmac ping 不需要由 MEP 发起，目的节点也不需要是 RMEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac ping。
- 故障定位
  - 802.1ag MAC Trace

    802.1ag MAC Trace 与 Traceroute（或 Tracert）类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。802.1ag MAC Trace 在同一个 MA 内进行，由 MEP 发起，目的节点可以是 RMEP 或 MIP。
  - 通用 Gmac trace

    通用 Gmac trace 和 802.1ag MAC Trace 原理相似，但是通用 Gmac trace 不需要由 MEP 发起，中间节点和目的节点也不需要是 RMEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac trace，所有中间设备均回应 LTR（Linktrace Reply）消息。

故障联动

- EFM OAM 与接口联动

  可以配置以下两种方式的 EFM OAM 与接口联动：
  - 配置 EFM OAM 检测到故障后，OAM 管理模块对该接口进行闪断处理，即先关闭该接口 7 秒，然后再打开该接口。
  - 配置当 EFM OAM 检测到故障时，与其绑定的接口会被关闭或发送 DOWN 事件。当接口 DOWN 时，通过联动将故障传递至 EFM OAM 的对端设备。

  EFM OAM 与接口联动是指当 EFM OAM 检测到链路连通性故障后，接口下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

  此外，请务必确保两端 EFM OAM 协议状态变为 detect 之后再配置 EFM OAM 和当前接口联动功能。
- EFM OAM 和 EFM OAM 联动

  EFM OAM 和 EFM OAM 联动是指检测到故障后，OAM 管理模块通过绑定关系将传递该故障。
  - 某侧 EFM OAM 向另一侧 EFM OAM 传递故障
  - 两侧 EFM OAM 双向传递故障
- 以太网 CFM 与接口联动

  可以配置以下两种方式的以太网 CFM 与接口联动

版权所有 © 华为技术有限公司

- 配置某个 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障后，OAM 管理模块对该接口进行闪断处理，即先关闭该接口 7 秒，然后再打开该接口。
- 配置当以太网 CFM 检测到故障时，与其绑定的接口会被关闭或发送 DOWN 事件；配置当接口 DOWN 时，与其绑定的以太 CFM 状态会变为 Down。

- 以太网 CFM 和 EFM OAM 联动

  以太网 CFM 和 EFM OAM 联动是指 MA 内检测到故障后，OAM 管理模块通过接口将故障传递到 EFM OAM 的对端；EFM OAM 模块检测到故障后，OAM 管理模块通过接口将故障传递到 MA。

  - 以太网 CFM 向 EFM OAM 传递故障
  - EFM OAM 向以太网 CFM 传递故障
  - 以太网 CFM 和 EFM OAM 双向传递故障

- 以太网 CFM 和以太网 CFM 联动

  以太网 CFM 和以太网 CFM 联动是指 MA 内检测到故障后，OAM 管理模块通过绑定关系将该故障传递到另一侧的 MA：

  - 某侧以太网 CFM 向另一侧以太网 CFM 传递故障
  - 两侧以太网 CFM 双向传递故障

9.4.3 配置 EFM OAM 基本功能

通过配置 EFM OAM 基本功能，检测两直连设备之间链路的连通性。

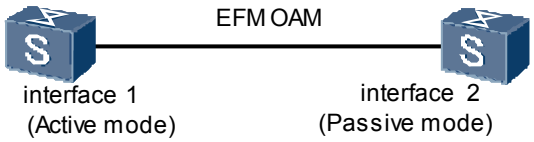
建立配置任务

在配置 EFM OAM 基本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-20 所示，当需要检测两直连设备之间链路的连通性时，可执行本配置任务。

图 9-20 配置 EFM OAM 基本功能



前置任务

无

数据准备

在配置 EFM OAM 基本功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	（可选）EFM OAM 协议报文的最大尺寸

全局使能 EFM OAM 功能

全局使能 EFM OAM 功能是所有使用 EFM OAM 功能的前提条件。

背景信息

请在链路两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **efm enable**，全局使能 EFM OAM 功能。

缺省情况下，EFM OAM 功能处于全局禁止状态。

----结束

配置接口的 EFM OAM 工作模式

EFM OAM 工作模式是具备 EFM OAM 接口的一个属性，包括两种模式：主动模式和被动模式。

背景信息

说明

只能在 EFM OAM 功能全局使能后，接口的 EFM OAM 功能使能前，配置接口的 EFM OAM 工作模式。在接口的 EFM OAM 功能使能后，设备不允许再改变接口的 EFM OAM 工作模式。

请在链路两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm mode** { **active** | **passive** }，配置接口的 EFM OAM 工作模式。

缺省情况下，接口的 EFM OAM 工作模式是主动模式。

应将链路两端中至少一端的接口配置为主动模式。配置为主动模式的接口，在使能了接口的 EFM OAM 功能后，会主动发起 EFM OAM 对端发现。而配置为被动模式的接口则不会主动发起 EFM OAM 对端发现过程，而是等待对端发送的协议报文。如果两端都配置成为主动模式，链路检测也可以进行；如果两端都配置成为被动模式，则链路检测无法进行。

版权所有 © 华为技术有限公司

说明

必须在配置 EFM OAM 的接口下使能 **bpdu enable**，否则 OAMPDU 报文会被丢弃。

----结束

（可选）配置 EFM OAM 协议报文的最大尺寸

可以在接口上配置 EFM OAM 协议报文的最大尺寸。在当前接口上，超过此尺寸的 EFM OAM 协议报文被作为非法报文丢弃。

背景信息

请在链路两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm packet max-size** *size*，配置 EFM OAM 协议报文的最大尺寸。

缺省情况下，接口的 EFM OAM 协议报文的最大尺寸是 128 字节。

超过最大尺寸的 EFM OAM 协议报文被作为非法报文丢弃。

如果将链路两端接口的 EFM OAM 协议报文最大尺寸参数配置为不同的值，两端接口在发现阶段通过协商确定此参数值。协商的结果是取配置值较小的一端的配置值。

----结束

使能接口的 EFM OAM 功能

只有使能两端端口的 EFM OAM 功能后，才开始点到点的 EFM 链路检测。

背景信息

请在链路两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm enable**，使能接口的 EFM OAM 功能。

缺省情况下，接口的 EFM OAM 功能处于禁止状态。

----结束

检查配置结果

通过查看 EFM OAM 配置信息等内容，来检查配置是否成功。

版权所有 © 华为技术有限公司

前提条件

已经完成 EFM OAM 基本功能的所有配置。

操作步骤

- 使用 **display efm** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 配置信息。
- 使用 **display efm session** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 协议状态。

----结束

任务示例

执行命令 **display efm**，可以查看本端接口的所有 EFM OAM 配置和对端接口的部分 EFM OAM 配置。

```
<Quidway> display efm interface gigabitethernet 0/0/1
  Item                          Value
  ------------------------------------------------------
  Interface:                    GigabitEthernet0/0/1
  EFM Enable Flag:              enable
  Mode:                         active
  OAMPDU MaxSize:               128
  ErrCodeNotification:          disable
  ErrCodePeriod:                1
  ErrCodeThreshold:             1
  ErrFrameNotification:         disable
  ErrFramePeriod:               1
  ErrFrameThreshold:            1
  ErrFrameSecondNotification:   disable
  ErrFrameSecondPeriod:         60
  ErrFrameSecondThreshold:      1
  Hold Up Time:                 0
  ThresholdEvtTriggerErrDown:   disable
  TriggerIfDown:                disable
  TriggerMacRenew:              disable
  Remote MAC:                   00e0-fc7f-724f
  Remote EFM Enable Flag:       enable
  Remote Mode:                  passive
  Remote MaxSize:               128
  Remote State:                 --
```

如果配置正确，两端接口成功协商后进入握手阶段，此时执行 **display efm session** 命令，可看到接口的 EFM OAM 协议状态为 detect。

```
<Quidway> display efm session interface gigabitethernet 0/0/1
  Interface               EFM State               Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/1    detect                  --
```

9.4.4 配置 EFM OAM 链路监控

通过配置 EFM OAM 误帧、误码和误帧秒检测，能够更好的检测和发现链路层的故障。

建立配置任务

在配置 EFM OAM 链路监控功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

链路监控用于在各种情况下检测和发现链路层的故障。链路监控使用事件通知的OAMPDU，当链路故障发生时，本地链路监控到故障后通过事件的方式通知远端的 OAM 实体。

前置任务

在配置 EFM OAM 链路监控之前，需完成以下任务：

- **配置 EFM OAM 基本功能**

数据准备

在配置 EFM OAM 链路监控之前，需要准备以下数据。

序号	数据
1	（可选）EFM OAM 误帧检测观察时长、阈值
2	（可选）EFM OAM 误码检测观察时长、阈值
3	（可选）EFM OAM 误帧秒检测观察时长、阈值

（可选）配置 EFM OAM 误帧检测

误帧是指 1 秒钟内错误的帧数。当 EFM OAM 误帧检测上报功能使能后，如果在设置的观察时长内，接口检测到的误帧数量达到或者超过门限值，那么设备将产生误帧越限事件，并通告对端设备。

背景信息

请在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm error-frame period** *period*，配置接口的 EFM OAM 误帧检测观察时长。

缺省情况下，接口的 EFM OAM 误帧检测观察时长是 1 秒。

步骤 4 执行命令 **efm error-frame threshold** *threshold*，配置接口的 EFM OAM 误帧检测门限。

缺省情况下，接口的 EFM OAM 误帧检测门限是 1。

步骤 5 执行命令 **efm error-frame notification enable**，使能接口的 EFM OAM 误帧检测上报功能。

缺省情况下，接口的 EFM OAM 误帧检测上报功能处于禁止状态。

----结束

版权所有 © 华为技术有限公司

（可选）配置 EFM OAM 误码检测

误码是指 1 秒钟内错误的编码数。当 EFM OAM 误码检测上报功能使能后，如果在设置的观察时长内，接口检测到的误码数量达到或者超过门限值，那么设备将产生误码越限事件，并通告对端设备。

背景信息

请在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm error-code period** *period*，配置接口的 EFM OAM 误码检测观察时长。

缺省情况下，接口的 EFM OAM 误码检测观察时长是 1 秒。

步骤 4 执行命令 **efm error-code threshold** *threshold*，配置接口的 EFM OAM 误码检测门限。

缺省情况下，接口的 EFM OAM 误码检测门限是 1。

步骤 5 执行命令 **efm error-code notification enable**，使能接口的 EFM OAM 误码检测上报功能。

缺省情况下，接口的 EFM OAM 误码检测上报功能处于禁止状态。

----结束

（可选）配置 EFM OAM 误帧秒检测

当 EFM OAM 误帧秒检测上报功能使能后，如果在设置的观察时长内，接口检测到的误帧秒数量达到或者超过门限值，那么设备将产生误帧秒越限事件，并通告对端设备。

背景信息

误帧秒是指将设定的观察时长划分为若干个以 1 秒为单位的时间段，如果在某个时间段内检测到了至少一个误帧，则该时间段称为一个误帧秒。即指定 M 秒数下有错误帧的时间数。

请在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm error-frame-second period** *period*，配置接口的 EFM OAM 误帧秒检测观察时长。

缺省情况下，接口的 EFM OAM 误帧秒检测观察时长是 60 秒。

步骤 4 执行命令 **efm error-frame-second threshold** *threshold*，配置接口的 EFM OAM 误帧秒检测门限。

版权所有 © 华为技术有限公司

缺省情况下，接口的 EFM OAM 误帧秒检测门限是 1。

步骤 5 执行命令 **efm error-frame-second notification enable**，使能接口的 EFM OAM 误帧秒检测上报功能。

缺省情况下，接口的 EFM OAM 误帧秒检测上报功能处于禁止状态。

----结束

（可选）配置越限事件同接口联动

配置越限事件和接口联动功能后，系统会将接口的管理状态置为 Down，从而阻塞该接口上的所有业务。

背景信息

配置了误帧、误码或者误帧秒检测功能后，如果在设置的观察时长内，接口检测到的误帧、误码或者误帧秒数量达到或者超过门限值，则用户可以认为此链路不可以用，此时可以配置越限时事件和接口联动功能。

请在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm threshold-event trigger error-down**，配置越限事件和接口联动功能。

缺省情况下，越限事件和当前接口不联动。

----结束

后续处理

配置越限事件和接口联动功能后，用户可以通过配置将接口的管理状态恢复为 Up。有两种方法，请选择执行其一：

- 在系统视图下，使用 **efm holdup-timer** 命令配置接口的管理状态自动恢复为 Up 的延迟时间。
- 在接口视图下，先使用 **shutdown** 命令，然后再使用 **undo shutdown** 命令将接口的管理状态恢复为 Up。

检查配置结果

通过查看 EFM OAM 配置信息等内容，来检查配置是否成功。

前提条件

已经完成 EFM OAM 链路监控功能的所有配置。

操作步骤

- 使用 **display efm** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 配置信息。

版权所有 © 华为技术有限公司

- 使用 **display efm session** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 协议状态。

----结束

任务示例

执行命令 **display efm**，可以查看接口的 EFM OAM 链路监控配置。

```
<Quidway> display efm interface gigabitethernet 0/0/1
    Item                              Value
    ------------------------------------------------------------
    Interface:                        GigabitEthernet0/0/1
    EFM Enable Flag:                  enable
    Mode:                             active
    OAMPDU MaxSize:                   128
    ErrCodeNotification:              enable
    ErrCodePeriod:                    1
    ErrCodeThreshold:                 1
    ErrFrameNotification:             enable
    ErrFramePeriod:                   1
    ErrFrameThreshold:                1
    ErrFrameSecondNotification:       enable
    ErrFrameSecondPeriod:             60
    ErrFrameSecondThreshold:          1
    Hold Up Time:                     0
    ThresholdEvtTriggerErrDown:       enable
    TriggerIfDown:                    disable
    TriggerMacRenew:                  disable
    RemoteMAC:                        00e0-fc7f-7258
    Remote EFM Enable Flag:           enable
    Remote Mode:                      passive
    Remote  MaxSize:                  128
    Remote State:                     --
```

9.4.5 配置物理链路丢包率检测

可以检测物理链路的丢包率，以便用户能够采取有效的措施来保证链路更好的工作。

建立配置任务

在配置物理链路丢包率检测功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

注意

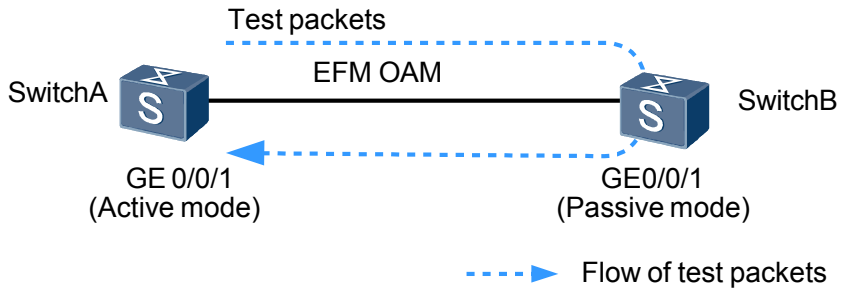
EFM OAM 远端环回影响业务数据的正常转发，请在不需转发业务数据的链路上配置。

当需要检测某段链路的丢包率时，可执行本配置任务。

例如：如图 9-21 所示，在 SwitchA 和 SwitchB 之间配置 EFM OAM，在 SwitchA 的接口 GE0/0/1 上配置远端环回。然后从 SwitchA 向 SwitchB 发送测试报文，在 SwitchA 上观察测试报文的返回情况，从而得到链路的丢包率。

版权所有 © 华为技术有限公司

图 9-21 测试链路丢包率



前置任务

在测试链路丢包率之前，需完成以下任务：

- **配置 EFM OAM 基本功能**

数据准备

在测试链路丢包率之前，需要准备以下数据。

序号	数据
1	远端环回的超时时间
2	测试报文的目的 MAC 地址、所属 VLAN、测试报文的出接口、测试报文的大小、数量、发送速率

配置 EFM OAM 远端环回

EFM OAM 远端环回可用来定位远端故障和测试链路质量。

背景信息

EFM OAM 远端环回功能为用户提供了一种测试链路性能的手段，其具体的实现过程为

1. 主动模式下的 OAM 实体向对端设备发起远端环回请求。
2. 手动或者自动取消发起端设备的远端环回功能。

操作步骤

步骤 1 请在主动模式的发起端设备上配置远端环回请求功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **efm loopback start** [**timeout** *timeout*]，配置接口发起 EFM OAM 远端环回。

版权所有 © 华为技术有限公司

注意

EFM 远端环回功能会影响数据和协议报文的正常转发，建议不要环回端口上配置其它业务。

缺省情况下，远端环回的超时时间是 20 分钟。到达此时间，远端环回自动取消。如果需要使某链路一直处于远端环回状态，可将超时时间设置为 0。

修改 **timeout** *timeout* 值时，需要先使用 **efm loopback stop** 命令停止接口的远端环回功能。

只有在两端的 EFM OAM 协议处于 detect 状态，本端的 EFM OAM 工作模式为主动模式时，远端环回才能成功进行。可使用 **display efm session** 命令查询本端和对端之间 EFM OAM 协议是否处于 detect 状态。

----结束

发送测试报文

发送的测试报文是为测试链路的丢包率构造的一种以太类型的报文。它可与 EFM OAM 远端环回功能配合使用，来测试链路的丢包率。

背景信息

在链路两端设备当中主动模式接口所在设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **test-packet start** [**mac** *mac-address*] [**vlan** *vlan-id*] **interface** *interface-type interface-number* [**-c** *count* | **-s** *size*] *，发送测试报文。

缺省情况下，测试报文的大小是 64 字节，发送数量是 5 个。

测试报文的出接口应配置为连接被测链路的接口。

----结束

后续处理

在发送测试报文进行过程中，不能修改发送测试报文的参数。

如需终止发送测试报文，可按<Ctrl+C>快捷键。

查看测试报文的返回统计

通过查看测试报文的返回统计来计算链路的丢包率。

背景信息

在链路两端设备当中主动模式接口所在设备上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **display test-packet result**，查看测试报文的返回统计。

display test-packet result 命令的显示信息包括：

- 发送测试报文的个数
- 接收报文的个数
- 丢弃报文的个数
- 发送报文的总字节数
- 接收报文的总字节数
- 丢弃报文的总字节数
- 发送开始时间
- 发送结束时间

根据以上数据可计算链路的丢包率。

----结束

（可选）手动取消 EFM OAM 远端环回

EFM OAM 远端换回既可以超时自动取消也可以手动取消。

背景信息

在链路两端设备当中主动模式接口所在设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **efm loopback stop**，配置接口取消 EFM OAM 远端环回。

为避免由于用户忘记停止 EFM OAM 远端环回而造成链路长时间无法正常转发业务数据，AC6605 设备的 EFM OAM 远端环回具有超时自动取消功能。缺省情况下，远端环回的超时时间是 20 分钟，到达此时间，远端环回自动取消。如果需要手工取消远端环回，可执行以上配置步骤。

----结束

检查配置结果

操作步骤

步骤 1 **display efm session** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 协议状态。

----结束

版权所有 © 华为技术有限公司

任务示例

配置 EFM OAM 远端环回成功后，在链路两端设备当中主动模式接口所在设备上执行 **display efm session** 命令，可以看到主动模式接口的 EFM OAM 协议状态为 Loopback（control），即远端环回状态（且为远端环回的发起方）。

```
<Quidway> display efm session interface gigabitethernet 0/0/1
  Interface                EFM State                 Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/1     Loopback(control)          20
```

配置 EFM OAM 远端环回成功后，在链路两端设备当中被动模式接口所在设备上执行 **display efm session** 命令，可以看到被动模式接口的 EFM OAM 协议状态为 Loopback（be controlled），即远端环回状态（且为远端环回的响应方）。

```
<Quidway> display efm session interface gigabitethernet 0/0/1
  Interface                EFM State                 Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/1     Loopback(be controlled)   --
```

在远端环回自动取消或手动取消后，在链路两端中任一端设备上执行 **display efm session** 命令，可以看到链路两端接口的 EFM OAM 协议状态为 Detect 或 Discovery，即握手状态或对端发现状态。

```
<Quidway> display efm session interface gigabitethernet 0/0/1
  Interface                EFM State                 Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/1     detect                    --
```

9.4.6 配置 EFM OAM 和接口联动

一旦 EFM OAM 和接口联动后，可能对业务产生很大影响，例如二三层业务全部被阻塞。

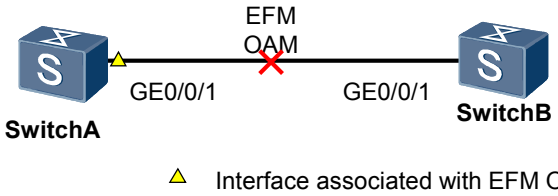
建立配置任务

在配置 EFM OAM 和接口联动功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-22 所示，两台设备之间配置了 EFM OAM 功能，并配置了 EFM OAM 和 SwitchA 的接口 GE0/0/1 联动。在 SwitchA 上，当 EFM OAM 模块检测到和 SwitchB 之间有连通性故障时，接口 GE0/0/1 下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

图 9-22 EFM OAM 和接口联动示意图



版权所有 © 华为技术有限公司

前置任务

在配置 EFM OAM 和接口联动之前，需完成以下任务：

- **配置 EFM OAM 基本功能**

数据准备

在配置 EFM OAM 和接口联动前，需要准备以下数据。

序号	数据
1	接口的类型和编号
2	（可选）故障状态的保持时间

配置 EFM OAM 和接口联动

通过在物理端口上绑定 EFM OAM，实现当 EFM OAM 检测到故障后，OAM Manager 管理模块通知与其绑定的接口管理模块做故障处理。

背景信息

使能 EFM OAM 和接口联动功能后，当该接口收到携带链路故障状态标记的 OAM PDU 控制请求报文时，就调整其接口状态。

联动方式为：

- 错误事件和接口联动（阻塞端口）：指除了 EFM 协议报文外，其他流量全部中断，适用于存在主备链路的网络中，链路故障恢复后，系统可自动回切的场景。
- 错误事件和接口联动（Shutdown 端口）:指中断全部流量，适用于存在主备链路的网络中，链路故障恢复后，用户需检查确认无误再手动回切的场景。

在链路一端或两端设备上进行以下配置。

操作步骤

- 错误事件和接口联动：阻塞端口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入链路一端接口的接口视图。
  3. 执行命令 **efm trigger if-down**，配置 EFM OAM 和接口联动。

     缺省情况下，接口不和 EFM OAM 联动。

     当前接口必须已使用 **efm enable** 命令使能了 EFM OAM。

     如果使能了 EFM OAM 和当前接口联动功能，当 EFM OAM 检测到链路连通性故障后，接口下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢

版权所有 © 华为技术有限公司

复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

此外，请务必确保两端 EFM OAM 协议状态变为 detect 之后再配置 EFM OAM 和当前接口联动功能。

如果由于人为误操作导致二三层业务被阻塞，可通过在接口视图下执行命令 **undo efm trigger if-down** 恢复业务。

- 错误事件和接口联动：Shutdown 端口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入链路一端接口的接口视图。
  3. 执行命令 **efm** { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**，配置错误事件和接口联动功能。

     缺省情况下，错误事件和当前接口不联动。

     执行 **efm trigger error-down** 命令使能错误事件和当前接口联动功能时，当 EFM OAM 检测到故障事件 **critical-event**、**dying-gasp**、**link-fault** 或 **timeout** 后，相应接口的协议状态变为 Down，接口上的所有业务将全部被中断。即使当前接口通过 EFM OAM 检测到链路连通性故障恢复，相应接口的协议状态也不会改变，需要用户手工检测链路质量再决定是否回切。

----结束

（可选）配置故障状态保持时间

通过在物理端口上配置 EFM OAM 的故障状态的保持时间，避免由于链路不稳定而导致接口频繁 Up/Down 震荡。

背景信息

在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路一端接口的接口视图。

步骤 3 执行命令 **efm holdup-timer** *time*，配置故障状态的保持时间。

缺省情况下，当前接口的故障状态保持时间是 0 秒。

使用 **efm trigger if-down** 命令配置 EFM OAM 和当前接口联动功能后，如果 EFM OAM 检测到连通性故障后，则在用户设置的保持时间内，接口的 EFM OAM 故障状态保持不变。在保持时间超时后，EFM OAM 才开始检测连通性故障是否恢复。

----结束

检查配置结果

通过查看 TriggerIfDown 等内容，来检查配置是否成功。

版权所有 © 华为技术有限公司

前提条件

已经完成 EFM OAM 和接口联动功能的所有配置。

操作步骤

步骤 1 使用 **display efm** { **all** | **interface** *interface-type interface-number* }命令查看接口的 EFM OAM 配置信息。

----结束

任务示例

如果接口和 EFM OAM 联动功能配置成功，执行 **display efm** 命令，可以看到 TriggerIfDown 项目的值为 enable。

```
<Quidway> display efm interface gigabitethernet 0/0/1
  Item                           Value
  ------------------------------------------------------
  Interface:                     GigabitEthernet0/0/1
  EFM Enable Flag:               enable
  Mode:                          active

  OAMPDU MaxSize:                128
  ErrCodeNotification:           disable
  ErrCodePeriod:                 1
  ErrCodeThreshold:              1
  ErrFrameNotification:          disable
  ErrFramePeriod:                1
  ErrFrameThreshold:             1
  ErrFrameSecondNotification:    disable
  ErrFrameSecondPeriod:          60
  ErrFrameSecondThreshold:       1
  Hold Up Time:                  0
  ThresholdEvtTriggerErrDown:    enable
  TriggerIfDown:                 enable
  TriggerMacRenew:               disable
  Remote MAC:                    0018-8200-0001
  Remote EFM Enable Flag:        enable
  Remote Mode:                   passive
  Remote MaxSize:                128

  Remote State:                  --
```

9.4.7 配置 EFM OAM 与接口联动（触发与 EFM OAM 联动的接口物理状态变为 Down）

当设备在 OAM 管理视图下配置了 EFM OAM 和接口联动功能，EFM OAM 检测到故障时，本端设备上的 EFM OAM 通知 OAM 管理模块，触发绑定 EFM OAM 的接口物理状态变为 Down。反之，当接口的物理状态变为 Down 时，OAM 管理模块通知 EFM OAM 发生故障，通过以 EFM OAM 协议报文会将故障消息传递到远端设备。

建立配置任务

配置 EFM OAM 与接口联动功能之前，设备必须先全局使能 EFM OAM 功能，然后在 EFM 协议的出接口的接口视图下使能 EFM 功能。

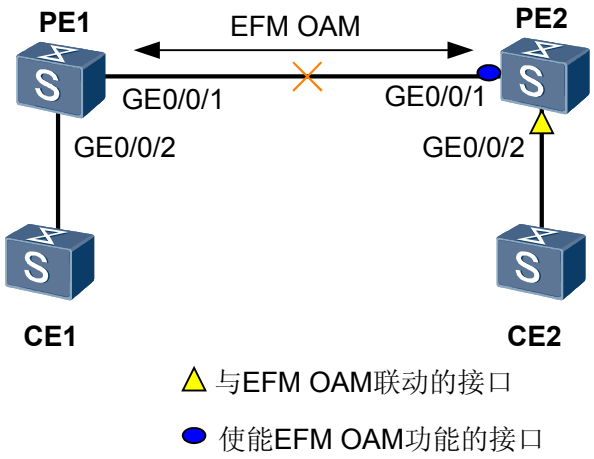
应用环境

如图 9-23 所示，PE1、PE2 都使能了 EFM OAM 功能。当 PE 之间的链路出现故障时，CE 需要感知故障，以确保业务可靠传输。此时，可在 PE 上部署 EFM OAM 与接口联

版权所有 © 华为技术有限公司

动功能。以 PE2 设备为例，当 EFM OAM 检测到链路故障时，PE2 设备上的 EFM OAM 将故障消息通知OAM 管理模块。触发绑定 EFM OAM 的接口 GE0/0/2 的物理状态变为 Down，从而使 CE2 感知故障，实现业务可靠传输。

图 9-23 EFM OAM 与接口联动示意图



如果 PE 上配置的是 EFM OAM 与接口双向联动功能，当 PE2 与 CE2 相连的接口 GE0/0/2 状态变为 Down 时，OAM 管理模块将故障消息传递给与接口绑定的 EFM OAM。故障消息通过 EFM OAM 协议报文传递到 PE1 设备上，PE1 上的 OAM 管理模块收到故障消息后触发接口 GE0/0/2 的物理状态变为 Down，从而实现 CE1 感知到故障，实现业务可靠传输。

前置任务

在配置 EFM OAM 与接口联动（OAM 管理视图）之前，需完成以下任务：

- **9.4.3 配置 EFM OAM 基本功能**

数据准备

在配置 EFM OAM 与接口联动（OAM 管理视图）之前，需要准备以下数据。

序号	数据
1	与 EFM OAM 联动的接口类型和编号
2	使能 EFM OAM 功能的接口类型和编号

配置 EFM OAM 与接口联动功能

EFM OAM 与接口之间的绑定关系是一对一的。当接口与 EFM OAM 绑定以后，接口不能再与其他 EFM OAM 绑定。反之，EFM OAM 与指定接口绑定后，该 EFM OAM 也不能再与其他接口绑定。

版权所有 © 华为技术有限公司

背景信息

在 EFM OAM 与接口联动功能配置过程中，步骤 3、步骤 4 和步骤 5 是并列关系，用户根据需要选择配置即可。

选择步骤 5 等于同时选择步骤 3 和步骤 4。

在需要配置 EFM OAM 与接口联动功能的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **oam-mgr**，进入 oam-mgr 视图。

步骤 3 执行命令 **oam-bind ingress efm interface** *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*，配置 EFM OAM 向接口传递故障消息功能。

当 EFM OAM 检测到故障后，与 EFM OAM 绑定的接口物理状态变为 Down。

interface *interface-type1 interface-number1*：使能 EFM OAM 功能的接口。

interface *interface-type2 interface-number2*：与 EFM OAM 绑定的接口。

步骤 4 执行命令 **oam-bind ingress interface** *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**，配置接口向 EFM OAM 传递故障消息功能。

当绑定 EFM OAM 的接口状态变为 Down 时，OAM 管理模块将故障消息传递到与其绑定的 EFM OAM，再通过 EFM OAM 协议报文将故障消息传递到远端设备。

interface *interface-type1 interface-number1*：与 EFM OAM 绑定的接口。

interface *interface-type2 interface-number2*：使能 EFM OAM 功能的接口。

步骤 5 执行命令 **oam-bind efm interface** *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*，配置 EFM OAM 与接口之间双向故障消息传递功能。

interface *interface-type1 interface-number1*：使能 EFM OAM 功能的接口。

interface *interface-type2 interface-number2*：与 EFM OAM 绑定的接口。

说明

若选择执行步骤 5，配置文件中将显示 **oam-bind ingress efm interface** *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2* 和 **oam-bind ingress interface** *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down** 两条命令，故障传递的方向相反。

----结束

检查配置结果

EFM OAM 与接口联动配置成功后，您可以在 OAM 管理视图下查看到相关联动配置信息。

版权所有 © 华为技术有限公司

前提条件

已经完成 EFM OAM 与接口联动的所有配置。

操作步骤

步骤 1 在 OAM 管理视图下使用 **display this** 命令，查看是否成功配置了 EFM OAM 与接口绑定。

----结束

任务示例

执行命令 **display this**，查看 EFM OAM 与接口绑定信息。

```
[Quidway-oam-mgr] display this
#
oam-mgr
 oam-bind ingress interface GigabitEthernet0/0/1 egress efm interface GigabitEthernet0/0/2 trigger
if-down
 oam-bind ingress efm interface GigabitEthernet0/0/2 trigger if-down egress interface
GigabitEthernet0/0/1
#
return
```

9.4.8 配置 EFM OAM 和 EFM OAM 联动

EFM OAM 与 EFM OAM 联动应用于设备两侧都配置 EFM OAM 检测场景。当一侧的 EFM OAM 检测到链路故障时，本端设备的 EFM OAM 通知 OAM 管理模块，OAM 管理模块查找到对应的出接口，将故障消息通知给另一侧的 EFM OAM，EFM OAM 会将故障消息传递到另一端设备上，从而实现故障消息传递。

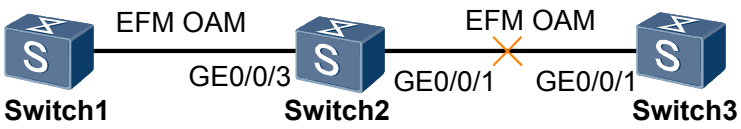
建立配置任务

配置 EFM OAM 与 EFM OAM 联动之前，指定的接口必须已经使能 EFM OAM 功能。

应用环境

EFM OAM 主要用于直连链路的检测。如图 9-24 所示，在 Switch1 和 Switch2、Switch2 和 Switch3 之间分别配置 EFM OAM。当 Switch2 和 Switch3 之间出现链路故障时，Switch1 需要感知故障，从而保证业务可靠传输。此时，可部署 EFM OAM 之间的联动功能。当 Switch2 和 Switch3 之间的 EFM OAM 检测到链路故障时，Switch2 上的 EFM OAM 将故障消息通知 OAM 管理模块，OAM 管理模块查找到对应的出接口 GE0/0/3，将故障消息通知给另一侧的 EFM OAM，EFM OAM 将故障消息传递到 Switch1，从而实现 EFM OAM 之间故障消息传递，保证了业务可靠传递。

图 9-24 ETH OAM 联动示意图



版权所有 © 华为技术有限公司

前置任务

在 EFM OAM 与 EFM OAM 联动之前，需完成以下任务：

- **9.4.3 配置 EFM OAM 基本功能**

数据准备

在 EFM OAM 与 EFM OAM 联动功能之前，需要准备以下数据。

序号	数据
1	联动的接口和编号

配置 EFM OAM 和 EFM OAM 联动

EFM OAM 与 EFM OAM 之间的绑定关系是一对一的。EFM OAM 与指定 EFM OAM 绑定以后，该 EFM OAM 不能再与其他 EFM OAM 绑定。

背景信息

在 EFM OAM 和 EFM OAM 联动功能配置过程中，步骤 3 和步骤 4 是并列关系，用户根据需要选择配置即可。

在需要配置 EFM OAM 和 EFM OAM 联动的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **oam-mgr**，进入 oam-mgr 视图。

步骤 3 执行命令 **oam-bind ingress efm interface** *interface-type interface-number* **egress efm interface** *interface-type interface-number* ，配置 EFM OAM 向另一个 EFM OAM 单向故障消息传递功能。

步骤 4 执行命令 **oam-bind efm interface** *interface-type interface-number* **efm interface** *interface-type interface-number*，配置 EFM OAM 与 EFM OAM 之间双向故障消息传递功能。

说明

若选择执行步骤 4，配置文件中将显示两条 **oam-bind ingress efm interface** *interface-type interface-number* **egress efm interface** *interface-type interface-number* 命令，故障传递的方向相反。

----结束

检查配置结果

EFM OAM 和 EFM OAM 联动配置成功后，您可以在 OAM 管理视图下查看到相关联动配置信息。

前提条件

已经完成 EFM OAM 和 EFM OAM 的联动配置。

版权所有 © 华为技术有限公司

操作步骤

- 在 OAM 管理视图下使用 **display this** 命令，查看是否配置了 EFM OAM 与 EFM OAM 的联动功能。

```
[Quidway-oam-mgr] display this
#
oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress efm interface
GigabitEthernet0/0/2
 oam-bind ingress efm interface GigabitEthernet0/0/2 egress efm interfaceGigabitEthernet0/0/1
#
return
```

----结束

9.4.9 配置以太网 CFM 基本功能

通过配置以太网 CFM 基本功能，实现端到端的连通性故障检测、故障通告、故障判定和故障定位功能。

建立配置任务

在配置以太网 CFM 基本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要在以太网中实现以下功能，可执行本配置任务：

- 端到端的连通性自动检测功能；
- 直连链路的连通性自动检测功能。

如果需要在以太网中实现端到端的连通性自动检测功能，在执行本配置任务前需先进行以下规划工作：

- 根据网络设备所属的 ISP（Internet Service Provider）划分 MD，把由相同 ISP 管理的所有具备以太网 CFM 功能的设备划分在同一个 MD 内。

  每台设备上可配置一个默认 MD，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。
- 根据业务实例划分 MA。每个 MA 关联一个 VLAN。通常一个 VLAN 对应一个业务实例。通过划分 MA 可实现对传输某个业务实例的网络的连通性故障检测。
- 确定哪些设备的哪些接口位于 MA 的边缘位置，即需要在哪些设备的哪些接口上配置 MEP。

在直连链路上实现连通性自动检测功能时：

- 应将两端设备配置在同一个 MD 的同一个 MA 中；
- MA 可以关联 VLAN 也可以不关联 VLAN；
- MEP 应配置在直连链路两端的接口上。

前置任务

无

版权所有 © 华为技术有限公司

数据准备

在配置以太网 CFM 基本功能之前，需要准备以下数据。

序号	数据
1	MD 的名称和级别
2	（可选）默认 MD 的名称和级别
3	MA 的名称、MA 关联的 VLAN 的 ID
4	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
5	（可选）RMEP 的 ID、RMEP 所在设备的桥 MAC 地址
6	MIP 的生成规则
7	MA 内 MEP 发送或探测 CCM 消息的时间间隔
8	（可选）指定 VLAN ID

切换版本

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，设备可以在这 2 个版本之间进行切换。

背景信息

缺省情况下，设备启用的是 802.1ag 协议 draft7 草案版本。如果需要使用 standard2007 标准版本，在所有需要切换版本的 AC6605 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm version** { **draft7** | **standard** }，切换版本。

说明

整网中的设备使用的版本必须一致，要么都是 draft7 草案版本要么都是 standard2007 标准版本，两个版本不能混用。

----结束

全局使能以太网 CFM 功能

全局使能以太网 CFM 功能是配置和使用所有 CFM 功能的前提条件。

背景信息

在所有需要实施以太网 CFM 管理的 AC6605 设备上进行以下配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm enable**，全局使能以太网 CFM 功能。

缺省情况下，AC6605 设备的 CFM 功能处于全局禁止状态。

----结束

创建 MD

MD 是指对其实施以太网 CFM 管理的一个网络或一个网络的一部分，一个 MD 由一个统一的 ISP 进行管理。

背景信息

在所有需要实施以太网 CFM 管理的 AC6605 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name* [**format** { **no-md-name** | **dnsname-and-mdname** | **mac-address** | **md-name** }] [**level** *level*]，创建 MD 并进入 MD 视图。

缺省情况下，MD 的级别是 0，即最低级别。

参数 **format**、**no-md-name**、**dnsname-and-mdname** 和 **mac-address** 仅在 802.1ag 标准版本中支持。

如果需要创建多个 MD，请重复执行步骤 2。一台设备最多可创建 16 个 MD。

说明

低级别 MD 的 802.1ag 协议报文进入高级别的 MD 或级别相同的后被丢弃，高级别 MD 的 802.1ag 协议报文可以穿越低级别的 MD。

----结束

（可选）创建默认 MD

默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，

背景信息

在所有需要实施以太网 CFM 管理的 AC6605 设备上进行以下配置。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，本命令只支持 standard2007 标准版本使用。所以必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本，才能使用此命令。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm default md** [**level** *level*]，创建默认 MD 并进入默认 MD 视图。

缺省情况下，默认 MD 的级别是 7，即最高级别。

每台设备上只能创建一个默认 MD。

说明

默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。

----结束

创建 MA

一个 MD 可以划分成一个或多个 MA。以太网 CFM 对每个 MA 分别进行连通性故障检测。

背景信息

在所有需要实施以太网 CFM 管理的 AC6605 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name* ，创建 MA 并进入 MA 视图。

AC6605 的同一个 MD 内，最多可创建 256 个 MA。一台 AC6605 设备上，最多可创建 256 个 MA。

一个或多个 MA 可对应一个 VLAN。

步骤 4 执行命令 **map vlan** *vlan-id*，配置 MA 关联 VLAN。

缺省情况下，MA 未和任何 VLAN 建立关联关系。

以太网 CFM 对每个 MA 分别进行连通性故障检测。配置某个 MA 和 1 个 VLAN 关联，可实现对该 VLAN 内的网络的连通性故障检测。

本步骤可选。如果某 MA 用于两个直连设备之间的连通性故障检测，则该 MA 可以不关联 VLAN，否则该 MA 应关联 VLAN。

----结束

后续处理

如需：

- 在同 1 个 MD 内创建多个 MA，请重复执行以上步骤 3 ～步骤 4。
- 在多个 MD 内创建 MA，请重复执行以上步骤 2 ～步骤 4。

版权所有 © 华为技术有限公司

创建 MEP

MEP 是 MA 的的边缘节点，它位于设备的接口上，需要手工创建。

背景信息

在 MA 内创建 MEP 时，对该 MA 是否关联 VLAN 和 MEP 所在接口的配置要求如下：

- 在创建 inward 型的 MEP 时，要求该 MA 必须已经关联了 VLAN，且指定的 MEP 所在接口必须已经加入该 VLAN。inward 型 MEP 发出的 802.1ag 协议报文通过当前 MA 关联 VLAN 内的所有接口（除 MEP 所在接口）向外发送，即在当前 MA 关联的 VLAN 内广播。
- outward 型 MEP 发出的协议报文直接通过该 MEP 所在的接口向外发送。

在同一台设备的同一个 MA 内，对创建 MEP 的数量和类型要求如下：

- inward 接口型 MEP 和 outward 接口型 MEP 不能同时存在。
- 只能创建 1 个 outward 接口型 MEP，可以创建多个 inward 接口型 MEP，但是同一个接口上只能创建 1 个 inward 接口型 MEP。

在所有 MA 的所有边缘设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** }，创建接口型 MEP。

----结束

后续处理

如需：

- 在同 1 个 MA 内创建多个 MEP，请重复执行步骤 4。
- 在多个 MA 内创建 MEP，请重复执行步骤 3 ～步骤 4。
- 在多个 MD 内创建 MEP，请重复执行步骤 2 ～步骤 4。

配置 RMEP

同一个 MA 内，其它设备上的 MEP 对本设备而言称为 RMEP。通过配置 RMEP，在同一个 MA 内实现和某个 RMEP 的连通性故障检测。

背景信息

如果需要检测本设备到某 RMEP 的连通性，则首先需要在本设备上配置该 RMEP。

在所有 MA 的所有边缘设备上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **remote-mep mep-id** *mep-id* [**mac** *mac-address*]，配置当前 MA 内的 RMEP。

----结束

后续处理

如需：

- 在同 1 个 MA 内配置多个 RMEP，请重复执行步骤 4。
- 在多个 MA 内配置 RMEP，请重复执行步骤 2 ～步骤 4。
- 在多个 MD 内配置 RMEP，请重复执行步骤 3 ～步骤 4。

（可选）配置 MIP 生成规则

背景信息

在所有需要实施以太网 CFM 管理的 AC6605 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 配置 MIP 生成规则

以下两个版本 MIP 配置规则，任选其一，不可以同时配置。

- 配置 draft7 草案中的 MIP 生成规则。

  执行命令 **mip create-type** { **default** | **explicit** | **none** } [**interface** *interface-type interface-number*]，配置 draft7 草案中 MIP 生成规则。

- 配置 standard2007 标准版本中的 MIP 生成规则。

  1. 执行命令 **cfm md** *md-name* [**format** { **no-md-name** | **dnsname-and-mdname** | **mac-address** | **md-name** }] [**level** *level*]，进入 MD 视图。

     或者，执行命令 **cfm default md** [**level** *level*]，进入默认 MD 视图。

  2. 执行命令 **mip create-type** { **default** | **explicit** | **none** }，配置 standard2007 标准版本中 MIP 生成规则。

缺省情况下，MIP 生成规则为 **none**。如果为：

- default：如果在指定 MD 或默认 MD 所属端口没有更高级别的 MEP，并且没有更低级别的 MIP，则可以在指定端口创建 MIP 节点。
- explicit：如果在指定 MD 或默认 MD 所属端口没有更低级的 MEP 节点，则不能创建 MIP；如果指定 MD 或默认 MD 所属端口没有更高级别的 MEP，并且没有更低级别的 MIP，则可以创建 MIP 节点。
- none：在指定 MD 或默认 MD 所属端口上不能创建 MIP 节点。

版权所有 © 华为技术有限公司

配置了 MIP 的生成规则为 default 类型或 explicit 类型后，设备会根据规则自动创建 MIP。

MIP 的级别由生成规则以及生成其的 MD 的级别决定。

----结束

配置 CC 检测

通过配置 CC 检测，实现以太网 CFM 通过 MEP 之间定期发送 CCM 来检测各 MEP 之间的连通性。

背景信息

在所有 MA 的所有边缘设备（即 MEP 所在设备）上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **ccm-interval** *interval*，配置本设备上当前 MA 内 MEP 发送或探测 CCM 消息的时间间隔。

缺省情况下，MA 内 MEP 发送或探测 CCM 消息的时间间隔是 1 秒。

如果某 MA 内：

- 已使用 **mep ccm-send enable** 命令使能了 CCM 消息发送功能
- 或已使用 **remote-mep ccm-receive enable** 命令使能了 CCM 消息接收功能

则不允许修改该 MA 内发送或探测 CCM 消息的时间间隔。如要修改，需先使用对应的 **undo** 命令禁止以上功能。

步骤 5 执行命令 **mep ccm-send** [**mep-id** *mep-id*] **enable**，使能 MEP 的 CCM 消息发送功能。

缺省情况下，MEP 的 CCM 消息发送功能处于禁止状态。

如果不指定 **mep-id** *mep-id* 参数，则表示使能本设备上当前 MA 内所有 MEP 的 CCM 消息发送功能。

步骤 6 执行命令 **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

缺省情况下，本地 MEP 不接收 RMEP 发送的 CCM 消息。

当在本端设备上使能了接收某个 RMEP 发送的 CCM 消息后，如果通过 CC 探测发现本端与该 RMEP 之间出现连通性故障，则本端设备上提示 RMEP 连通性告警。

如果不指定 **mep-id** *mep-id* 参数，则表示使能本设备当前 MA 内接收所有 RMEP 发送的 CCM 消息功能。

----结束

版权所有 © 华为技术有限公司

后续处理

如需：

- 在多个 MA 内配置 CC 检测，请重复执行步骤 3 ～步骤 6。
- 在多个 MD 内配置 CC 检测，请重复执行步骤 2 ～步骤 6。

（可选）创建指定 VLAN

通过将 VLAN 和默认 MD 相关联，指定 VLAN 内的所有接口将按照默认 MD 配置的 MIP 生成规则生成 MIP 节点。

背景信息

请在需要配置指定 VLAN 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm default md** [**level** *level*]，创建默认 MD 并进入默认 MD 视图。

步骤 3 执行命令 **vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，创建指定 VLAN。

----结束

检查配置结果

前提条件

已经完成以太网 CFM 基本功能的所有配置。

操作步骤

- 使用命令 **display cfm md** [*md-name*]查看 MD 的配置信息命令。
- 使用命令 **display cfm ma** [**md** *md-name* [**ma** *ma-name*]]查看 MA 的详细信息。
- 使用命令 **display cfm mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]查看 MEP 的详细信息。
- 使用命令 **display cfm remote-mep md** *md-name* **ma** *ma-name* [**mep-id** *mep-id*]或 **display cfm remote-mep** [**md** *md-name* [**ma** *ma-name*]] [**cfm-state** { **up** | **down** | **disable** }]查看 RMEP 的详细信息。
- 使用命令 **display mip create-type** [**interface** *interface-type interface-number*]查看 MIP 的创建规则。
- 使用命令 **display cfm mip** [**interface** *interface-type interface-number* | **level** *level*]查看 MIP 的信息。

----结束

任务示例

在 draft7 版本中，如果 MD 创建成功，执行命令 **display cfm md**，可以看到该 MD 和该 MD 的级别。

版权所有 © 华为技术有限公司

```
<Quidway> display cfm md
The total number of MDs is : 1
MD-Name                                         Level
--------------------------------------------------
md1                                             0
```

在 standard2007 标准版本中，如果 MD 创建成功，执行命令 **display cfm md**，可以看到该 MD 和该 MD 的级别。

```
<Quidway> display cfm md md1
 MD Name            : md1
 MD Name Format     : md-name
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA list            :
         MA Name            : ma1
         Interval           : 1000
         Vlan ID            : 10
         VSI Name           : --
         MA Name            : ma
         Interval           : 1000
         Vlan ID            : --
         VSI Name           : --
```

在 draft7 版本中，如果 MA 创建成功，执行命令 **display cfm ma**，可以看到该 MA 的信息。

```
<Quidway> display cfm ma
The total number of MAs is : 1
--------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 Interval           : 1000
 Priority           : 6
 Vlan ID            : --
 VSI Name           : --
 MEP Number         : 0
 RMEP Number        : 0
```

在 draft7 版本中，如果 MEP 创建成功，执行命令 **display cfm mep**，可以看到该 MEP 的信息。

```
<Quidway> display cfm mep
The total number of MEPs is : 2
--------------------------------------------------
 MD Name            : md2
 Level              : 7
 MA Name            : ma3
 MEP ID             : 40
 Vlan ID            : 10
 VSI Name           : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
```

在 standard2007 标准版本中，查看 md1 内 ma1 中 ID 为 10 的 MEP 的信息。

```
<Quidway> display cfm mep md md1 ma ma1 mep-id 10
 MD Name            : md1
 MD Name Format     : md-name
 Level              : 0
 MA Name            : ma1
 MEP ID             : 11
 Vlan ID            : 221
 VSI Name           : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : disabled
```


版权所有 © 华为技术有限公司

```
 Direction          : inward
 MAC Address        : 0018-2000-0083
```

如果 RMEP 配置成功，执行命令 **display cfm remote-mep**，可以看到该 RMEP 的信息。

```
<Quidway> display cfm remote-mep
The total number of RMEPs is 2
The status of RMEPS : 2 up, 0 down, 0 disable
--------------------------------------------------
 MD Name              : md2
 Level                : 7
 MA Name              : ma3
 RMEP ID              : 110
 Vlan ID              : 20
 VSI Name             : --
 MAC                  : 0000-0121-0222
 CCM Receive          : enabled
 Trigger-If-Down      : disabled
 CFM Status           : up
 Alarm Status         : None

 MD Name              : md2
 Level                : 4
 MA Name              : ma3
 RMEP ID              : 30
 Vlan ID              : --
 VSI Name             : --
 MAC                  : --
 CCM Receive          : enabled
 Trigger-If-Down      : disabled
 CFM Status           : up
 Alarm Status         : None
```

在 draft7 版本中，执行命令 **display mip create-type**，可查看 MIP 的创建规则，验证 MIP 创建规则配置是否正确。

```
<Quidway> display mip create-type interface gigabitethernet0/0/1
Interface Name               MIP Create-Type  MIP Create-Type On Interface
------------------------------------------------------------------------------
GigabitEthernet0/0/1        none             --
```

执行命令 **display cfm mip**，可查看 MIP 的信息。

```
<Quidway> display cfm mip
Interface Name               Level
----------------------------------
GigabitEthernet0/0/1         0
```

9.4.10 配置以太网 CFM 的相关参数

通过对以太网 CFM 的相关参数进行调整，在以太网中更好的实现端到端的连通性故障检测。

建立配置任务

在配置以太网 CFM 相关参数之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果在以太网中已经启动故障连通性检测功能，可以对相关检测参数进行调整。根据应用环境的不同，可以选择以下参数进行调整：

- RMEP 激活时间

版权所有 © 华为技术有限公司

当在本端设备上使能接收某个 RMEP 发送的 CCM 消息功能后，

- 如果通过 CC 探测发现本端 MEP 与该 RMEP 之间出现连通性故障，则本端设备上提示 RMEP 连通性告警。
- 如果本端 MEP 与 RMEP 之间物理连通正常，但是由于对端设备没有及时配置 MEP 或者 MEP 配置延后，此时进行 CC 探测，若本端 MEP 连续 3 个 CCM 发送周期没有接收到远端 MEP 发送的 CCM 消息，则认为和远端 MEP 之间发生了连通性故障，在本端设备上提示 RMEP 连通性告警。

  可以看出，此告警为误告警。为了解决这个问题，提出了 RMEP 激活时间这个概念。

若设备配置了 RMEP 激活时间，当在本端设备上使能接收某个 RMEP 发送的 CCM 消息功能后，等待配置的 RMEP 激活时间到达后，本端设备开始接收 CCM 报文。也就是说 RMEP 激活时间是预留给用户对远端 MEP 配置的时间。

如果配置的 RMEP 激活时间到达后，本端设备上的 MEP 连续 3 个 CCM 周期内没有收到 CCM 报文，则认为 MEP 之间发生了连通性故障，本端设备上才提示 RMEP 连通性告警。

- 告警产生和恢复的防抖时间

  对于每个 MA 下的所有 RMEP 有两个定时器，分别是：

  - 一个是告警产生定时器，周期是用户配置的告警产生防抖时间；
  - 另一个是告警恢复定时器，周期是用户配置的告警恢复防抖时间。

  当 RMEP 检测到告警时，告警定时器开始启动，等到定时器的时间到，上报告警；当每 RMEP 检测到告警恢复时，告警恢复定时器开始启动，等到定时器时间到，上报告警恢复。

  如果 RMEP 频繁的检测到告警和告警恢复信号，那么就会产生告警振荡。

  通过配置告警产生和恢复的防抖时间可以抑制告警振荡。

- 指定 VLAN 或 VLAN 链表

  指定 VLAN 内的所有接口将按照默认 MD 配置的 MIP 生成规则生成 MIP 节点。

前置任务

无

数据准备

在配置以太网 CFM 检测参数之前，需要准备以下数据。

序号	数据
1	（可选）RMEP 激活时间
2	（可选）告警恢复的防抖时间
3	（可选）告警产生的防抖时间

（可选）配置 RMEP 激活时间

RMEP 激活时间是预留给用户对远端 MEP 配置的时间。通过配置 RMEP 的激活时间，实现在配置的 RMEP 激活时间到达后，本端设备开始接收 CCM 报文。

版权所有 © 华为技术有限公司

背景信息

在所有 MA 的所有边缘设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **active time** *time*，配置 RMEP 激活时间。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，本命令只支持 standard2007 标准版本使用。所以必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本，才能使用此命令。

----结束

（可选）配置告警恢复防抖时间

通过配置告警恢复防抖时间可以抑制告警振荡。

背景信息

请在需要配置告警恢复防抖时间的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **alarm finish time** *time*，配置告警恢复防抖时间。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，本命令只支持 standard2007 标准版本使用。所以必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本，才能使用此命令。

----结束

（可选）配置告警产生防抖时间

通过配置告警产生防抖时间可以抑制告警振荡。

背景信息

请在需要配置告警产生的防抖时间的设备上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **alarm occur time** *time*，配置告警产生的防抖时间。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，本命令只支持 standard2007 标准版本使用。所以必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本，才能使用此命令。

----结束

9.4.11 配置以太网的故障确认

通过发送测试报文和接收应答报文来检测两台设备之间链路的连通性。

建立配置任务

应用场景

当需要手动检测两台设备之间链路的连通性时，可通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。根据被测链路的类型，可分为以下两种场景：

- 当需要在配置了 MD、MA、MEP 的网络中，检测同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性时，可执行 802.1ag MAC Ping。
- 当需要在未配置 MD、MA、MEP 的网络中，检测两台设备之间的连通性时，可执行通用 Gmac ping。

前置任务

在执行 802.1ag MAC Ping 之前，需完成以下任务：

- **配置以太网 CFM 基本功能**

数据准备

在手动检测以太网的连通性前，需要准备以下数据。

序号	数据
1	（可选）目的 MEP 的 MAC 地址或 ID
2	（可选）目的 MIP 的 MAC 地址
3	（可选）发送 MAC Ping 报文的个数、大小、超时时间、出接口
4	（可选）目的节点所属 VLAN

华为专有和保密信息
版权所有 © 华为技术有限公司

（可选）执行 802.1ag MAC Ping

通过执行 802.1ag MAC Ping，检测同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性。

背景信息

802.1ag MAC Ping 与 Ping 类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。同时还可以在发送端计算 Ping 操作的时间，以分析网络性能。

操作步骤

步骤 1 通常设备上会配置多个 MD 和 MA，为了精确检测两台或多台设备间的连通性，请在被测链路的任意一端 AC6605 设备上采用如下两种方式中的一种进行配置。

- MA 视图：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cfm md** *md-name*，进入 MD 视图。
  3. 执行命令 **ma** *ma-name*，进入 MA 视图。
  4. 执行命令 **ping mac-8021ag** { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**md** *md-name* **ma** *ma-name*] [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout*] *，检测和指定 RMEP 或 MIP 之间的连通性。
  - 不指定参数 **md** *md-name* **ma** *ma-name*，检测该 MA 内链路的连通性。
  - 指定参数 **md** *md-name* **ma** *ma-name*，根据指定 MD 和 MA 的名称来确定需要检测的链路。
- 除 MA 视图任意视图：

  执行命令 **ping mac-8021ag** { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } **md** *md-name* **ma** *ma-name* [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout*] *，检测和指定 RMEP 或 MIP 之间的连通性。

进行 802.1ag MAC Ping 操作时：

- 当前 MA 必须已关联了 VLAN。
- 当前 MA 必须已配置了 MEP。
- 如果指定出接口，则该接口不能是配置了 inward 型 MEP 的接口。该接口必须加入指定 VLAN 并关联了相应的 MA。
- 如果目的节点是 RMEP，可选用参数 **mac** *mac-address*，也可选用参数 **remote-mep mep-id** *mep-id*。如果选用参数 **remote-mep mep-id** *mep-id*，则该 RMEP 在当前设备上必须已使用 **remote-mep** 命令创建。
- 如果目的节点是 MIP，请选用参数 **mac** *mac-address*。

链路上的中间设备只是用来转发 LBM 和 LBR 报文，所以中间设备上均不需要配置 MD、MA 和 MEP。

----结束

（可选）执行通用 Gmac ping

通过执行通用 Gmac ping，检测两台设备之间的连通性。

版权所有 © 华为技术有限公司

背景信息

在被测链路的两端 AC6605 设备上执行步骤 1 ～步骤 2，在任意一端 AC6605 设备上执行步骤 3。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ping mac enable**，全局使能通用 Gmac ping 功能。

缺省情况下，通用 Gmac ping 功能处于禁止状态。

当通用 Gmac ping 功能处于使能状态时：

- 在 AC6605 设备上可以进行通用 Gmac ping 操作；
- AC6605 设备对接收到的通用 Gmac ping 报文进行回复。

步骤 3 执行命令 **ping mac** *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-c** *count* | **-s** *packetsize* | **-t** *timeout*] *，检测和对端设备之间的连通性。

通用 Gmac ping 不需要由 MEP 发起，目的节点也不需要是 MEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac ping。

两台设备上必须配置 802.1ag 协议的相同版本。如果本端设备上配置 Draft7 草案版本，对端设备上配置 standard2007 标准版本，此时用户使用 **ping mac** 命令检测这两台设备之间的连通性时，则本端设备无法 ping 通对端设备。

----结束

9.4.12 配置以太网的故障定位

通过发送测试报文和接收应答报文来定位两台设备之间链路的连通性故障。

建立配置任务

应用场景

当需要定位两台设备之间链路的连通性故障时，可通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。根据被检测链路的类型，分为以下两种场景：

- 当需要在配置了 MD、MA、MEP 的网络中，定位同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性故障时，可执行 802.1ag MAC Trace。
- 当需要在未配置 MD、MA、MEP 的网络中，定位两台设备之间的连通性故障时，可执行通用 Gmac trace。

前置任务

在执行 802.1ag MAC Trace 之前，需完成以下任务：

- **配置以太网 CFM 基本功能**

版权所有 © 华为技术有限公司

数据准备

在定位以太网的连通性故障前，需要准备以下数据。

序号	数据
1	（可选）目的 MEP 的 MAC 地址或 ID
2	（可选）目的 MIP 的 MAC 地址
3	（可选）发送 MAC Trace 报文出接口
4	（可选）等待应答报文的超时时间
5	（可选）最大跟踪跳数
6	（可选）目的节点所属 VLAN

（可选）执行 802.1ag MAC Trace

通过执行 802.1ag MAC Trace，定位同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性故障。

背景信息

802.1ag MAC Trace 与 Traceroute（或 Tracert）类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。

操作步骤

步骤 1 通常设备上会配置多个 MD 和 MA，为了精确判断一个 MA 内某个 MEP 到另一个 MEP 或 MIP 之间的实际转发路径或故障点，请在被测链路的任意一端 AC6605 设备上采用如下两种方式中的一种进行配置。

- MA 视图：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cfm md** *md-name*，进入 MD 视图。
  3. 执行命令 **ma** *ma-name*，进入 MA 视图。
  4. 执行命令 { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**md** *md-name* **ma** *ma-name*] [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *，定位和对端设备之间的连通性故障。

  - 不指定参数 **md** *md-name* **ma** *ma-name*，定位该 MA 内链路的实际转发路径和故障点。
  - 指定参数 **md** *md-name* **ma** *ma-name*，根据指定 MD 和 MA 的名称来确定 MA 内链路的实际转发路径和故障点。
- 除 MA 视图任意视图：

  执行命令 **trace mac-8021ag** { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } **md** *md-name* **ma** *ma-name* [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *，定位和对端设备之间的连通性故障。

进行 802.1ag MAC Trace 操作时：

版权所有 © 华为技术有限公司

- 当前 MA 必须已关联了 VLAN。
- 当前 MA 必须已配置了 MEP。
- 如果指定出接口，则该接口不能是配置了 inward 型 MEP 的接口。该接口必须加入 VLAN 并关联 MA。
- 如果目的节点是 RMEP，可选用参数 **mac** *mac-address*，也可选用参数 **remote-mep mep-id** *mep-id*。如果选用参数 **remote-mep mep-id** *mep-id*，则该 RMEP 在当前设备上必须已使用 **remote-mep** 命令创建。
- 如果目的节点是 MIP，请选用参数 **mac** *mac-address*。
- 如果 MAC 地址表中不存在目的节点对应的转发表项，则必须指定 **interface** *interface-type interface-number* 参数。

----结束

（可选）执行通用 Gmac trace

通过执行通用 Gmac ping，定位两台设备之间的连通性故障。

背景信息

在被测链路两端和中间 AC6605 设备上都需要进行配置。

操作步骤

步骤 1 配置两端和中间设备

在被测链路的两端和中间 AC6605 设备上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **trace mac enable**，全局使能通用 Gmac trace 功能。

   缺省情况下，通用 Gmac trace 功能处于禁止状态。

   只有当通用 Gmac trace 功能处于使能状态时：

   - 在 AC6605 设备上才能进行通用 Gmac trace 操作；
   - AC6605 设备才对接收到的通用 Gmac trace 报文进行回复。

步骤 2 执行 Gmac trace 探测

在被测链路的任意一端 AC6605 设备上执行 MAC Trace 探测。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **trace mac** *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-t** *timeout*] *，定位和对端设备之间的连通性故障。

   通用 Gmac trace 不需要由 MEP 发起，中间节点和目的节点也不需要是 MEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac trace，所有中间设备均回应 LTR 消息。

   两台设备上必须配置 802.1ag 协议的相同版本。如果本端设备上配置 Draft7 草案版本，对端设备上配置 standard2007 标准版本，此时用户使用 **trace mac** 命令定位这两台设备之间的连通性故障时，则无法定位成功。

----结束

版权所有 © 华为技术有限公司

9.4.13 配置以太网 CFM 和接口联动

以太网 CFM 与接口联动功能主要用于 LACP 静态链路聚合组或手工 1：1 主备模式链路聚合的活动链路快速故障检测和触发保护倒换。

建立配置任务

应用环境

当配置了以太网 CFM 和接口联动后，如果指定 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障，OAM 管理模块对该 MEP 所在接口进行闪断处理（即先关闭该接口，然后再打开该接口），以使其它模块感知到该故障。

图 9-25 以太网 CFM 和接口联动应用场景（一）

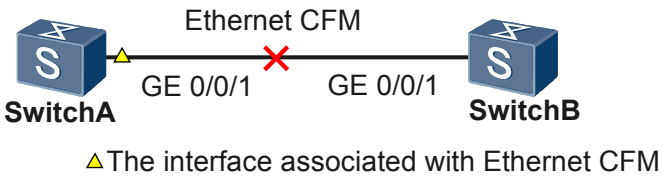


图 9-26 以太网 CFM 和接口联动应用场景（二）

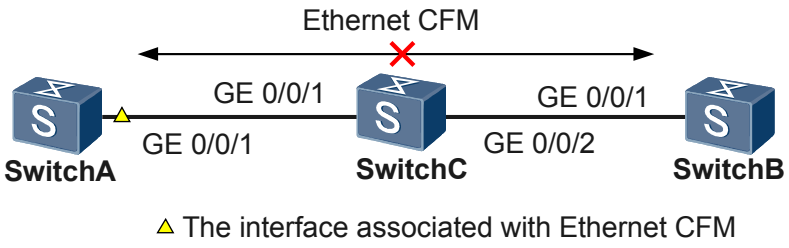
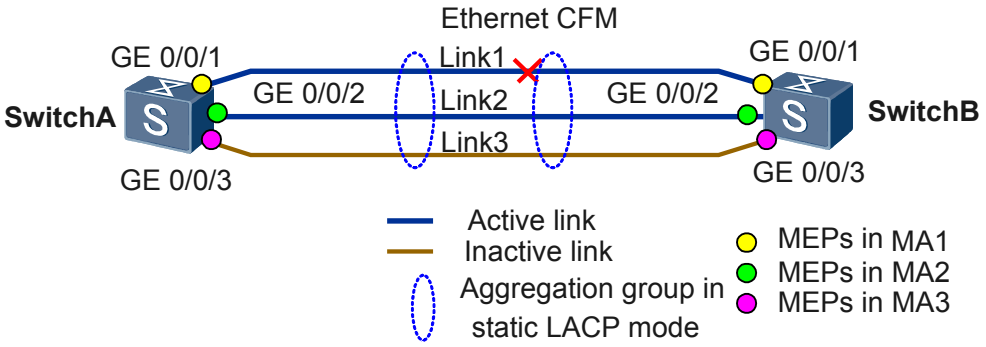


图 9-25 和图 9-26 中，CFM 分别用于直连链路和多跳链路检测。两台设备 SwitchA 和 SwitchB 之间配置了以太网 CFM 功能，并配置了 CFM 和 SwitchA 的接口 GE0/0/1 联动。在 SwitchA 上，当 CFM OAM 模块检测到和 SwitchB 之间有连通性故障时，OAM 管理模块对接口 GE0/0/1 进行闪断，即先关闭该接口再打开该接口，以使 SwitchA 的其它接口感知到此故障。

版权所有 © 华为技术有限公司

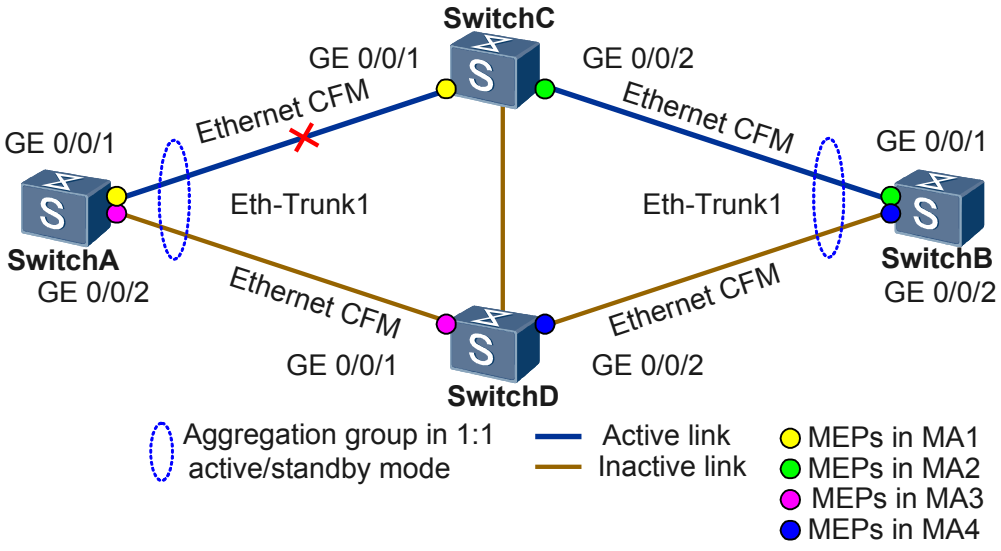
图 9-27 以太网 CFM 和接口联动应用场景（三）



SwitchA 和 SwitchB 配置了 LACP 静态链路聚合组。在 SwitchA 和 SwitchB 上配置以太网 CFM 功能：使 SwitchA 和 SwitchB 属于同一 MD；在链路聚合组的所有成员接口上配置 MEP，并使同一条链路两端接口上的 MEP 属于同一个 MA，不同链路两端接口上的 MEP 属于不同 MA。通过同一链路两端的 MEP 互发 CCM 消息检测链路的连通性。并配置以太网 CFM 和接口联动。

当 Link1 出现连通性故障时，SwitchA 和 SwitchB 的 OAM 管理模块分别对配置了以太网 CFM 功能，并配置了 CFM 和 SwitchA 的接口 GE0/0/1 接口进行闪断。于是，LACP 模块就可以感知到 Link1 出现故障，并将通过该链路转发的业务数据切换到非活动链路 Link3 上转发。在这种情况下，保护倒换时间可达到小于等于 50 毫秒，可满足电信级网络的要求。

图 9-28 以太网 CFM 和接口联动应用场景（四）



SwitchA 和 SwitchB 配置了手工 1：1 主备模式链路聚合组。在 SwitchA 和 SwitchC、SwitchA 和 SwitchD、SwitchB 和 SwitchC、SwitchB 和 SwitchD 之间分别配置以太网 CFM，并在 SwitchA 上配置以太网 CFM 和接口 GE0/0/1、GE0/0/2 联动，在 SwitchB 上配置以太网 CFM 和接口 GE0/0/1、GE0/0/2 联动。

版权所有 © 华为技术有限公司

当 SwitchA 和 SwitchC 之间的链路出现连通性故障时，以太网 CFM 模块检测到该故障并通知 OAM 管理模块。OAM 管理模块对 GE0/0/1 接口进行闪断，以使链路聚合组感知到该故障并将业务数据切换到非活动链路转发。其它链路的连通性故障的处理过程和以上SwitchA 和 SwitchC 之间的链路故障处理过程类似。在这种情况下，保护倒换时间可达到小于等于 50 毫秒，可满足电信级网络的要求。

前置任务

在配置以太网 CFM 和接口联动之前，需完成以下任务：

- 链路聚合配置
- 9.4.9 配置以太网 CFM 基本功能

数据准备

在配置以太网 CFM 和接口联动前，需要准备以下数据。

序号	数据
1	接口的类型和编号
2	MD 的名称、MA 的名称、RMEP 的 ID

配置以太网 CFM 和接口联动

可以配置以太网 CFM 和接口联动，实现指定 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障，OAM 管理模块对该 MEP 所在接口先关闭，然后在打开，以使其它模块感知到该故障。

背景信息

在配置了静态 LACP 聚合组的 AC6605 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入链路聚合组成员接口的接口视图。

步骤 3 执行命令 **cfm md** *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down**，配置以太网 CFM 和接口联动。

缺省情况下，接口不和以太网 CFM 联动。

使用 **cfm md** *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down** 命令配置以太网 CFM 和当前接口联动时，指定 MA 内必须已创建 outward 型的 MEP，且该 MEP 所在接口为当前接口。

每个接口仅支持和一个 RMEP 绑定，如果要改变接口和 MA 及 RMEP 的对应联动关系，需先删除原有的配置，再重新进行配置。

版权所有 © 华为技术有限公司

如果链路聚合组有多个成员接口，请重复执行步骤 2 ～步骤 3，配置以太网 CFM 和所有成员接口联动。

----结束

检查配置结果

通过查看 Trigger-If-down 字段等内容，来检查配置是否成功。

前提条件

已经完成以太网 CFM 和接口联动功能的所有配置。

操作步骤

步骤 1 使用 **display cfm remote-mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]命令查看 RMEP 的详细信息。

----结束

任务示例

如果以太网 CFM 和接口联动配置成功，执行 **display cfm remote-mep** 命令，可以看到对应 RMEP 的 Trigger If-down 字段显示为 enable。

```
<Quidway> display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPS : 0 up, 1 down, 0 disable
--------------------------------------------------
 MD Name            : md110
 Level              : 0
 MA Name            : ma110
 RMEP ID            : 2
 Vlan ID            : --
 VSI Name           : --
 L2VC ID            : 110 tagged
 MAC                : 0025-9eb1-bce6
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : RemoteAlarm
```

9.4.14 配置以太网 CFM 与接口联动（触发与以太网 CFM 联动的接口物理状态变为 Down）

当设备在 OAM 管理视图下配置了以太网 CFM 和接口联动功能，以太网 CFM 检测到故障时，本端设备上的以太网 CFM 通知 OAM 管理模块，触发绑定以太网 CFM 的接口物理状态变为 Down。反之，当接口的物理状态变为 Down 时，OAM 管理模块通知以太网 CFM 发生故障，通过以太网 CFM 协议报文会将故障消息传递到远端设备。

建立配置任务

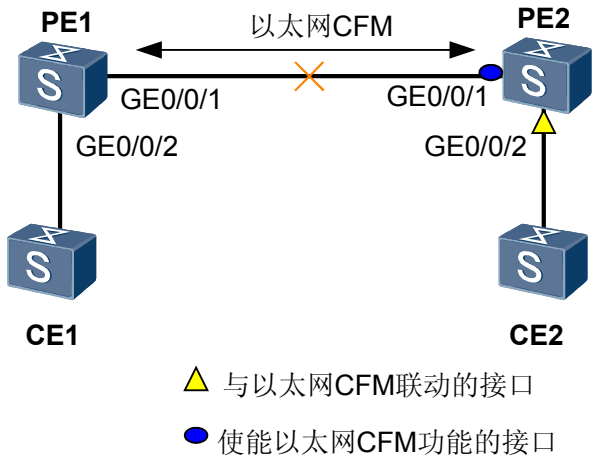
配置以太网 CFM 与接口联动功能之前，设备必须先全局使能以太网 CFM 功能，然后在 EFM 协议的出接口的接口视图下使能 EFM 功能。

版权所有 © 华为技术有限公司

应用环境

如图 9-29 所示，PE1、PE2 都使能了以太网 CFM 功能。当 PE 之间的链路出现故障时，CE 需要感知故障，以确保业务可靠传输。此时，可在 PE 上部署以太网 CFM 与接口联动功能。以 PE2 设备为例，当以太网 CFM 检测到链路故障时，PE2 设备上的以太网 CFM 将故障消息通知 OAM 管理模块。触发绑定以太网 CFM 的接口 GE1/0/2 的物理状态变为 Down，从而使 CE2 感知故障，实现业务可靠传输。

图 9-29 以太网 CFM 与接口联动示意图



如果 PE 上配置的是以太网 CFM 与接口双向联动功能，当 PE2 与 CE2 相连的接口 GE0/0/2 状态变为 Down 时，OAM 管理模块将故障消息传递给与接口绑定的以太网 CFM。故障消息通过以太网 CFM 协议报文传递到 PE1 设备上，PE1 上的 OAM 管理模块收到故障消息后触发接口 GE0/0/2 的物理状态变为 Down，从而实现 CE1 感知到故障，实现业务可靠传输。

前置任务

在配置以太网 CFM 与接口联动（OAM 管理视图）之前，需完成以下任务：

- **配置以太网 CFM 基本功能**

数据准备

在配置以太网 CFM 与接口联动（OAM 管理视图）之前，需要准备以下数据。

序号	数据
1	与以太网 CFM 联动的接口类型和编号
2	使能以太网 CFM 功能的接口类型和编号
3	MD 的名称和 MA 的名称

版权所有 © 华为技术有限公司

配置以太网 CFM 与接口联动功能

以太网 CFM 与接口之间的绑定关系是一对一的。当以太网 CFM 与接口绑定以后，该以太网 CFM 不能再与其他接口绑定。反之，该接口也不能再与其他以太网 CFM 绑定。

背景信息

在需要配置以太网 CFM 与接口联动功能的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **oam-mgr**，进入 oam-mgr 视图。

步骤 3 以太网 CFM 与接口之间的故障消息传递分为双向故障消息传递和单向故障消息传递两种场景。请根据具体的场景选择配置方案，选择原则如表 9-9 所示。

表 9-9 CFM 与接口联动功能说明

场景	配置方案 1	配置方案 2
部署以太网 CFM 与接口之间双向故障消息传递	请选择如下命令之一进行配置。2 条命令在功能和场景上没有任何区别，用户可以根据的配置习惯灵活地选择。 ● 如果习惯于先指定 MD 和 MA 后指定接口名称，那么请使用命令 oam-bind cfm md ma trigger if-down interface。 ● 如果习惯于先指定接口名称后指定 MD 和 MA，那么请使用命令 oam-bind interface cfm md ma trigger if-down。 **说明** 使用上述 2 条命令之一，部署完以太网 CFM 与接口之间双向故障消息传递功能后，再使用命令 display current-configuration 查看当前配置时，系统只会同时显示命令 oam-bind ingress cfm md ma egress interface 和 oam-bind ingress interface egress cfm md ma trigger if-down。而不会显示命令 oam-bind cfm md ma trigger if-down interface 或 oam-bind interface cfm md ma trigger if-down，故障传递的方向相反。	请同时使用下面 2 条命令进行配置。应用两个单向组合来实现双向的功能，2 条命令执行时没有先后顺序。 ● oam-bind ingress cfm md ma egress interface 当以太网 CFM 检测到故障后，与以太网 CFM 绑定的接口物理状态变为 Down。 ● oam-bind ingress interface egress cfm md ma trigger if-down 当绑定以太网 CFM 的接口状态变为 Down 时，OAM 管理模块将故障消息传递到与其绑定的以太网 CFM，再通过以太网 CFM 协议报文将故障消息传递到远端设备。

华为专有和保密信息
版权所有 © 华为技术有限公司

场景	配置方案 1	配置方案 2
部署以太网 CFM 与接口之间单向故障消息传递	请根据故障传递的方向，选择如下命令之一进行配置： ● 如果需要以太网 CFM 向接口单向传递故障消息，那么请使用命令 oam-bind ingress cfm md ma egress interface。 ● 如果需要接口向以太网 CFM 单向传递故障消息，那么请使用命令 oam-bind ingress interface egress cfm md ma trigger if-down。	无

----结束

检查配置结果

以太网 CFM 与接口联动配置成功后，您可以在 OAM 管理视图下查看到相关联动配置信息。

前提条件

已经完成以太网 CFM 与接口联动的所有配置。

操作步骤

步骤 1 在 OAM 管理视图下使用 **display this** 命令，查看是否成功配置了以太网 CFM 与接口绑定。

----结束

任务示例

执行命令 **display this**，查看以太网 CFM 与接口绑定信息。

```
[Quidway-oam-mgr] display this
#
oam-mgr
 oam-bind ingress interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1 trigger if-down
 oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface GigabitEthernet0/0/2
#
return
```

9.4.15 配置 EFM OAM 和以太网 CFM 之间的联动

介绍以太网 OAM 的 CFM 和 EFM 联动的配置方法。

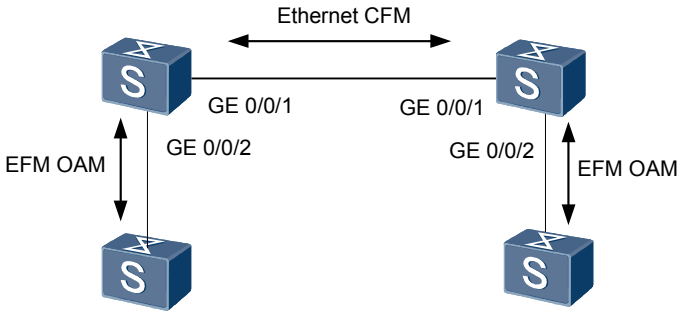
华为专有和保密信息
版权所有 © 华为技术有限公司

建立配置任务

应用环境

802.3ah 协议针对以太网最后一公里，主要用于 CE 和 PE 之间直连链路的检测。802.1ag 协议针对一组业务或一些特定的网络设备，主要用于对网络的故障检测，可以用于 CE 和 CE、PE 和 PE、CE 和 PE 之间。如图 9-30 所示，在 CE1 和 PE1、CE2 和 PE2 之间配置 EFM OAM，在 PE1 和 PE2 之间配置以太网 CFM，通过配置 ETH OAM 之间的联动，当 CE1 和 PE1 之间的链路发生故障时，通过以太网 CFM 向对端的 CE2 发出故障告警。

图 9-30 ETH OAM 联动示意图



前置任务

在配置 ETH OAM 联动之前，需完成以下任务：

- **9.4.3 配置 EFM OAM 基本功能**
- **9.4.9 配置以太网 CFM 基本功能**

数据准备

在配置 ETH OAM 联动功能之前，需要准备以下数据。

序号	数据
1	联动的接口和编号
2	MD 的名称和 MA 的名称

配置 ETH OAM 联动

背景信息

在 CE 设备上进行如下配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **oam-mgr**，进入 OAM 管理视图。

步骤 3 请根据实际情况选择以下配置。

- 执行命令 **oam-bind cfm md** *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*，配置 EFM OAM 和以太网 CFM 双向故障传递。
- 执行命令 **oam-bind ingress efm interface** *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*，配置 EFM OAM 向以太网 CFM 传递故障。
- 执行命令 **oam-bind ingress cfm md** *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*，配置以太网 CFM 向 EFM OAM 传递故障。

说明

在配置 ETH OAM 和其它功能模块联动后，

- 如果去使能端口的 EFM 功能，则会导致和 EFM 的联动功能被删除。
- 如果删除 MA 或 MD，则会导致和 CFM 的联动功能被删除。

若选择执行命令 **oam-bind cfm md** *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*，配置文件中将显示 **oam-bind ingress efm interface** *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* 和 **oam-bind ingress cfm md** *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number* 两条命令，故障传递的方向相反。

----结束

检查配置结果

前提条件

已经完成 EFM OAM 和以太 CFM 的联动配置。

操作步骤

步骤 1 在 OAM 管理视图下，使用命令 **display this** 查看 EFM OAM 和以太 CFM 联动配置信息。

----结束

任务示例

```
[Quidway-oam-mgr]display this
#
oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1
 oam-bind ingress cfm md md1 ma ma1 egress efm interface GigabitEthernet0/0/2
#
```

9.4.16 配置以太网 CFM 和以太网 CFM 联动

介绍以太网 CFM 和以太网 CFM 的配置方法。

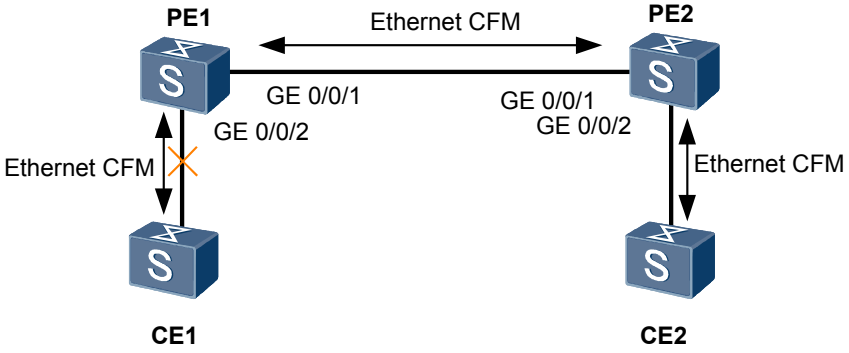
版权所有 © 华为技术有限公司

建立配置任务

应用环境

802.1ag 协议针对一组业务或一些特定的网络设备，主要用于对网络的故障检测，可以用于 CE 和 CE、PE 和 PE、CE 和 PE 之间。如图 9-31 所示，在 CE1 和 PE1、CE2 和 PE2 之间配置以太网 CFM，在 PE1 和 PE2 之间配置以太网 CFM，通过配置以太网 CFM 之间的联动，当 CE1 和 PE1 之间的链路发生故障时，通过以太网 CFM 向对端的 CE2 发出故障告警。

图 9-31 以太 CFM 联动示意图



前置任务

在配置以太 CFM 联动之前，需完成以下任务：

- 9.4.9 配置以太网 CFM 基本功能

数据准备

在配置以太 CFM 和以太 CFM 联动功能之前，需要准备以下数据。

序号	数据
1	联动的接口和编号
2	MD 的名称和 MA 的名称

配置以太网 CFM 和以太网 CFM 联动

背景信息

请在需要配置以太 CFM 联动的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **oam-mgr**，进入 OAM 管理视图。

步骤 3 （可选）执行命令 **oam-bind ingress cfm md** *md-name1* **ma** *ma-name1* **egress cfm md** *md-name2* **ma** *ma-name2*，配置以太 CFM 的单向故障传递功能。

步骤 4 （可选）执行命令 **oam-bind cfm md** *md-name1* **ma** *ma-name1* **cfm md** *md-name2* **ma** *ma-name2*，配置两侧以太网 CFM 双向传递故障功能。

步骤 3 和步骤 4 请根据需要选择执行。

说明

配置双向故障传递功能后，配置文件中实际显示两条方向不同的单向故障传递配置信息。

----结束

检查配置结果

前提条件

已经完成以太 CFM 与以太 CFM 联动的配置。

操作步骤

步骤 1 在 OAM 管理视图下，执行命令 **display this** 查看以太 CFM 与以太 CFM 的联动配置信息。

```
[Quidway-oam-mgr] display this
#
oam-mgr
 oam-bind ingress cfm md md1 ma ma1 egress cfm md md1 ma ma2
 oam-bind ingress cfm md md1 ma ma2 egress cfm md md1 ma ma1
#
```

----结束

9.4.17 配置以太网 CFM 和 SEP 联动

介绍以太网 CFM 和 SEP 的配置方法。

建立配置任务

应用环境

在 SEP 段的边缘设备上部署 SEP 和 CFM 联动功能。当 CFM 检测到上层网络产生故障时，边缘设备通过 CFM 协议报文将故障消息通知 OAM 管理模块，触发边缘设备上绑定 CFM 的端口物理状态变为 Down。

当边缘设备上绑定 CFM 的端口状态变为 Down 后，边缘设备的对端设备（位于 SEP 段上）上的端口需要发出 FLUSH-FDB 报文通知 SEP 段上其他节点拓扑发生变化。SEP 段上的设备接收到 FLUSH-FDB 报文后，SEP 段上的阻塞端口需要放开进入转发状态，并发送 FLUSH-FDB 报文，触发刷新 SEP 段上的节点 MAC 地址转发表和 ARP 表，从而实现下级网络感知上级网络故障，保证业务可靠传输。

前置任务

在配置以太 CFM 联动和 SEP 之前，需完成以下任务：

版权所有 © 华为技术有限公司

- 配置以太网 CFM 基本功能
- 配置 SEP 基本功能

数据准备

在配置以太 CFM 和 SEP 联动功能之前，需要准备以下数据。

序号	数据
1	联动的接口和编号
2	MD 的名称和 MA 的名称
3	SEP 段
4	加入 SEP 段的接口号

配置以太网 CFM 和 SEP 联动

背景信息

请在需要配置 CFM 和 SEP 联动功能的设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图

步骤 2 执行命令 **oam-mgr**，进入 OAM 管理视图。

步骤 3 执行命令 **oam-bind ingress cfm md** *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*，配置 SEP 与 CFM 联动功能。

interface *interface-type interface-number* 必须成功加入 SEP 段。

----结束

检查配置结果

前提条件

已经完成以太 CFM 与 SEP 联动的配置。

操作步骤

步骤 1 在 OAM 管理视图下，执行命令 **display this** 查看以太 CFM 与 SEP 的联动配置信息。

```
[Quidway-oam-mgr] display this
#
oam-mgr
  oam-bind ingress cfm md md1 ma ma1 egress sep segment 1 interface GigabitEthernet0/0/1
#
```

----结束

版权所有 © 华为技术有限公司

9.4.18 维护以太网 OAM

通过维护以太网 OAM，可以实现清除 CCM 消息统计数据、监控以太网 OAM 的运行状况。

调试 EFM OAM

调试完成后，应及时关闭调试开关。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 undo debugging all 命令关闭调试开关。

在出现 EFM OAM 运行故障时，请在用户视图下执行 **debugging** 命令对 EFM OAM 进行调试，查看调试信息，定位故障并分析故障原因。

打开调试开关的操作步骤请参见《AC6605 无线接入控制器 配置指南-设备管理》中“诊断和调试设备”的内容。

操作步骤

步骤 1 在用户视图下执行 **debugging efm interface** *interface-type interface-number* { **all** | **error** | **event** | **message** | **packet** { **all** | **receive** | **send** } | **process** }命令，打开指定接口的 EFM OAM 模块的调试信息开关。

----结束

9.4.19 配置举例

介绍以太网 OAM 的各种组网举例。

配置 EFM OAM 示例

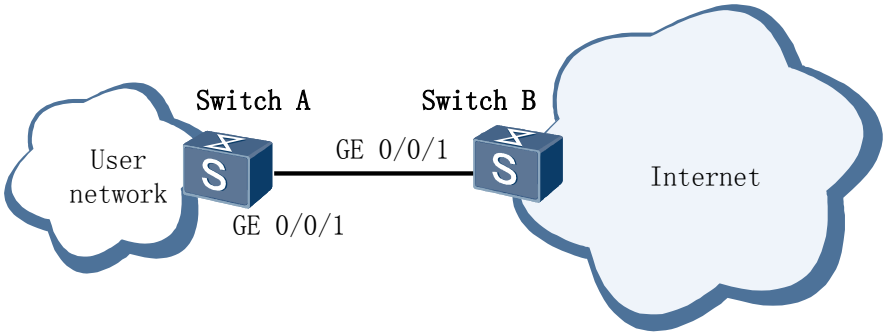
组网需求

如图 9-32 所示，某用户网络通过 SwitchA 和 SwitchB 设备连接到 ISP 网络上。其中，SwitchA 是 CE 设备，SwitchB 是 UPE 设备。要求：

- 实现 SwitchA 和 SwitchB 之间连通性故障自动检测功能，并且如检测到连通性故障 SwitchA 设备和 SwitchB 设备上产生报警信息。
- SwitchB 监测本设备上的接口 GE0/0/1 的误帧、误码和误帧秒，如误帧、误码和误帧秒超过设定的门限值则 SwitchB 设备上产生报警信息。

版权所有 © 华为技术有限公司

图 9-32 配置 EFM OAM 示例组网图



配置思路

采用如下的思路配置 EFM OAM：

1. 全局使能 SwitchA 和 SwitchB 的 EFM OAM 功能。
2. 配置 SwitchA 的接口 GE0/0/1 的 EFM OAM 工作模式为被动模式。
3. 使能 SwitchB 的接口 GE0/0/1 和 SwitchA 的接口 GE0/0/1 的 EFM OAM 功能。
4. 在 SwitchB 上配置接口 GE0/0/1 的误帧、误码、误帧秒检测功能。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchB 上接口 GE0/0/1 的误帧观察时长为 5 秒，门限为 5。
- SwitchB 上接口 GE0/0/1 的误码观察时长为 5 秒，门限为 5。
- SwitchB 上接口 GE0/0/1 的误帧秒观察时长为 120 秒，门限为 5。

操作步骤

步骤 1 全局使能 EFM OAM 功能

全局使能 SwitchA 的 EFM OAM 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] efm enable
```

全局使能 SwitchB 的 EFM OAM 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] efm enable
```

步骤 2 配置 SwitchA 的接口 GE0/0/1 的 EFM OAM 工作模式为被动模式

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] efm mode passive
```

步骤 3 使能 SwitchB 的接口 GE0/0/1 和 SwitchA 的接口 GE0/0/1 的 EFM OAM 功能

使能 SwitchA 的接口 GigabitEthernet 的 EFM OAM 功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/1] efm enable
[SwitchA-GigabitEthernet0/0/1] quit
```

使能 SwitchB 的接口 GE0/0/1 的 EFM OAM 功能。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] efm enable
[SwitchB-GigabitEthernet0/0/1] bpdu enable
```

步骤 4 在 SwitchB 上配置接口 GE0/0/1 的误帧、误码、误帧秒检测功能

在 SwitchB 上配置接口 GE0/0/1 的误帧检测功能。

```
[SwitchB-GigabitEthernet0/0/1] efm error-frame period 5
[SwitchB-GigabitEthernet0/0/1] efm error-frame threshold 5
[SwitchB-GigabitEthernet0/0/1] efm error-frame notification enable
```

在 SwitchB 上配置接口 GE0/0/1 的误码检测功能。

```
[SwitchB-GigabitEthernet0/0/1] efm error-code period 5
[SwitchB-GigabitEthernet0/0/1] efm error-code threshold 5
[SwitchB-GigabitEthernet0/0/1] efm error-code notification enable
```

在 SwitchB 上配置接口 GE0/0/1 的误帧秒检测功能。

```
[SwitchB-GigabitEthernet0/0/1] efm error-frame-second period 120
[SwitchB-GigabitEthernet0/0/1] efm error-frame-second threshold 5
[SwitchB-GigabitEthernet0/0/1] efm error-frame-second notification enable
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 5 检查配置结果

如果 SwitchA 和 SwitchB 的 EFM OAM 配置正确，接口 GE0/0/1 和接口 GE0/0/1 成功协商后进入握手阶段，此时在 SwitchA 或 SwitchB 上执行 **display efm session** 命令，可看到接口 GE0/0/1 或接口 GE0/0/1 的 EFM OAM 协议状态为 detect。

```
[SwitchB] display efm session interface gigabitehternet 0/0/1
  Interface               EFM State               Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/1          detect                    --
```

如果 SwitchB 上接口 GE0/0/1 的误帧、误码、误帧秒检测功能配置正确，执行命令 **display efm**，接口的 EFM OAM 配置信息如下：

```
[SwitchB] display efm interface gigabitethernet 0/0/1
    Item                          Value
    ------------------------------------
    Interface:                    GigabitEthernet0/0/1
    EFM Enable Flag:              enable
    Mode:                         active
    OAMPDU MaxSize:               128
    ErrCodeNotification:          enable
    ErrCodePeriod:                5
    ErrCodeThreshold:             5
    ErrFrameNotification:         enable
    ErrFramePeriod:               5
    ErrFrameThreshold:            5
    ErrFrameSecondNotification:   enable
    ErrFrameSecondPeriod:         120
    ErrFrameSecondThreshold:      5
    Hold Up Time:                 10
    ThresholdEvtTriggerErrDown:   enable
    TriggerIfDown:                disable
    TriggerMacRenew:              disable
    Remote MAC:                   0010-0010-0010
    Remote EFM Enable Flag:       enable
    Remote Mode:                  passive
```


版权所有 © 华为技术有限公司

```
Remote  MaxSize:            128
Remote State:                 --
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
 efm enable
#
 interface GigabitEthernet0/0/1
 efm mode passive
 efm enable
#
return
```

- SwitchB 的配置文件

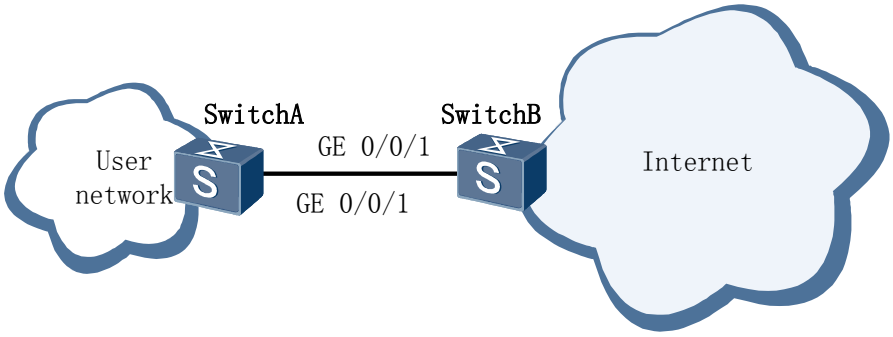
```
#
sysname SwitchB
#
 efm enable
#
interface GigabitEthernet0/0/1
 efm enable
 efm error-frame period 5
 efm error-frame threshold 5
 efm error-frame notification enable
 efm error-frame-second period 120
 efm error-frame-second threshold 5
 efm error-frame-second notification enable
 efm error-code period 5
 efm error-code threshold 5
 efm error-code notification enable
#
return
```

配置链路丢包率检测示例

组网需求

如图 9-33 所示，某用户网络准备通过 SwitchA 和 SwitchB 连接到 ISP 网络上。其中，SwitchA 是 CE 设备，SwitchB 是 UPE 设备。由于 SwitchA 和 SwitchB 之间的链路是一条新搭建的链路，在正式启用前，ISP 需要在 SwitchB 上对该链路进行丢包率测试。

图 9-33 测试链路丢包率示例组网图



华为专有和保密信息
版权所有 © 华为技术有限公司

配置思路

采用如下的思路测试链路丢包率：

1. 在 SwitchA 和 SwitchB 上配置 EFM OAM 基本功能，并将 SwitchA 的接口 GEO/O/1 的 EFM OAM 工作模式配置为被动模式。
2. 在 SwitchB 上配置 EFM OAM 远端环回。
3. 从 SwitchB 向 SwitchA 发送测试报文。
4. 在 SwitchB 上查看测试报文的返回情况。

数据准备

为完成此配置例，需准备如下的数据：

- EFM OAM 远端环回的超时时间
- 测试报文的大小、数量和发送速率

操作步骤

步骤 1 配置 EFM OAM 基本功能

全局使能 SwitchB 的 EFM OAM 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] efm enable
```

全局使能 SwitchA 的 EFM OAM 功能。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] efm enable
```

配置 SwitchA 的 GEO/O/1 接口的 EFM OAM 工作模式为被动模式。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] efm mode passive
```

使能 SwitchA 上接口 GEO/O/1 的 EFM OAM 功能。

```
[SwitchA-GigabitEthernet0/0/1] efm enable
[SwitchA-GigabitEthernet0/0/1] quit
```

使能 SwitchB 上接口 GEO/O/1 的 EFM OAM 功能。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] efm enable
[SwitchB-GigabitEthernet0/0/1] quit
```

检查配置结果。

如果 SwitchA 和 SwitchB 的 EFM OAM 配置正确，接口成功协商后进入握手阶段，此时在 SwitchA 或 SwitchB 上执行 **display efm session** 命令，可看到接口 SwitchA 的 GEO/O/1 的 EFM OAM 协议状态为 detect。

```
[SwitchB] display efm session interface gigabitethernet 0/0/1
  Interface              EFM State                    Loopback Timeout
```


版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------
GigabitEthernet0/0/1          detect                    --
```

步骤 2 配置 EFM OAM 远端环回

在 SwitchB 上配置 EFM OAM 远端环回。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] efm loopback start
[SwitchB-GigabitEthernet0/0/1] quit
```

检查配置结果。

配置 EFM OAM 远端环回成功后，在 SwitchB 上执行 **display efm session** 命令，可以看到接口 SwitchA 的 GEO/O/1 的 EFM OAM 协议状态为 Loopback（control），即远端环回状态（且为远端环回的发起方）。

```
[SwitchB] display efm session interface gigabitethernet 0/0/1
Interface               EFM State              Loopback Timeout
--------------------------------------------------------------------
GigabitEthernet0/0/1          Loopback(control)       20
```

配置 EFM OAM 远端环回成功后，在 SwitchA 上执行 **display efm session** 命令，可以看到接口 SwitchA 的 GEO/O/1 的 EFM OAM 协议状态为 Loopback（be controlled），即远端环回状态（且为远端环回的响应方）。

```
[SwitchA] display efm session interface gigabitethernet 0/0/1
Interface               EFM State               Loopback Timeout
--------------------------------------------------------------------
GigabitEthernet0/0/1          Loopback(be controlled)  --
```

步骤 3 从 SwitchB 向 SwitchA 发送测试报文

```
[SwitchB] test-packet start interface gigabitethernet 0/0/1
Please wait.............
Info: The test is completed.
```

步骤 4 在 SwitchB 上查看测试报文的返回情况

```
[SwitchB] display test-packet result
 Test Result            Value
 ----------------------------------------
 PacketsSend :          5
 PacketsReceive :       5
 PacketsLost :          0
 BytesSend  :           128
 BytesReceive :         128
 BytesLost  :           0
 StartTime  :           2009-02-21 18:07:01
 EndTime :              2009-02-21 18:07:02
```

根据以上数据可计算链路的丢包率。

步骤 5 取消 EFM OAM 远端环回

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] efm loopback stop
[SwitchB-GigabitEthernet0/0/1] quit
```

说明

缺省情况下，远端环回的超时时间是 20 分钟，到达此时间，远端环回自动停止。如果需要提前取消远端环回，可执行以上步骤。

步骤 6 检查配置结果

在远端环回自动取消或手动取消后，在 SwitchA 或 SwitchB 上执行 **display efm session** 命令，可以看到链路两端接口的 EFM OAM 协议状态为 Detect 或 Discovery，即握手状态或对端发现状态。例如：

版权所有 © 华为技术有限公司

```
[SwitchB] display efm session interface gigabitethernet 0/0/1
Interface                 EFM State               Loopback Timeout
------------------------------------------------------------------------------
GigabitEthernet0/0/1              detect                    --
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
 efm enable
#
interface GigabitEthernet0/0/1
 efm mode passive
 efm enable
#
return
```

- SwitchB 的配置文件

```
#
sysname SwitchB
#
 efm enable
#
interface GigabitEthernet0/0/1
 efm enable
#
return
```

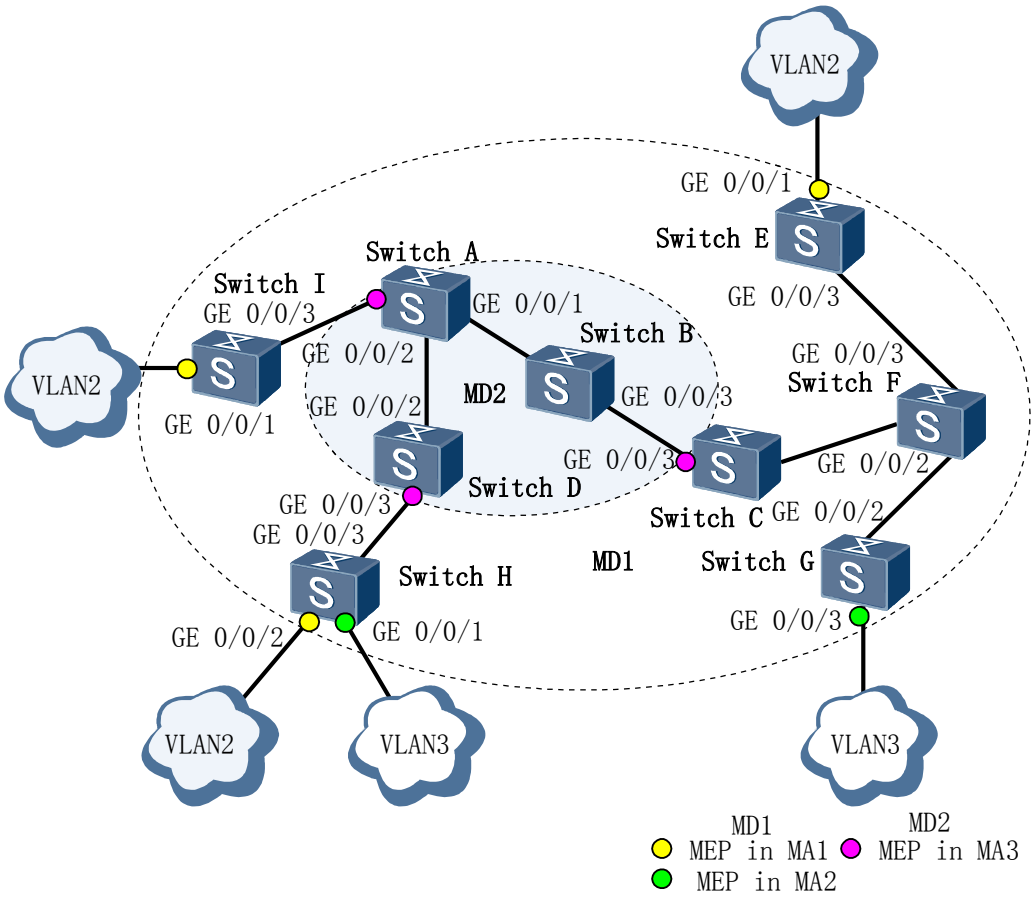
配置以太网 CFM 基本功能示例

组网需求

如图 9-34 所示的以太网由两个 ISP 管理，其中 SwitchA、SwitchB、SwitchD 由 ISP1 管理，SwitchC、SwitchE、SwitchF、SwitchG、SwitchH、SwitchI 由 ISP2 管理。要求在该网络中实现连通性故障检测功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 9-34 配置以太网 CFM 基本功能示例组网图



配置思路

采用如下的思路配置以太网 CFM 基本功能：

1. 创建 VLAN，并将相关接口加入对应的 VLAN。
2. 在所有设备上创建 MD1，MD1 的级别为 6。
3. 在除 SwitchG 外的所有设备上的 MD1 下创建并配置 MA1。（MA1 和 VLAN2 关联。）
4. 在除 SwitchE、SwitchI 外的所有设备上的 MD1 下创建并配置 MA2。（MA2 和 VLAN3 关联。）
5. 在 SwitchA、SwitchB、SwitchC、SwitchD 上创建 MD2，MD2 的级别为 4；并在 MD2 下创建并配置 MA3。（MA3 和 VLAN4 关联。）
6. 在 SwitchI、SwitchH、SwitchE 上的 MD1 的 MA1 下创建 MEP 和 RMEP。
7. 在 SwitchH、SwitchG 上的 MD1 的 MA2 下配置 MEP 和 RMEP。
8. 在 SwitchA、SwitchC、SwitchD 上的 MD2 的 MA3 下配置 MEP 和 RMEP。
9. 使能 CCM 消息的发送和接收功能。

数据准备

为完成此配置例，需准备如下的数据。

华为专有和保密信息
版权所有 © 华为技术有限公司

- MD1 的级别为 6
- MD2 的级别为 4

操作步骤

步骤 1 创建 VLAN，并将相关接口加入对应的 VLAN（略）

步骤 2 创建 MD1

在 SwitchA 上创建 MD1。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] cfm enable
[SwitchA] cfm md md1 level 6
```

在 SwitchB、SwitchC、SwitchD、SwitchE、SwitchF、SwitchG、SwitchH、SwitchI 上创建 MD1。

与在 SwitchA 上创建 MD1 的方法类似，此处不再赘述。

步骤 3 在除 SwitchG 外的所有设备上的 MD1 下创建并配置 MA1

在 SwitchA 上的 MD1 下创建并配置 MA1。

```
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] map vlan 2
[SwitchA-md-md1-ma-ma1] quit
```

在 SwitchB、SwitchC、SwitchD、SwitchE、SwitchF、SwitchH、SwitchI 上的 MD1 下创建并配置 MA1。

略。与在 SwitchA 上的 MD1 下创建并配置 MA1 的方法类似，此处不再赘述。

步骤 4 在除 SwitchE、SwitchI 外的所有设备上的 MD1 下创建并配置 MA2

在 SwitchA 上的 MD1 下创建并配置 MA2。

```
[SwitchA-md-md1] ma ma2
[SwitchA-md-md1-ma-ma2] map vlan 3
[SwitchA-md-md1-ma-ma2] quit
[SwitchA-md-md1] quit
```

在 SwitchB、SwitchC、SwitchD、SwitchF、SwitchG、SwitchH 上的 MD1 下创建并配置 MA2。

略。与在 SwitchA 上的 MD1 下创建并配置 MA2 的方法类似，此处不再赘述。

步骤 5 在 SwitchA、SwitchB、SwitchC、SwitchD 上创建 MD2，并在 MD2 下创建并配置 MA3

在 SwitchA 上创建 MD2，并在 MD2 下创建并配置 MA3。

```
[SwitchA] cfm md md2 level 4
[SwitchA-md-md2] ma ma3
[SwitchA-md-md2-ma-ma3] map vlan 4
[SwitchA-md-md2-ma-ma3] quit
[SwitchA-md-md2] quit
```

在 SwitchB、SwitchC、SwitchD 上创建 MD2，并在 MD2 下创建并配置 MA3。

略。与在 SwitchA 上创建 MD2，并在 MD2 下创建并配置 MA3 的方法类似，此处不再赘述。

版权所有 © 华为技术有限公司

步骤 6 在 SwitchE、SwitchH、SwitchI 上的 MD1 的 MA1 下配置 MEP 和 RMEP

在 SwitchE 上的 MD1 的 MA1 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchE
[SwitchE] cfm md md1
[SwitchE-md-md1] ma ma1
[SwitchE-md-md1-ma-ma1] mep mep-id 3 interface gigabitethernet 0/0/1 inward
```

在 SwitchH 上的 MD1 的 MA1 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchH
[SwitchH] cfm md md1
[SwitchH-md-md1] ma ma1
[SwitchH-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/2 inward
```

在 SwitchI 上的 MD1 的 MA1 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchI
[SwitchI] cfm md md1
[SwitchI-md-md1] ma ma1
[SwitchI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
```

在 SwitchE 上的 MD1 的 MA1 下配置 RMEP。

```
[SwitchE-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchE-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchE-md-md1-ma-ma1] quit
[SwitchE-md-md1] quit
```

在 SwitchH 上的 MD1 的 MA1 下配置 RMEP。

```
[SwitchH-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchH-md-md1-ma-ma1] remote-mep mep-id 3
[SwitchH-md-md1-ma-ma1] quit
[SwitchH-md-md1] quit
```

在 SwitchI 上的 MD1 的 MA1 下配置 RMEP。

```
[SwitchI-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchI-md-md1-ma-ma1] remote-mep mep-id 3
[SwitchI-md-md1-ma-ma1] quit
[SwitchI-md-md1] quit
```

步骤 7 在 SwitchH、SwitchG 上的 MD1 的 MA2 下配置 MEP 和 RMEP

在 SwitchH 上的 MD1 的 MA2 下配置 MEP。

```
[SwitchH] cfm md md1
[SwitchH-md-md1] ma ma2
[SwitchH-md-md1-ma-ma2] mep mep-id 1 interface gigabitethernet 0/0/1 inward
```

在 SwitchG 上的 MD1 的 MA2 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchG
[SwitchG] cfm md md1
[SwitchG-md-md1] ma ma2
[SwitchG-md-md1-ma-ma2] mep mep-id 2 interface gigabitethernet 0/0/3 inward
```

在 SwitchH 上的 MD1 的 MA2 下配置 RMEP。

```
[SwitchH-md-md1-ma-ma2] remote-mep mep-id 2
[SwitchH-md-md1-ma-ma2] quit
[SwitchH-md-md1] quit
```

在 SwitchG 上的 MD1 的 MA2 下配置 RMEP。

版权所有 © 华为技术有限公司

```
[SwitchG-md-md1-ma-ma2] remote-mep mep-id 1
[SwitchG-md-md1-ma-ma2] quit
[SwitchG-md-md1] quit
```

步骤 8 在 SwitchA、SwitchC、SwitchD 上的 MD2 的 MA3 下配置 MEP 和 RMEP

在 SwitchA 上的 MD2 的 MA3 下配置 MEP。

```
[SwitchA] cfm md md2
[SwitchA-md-md2] ma ma3
[SwitchA-md-md2-ma-ma3] mep mep-id 1 interface gigabitethernet 0/0/3 inward
```

在 SwitchC 上的 MD2 的 MA3 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] cfm md md2
[SwitchC-md-md2] ma ma3
[SwitchC-md-md2-ma-ma3] mep mep-id 2 interface gigabitethernet 0/0/3 outward
```

在 SwitchD 上的 MD2 的 MA3 下配置 MEP。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] cfm md md2
[SwitchD-md-md2] ma ma3
[SwitchD-md-md2-ma-ma3] mep mep-id 3 interface gigabitethernet 0/0/3 inward
```

在 SwitchA 上的 MD2 的 MA3 下配置 RMEP。

```
[SwitchA-md-md2-ma-ma3] remote-mep mep-id 2
[SwitchA-md-md2-ma-ma3] remote-mep mep-id 3
```

在 SwitchC 上的 MD2 的 MA3 下配置 RMEP。

```
[SwitchC-md-md2-ma-ma3] remote-mep mep-id 1
[SwitchC-md-md2-ma-ma3] remote-mep mep-id 3
[SwitchC-md-md2-ma-ma3] quit
[SwitchC-md-md2] quit
```

在 SwitchD 上的 MD2 的 MA3 下配置 RMEP。

```
[SwitchD-md-md2-ma-ma3] remote-mep mep-id 1
[SwitchD-md-md2-ma-ma3] remote-mep mep-id 2
[SwitchD-md-md2-ma-ma3] quit
[SwitchD-md-md2] quit
```

步骤 9 使能 CCM 消息的发送和接收功能

在 SwitchA 上使能所有 MEP 的 CCM 消息发送功能。

```
[SwitchA-md-md2-ma-ma3] mep ccm-send enable
```

在 SwitchA 上使能接收所有 RMEP 发送的 CCM 消息功能。

```
[SwitchA-md-md2-ma-ma3] remote-mep ccm-receive enable
[SwitchA-md-md2-ma-ma3] quit
[SwitchA-md-md2] quit
```

在 SwitchB、SwitchC、SwitchD、SwitchE、SwitchF、SwitchG、SwitchH、SwitchI 上使能所有 MEP 的 CCM 消息发送功能，并使能接收所有 RMEP 发送的 CC 报文功能。

与在 SwitchA 上使能所有 MEP 的 CCM 消息发送功能和使能接收所有 RMEP 发送的 CCM 消息功能的配置方法类似，此处不再赘述。

步骤 10 检查配置结果

使用命令 **display cfm remote-mep** 查看 RMEP 的详细信息，可以看到 RMEP 的状态，以确认 CFM 配置是否成功。

版权所有 © 华为技术有限公司

在 SwitchA 上查看 RMEP 详细信息。

```
[SwitchA] display cfm remote-mep
The total number of RMEPs is : 2
The status of RMEPS : 2 up, 0 down, 0 disable
--------------------------------------------------

 MD Name            : md2
 Level              : 4
 MA Name            : ma3
 RMEP ID            : 2
 Vlan ID            : 4
 VSI Name           : --
 MAC                : 0000-0121-0222
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarm

 MD Name            : md2
 Level              : 4
 MA Name            : ma3
 RMEP ID            : 3
 Vlan ID            : 4
 VSI Name           : --
 MAC                : 0000-0121-0333
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarm
```

在 SwitchH 上查看 RMEP 详细信息。

```
[SwitchA] display cfm remote-mep
The total number of RMEPs is : 3
The status of RMEPS : 2 up, 0 down, 0 disable
--------------------------------------------------

 MD Name            : md1
 Level              : 6
 MA Name            : ma1
 RMEP ID            : 1
 Vlan ID            : 2
 VSI Name           : --
 MAC                : 0000-0121-0555
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarm

 MD Name            : md1
 Level              : 6
 MA Name            : ma1
 RMEP ID            : 3
 Vlan ID            : 2
 VSI Name           : --
 MAC                : 0000-0121-0666
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarm

 MD Name            : md1
 Level              : 6
 MA Name            : ma2
 RMEP ID            : 2
 Vlan ID            : 3
 VSI Name           : --
 MAC                : 0000-0121-0888
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
```


版权所有 © 华为技术有限公司

Alarm Status : RemoteAlarm

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
   map vlan 4
   mep mep-id 1 interface gigabitethernet0/0/3 inward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
```


版权所有 © 华为技术有限公司

```
   map vlan 4
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
   map vlan 4
   mep mep-id 2 interface gigabitethernet0/0/3 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
   map vlan 4
   mep mep-id 3 interface gigabitethernet0/0/3 inward
   mep ccm-send mep-id 3 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
vlan batch 2
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
   mep mep-id 3 interface gigabitethernet0/0/1 inward
   mep ccm-send mep-id 3 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

- SwitchF 的配置文件

```
#
 sysname SwitchF
#
vlan batch 2 to 3
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
return
```

- SwitchG 的配置文件

```
#
 sysname SwitchG
#
vlan batch 3
#
cfm enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 3
#
 cfm md md1 level 6
  ma ma2
   map vlan 3
   mep mep-id 2 interface gigabitethernet0/0/3 inward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
#
return
```

- SwitchH 的配置文件

```
#
 sysname SwitchH
#
vlan batch 2 to 3
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
   mep mep-id 2 interface gigabitethernet0/0/2 inward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
  ma ma2
   map vlan 3
   mep mep-id 1 interface gigabitethernet0/0/1 inward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

- SwitchI 的配置文件

```
#
 sysname SwitchI
#
vlan batch 2
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
```


版权所有 © 华为技术有限公司

```
 cfm md md1 level 6
  ma ma1
   map vlan 2
   mep mep-id 1 interface gigabitethernet0/0/1 inward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
#
return
```

配置以太网 CFM 默认 MD 功能示例

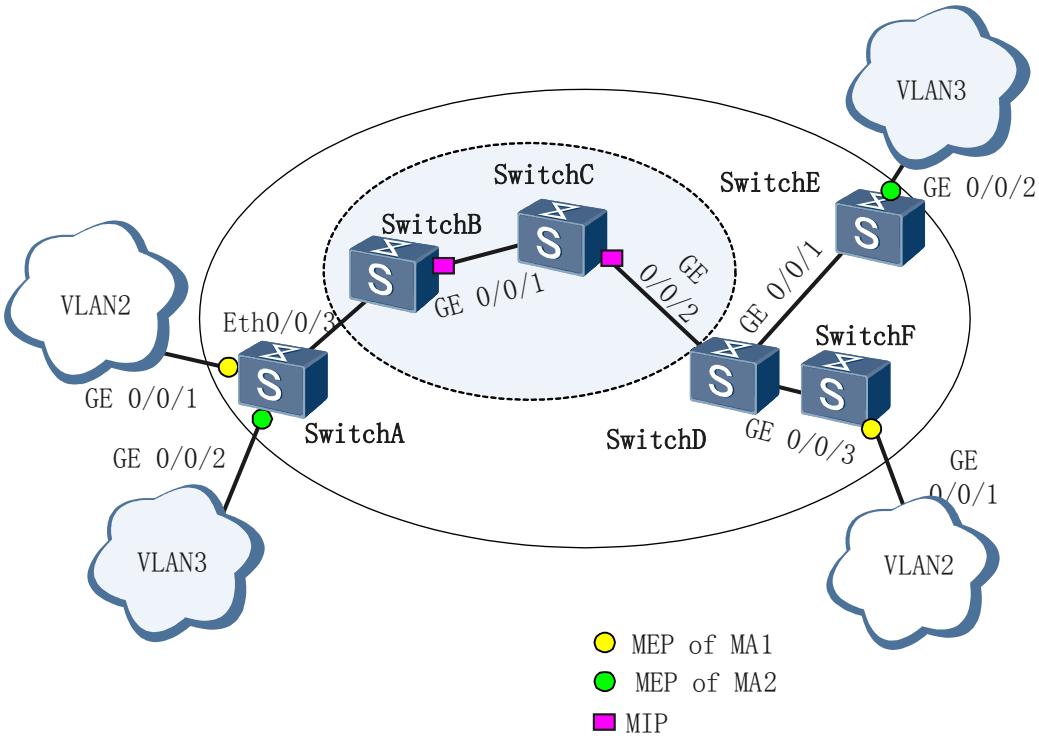
规格

S2300SI 交换机不适用、S6300 交换机不适用，其它类型交换机都适用。

组网需求

如图 9-35 所示的以太网由两个 ISP 管理，其中 SwitchB 和 SwitchC 由 ISP1 管理，SwitchA、SwitchD、SwitchE 和 SwitchF 由 ISP2 管理。通过在低级别的 MD 设备上配置默认 MD 实现网络中连通性故障检测功能。

图 9-35 配置以太网 CFM 默认 MD 功能示例组网图



操作步骤

- 配置 SwitchA

版权所有 © 华为技术有限公司

```
#
 sysname SwitchA
#
 vlan batch 2 to 3
#
 cfm version standard //配置版本为标准版本
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 //配置端口允许VLAN2的报文通过
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
 cfm md md1 level 6 //创建MD1
  ma ma1 //创建MA1
   map vlan 2 //配置MA1
   mep mep-id 2 interface gigabitethernet 0/0/1 inward //配置MEP
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1 //配置RMEP
   remote-mep ccm-receive mep-id 1 enable
  ma ma2
   map vlan 3
   mep mep-id 1 interface gigabitethernet 0/0/2 inward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

- 配置 SwitchB

```
#
 sysname SwitchB
#
vlan batch 2 to 3
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
 cfm md md2 level 4
#
 cfm default md level 6 //创建默认MD
  mip create-type default
   vlan 2 to 3 //配置关联VLAN2，VLAN3
#
return
```

- 配置 SwitchC

```
#
 sysname SwitchC
#
vlan batch 2 to 3
#
 cfm version standard
 cfm enable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
 cfm md md2 level 4
#
 cfm default md level 6
  mip create-type default
  vlan 2 to 3
#
return
```

- 配置 SwitchD

```
#
 sysname SwitchD
#
vlan batch 2 to 3
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
return
```

- 配置 SwitchE

```
#
 sysname SwitchE
#
vlan batch 3
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 3
#
 cfm md md1 level 6
  ma ma2
   map vlan 3
   mep mep-id 2 interface gigabitethernet 0/0/2 inward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
```


版权所有 © 华为技术有限公司

```
#
return
```

- 配置 SwitchF

```
#
 sysname SwitchF
#
vlan batch 2
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
   mep mep-id 1 interface gigabitethernet 0/0/1 inward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

说明

缺省情况下，设备启用的是 draft7 草案版本。

说明

整网中的设备使用的版本必须一致，要么都是 draft7 版本，要么都是 standard 标准版本，两个版本不能混用。

验证配置结果

经过以上配置，在网络稳定后，执行以下操作，验证配置结果。以 SwitchA 和 SwitchB 为例。

- 在 SwitchB 上执行 **display cfm default md** 命令，查看结果如下：

```
[SwitchB] display cfm default md
Level   MIP Create-type   SenderID TLV-type   VLAN List
------------------------------------------------------------------------------
6       default           Defer             2 to 3
```

可以看到 SwitchB 上配置了级别为 6 的默认 MD 并关联了 VLAN2 和 VLAN3，MIP 节点的生成规则为 default。

- 在 SwitchA 上执行 802.1ag MAC Trace 操作，可以看到 SwitchA 和 SwitchE 之间没有发生连通性故障，802.1ag MAC Trace 操作执行成功。查看结果如下：

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] trace mac-8021ag mac aa99-6600-5600
Tracing the route to aa99-6600-5600 over a maximum of 255 hops:
 Hops     Mac               Ingress                   Ingress Action      Relay Action
          Forwarded         Egress                    Egress Action       Ismep
 1        2155-2201-3302    GigabitEthernet0/0/3              IngOK
RlyFDB
          Forwarded         GigabitEthernet0/0/1              EgrOK               No
 2        5522-1101-5503    GigabitEthernet0/0/1              IngOK
RlyFDB
          Forwarded         GigabitEthernet0/0/2              EgrOk               No
 3        2234-6432-3344    GigabitEthernet0/0/2              IngOK
RlyFDB
```


版权所有 © 华为技术有限公司

```
          Forwarded          GigabitEthernet0/0/3          EgrOk              No
 4        4323-5332-5522     GigabitEthernet0/0/3          IngOK
RlyFDB
          Forwarded          GigabitEthernet0/0/1          EgrOk              No
 5        aa99-6600-5600     GigabitEthernet0/0/1          IngOK
RlyHit
          Not Forwarded                                                   IsMep
 Info: Succeed in tracing the destination address aa99-6600-5600.
```

配置注意事项

默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越。

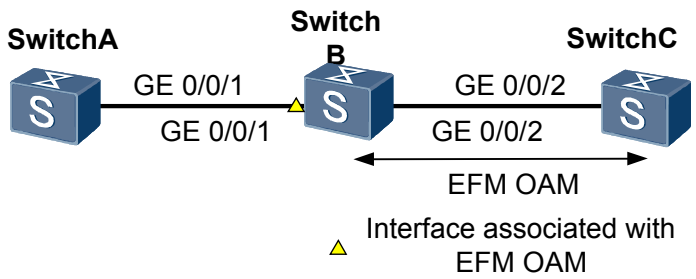
配置 EFM OAM 与接口联动（触发与 EFM OAM 联动的接口物理状态变为 Down）示例

该组网的特点是如果设备上配置了 EFM OAM 和接口联动，当 EFM OAM 检测到故障时，本端设备上的 EFM OAM 将故障消息通知 OAM 管理模块，触发绑定 EFM OAM 的接口物理状态变为 Down。反之，当接口的物理状态变为 Down 时，OAM 管理模块通知 EFM OAM 发生故障，EFM OAM 会将故障消息传递到远端设备。

组网需求

如图 9-36 所示，在 SwitchB 与 SwitchC 之间配置 EFM OAM。当 SwitchB 的 GE0/0/2 接口 DOWN 时，通过联动机制，EFM OAM 将故障传递至远端 SwitchB 的 GE0/0/1 接口，GE0/0/1 接口状态变为 down。

图 9-36 配置 EFM OAM 和接口联动组网图



配置思路

采用如下的思路配置 EFM OAM 和接口联动功能：

1. 在 SwitchB 和 SwitchC 之间配置 EFM OAM 功能。
2. 在 SwitchB 上配置 EFM OAM 与接口 GE0/0/1 的联动功能。

操作步骤

步骤 1 配置 SwitchB 和 SwitchC 之间的 EFM OAM 功能。

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
```


版权所有 © 华为技术有限公司

```
[SwitchB] efm enable
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] bpdu enable
[SwitchB-GigabitEthernet0/0/2] efm mode passive
[SwitchB-GigabitEthernet0/0/2] efm enable
[SwitchB-GigabitEthernet0/0/2] quit
```

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] efm enable
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] bpdu enable
[SwitchC-GigabitEthernet0/0/2] efm enable
[SwitchC-GigabitEthernet0/0/2] quit
```

在 SwitchB 上执行 **display efm session interface** 查看 EFM OAM 状态，显示结果为 detect。

```
[SwitchB] display efm session interface gigabitethernet 0/0/2
  Interface               EFM State                Loopback Timeout
  ------------------------------------------------------------------
  GigabitEthernet0/0/2            detect                --
```

步骤 2 配置 EFM OAM 和接口的联动。

配置 SwitchB 的接口 GE0/0/1 和 SwitchB 与 SwitchC 之间的 EFM OAM 的双向联动。

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind efm interface gigabitethernet 0/0/2 trigger if-down interface
gigabitethernet 0/0/1
[SwitchB-oam-mgr] quit
```

步骤 3 检查配置结果。

在 SwitchB 上关闭接口 GE0/0/2,EFM OAM 将故障传递至 GE0/0/1 接口，GE0/0/1 接口状态变为 TRIGGER DOWN （3AH）。

```
[SwitchB] display interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 current state : TRIGGER DOWN (3AH)
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port,PVID :    1,The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-8211-1111
Port Mode: COMBO AUTO
Current Work Mode: COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -
Input:  0 packets, 0 bytes
Unicast        :                0,Multicast          :                0
Broadcast      :                0,Jumbo              :                0
CRC            :                0,Giants             :                0
Jabbers        :                0,Throttles          :                0
Runts          :                0,DropEvents         :                0
Alignments     :                0,Symbols            :                0
Ignoreds       :                0,Frames             :                0
Discard        :                0,Total Error        :                0
Output:  0 packets, 0 bytes
Unicast        :                0,Multicast          :                0
Broadcast      :                0,Jumbo              :                0
Collisions     :                0,Deferreds          :                0
Late Collisions:                0,ExcessiveCollisions:                0
Buffers Purged :                0
```


版权所有 © 华为技术有限公司

```
Discard        :                  0,Total Error        :                  0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

----结束

配置文件

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
efm enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
 efm mode passive
 efm enable
 bpdu enable
#
 oam-mgr
  oam-bind ingress interface GigabitEthernet0/0/2 egress efm interface GigabitEthernet0/0/1
trigger if-down
  oam-bind ingress efm interface GigabitEthernet0/0/1 trigger if-down egress interface
GigabitEthernet0/0/2
#
return
```

- SwitchC 的配置文件

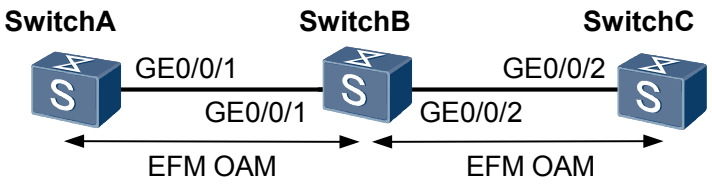
```
#
 sysname SwitchC
#
efm enable
#
interface GigabitEthernet0/0/2
 efm enable
 bpdu enable
#
return
```

配置 EFM OAM 与 EFM OAM 联动示例

组网需求

如图 9-37 所示，为了实现端到端链路故障检测，在 SwitchA 和 SwitchB、SwitchB 和 SwitchC 之间分别配置 EFM OAM，当 SwitchA 和 SwitchB 之间有链路故障发生时，SwitchA 和 SwitchB 之间的 EFM OAM 检测到故障，通过联动机制向 SwitchC 发送告警。

图 9-37 配置 EFM 和 EFM 联动组网示意图



版权所有 © 华为技术有限公司

配置思路

采用如下思路配置 EFM OAM 和 EFM OAM 的联动功能：

1. 全局使能 SwitchA、SwitchB、SwitchC 的 EFM OAM 功能。
2. 配置 SwitchB 的 GE0/0/1、SwitchC 的 GE0/0/2 的 EFM OAM 工作模式为被动模式。
3. 配置设备上各接口的 EFM OAM 功能。
4. 在 SwitchB 上配置 EFM OAM 联动功能。

操作步骤

步骤 1 配置全局 EFM OAM 功能

#配置 SwitchA

```
<SwitchA> system-view
[SwitchA] efm enable
```

#配置 SwitchB

```
<SwitchB> system-view
[SwitchB] efm enable
```

#配置 SwitchC

```
<SwitchC> system-view
[SwitchC] efm enable
```

步骤 2 配置接口的工作模式

#配置 SwitchB

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] efm mode passive
[SwitchB-GigabitEthernet0/0/1] quit
```

#配置 SwitchC

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] bpdu enable
[SwitchC-GigabitEthernet0/0/2] efm mode passive
[SwitchC-GigabitEthernet0/0/2] quit
```

步骤 3 使能接口的 EFM OAM 功能

#配置 SwitchA

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] efm enable
[SwitchA-GigabitEthernet0/0/1] quit
```

#配置 SwitchB

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] efm enable
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] bpdu enable
[SwitchB-GigabitEthernet0/0/2] efm enable
[SwitchB-GigabitEthernet0/0/2] quit
```

#配置 SwitchC

版权所有 © 华为技术有限公司

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] efm enable
[SwitchC-GigabitEthernet0/0/2] quit
```

执行 **display efm session all** 查看 EFM OAM 的状态，显示为 detect，以 SwitchB 的显示为例：

```
[SwitchB] display efm session all
  Interface                EFM State                   Loopback Timeout
  ------------------------------------------------------------------------
  GigabitEthernet0/0/1     detect                      --
  GigabitEthernet0/0/2     detect                      --
```

步骤 4 配置 EFM OAM 与 EFM OAM 双向联动功能

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind efm interface gigabitethernet 0/0/1 efm interface gigabitethernet 0/0/2
```

在 OAM 管理视图下，执行命令 **display this** 查看联动的配置情况，显示为两个方向相反的单项联动配置信息：

```
[SwitchB-oam-mgr] display this
#
oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress efm interface GigabitEthernet0/0/2
 oam-bind ingress efm interface GigabitEthernet0/0/2 egress efm interface GigabitEthernet0/0/1
#
```

步骤 5 检查配置结果

在 SwitchC 上使能向终端发送调试信息功能。

```
<SwitchC> terminal logging
<SwitchC> terminal monitor
```

在关闭 SwitchA 的接口 SwitchC 的 GE0/0/1，模拟链路故障。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] shutdown
```

SwitchA 和 SwitchB 之间的故障可以通过联动机制传递给 SwitchC，SwitchC 上产生告警。

```
<SwitchC>
 Mar  9 2010 14:52:33 SwitchC %%01EFM/2/NONTHRESHOLD(l): OID 1.3.6.1.4.1.2011.5
.25.136.1.6.5 Non-threshold-crossing event occurred. (InterfaceName=GigabitEthernet0/0/1,
EventLogIndex=0, EventLogTimestamp=148983996, EventLogOui=[01.80.c2 (h
ex)], EventLogType=258, EventLogLocation=2, EventLogRunningTotal=0 3)
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 efm
#
interface GigabitEthernet0/0/1
 efm enable
 bpdu enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
```


版权所有 © 华为技术有限公司

```
#
 efm
#
interface GigabitEthernet0/0/1
 efm mode passive
 efm enable
 bpdu enable
#
interface GigabitEthernet0/0/2
 efm enable
#
oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress efm interface
GigabitEthernet0/0/2
 oam-bind ingress efm interface GigabitEthernet0/0/2 egress efm interface
GigabitEthernet0/0/1
#
 return
```

- SwitchC 的配置文件

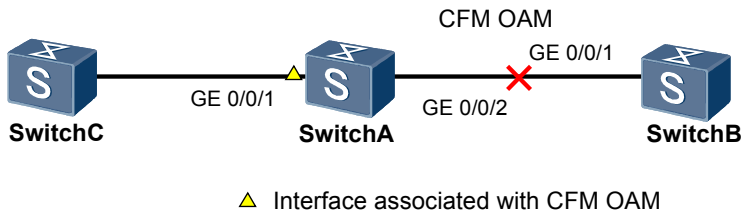
```
#
 sysname SwitchC
#
 efm
#
interface GigabitEthernet0/0/2
 efm mode passive
 efm enable
 bpdu enable
#
return
```

配置以太网 CFM 与接口联动（触发与 CFM 联动的接口物理状态变为 Down）示例

组网环境

如图 9-38，CFM 分别用于直连链路和多跳链路检测。两台设备 SwitchA 和 SwitchB 之间配置了以太网 CFM 功能，并配置了 CFM 和 SwitchA 的接口 GE0/0/1 联动。在 SwitchA 上，当 CFM OAM 模块检测到和 SwitchB 之间有连通性故障时，OAM 管理模块直接关闭该接口 GE0/0/1，以使 SwitchA 的对端设备感知到此故障。

图 9-38 以太网 CFM 和接口联动组网图



配置思路

按照如下思路配置以太 CFM 与接口联动示例：

1. 在 SwitchA 上和 SwitchB 上分别配置以太 CFM
2. 在 SwitchA 上配置以太 CFM 与 GE0/0/1 的联动功能

版权所有 © 华为技术有限公司

操作步骤

步骤 1 创建 VLAN，配置接口加入 VLAN

#配置 SwitchA

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
```

#配置 SwitchB

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 2 配置以太 CFM 功能

#在 SwitchA 上全局使能以太 CFM 功能

```
[SwitchA] cfm enable
```

#SwitchA 上创建 MD、MA、MEP 和 RMEP

```
[SwitchA]cfm md md1
[SwitchA-md-md1]ma ma1
[SwitchA-md-md1-ma-ma1] map vlan 10
[SwitchA-md-md1-ma-ma1] ccm-interval 10000
[SwitchA-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/2 outward
[SwitchA-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchA-md-md1-ma-ma1] mep ccm-send enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

#在 SwitchB 上全局使能以太 CFM 功能

```
[SwitchB] cfm enable
```

#SwitchB 上创建 MD、MA、MEP 和 RMEP

```
[SwitchB]cfm md md1
[SwitchB-md-md1]ma ma1
[SwitchB-md-md1-ma-ma1] map vlan 10
[SwitchB-md-md1-ma-ma1] ccm-interval 10000
[SwitchB-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[SwitchB-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchB-md-md1-ma-ma1] mep ccm-send enable
[SwitchB-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

检查配置结果

SwitchA 和 SwitchB 上的以太网 CFM 功能配置成功后，在 SwitchA 或 SwitchB 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，显示结果如下：

```
[SwitchB]display cfm mep md md1
The total number of MEPs is : 1
```


版权所有 © 华为技术有限公司

```
-------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 MEP ID             : 1
 Vlan ID            : 10
 VSI Name           : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
[SwitchB] display cfm remote-mep md md1
The total number of RMEPs is 1
 MD Name              : md1
 Level                : 0
 MA Name              : ma1
 RMEP ID              : 2
 Vlan ID              : 10
 VSI Name             : --
 MAC                  : --
 CCM Receive          : enabled
 Trigger-If-Down      : disabled
 CFM Status           : up
 Alarm Status         : RemoteAlarm
```

步骤 3 配置以太 CFM 与接口联动功能

#配置 SwitchA 上以太 CFM 与接口联动功能

```
[SwitchA] oam-mgr
[SwitchA-oam-mgr] oam-bind cfm md md1 ma ma1 trigger if-down interface gigabitethernet 0/0/1
[SwitchA-oam-mgr] quit
```

步骤 4 检查配置结果

关闭 SwitchA 的接口 0GE/0/2

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] shutdown
[SwitchA-GigabitEthernet0/0/2] quit
```

关闭 SwitchA 的接口后，OAM 模块会把故障传递到 GE0/0/1 接口，GE0/0/1 接口状态变为 TRIGGER DOWN (1AG)。

```
[SwitchA] display interface gigabitethernet 0/0/1

GigabitEthernet0/0/1 current state : TRIGGER DOWN (1AG)
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port,PVID :    1,The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-8211-1111
Port Mode: COMBO AUTO
Current Work Mode: COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: DISABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -
Input:  0 packets, 0 bytes
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
CRC            :                  0,Giants             :                  0
Jabbers        :                  0,Throttles          :                  0
Runts          :                  0,DropEvents         :                  0
Alignments     :                  0,Symbols            :                  0
Ignoreds       :                  0,Frames             :                  0
Discard        :                  0,Total Error        :                  0
Output:  0 packets, 0 bytes
```


版权所有 © 华为技术有限公司

```
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
Collisions     :                  0,Deferreds          :                  0
Late Collisions:                  0,ExcessiveCollisions:                  0
Buffers Purged :                  0
Discard        :                  0,Total Error        :                  0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

----结束

任务示例

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 10
#
cfm enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass 10
#
 cfm md md1
  ma ma1
   map vlan 10
   ccm-interval 10000
   mep mep-id 2 interface GigabitEthernet0/0/2 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
#
oam-mgr
 oam-bind ingress interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1
 oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface GigabitEthernet0/0/1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass 10
#
 cfm md md1
  ma ma1
   map vlan 10
   ccm-interval 10000
   mep mep-id 1 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

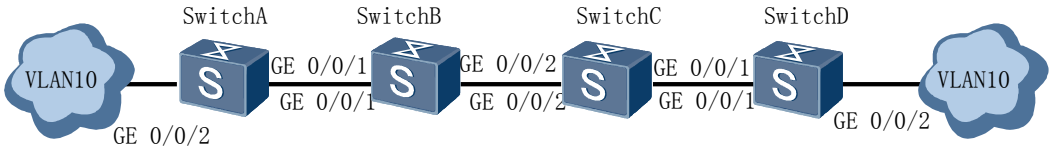

版权所有 © 华为技术有限公司

配置 EFM OAM 和以太网 CFM 联动示例

组网需求

如图 9-39 所示，为了实现端到端链路故障检测，在 SwitchA 和 SwitchB 之间配置 EFM OAM，在 SwitchB 与 SwitchC 之间配置以太网 CFM，SwitchC 与 SwitchD 之间配置 EFM OAM。当 SwitchA 与 SwitchB 之间有链路故障发生时，触发以太网 CFM 向远端 SwitchD 设备发故障告警。当 SwitchC 与 SwitchD 之间有链路故障发生时，触发以太网 CFM 向远端 SwitchA 设备发故障告警。

图 9-39 配置 EFM 和 CFM 联动示例组网图



配置思路

采用如下的思路配置 EFM OAM 和以太网 CFM 联动功能：

1. 创建 VLAN，并将相关接口加入对应的 VLAN。
2. 在 SwitchA 和 SwitchB 之间配置 EFM OAM 功能。
3. 在 SwitchB 和 SwitchC 之间配置以太网 CFM 功能。
4. 在 SwitchC 和 SwitchD 之间配置 EFM OAM 功能。
5. 在 SwitchB 和 SwitchC 上配置 EFM OAM 和以太网 CFM 的联动功能。

操作步骤

步骤 1 创建 VLAN10，并将相关接口加入对应的 VLAN。

步骤 2 配置 SwitchA 和 SwitchB 的 EFM OAM 功能。

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] efm enable
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
[SwitchA-GigabitEthernet0/0/1] efm mode passive
[SwitchA-GigabitEthernet0/0/1] efm enable
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] efm enable
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] bpdu enable
[SwitchB-GigabitEthernet0/0/1] efm enable
[SwitchB-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

步骤 3 配置 SwitchB 和 SwitchC 之间的以太网 CFM 功能。

配置 SwitchB。

```
[SwitchB] cfm enable
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] map vlan 10
[SwitchB-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/2 outward
[SwitchB-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchB-md-md1-ma-ma1] mep ccm-send enable
[SwitchB-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchB-md-md1-ma-ma1] return
```

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] cfm enable
[SwitchC] cfm md md1
[SwitchC-md-md1] ma ma1
[SwitchC-md-md1-ma-ma1] map vlan 10
[SwitchC-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/2 outward
[SwitchC-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchC-md-md1-ma-ma1] mep ccm-send enable
[SwitchC-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchC-md-md1-ma-ma1] return
```

步骤 4 配置 SwitchC 和 SwitchD 之间的 EFM OAM 功能。

配置 SwitchC。

```
[SwitchC] efm enable
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] bpdu enable
[SwitchC-GigabitEthernet0/0/1] efm enable
[SwitchC-GigabitEthernet0/0/1] quit
```

配置 SwitchD。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] efm enable
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] bpdu enable
[SwitchD-GigabitEthernet0/0/1] efm mode passive
[SwitchD-GigabitEthernet0/0/1] efm enable
[SwitchD-GigabitEthernet0/0/1] quit
```

步骤 5 配置 EFM OAM 和以太网 CFM 的联动。

配置 SwitchA 与 SwitchB 之间的 EFM OAM 和 SwitchB 与 SwitchC 之间的以太网 CFM 的双向联动。

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind cfm md md1 ma ma1 efm interface gigabitethernet 0/0/1
[SwitchB-oam-mgr] quit
```

配置 SwitchB 与 SwitchC 之间的以太网 CFM 和 SwitchC 与 SwitchD 之间的 EFM OAM 的双向联动。

```
[SwitchC] oam-mgr
[SwitchC-oam-mgr] oam-bind cfm md md1 ma ma1 efm interface gigabitethernet 0/0/1
[SwitchC-oam-mgr] quit
```

步骤 6 检查配置结果。

在 SwitchD 上使能向终端发送调试信息功能。

版权所有 © 华为技术有限公司

```
<SwitchD> terminal logging
 <SwitchD> terminal monitor
```

在关闭 SwitchA 的接口 GE0/0/1，模拟链路故障。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] shutdown
[SwitchA-GigabitEthernet0/0/1] quit
```

SwitchA 和 SwitchB 之间 EFM OAM 检测到的故障，可以通过以太网 CFM 通告给 SwitchC 和 SwitchD 之间的 EFM OAM。

```
<SwitchD>
Nov 23 2007 18:31:27-05:00 SwitchD %%01EFM/2/NONTHRESHOLD(l)[0]:OID 1.3.6.1.4.
1.2011.5.25.136.1.6.5 Non-threshold-crossing event occurred. (InterfaceName=GigabitEthernet0/0/1,
EventLogIndex=0, EventLogTimestamp=7357971, EventLogOui=[01.80
.c2 (hex)], EventLogType=258, EventLogLocation=1, EventLogRunningTotal=0 1)
Nov 23 2007 18:31:27-05:00 SwitchD %%01OAMMGR/4/CFM_TO_EFM(l)[1]:802.1AG notif
ied malfunction to 802.3AH. (Ma=ma1, Md=md1, InterfaceName=GigabitEthernet0/0/1,
 FaultState=1)
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
efm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 efm mode passive
 efm enable
 bpdu enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10
#
efm enable
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 efm enable
 bpdu enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
 cfm md md1
  ma ma1
```


版权所有 © 华为技术有限公司

```
   map vlan 10
   mep mep-id 1 interface gigabitethernet0/0/2 outward
   mep ccm-send enable
   remote-mep mep-id 2
   remote-mep ccm-receive enable
#
oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1
 oam-bind ingress cfm md md1 ma ma1 egress efm interface GigabitEthernet0/0/1

#
return
```

- SwitchC 配置文件

```
#
 sysname SwitchC
#
vlan batch 10
#
efm enable
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 efm enable
 bpdu enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
 cfm md md1
  ma ma1
   map vlan 10
   mep mep-id 2 interface GigabitEthernet0/0/2 outward
   mep ccm-send enable
   remote-mep mep-id 1
   remote-mep ccm-receive enable
#
 oam-mgr
 oam-bind ingress efm interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1
 oam-bind ingress cfm md md1 ma ma1 egress efm interface GigabitEthernet0/0/1
#
return
```

- SwitchD 配置文件

```
#
 sysname SwitchD
#
 vlan batch 10
#
efm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 efm mode passive
 efm enable
 bpdu enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

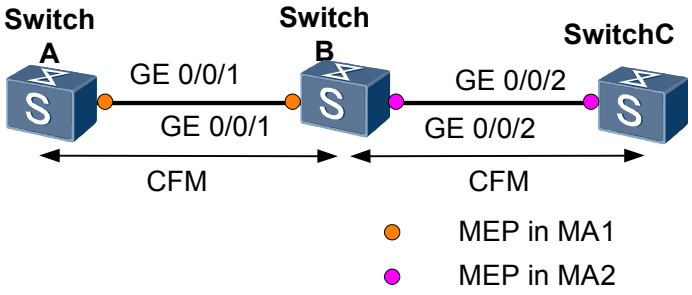

版权所有 © 华为技术有限公司

配置以太网 CFM 与以太网 CFM 联动示例

组网需求

如图 9-40 所示，在 SwitchA 和 SwitchB 之间配置以太网 CFM，在 SwitchB 与 SwitchC 之间配置以太网 CFM。当 SwitchA 与 SwitchB 之间有链路故障发生时，触发以太网 CFM 向远端 SwitchC 设备发故障告警。

图 9-40 配置以太 CFM 和以太 CFM 联动组网图



配置思路

采用如下的思路配置以太网 CFM 和以太 CFM 联动功能：

1. 创建 VLAN，并将相关接口加入对应的 VLAN。
2. 在 SwitchA 和 SwitchB、SwitchB 和 SwitchC 之间分别配置以太 CFM 功能。
3. 在 SwitchB 和 SwitchC 上配置以太网 CFM 的联动功能。

操作步骤

步骤 1 创建 VLAN，并将相关接口加入对应的 VLAN。

步骤 2 配置 SwitchA 和 SwitchB 之间的以太网 CFM 功能。

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] cfm enable
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] map vlan 10
[SwitchA-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[SwitchA-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchA-md-md1-ma-ma1] mep ccm-send enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] cfm enable
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[SwitchB-md-md1-ma-ma1] map vlan 10
[SwitchB-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/1 outward
[SwitchB-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchB-md-md1-ma-ma1] mep ccm-send enable
[SwitchB-md-md1-ma-ma1] remote-mep ccm-receive enable
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 3 配置 SwitchB 和 SwitchC 之间的以太网 CFM 功能。

配置 SwitchB。

```
[SwitchB] cfm enable
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma2
[SwitchB-md-md1-ma-ma2] map vlan 20
[SwitchB-md-md1-ma-ma2] mep mep-id 1 interface gigabitethernet 0/0/2 outward
[SwitchB-md-md1-ma-ma2] remote-mep mep-id 2
[SwitchB-md-md1-ma-ma2] mep ccm-send enable
[SwitchB-md-md1-ma-ma2] remote-mep ccm-receive enable
[SwitchB-md-md1-ma-ma2] quit
[SwitchB-md-md1] quit
```

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] cfm enable
[SwitchC] cfm md md1
[SwitchC-md-md1] ma ma2
[SwitchC-md-md1-ma-ma2] map vlan 20
[SwitchC-md-md1-ma-ma2] mep mep-id 2 interface gigabitethernet 0/0/2 outward
[SwitchB-md-md1-ma-ma2] remote-mep mep-id 1
[SwitchC-md-md1-ma-ma2] mep ccm-send enable
[SwitchC-md-md1-ma-ma2] remote-mep ccm-receive enable
[SwitchC-md-md1-ma-ma2] quit
[SwitchC-md-md1] quit
```

在 SwitchB 上执行 **display cfm remote-mep** 查看 CFM 状态，显示结果为 UP。

```
[SwitchB] display  cfm remote-mep
The total number of RMEPs is : 2
------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 1
 Vlan ID            : 10
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarms

 MD Name            : md1
 Level              : 0
 MA Name            : ma2
 RMEP ID            : 2
 Vlan ID            : 20
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarms
```

步骤 4 配置以太 CFM 和以太网 CFM 的联动。

版权所有 © 华为技术有限公司

配置 SwitchA 与 SwitchB 之间的以太 CFM 和 SwitchB 与 SwitchC 之间的以太网 CFM 的双向联动。

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind cfm md md1 ma ma1 cfm md md1 ma ma2
[SwitchB-oam-mgr] quit
```

步骤 5 检查配置结果。

关闭 SwitchB 的接口 GE0/0/2，在 SwitchA 上执行命令 **display cfm remote-mep** 查看 SwitchA 和 SwitchB 之间的 CFM 状态，显示 CFM 的状态为 Down。

```
[SwitchA]display  cfm remote-mep
The total number of RMEPs is : 1
------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 2
 Vlan ID            : 10
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : RemoteAlarms
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
 cfm md md1
  ma ma1
   map vlan 10
   mep mep-id 1 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10 20
#
cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 20
#
  cfm md md1
  ma ma1
   map vlan 10
   mep mep-id 2 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
  ma ma2
   map vlan 20
   mep mep-id 1 interface GigabitEthernet0/0/2 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
#
oam-mgr
 oam-bind ingress cfm md md1 ma ma1 egress cfm md md1 ma ma2
 oam-bind ingress cfm md md1 ma ma2 egress cfm md md1 ma ma1
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 20
#
cfm enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
 cfm md md1
  ma ma2
   map vlan 20
   mep mep-id 2 interface GigabitEthernet0/0/2 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
#
return
```

配置以太网 CFM 与 RRPP 联动示例

组网需求

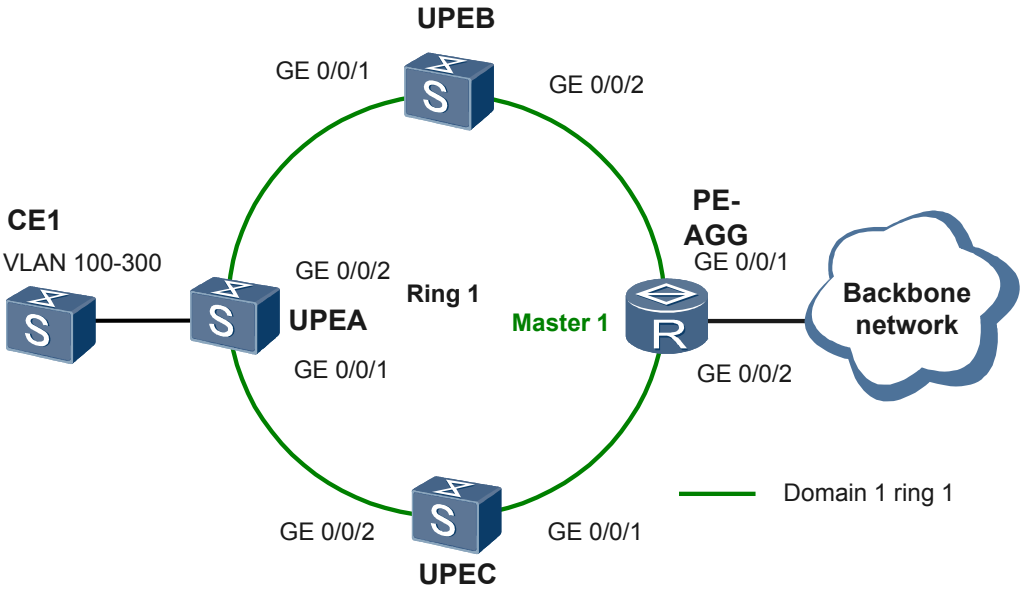
如图 9-41 所示，UPEA、UPEB、UPEC 和 PE-AGG 组成 RRPP 单环。

从 CE 处接入的 VLAN 范围是 VLAN100 ～ 300。报文在域 1 环 1 中传输。

在 UPEA 和 PE-AGG 之间配置以太 CFM 检测链路故障，并配置以太 CFM 与 RRPP 环的主副接口联动。

版权所有 © 华为技术有限公司

图 9-41 配置以太 CFM 和 RRPP 多实例联动组网图



域 1 的保护 VLAN 以及保护 VLAN 所属实例详见表 9-10。

表 9-10 实例与保护 VLAN 的映射关系表

Ring ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
域 1	VLAN 5、VLAN 6	Instance 1	VLAN 100 ～ 300	Instance 1

环中的主节点以及主节点上的主、副端口详见表 9-11。

表 9-11 主节点以及主、副端口信息表

Ring ID	Master Node	Primary Port	Secondary Port
域 1 环 1	PE-AGG	GE0/0/1	GE0/0/2

配置思路

采用如下的思路配置 RRPP 多实例单环示例：

1. 配置实例 1 映射 VLAN100 ～ 300。
2. 将 UPEA、UPEB、UPEC 和 PE-AGG 配置为域 1 的环 1。
3. 配置域 1 的保护 VLAN 和控制 VLAN。
4. 配置 PE-AGG 为域 1 环 1 的主节点，UPEA、UPEB、UPEC 为传输节点。

版权所有 © 华为技术有限公司

5. 配置 PE-AGG 和 UPEA 上的以太 CFM 功能，分别对 PE-AGG 和 UPEA 间的两条链路进行故障检测。
6. 在 PE-AGG 上配置以太 CFM 与 RRPP 主副端口的联动。

数据准备

为完成此配置例，需准备如下的数据：

- 实例 ID
- 保护 VLAN 范围
- 控制 VLAN ID
- RRPP 接口的接口编号

操作步骤

步骤 1 创建实例

- 配置 UPEA

  # 在 UPEA 上创建数据 VLAN 100 ～ 300。

  ```
  <Quidway> system-view
  [Quidway] sysname UPEA
  [UPEA] vlan batch 100 to 300
  ```

  # 创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

  ```
  [UPEA] stp region-configuration
  [UPEA-mst-region] instance 1 vlan 5 6 100 to 300
  ```

  # 激活配置。

  ```
  [UPEA-mst-region] active region-configuration
  [UPEA-mst-region] quit
  ```

- 配置 UPEB

  # 在 UPEB 上创建数据 VLAN 100 ～ 300。

  ```
  <Quidway> system-view
  [Quidway] sysname UPEB
  [UPEB] vlan batch 100 to 300
  ```

  # 创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 300。

  ```
  [UPEB] stp region-configuration
  [UPEB-mst-region] instance 1 vlan 5 6 100 to 300
  ```

  # 激活配置。

  ```
  [UPEB-mst-region] active region-configuration
  [UPEB-mst-region] quit
  ```

- 配置 UPEC

  # 在 UPEC 上创建数据 VLAN 100 ～ 300。

  ```
  <Quidway> system-view
  [Quidway] sysname UPEC
  [UPEC] vlan batch 100 to 300
  ```

  # 创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 300。

  ```
  [UPEC] stp region-configuration
  [UPEC-mst-region] instance 1 vlan 5 6 100 to 300
  ```

  # 激活配置。

  ```
  [UPEC-mst-region] active region-configuration
  [UPEC-mst-region] quit
  ```


版权所有 © 华为技术有限公司

- 配置 PE-AGG

  # 在 PE-AGG 上创建数据 VLAN 100 ～ 300。

```
<Quidway> system-view
[Quidway] sysname PE-AGG
[PE-AGG] vlan batch 100 to 300
```

  # 创建实例 1，对应域 1 的控制 VLAN5、VLAN6 和数据 VLAN100 ～ 200。

```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 5 6 100 to 300
```

  # 激活配置。

```
[PE-AGG-mst-region] active region-configuration
[PE-AGG-mst-region] quit
```

- 检查配置结果

  经过以上配置，执行以下操作查看实例与 VLAN 的映射关系，以 UPEA 为例。

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :001820000083
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
      1       5 to 6, 100 to 300
```

步骤 2 配置加入 RRPP 环的端口

- 配置 UPEA

  # 去使能 UPEA 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEA] interface gigabitethernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port link-type trunk
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface gigabitethernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port link-type trunk
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- 配置 UPEB

  # 去使能 UPEB 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEB] interface gigabitethernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port link-type trunk
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface gigabitethernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port link-type trunk
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
```

- 配置 UPEC

  # 去使能 UPEC 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[UPEC] interface gigabitethernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port link-type trunk
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
```


版权所有 © 华为技术有限公司

```
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface gigabitethernet 0/0/2
[UPEC-GigabitEthernet0/0/2]port link-type trunk
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
```

- 配置 PE-AGG

  # 去使能 PE-AGG 上即将加入 RRPP 环的接口的 STP 功能。配置端口允许 VLAN100 ～ 300 的报文通过。

```
[PE-AGG] interface gigabitethernet 0/0/1
[PE-AGG-GigabitEthernet0/0/1]port link-type trunk
[PE-AGG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/1] stp disable
[PE-AGG-GigabitEthernet0/0/1] quit
[PE-AGG] interface gigabitethernet 0/0/2
[PE-AGG-GigabitEthernet0/0/2] port link-type trunk
[PE-AGG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/2] stp disable
[PE-AGG-GigabitEthernet0/0/2] quit
```

步骤 3 创建 RRPP 域，配置保护 VLAN 和控制 VLAN。

- 配置 UPEA

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

- 配置 UPEB

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

- 配置 UPEC

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

- 配置 PE-AGG

  # 配置域 1 的保护 VLAN 为 instance 1 映射的 VLAN。控制 VLAN 为 VLAN5。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 5
[PE-AGG-rrpp-domain-region1] quit
```

步骤 4 创建 RRPP 环

- 配置 UPEA

  # 配置 UPEA 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

- 配置 UPEB

  # 配置 UPEB 为域 1 环 1 的传输节点，并指定主副接口。

版权所有 © 华为技术有限公司

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitehternet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

- 配置 UPEC

  # 配置 UPEC 为域 1 环 1 的传输节点，并指定主副接口。

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

- 配置 PE-AGG

  # 配置 PE-AGG 为域 1 环 1 的主节点，主接口为 GE0/0/1，副接口为 GE0/0/2。

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port gigabitethernet 0/0/1 secondary-port gigabitethernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

步骤 5 使能 RRPP 协议

在完成配置 RRPP 环后，需要在环上的每个节点上使能 RRPP 协议，这样 RRPP 环才能够被激活，配置步骤如下：

- 配置 UPEA

  # 使能 RRPP 协议。

```
[UPEA] rrpp enable
```

- 配置 UPEB

  # 使能 RRPP 协议。

```
[UPEB] rrpp enable
```

- 配置 UPEC

  # 使能 RRPP 协议。

```
[UPEC] rrpp enable
```

- 配置 PE-AGG

  # 使能 RRPP 协议。

```
[PE-AGG] rrpp enable
```

  经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。以 UPEA 和 PE-AGG 为例。

- 在 UPEA 上执行 **display rrppbrief** 或者 **display rrpp verbose domain** 命令，查看结果如下：

  #查看 UPEA 的 RRPP 简要信息

```
[UPEA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)
```


版权所有 © 华为技术有限公司

```
 Ring  Ring   Node  Primary                 Secondary/Edge          Is
 ID    Level  Mode  Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1     0      T     GigabitEthernet0/0/1          GigabitEthernet0/0/2          Yes
```

UPEA 上 RRPP 已经使能，在域 1 中的主控制 VLAN 为 5，保护 VLAN 为 Instance 1，UPEA 为环 1 的传输节点。主端口为 0GE/0/1，副端口为 0GE/0/2。

查看 UPEA 在域 1 中的详细信息。

```
[UPEA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
ello Timer    : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                      Is Active : Yes
Primary port  : GigabitEthernet0/0/1              Port status: UP
Secondary port: GigabitEthernet0/0/2              Port status: UP
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。UPEA 在域 1 中是传输节点，节点状态为 LinkUp。UPEA 的上已经使能了 RRPP 协议。

#查看 PE-AGG 上 RRPP 的简要信息

```
[PE-AGG] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                      Port                  Enabled
 ------------------------------------------------------------------------------
 1      0       M         GigabitEthernet0/0/1           GigabitEthernet0/0/2          Yes
```

可以看到 PE-AGG 上已经使能了 RRPP 协议。在域 1 中的主控制 VLAN 为 5，保护 VLAN 为 Instance 1，PE-AGG 为环 1 的主节点。主端口为 GE0/0/1，副端口为 GE0/0/2。

#查看 PE-AGG 在域 1 中的详细信息

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
ello Timer    : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1              Port status: UP
Secondary port: GigabitEthernet0/0/2              Port status: BLOCKED
```

可以看到域 1 的控制 VLAN 是 VLAN5，保护 VLAN 是 Instance 1。PE-AGG 在域 1 中是主节点，节点状态为 Complete。主端口是 GE0/0/1，副端口是 GE0/0/2。

版权所有 © 华为技术有限公司

步骤 6 配置以太 CFM

配置 UPEA

```
[UPEA] cfm md md1
[UPEA-md-md1] ma ma1
[UPEA-md-md1-ma-ma1]  map vlan 100
[UPEA-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/2 outward
[UPEA-md-md1-ma-ma1] remote-mep mep-id 2
[UPEA-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[UPEA-md-md1-ma-ma1] mep ccm-send enable
[UPEA-md-md1-ma-ma1] quit
[UPEA-md-md1] ma ma2
[UPEA-md-md1-ma-ma2]  map vlan 100
[UPEA-md-md1-ma-ma2] mep mep-id 3 interface gigabitethernet 0/0/1 outward
[UPEA-md-md1-ma-ma2] remote-mep mep-id 4
[UPEA-md-md1-ma-ma2] remote-mep ccm-receive mep-id 4 enable
[UPEA-md-md1-ma-ma2] mep ccm-send enable
[UPEA-md-md1-ma-ma2] quit
[UPEA-md-md1] quit
```

配置 PE-AGG

```
[PE-AGG] cfm md md1
[PE-AGG-md-md1] ma ma1
[PE-AGG-md-md1-ma-ma1]  map vlan 100
[PE-AGG-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/1 outward
[PE-AGG-md-md1-ma-ma1] remote-mep mep-id 1
[PE-AGG-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE-AGG-md-md1-ma-ma1] mep ccm-send enable
[PE-AGG-md-md1-ma-ma1] quit
[PE-AGG-md-md1] ma ma2
[PE-AGG-md-md1-ma-ma2]  map vlan 100
[PE-AGG-md-md1-ma-ma2] mep mep-id 4 interface gigabitethernet 0/0/2 outward
[PE-AGG-md-md1-ma-ma2] remote-mep mep-id 3
[PE-AGG-md-md1-ma-ma2] remote-mep ccm-receive mep-id 3 enable
[PE-AGG-md-md1-ma-ma2] mep ccm-send enable
[PE-AGG-md-md1-ma-ma2] quit
[PE-AGG-md-md1] quit
```

使用命令 **display cfm remote-mep** 在 UPEA 或者 PE-AGG 上查看以太 CFM 的状态，CFM 的状态显示为 up，以 PE-AGG 的显示为例：

```
[PE-AGG] display cfm remote-mep
The total number of RMEPs is : 2
------------------------------------------------

 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 1
 Vlan ID            : 100
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarms

 MD Name            : md1
 Level              : 0
 MA Name            : ma2
 RMEP ID            : 3
 Vlan ID            : 100
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarms
```


版权所有 © 华为技术有限公司

步骤 7 配置以太 CFM 与接口联动

#配置 PE-AGG

```
[PE-AGG] oam-mgr
[PE-AGG-oam-mgr] oam-bind cfm md md1 ma ma1 trigger if-down interface gigabitethernet 0/0/1
[PE-AGG-oam-mgr] oam-bind cfm md md1 ma ma2 trigger if-down interface gigabitethernet 0/0/2
[PE-AGG-oam-mgr] quit
```

步骤 8 检查配置结果

关闭 UPEB 的 GE0/0/1 接口模拟链路，在 PE-AGG 上使用命令 **display cfm remote-mep** 查看 CFM 状态，显示如下：

```
[PE-AGG] display cfm remote-mep
The total number of RMEPs is : 2
------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 1
 Vlan ID            : 100
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : RemoteAlarms

 MD Name            : md1
 Level              : 0
 MA Name            : ma2
 RMEP ID            : 3
 Vlan ID            : 100
 VSI Name           : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : up
 Alarm Status       : RemoteAlarms
```

在 PE-AGG 上执行命令 **display interface** 查看 GE0/0/1 的状态，显示为 **TRIGGER DOWN (1AG)**。

```
[PE-AGG] display interface gigabitethernet0/0/1
GigabitEthernet0/0/1 current state : TRIGGER DOWN (1AG)
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port,PVID :    1,The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-8211-1111
Port Mode: COMBO AUTO
Current Work Mode: COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: DISABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -
Input:  0 packets, 0 bytes
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
CRC            :                  0,Giants             :                  0
Jabbers        :                  0,Throttles          :                  0
Runts          :                  0,DropEvents         :                  0
Alignments     :                  0,Symbols            :                  0
Ignoreds       :                  0,Frames             :                  0
Discard        :                  0,Total Error        :                  0
Output:  0 packets, 0 bytes
```


版权所有 © 华为技术有限公司

```
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
Collisions     :                  0,Deferreds          :                  0
Late Collisions:                  0,ExcessiveCollisions:                  0
Buffers Purged :                  0
Discard        :                  0,Total Error        :                  0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

在 PE-AGG 上执行命令 **display rrpp verbose domain 1** 查看 RRPP 的环状态和接口状态，显示如下：

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
ello Timer    : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Failed
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1              Port status: DOWN
Secondary port: GigabitEthernet0/0/2              Port status: UP
```

Ring 的状态变为 Failed，副端口的状态由 BLOCKED 变为 UP。

重新开启 UPEB 的 GE0/0/1 接口，PE-AGG 上 CFM 的状态变为 UP，在 PE-AGG 上执行命令 **display rrpp verbose domain 1** 查看 RRPP 的环状态和接口状态，Ring 的状态变为 Complete，显示如下：

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
ello Timer    : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                Is Active : Yes
Primary port  : GigabitEthernet0/0/1              Port status: UP
Secondary port: GigabitEthernet0/0/2              Port status: BLOCKED
```

----结束

配置文件

- UPEA 的配置文件

```
#
sysname UPEA
#
vlan batch 5 to 6 100 to 300
#
 rrpp enable
#
 cfm enable
#
stp region-configuration
 instance 1 vlan 5 6 100 to 300
 active region-configuration
#
rrpp domain 1
```


版权所有 © 华为技术有限公司

```
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6  100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6  100 to 300
 stp disable
#
 cfm md md1
  ma ma1
   map vlan 100
   mep mep-id 1 interface GigabitEthernet0/0/2 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
  ma ma2
   map vlan 100
   mep mep-id 3 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 3 enable
   remote-mep mep-id 4
   remote-mep ccm-receive mep-id 4 enable
#
oam-mgr
 oam-bind ingress interface GigabitEthernet0/0/2 egress cfm md md1 ma ma1
 oam-bind ingress interface GigabitEthernet0/0/1 egress cfm md md1 ma ma2
 oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface GigabitEthernet0/0/2
 oam-bind ingress cfm md md1 ma ma2 trigger if-down egress interface GigabitEthernet0/0/1
#
return
```

- UPEB 的配置文件

```
#
sysname UPEB
#
vlan batch 5 to 6 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 6 100 to 200
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
return
```

- UPEC 的配置文件

版权所有 © 华为技术有限公司

```
#
sysname UPEC
#
vlan batch 5 to 6 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 6 100 to 200
 active region-configuration
#
rrpp domain 1
control-vlan 5
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2
level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
Return
```

- PE-AGG 的配置文件

```
#
sysname PE-AGG
#
 vlan batch 5 to 6 100 to 300
#
 rrpp enable
#
 cfm enable
#
stp region-configuration
 instance 1 vlan 5 6 100 to 200
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2
level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 100 to 300
 stp disable
#
 cfm md md1
  ma ma1
   map vlan 100
   mep mep-id 2 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
  ma ma2
   map vlan 100
```


版权所有 © 华为技术有限公司

```
   mep mep-id 4 interface GigabitEthernet0/0/2 outward
   mep ccm-send mep-id 4 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
#
oam-mgr
 oam-bind ingress interface GigabitEthernet0/0/1 egress cfm md md1 ma ma1
 oam-bind ingress interface GigabitEthernet0/0/2 egress cfm md md1 ma ma2
 oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface GigabitEthernet0/0/1
 oam-bind ingress cfm md md1 ma ma2 trigger if-down egress interface GigabitEthernet0/0/2
#
return
```

9.5 Y.1731 配置

Y.1731 对 MEP 之间进行基于业务的丢包检测、时延统计，实现与 IEEE 802.1ag 类似的故障检测功能。

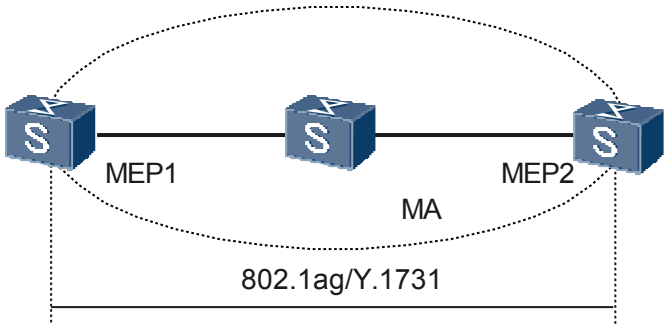
9.5.1 Y.1731 概述

Y.1731 作为 ITU-T 标准组织提出的 OAM 协议，能够实现城域以太网的端到端连通性检测、环回和链路跟踪外，还提供了性能管理（包括丢包率统计、帧时延统计、帧时延抖动统计、吞吐量统计）功能。

Y.1731 是由 ITU-T 标准组织提出的 OAM 协议，它不仅包含 IEEE802.1ag 所规定的内容，而且又增加了更多的 OAM 消息组合，包括 RDI（Remote Defect Indication），锁信号 LCK（Locked Signal），测试信号，自动保护切换 APS（Automatic Protection Switching），维护通信渠道 MCC（Maintenance Communication Channel），试验 EXP（Experimental OAM），供应商特定的 VSP（Vendor Specific OAM）故障管理以及用于性能监视的丢包管理 LM（Loss Measurement）和延迟评估 DM（Delay Measurement）等。

如图 9-42 所示，Y.1731 一般部署于 MEP 节点设备，用于端到端的业务故障快速检测和性能监视。

图 9-42 Y.1731 典型应用场景



当用户认为购买的以太网隧道业务出现了服务质量问题，或对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具进行检测。例如通过发送和接收 CCM 报文来计算丢包率统计，以及双向帧的延迟和抖动。

版权所有 © 华为技术有限公司

9.5.2 AC6605 支持的 Y.1731 特性

AC6605 支持的 Y.1731 特性包括：VLAN 单向延时统计功能、VLAN 双向时延统计功能。

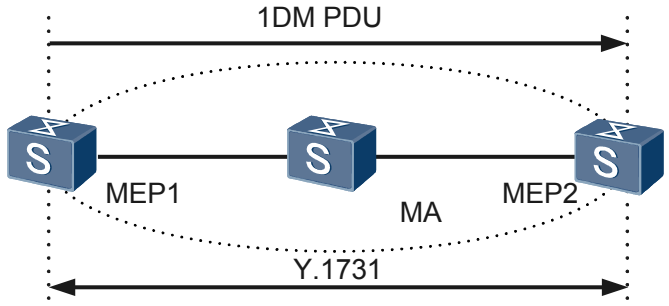
单向时延统计

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，Y.1731 特性只支持 standard2007 标准版本使用。所以在配置 Y.1731 前，必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本。

如图 9-43 所示，单向时延统计需要在点到点的 MEP 上进行，MEP 收到对端设备发送来的 DM 帧后，根据帧中携带的时间戳信息与本地时间信息计算出时延。此外，单向时延统计时，必需保证 MEP 节点之间的时钟同步。

图 9-43 单向时延统计组网图



单向时延统计是在端到端 MEP 之间进行，通过发送/接收 DM 报文进行计算。当单向时延统计功能配置成功后，MEP 将周期性地发送带有 TxTimeStampf（DM 传输时的时间戳）数值的 DM 帧。RMEP 接收到 DM 报文后，解析出 DM 报文中 TxTimeStampf 值，与自身接收 DM 报文的时间 RxTimef 进行比较，得出单向时延值。计算公式如下：

帧时延 = RxTimef － TxTimeStampf

通过上面公式中的帧时延还可以计算出帧时延变化，即帧时延抖动。

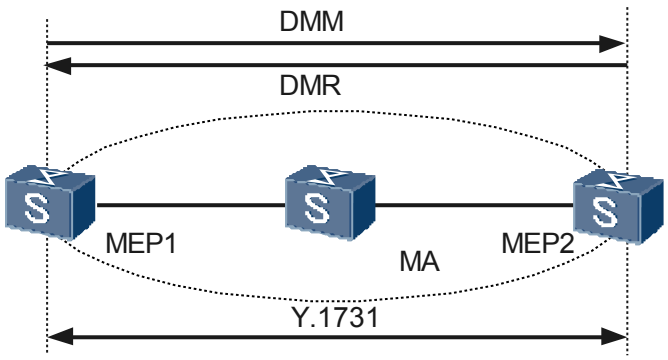
时延抖动：是对一对业务帧之间帧时延变化的度量，本次时延与上次时延之间的绝对差值。

双向时延统计

如果需要在一个指定的时间段内，对双向的业务流量时延进行统计时，可以使用双向时延统计功能。

版权所有 © 华为技术有限公司

图 9-44 双向时延统计图



双向时延统计是在端到端 MEP 之间进行，通过接收 DMM 帧和发送 DMR 帧进行计算。当双向时延统计功能配置成功后，MEP 将周期性地发送带有 TxTimeStampf（DM 传输时的时间戳）数值的 DMM 帧。RMEP 接收到 DMM 帧后，填充 DMM 帧接收的时间戳值 RxTimeStampf，然后修改帧的类型为 DMR 帧，并交换帧的目的 MAC 和源 MAC 发送出去，同时带上发送时间戳 TxTimeStampb。当 DMM 发送端收到 DMR 时与接收到 DMR 帧的时间 RxTimeb 进行比较，得出双向时延值。计算公式如下：

帧时延 = (RxTimeb － TxTimeStampf) － (TxTimeStampb － RxTimeStampf)

通过上面公式中的帧时延还可以计算出帧时延变化，即帧时延抖动。

时延抖动：是对一对业务帧之间帧时延变化的度量，本次时延与上次时延之间的绝对差值。

9.5.3 配置 VLAN 的单向时延统计功能

通过在 MA 内配置 VLAN 的单向时延统计功能，用户可以根据时延来评估业务提供的质量。

建立配置任务

在配置 VLAN 的单向时延统计功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要在一个指定的时间段内，对单向的业务流量时延进行统计时，可以使用单向时延统计功能。

单向时延统计需要在点到点的 MEP 上进行，MEP 收到对端设备发送来的 DM 报文后，根据报文中携带的时间戳信息与本地时间信息计算出时延。此外，单向时延统计时，必需保证 MEP 节点之间的时钟同步。

说明

在本端设备使能 VLAN 的单向时延统计功能之前，必须在对端设备上配置接收 DM 报文功能，用于单向时延统计。

版权所有 © 华为技术有限公司

前置任务

在 VLAN 的单向时延统计功能之前，需要完成以下任务：

- 配置时钟同步，配置过程请参见**配置 NTP**
- 配置 VLAN，配置过程请参见**配置 VLAN**
- **配置以太网 CFM 基本功能**

数据准备

在 VLAN 的单向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD 和 MA 的名称
2	MEP 的 ID、MEP 所在的接口名称和 MEP 的类型
3	与 MA 绑定的 VLAN ID 名称
4	（可选）单向时延告警门限值

配置 MA 与 VLAN 绑定

配置 MA 与 VLAN 绑定是配置 VLAN 的单向时延统计功能的首要步骤。

背景信息

请在配置 MEP 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm version** { **draft7** | **standard** }，切换 802.1ag 版本为 standard 版本。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，Y.1731 特性只支持 standard2007 标准版本使用。所以在配置 Y.1731 前，必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本。

注意

切换版本后，原来的 CFM 的所有配置将被删除，请谨慎使用。

步骤 3 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 4 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 5 执行命令 **map vlan** *vlan-id*，配置当前 MA 与 VLAN 进行绑定。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

（可选）配置单向时延告警门限

针对一个 MA 设置单向时延统计观察点，当单向时延超过设置的观察点就会触发告警。

背景信息

请在配置 MEP 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure one-way threshold** *threshold-value*，配置单向时延统计的告警门限值。

----结束

配置对端设备接收 DM 报文功能

只有使能对端设备接收 DM 报文，单向时延统计才有可能正常工作。

背景信息

请在 RMEP 所在的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure one-way receive**，配置对端设备接收 DM 报文功能。

----结束

使能 VLAN 的单向时延统计

打开 VLAN 的单向时延统计功能的开关，单向时延统计才能正常工作。

背景信息

通过指定 RMEP ID 或者目的 MAC 地址，DM 报文发送时间间隔、统计次数进行单向时延统计。

- 如果本端 MEP 没有学到 RMEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行单向时延统计。
- 如果本端 MEP 已经学到 RMEP 的 MAC 地址，则可以使用指定目的远端 MEP 号的方式进行单向时延统计。

版权所有 © 华为技术有限公司

单向时延统计是在端到端 MEP 之间进行，通过发送/接收 DM 报文进行计算。当单向时延统计功能配置成功后，MEP 将周期性地发送带有 TxTimeStampf（DM 传输时的时间戳）数值的 DM 帧。RMEP 接收到 DM 报文后，解析出 DM 报文中 TxTimeStampf 值，与自身接收DM 报文的时间 RxTimef 进行比较，得出单向时延值。计算公式如下：

帧时延 = RxTimef － TxTimeStampf

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure one-way** { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } **interval** *interval-value* **count** *count-value*，配置单向时延统计功能。

----结束

检查配置结果

VLAN 的单向时延统计功能配置成功后，可以查看 VLAN 单向时延统计信息。

前提条件

已经完成 VLAN 的单向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type oneway-delay md** *md-name* **ma** *ma-name* [**count** *count-value*]命令查看 Y.1731 的性能统计信息。

----结束

任务示例

配置成功后，在 MEP 所在的设备上执行 **display y1731 statistic-type** 命令，可以看到“Average delay”的值。

```
[SwitchB] display y1731 statistic-type oneway-delay md md1 ma ma1

01   1DM received  Delay:       41640 usec   Delay variation:          0 usec
02   1DM received  Delay:       43501 usec   Delay variation:       1861 usec
03   1DM received  Delay:        8787 usec   Delay variation:      34714 usec
04   1DM received  Delay:       43335 usec   Delay variation:      34548 usec
05   1DM received  Delay:       43333 usec   Delay variation:          2 usec
06   1DM received  Delay:       33993 usec   Delay variation:       9340 usec
07   1DM received  Delay:       43321 usec   Delay variation:       9328 usec
08   1DM received  Delay:       33511 usec   Delay variation:       9810 usec
09   1DM received  Delay:       21293 usec   Delay variation:      12218 usec
10   1DM received  Delay:       51967 usec   Delay variation:      30674 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 36468 usec, Average delay variation: 15832 usec
Best case delay: 8787 usec, Worst case delay: 51967 usec
```


版权所有 © 华为技术有限公司

9.5.4 配置 VLAN 的双向时延统计功能

通过在 MA 内配置 VLAN 的双向时延统计功能，用户可以根据时延来评估业务提供的质量。

建立配置任务

在配置 VLAN 的双向时延统计功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要在一个指定的时间段内，对双向的业务流量时延进行统计时，可以使用双向时延统计功能。

双向时延统计是在端到端的 MEP 之间进行，远端 MEP 收到对方发送的 DMM 报文后，填充接收 DMM 报文时的时间戳值，然后修改报文的类型为 DMR 报文，并交换报文的目的 MAC 和源 MAC 发送出去，同时带上发送时时间戳 TxTimeStampb。本端 MEP 接收到 DMR 报文后解析出携带的时间戳，从而对业务流量时延进行统计。

说明

在本端设备使能 VLAN 的双向时延统计功能之前，必须在对端设备上配置接收 DMM 报文功能，用于双向时延统计。

前置任务

在 VLAN 的双向时延统计功能之前，需要完成以下任务：

- 配置 VLAN，配置过程请参见**配置 VLAN**
- **配置以太网 CFM 基本功能**

数据准备

在 VLAN 的双向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD 和 MA 的名称
2	MEP 的 ID、MEP 所在的接口名称和 MEP 的类型
3	与 MA 绑定的 VLAN ID 名称
4	（可选）双向时延告警门限值

配置 MA 与 VLAN 绑定

配置 MA 与 VLAN 绑定是配置 VLAN 的单向时延统计功能的首要步骤。

背景信息

请在配置 MEP 的设备上进行以下配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm version** { **draft7** | **standard** }，切换 802.1ag 版本为 standard 版本。

说明

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，Y.1731 特性只支持 standard2007 标准版本使用。所以在配置 Y.1731 前，必须首先使用 cfm version 命令配置 802.1ag 为 standard2007 标准版本。

注意

切换版本后，原来的 CFM 的所有配置将被删除，请谨慎使用。

步骤 3 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 4 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 5 执行命令 **map vlan** *vlan-id*，配置当前 MA 与 VLAN 进行绑定。

----结束

（可选）配置双向时延告警门限

针对一个 MA 设置双时延统计观察点，当双向时延超过设置的观察点就会触发告警。

背景信息

请在配置 MEP 的两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure two-way threshold** *threshold-value*，配置双向时延统计的告警门限值。

----结束

配置双向接收 DMM 报文功能

只有使能两端设备接收 DMM 报文，双向时延统计才有可能正常工作。

背景信息

请在配置 MEP 的两端设备上进行以下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure two-way receive**，配置双向接收 DMM 报文功能。
只有使能两端设备接收 DMM 报文，双向时延统计才有可能正常工作。

----结束

使能 VLAN 的双向时延统计

打开 VLAN 的双向时延统计功能的开关，双向时延统计才能正常工作。

背景信息

通过指定 RMEP ID 或者目的 MAC 地址，DMM 文发送时间间隔、DMM 报文的发送个数进行双向时延统计。

- 如果本端 MEP 没有学到 RMEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行双向时延统计。
- 如果本端 MEP 已经学到 RMEP 的 MAC 地址，则可以使用指定目的远端 MEP 号的方式进行双向向时延统计。

双向时延是在端到端的 MEP 之间进行，通过接收 DMM 报文和发送 DMR 报文进行计算。当双向时延统计功能配置成功后，MEP 将周期性地发送带有 TxTimeStampf（DM 传输时的时间戳）数值的 DMM 帧。RMEP 接收到 DMM 报文后，填充 DMM 报文接收的时间戳值 RxTimeStampf，然后修改报文的类型为 DMR 报文，并交换报文的目的 MAC 和源 MAC 发送出去，同时带上发送时间戳 TxTimeStampb。当自身收到 DMR 时与接收到 DMR 报文的时间 RxTimeb 进行比较，得出双向时延值。计算公式如下：

帧时延 = (RxTimeb － TxTimeStampf) － (TxTimeStampb － RxTimeStampf)

请在配置 MEP 的两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **delay-measure two-way** { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } **interval** *interval-value* **count** *count-value*，配置双向时延统计功能。

----结束

检查配置结果

VLAN 的双向时延统计功能配置成功后，可以通过查看 VLAN 双向时延统计信息。

版权所有 © 华为技术有限公司

前提条件

已经完成 VLAN 的双向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type twoway-delay md** *md-name* **ma** *ma-name* [**count** *count-value*]命令查看 Y.1731 的性能统计信息。

----结束

任务示例

配置成功后，在 MEP 所在的设备上执行 **display y1731 statistic-type** 命令，可以看到“Average delay”的值。

```
<Quidway> display y1731 statistic-type twoway-delay md md1 ma ma1


01  DMR received from 0025-9e80-2494 Delay:      498 usec  Variation:       0 us
ec
02  DMR received from 0025-9e80-2494 Delay:      508 usec  Variation:      10 us
ec

--- Delay measurement statistics ---
Packets transmitted: 2, Valid packets received: 2
Average delay: 503 usec, Average delay variation: 10 usec
Best case delay: 498 usec, Worst case delay: 508 usec
```

9.5.5 配置举例

介绍 Y.1731 的各种组网举例。

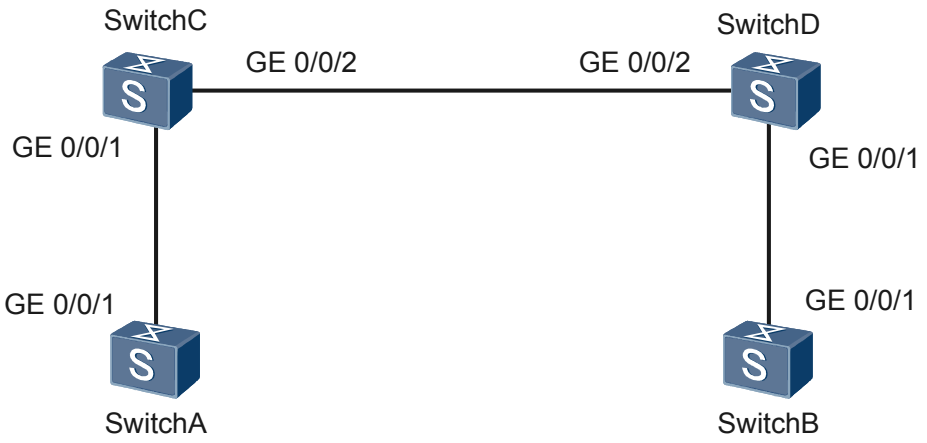
配置 VLAN 的单向时延统计功能示例

本示例中，当用户需要评估业务提供的质量时，通过在端到端的 MEP 之间配置单向时延功能，得知网络的性能。

组网需求

如图 9-45 所示，在 SwitchA 上部署单向时延统计功能，并且指定发送 DMM 报文的时间间隔为 10 秒，发送 DMM 报文的格式是 10 个。

图 9-45 配置 VLAN 的双向时延统计功能组网图



华为专有和保密信息
版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 VLAN 的双向时延统计功能：

1. 在 SwitchA、SwitchB、SwitchC 和 SwitchD 上配置 VLAN。
2. 在 SwitchA 和 SwitchB 上分别配置 MD 和 MA。
3. 在 SwitchA 和 SwitchB 上配置 OUTWARD 类型的 MEP。
4. 在 SwitchA 上配置单向时延告警门限值。
5. 在 SwitchA 上使能 VLAN 的单向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VLAN ID
- 单向时延告警门限值
- MD 和 MA 的名称

操作步骤

步骤 1 配置时钟同步

略，详细配置过程请参见**配置 NTP**

步骤 2 配置 VLAN

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet0/0/1] quit
```

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 2
[SwitchC-vlan2] quit
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet0/0/2] quit
```

配置 SwitchD。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan 2
[SwitchD-vlan2] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] port link-type trunk
[SwitchD-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchD-GigabitEthernet0/0/2] quit
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] port link-type trunk
[SwitchD-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchD-GigabitEthernet0/0/1] quit
```

步骤 3 配置以太网 CFM 的基本功能

配置 SwitchA。

```
[SwitchA] cfm version standard
[SwitchA] cfm enable
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] map vlan 2
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm version standard
[SwitchB] cfm enable
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] map vlan 2
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 4 配置 OUTWARD 类型的 MEP

配置 SwitchA。

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[SwitchA-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchA-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/1 outward
[SwitchB-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchB-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 5 在 SwitchA 配置单向时延告警门限值为 1000

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] delay-measure one-way threshold 1000
```


版权所有 © 华为技术有限公司

```
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

步骤 6 配置 VLAN 的单向时延统计功能

配置 SwitchA。

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] delay-measure one-way remote-mep mep-id 2 interval 10000 count 10
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] delay-measure one-way receive
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 7 检查配置结果

配置完成后，在 SwitchB 上执行 **display y1731 statistics-type oneway-delay md md1 ma ma1**，可以看到单向时延的性能统计信息。

```
[SwitchB] display y1731 statistic-type oneway-delay md md1 ma ma1

01   1DM received  Delay:       41640 usec   Delay variation:          0 usec
02   1DM received  Delay:       43501 usec   Delay variation:       1861 usec
03   1DM received  Delay:        8787 usec   Delay variation:      34714 usec
04   1DM received  Delay:       43335 usec   Delay variation:      34548 usec
05   1DM received  Delay:       43333 usec   Delay variation:          2 usec
06   1DM received  Delay:       33993 usec   Delay variation:       9340 usec
07   1DM received  Delay:       43321 usec   Delay variation:       9328 usec
08   1DM received  Delay:       33511 usec   Delay variation:       9810 usec
09   1DM received  Delay:       21293 usec   Delay variation:      12218 usec
10   1DM received  Delay:       51967 usec   Delay variation:      30674 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 36468 usec, Average delay variation: 15832 usec
Best case delay: 8787 usec, Worst case delay: 51967 usec
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 2
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1
  ma ma1
   map vlan 2
   mep mep-id 1 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
```


版权所有 © 华为技术有限公司

```
   delay-measure one-way threshold 1000
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 2
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1 outward
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1
  ma ma1
   map vlan 2
   mep mep-id 2 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   delay-measure one-way receive
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 2
#
interface GigabitEthernet0/0/1
  port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

配置 VLAN 的双向时延统计功能示例

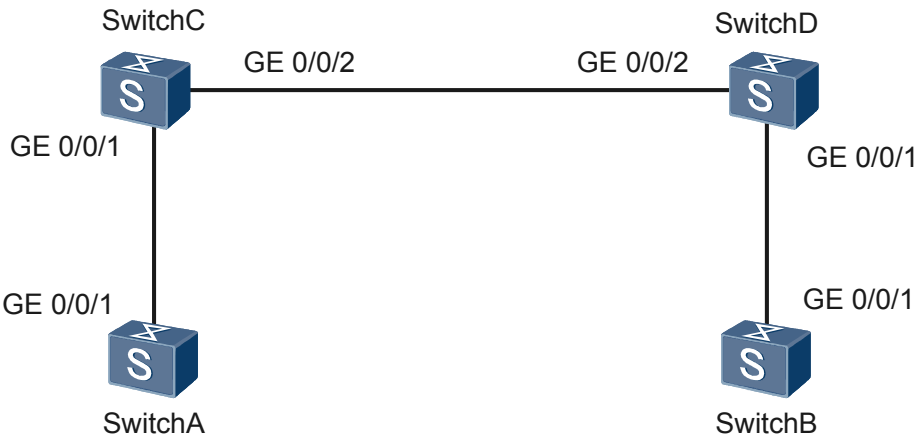
本示例中，当用户需要评估业务提供的质量时，通过在点到点的 MEP 之间配置双向时延功能，得知网络的性能。

版权所有 © 华为技术有限公司

组网需求

如图 9-46 所示，在 SwitchA 和 SwitchB 上部署双向时延功能，并且指定发送 DMM 报文的时间间隔为 10 秒，发送 DMM 报文的格式是 10 个。

图 9-46 配置 VLAN 的双向时延统计功能组网图



配置思路

采用如下的思路配置 VLAN 的双向时延统计功能：

1. 在 SwitchA、SwitchB、SwitchC 和 SwitchD 上配置 VLAN。
2. 在 SwitchA 和 SwitchB 上分别配置 MD 和 MA。
3. 在 SwitchA 和 SwitchB 上配置 OUTWARD 类型的 MEP。
4. 在 SwitchA 和 SwitchB 上分别配置双向时延告警门限值。
5. 在 SwitchA 和 SwitchB 上分别使能 VLAN 的双向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VLAN ID
- 双向时延告警门限值
- MD 和 MA 的名称

操作步骤

步骤 1 配置 VLAN

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet0/0/1] quit
```

配置 SwitchC。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 2
[SwitchC-vlan2] quit
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet0/0/2] quit
```

配置 SwitchD。

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan 2
[SwitchD-vlan2] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/1] port link-type trunk
[SwitchD-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface gigabitethernet 0/0/2
[SwitchD-GigabitEthernet0/0/2] port link-type trunk
[SwitchD-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchD-GigabitEthernet0/0/2] quit
```

步骤 2 配置以太网 CFM 的基本功能

配置 SwitchA。

```
[SwitchA] cfm version standard
[SwitchA] cfm enable
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] map vlan 2
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm version standard
[SwitchB] cfm enable
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] map vlan 2
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 3 配置 OUTWARD 类型的 MEP

配置 SwitchA。

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
```


版权所有 © 华为技术有限公司

```
[SwitchA-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[SwitchA-md-md1-ma-ma1] remote-mep mep-id 2
[SwitchA-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 0/0/1 outward
[SwitchB-md-md1-ma-ma1] remote-mep mep-id 1
[SwitchB-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[SwitchA-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 4 配置双向时延告警门限值为 1000

配置 SwitchA。

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] delay-measure two-way threshold 1000
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] delay-measure two-way threshold 1000
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 5 配置 VLAN 的双向时延统计功能

配置 SwitchA。

```
[SwitchA] cfm md md1
[SwitchA-md-md1] ma ma1
[SwitchA-md-md1-ma-ma1] delay-measure two-way receive
[SwitchA-md-md1-ma-ma1] delay-measure two-way remote-mep mep-id 2 interval 10000 count 10
[SwitchA-md-md1-ma-ma1] quit
[SwitchA-md-md1] quit
```

配置 SwitchB。

```
[SwitchB] cfm md md1
[SwitchB-md-md1] ma ma1
[SwitchB-md-md1-ma-ma1] delay-measure two-way receive
[SwitchB-md-md1-ma-ma1] delay-measure two-way remote-mep mep-id 1 interval 10000 count 10
[SwitchB-md-md1-ma-ma1] quit
[SwitchB-md-md1] quit
```

步骤 6 检查配置结果

#配置完成后，在 SwitchA 上执行 **display y1731 statistics-type twoway-delay md md1 ma ma1**，可以看到双向时延的性能统计信息。

```
[Quidway] display y1731 statistic-type twoway-delay md md1 ma ma1

01  DMR received from 0025-9e80-2494 Delay:      498 usec  Variation:       0 us
ec
02  DMR received from 0025-9e80-2494 Delay:      508 usec  Variation:      10 us
ec

--- Delay measurement statistics ---
```


版权所有 © 华为技术有限公司

```
Packets transmitted: 2, Valid packets received: 2
Average delay: 503 usec, Average delay variation: 10 usec
Best case delay: 498 usec, Worst case delay: 508 usec
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 2
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1
  ma ma1
   map vlan 2
   mep mep-id 1 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
   delay-measure two-way threshold 1000
   delay-measure two-way receive
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 2
#
 cfm version standard
 cfm enable
#
interface GigabitEthernet0/0/1 outward
 port link-type trunk
 port trunk allow-pass vlan 2
#
 cfm md md1
  ma ma1
   map vlan 2
   mep mep-id 2 interface GigabitEthernet0/0/1 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
   delay-measure two-way threshold 1000
   delay-measure two-way receive
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

9.6 BFD 配置

通过创建 BFD 会话，可以实现快速检测网络中链路故障。

9.6.1 BFD 概述

BFD 是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

在现有网络中，通常采用以下几种方法检测链路故障：

- 通过硬件检测信号，如 SDH 告警，检测链路硬件故障。它的优点是可以很快的发现故障。
- 如果无法通过硬件信号检测故障，通常采用路由协议的 Hello 报文机制。

存在的问题如下：

- 并不是所有的介质都能够提供硬件检测。
- 路由协议的 Hello 报文机制检测到故障所需时间比较长，超过 1 秒钟。当数据达到吉比特速率级时，在此检测时间内，大量数据将会丢失。
- 在小型三层网络中，如果没有部署路由协议，则无法使用路由协议的 Hello 报文机制来检测故障。这对系统间互联互通定位故障造成困难。

BFD 就是为解决上述三个问题而产生的。

BFD 提供如下功能：

- 对相邻转发引擎之间的通道故障提供轻负荷、短持续时间的检测。
- 用单一的机制对任何介质、任何协议层进行实时检测，并支持不同的检测时间与开销。

9.6.2 AC6605 支持的 BFD 特性

介绍 BFD 特性在 AC6605 中的支持情况。

版权所有 © 华为技术有限公司

AC6605 设备间按照协商好的周期发送 BFD 控制报文，如果某台设备在检测时间内没有收到对端发来的报文，置 BFD 会话为 Down。上层应用可以根据 BFD 会话的状态，采取相应的处理方法。

AC6605 支持的 BFD 会话建立方式

BFD 使用本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）区分同一对系统之间的多个 BFD 会话。按照本地标识符和远端标识符创建方式的差异区分，AC6605 支持以下 BFD 会话类型：

- 手工指定标志符的静态 BFD 会话
- 静态标志符自协商 BFD 会话
- 协议触发的动态 BFD 会话

协议触发的动态 BFD 会话的实现方式是：

- 动态分配本端标识符
- 自学习远端标识符

当建立 BFD 会话的两端采用的创建标识符的方式不同时：

- 如果本端采用手工指定标识符，则对端也必须手工指定标识符。
- 如果本端采用静态标识符自协商，则对端既可以配置静态标识符自协商，也可以配置动态 BFD。
- 当本端既配置了静态标识符自协商 BFD，又配置了动态 BFD 时，将按如下原则处理：
  - 如果动态 BFD 和静态标识符自协商 BFD 共用同一个配置属性四元组（源地址、目的地址、出接口、VPN 索引），将采用动态会话共享会话的流程，将静态标识符自协商类型和动态会话共用。
  - 如果先配置了动态 BFD（此时的配置名称为 DYN_本端标识符），然后再配置标识符自协商的静态 BFD，将更新配置名称为静态 BFD 名称。
  - 共用会话的参数采用共用会话的最小值。

单跳检测

“跳”指 IP 网络中的一跳，单跳检测指检测两台直连设备间转发链路的连通性。

在进行 BFD 单跳检测的两个系统中，对于一种给定的数据协议，在指定接口上只存在一个 BFD 会话。因此，BFD 会话是与接口绑定的，AC6605 支持 BFD 会话绑定二层接口。

多跳检测

多跳检测指检测两台非直连设备间任意路径的 IP 连通性，这些路径可能跨越很多跳，也可能在某些部分重叠。多跳检测一般用来检查两台设备间是否存在可达路由。

AC6605 支持对静态路由进行 BFD 多跳检测。通常情况下静态路由自身没有检测机制，当网络发生故障时需要管理员介入。可以利用多跳检测查看静态路由的状态，路由管理模块根据 BFD 会话的状态决定静态路由是否可用。

BFD for 静态路由

静态路由自身没有检测机制，当网络发生故障时需要管理员介入。

版权所有 © 华为技术有限公司

使用 BFD for 静态路由特性，可以利用 BFD 会话检测对公网 IPv4 静态路由的状态。路由管理系统根据 BFD 会话的状态决定静态路由是否可用。

说明

BFD for 静态路由的具体配置请参考《AC6605 无线接入控制器 配置指南 IP 路由》中的**配置 BFD for 公网 IPv4 静态路由**。

BFD for 路由协议

BFD 使用本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）区分同一对系统之间的多个 BFD 会话。OSPF 协议支持动态建立 BFD 会话。

路由协议动态触发建立 BFD 会话的实现方式是：

- 动态分配本地标识符
- 自学习远端标识符

当路由协议邻居建立成功时，路由协议通过路由管理模块通知 BFD 建立会话，对路由协议的邻居关系进行快速检测。BFD 会话的检测参数由路由协议设置。

当 BFD 会话检测到故障时，状态变为 Down，BFD 通过路由管理模块触发路由收敛。

当邻居状态不可达时，路由协议通过路由管理模块通知 BFD 删除相应会话。

动态改变 BFD 参数

BFD 会话建立后，用户仍可以改变 BFD 的相关参数配置，例如 BFD 报文期望发送间隔、最小接收间隔以及本地检测倍数，不影响会话的当前状态。

9.6.3 配置 BFD 单跳检测

通过配置 BFD 单跳检测，实现快速检测和监控网络中的直连链路。

建立配置任务

在配置 BFD 单跳检测功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要快速检测和监控网络中的直连链路，可以配置 BFD 单跳检测。

前置任务

在配置 BFD 单跳检测之前，需完成以下任务：

- 正确连接各接口
- 对于三层接口，正确配置接口 IP 地址

数据准备

在配置 BFD 单跳检测功能之前，需要准备以下数据。

华为专有和保密信息
版权所有 © 华为技术有限公司

序号	数据
1	BFD 配置名
2	BFD 检测的直连链路的对端 IP 地址、本端接口名称和编号。如果检测链路的物理层状态，还需要准备 BFD 使用的缺省组播地址。
3	BFD 会话参数：本地、远端标识符

使能全局 BFD 功能

背景信息

在需要检测的链路两端 AC6605 设备上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 视图。

缺省情况下，全局 BFD 功能处于禁止状态。在进行 BFD 的相关配置前，必须先使能全局 BFD 功能，否则无法配置。

----结束

（可选）配置 BFD 缺省组播 IP 地址

背景信息

在需要检测的链路两端 AC6605 设备上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，进入 BFD 视图。

步骤 3 执行命令 **default-ip-address** *ip-address*，配置 BFD 缺省组播 IP 地址。

如果对二层转发链路进行 BFD 单跳检测，需要使用组播 IP 地址。缺省情况下，BFD 使用组播 IP 地址 224.0.0.184。

说明

- 当前网络中存在其他协议使用该组播 IP 地址时，必须更改缺省组播 IP 地址。 BFD 会话两端的 AC6605 设备上必须使用相同的组播 IP 地址。
- 如果 BFD 检测路径上存在重叠的 BFD 会话，例如，三层接口通过具有 BFD 功能的二层交换设备连接，不同 BFD 会话所在的设备必须配置不同的缺省组播 IP 地址，以避免 BFD 报文被错误地转发。

----结束

版权所有 © 华为技术有限公司

创建 BFD 会话

背景信息

在需要检测的链路两端 AC6605 设备上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 BFD 是检测接口类型的不同，选择执行如下步骤之一：

- 对于有 IP 地址的 VLANIF 接口，执行命令：

  bfd *cfg-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ip** *source-ip*]

  - 在第一次创建单跳 BFD 会话时，必须绑定对端 IP 地址和本端相应接口，且创建后不可修改。
  - 在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性。绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立。
  - 当 BFD 与单播逆向路径转发 URPF（Unicast Reverse Path Forwarding）特性一起应用时，由于 URPF 会对接收到的报文进行源 IP 地址检查，用户在创建 BFD 绑定时，需要使用 **source-ip** 选项手工指定正确的源 IP 地址，以免 BFD 报文被错误地丢弃。

- 对于二层接口，执行命令：

  bfd *cfg-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *source-ip*]

步骤 3 配置标识符。

- 执行命令 **discriminator local** *discr-value*，配置本地标识符。
- 执行命令 **discriminator remote** *discr-value*，配置远端标识符。

配置标识符时，本端的本地标识符与对端的远端标识符必需相同，否则 BFD 会话无法正确建立。本地标识符和远端标识符配置成功后不可修改。

说明

对于使用缺省组播 IP 地址的 BFD 会话，本地标识符和远端标识符不能相同。

----结束

检查配置结果

操作步骤

- 使用命令 **display bfd configuration** { **all** | **static** [**for-ip** | **name** *cfg-name*] | **discriminator** *local-discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**]查看 BFD 配置信息。
- 使用命令 **display bfd interface** [*interface-type interface-number*]查看 BFD 接口信息。
- 使用命令 **display bfd session** { { **all** |**static** } [**for-ip**] | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**]查看 BFD 会话信息。

版权所有 © 华为技术有限公司

- 使用命令 **display bfd statistics session** { { **all** | **static** } [**for-ip**] | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** }查看 BFD 会话统计信息。

----结束

任务示例

执行 **display bfd configuration** 命令，可以查看 BFD 会话的配置信息。

```
<Quidway> display bfd configuration static name bfd1 verbose
------------------------------------------------------------------------------
  BFD Session Configuration Name : bfd1
------------------------------------------------------------------------------
  Local Discriminator    : 20              Remote Discriminator   : 10
  BFD Bind Type          : Interface(GigabitEthernet0/0/1)
  Bind Session Type      : Static
  Bind Peer IP Address   : 224.0.0.184
  Bind Interface         : GigabitEthernet0/0/1
  TOS-EXP                : 7               Local Detect Multi     : 3
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Proc Interface Status  : Disable         WTR Interval (ms)      : -
  Bind Application       : No Application Bind
  Session Description    : -
------------------------------------------------------------------------------
```

执行 **display bfd interface** 命令，可以查看指定接口上的 BFD 会话的信息。

```
<Quidway> display bfd interface GigabitEthernet 0/0/1
------------------------------------------------------------------------------
Interface Name                MIndex        Sess-Count      BFD-State
------------------------------------------------------------------------------
GigabitEthernet0/0/1                1025          1               up
```

执行 **display bfd session** 命令，可以查看 BFD 会话的信息。

```
<Quidway> display bfd session all
------------------------------------------------------------------------------
Local Remote PeerIpAddr      State     Type        InterfaceName
------------------------------------------------------------------------------
20    10     224.0.0.184     UP      S_IP_IF    GigabitEthernet0/0/1
------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 0/1
```

执行 **display bfd statistics session** 命令，可以查看 BFD 会话的统计信息。

```
<Quidway> display bfd statistics session static for-ip
------------------------------------------------------------------------------
Session MIndex : 4097      (One Hop) State : Init      Name : 9to6
------------------------------------------------------------------------------
  Session Type                      : Static
  Bind Type                         : IP
  Local/Remote Discriminator        : 20/10
  Received Packets                  : 97
  Send Packets                      : 314
  Received Bad Packets              : 169
  Send Bad Packets                  : 0
  Down Count                        : 32
  ShortBreak Count                  : 0
  Send Lsp Ping Count               : 0
  Dynamic Session Delete Count      : 0
  Create Time                       : 2007/10/14 16:48:13
  Last Down Time                    : 2007/10/14 17:09:11
  Total Time From Last DOWN         : ---D:--H:--M:--S
  Total Time From Create            : 000D:00H:20M:59S
------------------------------------------------------------------------------


     Total Session Number : 1
```


版权所有 © 华为技术有限公司

9.6.4 配置 BFD 多跳检测

配置 BFD 多跳检测，实现快速检测和监控网络中的多跳路径。

建立配置任务

在配置 BFD 多跳检测功能之前，应了解其应用环境和数据准备。

应用环境

如果需要快速检测和监控 IP 路由的转发连通状况，可以配置 BFD 多跳检测。

前置任务

在配置 BFD 多跳检测之前，需完成以下任务：

- 正确连接各接口并配置 IP 地址
- 配置路由协议，保证网络层可达

数据准备

在配置 BFD 多跳检测功能之前，需要准备以下数据。

序号	数据
1	对端 IP 地址
2	BFD 配置名
3	BFD 会话参数：本地、远端标识符

使能全局 BFD 功能

只有全局使能 BFD 功能后，才能进行 BFD 的相关配置。

背景信息

在需要建立 BFD 会话的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 全局视图。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

建立 BFD 会话

背景信息

在需要建立 BFD 会话的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *cfg-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**source-ip** *source-ip*]，创建 BFD 会话。

- 在第一次创建 BFD 会话时，必须绑定对端的 IP 地址，且创建后不可修改。
- 在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性。绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立。
- 当 BFD 与单播逆向路径转发 URPF（Unicast Reverse Path Forwarding）特性一起应用时，由于 URPF 会对接收到的报文进行源 IP 地址检查，用户在创建 BFD 绑定时，需要使用 source-ip 选项手工指定正确的 BFD 报文的源 IP 地址，以免 BFD 报文被错误地丢弃。

步骤 3 配置标识符：

- 执行命令 **discriminator local** *discr-value*，配置本地标识符。
- 执行命令 **discriminator remote** *discr-value*，配置远端标识符。

说明

BFD 会话两端设备的本地标识符和远端标识符需要分别对应，即，本端的本地标识符与对端的远端标识符相同，否则会话无法正确建立。并且，本地标识符和远端标识符配置成功后不可修改。

----结束

检查配置结果

操作步骤

- 使用命令 **display bfd configuration** { **all** | **static** [**for-ip** | **name** *cfg-name*] | **discriminator** *local-discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**]查看 BFD 配置信息。
- 使用命令 **display bfd session** { { **all** |**static** } [**for-ip**] | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**]查看 BFD 会话信息。
- 使用命令 **display bfd statistics session** { { **all** | **static** } [**for-ip**] | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** }查看 BFD 会话统计信息。

----结束

任务示例

执行 **display bfd configuration** 命令，可以查看 BFD 会话的配置信息。

```
<Quidway> display bfd configuration static name bfd1 verbose
--------------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
  BFD Session Configuration Name : bfd1
------------------------------------------------------------------------------
  Local Discriminator    : 20              Remote Discriminator   : 10
  BFD Bind Type          : Interface(Vlanif110)
  Bind Session Type      : Static
  Bind Peer IP Address   : 11.1.1.1
  Bind Interface         : Vlanif110
  TOS-EXP                : 7               Local Detect Multi     : 3
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Proc Interface Status  : Disable         WTR Interval (ms)      : -
  Bind Application       : No Application Bind
  Session Description    : -
------------------------------------------------------------------------------
```

执行 **display bfd session** 命令，可以查看 BFD 会话信息。

```
<Quidway> display bfd session discriminator 22 verbose
------------------------------------------------------------------------------
Session MIndex : 4096      (One Hop) State : Up        Name : bfd1
------------------------------------------------------------------------------
  Local Discriminator    : 22              Remote Discriminator   : 11
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(GigabitEthernet0/0/1)
  Bind Session Type      : Static
  Bind Peer IP Address   : 224.0.0.184
  NextHop Ip Address     : 224.0.0.184
  Bind Interface         : GigabitEthernet0/0/1
  FSM Board Id           : 0               TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000            Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3               Detect Interval (ms)   : 3000
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 255
  Proc Interface Status  : Disable         Process PST            : Disable
  WTR Interval (ms)      : -               Local Demand Mode      : Disable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : 16394           Session Detect TmrID   : 16395
  Session Init TmrID     : -               Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
------------------------------------------------------------------------------
```

执行 **display bfd statistics session** 命令，查看 BFD 会话的统计信息。

```
<Quidway> display bfd statistics session all
------------------------------------------------------------------------------
Session MIndex : 4096      (One Hop) State : Up        Name : bfd1
------------------------------------------------------------------------------
  Session Type                      : Static
  Bind Type                         : IP
  Local/Remote Discriminator        : 22/11
  Received Packets                  : 178
  Send Packets                      : 177
  Received Bad Packets              : 0
  Send Bad Packets                  : 0
  Down Count                        : 0
  ShortBreak Count                  : 0
  Send Lsp Ping Count               : 0
  Dynamic Session Delete Count      : 0
  Create Time                       : 2007/10/14 22:26:53
  Last Down Time                    : 0000/00/00 00:00:00
  Total Time From Last DOWN         : ---D:--H:--M:--S
  Total Time From Create            : 000D:00H:03M:03S
------------------------------------------------------------------------------

    Total Session Number : 1
```


版权所有 © 华为技术有限公司

9.6.5 配置静态标识符自协商 BFD

通过配置静态标识符自协商 BFD，实现与采用动态建立 BFD 会话的设备互通。它主要应用在静态路由中。

建立配置任务

在配置静态标识符自协商 BFD 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现静态路由 Track BFD，此时必须配置静态标识符自协商 BFD。

前置任务

在配置静态标识符自协商 BFD 之前，需完成以下任务：

- 正确连接各接口
- 对于三层接口，正确配置接口 IP 地址

数据准备

在配置静态标识符自协商 BFD 之前，需要准备以下数据。

序号	数据
1	BFD 配置名
2	BFD 检测链路的本端和对端 IP 地址、本端接口名称和编号

使能全局 BFD 功能

只有全局使能 BFD 功能后，才能进行 BFD 的相关配置。

背景信息

在需要使用静态标识符自协商 BFD 检测链路的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 全局视图。

----结束

版权所有 © 华为技术有限公司

配置静态标识符自协商 BFD

背景信息

在需要使用静态标识符自协商 BFD 检测链路的 AC6605 上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *cfg-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] **source-ip** *ip-address* **auto**，根据检测的链路类型，使用不同的命令选项创建 BFD 会话。

创建 BFD 会话时：

- 在第一次创建单跳 BFD 会话时，必须绑定对端 IP 地址和本端相应接口，且创建后不可修改。
- 必须配置源地址。
- 必须指定明确的对端 IP 地址，不能使用组播 IP 地址。

----结束

检查配置结果

背景信息

已经完成静态标志符自协商 BFD 功能的所有配置。

操作步骤

- 使用 **display bfd session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] } [**verbose**]命令查看 BFD 会话信息。

----结束

任务示例

#查看所有 BFD 会话详细信息。

```
<Quidway> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 258       (Multi Hop) State : Up        Name : bfd1
--------------------------------------------------------------------------------
  Local Discriminator    : 8192             Remote Discriminator   : 8192
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address
  Bind Session Type      : Static_Auto
  Bind Peer IP Address   : 11.1.1.1
  Bind Interface         : -
  Bind Source IP Address : 11.1.1.2
  FSM Board Id           : 0                TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 253
  Proc Interface Status  : Disable
```


版权所有 © 华为技术有限公司

```
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : AUTO
  Session TX TmrID       : -                Session Detect TmrID   : -
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 1/0
```

可以看到建立了一个会话类型为 **Static_Auto** 的 BFD 会话，通过自协商方式获得的该会话的本端和远端标志符分别为 8192 和 8192。

9.6.6 调整 BFD 检测参数

通过调整 BFD 检测参数，实现 BFD 会话更好、更快速的检测和监控网络中的链路。

建立配置任务

在调整 BFD 检测参数功能之前，应了解其应用环境和数据准备，并需要配置 BFD 会话等前置任务。

应用环境

在建立 BFD 会话时，可以根据网络状况和性能需求，调整设备的 BFD 报文发送间隔、接收间隔以及本地检测倍数。

用户可以通过配置 BFD 会话的等待恢复时间 WTR（Wait to Recovery），来避免 BFD 会话震荡导致的 BFD 应用在主备之间频繁切换。

用户还可以通过配置 BFD 会话的描述信息对 BFD 会话监视的链路进行简单描述，方便用户识别不同的 BFD 会话。

通常情况下，使用系统的缺省配置即可。

前置任务

在调整 BFD 检测参数之前，需完成以下任务：

- 完成 BFD 会话的创建

数据准备

在调整 BFD 检测参数之前，需要准备以下数据。

序号	数据
1	BFD 配置名
2	BFD 报文的本地发送间隔、接收间隔
3	BFD 报文的本地检测倍数
4	BFD 报文的优先级

版权所有 © 华为技术有限公司

调整 BFD 检测时间

背景信息

为降低对系统资源的占用，一旦检测到 BFD 会话 Down，系统自动将本端的发送间隔和接收间隔调整为 1000 毫秒～ 3000 毫秒之间的一个随机值。当 BFD 会话的状态重新变为 Up 后，再恢复成用户配置的间隔时间。

请在需要调整 BFD 检测参数的 AC6605 设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *configuration-name*，进入 BFD 会话视图。

步骤 3 执行命令 **min-tx-interval** *interval*，配置 BFD 报文的最小发送间隔。

步骤 4 执行命令 **min-rx-interval** *interval*，配置 BFD 报文的最小接收间隔。

步骤 5 执行命令 **detect-multiplier** *multiplier*，配置本地检测倍数。

缺省情况下，本地检测倍数为 3。

步骤 6 执行命令 **commit**，使配置生效。

----结束

配置 BFD 会话的描述信息

通过配置 BFD 会话的描述信息，识别不同的 BFD 会话。

背景信息

说明

description 命令只对静态配置的 BFD 会话有效，对于动态配置的 BFD 会话和静态标识符自协商 BFD 会话无效。

请在交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *cfg-name*，进入 BFD 会话视图。

步骤 3 执行命令 **description** *description*，配置 BFD 会话的描述信息。

description 是字符串类型，长度范围是 1 ～ 51。

缺省情况下，BFD 会话的描述信息是空。

可以执行 **undo description** 命令来删除 BFD 会话的描述信息。

----结束

版权所有 © 华为技术有限公司

配置 BFD 等待恢复时间

通过配置 BFD 会话的等待恢复时间，可以避免因 BFD 会话振荡而导致的应用在主备设备之间频繁切换。

背景信息

如果 BFD 会话发生震荡，使用 BFD 的应用将在主备之间频繁切换。为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间。当 BFD 会话从 Down 变为 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用。

请在交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *cfg-name*，进入 BFD 会话视图。

步骤 3 执行命令 **wtr** *wtr-value*，配置等待恢复时间。

缺省情况下，等待恢复时间 WTR 为 0，即不等待。

步骤 4 执行命令 **commit**，提交配置。

----结束

配置 BFD 报文的优先级

背景信息

修改 BFD 报文的优先级可以用来实现：

- 检测同一链路上不同优先级的报文转发是否畅通。
- 将 BFD 报文设置为高优先级报文后，优先保证 BFD 报文的转发。

请在需要调整 BFD 检测参数的 AC6605 设备上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd** *configuration-name*，进入 BFD 会话视图。

步骤 3 执行命令 **tos-exp** *tos*，配置 BFD 报文的优先级。

缺省情况下，BFD 报文的优先级为 7，0 为最低优先级，7 为最高优先级。

步骤 4 执行命令 **commit**，提交配置。

----结束

检查配置结果

版权所有 © 华为技术有限公司

操作步骤

步骤 1 使用命令 **display bfd configuration** { **all** | **static** [**for-ip** | **name** *cfg-name*] | **discriminator** *local-discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**] 查看 BFD 配置信息。

步骤 2 使用命令 **display bfd session** { { **all** |**static** } [**for-ip**] | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** } [**verbose**]查看 BFD 会话信息。

----结束

任务示例

执行 **display bfd configuration** 命令，查看 BFD 配置信息。

```
<Quidway> display bfd configuration static for-ip verbose
------------------------------------------------------------------------------
  BFD Session Configuration Name : bfd2
------------------------------------------------------------------------------
  Local Discriminator    : 20              Remote Discriminator   : 10
  BFD Bind Type          : Interface(Vlanif110)
  Bind Session Type      : Static
  Bind Peer IP Address   : 11.1.1.1
  Bind Interface         : Vlanif110
  TOS-EXP                : 7               Local Detect Multi     : 3
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Proc Interface Status  : Disable         WTR Interval (ms)      : -
  Bind Application       : No Application Bind
  Session Description    : -
------------------------------------------------------------------------------

    Total Commit/Uncommit CFG Number : 1/0
```

执行 **display bfd session** 命令，查看 BFD 会话信息。

```
<Quidway> display bfd session all for-ip verbose
------------------------------------------------------------------------------
Session MIndex : 258       (One Hop) State : Up        Name : bfd2
------------------------------------------------------------------------------
  Local Discriminator    : 20              Remote Discriminator   : 10
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(Vlanif110)
  Bind Session Type      : Static
  Bind Peer IP Address   : 11.1.1.1
  NextHop Ip Address     : 11.1.1.1
  Bind Interface         : Vlanif110
  FSM Board Id           : 0               TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000            Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3               Detect Interval (ms)   : 3000
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 255
  Proc Interface Status  : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : 4491            Session Detect TmrID   : 4492
  Session Init TmrID     : -               Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 1/0
```


版权所有 © 华为技术有限公司

9.6.7 配置 Trap 消息定时器的时间间隔

通过配置 Trap 消息定时器的时间间隔，实现对 BFD 的告警信息进行抑制。

建立配置任务

在配置 Trap 消息定时器的时间间隔功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果 BFD 使能了 SNMP 告警，则在网管侧将会接收到 BFD 会话的 Up 或 Down 消息。此时如果 BFD 会话振荡，则网管侧将会接收到大量的告警信息，因此，需要对 BFD 的 Trap 消息进行抑致。通过配置发送 Trap 消息定时器的时间间隔可以实现对 BFD 的告警信息进行抑制。

前置任务

在配置 TRAP 消息定时器的时间间隔功能之前，需完成以下任务：

- 全局使能 BFD 功能

数据准备

在配置 Trap 消息定时器的时间间隔之前，需要准备以下数据。

序号	数据
1	发送 Trap 消息定时器的时间间隔

配置发送告警消息定时器的时间间隔

BFD 会话震荡时，网管侧会收到大量的告警信息，此时可以配置发送告警消息定时器的时间间隔对告警信息进行抑致。

背景信息

请在需要配置发送告警消息定时器的时间间隔交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能 BFD 全局能力并进入 BFD 全局视图。

步骤 3 执行命令 **snmp-agent bfd trap-interval** *interval*，设置发送 TRAP 消息定时器的时间间隔。

缺省情况下，发送 TRAP 消息定时器的时间间隔是 120 秒。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

检查配置结果

通过查看 Trap 消息定时器的时间间隔等内容，来检查配置是否成功。

前提条件

已经完成 TRAP 消息定时器的时间间隔功能的所有配置。

操作步骤

- 使用 **display current-configuration configuration bfd** 命令查看 BFD 的告警功能。

----结束

任务示例

使用 **display current-configuration configuration bfd** 命令可以看到发送 TRAP 消息定时器的时间间隔是 300 秒。

```
<Quidway> display current-configuration configuration bfd
#
 bfd
 snmp-agent bfd trap-interval 300
#
return
```

9.6.8 维护 BFD

通过维护 BFD，可以实现清除 BFD 统计数据和监控 BFD 的运行状况的目的。

清除 BFD 的统计数据

在查看一段时间内的 BFD 的统计信息之前，建议清除 BFD 的统计信息。

背景信息

注意

清除 BFD 的统计信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除 BFD 的统计信息后，请在用户视图下执行 **reset bfd statistics** { **all** | **discriminator** *discr-value* }命令。

----结束

调试 BFD

调试完成后，应及时关闭调试开关。

版权所有 © 华为技术有限公司

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 BFD 运行故障时，请在用户视图下执行 **debugging** 命令对 BFD 进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

步骤 1 在用户视图下执行 **debugging bfd** { **all** | **defect-detect** | **error** | **event** | **fsm** | **ha** | **packet** | **process** | **product-interface** | **session-management** | **timer** }命令，打开 BFD 模块的调试开关。

----结束

9.6.9 配置举例

介绍 BFD 的配置举例。

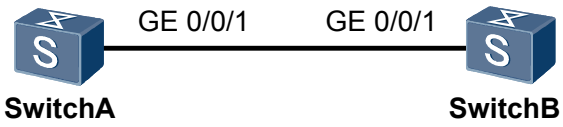
配置 BFD 单跳检测二层链路示例

组网需求

AC6605 的接口为二层接口，如果需要检测两台直连 AC6605 间二层转发链路的连通性，可以配置 BFD 单跳检测，使 BFD 会话绑定组播 IP 地址和本端接口。

如图 9-47 所示，通过配置 BFD 会话检测 SwitchA、SwitchB 之间二层链路的连通性。

图 9-47 配置 BFD 单跳检测二层链路示例组网图



配置思路

采用如下思路配置 BFD 单跳检测：

1. 在 SwitchA 上配置 BFD 会话，检测 SwitchA 到 SwitchB 的直连链路。
2. 在 SwitchB 上配置 BFD 会话，检测 SwitchB 到 SwitchA 的直连链路。

数据准备

为完成此配置例，需要准备如下数据：

版权所有 © 华为技术有限公司

- 与 BFD 会话绑定的接口类型、接口编号
- BFD 会话的本地标志符和远端标识符

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 SwitchA 的 BFD 单跳检测

使能 SwitchA 上的 BFD 能力。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] bfd
[SwitchA-bfd] quit
```

配置 SwitchA 上的 BFD 会话。

```
[SwitchA] bfd atob bind peer-ip default-ip interface gigabitethernet 0/0/1
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

步骤 2 配置 SwitchB 的 BFD 单跳检测

使能 SwitchB 上的 BFD 能力。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
```

配置 SwitchB 上的 BFD 会话。

```
[SwitchB] bfd btoa bind peer-ip default-ip interface gigabitethernet 0/0/1
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

步骤 3 验证配置结果

配置完成后，在 SwitchA 和 SwitchB 上执行 **display bfd session** 命令，可以看到建立了一个单跳检测的 BFD 会话，且会话状态为 Up。

以 SwitchA 上的显示为例。

```
<SwitchA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097      (One Hop) State : Up        Name : atob
--------------------------------------------------------------------------------
  Local Discriminator    : 1              Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(GigabitEthernet0/0/1)
  Bind Session Type      : Static
  Bind Peer IP Address   : 224.0.0.184
  NextHop Ip Address     : 224.0.0.184
  Bind Interface         : GigabitEthernet0/0/1
  FSM Board Id           : 0                TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 255
  Proc Interface Status  : Disable
```


版权所有 © 华为技术有限公司

```
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : -                Session Detect TmrID   : -
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 1/0
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 bfd
#
bfd atob bind peer-ip default-ip interface GigabitEthernet0/0/1
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 bfd
#
bfd btoa bind peer-ip default-ip interface GigabitEthernet0/0/1
 discriminator local 2
 discriminator remote 1
 commit
#
return
```

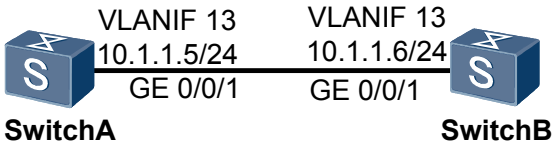
配置 VLANIF 接口 BFD 单跳检测示例

组网需求

AC6605 之间通过 VLANIF 接口实现三层互通，如果需要检测两台直连 AC6605 间 VLANIF 接口的连通性，可以配置 BFD 单跳检测，使 BFD 会话绑定 VLANIF 接口的 IP 地址和 VLANIF 接口。

如图 9-48 所示，通过配置 BFD 会话检测 SwitchA、SwitchB 之间 VLANIF 接口的连通性。

图 9-48 配置 VLANIF 接口 BFD 单跳检测示例组网图



版权所有 © 华为技术有限公司

配置思路

采用如下思路配置 BFD 单跳检测：

1. 在 SwitchA 和 SwitchB 上分别创建 VLAN13。
2. 在 SwitchA 和 SwitchB 上的 GE0/0/1 接口都配置为 hybrid 接口。
3. 在 SwitchASwitchB 创建 VLANIF13 接口，并且为 VLANIF 配置 IP 地址。
4. 在 SwitchA 上配置 BFD 会话，检测 SwitchA 到 SwitchB 的链路。
5. 在 SwitchB 上配置 BFD 会话，检测 SwitchB 到 SwitchA 的链路。

数据准备

为完成此配置例，需要准备如下数据：

- 与 BFD 会话绑定 VLANIF 接口号
- VLANIF 接口的 IP 地址
- BFD 会话的本地标志符和远端标识符

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 在 SwitchA 和 SwitchB 上创建 VLAN，将 GE0/0/1 接口配置为 hybrid 接口并加入 VLAN

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 13
[SwitchA-vlan13] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 13
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 13
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 13
[SwitchB-vlan13] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 13
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 13
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 2 为 VLANIF 接口配置 IP 地址，使 SwitchA 和 SwitchB 之间实现三层互通

配置 SwitchA

```
[SwitchA] interface vlanif13
[SwitchA-Vlanif13] ip address 10.1.1.5 24
[SwitchA-Vlanif13] quit
```

配置 SwitchB

```
[SwitchB] interface vlanif13
[SwitchB-Vlanif13] ip address 10.1.1.6 24
[SwitchB-Vlanif13] quit
```


版权所有 © 华为技术有限公司

配置完成后，在 SwitchA 或 SwitchB 上执行 **display interface vlanif** 命令，可以看到 VLANIF 接口状态为 UP。

```
[SwitchA] display interface vlanif 13
Vlanif13 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif13 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-827d-75f5
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 3 配置 SwitchA 的 BFD 单跳检测

使能 SwitchA 上的 BFD 能力。

```
[SwitchA] bfd
[SwitchA-bfd] quit
```

配置 SwitchA 上的 BFD 会话。

```
[SwitchA] bfd atob bind peer-ip 10.1.1.6 interface vlanif 13
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

步骤 4 配置 SwitchB 的 BFD 单跳检测

使能 SwitchB 上的 BFD 能力。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
```

配置 SwitchB 上的 BFD 会话。

```
[SwitchB] bfd btoa bind peer-ip 10.1.1.5 interface vlanif 13
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

步骤 5 验证配置结果

配置完成后，在 SwitchA 和 SwitchB 上执行 **display bfd session** 命令，可以看到建立了一个单跳检测的 BFD 会话，且会话状态为 Up。

以 SwitchA 上的显示为例。

```
<SwitchA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097      (One Hop) State : Up        Name : atob
--------------------------------------------------------------------------------
  Local Discriminator    : 1               Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(Vlanif13)
  Bind Session Type      : Static
  Bind Peer IP Address   : 10.1.1.6
  Bind Interface         : Vlanif13
  FSM Board Id           : 0               TOS-EXP                : 7
```


版权所有 © 华为技术有限公司

```
 Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
 Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
 Local Detect Multi     : 3                Detect Interval (ms)   : -
 Echo Passive           : Disable          Acl Number             : -
 Destination Port       : 3784             TTL                    : 255
 Proc Interface Status  : Disable
 WTR Interval (ms)      : -
 Active Multi           : -
 Last Local Diagnostic  : No Diagnostic
 Bind Application       : No Application Bind
 Session TX TmrID       : 16392            Session Detect TmrID   : -
 Session Init TmrID     : -                Session WTR TmrID      : -
 Session Echo Tx TmrID  : -
 PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
 Session Description    : -
--------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 0/1
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 13
#
 bfd
#
interface Vlanif13
 ip address 10.1.1.5 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
bfd atob bind peer-ip 10.1.1.6 interface Vlanif13
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 13
#
 bfd
#
interface Vlanif13
 ip address 10.1.1.6 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
bfd btoa bind peer-ip 10.1.1.5 interface Vlanif13
 discriminator local 2
 discriminator remote 1
 commit
#
return
```


版权所有 © 华为技术有限公司

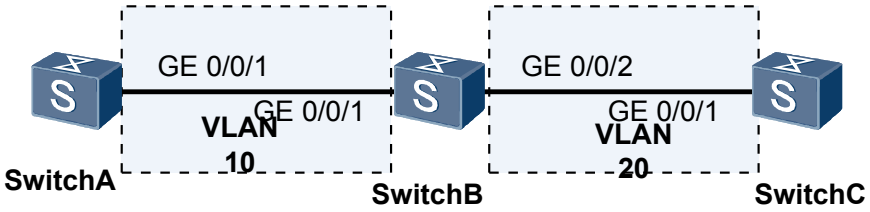
配置 BFD 多跳检测示例

组网需求

如图 9-49 所示，通过 BFD 会话检测 SwitchA、SwitchC 之间的多跳路径。

Switch 的接口为二层接口，配置 BFD 多跳检测时需将接口加入 VLAN、创建接口 VLANIF 并配置在接口 VLANIF 上配置 IP 地址。

图 9-49 配置 BFD 多跳检测组网图



配置思路

采用如下思路配置 BFD：

1. 在 SwitchA 上配置 BFD 会话，检测 SwitchA 到 SwitchC 的多跳路径。
2. 在 SwitchC 上配置 BFD 会话，检测 SwitchC 到 SwitchA 的多跳路径。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 会话绑定的对端 IP 地址
- BFD 会话的本地标志符和远端标识符
- SwitchA 上接口 VLANIF10 的 IP 地址为 10.1.1.1/16
- SwitchB 上接口 VLANIF10 的 IP 地址为 10.1.1.2/16
- SwitchB 上接口 VLANIF20 的 IP 地址为 10.2.1.1/16
- SwitchC 上接口 VLANIF20 的 IP 地址为 10.2.1.2/16

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值

操作步骤

步骤 1 将接口加入 VLAN 并创建接口 VLANIF，在接口 VLANIF 上配置 IP 地址

在 SwitchA 上创建 VLAN 并将接口加入 VLAN。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 10
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

在 SwitchA 上创建接口 VLANIF 并配置接口 VLANIF 的 IP 地址。

版权所有 © 华为技术有限公司

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 16
[SwitchA-Vlanif10] quit
```

在 SwitchB 和 SwitchC 上的配置方法与 SwitchA 相同，具体配置过程略。

步骤 2 配置静态路由，使 SwitchA、SwitchC 之间有可达路由

```
[SwitchA] ip route-static 10.2.0.0 16 10.1.1.2
```

在 SwitchC 上的配置方法与 SwitchA 相同，具体配置过程略。

步骤 3 在 SwitchA 和 SwitchC 上配置多跳 BFD 检测

在 SwitchA 上配置与 SwitchC 之间的 BFD 会话。

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atoc bind peer-ip 10.2.1.2
[SwitchA-bfd-session-atoc] discriminator local 10
[SwitchA-bfd-session-atoc] discriminator remote 20
[SwitchA-bfd-session-atoc] commit
[SwitchA-bfd-session-atoc] quit
```

在 SwitchC 上配置与 SwitchA 之间的 BFD 会话。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] bfd
[SwitchC-bfd] quit
[SwitchC] bfd ctoa bind peer-ip 10.1.1.1
[SwitchC-bfd-session-ctoa] discriminator local 20
[SwitchC-bfd-session-ctoa] discriminator remote 10
[SwitchC-bfd-session-ctoa] commit
[SwitchC-bfd-session-ctoa] quit
```

步骤 4 验证配置结果

配置完成后，在 SwitchA 和 SwitchC 上执行 **display bfd session** 命令，可以看到建立了一个 BFD 会话，且状态为 Up。

以 SwitchA 上的显示为例。

```
<SwitchA> display bfd session all verbose
-------------------------------------------------------------------------------
Session MIndex : 4096      (Multi Hop) State : Up       Name : atoc
-------------------------------------------------------------------------------
  Local Discriminator    : 10              Remote Discriminator   : 20
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address
  Bind Session Type      : Static
  Bind Peer IP Address   : 10.2.1.2
  Bind Interface         : -
  FSM Board Id           : 0               TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000            Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3               Detect Interval (ms)   : 3000
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 255
  Proc Interface Status  : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : Control Detection Time Expired
  Bind Application       : No Application Bind
  Session TX TmrID       : 16445           Session Detect TmrID   : -
  Session Init TmrID     : 16447           Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
```


版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 0/1
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
 bfd
#
interface Vlanif10
 ip address 10.1.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
bfd atoc bind peer-ip 10.2.1.2
 discriminator local 10
 discriminator remote 20
 commit
#
 ip route-static 10.2.0.0 255.255.0.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.0.0
#
interface Vlanif20
 ip address 10.2.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 bfd
#
 vlan batch 20
#
interface Vlanif20
 ip address 10.2.1.2 255.255.0.0
#
interface GigabitEthernet0/0/1
  port hybrid pvid vlan 20
```


版权所有 © 华为技术有限公司

```
 port hybrid untagged vlan 20
#
bfd ctoa bind peer-ip 10.1.1.1
 discriminator local 20
 discriminator remote 10
 commit
#
 ip route-static 10.1.0.0 255.255.0.0 10.2.1.1
#
return
```

9.7 VRRP 和 VRRP6 配置

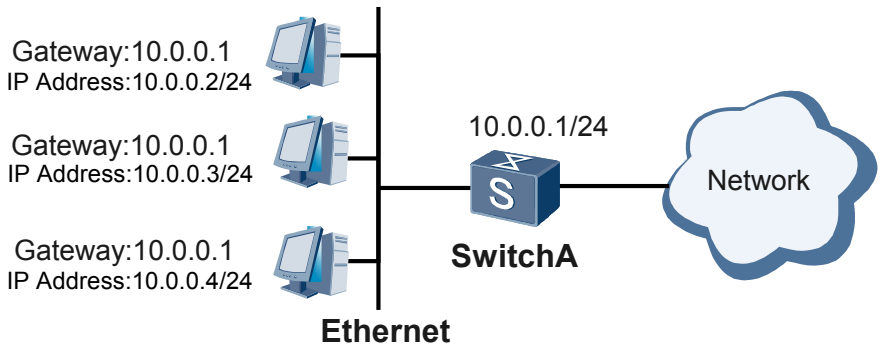
通过创建 VRRP 或 VRRP6 备份组，实现当主用设备出现故障时，由备用设备承担网路流量。

9.7.1 VRRP 概述

VRRP 将一组路由器联合组成一台虚拟路由器，将网络内主机的缺省网关设置为该虚拟路由器的 IP 地址。

通常情况下，网络内部的所有主机都设置一条相同的缺省路由，指向出口网关（即图 9-50 中的交换机 SwitchA），实现主机与外部网络的通信。当出口网关发生故障时，主机与外部网络的通信就会中断。

图 9-50 局域网缺省网关



配置多个出口网关是提高系统可靠性的常见方法，但需要解决如何在多个出口网关之间进行选路的问题。

VRRP 是 RFC3768 定义的一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路，很好地解决了上述问题。

在具有多播或广播能力的局域网（如以太网）中，VRRP 提供逻辑网关确保高利用度的传输链路，不仅能够解决因某网关设备故障带来的业务中断，而且无需修改路由协议的配置。

版权所有 © 华为技术有限公司

9.7.2 AC6605 支持的 VRRP 特性

VRRP 包括：主备备份 VRRP、负载分担 VRRP、监视接口状态、VRRP 快速切换、虚拟 IP 地址 Ping 开关、VRRP 的安全功能、VRRP 平滑倒换功能和管理 VRRP。

主备备份 VRRP

这是 VRRP 提供 IP 地址备份功能的基本方式。主备备份方式需要建立一个虚拟路由器，该虚拟路由器包括一个 Master 设备和若干 Backup 设备，这些设备构成一个备份组。Master 设备和 Backup 设备在备份组中拥有不同的优先级，优先级最高的交换机作为 Master 设备。正常情况下，业务全部由 Master 设备承担。Master 设备出现故障时，Backup 设备接替工作。

负载分担 VRRP

负载分担方式是指建立两个或更多备份组，多台交换机同时承担业务。在这种模式下，VRRP 备份组的特性如下：

- AC6605 中允许一台交换机加入多个备份组，在不同备份组中有不同的优先级。通过多虚拟交换机设置可以实现负载分担。
- 每个备份组都包括一个 Master 设备和若干 Backup 设备。
- 各备份组的 Master 可以不同。

监视接口状态

AC6605 支持监控接口的状态，当接口状态变化时，交换机的优先级自动调整，从而使备份组中各交换机优选级高低顺序发生变化，VRRP 重新确定 Master 设备。

VRRP 快速切换

AC6605 实现双向转发检测 BFD（Bidirectional Forwarding Detection）机制，能够快速检测、监控网络中链路或者 IP 路由的连通状况，VRRP 通过监视 BFD 会话状态实现主备快速切换，可以配置 8 个 BFD Session，主备切换的时间控制在 1 秒以内。结合使用 BFD 会话的检测结果，可以加快 VRRP 主备倒换的速度。

虚拟 IP 地址 Ping 开关

VRRP 备份组使用虚拟 IP 地址，能够 Ping 通虚拟 IP 地址可以比较方便的监控虚拟路由器的工作情况，但是可能遭到 ICMP 攻击的隐患。在 AC6605 中，提供了控制 Ping 通虚拟 IP 地址的开关命令，用户可以选择是否打开。

VRRP 的安全功能

对于安全程度不同的网络环境，可以在 VRRP 报头上设定不同的认证方式和认证字。

在一个安全的网络中，可以采用缺省设置：交换机对要发送的 VRRP 报文不进行任何认证处理，收到 VRRP 报文的交换机也不进行任何认证，认为收到的都是真实的、合法的 VRRP 报文。这种情况下，不需要设置认证字。

在有可能受到安全威胁的网络中，VRRP 提供了简单字符（Simple）认证方式和 MD5 认证方式。对于简单认证字方式，可以设置长度为 1 ～ 8 的认证字；对于 MD5 认证方式，明文长度范围是 1 ～ 8，密文长度为 24。

版权所有 © 华为技术有限公司

管理 VRRP

为了满足不同的业务需要，交换机之间可以运行多个 VRRP 备份组。如果每个 VRRP 备份组都需要维护自己的状态机，这样交换机之间就会存在大量的 VRRP 协议报文。为了简化协议操作，减少协议报文对带宽的占用，可以将其中一个 VRRP 备份组配置为管理备份组，其余成员备份组与管理备份组绑定，从而成员备份组的状态和管理备份组的状态保持一致。

VRRP6

VRRP6 是 VRRP for IPv6 的简称。它是一种容错协议，是对 VRRP 协议的扩展。它通过把几台路由设备联合组成一台虚拟的路由设备，并通过一定的机制保证当主机的下一跳设备出现故障时，及时将业务切换到其它设备，从而保持通讯的连续性和可靠性。

可以根据 VRRP6 和 VRRP for IPv4 所支持的功能，来查看它们的异同点。

VRRP6/VRRP for IPv4 支持的功能	VRRP6	VRRP for IPv4
主备备份 VRRP	是	是
负载分担 VRRP	是	是
监视接口状态	是	是
VRRP 快速切换	是	是
虚拟 IP 地址 Ping 开关	是	是
VRRP 的安全认证功能	否	是
VRRP 平滑倒换	否	是
管理 VRRP	是	是

9.7.3 配置 VRRP 备份组

通过配置主备备份方式或者是负载分担方式的 VRRP 备份组，实现局域网内的主机和外部网络的通信。

建立配置任务

在配置 VRRP 备份组功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

VRRP 备份组分主备备份方式和负载分担方式。

- 主备备份是 VRRP 提供的基本功能，其工作方式如下：
  - 仅有一个备份组。
  - 备份组内优先级最高的一台交换机作为 Master 设备，承担业务。

版权所有 © 华为技术有限公司

- 除了 Master，其它交换机是备份组内的 Backup 设备，处于就绪监听状态。
- 如果 Master 设备发生故障，Backup 设备将根据优先级选出一个新的 Master 设备提供路由服务。

- 负载分担是通过建立多个备份组的方式来分担网络流量，一台交换机可以属于多个备份组，其工作方式如下：
  - SwitchA 作为备份组 1 的 Master，同时又是备份组 2 的 Backup。
  - SwitchB 作为备份组 2 的 Master，同时又是备份组 1 的 Backup。
  - 网络内部分主机使用备份组 1 作网关，部分主机使用备份组 2 作为网关。

  这样，既达到相互备份的目的，又可以分担网络流量。

说明

只有 VLANIF 接口支持 VRRP 功能。

前置任务

在配置 VRRP 备份组之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通

数据准备

配置 VRRP 备份组之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	备份组的虚拟 IP 地址
3	VRRP 备份组中各交换机的优先级

创建备份组并配置虚拟 IP 地址

通过创建备份组，实现局域网内的主机的缺省网关为该备份组的 IP 地址。

背景信息

请在备份组的各交换机上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入 VLANIF 接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建备份组并配置虚拟 IP 地址。

版权所有 © 华为技术有限公司

说明

- AC6605 只有 VLANIF 接口支持 VRRP 功能。
- 虚拟 IP 地址必须和当前接口 IP 地址在同一网段。
- 各备份组之间的虚拟 IP 地址不能重复。
- 保证同一备份组的两端设备上配置相同的备份组 ID。
- 不同接口之间的备份组 ID 可以重复使用。

当指定第一个虚拟 IP 地址到 VRRP 备份组时，系统会创建这个备份组。以后再指定虚拟 IP 地址到这个备份组时，系统将这个地址添加到备份组的虚拟 IP 地址列表中。

对于网络中具有相同 VRRP 可靠性需求的用户，为了便于管理，并避免用户侧缺省网关地址随 VRRP 配置而改变，可以为同一个备份组配置多个虚拟 IP 地址，不同的虚拟 IP 地址为不同用户群服务，每个备份组最多可配置 16 个虚拟 IP 地址。

对于负载分担方式 VRRP 备份组，需要重复执行该步骤，在接口上配置多个备份组。至少需要在接口上配置两个备份组，各备份组之间以 VRID 区分。各备份组间的虚拟 IP 地址不能重复。

说明

AC6605 的每个接口上，最多可以配置 24 个备份组。如果需要配置满规格，需要使用将 VRRP 协议报文的 CPCAR 配置到 256kbps。

注意

- 在设备上同时配置 VRRP 和静态 ARP 时，需要注意：不能将与这些接口相关的静态 ARP 表项对应的映射 IP 地址作为 VRRP 的虚拟地址。否则会生成错误的主机路由，影响设备之间的正常转发。
- 不能将 VRRP 虚 MAC 地址配置为静态 MAC 地址或者黑洞 MAC 地址。
- 建议不要在 Super VLAN 对应的 VLANIF 接口下创建 VRRP 备份组,以免对主机性能产生影响。

- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]，创建备份组并配置虚拟 IPv6 地址。

     说明

     - 各备份组之间的虚拟 IP 地址不能重复。
     - 保证同一备份组的两端设备上配置相同的备份组 ID。
     - 不同接口之间的备份组 ID 可以重复使用。

     link-local：指定 VRRP6 的虚拟 IPv6 地址为链路本地地址。链路本地地址前缀是 FE80 的 IPv6 地址，用于同一链路的相邻节点间通信，有效域仅限于本地链路。链路本地地址的报文永远不会被 IPv6 交换机转发。配置 VRRP6 的虚拟 IPv6 地址时，第一个虚拟 IPv6 地址必须是链路本地地址。

版权所有 © 华为技术有限公司

当指定第一个虚拟 IPv6 地址到 VRRP 备份组时，系统会创建这个备份组。以后再指定虚拟 IP 地址到这个备份组时，系统将这个地址添加到备份组的虚拟 IPv6 地址列表中。

对于负载分担方式 VRRP6 备份组，需要重复执行该步骤，在接口上配置多个备份组。至少需要在接口上配置两个备份组，各备份组之间以 VRID 区分。各备份组间的虚拟 IPv6 地址不能重复。

----结束

配置接口在备份组中的优先级

通过创建接口在备份组中的优先级，实现主用设备承担网络流量。

背景信息

主备备份方式只有一个备份组，不同交换机在该备份组中拥有不同优先级，优先级最高的成为 Master，其他均为 Backup 状态。

负载分担方式有两个或更多的备份组，VRRP 根据优先级来确定备份组中每台交换机的地位，各交换机在不同备份组中拥有不同的优先级。重复执行该步骤，保证各个 VRRP 备份组的 Master 分布在不同的交换机上。

请在备份组的各交换机接口上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入 VLANIF 接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **priority** *priority-value*，配置交换机在备份组中的优先级。

     缺省情况下，优先级的取值是 100。优先级 0 是系统保留作为特殊用途的，优先级值 255 保留给 IP 地址拥有者，IP 地址拥有者的优先级不可配置。通过命令可以配置的优先级取值范围是 1 ～ 254。
- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入 VLANIF 接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **priority** *priority-value*，配置交换机在备份组中的优先级。

     缺省情况下，优先级的取值是 100。优先级 0 是系统保留作为特殊用途的，优先级值 255 保留给 IP 地址拥有者，IP 地址拥有者的优先级不可配置。通过命令可以配置的优先级取值范围是 1 ～ 254。

----结束

（可选）super-VLAN 中 VRRP 报文发送方式

可以根据需要在 VLANIF 接口上配置 super-VLAN 中的 VRRP 通告报文发送方式。

版权所有 © 华为技术有限公司

背景信息

请在配置 super-VLAN 的 VRRP 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface vlanif** *vlan-id*，进入 VLAN 接口视图。

步骤 3 执行命令 **vrrp advertise send-mode** { *sub-vlan-id* | **all** }，配置 VRRP 通告报文发送方式。

缺省情况下，Super-VLAN 仅向自己的状态为 UP 的 VLANID 最小的 Sub-VLAN 发送 VRRP 通告报文。

----结束

检查配置结果

通过查看 VRRP 备份组的状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 备份组功能的所有配置。

操作步骤

- 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]] [**brief**]命令查看 VRRP 备份组的状态信息。
- 使用 **display vrrp6** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**brief**]命令查看 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

对于主备备份方式，配置成功后，执行 **display vrrp** 命令，可以看到 VRRP 备份组的状态。

```
<Quidway> display vrrp
  Vlanif100 | Virtual Router 1
    state         : Master
    Virtual IP    : 10.1.1.111
    Master IP     : 10.1.1.1
    PriorityRun   : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt       : YES     Delay Time   : 20
    TimerRun      : 1
    TimerConfig   : 1
    Auth Type     : NONE
    Virtual Mac   : 0000-5e00-0201
    Check TTL     : YES
    Config type   : normal-vrrp
    Config track link-bfd down-number : 0
```

对于负载分担方式，配置成功后，在交换机上执行 **display vrrp** 命令，可以看到交换机在不同备份组中的状态。

```
<Quidway> display vrrp
```


版权所有 © 华为技术有限公司

```
  Vlanif10 | Virtual Router 1
    state           : Master
    Virtual IP      : 10.1.1.111
    Master IP       : 10.1.1.1
    PriorityRun     : 120
    PriorityConfig  : 120
    MasterPriority  : 120
    Preempt         : YES     Delay Time   : 0
    TimerRun        : 1
    TimerConfig     : 1
    Auth Type       : NONE
    Virtual Mac     : 0000-5e00-0201
    Check TTL       : YES
    Config type     : normal-vrrp
    Config track link-bfd down-number : 0
   Vlanif100 | Virtual Router 2
    state           : Backup
    Virtual IP      : 10.1.1.112
    Master IP       : 10.1.1.1
    PriorityRun     : 100
    PriorityConfig  : 100
    MasterPriority  : 120
    Preempt         : YES      Delay Time    : 0
    TimerRun        : 1
    TimerConfig     : 1
    Auth Type       : NONE
    Virtual Mac     : 0000-5e00-0102
    Check TTL       : YES
    Config type     : normal-vrrp
Config track link-bfd down-number : 0
```

配置成功后，在交换机上执行 **display vrrp6** 命令，查看 VRRP6 备份组的信息。

```
<Quidway> display vrrp6
  Vlanif100 | Virtual Router 1
    State             : Master
    Virtual IP        : FE80::1:2
    Master IP : FE80::218:82FF:FED3:2AF1
    PriorityRun       : 200
    PriorityConfig    : 200
    MasterPriority    : 200
    Preempt           : YES      Delay Time : 0
    TimerRun          : 100
    TimerConfig       : 100
    Virtual Mac       : 0000-5e00-0201
    Uncheck hop limit : YES
    Accept Mode       : ON
    Config type       : normal-vrrp
    Track If          : GigabitEthernet0/0/2   priority reduced : 70
    IF State          : UP
```

9.7.4 配置 VRRP 监视接口状态

通过配置 VRRP 备份组监视接口状态，实现接口故障时提供的备份功能。

建立配置任务

在配置 VRRP 备份组监视接口状态的功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

VRRP 具备监视接口状态的功能，即不仅在备份组所在的接口出现故障时提供备份功能，而且在交换机的某个其它端口出现故障时也提供备份功能。

版权所有 © 华为技术有限公司

监视接口状态的实现方式是：

1. 当被监视的接口 Down 时，这个交换机在备份组的优先级自动减低一个数额（priority-reduced），致使备份组内其它的交换机的优先级高于这个交换机的优先级。
2. 优先级最高的交换机转变为 Master，完成主备切换。

前置任务

在配置 VRRP 监视接口状态之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在配置 VRRP 监视接口状态之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	需要监视的接口和升高或降低的优先级

配置 VRRP 监视接口状态

通过在接口上配置 VRRP 备份组监视接口状态，可以实现 VRRP 主备快速切换的功能。

背景信息

可以在交换机其它接口不可用时进行备份，在 NAT 应用中需要配置该特性。

在欲监视的接口所在的交换机上进行如下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]，监视指定接口的状态。
     - 缺省情况下，当被监视的接口变为 Down 时，优先级的数值降低 10。
     - **increased** *value-increased*：设置当被监视的接口状态变为 Down 时，优先级增加的数值。取值范围是 1 ～ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。
     - **reduced** *value-decreased*：设置当被监视的接口状态变为 Down 时，优先级降低的数值。取值范围 1 ～ 255。优先级最低可以降至 1，降至 1 时会发优先级为 0 的 VRRP 通告报文。优先级 0 由系统保留为特殊用途，当 Backup

版权所有 © 华为技术有限公司

设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。

- 如果 VRRP 同时监视 BFD 会话和监视接口，则所监视的 BFD 会话和接口的总数最多为 8 个。
  - 如果配置 VRRP 监视 BFD 会话和接口时全部是增加优先级，则当监视的 BFD 会话或接口全部 Down 时，Backup 端 VRRP 优先级的总和可以超过 Master 端的优先级。
  - 如果配置 VRRP 监视 BFD 会话和接口时不全部是增加优先级，一个或其中几个 BFD 会话或接口 Down，VRRP 优先级重新增加计算就已经超过对端，则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就不会产生任何影响。

说明

一台交换机上最多可以配置监视 8 个接口。并且，当交换机为 IP 地址拥有者时，不允许对其配置监视接口。

- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]，监视指定接口的状态。
     - 缺省情况下，当被监视的接口变为 Down 时，优先级的数值降低 10。
     - **increased** *value-increased*：设置当被监视的接口状态变为 Down 时，优先级增加的数值。取值范围是 1 ～ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。
     - **reduced** *value-reduced*：设置当被监视的接口状态变为 Down 时，优先级降低的数值。取值范围 1 ～ 255。优先级最低可以降至 1，降至 1 时会发优先级为 0 的 VRRP6 通告报文。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。
     - 配置 VRRP6 备份组监视接口状态时，若被监视接口的地址配置了 IPv4 地址，IPv4 协议状态发生变化时，VRRP6 备份组会重新选举 Master。若 VRRP6 备份组监视的接口配置了 IPv6 地址，接口的 IPv6 协议状态变化不会影响 VRRP6 备份组的状态。

----结束

检查配置结果

通过查看备份组所监视的接口及状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 监视接口状态功能的所有配置。

操作步骤

- 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]] [**brief**]命令查看 VRRP 备份组的状态信息。

版权所有 © 华为技术有限公司

- 使用 **display vrrp6** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**brief**]命令查看当前 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

执行 **display vrrp** 或者 **display vrrp6** 命令可以看到 Track IF 和 IF State 字段的信息，Track IF 显示所监视的接口类型和编号，IF State 显示所监视接口的状态是 UP 还是 DOWN。

```
<Quidway> display vrrp
  Vlanif100 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.1
    PriorityRun      : 130
    PriorityConfig   : 130
    MasterPriority   : 130
    Preempt          : YES      Delay Time    : 0
    TimerRun         : 1
    TimerConfig      : 1
    Auth Type        : NONE
    Virtual Mac      : 0000-5e00-0201
    Check TTL        : YES
    Config type      : normal-vrrp
    Config track link-bfd down-number : 0
    Track IF         : GigabitEthernet0/0/2     priority reduced    : 10
    IF State         : UP
<Quidway> display vrrp6
  Vlanif10 | Virtual Router 1
    State             : Master
    Virtual IP        : FE80::1:2
    Master IP : FE80::218:82FF:FED3:2AF1
    PriorityRun       : 200
    PriorityConfig    : 200
    MasterPriority    : 200
    Preempt           : YES      Delay Time : 0
    TimerRun          : 100
    TimerConfig       : 100
    Virtual Mac       : 0000-5e00-0201
    Uncheck hop limit : YES
    Accept Mode       : ON
    Config type       : normal-vrrp
    Track If          : GigabitEthernet0/0/2   priority reduced : 70
    IF State          : UP
```

9.7.5 配置 VRRP 监视 BFD 会话状态

介绍如何配置 VRRP 监视 BFD Session 状态来实现快速切换功能。

建立配置任务

应用环境

使用 VRRP 监视 BFD session，在 BFD session 会话状态改变后通知 VRRP 模块，实现 VRRP 快速切换。

一个 VRRP 备份组可以监视多个 Normal BFD 或多个接口状态。

同时配置监视多个 BFD 的情况下，各个配置相互独立，彼此没有影响。

版权所有 © 华为技术有限公司

VRRP 备份组监视普通 BFD 时，当 BFD 状态变化时，通过修改备份组优先级改变主备状态，被监视的 BFD 会话状态恢复时，交换机在备份组中的优先级将恢复原来的值。

前置任务

在配置 VRRP 监视 BFD 会话状态功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组
- 配置 BFD 会话

数据准备

在配置 VRRP 监视 BFD 会话状态功能之前，需准备以下数据：

序号	数据
1	VRRP 备份组 ID
2	被监视的 BFD 会话 ID 或者 BFD 会话名

配置监视 BFD 会话状态

使用 VRRP 备份组监视 BFD 会话，在 BFD 会话状态改变后通知 VRRP 备份组，实现 VRRP 备份组的快速切换。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

说明

在配置 VRRP 快速切换时，若 VRRP 监视 peer BFD 会话，则必须在两端设备上配置 peer BFD 会话，否则 VRRP 会产生振荡。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入 VRRP 备份组所在的接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-name* } [**increased** *value-increased* | **reduced** *value-reduced*]，监视普通 BFD Session 状态。

     increased *value-increased*：设置当被监视的 BFD session 状态变为 Down 时，优先级增加的数值。取值范围是 1 ～ 255。优先级最高可以达到 254。

     reduced *value-reduced*：设置当被监视的 BFD session 状态变为 Down 时，优先级降低的数值。取值范围 1 ～ 255。优先级最低可以降至 1，降至 1 时会发优

版权所有 © 华为技术有限公司

先级为 0 的 VRRP 通告报文。缺省情况下，当被监视的 BFD session 变为 Down 时，优先级的数值降低 10。

在配置优先级增加值或减少值时，要注意在增加或减少优先级后备份组内 Backup 的优先级高于 Master，从而使 VRRP 状态快速切换，这一点在使用缺省值时尤其要注意。

如果 VRRP 同时监视 BFD 会话和监视接口，所监视的 BFD 会话和接口最多各为 8 个。如果配置监视 BFD 会话和监视接口时全部是增加优先级，当监视的 BFD 会话或接口全部 Down 时，VRRP 的优先级增加的总和可以超过 Master 端的优先级。如果一个或其中几个 BFD 会话或者接口 DOWN，VRRP 优先级就已经超过对端，当再有 BFD 会话或者接口 DOWN 时，所有的 VRRP 监听 BFD 会话和监听接口就都没有任何意义了。

说明

在配置 VRRP 备份组监视 BFD 会话状态时：

- 如果选择参数 **session-name** *bfd-configure-name*，只能绑定动态的 BFD 会话类型。
- 如果选择参数 *session-id*，只能绑定静态的 BFD 会话类型。

- 对于 VRRP for IPv6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入 VRRP 备份组所在的接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]，配置 VRRP6 备份组监视普通 BFD 会话状态。

     increased *value-increased*：当被监视的 BFD 会话状态变为 Down 时，优先级增加的数值。整数形式，取值范围是 1 ～ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。只有 VRRP 备份组的状态为 Backup 时，该参数才生效。

     reduced value-reduced：当被监视的 BFD 会话状态变为 Down 时，优先级降低的数值。整数形式，取值范围时 1 ～ 254。优先级最低可以降至 1，降至 1 时会发优先级为 0 的 VRRP 通告报文。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。缺省情况下，优先级的数值降低 10。

     说明

     在配置优先级值增加或者减少时，需要注意在增加或者减小优先级后，备份组内 Backup 的优先级高于 Master，从而使 VRRP6 备份组快速切换。

     在配置 VRRP6 备份组监视 BFD 会话状态时：

     - 如果选择参数 **session-name** *bfd-configure-name*，只能绑定动态的 BFD 会话类型。
     - 如果选择参数 *session-id*，只能绑定静态的 BFD 会话类型。

----结束

检查配置结果

前提条件

已经完成 VRRP 快速切换功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]]命令查看 VRRP 的状态信息。

----结束

任务示例

执行命令 **display vrrp**，可以看到 VRRP 所监视的 BFD 会话状态是 Up。例如：

```
<Quidway> display vrrp
  Vlanif211 | Virtual Router 10
    State : Master
    Virtual IP : 11.1.1.10
    PriorityRun : 90
    PriorityConfig : 90
    MasterPriority : 90
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-010a
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
    Track BFD : 1  Priority reduced : 10
    BFD-session state : UP
```

9.7.6 配置 VRRP 安全功能

在有可能受到安全威胁的网络中，可以配置 VRRP 报文的认证方式，从而避免设备受到非法的攻击。

建立配置任务

在配置 VRRP 安全功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

在一个安全的网络中，可以采用缺省设置：交换机对要发送的 VRRP 报文不进行任何认证处理，收到 VRRP 报文的交换机也不进行任何认证，认为收到的都是真实的、合法的 VRRP 报文。这种情况下，不需要设置认证字。

在有可能受到安全威胁的网络中，VRRP 提供了简单字符（Simple）认证方式和 MD5 认证方式。对于简单认证字方式，可以设置长度为 1 ～ 8 的认证字；对于 MD5 认证方式，明文长度范围是 1 ～ 8，密文长度为 24。

简单字符认证方式的工作过程主要包括：

- 发送方交换机将认证字填入到 VRRP 报文中。
- 接收方将收到的 VRRP 报文中的认证字与本地配置的认证字比较。如果相同，认为是真实的、合法的 VRRP 报文；如果不同，则认为是非法报文，丢弃，并会向网管发送告警消息（Trap）。

MD5 认证方式的工作过程主要包括：

- 发送方交换机将认证字填入到 VRRP 报文中。

版权所有 © 华为技术有限公司

- 接收方将根据本地配置的认证字而形成摘要，将收到的 VRRP 报文中的摘要和形成的摘要进行比较，如果相同，认为是真实的、合法的 VRRP 报文；如果不同，则认为是非法报文，丢弃，并会向网管发送告警消息（Trap）。

前置任务

在配置 VRRP 安全功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在配置 VRRP 安全功能之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	备份组的虚拟 IP 地址
3	VRRP 报文安全认证字

配置 VRRP 报文认证方式

VRRP 报文有两种认证方式：简单字符认证方式和 MD5 认证方式。

背景信息

请在需要配置 VRRP 报文认证方式的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建备份组并配置虚拟 IP 地址。

步骤 4 （可选）执行命令 **vrrp vrid** *virtual-router-id* **priority** *priority-value*，配置交换机在备份组中的优先级。

步骤 5 执行命令 **vrrp vrid** *virtual-router-id* **authentication-mode** { **simple** *key* | **md5** *md5-key* }，配置 VRRP 报文认证方式。

同一 VRRP 备份组的认证方式必须相同，否则 Master 设备和 Backup 设备无法协商成功。

由于符号$@$@作为变长密码的前缀和后缀，用来识别变长密码，不支持以“$@$@”同时作为明文密码的起始和结束字符。

----结束

版权所有 © 华为技术有限公司

检查配置结果

通过查看 VRRP 报文的认证方式和认证字等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 安全功能的所有配置。

操作步骤

步骤 1 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]]命令查看 VRRP 的状态信息。

----结束

任务示例

配置成功后，使用 **display vrrp** 可以看到报文认证方式。

```
<Quidway> display vrrp
  Vlanif100 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig   : 120
    MasterPriority   : 120
    Preempt          : YES            Delay Time : 20
    TimerRun         : 1
    TimerConfig      : 1
    Auth Type        : MD5            Auth key : >6M*PO438G/Q=^Q`MAF4<1!!
    Virtual Mac      : 0000-5e00-0101
    Check TTL        : YES
    Config type      : normal-vrrp
    Config track link-bfd down-number : 0
```

在以上显示信息中，可以看到“Auth Type”字段显示为“**MD5**”，“Auth key”字段显示为“**>6M*PO438G/Q=^Q`MAF4<1!!**”，即 VRRP 备份组 1 的报文认证方式为 MD5 认证，密文为“**>6M*PO438G/Q=^Q`MAF4<1!!**”。

9.7.7 调整优化 VRRP

可以调整 VRRP 备份组的参数来优化 VRRP 备份组的功能。

建立配置任务

在调整优化 VRRP 功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

配置 VRRP 报文的相关参数可以优化备份组功能：

- 通过增大虚拟交换机发送 VRRP 通告报文的时间间隔，可以减轻协议报文造成的网络负荷。
- VRRP 报文的通告时间间隔：

版权所有 © 华为技术有限公司

- 对于 VRRP for IPv4，通过设置备份组内成员发送的 VRRP 通告报文时间间隔一致，可以避免同一备份组内出现多个 Master。
- 对于 VRRP6，即使设置备份组内成员发送的 VRRP 通告报文的时间间隔不一致，同一备份组内也不会出现多个 Master。

- 通过配置备份组交换机的抢占方式和抢占延迟时间，可以加快或减慢主备设备之间的切换速度。
- 通过使能虚拟 IP 地址可达性测试开关，可以使用 Ping 功能检测网络的连通性。
- 通过禁止检测 VRRP 报文的跳数值，可以提高不同厂商设备的兼容性。

前置任务

在调整优化 VRRP 之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在调整优化 VRRP 之前，需要准备以下数据。

序号	数据
1	发送 VRRP 通告报文的时间间隔
2	备份组中交换机的抢占延迟时间
3	Master 发送免费 ARP 报文的超时时间

配置发送 VRRP 通告报文的时间间隔

通过增大虚拟交换机发送 VRRP 通告报文的时间间隔，可以减轻协议报文造成的网络负荷。

背景信息

Master 设备每隔一定时间向组内其他 Backup 设备发送 VRRP 通告报文，通知自己工作正常。如果 Backup 定时器超时后仍未收到 VRRP 通告报文，则优先级最高的 Backup 自动变成 Master。

请在需要调整 VRRP 通告报文时间间隔的交换机上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **timer advertise** *advertise-interval*，配置发送 VRRP 通告报文的间隔时间。

版权所有 © 华为技术有限公司

缺省情况下，发送 VRRP 通告报文的时间是 1 秒。在存在多个备份组的情况下，时间间隔太短会导致 VRRP 状态频繁倒换，可能需要增大时间间隔。

说明

- 如果两台 VRRP 设备配置 *interval* 一致，则两台才能形成主备关系。
- 如果两台 VRRP 设备配置 *interval* 不一致，则两台设备都是 Master。

- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **timer advertise** *interval*，配置发送 VRRP6 通告报文的时间间隔。

     缺省情况下，Master 设备发送 VRRP6 通告报文的时间间隔为 100 厘秒，即 1 秒。

     Master 路由设备在间隔时间内发送 VRRP6 通告报文告知备份组内的 Backup 路由设备其正常工作。如果 Backup 路由设备在计时器老化之前没有收到 VRRP6 通告报文，那么优先级最高的 Backup 路由设备自动成为 Master 路由设备。

----结束

设置备份组中交换机的抢占延迟时间

通过设置备份组中交换机的抢占延迟时间，可以加快或者减慢主备之间的切换速度。

背景信息

请在需要调整抢占延迟时间的 VRRP 备份组交换机上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value*，配置备份组中交换机的抢占延迟时间。

     缺省方式是抢占方式，延迟时间为 0，即立即抢占。立即抢占方式下，Backup 设备一旦发现自己的优先级比当前的 Master 的优先级高，就会成为 Master；相应地，原来的 Master 将会变成 Backup。设置抢占延迟时间，可以使 Backup 延迟一段时间成为 Master。

     可以执行 **vrrp vrid** *virtual-router-id* **preempt-mode disable** 命令设置备份组中交换机采用非抢占方式。在非抢占方式下，一旦备份组中的某台交换机成为 Master，只要它没有出现故障，其它交换机即使随后被配置更高的优先级也不会成为 Master。

     当 IP 地址拥有者故障恢复后，不会等待延时抢占，会立即切换到 Master。而延时抢占功能是指 Backup 设备切换到 Master 的等待时间，所以，IP 地址拥有者和延时抢占功能不相关。对于需要支持延时抢占功能的备份组，不能把 VRRP 备份组的主用设备配置成 IP 地址拥有者。

版权所有 © 华为技术有限公司

执行 **undo vrrp vrid** *virtual-router-id* **preempt-mode** 命令用来恢复缺省的抢占方式。

说明

在配置 VRRP 备份组内各交换机的延迟方式时，建议将 Backup 配置为立即抢占，即不延迟（延迟时间为 0），而将 Master 配置为抢占，并且配置一定的延迟时间。这样配置的目的是为了在网络环境不稳定时，为上下行链路的状态恢复一致性等待一定时间，以免出现双 Master 或由于双方频繁抢占导致用户设备学习到错误的 Master 设备地址。

- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value*，配置备份组中交换机的抢占延迟时间。

     缺省方式是抢占方式，延迟时间为 0，即立即抢占。立即抢占方式下，Backup 设备一旦发现自己的优先级比当前的 Master 的优先级高，就会成为 Master；相应地，原来的 Master 将会变成 Backup。设置抢占延迟时间，可以使 Backup 延迟一段时间成为 Master。

     可以执行 **vrrp6 vrid preempt-mode disable** 命令设置备份组中交换机采用非抢占方式。在非抢占方式下，一旦备份组中的某台交换机成为 Master，只要它没有出现故障，其它交换机即使随后被配置更高的优先级也不会成为 Master。

     当 IP 地址拥有者故障恢复后，不会等待延时抢占，会立即切换到 Master。而延时抢占功能是指 Backup 设备切换到 Master 的等待时间，所以，IP 地址拥有者和延时抢占功能不相关。对于需要支持延时抢占功能的备份组，不能把 VRRP 备份组的主用设备配置成 IP 地址拥有者。

     执行 **undo vrrp6 vrid preempt-mode** 命令用来恢复缺省的抢占方式。

     说明

     在配置 VRRP 备份组内各交换机的延迟方式时，建议将 Backup 配置为立即抢占，即不延迟（延迟时间为 0），而将 Master 配置为抢占，并且配置一定的延迟时间。这样配置的目的是为了在网络环境不稳定时，为上下行链路的状态恢复一致性等待一定时间，以免出现双 Master 或由于双方频繁抢占导致用户设备学习到错误的 Master 设备地址。

----结束

使能虚拟地址可达性测试开关

通过使能虚拟 IP 地址可达性开关，可以使用 Ping 功能检测网络可达性。

背景信息

AC6605 支持对虚拟 IP 地址的 Ping 功能，可用于：

- 检测备份组中的 Master 设备是否起作用。
- 检测是否能通过使用某虚拟 IP 地址作为默认网关与外部通信。

请在需要使能虚拟地址可达的交换机上进行以下配置。

该场景对于 VRRP for IPv4 和 VRRP6 同时有效。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp virtual-ip ping enable**，使能虚拟地址可达性测试开关。

缺省情况下，该功能是打开的，Master 设备响应对本备份组虚拟 IP 地址的 Ping 报文。

能够 Ping 通虚拟 IP 地址，带来可能遭受 ICMP 攻击的隐患，可以执行 **undo vrrp virtual-ip ping enable** 命令来关闭虚拟地址可达性开关。

----结束

禁止检测 VRRP 报文的跳数

过禁止检测 VRRP 报文的跳数，可以提高不同厂商设备的兼容性。

背景信息

按照 RFC3768 定义，系统对收到的 VRRP 报文的跳数值进行检测，如果这个值不等于 255，报文将被丢弃。

在不同厂商的设备配合使用的组网环境中，检测 VRRP 报文的跳数值可能导致错误地丢弃报文。这时可以配置系统不检测 VRRP 报文的跳数值。

请在需要禁止检测 VRRP 报文的跳数的交换机上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp un-check ttl**，禁止检测 VRRP 报文的 TTL 值。

     缺省情况下，检测 VRRP 报文的 TTL 值。可以执行 **undo vrrp un-check ttl** 命令来启动对 VRRP 报文 TTL 值的检测。
- 对于 VRRP6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 un-check hop-limit**，禁止检测 VRRP6 报文跳数值。

     缺省情况下，检测 VRRP6 报文的跳数值。可以执行 **undo vrrp6 un-check hop-limit** 命令来启动对 VRRP6 报文跳数值的检测。

----结束

配置 Master 发送免费 ARP 报文的超时时间

通过调整 Master 设备发送免费 ARP 报文的时间间隔，可以减轻协议报文造成的网络负荷。

版权所有 © 华为技术有限公司

背景信息

请在需要配置发送免费 ARP 报文的交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp gratuitous-arp timeout** *time*，配置 Master 发送免费 ARP 报文的超时时间。

Master 设备发送 ARP 报文时携带的是虚拟 MAC 地址。缺省情况下，Master 每隔 120 秒（2 分钟）发送一次免费 ARP 报文。

如果要恢复 Master 发送免费 ARP 报文的缺省超时时间，请在系统视图下执行 **undo vrrp gratuitous-arp timeout** 命令。

如果不需要发送免费 ARP 报文，请在系统视图下执行 **vrrp gratuitous-arp timeout disable** 命令。

----结束

检查配置结果

通过查看调整后的 VRRP 备份组的参数，来检查配置是否成功。

前提条件

已经完成调整优化 VRRP 功能的所有配置。

操作步骤

- 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]] [**brief**]命令查看 VRRP 备份组的状态信息。
- 使用 **display vrrp6** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**brief**]查看当前 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

执行 **display vrrp** 命令，可以看到对 VRRP 的调整结果，例如，“TimerRun”和“TimerConfig”字段显示为“20”，将发送 VRRP 通告报文的时间调整为 20 秒（默认情况下为 1 秒）。

```
<Quidway> display vrrp
  Vlanif100 | Virtual Router 1
    State             : Master
    Virtual IP        : 100.1.1.111
    Master IP         : 10.1.1.1
    PriorityRun       : 120
    PriorityConfig    : 120
    MasterPriority    : 120
    Preempt           : YES       Delay Time : 0
    TimerRun          : 20
    TimerConfig       : 20
    Auth Type         : NONE
    Virtual Mac       : 0000-5e00-0201
    Check TTL         : YES
```


版权所有 © 华为技术有限公司

```
    Config type      : normal-vrrp
    Config track link-bfd down-number : 0
<Quidway> display vrrp6
  GigabitEthernet1/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : FE80::1:2
    Master IP : FE80::218:82FF:FED3:2AF1
    PriorityRun      : 200
    PriorityConfig   : 200
    MasterPriority   : 200
    Preempt          : YES      Delay Time : 0
    TimerRun         : 200
    TimerConfig      : 20
    Virtual Mac      : 0000-5e00-0201
    Uncheck hop limit : YES
    Accept Mode      : ON
    Config type      : normal-vrrp
    Track If         : GigabitEthernet0/0/1   priority reduced : 70
    IF State         : UP
```

9.7.8 配置管理 VRRP 备份组

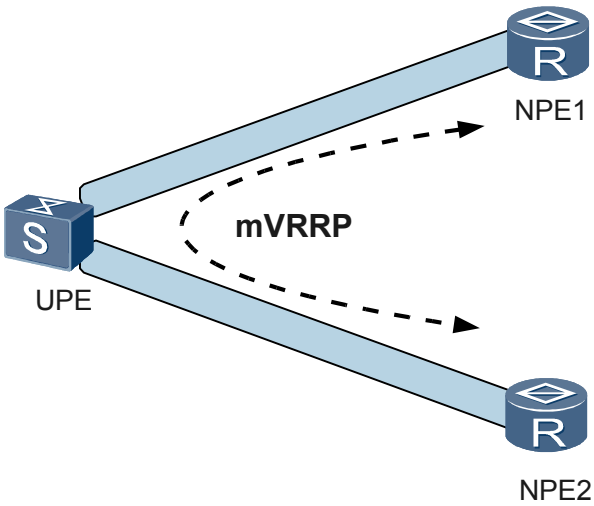
管理 VRRP 备份组可以绑定其它的业务备份组，并根据绑定关系，决定相关业务备份组的状态。它主要解决城域以太网中的主备双归属问题。

建立配置任务

在配置管理 VRRP 备份组功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

图 9-51 管理 VRRP 决定主备双归属



如图 9-51 所示，当城域以太网的汇聚层使用汇聚时，为了提高可靠性，通常部署双 NPE。NPE 之间通过运行管理 VRRP 来决定主备关系。

管理 VRRP 备份组从本质上讲就是普通的 VRRP 备份组，它与普通 VRRP 备份组的唯一区别在于：管理 VRRP 备份组可以绑定其他的业务备份组，并根据绑定关系，决定相关业务备份组的状态。

版权所有 © 华为技术有限公司

一个管理 VRRP 备份组可以绑定多个业务备份组，但它不能作为业务备份组与其他管理备份组进行绑定。

根据不同的应用场景，管理 VRRP 的绑定关系可分为：

- 成员 VRRP 备份组与管理 VRRP 备份组绑定：UPE 双归属到 NPE，NPE 之间运行 VRRP，通过配置 VRRP 的优先级来决定主用 NPE 和备用 NPE。为了满足不同的业务需要，NPE 之间可以运行多个 VRRP 备份组。

  每个 VRRP 备份组都需要维护自己的状态机，这样 NPE 之间就会存在大量的 VRRP 协议报文。为了简化协议操作，减少协议报文对带宽的占用，可以将其中一个 VRRP 备份组配置为管理备份组，其余业务备份组与管理备份组进行绑定，并根据绑定管理直接决定业务备份组的状态。
- 业务接口与管理 VRRP 备份组绑定：如果 UPE 通过两条物理链路双归属到 NPE，可以配置业务接口与管理 VRRP 绑定来决定主用业务接口和备用业务接口。

前置任务

在配置管理 VRRP 之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通

数据准备

在配置管理 VRRP 备份组之前，需要准备以下数据。

序号	数据
1	管理 VRRP 和成员 VRRP 备份组 ID
2	管理 VRRP 和成员 VRRP 备份组虚拟 IP 地址
3	管理 VRRP 优先级
4	业务接口编号

配置管理 VRRP 备份组

每个 VRRP 备份组都要维护自己的状态机，配置管理 VRRP 备份组，可以减少协议报文对带宽的占用。

背景信息

请在管理 VRRP 备份组所在的交换机上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

版权所有 © 华为技术有限公司

3. 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建备份组并配置虚拟 IP 地址。
4. 执行命令 **vrrp vrid** *virtual-router-id* **priority** *priority-value*，配置 VRRP 备份组的优先级。
5. 执行命令 **admin-vrrp vrid** *virtual-router-id*，配置该 VRRP 备份组为管理 VRRP 备份组。

- 对于 VRRP for IPv6：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]，创建备份组并配置虚拟 IPv6 地址。
  4. 执行命令 **vrrp6 vrid** *virtual-router-id* **priority** *priority-value*，配置备份组的优先级。
  5. 执行命令 **admin-vrrp6 vrid** *virtual-router-id*，配置该备份组为管理 VRRP6 备份组。

----结束

（可选）配置成员 VRRP 备份组并将其与管理 VRRP 备份组绑定

配置成员 VRRP 备份组与管理 VRRP 备份组绑定，实现成员 VRRP 备份组和管理 VRRP 备份组状态机的一致性。

背景信息

请在需要将成员 VRRP 备份组与管理 VRRP 绑定的交换机上进行以下配置。

操作步骤

- 对于 VRRP for IPv4：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入运行成员 VRRP 备份组所在的接口视图。
  3. 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建成员 VRRP 备份组并配置虚拟 IP 地址。

     由于成员 VRRP 备份组的状态由管理 VRRP 备份组决定，因此，无需为成员 VRRP 备份组配置优先级。
  4. 执行命令 **vrrp vrid** *virtual-router-id1* **track admin-vrrp interface** *interface-type interface-number* **vrid** *virtual-router-id2*，将成员 VRRP 备份组与管理 VRRP 备份组绑定。

     成员 VRRP 备份组与管理 VRRP 备份组绑定之后，成员 VRRP 状态机就丧失了独立性，即会删除协议定时器、不再收发协议报文，通过直接拷贝管理备份组的状态来实现自己的状态机。成员 VRRP 备份组只能绑定到一个管理 VRRP 备份组。

     说明
     一个接口上仅能配置一个业务 VRRP。
- 对于 VRRP for IPv6：

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入运行成员 VRRP6 备份组所在的接口视图。
3. 执行命令 **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]，创建成员 VRRP6 备份组并配置虚拟 IPv6 地址。

   由于成员 VRRP6 备份组的状态由管理 VRRP6 备份组决定，因此，无需为成员 VRRP6 备份组配置优先级。
4. 执行命令 **vrrp6 vrid** *virtual-router-id1* **track admin-vrrp6 interface** *interface-type interface-number* **vrid** *virtual-router-id2*，将成员 VRRP6 备份组与管理 VRRP6 备份组绑定。

   成员 VRRP6 备份组与管理 VRRP6 备份组绑定之后，成员 VRRP6 备份组的状态机就丧失了独立性，即会删除协议定时器、不再收发协议报文，通过直接拷贝管理 VRRP6 备份组的状态来实现自己的状态机。成员 VRRP6 备份组只能绑定到一个管理 VRRP6 备份组。

   说明
   一个接口上仅能配置一个业务 VRRP6。

----结束

检查配置结果

通过查看管理 VRRP 备份组的所有绑定信息，来检查配置是否成功。

前提条件

已经完成管理 VRRP 备份组功能的所有配置。

操作步骤

- 使用 **display vrrp binding admin-vrrp** [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*]命令查看管理 VRRP 所有的绑定信息。
- 使用 **display vrrp binding admin-vrrp** [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id1*] **member-vrrp** [**interface** *interface-type2 interface-number2*] [**vrid** *virtual-router-id2*]命令查看管理 VRRP 备份组与成员 VRRP 备份组的绑定关系。
- 使用 **display vrrp binding admin-vrrp** [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id*] **member-interface** [**interface** *interface-type2 interface-number2*]命令查看管理 VRRP 备份组与成员业务接口的绑定关系。
- 使用 **display vrrp admin-vrrp** 查看当前配置中所有管理 VRRP 的状态。

----结束

任务示例

配置完成后，执行 **display vrrp binding admin-vrrp** 命令可以看到管理 VRRP 所有的绑定信息，包括成员 VRRP、业务接口和成员 PW。

```
<Quidway> display vrrp binding admin-vrrp
Interface: Vlanif 100, admin-vrrp vrid: 6, state: Master
  Member-vrrp number: 1
    Interface: Vlanif 200, vrid: 8, state: Master
```


版权所有 © 华为技术有限公司

```
Member-interface number: 1
  Interface: Vlanif 300, state: Up
```

9.7.9 配置 VRRP 协议版本升级

通过将 VRRP 协议由版本 2 升级到版本 3，实现 VRRP 协议既支持 IPv6 网络也支持 IPv4 网络。

建立配置任务

在配置 VRRP 协议版本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

目前，VRRP 协议的版本号是 2。VRRP for IPv4 只支持 VRRPv2 报文格式，而 VRRP for IPv6 既支持 VRRPv3 报文格式，也支持 VRRPv2 报文格式。如果用户需要将 VRRP 协议的版本进行升级，则可以执行此配置。

前置任务

在配置 VRRP 协议版本升级之前，需完成以下任务：

- 设备安装完毕并加电启动正常
- 当前 VRRP 协议的版本号是 2

数据准备

配置 VRRP 协议版本升级之前，需要准备以下数据。

序号	数据
1	VRRP 协议的版本号

配置 VRRPv3 版本

通过配置 VRRPv3 版本，实现备份组既能接收版本 v2 的通告报文，也能接收版本 v3 的通告报文。

背景信息

请在备份组的各交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp version v3**，设置当前设备的 VRRP 协议版本号是 3。

步骤 3 （可选）执行命令 **vrrp version-3 send-packet-mode** { **v2-only** | **v3-only** | **v2v3-both** }，设置 VRRPv3 发送通告报文的模式。

版权所有 © 华为技术有限公司

缺省情况下，VRRP 版本协议为 v2。切换到 v3 模式下，缺省的通告报文模式为 **v3-only**。

----结束

检查配置结果

通过查看 VRRP 协议的版本信息，检查配置是否成功。

前提条件

已经完成 VRRP 协议版本升级功能的所有配置。

操作步骤

- 使用 **display vrrp protocol-information** 命令查看 VRRP 协议的相关信息。

----结束

任务示例

配置成功后，执行 **display vrrp protocol-information** 命令，可以看到 VRRP 协议的版本是 **v3**，发送通告报文的模式是 **send v3 only**

```
<Quidway> display vrrp protocol-information
VRRP protocol information is shown as below:
                        VRRP protocol version : v3
               Send advertisement packet mode : send v3 only
```

9.7.10 维护 VRRP

通过维护 VRRP，可以实现清除 VRRP 统计数据和监控 VRRP 的运行状况的目的。

调试 VRRP

调试完成后，应及时关闭调试开关。

背景信息



注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 VRRP 运行故障时，请在用户视图下执行下面的 **debugging** 命令对 VRRP 进行调试，查看调试信息，并定位故障的原因。

操作步骤

- 使用 **debugging vrrp packet** 命令打开 VRRP 报文调试开关。
- 使用 **debugging vrrp state** 命令打开 VRRP 状态调试开关。

版权所有 © 华为技术有限公司

- 使用 **debugging vrrp timer** 令打开 VRRP 定时器调试开关。

----结束

9.7.11 配置举例

介绍 VRRP 的配置举例。

配置主备备份 VRRP 示例

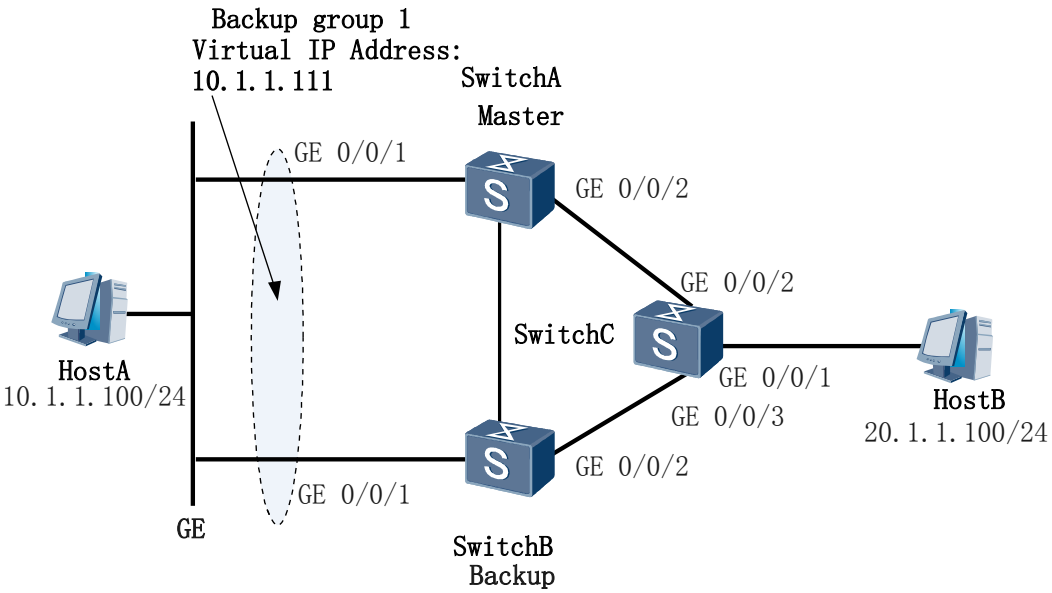
组网需求

如图 9-52 所示。主机 HostA 通过缺省网关访问主机 HostB。

需求如下：

- SwitchA 和 SwitchB 组成 VRRP 备份组，作为 HostA 的缺省网关。
- 正常情况下，SwitchA 承担网关工作；当 SwitchA 出现故障时，SwitchB 接替执行网关工作。
- SwitchA 恢复后，能在 20 秒内抢占成为 Master。

图 9-52 配置主备备份 VRRP 组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE0/0/1	VLANIF100	10.1.1.1/24
	GE0/0/2	VLANIF200	192.168.1.1/24
SwitchB	GE0/0/1	VLANIF100	10.1.1.2/24
	GE0/0/2	VLANIF400	192.168.2.1/24
SwitchC	GE0/0/1	VLANIF300	20.1.1.1/24
	GE0/0/2	VLANIF200	192.168.1.2/24

版权所有 © 华为技术有限公司

GE0/0/3	VLANIF400	192.168.2.2/24

配置思路

采用如下思路配置主备备份 VRRP：

1. 在 SwitchA 的 VLANIF100 接口下创建备份组 1，并配置 SwitchA 在该备份组中具有高优先级，确保 SwitchA 为 Master，配置抢占方式。
2. 在 SwitchB 的 VLANIF100 接口下创建备份组 1，使用缺省优先级。

数据准备

为完成此配置例，需准备如下的数据：

- 创建 VLAN，在 VLANIF 接口配置 IP 地址
- SwitchA、SwitchB 和 SwitchC 之间配置 OSPF 协议互连。
- VRRP 备份组 ID、虚拟 IP 地址
- 交换机在备份组中的优先级
- 抢占方式

操作步骤

步骤 1 创建 VLAN，在 VLANIF 接口配置 IP 地址

创建 VLAN，将物理接口加入 VLAN。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-GigabitEthernet0/0/1] quit
```

SwitchB、SwitchC 和 SwitchA 配置相似。

在 SwitchA 的 VLANIF 接口配置 IP 地址。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] ip address 192.168.1.1 24
[SwitchA-Vlanif200] quit
```

在 SwitchB 的 VLANIF 接口配置 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 400
[SwitchB-Vlanif400] ip address 192.168.2.1 24
[SwitchB-Vlanif400] quit
```

在 SwitchC 的 VLANIF 接口配置 IP 地址。

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] interface vlanif 200
[SwitchC-Vlanif200] ip address 192.168.1.2 24
[SwitchC-Vlanif200] quit
[SwitchC] interface vlanif 300
[SwitchC-Vlanif300] ip address 20.1.1.1 24
[SwitchC-Vlanif300] quit
[SwitchC] interface vlanif 400
[SwitchC-Vlanif400] ip address 192.168.2.2 24
[SwitchC-Vlanif400] quit
```

步骤 2 配置设备之间的网络互连，在 SwitchA、SwitchB、SwitchC 之间采用 OSPF 协议进行互连

配置 SwitchA

```
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 SwitchB

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 SwitchC

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

设置主机 HostA 的缺省网关为 10.1.1.111，HostB 的缺省网关为 20.1.1.1。

步骤 3 配置 VRRP

在 SwitchA 上创建备份组 1，并配置 SwitchA 在该备份组中的优先级为 120（作为 Master）。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

在 SwitchB 上创建备份组 1，并配置 SwitchB 在该备份组中的优先级为缺省值（作为 Backup）。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

步骤 4 检验配置结果

- 验证 VRRP 备份组能够正常提供网关功能

版权所有 © 华为技术有限公司

完成以上配置后，在主机 HostA 上能够 Ping 通 HostB，在 SwitchA 上执行 **display vrrp** 命令可以看到 SwitchA 的状态是 Master，在 SwitchB 上执行 **display vrrp** 命令可以看到 SwitchB 的状态是 Backup，如下所示。

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 20
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 1
    state : Backup
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

在 SwitchA 和 SwitchB 上执行 **display ip routing-table** 命令，SwitchA 上可以看到路由表中有一条目的地址为虚拟 IP 地址的直连路由，而 SwitchB 上该路由为 OSPF 路由。SwitchA 和 SwitchB 上的显示信息如下。

```
[SwitchA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 10
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct 0    0           D   10.1.1.1        Vlanif100
       10.1.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
       20.1.1.0/24  OSPF   10   2           D   192.168.1.2     Vlanif200
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D   192.168.1.1     Vlanif200
    192.168.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0           D   192.168.1.2     Vlanif200
    192.168.2.0/24  OSPF   10   2           D   10.1.1.2        Vlanif200
[SwitchB] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 10
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct 0    0           D   10.1.1.2        Vlanif100
       10.1.1.2/32  Direct 0    0           D   127.0.0.1       InLoopBack0
       20.1.1.0/24  OSPF   10   2           D   192.168.2.2     Vlanif300
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF   10   2           D   10.1.1.1        Vlanif200
```


版权所有 © 华为技术有限公司

```
192.168.2.0/24  Direct 0    0           D  192.168.2.1     Vlanif400
192.168.2.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
192.168.2.2/32  Direct 0    0           D  192.168.2.2     Vlanif400
```

- 验证 SwitchA 故障时 SwitchB 能够成为 Master

对 SwitchA 的 VLANIF100 接口执行 **shutdown** 命令，模拟 SwitchA 出现故障。

在 SwitchB 上使用 **display vrrp** 命令查看 VRRP 状态信息，应能够看到 SwitchB 的状态是 Master，如下。

```
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

- 验证 SwitchA 恢复后能够抢占

对 SwitchA 的 VLANIF100 接口执行 **undo shutdown** 命令，VLANIF100 接口恢复 UP 状态后，等待 20 秒，在 SwitchA 上使用 **display vrrp** 命令查看 VRRP 状态信息，应能够看到 SwitchA 的状态恢复成 Master。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
#
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100 400
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
#
interface Vlanif400
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif300
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif400
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

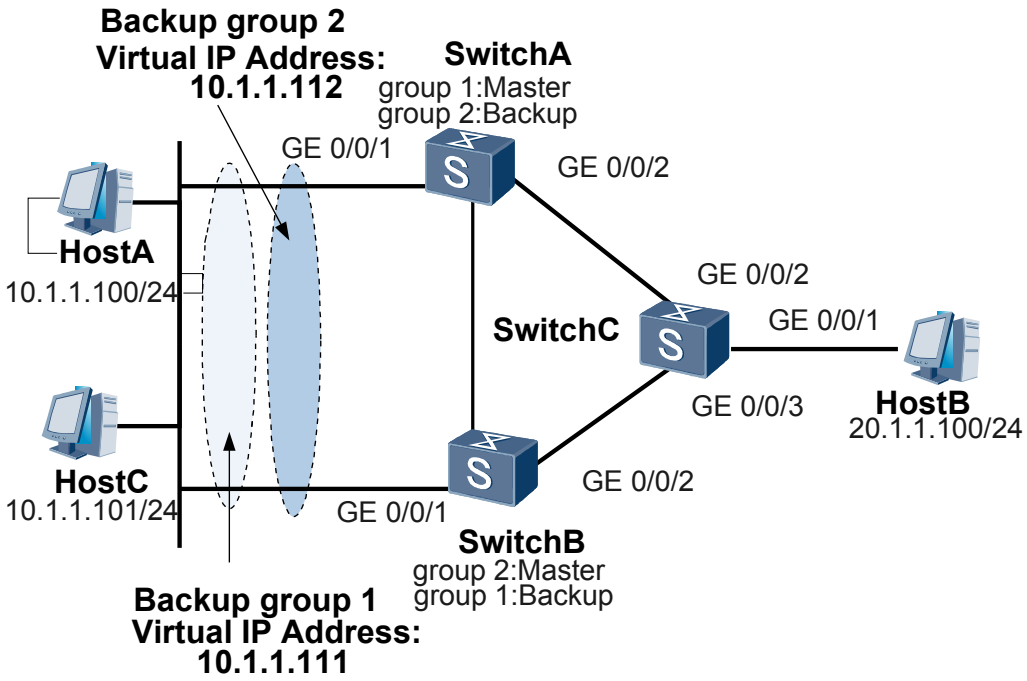
配置负载分担 VRRP 示例

组网需求

如图 9-53 所示。

- SwitchA 作为备份组 1 的 Master，兼任备份组 2 的 Backup。
- SwitchB 作为备份组 2 的 Master，兼任备份组 1 的 Backup。
- 内部网络中的 HostA 使用备份组 1 作网关，HostC 主机使用备份组 2 作为网关，达到分担数据流而又相互备份的目的。

图 9-53 配置负载分担 VRRP 组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE0/0/1	VLANIF100	10.1.1.1/24
	GE0/0/2	VLANIF200	192.168.1.1/24
SwitchB	GE0/0/1	VLANIF100	10.1.1.2/24
	GE0/0/2	VLANIF400	192.168.2.1/24
SwitchC	GE0/0/1	VLANIF300	20.1.1.1/24
	GE0/0/2	VLANIF200	192.168.1.2/24
	GE0/0/3	VLANIF400	192.168.2.2/24

配置思路

采用如下思路配置负载分担 VRRP：

版权所有 © 华为技术有限公司

1. 配置设备之间的网络互连。
2. 在 SwitchA 的 VLANIF100 接口下创建 2 个备份组，SwitchA 在备份组 1 中作为 Master，在备份组 2 中作为 Backup。
3. 在 SwitchB 的 VLANIF100 接口下创建 2 个备份组，SwitchB 在备份组 1 中作为 Backup，在备份组 2 中作为 Master。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址
- 交换机在备份组中的优先级

操作步骤

步骤 1 配置设备之间的网络互连

配置主机 HostA 的缺省网关为备份组 1 的虚拟 IP 地址 10.1.1.111，配置主机 HostB 的缺省网关为 20.1.1.1，配置主机 HostC 的缺省网关为备份组 2 的虚拟 IP 地址 10.1.1.112。

配置 SwitchA、SwitchB、SwitchC 之间运行 OSPF。

详细配置过程请参看“**5.4 OSPF 配置**”。

步骤 2 配置 VRRP

在 SwitchA 上配置接口 VLANIF100，创建备份组 1，并配置 SwitchA 在备份组 1 中的优先级为 120（作为 Master）。创建备份组 2，并配置 SwitchA 在备份组 2 中的优先级为缺省值 100（作为 Backup）。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface Vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchA-Vlanif100] quit
```

在 SwitchB 上配置接口 VLANIF100，创建备份组 1，并配置 SwitchB 在备份组 1 中的优先级为缺省值 100（作为 Backup）。创建备份组 2，并配置 SwitchB 在备份组 2 中的优先级为 120（作为 Master）。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchB-Vlanif100] vrrp vrid 2 priority 120
[SwitchB-Vlanif100] quit
```

步骤 3 检验配置结果

完成以上配置后，网络中 HostA、HostC 主机分别能够 Ping 通 HostB。

在 HostA 和 HostC 上分别对 HostB 的地址进行 **tracert** 测试，可以看到 HostA 经过 SwitchA 和 SwitchC 到达 HostB，而 HostC 经过 SwitchB 和 SwitchC 到达 HostB。即，SwitchA 和 SwitchB 对内部网络来的流量进行负载分担。

版权所有 © 华为技术有限公司

```
<HostA> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100) 30 hops max,40 bytes packet
 1 10.1.1.1 120 ms  50 ms  60 ms
 2 192.168.1.2 100 ms  60 ms  60 ms
 3 20.1.1.100 130 ms  90 ms  90 ms
<HostC> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100) 30 hops max,40 bytes packet
 1 10.1.1.2 30 ms  60 ms  40 ms
 2 192.168.2.2 90 ms  60 ms  60 ms
 3 20.1.1.100 70 ms  60 ms  90 ms
```

在 SwitchA 上执行 **display vrrp** 命令，可以看到 SwitchA 分别作为备份组 1 的 Master 和备份组 2 的 Backup。

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
Vlanif100 | Virtual Router 2
    state : Backup
    Virtual IP : 10.1.1.112
    Master IP : 10.1.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 2 virtual-ip 10.1.1.112
#
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 400
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 2 virtual-ip 10.1.1.112
 vrrp vrid 2 priority 120
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif300
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif400
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
```


版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```

配置 VRRP 快速切换功能示例

组网需求

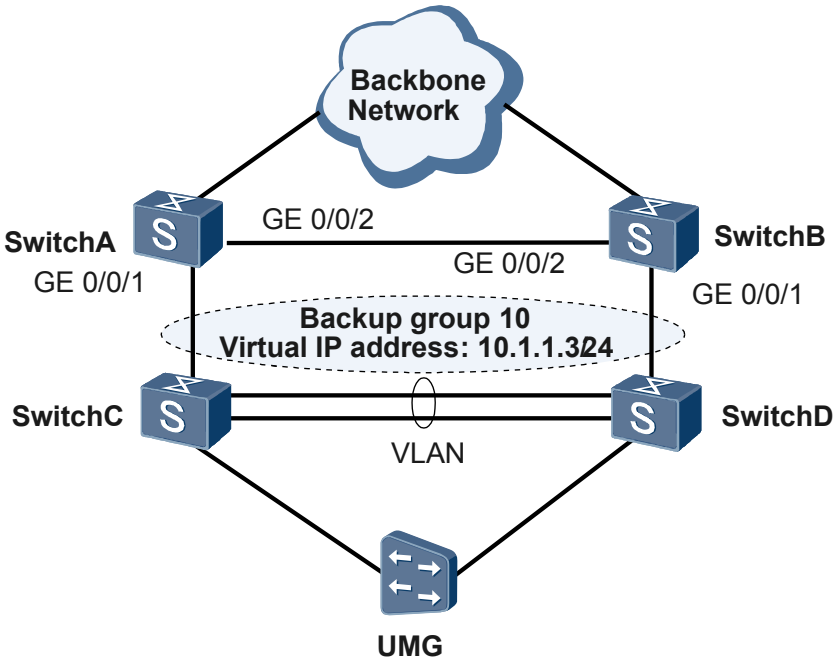
如图 9-54 所示，SwitchA、SwitchB、SwitchC、SwitchD 和通用媒体网关 UMG 设备组成一个简单的 NGN 承载网。

其中：

- UMG 通过交换机 SwitchC 和 SwitchD 双归属到 SwitchA 和 SwitchB。
- SwitchA 和 SwitchB 之间运行 VRRP，SwitchA 作为 Master，SwitchB 作为 Backup。

要求当 SwitchA 发生故障、或 SwitchA 与 SwitchB 之间的链路故障时，VRRP 主备切换的时间不超过 1 秒，以实现承载网的快速收敛。

图 9-54 配置 VRRP 快速切换功能组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE0/0/1	VLANIF100	10.1.1.1/24
	GE0/0/2	VLANIF200	192.168.0.1/24
SwitchB	GE0/0/1	VLANIF100	10.1.1.2/24
	GE0/0/2	VLANIF200	192.168.0.2/24

华为专有和保密信息
版权所有 © 华为技术有限公司

配置思路

采用如下思路实现 VRRP 快速切换：

1. 配置设备之间的网络互连。
2. 在 SwitchA 和 SwitchB 之间配置 BFD Session，同时实现对 SwitchA 和下行链路 SwitchA—SwitchC—SwitchD—SwitchB 的监测。
3. 在作为 Backup 的 SwitchB 上配置 VRRP 监视 BFD Session，一旦 BFD Session 的状态变为 Down，SwitchB 的优先级增加 40，进行主备切换。

说明

本示例只介绍 SwitchA 和 SwitchB 上的配置。

数据准备

为完成此配置例，需准备如下的数据：

- 本地和对端的 BFD 会话标识符
- VRRP 备份组 ID、虚拟 IP 地址
- Switch 在备份组中的优先级

操作步骤

步骤 1 配置设备之间的网络互连

配置各接口 IP 地址。配置 SwitchA、SwitchB、SwitchC 之间运行 OSPF。

详细配置过程请参考“图 9-54”。

步骤 2 配置 BFD 基本功能

在 SwitchA 上配置 BFD Session。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atob bind peer-ip 10.1.1.2 interface vlanif 200
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

在 SwitchB 上配置 BFD Session。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd btoa bind peer-ip 10.1.1.1 interface vlanif 200
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

配置完成后，在 SwitchA 或 SwitchB 上执行 **display bfd session** 命令，可以看到 BFD Session 会话的状态为 Up。以 SwitchA 的显示为例。

```
[SwitchA] display bfd session all
--------------------------------------------------------------------------------
Local Remote PeerIpAddr      State     Type        InterfaceName
```


版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------------------
1     2       10.1.1.2  4     Up         Static      Vlanif200
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

步骤 3 配置 VRRP 快速切换

创建备份组 10，配置 SwitchA 在备份组 10 中的优先级为 160，为 Master。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 10 virtual-ip 10.1.1.3
[SwitchA-Vlanif100] vrrp vrid 10 priority 160
[SwitchA-Vlanif100] quit
```

创建备份组 10，配置 SwitchB 在备份组 10 中的优先级为 140，为 Backup。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 10 virtual-ip 10.1.1.3
[SwitchB-Vlanif100] vrrp vrid 10 priority 140
```

在 Backup 侧配置监视 BFD Session 的状态，如果 BFD Session 状态变为 Down，SwitchB 的 VRRP 优先级增加 40。

```
[SwitchB-Vlanif100] vrrp vrid 10 track bfd-session 2 increased 40
[SwitchB-Vlanif100] quit
```

配置完成后，在 SwitchA 或 SwitchB 上执行 **display vrrp** 命令，可以看到 SwitchA 是 Master，SwitchB 是 Backup。在 SwitchB 上还能看到对 BFD Session 的监测设置以及 BFD Session 的当前状态。

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 10
    state : Master
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 160
    PriorityConfig : 160
    MasterPriority : 160
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 10
    state : Backup
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 140
    PriorityConfig : 140
    MasterPriority : 160
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Track BFD : 2  Priority increased : 40
    BFD-Session State : UP
    Config track link-bfd down-number : 0
```

步骤 4 验证配置结果

对 SwitchA 的接口 VLANIF200 执行 **shutdown** 操作，模拟链路故障。

版权所有 © 华为技术有限公司

```
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] shutdown
[SwitchA-Vlanif200] quit
```

在 SwitchB 上可以看到：VRRP 接收到 BFD 的故障报告后进行主备切换。

```
%May 10 15:48:30 2008 SwitchB BFD/5/BFD:Slot=1;IO(1) BFD Session(Discr:2) FSM Change To Down
(Detect)
%May 10 15:48:30 2008 SwitchB VRRP/5/BfdWarning:
 Virtual Router 10 | BFD-SESSION 2 : BFD_STATE_UP --> BFD_STATE_DOWN
%May 10 15:48:30 2008 SwitchB VRRP/5/StateWarning:
 Vlanif100 | Virtual Router 10 :  BACKUP --> MASTER
```

此时在 SwitchA 上执行 **display vrrp** 命令，可以看到 SwitchA 的状态变为 Initialize。

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 10
    state : Initialize
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 160
    PriorityConfig : 160
    MasterPriority : 0
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

在 SwitchB 上执行 **display vrrp** 命令，可以看到 SwitchB 的状态切换成 Master，BFD Session 的状态变为 Down。

```
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 10
    state : Master
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.2
    PriorityRun : 180
    PriorityConfig : 140
    MasterPriority : 180
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Track BFD : 2  Priority increased : 40
    BFD-Session State : DOWN
    Config track link-bfd down-number : 0
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
  vlan batch 100 200
#
 bfd
#
#
interface Vlanif100
```


版权所有 © 华为技术有限公司

```
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 160
#
interface Vlanif200
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
bfd atob bind peer-ip 10.1.1.2 interface Vlanif 200
 discriminator local 1
 discriminator remote 2
 commit
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
  vlan batch 100 200
#
 bfd
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 140
 vrrp vrid 10 track bfd-session 2 increased 40
#
interface Vlanif200
 ip address 192.168.0.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
bfd btoa bind peer-ip 10.1.1.1 interface Vlanif 200
 discriminator local 2
 discriminator remote 1
 commit
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

配置接口 VRRP6 示例

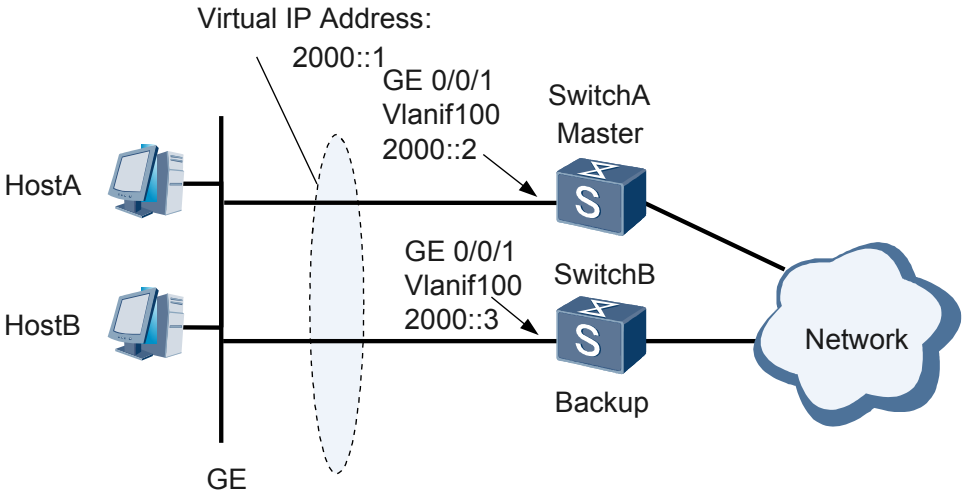
组网需求

SwitchA 和 SwitchB 根据配置的优先级来确定 VRRP6 备份组内的 Master。

一旦选定了备份组的 Master，就只有 Master 响应 IPv6 报文。无论因为任何原因，Master 的状态变为 Down，Backup 将替换 Master 使主机可以与外网通信。

配置的虚拟地址可以和 SwitchA 或者 SwitchB 接口的地址相同。

图 9-55 配置 VRRP6 组网图



配置思路

配置思路如下:

1. 在接口上配置 IPv6 地址。
2. 配置虚拟 IPv6 地址。

数据准备

为完成此配置例，需准备如下的数据:

- 备份组号
- 备份组优先级
- 需要在接口上配置的 IPv6 地址
- 需要在备份组的接口上配置的虚拟 IPv6 地址

操作步骤

步骤 1 使能 IPv6 转发

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
```


华为专有和保密信息
版权所有 © 华为技术有限公司

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
```

步骤 2 在接口上配置 IPv6 地址

配置 SwitchA。

```
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] interface gigabitethernet0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ipv6 enable
[SwitchA-Vlanif100] ipv6 address 2000::2 64
```

配置 SwitchB。

```
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ipv6 enable
[SwitchB-Vlanif100] ipv6 address 2000::3 64
```

步骤 3 在备份组的接口上配置虚拟 IPv6 地址

配置 SwitchA。

```
[SwitchA-Vlanif100] vrrp6 vrid 24 virtual-ip fe80::1 link-local
[SwitchA-Vlanif100] vrrp6 vrid 24 virtual-ip 2000::1
[SwitchA-Vlanif100] quit
```

配置 SwitchB。

```
[SwitchB-Vlanif100] vrrp6 vrid 24 virtual-ip fe80::1 link-local
[SwitchB-Vlanif100] vrrp6 vrid 24 virtual-ip 2000::1
```

步骤 4 配置 SwitchB 优先级低于 SwitchA

```
[SwitchB-Vlanif100] vrrp6 vrid 24 priority 25
[SwitchB-Vlanif100] quit
```

步骤 5 检查配置结果

可以看到 SwitchA 为 Master，SwitchB 为 backup。

```
[SwitchA] display vrrp6 interface vlanif 100
Vlanif100 | Virtual Router 24
    State : Master
    Virtual IP : FE80::1
                 2000::1
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 25
    PriorityConfig : 25
    MasterPriority : 25
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0218
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```


版权所有 © 华为技术有限公司

```
[SwitchB] display vrrp6 interface vlanif100
  Vlanif100 | Virtual Router 24
    State : Backup
    Virtual IP : FE80::1
                 2000::1
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 25
    PriorityConfig : 25
    MasterPriority : 25
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0218
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::2/64
 vrrp6 vrid 24 virtual-ip FE80::1 link-local
 vrrp6 vrid 24 virtual-ip 2000::1
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::3/64
 vrrp6 vrid 24 virtual-ip FE80::1 link-local
 vrrp6 vrid 24 virtual-ip 2000::1
 vrrp6 vrid 24 priority 25
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```


版权所有 © 华为技术有限公司

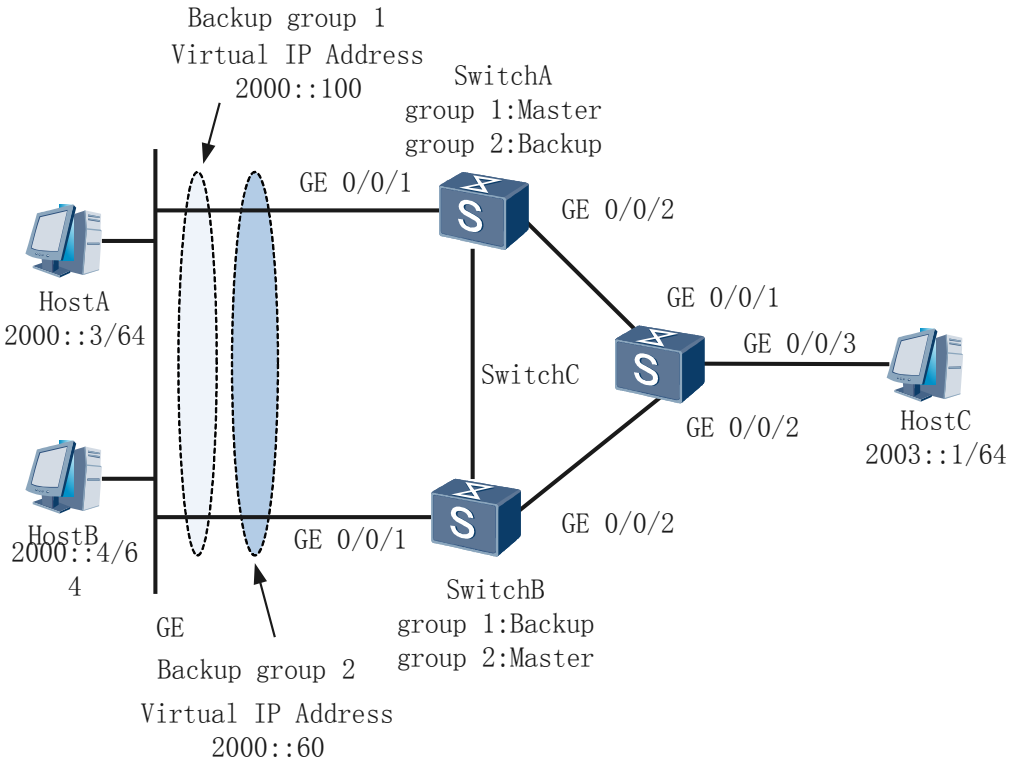
配置负载分担 VRRP6 示例

组网需求

如图 9-56 所示。

- SwitchA 作为备份 1 的 Master 设备，同时兼任备份组 2 的 Backup 设备。
- SwitchB 作为备份组 2 的 Master 设备，同时兼任备份组 1 的 Backup 设备。
- 局域网中的主机 HostA 使用备份组 1 的虚拟 IPv6 地址作为网关，HostB 使用备份组 2 的虚拟 Pv6 地址作为网关，达到分担数据流而又相互备份的目的。

图 9-56 配置负载分担 VRRP6 组网图



设备	接口	对应的 VLANIF	IP 地址
SwitchA	GE0/0/1	VLANIF100	2000::1/64
	GE0/0/2	VLANIF200	2002::1/64
SwitchB	GE0/0/1	VLANIF100	2000::2/64
	GE0/0/2	VLANIF400	2001::1/64
SwitchC	GE0/0/1	VLANIF200	2002::2/64
	GE0/0/2	VLANIF400	2001::2/64
	GE0/0/3	VLANIF300	2003::2/64

配置思路

采用如下思路配置负载分担 VRRP6 备份组：

版权所有 © 华为技术有限公司

1. 在 SwitchA 的接口 VLANIF100 下创建备份组 1 和备份组 2。其中，SwitchA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。
2. 在 SwitchB 的接口 VLANIF100 下创建备份组 1 和备份组 2。其中，SwitchB 在备份组 1 中作为 Backup 设备，在备份组 1 中作为 Master 设备。

数据准备

为完成此配置例，需准备如下的数据：

- 各个接口的 IPv6 地址
- 备份组的 ID 和虚拟 IPv6 地址
- 交换机在备份组中的优先级

操作步骤

步骤 1 配置各个接口的 IP 地址（略）

步骤 2 在 SwitchA、SwitchB 和 SwitchC 路由器之间采用 OSPFv3 协议进行互连（略）

步骤 3 配置主机

配置主机 HostA 的缺省网关为备份组 1 的虚拟 IPv6 地址 2000::100，主机 HostB 的缺省网关为备份组 2 的 IPv6 地址 2000::60，主机 HostC 的缺省网关为 2003::2。

步骤 4 配置 VRRP6 备份组

在 SwitchA 的 VLANIF100 接口上创建备份组 1 和备份组 2，并配置 SwitchA 在备份组 1 中的优先级为 120，确保 SwitchA 为 Master 设备；在备份组 2 中的优先级使用缺省值，确保 SwitchA 为 Backup 设备。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface vlanif100
[SwitchA-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[SwitchA-Vlanif100] vrrp6 vrid 1 virtual-ip 2000::100
[SwitchA-Vlanif100] vrrp6 vrid 1 priority 120
[SwitchA-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[SwitchA-Vlanif100] vrrp6 vrid 2 virtual-ip 2000::60
[SwitchA-Vlanif100] quit
```

在 SwitchB 的 VLANIF100 接口上创建备份组 1 和备份组 2，并配置 SwitchB 在备份组 1 中的优先级使用缺省值，确保 SwitchB 为 Backup 设备；在备份组 2 中的优先级为 120，确保 SwitchB 为 Master 设备。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[SwitchB-Vlanif100] vrrp6 vrid 1 virtual-ip 2000::100
[SwitchB-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[SwitchB-Vlanif100] vrrp6 vrid 2 virtual-ip 2000::60
[SwitchB-Vlanif100] vrrp6 vrid 2 priority 120
[SwitchB-Vlanif100] quit
```

步骤 5 检查配置结果

完成上述配置后，网络中的 HostA 和 HostB 分别能够 Ping 通 HostC。在 SwitchA 上使用 **display vrrp6** 命令，可以看到创建了两个备份组，备份组 1 和备份组 2。其中，SwitchA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。

```
[SwitchA] display vrrp6
Vlanif100 | Virtual Router 1
```


版权所有 © 华为技术有限公司

```
    State : Master
    Virtual IP : FE80::1
                 2000::100
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0201
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0

  Vlanif100 | Virtual Router 2
    State : Backup
    Virtual IP : FE80::2
                 2000::60
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0202
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

在 SwitchB 上使用 **display vrrp6** 命令，可以看考创建了两个备份组，备份组 1 和备份组 2。其中，SwitchA 在备份组 1 中作为 Backup 设备，SwitchB 在备份组 2 中作为 Master 设备。

```
[SwitchB] display vrrp6
Vlanif100 | Virtual Router 1
    State : Backup
    Virtual IP : FE80::1
                 2000::100
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0201
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0

  Vlanif100 | Virtual Router 2
    State : Master
    Virtual IP : FE80::2
                 2000::60
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0202
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

----结束

版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
 ipv6
#
ospfv3 1
 router-id 1.1.1.1
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::1/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtual-ip 2000::100
 vrrp6 vrid 1 priority 120
 vrrp6 vrid 2 virtual-ip FE80::2 link-local
 vrrp6 vrid 2 virtual-ip 2000::60
 ospfv3 1 area 0.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid pvid untagged 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid pvid untagged 200
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100 400
#
 ipv6
#
ospfv3 1
 router-id 2.2.2.2
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::2/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtual-ip 2000::100
 vrrp6 vrid 2 virtual-ip FE80::2 link-local
 vrrp6 vrid 2 virtual-ip 2000::60
 vrrp6 vrid 2 priority 120
 ospfv3 1 area 0.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid pvid untagged 100
#
interface GigabitEthernet0/0/2
```


版权所有 © 华为技术有限公司

```
 port hybrid pvid vlan 400
 port hybrid pvid untagged 400
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
ipv6
#
ospfv3 1
 router-id 3.3.3.3
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002::2
 ospfv3 1 area 0.0.0.0
#
interface Vlanif300
 ipv6 enable
 ipv6 address 2003::2/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif400
 ipv6 enable
 ipv6 address 2001::2/64
 ospfv3 1 area 0.0.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid pvid untagged 200
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid pvid untagged 300
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 300
 port hybrid pvid untagged 300
#
return
```

9.8 联动配置举例集

汇总提供以太网 OAM 与接口、以太网 OAM 与其他协议联动的配置举例，便于工程师能方便的找到需要的内容。

背景信息

AC6605 支持以太 CFM、EFM OAM、接口相互之间的故障传递。

本手册提供以下几种联动功能的配置举例：

- **配置 EFM OAM 与接口联动（触发与 EFM OAM 联动的接口物理状态变为 Down）示例**
- **配置以太网 CFM 与接口联动（触发与 CFM 联动的接口物理状态变为 Down）示例**
- **配置 EFM OAM 和以太网 CFM 联动示例**
- **配置以太网 CFM 与以太网 CFM 联动示例**

华为专有和保密信息
版权所有 © 华为技术有限公司

- 配置以太网 CFM 与 RRPP 联动示例

9.9 MAC SWAP 环回测试配置

介绍 MAC SWAP 环回测试的原理和配置。

9.9.1 MAC SWAP 环回测试概述

MAC SWAP 环回测试是指在收到以太帧的同时，修改以太帧头，交换帧头中的源 MAC 和目的 MAC，该帧最终被转发回发送端。该功能主要用于检测以太网连通性和网络质量。

MAC SWAP 环回测试是一种网络性能检测技术，和网络性能测试仪配合，可以对以太网进行连通性检测、吞吐量测试、QoS 验证。

MAC SWAP 环回测试只支持净荷为 IP 报文的以太帧。

9.9.2 AC6605 支持的 MAC SWAP 环回测试特性

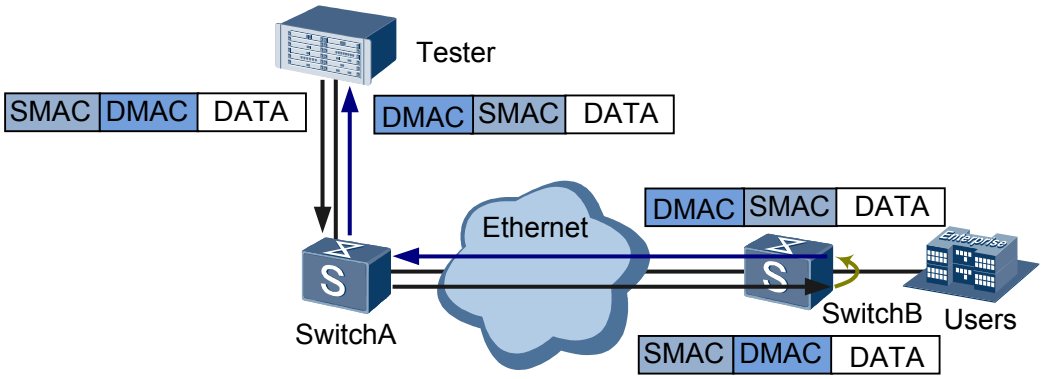
AC6605 支持本端 MAC SWAP 环回测试和远端 MAC SWAP 环回测试。本章介绍本端 MAC SWAP 环回测试和远端 MAC SWAP 环回测试的功能和原理。

本端 MAC SWAP 环回测试

本端 MAC SWAP 环回测试是针对从测试仪到被测交换机之间的网络的连通性和网络质量，包括被测试交换机本身。如图 9-57 所示，从测试仪发出测试以太帧，穿越以太网到达被测交换机，被测交换机在收到测试以太帧后，将测试以太帧被发送到配置本端 MAC SWAP 环回测试的端口出方向，所有符合条件的以太帧会被交换源 MAC 和目的 MAC，并通过指定接口返回到测试仪，测试仪根据返回的以太帧对网络性能进行分析。

本端 MAC SWAP 环回测试是一种业务中断型的性能检测技术，被测端口的所有业务会因为被环回而中断，但不影响其他端口。需要注意的是，当测试流量过大，会挤占返回测试以太帧接口中其他业务的带宽。

图 9-57 本端 MAC SWAP 环回测试示意图



远端 MAC SWAP 环回测试

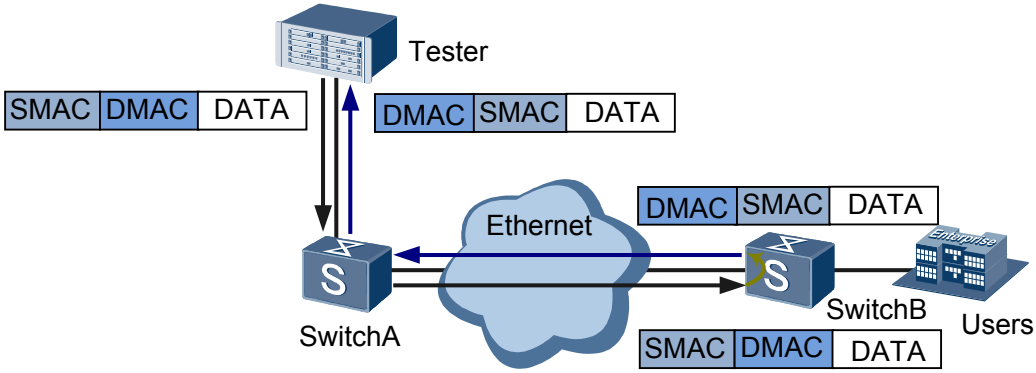
远端 MAC SWAP 环回测试是针对从测试仪到被测交换机之间的网络的连通性和网络质量，不包括被测试交换机本身。如图 9-58 所示，从测试仪发出测试以太帧，穿越以太

版权所有 © 华为技术有限公司

网到达被测交换机，被测交换机的上行接口在收到测试以太帧后，对符合条件的以太帧交换源 MAC 和目的 MAC，并从本接口返回到测试仪，测试仪根据返回的以太帧对网络性能进行分析。

远端 MAC SWAP 环回测试是一种非业务中断型的性能检测技术，只对匹配配置参数的以太帧做环回处理，其他以太帧正常转发。但是需要注意的是，当测试流量过大，会挤占被测接口的其他业务的带宽。

图 9-58 远端 MAC SWAP 环回测试示意图



9.9.3 本端 MAC SWAP 环回测试配置

通过配置本端 MAC SWAP 环回测试，完成对以太网（包括被测交换机）的连通性和性能测试。

建立配置任务

在配置本端 MAC SWAP 环回测试功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 正式为用户提供服务前，为了保证业务能够正常运行，可以在 AC6605 上配置 MAC SWAP 本地环回测试功能，测试远端设备到 AC6605 下行接口之间网络的连通性和 QoS CAR；还可以测试下行接口上配置的 VLAN mapping 和 VLAN Stacking 功能配置是否成功。

本端 MAC SWAP 环回测试是针对从测试仪到被测交换机之间的网络，包括被测试交换机本身。

前置任务

在配置本端 MAC SWAP 环回测试功能之前，需完成以下任务：

- 创建 VLAN，并且接口已经加入 VLAN。
- 如果验证 QoS CAR，需要首先完成 QoS CAR 配置，具体配置过程请参见《AC6605 无线接入控制器 配置指南-QoS》。

数据准备

配置本端 MAC SWAP 环回测试功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	配置本端 MAC SWAP 环回测试功能的接口类型和编号
2	返回测试报文的接口类型和编号。
3	接口所属 VLAN
4	（可选）内层 VLAN ID
5	环回超时时间

配置本端 MAC SWAP 环回测试

通过在接口上配置本端 MAC SWAP 环回测试，可以测试从测试仪到被测交换机之间的网络的连通性和网络质量，包括被测试交换机本身。

背景信息

在进行本端 MAC SWAP 环回测试之前，需要在 AC6605 上配置测试报文的源 MAC、目的 MAC 和 VLAN，只有源 MAC、目的 MAC 和 VLAN 能够匹配的报文才能被环回。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback local swap-mac source-mac** *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] **interface** *interface-type interface-number* [**timeout** { *time-value* | **none** }]，配置 MAC SWAP 本端环回测试功能。

注意

本端 MAC SWAP 环回测试是一种业务中断型的性能检测技术，被测端口的所有业务会因为被环回而中断，但不影响其他端口。需要注意的是，当测试流量过大，会挤占返回测试以太帧接口中其他业务的带宽。

如果设备上配置的是单层 VLAN，则发送的测试报文不能为双层 VLAN 报文。

----结束

打开 MAC SWAP 环回测试功能

介绍如何打开环 MAC SWAP 回测试功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

背景信息

环回测试会影响到网络的正常运行，而且当测试流量过大，会挤占接口其他业务的带宽。为了使 MAC SWAP 环回测试不影响网络质量，可以在进行测试时打开 MAC SWAP 环回测试功能，测试完成后迅速关闭 MAC SWAP 环回测试功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback swap-mac start**，打开 MAC SWAP 本地环回测试功能。

该命令为单次行为，不会保存到配置文件。

建议在测试完成后，请使用 **loopback swap-mac stop** 命令及时关闭环回测试功能，否则会影响接口业务的正常运行。

----结束

关闭 MAC SWAP 环回测试功能

介绍如何关闭 MAC SWAP 环回测试功能。

背景信息

环回测试会影响到网络的正常运行，而且当测试流量过大，会挤占接口的其他业务的带宽，所以测试完成后需要关闭 MAC SWAP 环回测试功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback swap-mac stop**，关闭 MAC SWAP 本地环回测试功能。

该命令为单次行为，不会保存到配置文件。

手动停止或者测试时间超时，环回测试功能均会停止，如果希望进行下一次测试，需要重新通过 **loopback swap-mac start** 命令打开 MAC SWAP 环回测试功能。

----结束

检查配置结果

通过查看本端 MAC SWAP 环回测试配置信息，来检查配置是否成功。

前提条件

已经完成本端 MAC SWAP 环回测试功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display loopback swap-mac information** 命令查看 MAC SWAP 环回测试的配置信息。

----结束

任务示例

执行 **display loopback swap-mac information** 命令查看配置本端 MAC SWAP 环回测试配置是否正确。发送测试报文后，可以查看了收到多少测试报文，丢弃了多少不符合要求的报文。

```
<Quidway> display loopback swap-mac information
  Loopback type             : local
  Loopback state            : running
  Loopback test time(s)     : 60
  Loopback interface        : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/2
  Loopback source MAC       : 0001-0001-0001
  Loopback destination MAC  : 0002-0002-0002
  Loopback vlan             : 10
  Loopback inner vlan       : 0
  Loopback packets          : 0
  Drop packets              : 3
```

9.9.4 远端 MAC SWAP 环回测试配置

通过配置远端 MAC SWAP 环回测试，完成对以太网（不包括被测交换机）的连通性和性能测试。

建立配置任务

在配置远端 MAC SWAP 环回测试功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AC6605 正式为用户提供服务前，为了保证上行链路的连通性，可以在 AC6605 上配置 MAC SWAP 远端环回测试功能，从远端设备测试到 AC6605 上行接口之间网络的连通性和网络质量。通过远端环回测试功能，还可以测试上行接口配置的 VLAN mapping 和 VLAN Stacking 功能配置是否成功。

远端 MAC SWAP 环回测试是针对从测试仪到被测交换机之间的网络，不包括被测试交换机本身。

前置任务

在配置远端 MAC SWAP 环回测试功能之前，需完成以下任务：

- 创建 VLAN，并且接口已经加入 VLAN。
- 如果测试 VLAN Mapping 或 VLAN Stacking 功能，需要首先完成 VLAN Mapping 或 VLAN Stacking 配置。

数据准备

配置远端 MAC SWAP 环回测试功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	配置远端 MAC SWAP 环回测试功能的接口类型和编号
2	接口所属 VLAN
3	（可选）内层 VLAN ID
4	环回测试超时时间

配置远端 MAC SWAP 环回测试

通过在接口上配置远端 MAC SWAP 环回测试，可以测试从测试仪到被测交换机之间的网络的连通性和网络质量，不包括被测试交换机本身。

背景信息

在进行远端 MAC SWAP 环回测试之前，需要在 AC6605 上配置测试报文的源 MAC、目的 MAC 和 VLAN，只有源 MAC、目的 MAC 和 VLAN 能够匹配的报文才能被环回。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback remote swap-mac source-mac** *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] [**timeout** { *time-value* | **none** }]，配置 MAC SWAP 远端环回测试功能。

注意

远端 MAC SWAP 环回测试是一种非业务中断型的性能检测技术，只对匹配配置参数的以太帧做环回处理，其他以太帧正常转发。但是需要注意的是，当测试流量过大，会挤占被测接口的其他业务的带宽。

如果设备上配置的是单层 VLAN，则发送的测试报文不能为双层 VLAN 报文。

----结束

打开 MAC SWAP 环回测试功能

介绍如何打开环 MAC SWAP 回测试功能。

背景信息

环回测试会影响到网络的正常运行，而且当测试流量过大，会挤占接口其他业务的带宽。为了使 MAC SWAP 环回测试不影响网络质量，可以在进行测试时打开 MAC SWAP 环回测试功能，测试完成后迅速关闭 MAC SWAP 环回测试功能。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback swap-mac start**，打开 MAC SWAP 本地环回测试功能。

该命令为单次行为，不会保存到配置文件。

建议在测试完成后，请使用 **loopback swap-mac stop** 命令及时关闭环回测试功能，否则会影响接口业务的正常运行。

----结束

打开 MAC SWAP 环回测试功能

介绍如何关闭 MAC SWAP 环回测试功能。

背景信息

环回测试会影响到网络的正常运行，而且当测试流量过大，会挤占接口的其他业务的带宽，所以测试完成后需要关闭 MAC SWAP 环回测试功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

Eth-Trunk 接口及其成员端口不支持 MAC SWAP 环回测试功能。

步骤 3 执行命令 **loopback swap-mac stop**，关闭 MAC SWAP 本地环回测试功能。

该命令为单次行为，不会保存到配置文件。

手动停止或者测试时间超时，环回测试功能均会停止，如果希望进行下一次测试，需要重新通过 **loopback swap-mac start** 命令打开 MAC SWAP 环回测试功能。

----结束

检查配置结果

通过查看远端 MAC SWAP 环回测试配置信息，来检查配置是否成功。

前提条件

已经完成远端 MAC SWAP 环回测试功能的所有配置。

操作步骤

- 使用 **display loopback swap-mac information** 命令查看远端 MAC SWAP 环回测试的配置信息。

----结束

版权所有 © 华为技术有限公司

任务示例

执行 **display loopback swap-mac information** 命令查看配置 MAC SWAP 环回测试配置是否正确，并可以查看接收了多少环回报文。

```
<Quidway> display loopback swap-mac information
  Loopback type             : remote
  Loopback state            : running
  Loopback test time(s)     : 60
  Loopback interface        : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/1
  Loopback source MAC       : 0001-0001-0001
  Loopback destination MAC  : 0002-0002-0002
  Loopback vlan             : 10
  Loopback inner vlan       : 0
  Loopback packets          : 0
```

9.9.5 配置举例

介绍 MAC SWAP 环回测试配置举例。

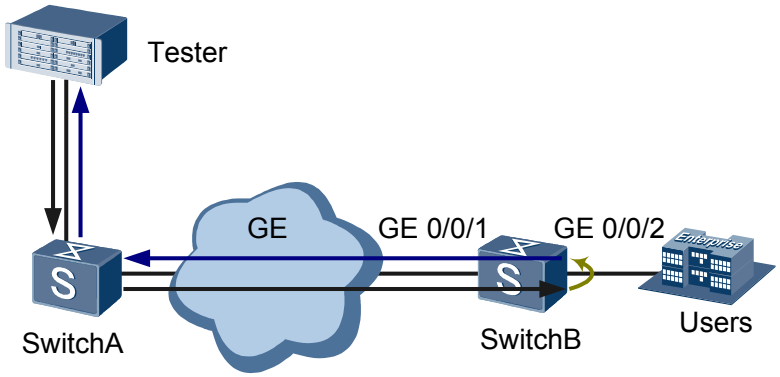
配置本端 MAC SWAP 环回测试示例

组网需求

如图 9-59 所示，SwitchB 是 AC6605，通过 GE0/0/1 接口连接到以太网，GE0/0/2 接口下连接用户。

在 SwitchB 的 GE0/0/2 接口上配置本端 MAC SWAP 环回测试功能。测试仪器发送测试以太帧到 SwitchB，GE0/0/2 接口对以太帧源 MAC 和目的 MAC 进行交换后，通过 GE0/0/1 接口发回到测试仪。测试仪通过对收到的以太帧进行分析，测试以太网的连通性和网络性能，测试范围包括 SwitchB。

图 9-59 配置本端 MAC SWAP 环回测试组网图



配置思路

采用如下思路配置本端 MAC SWAP 环回测试功能：

1. 创建 VLAN，GE0/0/1 接口以 Trunk 方式加入 VLAN，GE0/0/2 以 hybrid 方式加入 VLAN。

版权所有 © 华为技术有限公司

2. 在 SwitchB 上配置本端 MAC SWAP 环回测试功能。
3. 在 SwitchB 上打开环回测试功能。

数据准备

为完成此配置例，需准备如下的数据：

- 接口所属 VLAN ID 为 100。
- 环回测试以太帧的源 MAC 为 0018-2000-0085，目的 MAC 为 0018-2000-0070。
- 环回测试超时时间为 80 秒。

操作步骤

步骤 1 在 SwitchB 上创建 VLAN 100，GE0/0/1 接口以 Trunk 方式加入 VLAN 100，GE0/0/2 以 hybrid 方式加入 VLAN 100。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet0/0/2
[SwitchB-GigabitEthernet0/0/2] port hybrid pvid vlan 100
[SwitchB-GigabitEthernet0/0/2] port hybrid untagged vlan 100
```

步骤 2 在 SwitchB 的 GE0/0/2 接口上配置本端 MAC SWAP 环回测试功能，通过 GE0/0/1 接口把交换 MAC 后以太帧返回到测试仪器，然后打开环回测试功能。

```
[SwitchB-GigabitEthernet0/0/2] loopback local swap-mac source-mac 0018-2000-0085 dest-mac
018-2000-0070 vlan 100 interface gigabitethernet 0/0/1 timeout 80
[SwitchB-GigabitEthernet0/0/2] loopback swap-mac start
[SwitchB-GigabitEthernet0/0/2] quit
```

步骤 3 检验配置结果

完成以上配置后，可以使用 **display loopback swap-mac information** 命令检查配置是否正确，如果检查配置没问题，可以用测试仪发送以太帧，并对网络性能进行分析。

```
[SwitchB] display loopback swap-mac information
  Loopback type             : local
  Loopback state            : running
  Loopback test time(s)     : 80
  Loopback interface        : GigabitEthernet0/0/2
  Loopback output interface : GigabitEthernet0/0/1
  Loopback source MAC       : 0018-2000-0085
  Loopback destination MAC  : 0018-2000-0070
  Loopback vlan             : 100
  Loopback inner vlan       : 0
  Loopback packets          : 0
  Drop packets              : 3
```

----结束

配置文件

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 loopback local swap-mac source-mac 0018-2000-0085 dest-mac 0018-2000-0070 vlan
100 interface GigabitEthernet0/0/1 timeout 80
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

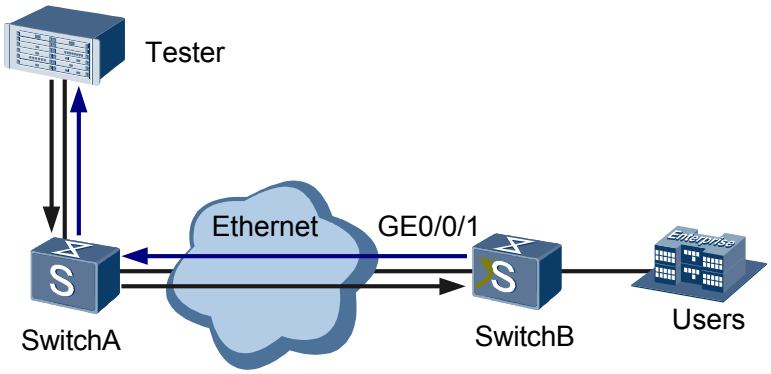
配置远端 MAC SWAP 环回测试示例

组网需求

如图 9-60 所示，SwitchB 是 AC6605，通过 GE0/0/1 接口连接到以太网。

在 SwitchB 的 GE0/0/1 接口上配置远端 MAC SWAP 环回测试功能。当测试仪发送测试以太帧到 SwitchB，GE0/0/1 接口对测试帧的源 MAC 和目的 MAC 进行互换，并发回到测试仪。测试仪通过对收到的以太帧进行分析，测试 SwitchB 上行网络的连通性和网络性能，测试范围不包括 SwitchB。

图 9-60 配置远端 MAC SWAP 环回测试组网图



配置思路

采用如下思路配置远端 MAC SWAP 环回测试功能：

1. 创建 VLAN，GE0/0/1 接口以 Trunk 方式加入 VLAN。
2. 在 SwitchB 上配置远端 MAC SWAP 环回测试功能。
3. 在 SwitchB 上打开环回测试功能。

数据准备

为完成此配置例，需准备如下的数据：

- 接口所属 VLAN ID 为 100。
- 环回测试以太帧的源 MAC 为 0018-2000-0085，目的 MAC 为 0018-2000-0070。
- 环回测试超时时间为 80 秒。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 SwitchB 上创建 VLAN 100，GE0/0/1 接口以 Trunk 方式加入 VLAN 100。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 2 在 SwitchB 的 GE0/0/1 接口上配置远端 MAC SWAP 环回测试功能，然后打开环回测试功能。

```
[SwitchB-GigabitEthernet0/0/1] loopback remote swap-mac source-mac 0018-2000-0085 dest-mac
018-2000-0070 vlan 100 timeout 80
[SwitchB-GigabitEthernet0/0/1] loopback swap-mac start
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 3 检验配置结果

完成以上配置后，可以使用 **display loopback swap-mac information** 命令检查配置是否正确，如果检查配置没问题，可以用测试仪发送以太帧，并对网络性能进行分析。

```
[SwitchB] display loopback swap-mac information
  Loopback type             : remote
  Loopback state            : running
  Loopback test time(s)     : 80
  Loopback interface        : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/1
  Loopback source MAC       : 0018-2000-0085
  Loopback destination MAC  : 0018-2000-0070
  Loopback vlan             : 100
  Loopback inner vlan       : 0
  Loopback packets          : 0
```

----结束

配置文件

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 loopback remote swap-mac source-mac 0018-2000-0085 dest-mac 0018-2000-0070 vlan
 100 timeout 80
#
return
```


版权所有 © 华为技术有限公司

10 网络管理配置

关于本章

本文档从配置过程和配置举例等方面对 AC6605 的网络管理特性 SNMP、RMON、NTP、LLDP、NQA 及 Ping&Tracert 进行了介绍。阅读本文档能指导用户了解和掌握 AC6605 网络管理的配置方法。

10.1 SNMP 配置
简单网络管理协议 SNMP（Simple Network Management Protocol）是广泛用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站 NMS）来管理网元的方法。共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3，用户可以根据情况选择同时配置一个或多个版本。

10.2 LLDP 配置
介绍 LLDP 的应用场景、配置步骤以及配置举例。

10.3 HGMP 配置
通过配置 HGMP 协议，利用一台命令交换机建立集群，对加入集群的大量以太网交换机进行集中管理和配置，可以减轻工程和维护的工作量。

10.4 NTP 配置
通过配置 NTP，可以保持网络中各设备的时钟运行一致。

10.5 Ping 和 Tracert 配置
介绍 Ping 和 Tracert 命令的基本概念和使用。

10.6 NQA 配置
通过配置 NQA，可以有效的检测网络运行的状态，使用户能够实时采集到各种网络运行指标。

10.7 RMON 配置
通过 RMON(Remote Network Monitoring)可以实现对以太接口的监控。

版权所有 © 华为技术有限公司

10.1 SNMP 配置

简单网络管理协议 SNMP（Simple Network Management Protocol）是广泛用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站 NMS）来管理网元的方法。共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3，用户可以根据情况选择同时配置一个或多个版本。

10.1.1 SNMP 简介

SNMP 为网管和设备间的通信提供一套标准协议，保证网管能够正常的管理设备和接收设备的告警。

SNMP 概述

网管通过在被管理设备中运行的 Agent 客户端上执行 GET-SET 操作来管理设备上的节点，设备上的节点由 MIB（Management Information Base）来唯一标识。

随着网络业务的日益发展，现有的网络中，设备数量日益庞大，且这些设备与网络管理员所在的中心机房距离较远。当这些设备发生故障时，由于设备无法主动上报故障，导致网络管理员无法及时感知、及时定位和排除故障，从而导致网络的维护效率降低，维护工作量大大增加。

为了解决这个问题，设备制造商已经在一些设备中提供了网络管理的功能，这样网管就可以远程询问设备的状态，同样设备能够在特定类型的事件发生时向网络管理工作站发出警告。

SNMP 就是规定网管站和设备之间如何传递管理信息的应用层协议。SNMP 定义了网管管理设备的几种操作，以及设备故障时能向网管主动发送告警。

网管使用 SNMP 协议管理设备时，存在网管站、Agent 和被管理设备三个角色。网管通过管理信息库 MIB 来唯一标识和管理设备上的节点。网管管理设备的操作包括：GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest、以及设备主动发送告警。关于角色、MIB 和操作的定义和作用请参考下面的具体内容。

SNMP 定义的三类角色

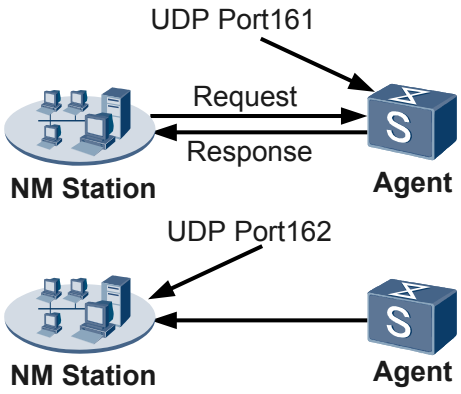
在网管通过 SNMP 协议管理设备过程中，定义了三类角色：

- 网管站：向被管理设备发送各种查询报文，以及接收被管理设备发送的告警。
- Agent：驻留在被管理设备上的一个进程。Agent 的作用如下：
  - 接收、解析来自网管站的查询报文。
  - 根据报文类型对管理变量进行 Read 或 Write 操作，并生成响应报文，返回给网管站。
  - 根据各协议模块对告警触发条件的定义，在达到触发条件后，如进入、退出系统视图或设备重新启动等，相应的模块通过 Agent 主动向网管站发送告警，报告所发生的事件。
- 被管理设备：接受网管的管理，产生和主动上报告警。

网管站与 Agent 的关系如图 10-1 所示。

版权所有 © 华为技术有限公司

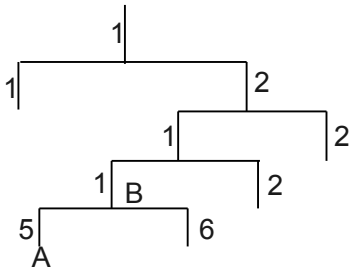
图 10-1 SNMP 结构示意图



MIB

为了在 SNMP 报文中唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象，整个层次结构就象一棵树，树的节点表示管理对象，如图 10-2 所示，它可以用从根开始的一条路径进行识别。

图 10-2 MIB 树结构



在图 10-2 中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的客体标识符（Object Identifier）。而 MIB 的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。

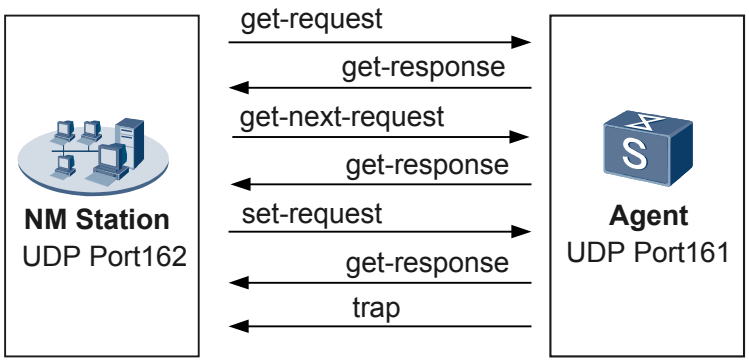
用户可以采用管理信息库标准 MIB，也可以按标准方式定义自己的 MIB。使用标准 MIB 能够降低部署代理部件的成本，从而降低整个网管系统的成本。

SNMP 操作

SNMP 以 GET-SET 操作方式替代复杂的命令集，利用如图 10-3 的操作实现全部功能。

版权所有 © 华为技术有限公司

图 10-3 SNMP 操作示意图



SNMP 的操作如表 10-1 所示。

表 10-1 SNMP 的操作

操作	功能
GetRequest	从某变量中取值，获取设备某功能节点状态，是网管向设备发出的请求。
GetNextRequest	在 MIB 表项中取下一项值，获取设备某功能的另一节点状态，是网管向设备发出的请求。
GetResponse	对 GetRequest、GetNextRequest、SetRequest 的响应，设备向网管的回应。
GetBulk	该操作相当于连续执行多次 GetNext 操作，是网管向设备发出的请求。
SetRequest	设置具体变量的值，对设备功能节点状态进行调整，是网管向设备发出的指令。
Trap	报告事件信息，是设备主动向网管报告事件。

AC6605 支持的 SNMP 特性

通过对 SNMP 协议各个版本特性支持情况的对比，以及各个版本适用的应用场景介绍，为用户进行网络部署时选取 SNMP 协议的版本提供参考依据。

AC6605 系统中支持 SNMPv1、SNMPv2c 和 SNMPv3 三个协议版本。各特性的功能如表 10-2 所示，各版本支持的特性列表如表 10-3 所示。SNMP 各版本的应用场景如表 10-4 所示，用户可以根据现网的运营情况，选择需要的版本使网管和被管理设备之间进行通信。

说明

在网络中存在多个网管管理同一设备的情况，各网管站可能选用不同的 SNMP 协议版本与设备进行通信。为了满足这些网管和设备的正常通信，可以在设备上同时部署 SNMPv1、v2c、v3。

版权所有 © 华为技术有限公司

表 10-2 SNMP 支持的特性功能介绍

特性	功能描述
访问控制	访问控制主要用来限制管理设备的用户的权限。通过该功能可以限制指定的用户管理设备上的指定节点，从而提升精细化管理。
认证加密	认证加密主要是通过对网管和被管理设备传送的报文进行认证和加密，避免数据报文被窃取或篡改，从而提升数据传输的安全性。
错误码	错误码用来标识特定的故障现象，有助于管理员快速定位和解决故障，因此错误码越丰富越有利于管理员对设备进行管理。
Trap 告警	Trap 告警是被管理设备主动向网管发送告警。以便管理员能够及时发现设备的异常。 被管理设备发送 Trap 告警后，不需要网管进行接收确认。
Inform 告警	Inform 告警也是被管理设备向网管主动发送告警。 被管理设备发送 Inform 告警后，需要网管进行接收确认，被管理设备没有收到确认信息时会重复发送该告警，并且生成相应的告警日志，方便网管重启后，能够同步重启时间内发送的告警。 系统没有收到 inform 告警的确认信息时，将告警暂时保存在内存中，因此使用 Inform 告警可能会占用较多的系统资源。
GetBulk	Get-Bulk 主要方便管理员进行批量的 Get-next 操作。网络规模较大时，以节省管理员的工作量，提升管理效率。

表 10-3 SNMP 各版本支持的特性概况

特性列表	SNMPv1	SNMPv2c	SNMPv3
访问控制	基于团体名进行访问控制	基于团体名进行访问控制	基于用户和用户组进行访问控制

版权所有 © 华为技术有限公司

特性列表	SNMPv1	SNMPv2c	SNMPv3
认证加密	不支持	不支持	支持认证和加密，认证和加密的方式如下： 认证： ● MD5 ● SHA 加密：DES56
错误码	支持 6 个错误码	支持 16 个错误码	支持 16 个错误码
Trap 告警	支持	支持	支持
Inform 告警	不支持	支持	不支持
GetBulk	不支持	支持	支持

表 10-4 SNMP 各版本的应用场景

版本	应用场景
SNMPv1	适用于小型网络，组网简单，对网络安全性要求不高或者网络环境本身比较安全，且比较稳定的网络，比如校园网，小型企业网。
SNMPv2c	适用于大中型网络，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞的网络。 通过配置 Infrom 告警可以确保被管理设备发送的告警能够被网管收到。
SNMPv3	适用于各种规模的网络，尤其是对网络的安全性要求较高，确保合法的管理员才能对网络设备进行管理的网络。比如网管和被管理设备间的通信数据需要在公网上进行传输。

如果用户是统一规划建设新网络，建议根据上面的应用场景选择 SNMP 协议的版本。如果用户是网络扩建或升级，建议用户根据网管使用的版本选择在设备上配置对应的 SNMP 协议版本，保证设备和网管的通信。

10.1.2 配置设备使用 SNMPv1 与网管通信

配置 SNMPv1 功能后，网管和设备之间将使用 SNMPv1 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

版权所有 © 华为技术有限公司

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

建立配置任务

在配置网管使用 SNMPv1 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较小，网络设备较少，且网络设备环境本身比较安全时（比如校园网、小型企业网），可以选择使用 SNMPv1 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv1 管理设备功能之前，需完成以下任务：

- 配置路由协议，使交换机和网管站之间可达

数据准备

在配置网管使用 SNMPv1 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方法和位置、SNMP 报文的尺寸
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间
4	（可选）固定索引的接口数目

配置 SNMPv1 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 **3**、**4**、**5** 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 **snmp-agent sys-info version v1**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。

使能 SNMPv1 后，被管理设备将同时支持 SNMPv1 和 SNMPv3，能同时满足使用 SNMPv1 和 SNMPv3 的网管对设备进行监控和管理。

步骤 4 执行命令 **snmp-agent community** { **read** | **write** } *community-name*，配置设备的读写团体名。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

步骤 5 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

- 如果是 IPv4 网络，请执行命令 **snmp-agent target-host trap address udp-domain** *ip-address* [**udp-port** *port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1**] [**private-netmanager**] [**ext-vb**]，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。
- 命令关键字 **ext-vb** 用于设置设备对目的主机发送的告警携带扩展绑定变量。缺省情况下，设备对目的主机发送的告警不携带扩展绑定变量。

步骤 6 （可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

版权所有 © 华为技术有限公司

如果需要同时配置网络管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

步骤 7 （可选）执行命令 **snmp-agent packet max-size** *byte-count*，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该团体名的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择**配置接口索引固定特性**，保证设备重启、接口重启等不会变更接口索引。

（可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 **5** 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，步骤 **2**、**3**、**4** 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree*，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 Viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community** { **read** | **write** } { *community-name* | **cipher** *community-name* } [**mib-view** *view-name* | **acl** *acl-number*]*，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 为了加强安全性，用户可以选择配置 **cipher** 参数，使团体名以密文形式显示。该形式下，需要管理员妥善保管团体名称，否则忘记团体名时将无法通过设备查看获得。
- 如果需要使用该团体名的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **mib-view** *view-name* 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

（可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

（可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 4 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

交换机端配置的 Trap 报文的源接口和网管站配置的交换机发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 5 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在交换机发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 6 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在交换机发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

版权所有 © 华为技术有限公司

（可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

步骤 3 执行命令 **set constant-ifindex max-number** *number*，设置索引固定的接口最大数量。

随着系统的运行，频繁增删接口，保存在存储设备中的接口索引文件可能会变得很大，占用过多的系统资源。为了保证接口索引文件不超过预期的大小，可以设置索引固定的接口最大数量。

限定固定索引的接口数量后，系统根据特定的方式将配置数量范围内的接口索引固定。如果配置的接口最大值小于现有的固定索引接口数量，根据启动的时间选取配置数量范围内的接口固定索引，多余的接口不再固定索引。

缺省情况下，最多可以固定 131070 个接口的索引值。配置固定索引接口数量为 0 时，不固定任何接口的索引。

步骤 4 执行命令 **set constant-ifindex subinterface** { **dense-mode** | **sparse-mode** }，设置子接口索引的内存分配模式。

当新建子接口时，系统会在内存中按照特定的方式生成子接口的索引映像文件。用户在指定子接口编号时可能会采用不同的方式，比如连续分配或者不连续分配。为了适应不同的情况，可以设置子接口索引的内存分配模式。使用情况如下：

- 松散模式：当子接口编号不连续，分布比较松散时选用。
- 紧凑模式：子接口编号连续时选用。

----结束

检查配置结果

配置 SNMPv1 成功后，用户可以查看到 SNMPv1 的配置情况。

前提条件

已经完成 SNMPv1 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** 命令查看当前配置的团体名。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。

版权所有 © 华为技术有限公司

- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。
- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

10.1.3 配置设备使用 SNMPv2c 与网管通信

配置 SNMPv2c 功能后，网管和设备之间将使用 SNMPv2c 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

建立配置任务

在配置网管使用 SNMPv2c 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较大，网络设备较多，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞时，可以选择使用 SNMPv2c 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv2c 管理设备功能之前，需完成以下任务：

- 配置路由协议，使交换机和网管站之间可达

数据准备

在配置网管使用 SNMPv2c 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方法和位置、SNMP 报文的尺寸

版权所有 © 华为技术有限公司

序号	数据
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间、Inform 告警的超时时间、重复发送次数、待确认的最大条数、告警日志的老化时间、日志缓冲区中最多能保存的告警日志条数
4	（可选）固定索引的接口数目

配置 SNMPv2c 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 3、4、5 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 **snmp-agent sys-info version v2c**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。

使能 SNMPv2c 后，被管理设备将同时支持 SNMPv2c 和 SNMPv3，能同时满足使用 SNMPv2c 和 SNMPv3 的网管对设备进行监控和管理。

步骤 4 执行命令 **snmp-agent community** { **read** | **write** } *community-name*，配置设备的读写团体名。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

步骤 5 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

- 如果是 IPv4 网络，请根据需要选择配置 Trap 方式告警或 Inform 方式告警：

版权所有 © 华为技术有限公司

说明

Trap 方式告警和 Inform 方式告警的区别如下:

- 被管理设备发送 Trap 方式告警时，不需要告警主机回应确认信息。
- 被管理设备发送 Inform 方式告警时，需要告警主机回应确认消息，在超时时间范围内没有收到告警主机的回应消息时，被管理设备将重新发送该告警，直至发送的告警个数达到配置的重复发送最大次数。

  被管理设备发送 Inform 告警时，同时记录告警日志，方便告警主机故障或链路故障恢复后，告警主机能够同步故障时间内产生的告警。

因此，Inform 告警相比 Trap 方式告警更加可靠，但由于重传机制的存在，可能导致设备需要缓存大量的告警信息，占用设备较多内存资源。

建议用户在网络比较稳定时选择 Trap 方式告警；在设备资源充足且网络不太稳定的环境下，选择配置 Inform 方式告警。

- Trap 告警：执行命令 **snmp-agent target-host trap address udp-domain** *ip-address* [**udp-port** *port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v2c**] [**private-netmanager**] [**ext-vb**]，配置设备发送 Trap 告警和错误码的目的主机。
- Inform 告警：执行命令 **snmp-agent target-host inform address udp-domain** *ip-address* [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v2c** [**ext-vb**]，配置设备发送 Inform 告警和错误码的目标主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。
- 命令关键字 **ext-vb** 用于设置设备对目的主机发送的告警携带扩展绑定变量。缺省情况下，设备对目的主机发送的告警不携带扩展绑定变量。

步骤 6 （可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置网络管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

步骤 7 （可选）执行命令 **snmp-agent packet max-size** *byte-count*，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

版权所有 © 华为技术有限公司

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该团体名的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择**配置接口索引固定特性**，保证设备重启、接口重启等不会变更接口索引。

（可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 **5** 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，步骤 **2**、**3**、**4** 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

版权所有 © 华为技术有限公司

步骤 5 执行命令 **snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree*，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 Viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community** { **read** | **write** } { *community-name* | **cipher** *community-name* } [**mib-view** *view-name* | **acl** *acl-number*]*，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 为了加强安全性，用户可以选择配置 **cipher** 参数，使团体名以密文形式显示。该形式下，需要管理员妥善保管团体名称，否则忘记团体名时将无法通过设备查看获得。
- 如果需要使用该团体名的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **mib-view** *view-name* 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

（可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

（可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name* 命令一次关闭一个告警开关。

步骤 4 根据配置 SNMPv2c 的基本功能中选择的告警方式，配置对应的告警参数：

Trap 告警参数请参考 **Trap 告警参数配置**，Inform 告警参数配置请参考 **Inform 告警参数配置**

Trap 告警参数配置：

1. 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

   指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

   交换机端配置的 Trap 报文的源接口和网管站配置的交换机发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

2. 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

   为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在交换机发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

3. 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

   为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在交换机发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

Inform 告警参数配置：

1. 执行命令 **snmp-agent inform** { **timeout** *seconds* | **resend-times** *times* | **pending** *number* } *，配置确认告警的超时时间、重复发送告警的次数和待确认告警的最大条数。

   如果当前网络不稳定，那么增加告警确认的超时时间的同时，需要增加告警重复发送的次数和待确认告警的最大条数，缺省情况下，告警确认的超时时间为 15 秒，告警重复发送的次数为 3 次，待确认告警的最大条数为 39 条。

华为专有和保密信息
版权所有 © 华为技术有限公司

Inform 方式告警重复发送次数建议配置为小于等于 10 次，否则将影响设备性能。

2. 执行命令 **snmp-agent inform** { **timeout** *seconds* | **resend-times** *times* } * **address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string*，配置指定目标主机的告警确认超时时间和告警重复发送的次数。

   如果当前网络不稳定，那么增加告警确认的超时时间的同时，需要增加告警重复发送的次数和待确认告警的最大条数，缺省情况下，告警确认的超时时间为 15 秒，告警重复发送的次数为 3 次。

   Inform 方式告警重复发送次数建议配置为小于等于 10 次，否则将影响设备性能。

3. 执行命令 **snmp-agent notification-log enable**，使能告警日志功能。

   如果交换机与目标主机之间的链路发生故障，导致路由不可达。交换机不再发送 Inform 告警，但是继续记录告警日志。当链路恢复正常，路由变为可达后，目标主机将同步交换机在链路故障期间记录的告警日志。

   使能告警日志功能后，系统只记录 Inform 方式的告警，不记录 Trap 方式的告警。

   缺省情况下，告警日志功能关闭。

4. 执行命令 **snmp-agent notification-log** { **global-ageout** *ageout* | **global-limit** *limit* } *，配置告警日志的老化时间和日志缓冲区中最多能保存的告警日志条数。

   缺省情况下，告警日志的老化时间为 24 小时。超过 24 小时，告警日志被自动删除。

   缺省情况下，日志缓冲区中最多能保存的告警日志为 500 条。超出这个限制，将从最早的一条告警日志开始删除。

----结束

（可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

步骤 3 执行命令 **set constant-ifindex max-number** *number*，设置索引固定的接口最大数量。

随着系统的运行，频繁增删接口，保存在存储设备中的接口索引文件可能会变得很大，占用过多的系统资源。为了保证接口索引文件不超过预期的大小，可以设置索引固定的接口最大数量。

限定固定索引的接口数量后，系统根据特定的方式将配置数量范围内的接口索引固定。如果配置的接口最大值小于现有的固定索引接口数量，根据启动的时间选取配置数量范围内的接口固定索引，多余的接口不再固定索引。

版权所有 © 华为技术有限公司

缺省情况下，最多可以固定 131070 个接口的索引值。配置固定索引接口数量为 0 时，不固定任何接口的索引。

步骤 4 执行命令 **set constant-ifindex subinterface** { **dense-mode** | **sparse-mode** }，设置子接口索引的内存分配模式。

当新建子接口时，系统会在内存中按照特定的方式生成子接口的索引映像文件。用户在指定子接口编号时可能会采用不同的方式，比如连续分配或者不连续分配。为了适应不同的情况，可以设置子接口索引的内存分配模式。使用情况如下：

- 松散模式：当子接口编号不连续，分布比较松散时选用。
- 紧凑模式：子接口编号连续时选用。

----结束

检查配置结果

配置 SNMPv2c 成功后，用户可以查看到 SNMPv2c 的配置情况。

前提条件

已经完成 SNMPv2c 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** 命令查看当前配置的团体名。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display snmp-agent target-host** 命令查看目标主机的信息。
- 执行 **display snmp-agent inform** [**address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string*]命令查看全局或指定目标主机的 Inform 参数、主机统计信息。
- 执行 **display snmp-agent notification-log info** 命令查看告警日志缓冲区中的告警日志信息。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。
- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

10.1.4 配置设备使用 SNMPv3 与网管通信

配置 SNMPv3 功能后，网管和设备之间将使用 SNMPv3 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

版权所有 © 华为技术有限公司

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

建立配置任务

在配置网管使用 SNMPv3 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络对安全性要求较高，只有合法的管理员才能对网络设备进行管理，并且传输的网络数据需要保证其安全性和准确性时，比如网管和被管理设备间的通信数据需要在公网上进行传输，可以部署 SNMPv3，通过 SNMPv3 的认证和加密功能确保数据传输的安全性，保证网管和被管理设备之间的正常通信。

前置任务

在完成配置网管使用 SNMPv3 管理设备功能之前，需完成以下任务：

- 配置路由协议，使交换机和网管站之间可达

数据准备

在配置网管使用 SNMPv3 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、用户和用户组的名称、告警目的主机地址、管理员的联系方法和位置、SNMP 报文的尺寸
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间
4	（可选）固定索引的接口数目

配置 SNMPv3 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

版权所有 © 华为技术有限公司

背景信息

配置 SNMP 的基本功能中，步骤 4、5、6 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 （可选）执行命令 **snmp-agent sys-info version v3**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。故该步骤可选。

步骤 4 执行命令 **snmp-agent group v3** *group-name* [**authentication** | **privacy**]，配置 SNMP 用户组。

当网管和设备处在不安全的网络环境中时，比如容易遭受攻击等，建议用户配置参数 **authentication** 或 **privacy**，使能数据的认证和加密功能。

用户可以选择的认证加密模式如下：

- 不配置 **authentication** 和 **privacy** 参数：不认证不加密。适用于网络环境安全，且管理员比较固定的情况下。
- 配置 **authentication** 参数：只认证不加密。适用于网络环境安全，但管理员比较多，管理员对设备交叉操作比较频繁的情况下。通过认证可以限制拥有权限的管理员才可以访问该设备。
- 配置 **privacy** 参数：既认证又加密。适用于网络环境不太安全，管理员交叉操作多的情况下。通过认证和加密既可以限制特定的管理员访问设备，并且使网络数据以加密形式发送，避免网络数据被窃取，造成关键数据泄露。

步骤 5 执行命令 **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *password* [**privacy-mode des56** *password*]]，配置 SNMPv3 用户信息。

用户组和用户配置完成后，使用该用户名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

用户组使能认证和加密功能后，用户可以选择认证和加密的方式，对网络传输的数据进行认证和加密。

- 认证方式
  - MD5（Message Digest 5）：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
  - SHA-1（Secure Hash Algorithm）：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

  MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。
- 加密方式

  DES 使用 56bit 的密钥对一个 64bit 的明文块进行加密。

步骤 6 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

版权所有 © 华为技术有限公司

- 如果是 IPv4 网络，请执行命令 **snmp-agent target-host trap address udp-domain** *ip-address* [**udp-port** *port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v3** [**authentication** | **privacy**]] [**private-netmanager**] [**ext-vb**]，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。
- 命令关键字 **ext-vb** 用于设置设备对目的主机发送的告警携带扩展绑定变量。缺省情况下，设备对目的主机发送的告警不携带扩展绑定变量。

步骤 7 （可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置网络管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

步骤 8 （可选）执行命令 **snmp-agent packet max-size** *byte-count*，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该用户组的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该用户组中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。

版权所有 © 华为技术有限公司

- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择**配置接口索引固定特性**，保证设备重启、接口重启等不会变更接口索引。

（可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强使用 SNMPv3 进行通信的网管和被管理设备的安全性。

背景信息

当有多个网管使用同一个用户组名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用用户组名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 **5** 可以省略。
- 如果需要使用用户组名的所有网管管理设备上的指定节点，步骤 **2**、**3**、**4** 可以省略。
- 如果需要使用用户组名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree*，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* [**acl** *acl-number*]，配置用户组的读写权限。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read-view** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write-view** 参数。
- 用户希望筛选部分重要告警，过滤掉无关告警时，选择配置 **notify-view** *notify-view* 参数，限制被管理设备向网管发送告警的 MIB 节点。配置该参数后，设备产生的告警中匹配 **notify-view** 指定的 MIB 节点的告警才能发送到该用户的网管。
- 为了加强安全性，用户可以选择配置 **authentication** 或 **privacy** 参数，**authentication** 对用户只认证不加密，**privacy** 对用户既认证又加密，具体请参考认证和加密选取原则。
- 如果需要使用该用户组的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]可以省略。
- 如果需要使用该用户组的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该用户组的某些网管管理设备上的某些节点，ACL 和 MIB 视图都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

（可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

（可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

版权所有 © 华为技术有限公司

说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 4 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

交换机端配置的 Trap 报文的源接口和网管站配置的交换机发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 5 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在交换机发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 6 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在交换机发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

（可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

步骤 3 执行命令 **set constant-ifindex max-number** *number*，设置索引固定的接口最大数量。

版权所有 © 华为技术有限公司

随着系统的运行，频繁增删接口，保存在存储设备中的接口索引文件可能会变得很大，占用过多的系统资源。为了保证接口索引文件不超过预期的大小，可以设置索引固定的接口最大数量。

限定固定索引的接口数量后，系统根据特定的方式将配置数量范围内的接口索引固定。如果配置的接口最大值小于现有的固定索引接口数量，根据启动的时间选取配置数量范围内的接口固定索引，多余的接口不再固定索引。

缺省情况下，最多可以固定 131070 个接口的索引值。配置固定索引接口数量为 0 时，不固定任何接口的索引。

步骤 4 执行命令 **set constant-ifindex subinterface** { **dense-mode** | **sparse-mode** }，设置子接口索引的内存分配模式。

当新建子接口时，系统会在内存中按照特定的方式生成子接口的索引映像文件。用户在指定子接口编号时可能会采用不同的方式，比如连续分配或者不连续分配。为了适应不同的情况，可以设置子接口索引的内存分配模式。使用情况如下：

- 松散模式：当子接口编号不连续，分布比较松散时选用。
- 紧凑模式：子接口编号连续时选用。

----结束

检查配置结果

配置 SNMPv3 成功后，用户可以查看到 SNMPv3 的配置情况。

前提条件

已经完成 SNMPv3 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent usm-user** [**engineid** *engineid* | **group** *group-name* | **username** *user-name*]*命令查看用户信息。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。
- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

10.1.5 SNMP 配置举例

介绍 SNMP 的配置。请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

版权所有 © 华为技术有限公司

配置设备使用 SNMPv1 与网管通信示例

网管在管理设备时使用 SNMPv1 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

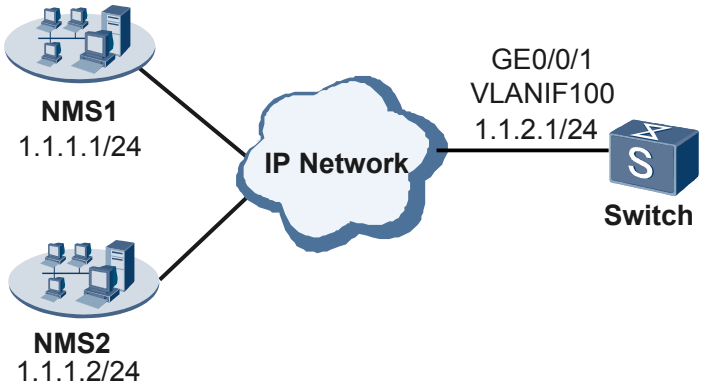
组网需求

如图 10-4 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理该设备上除 HGMP 之外的所有 ISO 节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上该设备管理员，以便对故障进行快速定位和排除，故要求在设备上配置设备管理员的联系方法。

图 10-4 配置使用 SNMPv1 与网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv1。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称

华为专有和保密信息
版权所有 © 华为技术有限公司

- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置交换机和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<Quidway> system-view
[Quidway] snmp-agent
```

步骤 3 配置 SNMP 的版本为 v1

```
[Quidway] snmp-agent sys-info version v1
```

查看配置的 SNMP 的版本信息。

```
[Quidway] display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv1 SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

配置 MIB 视图，限制 NMS2 可以管理设备上除 HGMP 之外的节点。

```
[Quidway] snmp-agent mib-view included allexthgmp iso
[Quidway] snmp-agent mib-view excluded allexthgmp 1.3.6.1.4.1.2011.6.7
```

配置团体名引用 ACL 和 MIB 视图。

```
[Quidway] snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
```

步骤 5 配置告警功能

```
[Quidway] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname 1.1.3.1
[Quidway] snmp-agent trap source Loopback0
[Quidway] snmp-agent trap queue-size 200
[Quidway] snmp-agent trap life 60
```

步骤 6 配置管理员联系方法

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<Quidway> display snmp-agent community
  Community name:adminnms2
      Group name:adminnms2
      Acl:2001
      Storage-type: nonVolatile
```


版权所有 © 华为技术有限公司

查看 ACL 配置。

```
<Quidway> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Quidway> display snmp-agent mib-view viewname allexthgmp
View name:allexthgmp
       MIB Subtree:hwCluster
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
```

查看告警的目标主机。

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : 1.1.3.1
  Port             : 162
  Type             : trap
  Version          : v1
  Level            : No authentication and privacy
  NMS type         : NMS
------------------------------------------------------------
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

交换机的配置文件

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
```


版权所有 © 华为技术有限公司

```
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface LoopBack0
 ip address 1.1.3.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
  network 1.1.3.1 0.0.0.0
 #
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v1  v3
 snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname 1.1.3.1

 snmp-agent mib-view included allexthgmp iso
 snmp-agent mib-view excluded allexthgmp hwCluster
 snmp-agent trap source LoopBack0
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
#
return
```

配置设备使用 SNMPv2c 与网管通信示例

网管在管理设备时使用 SNMPv2c 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

组网需求

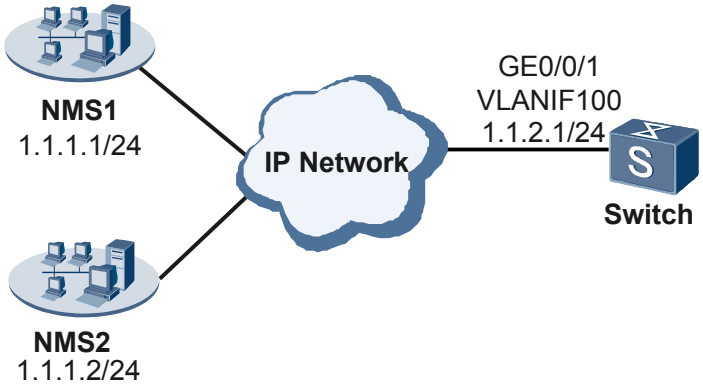
如图 10-5 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备上除 HGMP 之外的所有 ISO 节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。由于设备发送的告警需要经过公网才能被网管接收，为了保证告警接收的可靠性，采用 Inform 方式告警。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方法。

版权所有 © 华为技术有限公司

图 10-5 配置使用 SNMPv2c 管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv2c。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点。
4. 配置设备的 Inform 告警功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称
- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置交换机和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<Quidway> system-view
[Quidway] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v2c

```
[Quidway] snmp-agent sys-info version v2c
```

查看配置的 SNMP 的版本信息。

```
[Quidway] display snmp-agent sys-info version
SNMP version running in the system:
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
                SNMPv2c SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

配置 MIB 视图。

```
[Quidway] snmp-agent mib-view included allexthgmp iso
[Quidway] snmp-agent mib-view excluded allexthgmp 1.3.6.1.4.1.2011.6.7
```

配置团体名引用 ACL 和 MIB 视图。

```
[Quidway] snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
```

步骤 5 配置告警功能

```
[Quidway] snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname 1.1.2.1 v2c
[Quidway] snmp-agent inform timeout 15 resend-times 3 pending 39
[Quidway] snmp-agent notification-log enable
[Quidway] snmp-agent notification-log global-ageout 12
```

步骤 6 配置管理员联系方法

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<Quidway> display snmp-agent community
   Community name:adminnms2
       Group name:adminnms2
       Acl:2001
       Storage-type: nonVolatile
```

查看 ACL。

```
<Quidway> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Quidway> display snmp-agent mib-view viewname allexthgmp
View name:allexthgmp
       MIB Subtree:hwCluster
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
```

查看告警的目标主机。

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
-------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : 1.1.2.1
  Port             : 162
  Type             : inform
  Version          : v2c
  Level            : No authentication and privacy
  NMS type         : NMS
--------------------------------------------------------------
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

交换机的配置文件

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
#
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v2c v3
 snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname 1.1.2.1 v2c
 snmp-agent mib-view included allexthgmp iso
 snmp-agent mib-view excluded allexthgmp hwCluster
 snmp-agent inform timeout 15 resend-times 3 pending 39
 snmp-agent notification-log enable
 snmp-agent notification-log global-ageout 12
#
return
```


版权所有 © 华为技术有限公司

配置设备使用 SNMPv3 与网管通信示例

网管在管理设备时使用 SNMPv3 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

组网需求

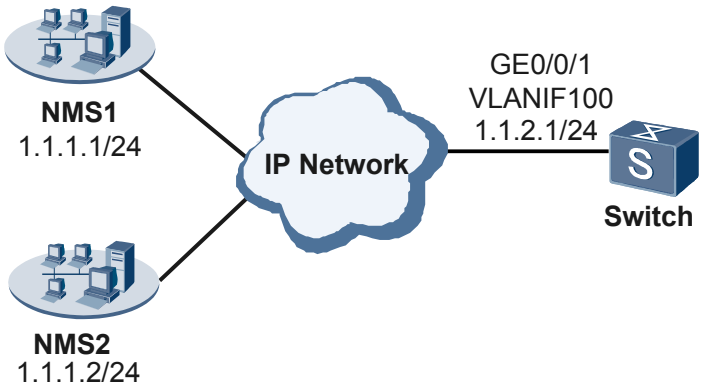
如图 10-6 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备上除 HGMP 之外的所有节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于 NMS2 和设备间的数据需要穿越公网，对用户的数据进行认证和加密。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方法。

图 10-6 配置使用 SNMPv3 网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv3。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点，并对用户进行数据加密。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

版权所有 © 华为技术有限公司

- SNMP 版本
- 用户组名称
- 用户名和密码
- 认证和加密算法
- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置交换机和网管站之间路由可达（略）

步骤 2 配置 SNMP Agent

```
<Quidway> system-view
[Quidway] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v3

```
[Quidway] snmp-agent sys-info version v3
```

查看配置的 SNMP 的版本信息。

```
[Quidway] display snmp-agent sys-info version
SNMP version running in the system:
          SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

配置 MIB 视图。

```
[Quidway] snmp-agent mib-view included testview iso
[Quidway] snmp-agent mib-view excluded testview 1.3.6.1.4.1.2011.6.7
```

配置用户组和用户，对用户的数据进行认证和加密。

```
[Quidway] snmp-agent usm-user v3 testuser testgroup authentication-mode md5 87654321 privacy-mode
des56 87654321
[Quidway] snmp-agent group v3 testgroup privacy write-view testview notify-view testview acl 2001
```

步骤 5 配置告警功能

```
[Quidway] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname testuser
[Quidway] snmp-agent trap source loopback0
[Quidway] snmp-agent trap queue-size 200
[Quidway] snmp-agent trap life 60
```

步骤 6 配置管理员联系方法

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置 NMS

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

版权所有 © 华为技术有限公司

查看用户组。

```
<Quidway> display snmp-agent group testgroup
   Group name: testgroup
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: testview
       Notifyview :testview
       Storage-type: nonVolatile
       Acl:2001
```

查看用用户。

```
<Quidway> display snmp-agent usm-user

       User name: testuser
       Engine ID: 000007DB7F00000100004C3F active
       Group name:testgroup
```

查看 ACL。

```
<Quidway> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Quidway> display snmp-agent mib-view viewname testview
       View name:testview
       MIB Subtree:iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active
```

查看告警的目标主机。

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : testuser
  Port             : 162
  Type             : trap
  Version          : v1
  Level            : No authentication and privacy
  NMS type         : NMS
------------------------------------------------------------
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```


版权所有 © 华为技术有限公司

查看管理员的联系方法。

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

交换机的配置文件

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface LoopBack0
 ip address 1.1.3.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
  network 1.1.3.1 0.0.0.0
#
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF000004A7
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v3
 snmp-agent group v3 testgroup privacy  write-view testview notify-view testview acl 2001
 snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname testuser
 snmp-agent mib-view included testview iso
 snmp-agent mib-view excluded testview hwCluster
 snmp-agent usm-user v3 testuser testgroup authentication-mode md5 N'!2Z[^HZOT&P'@XIM=F#Q!! privacy-
mode des56 N'!2Z[^HZOT&P'@XIM=F#Q!!
 snmp-agent trap source LoopBack0
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
#
return
```

10.2 LLDP 配置

介绍 LLDP 的应用场景、配置步骤以及配置举例。

10.2.1 LLDP 概述

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。

版权所有 © 华为技术有限公司

背景

目前以太网技术在网络中有着非常广泛的应用。随着大规模组网的需求越来越多，对网络管理（以下简写为网管）能力的要求也越来越高，例如获取相连设备的拓扑状态、设备间的配置冲突等。

而现阶段许多网管都使用“自动发现（Automated Discovery）”功能来跟踪拓扑的变化。但是绝大多数网管最多只能分析到第三层网络拓扑结构，将设备分组到各个 IP 子网。这些数据只是一些有关设备增加和移除的基本事件，无法确定设备通过哪些接口跟另外一个设备相连，也无法确定设备间是否存在配置冲突。

第二层发现（Layer 2 Discovery）准确定位了诸如哪些设备附带有哪些接口，以及哪些设备与其他设备相互连接等二层信息，并显示出了客户端、交换机、路由器和应用服务器以及网络服务器之间的路径。这些详细的信息对快速获取相连设备的拓扑状态、设备间的配置冲突、查询网络失败的根源将很有帮助。

链路层发现协议 LLDP（Link Layer Discovery Protocol）就是 IEEE 802.1ab 中定义的第二层发现协议。

LLDP 基本原理

图 10-7 LLDP 结构框图

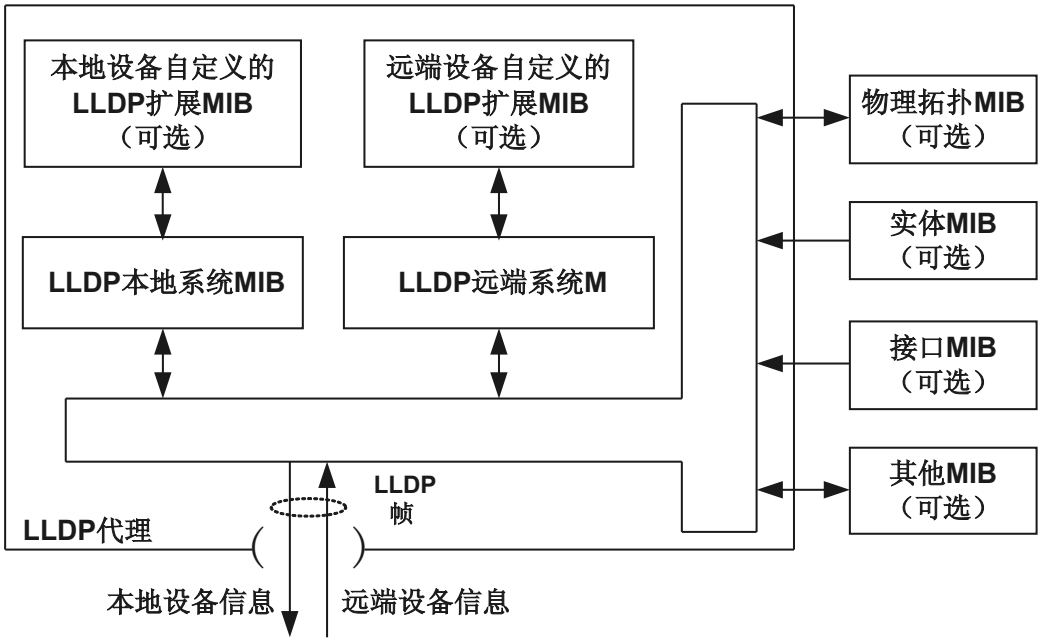


图 10-7 为 LLDP 结构框图。LLDP 与 MIB 密不可分，其基本实现原理为：

- LLDP 模块通过与设备上的 PTOPO MIB、Entity MIB、Interface MIB 以及 Other MIB 的交互，来更新自己的 LLDP local system MIB 库以及自己定义的 LLDP 扩展 MIB（图中的 Organizationally defined local device LLDP MIB extension）
- 然后通过 LLDP 帧，将自己的相关信息通过连接到远端设备的接口，发送给远端设备。
- 同时它接收远端设备发过来的 LLDP 帧，更新自己的 LLDP remote system MIB 即 LLDP 远端系统 MIB 库。

版权所有 © 华为技术有限公司

这样，通过 MIB 库，设备就很清楚的知道了自己相邻的设备的信息，包括连接的是远方设备的哪个接口，连接的远端设备的桥 MAC 地址等等。

MIB

MIB：管理信息数据库，MIB 分为 LLDP Local System MIB 和 LLDP Remote System MIB。

- LLDP Local System MIB：LLDP 本地系统管理信息数据库（以下简称 LLDP 本地 MIB），用来保存本端设备信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。
- LLDP Remote System MIB：LLDP 远端系统管理信息数据库（以下简称 LLDP 远端 MIB），用来保存相邻设备的信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。

LLDP Agent

LLDP Agent：LLDP 代理，用于管理接口的 LLDP 操作。

LLDP Agent 要完成下列任务：

- 维护 LLDP 本地 MIB 的信息。
- 在本端状态发生变化的情况下，提取 LLDP 本地 MIB 信息向邻居节点发送。在本端状态没有变化的情况下，按照一定的周期提取 LLDP 本地 MIB 信息向邻居节点发送。
- 识别并处理收到的 LLDP 报文。
- 维护 LLDP 远端 MIB 库。
- LLDP 本地 MIB 库或远端 MIB 库中的信息发生变化的情况下，向网管发送 LLDP 告警。

LLDP 管理地址

LLDP 管理地址（以下简称管理地址）是供网管系统标识 AC6605 并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，更有利于清晰地了解到当前的拓扑状态，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 字段中传送给邻居节点。

LLDP 告警

LLDP 告警是指 LLDP 本地 MIB 库或远端 MIB 库中的信息发生变化，设备向网管系统发送的更新拓扑的提示信息。触发告警的原因为：

- 全局 LLDP 使能的状态变化
- 本地管理地址改变
- 邻居信息发生变化（邻居管理地址变化，本地不会产生告警信息）

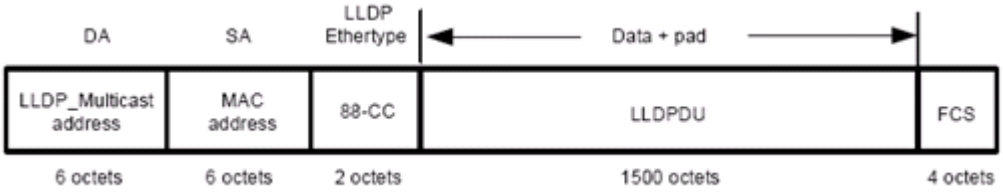
LLDP 告警功能对全局起作用，控制所有接口发送告警的能力。

LLDP 报文

LLDP 报文结构如图 10-8 所示。

版权所有 © 华为技术有限公司

图 10-8 LLDP 报文结构

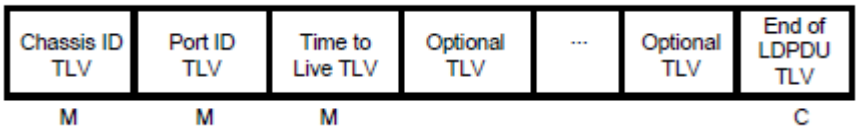


- DA：LLDP 帧的目的地址，它是一个组播地址其值为 01-80-C2-00-00-0E。
- SA：与设备相邻连接设备的桥 MAC。
- LLDP Ethertype：帧类型，设备通过此字节，就可以判断是一个 LLDP 帧，然后交给 LLDP 模块处理，它的值为 0x88CC。
- LLDPDU：LLDP Data Unit，LLDP 数据单元，它是 LLDP 信息交换的主体。
- FCS：帧校验位。

因为 LLDPDU 是 LLDP 信息交换的主体，它决定了通过 LLDP 协议可以发现设备的哪些二层信息，所以下面详细介绍一下该字段。

LLDPDU 结构如图 10-9 所示。

图 10-9 LLDPDU 结构



LLDPDU 中的基本信息单元是 TLV，其中：

- T 指的是信息的类型 TYPE
- L 是指的信息的长度 LENGTH
- V 是指的信息的值，也就是真正所要传输的内容 VALUE

在 LLDP 帧交互的过程中，LLDPDU 往往根据要求包含了很多种不同的 TLV，根据这些不同的 TLV 来传输或者接收自己和邻近设备的信息。

LLDPDU 固定以 Chassis ID TLV、Port ID TLV 和 Time to Live TLV 开始，以 End of LLDPDU TLV 为结束，这四个 TLV 为必选的 TLV。其他均为可选 TLV，可以由设备自行定义是否包含在 LLDPDU 中。

10.2.2 AC6605 支持的 LLDP 特性

介绍 LLDP 特性的应用场景及 AC6605 支持的 TLV 类型。

LLDP 应用场景

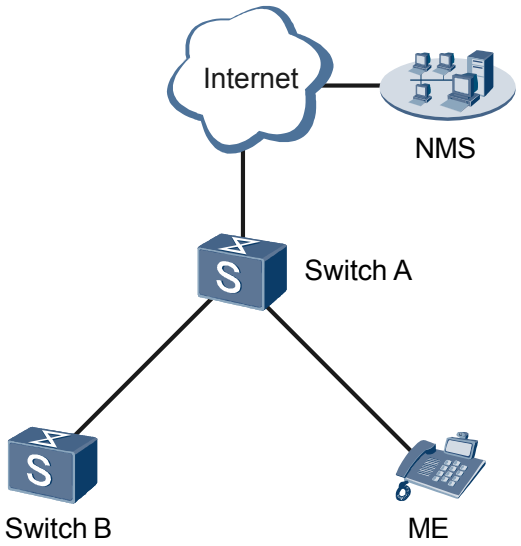
AC6605 支持在以下三种组网方式下应用 LLDP。

单邻居组网方式

版权所有 © 华为技术有限公司

单邻居组网是指交换机设备的端口之间或者交换机与媒体终端 ME（Media Endpoint）的端口之间是直接相连，中间没有跨任何的设备，而且端口只有一个远端邻居设备的情况。单邻居组网如图 10-10 所示，SwitchA 和 SwitchB 之间以及 SwitchA 和 ME 之间均是直接相连，SwitchA 和 SwitchB 的每一个端口都只有一个远端邻居。

图 10-10 单邻居组网方式

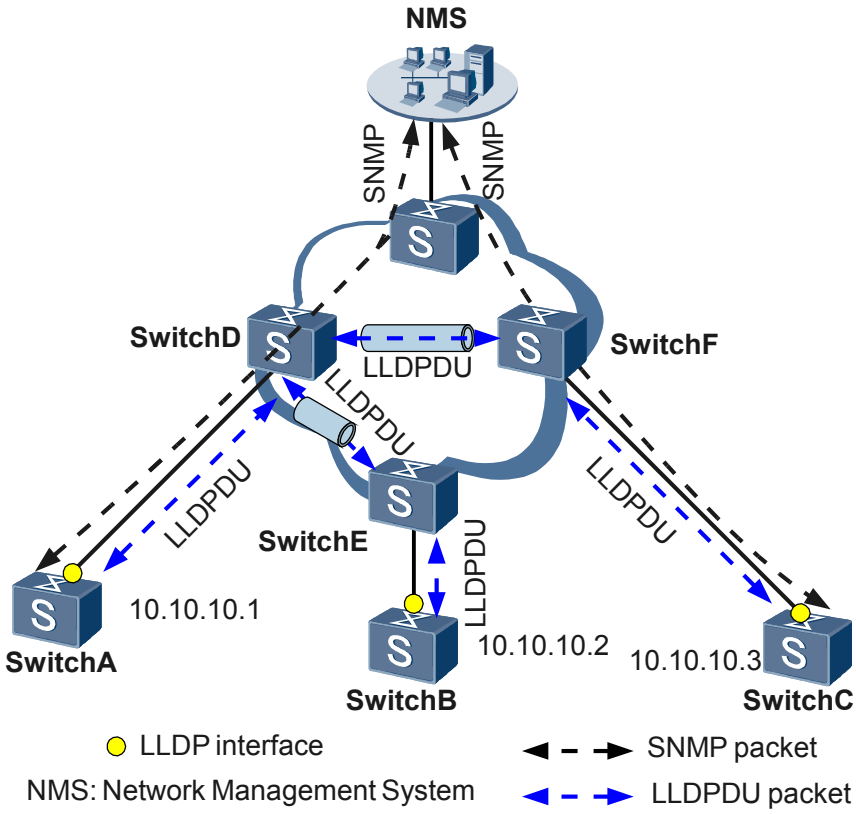


多邻居组网方式

多邻居组网方式是指交换机设备的端口之间不是直接相连，中间跨越了未知网络，这时每个端口的远端邻居不止一个。多邻居组网如图 10-11 所示，SwitchA、SwitchB 和 SwitchC 之间不是直接相连，中间跨越了未知网络，该网络中的设备未使能 LLDP 功能或者无需受 NMS 的管理，但该部分设备可以透传 LLDP 报文。这样 SwitchA、SwitchB 和 SwitchC 的端口都不止有一个远端邻居。

版权所有 © 华为技术有限公司

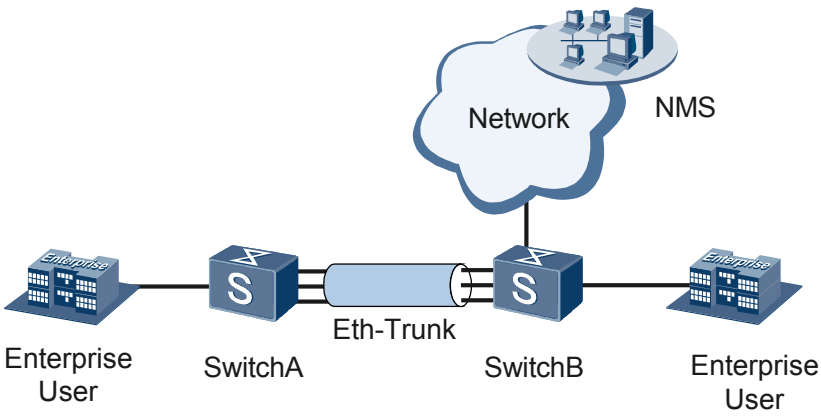
图 10-11 多邻居组网方式



存在链路聚合的组网方式

如图 10-12 所示交换机设备的端口之间存在链路聚合。该情况下，具体到链路聚合之间的每一个端口，都与单邻居组网模式的效果是一样的。

图 10-12 存在链路聚合的组网方式



版权所有 © 华为技术有限公司

AC6605 支持的可选 TLV 类型

除了必须支持的 Chassis ID TLV、Port ID TLV、Time to Live TLV 和 End of LDPDU 以外，AC6605 支持的可选 TLV 类型为：

- 基本 TLV

TLV 类型	说明
Management Address TLV	管理 IP 地址
Port Description TLV	端口描述
System Capabilities TLV	本端设备的支持能力： ● other：其它能力 ● repeater：中继器 ● bridge：桥设备 ● wlanAccessPoint：无线接入点 ● router：路由器 ● telephone：无线设备 ● docsisCableDevice：管理站 ● stationOnly：基站
System Description TLV	设备描述信息
System Name TLV	设备名称

- 802.1 组织定义 TLV

TLV 类型	说明
端口 VLAN TLV	端口的 VLAN ID
端口协议 VLAN TLV	端口的协议 VLAN ID
VLAN Name TLV	VLAN 名称
Protocol identity TLV	端口支持的协议类型

- 802.3 组织定义 TLV

TLV 类型	说明
Link Aggregation TLV	端口是否支持链路聚合以及是否已使能链路聚合
MAC/PHY Configuration/Status TLV	端口的速率和双工状态、是否支持端口速率自动协商、是否已使能自动协商功能以及当前的速率和双工状态
Maximum Frame Size TLV	端口支持的最大帧长度，取端口最大传输单元 MTU（Max Transmission Unit）

版权所有 © 华为技术有限公司

TLV 类型	说明
Power Via MDI TLV	端口的供电能力，比如是否支持 PoE，是供电设备还是受电设备

- LLDP-MED TLV

TLV 类型	说明
LLDP-MED Capabilities TLV	当前设备的设备类型以及在 LLDPDU 中可封装的 LLDP-MED TLV 类型
Inventory TLV	设备的制造厂商
Location Identification TLV	位置标识信息，供其它设备在基于位置的应用中使用
Network Policy TLV	Voice VLAN 的 VLAN ID、二层优先级以及 DSCP 值等
Extended Power-via-MDI TLV	当前设备的供电能力

缺省情况下，LLDP 发布除 Location Identification TLV 之外所有类型的 TLV。

10.2.3 配置 LLDP 功能

介绍如何配置 LLDP 功能。

建立配置任务

应用环境

为了方便 NMS 获得网络设备间的拓扑信息、设备的主要能力、管理地址、设备标识、接口标识等信息，可以在网络设备上使能 LLDP 功能。

前置任务

在配置 LLDP 功能之前，需完成以下任务：

- 交换机与 NMS 之间路由可达，且 SNMP 相关参数已经配置完成。
- 需要配置用于 LLDP 管理的 IP 地址。

说明

LLDP 报文中携带的 LLDP 管理地址是用来标识设备的，必须选用网管系统能够唯一标识设备并且方便管理的 IP 地址（如管理网口地址）。要求配置的 LLDP 管理地址必须是设备上已存在的 IP 地址。所以该 IP 地址需要在**（可选）配置 LLDP 管理地址**之前配置。

数据准备

在配置 LLDP 功能之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	用作 LLDP 管理地址的 IP 地址
2	（可选）发送 LLDP 报文的周期
3	（可选）发送 LLDP 报文的延迟时间
4	（可选）本端信息在邻居节点中保持的时间倍数
5	（可选）接口 LLDP 模块从禁用状态到重新使能的延迟时间
6	（可选）发送邻居信息变化告警的延迟时间

使能全局 LLDP 功能

使能设备 LLDP 功能的情况下，交换机能够向使能 LLDP 功能的邻居节点发送携带本端状态信息的 LLDP 报文，同时也能通过 LLDP 报文获取使能 LLDP 功能的邻居节点的状态信息。网管可从交换机上获取当前设备的二层的连接状态信息并进行网络拓扑的分析。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp enable**，使能全局 LLDP 功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **bpdu enable**，配置转发 BPDU 报文。

----结束

（可选）禁止接口 LLDP 功能

在使能全局 LLDP 功能的情况下，所有接口缺省情况下都处于使能 LLDP 功能的状态。当部分接口需要禁用 LLDP 功能的情况下，执行 **undo lldp enable** 命令禁止 LLDP 功能。

前提条件

已使能全局 LLDP 功能。

背景信息

LLDP 功能有两个开关，一个是全局开关一个是接口下的开关，两者的关系为：

- 使能全局的 LLDP 功能后，缺省情况下所有接口的 LLDP 功能都处于使能状态。
- 去使能全局的 LLDP 功能后，除了 LLDP 告警功能外的所有关于 LLDP 的配置恢复缺省值。所以去使能全局的 LLDP 功能后，接口的 LLDP 功能处于去使能状态。
- 只有全局和接口下的 LLDP 功能都处于使能状态时，该接口才会发送或接收 LLDP 报文。
- 去使能全局 LLDP 功能的情况下，使能和去使能接口的 LLDP 命令无效。

版权所有 © 华为技术有限公司

- 当部分接口需要使能 LLDP 功能，而另一部分接口需要去使能 LLDP 功能时，可以全局使能 LLDP 功能，并在需要去使能 LLDP 功能的接口视图下执行 **undo lldp enable** 命令。当禁用 LLDP 功能的接口需要重新使能 LLDP 功能的情况下，在需要重新使能 LLDP 功能的接口视图下执行 **lldp enable** 命令重新使能接口 LLDP 功能。

说明

- 针对 Eth-Trunk 接口，LLDP 功能只能在 Eth-Trunk 的成员接口上进行配置，并且各成员接口的 LLDP 使能情况互相之间没有影响。
- 接口使能/去使能 LLDP 命令只能在已经全局使能 LLDP 的物理端口的视图中使用，对于如 VLANIF、Eth-Trunk 等逻辑端口的视图中则不能使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **undo lldp enable**，禁止接口 LLDP 功能。

----结束

（可选）配置 LLDP 管理地址

配置 LLDP 管理地址，供网管系统标识设备。

前提条件

已使能全局 LLDP 功能。

背景信息

如果指定的 IP 地址不合法，或没有配置管理 IP 地址，系统将自动从 IP 地址列表中查找并指定一个 IP 地址作为 LLDP 的管理 IP 地址。查找的顺序为：Loopback 接口、管理网口、VLANIF 接口。对于同一种类型接口的 IP 地址，取最小的一个 IP 地址。如果没有找到缺省的 IP 地址，则用系统的桥 MAC。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp management-address** *ip-address*，配置 LLDP 管理地址。

ip-address 必须为一个合法的并且是已经存在于设备上的单播 IP 地址，推荐使用管理网口的 IP 地址作为 LLDP 管理地址。

----结束

（可选）配置 LLDPDU 发布的 TLV 属性

在 LLDP 帧交互的过程中，LLDPDU 往往根据要求包含了很多种不同的 TLV，根据这些不同的 TLV 来传输或者接收自己和邻近设备的信息。LLDP 可以封装的 TLV 包括基本 TLV、组织定义 TLV 以及媒体终端发现 MED（Media Endpoint Discovery）相关 TLV。

版权所有 © 华为技术有限公司

前提条件

- 已使能全局 LLDP 功能。
- 已使能接口的 LLDP 功能。

背景信息

端口发送的 802.3 Power via MDI TLV（通过 **lldp tlv-enable dot3-tlv power** 命令配置是否发布 802.3 Power via MDI TLV）有两种格式：

- 802.1ab 标准规定的格式：[TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]
- 802.3at 标准规定的格式：[TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

802.3at 在 802.1 ab 基础上扩展了后面 3 个字段 type/source/priority、PD requested power value 和 PSE allocated power value，用于提供更详细的信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **lldp tlv-enable** { **basic-tlv** { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **protocol-identity** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *Tel-Number* } | **network-policy** | **power-over-ethernet** } }，配置接口发布的 TLV 类型。

缺省情况下，LLDP 发布除 Location Identification TLV 之外所有类型的 TLV。

说明

- 配置发布基本类型 TLV、IEEE 802.1 组织类型 TLV 或 IEEE 802.3 组织类型 TLV 时，指定 **all** 参数，将发布该类型所有可选 TLV；配置发布 LLDP-MED 相关 TLV，指定 **all** 参数将发布除 Location Identification TLV 之外该类型的所有可选 TLV。

  不指定 **all** 参数，每次只能配置发布一种类型的可选 TLV，可以通过多次配置发布多种类型的可选 TLV。
- 必须首先配置发布 LLDP-MED Capabilities TLV，才能配置发布 LLDP-MED 其它类型的 TLV。

  必须首先禁止发布 LLDP-MED 其它类型的 TLV，才能禁止发布 LLDP-MED Capabilities TLV。

  必须首先禁止发布 LLDP-MED Capabilities TLV，才能禁止发布 MAC/PHY Configuration/Status TLV。
- 配置发布 802.3 的 MAC/PHY Configuration/Status TLV，必须通过配置发布 LLDP-MED Capabilities TLV 自动发布。
- 禁止发布 LLDP-MED 相关 TLV，指定 all 参数，不会自动禁止发布 MAC/PHY Configuration/Status TLV。

步骤 4 执行命令 **lldp dot3-tlv power** {**802.1ab** | **802.3at** }，配置端口发送 802.3 Power via MDI TLV 符合的标准。

缺省情况下，端口发送符合 802.1 ab 标准的 802.3 Power via MDI TLV。

版权所有 © 华为技术有限公司

说明

在选择发送哪种标准的 802.3 Power via MDI TLV 时，需要注意对端设备对这两种标准的支持情况，本端配置的标准需要对端支持。

----结束

（可选）配置 LLDP 时间属性

可以配置的 LLDP 时间属性包括：发送 LLDP 报文的周期、发送 LLDP 报文的延迟时间、本端信息在邻居节点中保持的时间倍数、接口 LLDP 功能重新使能的延迟时间和邻居信息变化告警的延迟时间。

前提条件

已使能全局 LLDP 功能。

背景信息

发送 LLDP 报文的周期和发送 LLDP 报文的延迟时间

LLDP 报文的发送时间周期是指设备状态一直没有发生变化的情况下接口模块周期性的向邻居节点发送 LLDP 报文的时间周期。设备统一配置该时间周期之后，每一个使能 LLDP 功能的接口都以该间隔为周期向邻居节点发送 LLDP 报文，但是各个接口发送报文的时间点可以不一致。LLDP 报文发送周期的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负担，造成资源的浪费。

发送 LLDP 报文的延迟时间是指设备状态频繁发生变化的时候，接口模块向邻居节点发送 LLDP 报文的最小延迟时间。设备统一配置该延迟时间之后，每一个使能 LLDP 功能的接口都以该值为最小延迟时间向邻居节点发送 LLDP 报文，但是各个接口发送报文的时间点可以不一致。当设备的状态信息频繁发生变化的时候可以通过延长该延迟时间来减少设备频繁向邻居节点发送信息，以达到抑制拓扑振荡目的。LLDP 报文发送延迟时间的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负载，造成资源的浪费。

LLDP 报文发送周期 interval 与延迟时间 delay 互相有制约关系，所以调整 interval 的取值时候需要注意与 delay 的取值的配合。

- 增加 *interval* 不受 *delay* 的制约，只要大于等于 5 且小于或等于 32768 就可以。
- 减小 *interval* 的时候，*interval* 的目标取值一定要大于或等于四倍的当前 *delay* 值。所以 *interval* 要取的目标值小于四倍的 *delay* 的时候，需要先将 *delay* 调整到小于或等于 *interval* 目标值的四分之一，然后再将 *interval* 减小到目标值。

版权所有 © 华为技术有限公司

说明

在 *interval* 的取值小于四倍的 *delay* 缺省值的情况下，无法用 **undo lldp message-transmission delay** 命令恢复 *delay* 的缺省值，会出现错误提示信息。需要先将 *interval* 的取值调整到大于或等于四倍的 *delay* 的缺省值，然后再执行 **undo lldp message-transmission delay** 命令。

本端信息在邻居节点中保持的时间倍数

本端信息在邻居节点中保持的时间倍数用于计算本次发送报文的有效时间。通过配置这个参数来调整设备信息在邻居节点中储存的有效时间。邻居节点接收到报文后，用这个有效时间更新其邻居节点（即发送端）的信息老化时间。

消息保持有效时间计算公式是：TTL = Min (65535，（*interval* × *hold*))

- TTL 代表 Time to live，表示设备信息在邻居节点中保持的时间，取 65535 和 *interval* × *hold* 中的较小值。
- *interval* 代表设备向邻居节点发送 LLDP 报文的时间周期，通过 **lldp message-transmission interval** 命令配置。
- *hold* 代表设备信息在邻居节点中保持的时间倍数。

当原来使能 LLDP 功能的设备去使能 LLDP 功能后，它的邻居设备不会马上老化掉该设备的信息，而是在等待 TTL 时间后再进行老化，以防止网络拓扑频繁变更。设备信息在邻居节点中保持的时间倍数的取值要适当。

- 取值大，能够减少网络拓扑的频繁变化。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够及时发现网络拓扑结构。但是取值过小会导致邻居设备频繁刷新该设备的信息，从而增加系统的负担，造成资源的浪费。
- 一般情况下建议使用缺省值。

接口 LLDP 功能重新使能的延迟时间

接口 LLDP 模块重新使能延迟时间是指设备上的接口 LLDP 模块从去使能状态重新使能的延迟时间。通过配置该参数能够抑制由于接口的 LLDP 协议状态频繁改变而导致的邻居节点的拓扑振荡。接口 LLDP 模块从去使能状态重新使能的延迟时间的取值要适当。

- 取值大，能够减少网络拓扑的频繁变化。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够及时发现网络拓扑结构。但是取值过小会导致邻居设备频繁刷新该设备的信息，从而增加系统的负担，造成资源的浪费。
- 一般情况下建议使用缺省值。

邻居信息变化告警的延迟时间

发送邻居信息变化告警的延迟时间是指在使能 LLDP 告警的情况下，设备向网管系统发送 LLDP 告警的最小延迟时间。当邻居信息频繁发生变化的时候，可以通过延长该延迟时间来减少设备频繁向网管系统发送信息的情况，以达到抑制拓扑振荡目的。设备统一配置该延迟时间之后，每一个使能 LLDP 功能的接口都以该值为最小延迟时间向网管系统发送邻居信息变化告警，但是各个接口发送告警的时间点可以不一致。

该延迟时间只对插入邻居节点数、删除邻居节点数、老化邻居节点数、丢弃邻居节点数等邻居信息变化的告警（LLDP_1.0.8802.1.1.2.0.0.1 lldpRemTablesChange）起作用，对其它告警无影响。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **lldp message-transmission interval** *interval*，配置发送 LLDP 报文的周期。

缺省情况下，LLDP 报文的周期为 30 秒。

步骤 3 执行命令 **lldp message-transmission delay** *delay*，配置发送 LLDP 报文的延迟时间。

缺省情况下，发送 LLDP 报文的延迟时间是 2 秒。

步骤 4 执行命令 **lldp message-transmission hold-multiplier** *hold*，配置本端信息在邻居节点中保持时间的倍数。

缺省值是 4。

说明

- 增加该值能够延长本端信息在邻居节点中保持的时间。
- *hold* 的取值范围是 2~10，但当 hold × *interval* 的值大于 65535 时，配置不生效。

步骤 5 执行命令 **lldp restart-delay** *delay*，配置接口 LLDP 功能重新使能的延迟时间。

缺省值是 2 秒。

在禁止 LLDP 功能的情况下，需要经过该延迟时间才能重新使能接口 LLDP 功能。

步骤 6 执行命令 **lldp trap-interval** *interval*，配置邻居信息变化告警的延迟时间。

缺省值是 5 秒。

----结束

（可选）使能 LLDP 告警

在邻居信息发生变化时，为了向网管系统发送告警信息，需要在交换机上使能 LLDP 告警功能。

背景信息

使能设备的 LLDP 告警功能后，当设备出现以下情况时，设备会向网管系统发送告警。

- 使能或去使能全局 LLDP 功能，对应告警 LLDP_1.3.6.1.4.1.2011.5.25.134.2.1 hwLldpEnabled 和 LLDP_1.3.6.1.4.1.2011.5.25.134.2.2 hwLldpDisabled。
- 本地管理地址改变，对应告警 LLDP_1.3.6.1.4.1.2011.5.25.134.2.5 hwLldpLocManIPAddrChange。
- 邻居信息发生变化（邻居管理地址变化本地不会产生告警信息），对应告警 LLDP_1.0.8802.1.1.2.0.0.1 lldpRemTablesChange。

LLDP 告警功能对全局起作用，控制所有接口发送告警的能力。使能告警功能不以 LLDP 全局使能为前提。在组网前期网络拓扑变化频繁，可以关闭 LLDP 告警功能，控制告警信息频繁上送网管系统。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable feature-name lldptrap**，使能 LLDP 告警功能。

缺省情况下，AC6605 的 LLDP 告警功能处于禁用状态。

----结束

版权所有 © 华为技术有限公司

检查配置结果

前提条件

已经完成上述所有配置。

操作步骤

- 使用 **display lldp local** [**interface** *interface-type interface-number*]命令查看设备的本地 LLDP 状态。
- 使用 **display lldp neighbor** [**interface** *interface-type interface-number*]命令查看设备接口的邻居信息。
- 使用 **display lldp neighbor brief** 命令查看设备邻居的概要信息。
- 使用 **display lldp tlv-config** 命令查看接口可以发送的 TLV 类型。

----结束

10.2.4 维护

维护 LLDP 功能，包括清除 LLDP 统计信息、监控 LLDP 运行状态。

清除 LLDP 统计信息

通过执行 reset 命令，清除 LLDP 的统计信息。

操作步骤

- 在用户视图下，使用 **reset lldp statistics** [**interface** *interface-type interface-number*] 命令清除关于 LLDP 报文的统计信息。

----结束

监控 LLDP 运行状态

通过 display 命令监控 LLDP 的运行情况。

操作步骤

- 使用 **display lldp local** [**interface** *interface-type interface-number*]命令查看全局或指定接口的当前 LLDP 状态。
- 使用 **display lldp statistics** [**interface** *interface-type interface-number*]命令查看设备接口收发报文统计信息。
- 使用 **display lldp neighbor** [**interface** *interface-type interface-number*]命令查看设备接口的邻居信息。

----结束

10.2.5 配置举例

介绍 LLDP 的不同组网中举例。

配置 LLDP 功能示例-单邻居组网

单邻居组网方式下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

版权所有 © 华为技术有限公司

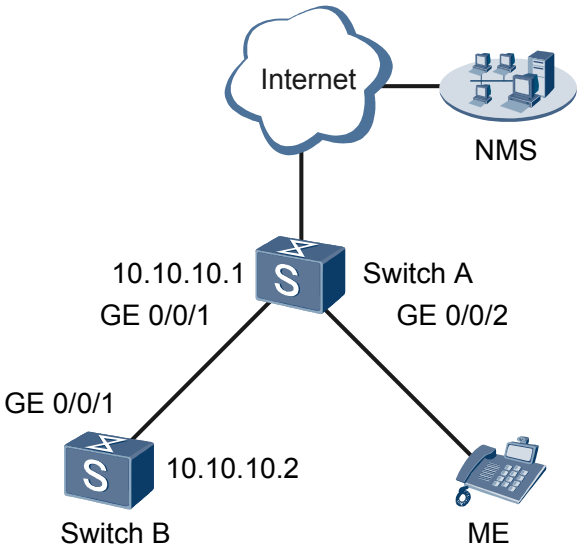
组网需求

如图 10-13 所示，SwitchA 和 SwitchB 之间、SwitchA 和 ME 均为直接相连。这时网络管理员希望在 NMS 上可以获取到 SwitchA、SwitchB 和 ME 的二层配置信息，用于了解网络的详细拓扑信息和判断网络中是否有配置冲突的情况。这时，可以通过在 SwitchA 和 SwitchB 上使能 LLDP 功能来实现网络管理员的需求。

另外，管理员希望当 LLDP 管理地址变化、全局 LLDP 功能使能或去使能以及邻居信息发生变化的时候，SwitchA、SwitchB 能主动向网管系统发送 LLDP 告警，这样便于管理员快速发现网络拓扑的变化。

组网中的 ME 设备支持 LLDP 功能，NMS 与 Switch 之间有可达路由且 SNMP 相关功能已经配置完成。

图 10-13 配置 LLDP 功能-单邻居组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 SwitchA 和 SwitchB 的全局 LLDP 功能。
2. 配置 SwitchA 和 SwitchB 处理 LLDP 的 BPDU 报文。
3. 配置 SwitchA 和 SwitchB 的管理 IP 地址方便网管系统进行管理。
4. 使能 SwitchA 和 SwitchB 的 LLDP 告警。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 和 SwitchB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 使能 SwitchA 和 SwitchB 的全局 LLDP 功能。

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] lldp enable
```

配置 SwitchB。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] lldp enable
```

步骤 2 配置 SwitchA 和 SwitchB 处理 LLDP 的 BPDU 报文。

配置 SwitchA。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
```

配置 SwitchB。

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] bpdu enable
```

步骤 3 配置 SwitchA 和 SwitchB 的管理 IP 地址。

配置 SwitchA。

```
[SwitchA] lldp management-address 10.10.10.1
```

配置 SwitchB。

```
[SwitchB] lldp management-address 10.10.10.2
```

步骤 4 使能 SwitchA 和 SwitchB 的 LLDP 告警。

配置 SwitchA。

```
[SwitchA] snmp-agent trap enable feature-name lldptrap
```

配置 SwitchB。

```
[SwitchB] snmp-agent trap enable feature-name lldptrap
```

步骤 5 验证配置结果。

查看各设备的 LLDP 是否使能、LLDP 管理地址是否配置以及 LLDP 告警功能是否使能。

- 查看 SwitchA。

```
[SwitchA] display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0011
System name    :SwitchA
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (AC6605 V100R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2009/2/13 18:31:37

MED system information
```


版权所有 © 华为技术有限公司

```
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V100R006C00

SerialNum         :NA
Manufacturer name :NA
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                    :enabled            (default is disabled)
LLDP Message Tx Interval       :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                 (default is 4)
LLDP Refresh Delay             :2                  (default is 2s)
LLDP Tx Delay                  :2                  (default is 2s)
LLDP Notification Interval     :5                  (default is 5s)
LLDP Notification Enable       :enabled            (default is disabled)
Management Address             :IP: 10.10.10.1

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 0 hours, 0 minutes, 0 seconds

Remote Neighbors Added          :0

Remote Neighbors Deleted        :0

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :1
Port information:


Port information:

Interface GigabitEthernet0/0/1:
LLDP Enable Status       :enabled            (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface


Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED port information
```


版权所有 © 华为技术有限公司

```
Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

查看 SwitchA 的邻居信息。

```
<SwitchA> display lldp neighbor interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 has 1 neighbors:


Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0011
Port ID type   :interfaceName
Port ID        :GigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
System name         :SwitchB
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (AC6605 V100R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :LE01MCUA VER.A
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V100R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Yes
```


版权所有 © 华为技术有限公司

```
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

- 查看 SwitchB。

  请参见 SwitchA 的查看过程。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 lldp enable
#
interface GigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
 lldp management-address  10.10.10.1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 lldp enable
#
interface GigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
 lldp management-address 10.10.10.2
#
return
```

配置 LLDP 功能示例-多邻居组网

多邻居组网方式下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

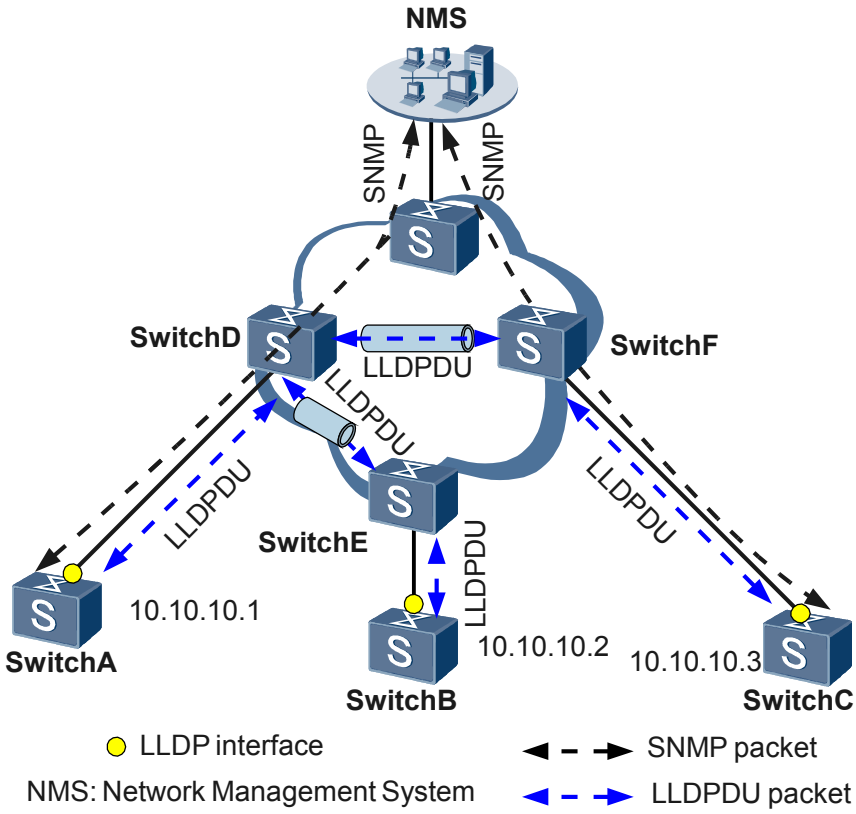
组网需求

如图 10-14 所示，SwitchA、SwitchB 和 SwitchC 之间通过一个未知网络相连，该未知网络无需 NMS 管理，但该网络可以透传 LLDP 报文。这时网络管理员希望在 NMS 上可以获取到 SwitchA、SwitchB 和 SwitchC 之间的二层配置信息，用于了解网络的详细拓扑信息和判断网络中是否有配置冲突的情况。这时，可以通过在 SwitchA、SwitchB 和 SwitchC 上使能 LLDP 功能来实现网络管理员的需求。

组网中 NMS 与 SwitchA、SwitchB 和 SwitchC 之间有可达路由且 SNMP 相关功能已经配置完成。

版权所有 © 华为技术有限公司

图 10-14 配置 LLDP 功能-多邻居组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 SwitchA、SwitchB 和 SwitchC 的全局 LLDP 功能。
2. 配置 SwitchA、SwitchB 和 SwitchC 处理 LLDP 的 BPDU 报文。
3. 配置 SwitchA、SwitchB 和 SwitchC 的管理 IP 地址方便网管系统进行管理。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA、SwitchB 和 SwitchC 的管理 IP 地址。

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 的 LLDP 全局使能。

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] lldp enable
```

配置 SwitchB。

版权所有 © 华为技术有限公司

请参见 SwitchA 的配置。

配置 SwitchC。

请参见 SwitchA 的配置。

步骤 2 配置 SwitchA、SwitchB 和 SwitchC 处理 LLDP 的 BPDU 报文。

配置 SwitchA。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] bpdu enable
```

配置 SwitchB。

请参见 SwitchA 的配置。

配置 SwitchC。

请参见 SwitchA 的配置。

步骤 3 配置 SwitchA、SwitchB 和 SwitchC 的管理 IP 地址。

配置 SwitchA。

```
[SwitchA] lldp management-address 10.10.10.1
```

配置 SwitchB。

```
[SwitchB] lldp management-address 10.10.10.2
```

配置 SwitchC。

```
[SwitchC] lldp management-address 10.10.10.3
```

步骤 4 验证配置结果。

查看各设备的 LLDP 功能是否使能、LLDP 管理地址是否配置。

- 查看 SwitchA 的配置。

  # 查看 SwitchA 的邻居信息。

```
<SwitchA> display lldp neighbor interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 has 2 neighbors:


Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0012
Port ID type   :interfaceName
Port ID        :GigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
System name         :SwitchB
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (AC6605 )
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM
```


版权所有 © 华为技术有限公司

```
Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V100R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Undefined
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Neighbor index : 2
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0013
Port ID type   :interfaceName
Port ID        :GigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
System name         :SwitchC
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (AC6605 )
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.3
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
```


版权所有 © 华为技术有限公司

```
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V100R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Undefined
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

- 查看 SwitchB 的配置。

  请参见 SwitchA 的查看过程。

- 查看 SwitchC 的配置。

  请参见 SwitchA 的查看过程。

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
#
 lldp enable
#
 lldp management-address 10.10.10.1
#
interface GigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
#
 lldp enable
#
 lldp management-address 10.10.10.2
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
#
 lldp enable
#
 lldp management-address 10.10.10.3
#
interface GigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

配置 LLDP 功能示例-组网中存在链路聚合

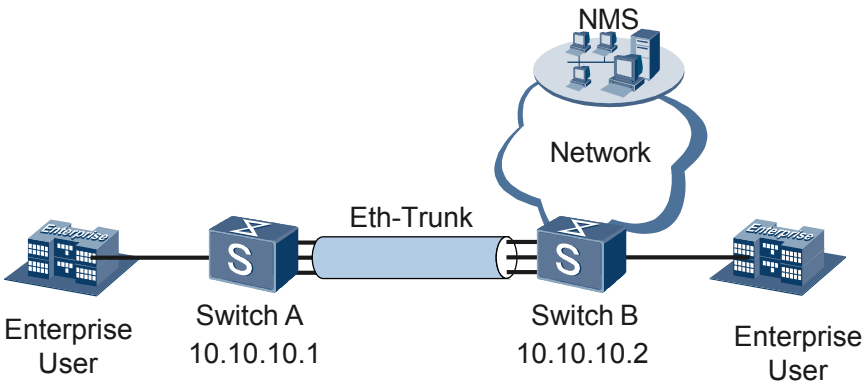
组网中存在链路聚合的情况下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

组网需求

如图 10-15 所示，SwitchA 与 SwitchB 之间通过 Eth-Trunk 相连。网络管理员希望在 NMS 上可以获取到 Switch 之间的二层配置信息，用于了解除未知网络以外的设备的详细拓扑信息和判断 Switch 中是否有配置错误的情况。这时，可以通过在 SwitchA 与 SwitchB 上使能 LLDP 功能来实现网络管理员的需求。

组网中 NMS 与 SwitchA 和 SwitchB 之间有可达路由且 SNMP 相关功能已经配置完成。

图 10-15 配置 LLDP 功能示例组网图-组网中存在链路聚合



配置思路

采用如下的思路配置 LLDP 功能：

1. 将 SwitchA 和 SwitchB 的以太网物理接口加入到 Eth-Trunk 中。

版权所有 © 华为技术有限公司

2. 使能 SwitchA 和 SwitchB 的全局 LLDP 功能。
3. 配置 SwitchA 和 SwitchB 处理 LLDP 的 BPDU 报文。
4. 配置 SwitchA 和 SwitchB 的管理 IP 地址方便网管系统进行管理。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchA 和 SwitchB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。
- SwitchA 和 SwitchB 相连的 Eth-Trunk 的编号，加入到该 Eth-Trunk 的成员接口的编号。

操作步骤

步骤 1 配置 SwitchA 和 SwitchB 的 Eth-Trunk。

配置 SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] trunkport gigabitethernet 0/0/1
[SwitchA-Eth-Trunk1] trunkport gigabitethernet 0/0/2
[SwitchA-Eth-Trunk1] trunkport gigabitethernet 0/0/3
[SwitchA-Eth-Trunk1] port link-type trunk
[SwitchA-Eth-Trunk1] port trunk allow-pass vlan 100
[SwitchA-Eth-Trunk1] quit
```

配置 SwitchB。

请参见 SwitchA 的配置。

步骤 2 使能 SwitchA 和 SwitchB 的全局 LLDP 功能。

配置 SwitchA。

```
[SwitchA] lldp enable
```

配置 SwitchB。

请参见 SwitchA 的配置。

步骤 3 配置 SwitchA 和 SwitchB 处理 LLDP 的 BPDU 报文。

配置 SwitchA。

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] bpdu enable
[SwitchA-Eth-Trunk1] quit
```

配置 SwitchB。

请参见 SwitchA 的配置。

步骤 4 配置 SwitchA 和 SwitchB 的管理 IP 地址以便在邻居设备中标识本端设备。

配置 SwitchA。

```
[SwitchA] lldp management-address 10.10.10.1
```

配置 SwitchB。

版权所有 © 华为技术有限公司

```
[SwitchB] lldp management-address 10.10.10.2
```

步骤 5 验证配置结果。

- 查看 SwitchA 的配置。

  # 查看各设备的成员接口是否已经加入到 Eth-Trunk1。

```
[SwitchA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                      Status      Weight
GigabitEthernet0/0/1          Up          1
GigabitEthernet0/0/2          Up          1
GigabitEthernet0/0/3          Up          1
```

  #查看设备当前的 LLDP 信息。

```
[SwitchA] display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0011
System name    :SwitchA
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (AC6605 V100R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2010/2/13 18:31:37

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER B
FirmwareRev       :NA
SoftwareRev       :Version 5.70 V100R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                     :enabled            (default is disabled)
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 15 hours, 1 minutes, 21 seconds
Remote Neighbors Added          :1

Remote Neighbors Deleted        :0

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:

Interface GigabitEthernet0/0/1:
```


版权所有 © 华为技术有限公司

```
LLDP Enable Status       :enabled            (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :1
Maximum frame Size       :1600
MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface GigabitEthernet0/0/2:
LLDP Enable Status       :enabled            (default is disabled)
Total Neighbors           :1

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet0/0/2
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/2 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :Yes
Aggregation port ID      :1
Maximum frame Size       :1600
```


版权所有 © 华为技术有限公司

```
MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface GigabitEthernet0/0/3:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors           :1

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet0/0/3
Port description    :HUAWEI, Quidway Series, GigabitEthernet0/0/3 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :Yes
Aggregation port ID      :1
Maximum frame Size       :1600

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

查看 SwitchA 的邻居信息。

```
[SwitchA] display lldp neighbor brief
Local Intf   Neighbor Dev            Neighbor Intf            Exptime
GE0/0/1      SwitchB                 GE0/0/1                  115
GE0/0/2      SwitchB                 GE0/0/2                  115
GE0/0/3      SwitchB                 GE0/0/3                  115
```

- 查看 SwitchB 的配置。

  请参见 SwitchA 的查看过程。

----结束

版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100
#
interface Vlanif1
 ip address 10.10.10.1 255.255.255.0
#
 lldp enable
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
 lldp management-address  10.10.10.1
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
interface Vlanif1
 ip address 10.10.10.2 255.255.255.0
#
 vlan batch 100
#
 lldp enable
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
 lldp management-address  10.10.10.2
#
return
```

10.3 HGMP 配置

通过配置 HGMP 协议，利用一台命令交换机建立集群，对加入集群的大量以太网交换机进行集中管理和配置，可以减轻工程和维护的工作量。

版权所有 © 华为技术有限公司

10.3.1 HGMP 概述

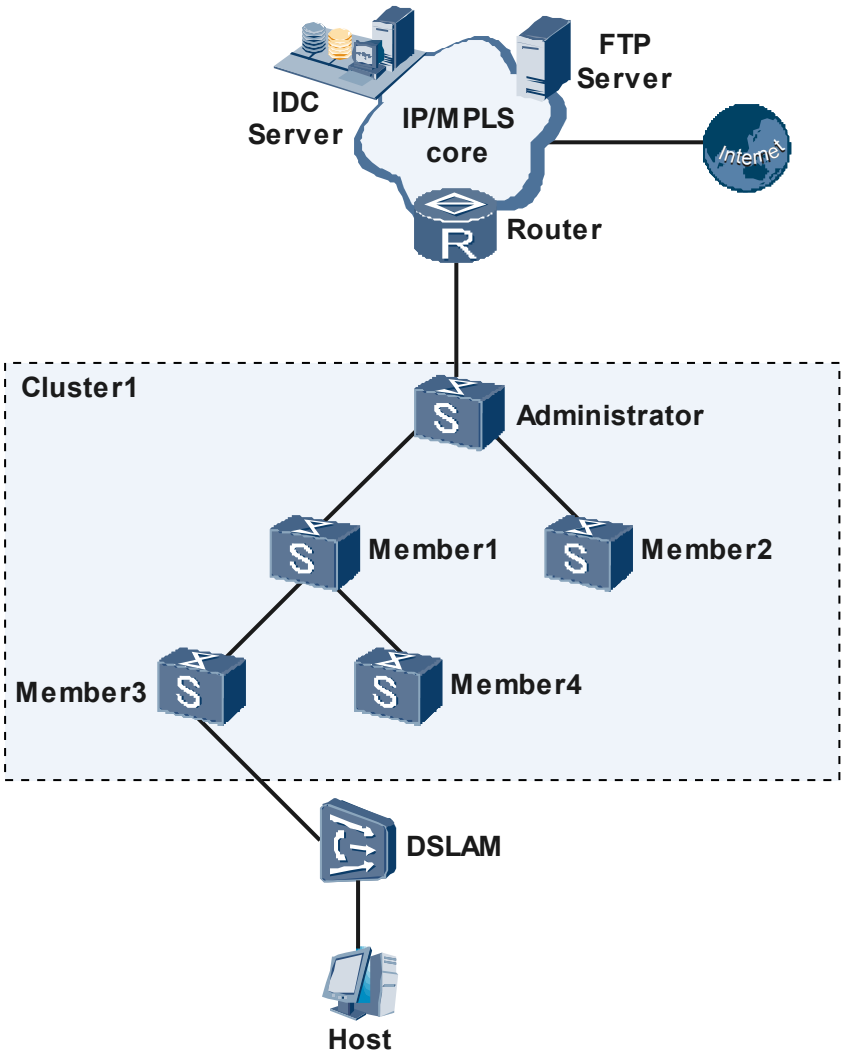
通过 HGMP 概述您可以了解到 HGMP 的引入原因和典型组网。

目前无论在城域网还是企业网中都广泛采用了以太网技术，随着网络规模的增大，在网络边缘使用大量的接入设备，由于这些设备数量巨大，又需要逐一管理维护，使管理工作非常繁琐，同时要为这些设备逐一配置 IP 地址，在目前 IP 地址资源比较紧张的情况下无疑是一种浪费。

HGMP（Huawei Group Management Protocol）即华为组管理协议，该协议是华为公司自主开发的用于管理一组以太网交换机的协议。通过 HGMP 协议，利用一台命令交换机建立集群，对加入集群的大量以太网交换机进行集中管理和配置，可以减轻工程和维护的工作量。此外由于一个集群对外只使用一个 IP 地址，这种管理方式还可以节约 IP 地址，缓解目前 IP 地址资源比较紧张的情况。

集群的基本组网图如图 10-16 和图 10-17 所示。

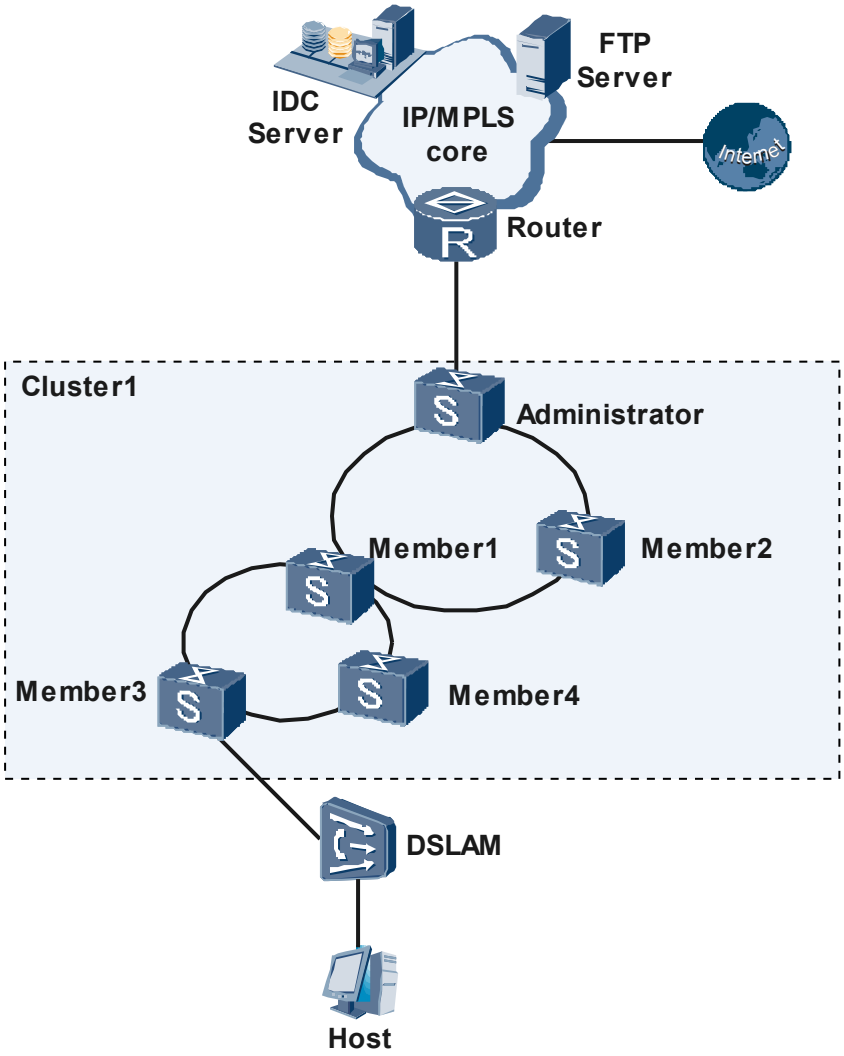
图 10-16 集群基本组网图（树型）



Administrator：命令交换机　　Member：成员交换机

华为专有和保密信息
版权所有 © 华为技术有限公司

图 10-17 集群基本组网图（RRPP）



Administrator：命令交换机　　Member：成员交换机

10.3.2 AC6605 支持的 HGMP 特性

您可以了解到 AC6605 对 HGMP 的支持情况。

NDP

NDP（Neighbor Discovery Protocol）是 HGMP 定义的邻居发现报文，用于收集直接相连的邻居站点信息。NDP 报文收集的邻居站点信息包括设备类型、软件版本、硬件版本、连接接口、成员编号、用于集群通信的私有 IP 地址、硬件平台等信息。

说明

任何支持 HGMP 的设备都不转发 NDP 报文。

设备在本机中建立 NDP 表，用于存储邻居站点信息。

版权所有 © 华为技术有限公司

当设备从邻居站点接收到 NDP 报文时，设备对报文内容和 NDP 表进行比较，更新相应的表项信息。

NTDP

NTDP（Network Topology Discovery Protocol）是 HGMP 定义的拓扑收集报文，用于收集网络拓扑信息。设备根据 NDP 表提供的邻居站点信息，发送和转发拓扑收集请求，在一定网络范围内收集每台设备中 NDP 表的表项。

当设备收到 NTDP 拓扑请求报文后，会立即发送 NTDP 拓扑响应报文。同时，设备根据 NTDP 转发原则，向其它接口转发接收到的 NTDP 报文。

集群角色

HGMP 定义了 4 种集群角色：命令交换机、成员交换机、候选交换机和备份交换机。

说明

目前 AC6605 暂不支持备份交换机的角色。

- 命令交换机是集群中的管理设备。为保证集群内部设备与集群外部设备的正常通信，命令交换机需要设置公网 IP 地址。
- 成员交换机是集群中的成员设备。对成员交换机的管理是通过命令交换机的代理来完成的。成员交换机可以不设置公网 IP 地址。
- 候选交换机是指具有集群功能，但未加入任何集群的设备。
- 备份交换机是指集群中为命令交换机提供备份功能的设备。当命令交换机失效时，备份交换机能够自动转换为命令交换机。

用户可以通过配置来指定设备的角色，各种角色可以按一定的规则进行切换。

基本集群管理

基本集群管理主要包括以下主要内容：

- 建立集群管理域
- 加入成员/删除成员
- 成员状态迁移
- 集群内部通讯
- 命令交换机/候选交换机的切换
- 拓扑显示
- 修改集群管理配置
- SNMP 自动配置

NAT

HGMP 通过 NAT 实现集群内成员与公网设备的互通，并可以通过开关控制是否通过 NAT 实现互通。

- 命令交换机是集群中的管理设备。为保证集群内部设备与集群外部设备的正常通信，命令交换机需要设置公网 IP 地址。
- 为保证集群内外设备通过 NAT 互通，命令交换机上要打开指定协议的 NAT 开关。

版权所有 © 华为技术有限公司

- 集群使用的 NAT 规则由命令交换机自动配置，对从集群内访问集群外设备，成员交换机会自动获取 NAT 映射端口，对从集群外访问集群内设备，需要计算成员设备指定服务的端口号。

批量下发

HGMP 提供对所管理的成员交换机批量下发的操作，批量下发的范围包括产品大包、设备配置文件、补丁。

- 只有命令交换机可以执行批量下发命令。
- 命令交换机上可以配置即插即用使用的 ip 地址、用户名和密码，当命令中不指定 ip 地址、用户名和密码时，将使用即插即用的 ip 地址、用户名和密码。当这两者都未配置时，命令不能执行。
- 成员交换机使用 FTP 从服务器上下载指定的文件，下载完成后，自动将文件设置为下次启动的默认值。
- 可以配置成员交换机同时进行 FTP 下载的数量，避免拥塞。

批量重启

HGMP 提供对指定的一组成员交换机批量重启。

- 批量重启时，成员交换机不会保存当前配置。
- 成员交换机收到批量重启命令后，会等待 1 秒保证控制报文在集群内充分扩散。

增量配置

在集群范围内，通常有一些成员设备有相同的配置，如创建 VLAN，打开某一特性。增量配置功能，是针对组选成员设备进行批量远程控制，1ToN 方式操作简单快捷，只需在命令设备上编辑控制命令列表，一次下发完成，并可查询各个成员设备各个控制命令的执行状况。组选方式可以是全选，根据设备类型，根据成员 ID 或根据 IP 地址。

- 增量配置只能在命令交换机上操作。
- 增量配置适应于批量成员设备统一操作场景，针对组选设备一次执行完成。
- 增量配置返回结果列表报告各成员执行情况，如遇到执行错误可针对序号找到具体执行错误的命令。
- 增量配置只保存最后一次执行结果，下一次执行下发后自动清除上次结果。
- 增量配置视图下编辑配置命令列表，命令执行和具体视图密切相关，执行顺序方法与单台设备上一致。

同步配置文件

集群建立，并且配置好基本功能后，可以通过同步配置命令，将集群成员的配置文件保存到指定的 FTP 服务器上。

- 同步配置，需要预先指定 FTP Server。

安全特性

集群建立完成，并配置好基本功能后，可根据需求将集群网络边界关闭，将集群的可管理范围确定下来。在打开即插即用功能以及 PAF 控制 HGMP 能力设备自动打开二层口 NDP 和 NTDP 协议后，成员设备上大量二层口自动配置了 NDP 和 NTDP 协议使能，在

版权所有 © 华为技术有限公司

一些集群不相关的端口上，可不必开启这些功能。关闭不相关端口 NDP/NTDP 协议状态减少报文负担，也确保集群拓扑不再轻易变化。

- 在命令交换机上执行集群内不相关端口 NDP/NTDP 协议状态关闭开启。
- 关闭集群不相关端口 NDP 协议状态，端口上 NDP 报文不再上送。
- 关闭集群不相关端口 NTDP 协议状态，端口上 NTDP 报文不再上送。
- 在集群范围确定之后，集群的不相关端口定义为没有 NDP 邻居的端口。

即插即用

一台将要加入集群的设备，需要人工完成一些集群相关的配置。在设备数量巨大的情况下，将及其耗费人力，即插即用可以解决这个问题。预先通过 PAF 控制设备做一些集群必须的基本配置，然后，物理接入集群设备，该设备就可以自动加入集群。

- 即插即用需要 PAF 控制设备，做一些基本配置。
- 命令交换机需要使能即插即用功能。
- 命令交换机和成员相连接的端口配置，需要以 TRUNK 方式加入管理 VLAN。
- 命令交换机需要启用 NTDP 定时收集功能。

10.3.3 配置 HGMP 的基本功能

通过配置 HGMP 的基本功能，可以建立或者管理一个集群。

建立配置任务

在配置 HGMP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当用户需要建立或管理一个集群时，此时可以配置 HGMP 的基本功能。

前置任务

在配置 HGMP 集群的基本功能之前，需完成以下任务：

- 设备正确上电，且工作正常
- 配置设备接口的基本属性

数据准备

在配置 HGMP 集群的基本功能之前，需要准备以下数据。

序号	数据
1	集群使用的私有 IP 地址范围
2	集群的名称
3	成员交换机的 MAC 地址

版权所有 © 华为技术有限公司

序号	数据
4	（可选）NDP 信息有效保留时间、NDP 报文的发送时间间隔
5	（可选）拓扑收集范围、NTDP 拓扑请求报文转发时的跳数延迟时间和接口延迟时间、定时收集拓扑的时间间隔
6	（可选）管理 VLAN 的 VLAN 编号、有效保留时间、握手报文定时发送时间、网管主机地址、FTP 服务器和 SFTP 服务器地址

配置 NDP

通过配置 NDP 来收集设备直接相连的邻居站点信息。

操作步骤

- 使能系统 NDP

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ndp enable**，使能系统 NDP。

     缺省情况下，系统 NDP 处于使能状态。

- 使能接口 NDP

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 这时可有两种选择：
     - 执行命令 **ndp enable interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>，在系统视图下使能接口 NDP。
     - 执行命令 **interface** *interface-type interface-number*，进入接口视图后，再执行命令 **ndp enable**，使能接口 NDP。

- （可选）配置 NDP 信息的有效保留时间

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ndp timer aging** *aging-time*，配置 NDP 信息的有效保留时间。

     缺省情况下，NDP 信息的有效保留时间为 180 秒。NDP 信息的有效保留时间必须比 NDP 报文发送的时间间隔长。

- （可选）配置 NDP 报文发送的时间间隔

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ndp timer hello** *interval*，配置 NDP 报文发送的时间间隔。

     缺省情况下，NDP 报文发送时间间隔为 60 秒。NDP 报文发送的时间间隔必须比 NDP 信息的有效保留时间短。

----结束

版权所有 © 华为技术有限公司

配置 NTDP

通过配置 NTDP 来收集网络拓扑信息。

操作步骤

- 使能系统 NTDP

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ntdp enable**，使能系统 NTDP。

     缺省情况下，系统 NTDP 处于使能状态。

- 使能接口 NTDP

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **ntdp enable**，使能接口 NTDP。

- （可选）配置拓扑收集范围

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ntdp hop** *max-hop-value*，配置拓扑收集范围。

     缺省情况下，拓扑收集范围为 3。拓扑收集范围越大，占用拓扑收集设备的内存越多。

- （可选）配置转发 NTDP 报文的延迟时间

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ntdp timer hop-delay** *hop-delay-time*，配置转发 NTDP 报文的跳数延迟时间。
  3. 执行命令 **ntdp timer port-delay** *port-delay-time*，配置转发 NTDP 报文的接口延迟时间。

     缺省情况下，NTDP 的跳数延迟时间为 200ms，NTDP 的接口延迟时间为 20ms。

- （可选）配置定时拓扑收集的时间间隔

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ntdp timer** *interval*，配置定时拓扑收集的时间间隔。

     缺省情况下，定时拓扑收集的时间间隔为 0 分钟，即不进行定时拓扑收集。

- （可选）启动拓扑信息收集

  请在命令交换机和成员交换机上执行下面的命令。

  1. 在用户视图下，执行命令 **ntdp explore**，启动拓扑信息的收集。

版权所有 © 华为技术有限公司

用户可以通过此命令随时收集网络拓扑。

----结束

创建集群

当用户需要通过集群来管理设备时，需要先创建集群。

操作步骤

- 配置管理 VLAN

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

     缺省情况下，设备的管理 VLAN 是 VLAN 1，且需要手工创建。

     - 如果不需要更改缺省的管理 VLAN，则可不执行步骤 6 和步骤 7。此时步骤 2 中的 vlan-id 是“1”。
     - 如果需要更改管理 VLAN 的 VLAN 编号，则步骤 2、步骤 4 和步骤 7 中的 vlan-id 必须相同。
  3. 执行命令 **quit**，退出 VLAN 视图。
  4. 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 并进入 VLANIF 视图。
  5. 执行命令 **quit**，退出 VLANIF 视图。
  6. 执行命令 **cluster**，进入集群视图。
  7. 执行命令 **mngvlanid** *vlan-id*，配置管理 VLAN。

     在命令交换机上更改管理 VLAN 的 VLAN 编号或者删除管理 VLAN 及相应的 VLANIF，则集群自动被删除。

     在成员交换机上更改管理 VLAN 的 VLAN 编号或者删除管理 VLAN 及相应的 VLANIF，则成员交换机自动退出集群。

- 使能集群功能

  请在命令交换机和成员交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster enable**，使能集群功能。

     缺省情况下，HGMP 集群功能处于使能状态。

- 创建集群

  AC6605 设备提供了手动创建集群和自动创建集群两种方式。

  说明

  创建 HGMP 集群后，如果重启命令交换机，那么成员交换机重新加入集群，其编号可能发生变化。

  手动创建集群

  下面的配置步骤只需要在一台设备上执行配置，该设备是命令交换机或者是 HGMP 集群建立后的命令交换机。

版权所有 © 华为技术有限公司

通过这种方式创建集群时，需要用户手动添加成员交换机。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **ip-pool** *administrator-ip-address* { *mask-length* | *mask* }，配置集群使用的 IP 地址范围。

   该步骤只能在集群还没有建立时才能执行。如果集群已经建立，系统不允许修改集群使用的私有 IP 地址范围。

   说明

   集群使用的 IP 地址不能与设备上的已经存在的 IP 地址重复。
4. 执行命令 **build** *cluster-name*，设置命令交换机及集群名称并创建集群。

自动创建集群

下面的配置步骤只需要在一台设备上执行，该设备是命令交换机或者是 HGMP 集群建立后的命令交换机。

通过这种方式创建集群时，命令交换机会提示用户是否将已发现的所有的候选交换机加入集群。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **ip-pool** *administrator-ip-address* { *mask-length* | *mask* }，配置集群使用的 IP 地址范围。

   该步骤只能在集群还没有创建时才能执行。如果集群已经创建，系统不允许修改集群 IP 地址范围。

   说明

   集群使用的 IP 地址不能与设备上的已经存在的 IP 地址重复。
4. 执行命令 **auto-build** [**recover**]，自动建立集群。

   auto-build 命令还可以用于自动添加成员交换机，具体配置过程请参见“添加成员交换机”。

   说明

   由于设备上的集群功能默认为使能，当使用 **auto-build** 自动建立集群并添加成员交换机后，命令交换机可以直接管理成员交换机。

----结束

添加成员交换机

当用户希望通过集群来管理某台设备，而该设备并不是该集群的成员交换机时，就可以配置增加成员交换机。

背景信息

创建集群后，可以通过以下两种方法来增加成员交换机。

说明

由于设备上的集群功能默认为使能，当建立集群并添加成员交换机后，命令交换机可以直接管理成员交换机。

版权所有 © 华为技术有限公司

操作步骤

- 手动增加成员交换机

  通过这种方式增加成员交换机时，需要用户手动指定成员交换机的 MAC 地址。

  本配置只能在命令交换机上执行。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **add-member** [*member-number*] **mac-address** *mac-address* [**password** *password*]，增加成员交换机。

- 自动增加成员交换机

  通过这种方式增加成员交换机时，命令交换机会提示用户是否将已发现的所有的候选交换机加入集群。但如果增加成员交换机的方式为验证方式时，命令交换机将退回自动增加成员交换机的操作。

  本配置只能在命令交换机上执行。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **auto-build** [**recover**]，自动增加成员交换机。

     auto-build 命令还可以用于自动创建集群，具体配置过程请参见“创建集群”。

     recover 用来将所有成员交换机重新加入 HGMP 集群，包括在命令交换机上丢失的成员交换机。

     说明

     如果 HGMP 集群 A 的命令交换机认为交换机 N 不属于集群 A，但交换机 N 却认为自己属于集群 A，则交换机 N 被称为在命令交换机上丢失的成员交换机。

----结束

（可选）删除或退出集群

背景信息

当用户不需要通过集群来管理设备，但之前又已经创建过集群时，可以将该设备删除或退出集群。

操作步骤

- 删除集群

  请在命令交换机上执行下面的命令，实现删除集群的功能。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入 HGMP 集群视图。
  3. 执行命令 **undo build**，删除集群。

     在命令交换机上执行本命令后，HGMP 集群视图下 **mngvlanid** 命令和 **ip-pool** 命令相关的配置仍存在，其它与命令交换机相关的配置将被删除。此外所有的成员交换机将自动退出集群。

版权所有 © 华为技术有限公司

- 禁用集群

  请在命令交换机或者成员交换机上执行下面的命令，实现禁用集群的功能。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **undo cluster enable**，禁用集群。
     - 在命令交换机上执行本命令后，HGMP 集群视图下 **mngvlanid** 命令相关的配置仍存在，其它与 HGMP 集群相关的配置将被删除。此外所有的成员交换机将自动退出集群。
     - 在成员交换机上执行本命令后，该成员交换机将自动退出集群，对其他的成员交换机和命令交换机无影响。

- 退出集群

  请在成员交换机上执行下面的命令，实现退出集群的功能。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入 HGMP 集群视图。
  3. 执行命令 **undo administrator-address**，退出集群。

     说明

     在成员交换机上使用 **undo administrator-address** 命令，只会使成员交换机短暂地退出集群，而不会导致命令交换机将该成员删除。如果要从一个 HGMP 集群中彻底删除成员交换机，建议用户使用 **delete-member** 命令。

----结束

（可选）删除成员交换机

当用户不再需要通过集群来管理某个管理域中的某台设备时，就可以配置删除成员交换 机。

背景信息

当用户不再需要通过集群来管理某个管理域中的某台设备时，就可以配置删除成员交换机。

本配置只能在命令交换机上执行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cluster**，进入集群视图。

步骤 3 执行命令 **delete-member** *member-number*，删除成员交换机。

----结束

检查配置结果

在配置 HGMP 的基本功能成功后，可以查看到已经完成的 HGMP 基本功能的配置。

前提条件

已经完成 HGMP 的基本功能的所有配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用命令 **display ndp**，查看系统 NDP 配置信息。
- 使用命令 **display ndp interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>，查看指定接口 NDP 发现的邻居信息。
- 使用命令 **display ntdp**,查看全局 NTDP 信息。
- 使用命令 **display ntdp device-list** [**verbose**]，查看 NTDP 收集到的设备信息。
- 使用命令 **display cluster**，查看集群状态和统计信息。
- 使用命令 **display cluster candidates** [**mac-address** *mac-address* | **verbose**]，查看候选交换机信息。
- 使用命令 **display cluster members** [*member-number* |**verbose**]，查看集群成员信息。

----结束

任务示例

如果 NDP 邻居正常建立，执行命令 **display ndp**，可以看到邻居节点的 MAC 地址和邻居节点的与本接口相连的接口号等信息。

```
<Quidway> display ndp
Neighbor discovery protocol is enabled.
Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
Interface: GigabitEthernet0/0/1
    Status: Disabled, Packets Sent: 0, Packets Received: 0, Packets Error: 0
Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0

    Neighbor 1:  Aging Time: 174(s)
       MAC Address : 0018-8203-39d8
       Port Name   : GigabitEthernet0/0/1
       Software Version: VRP 5.70 V100R006C00
       Device Name : AC6605
       Port Duplex : FULL
       Product Ver : AC6605
```

如果 NDP 邻居正常建立，执行命令 **display ndp interface**，可以看到邻居节点的 MAC 地址和邻居节点的与本接口相连的接口号等信息。

```
<Quidway> display ndp interface gigabitethernet 0/0/1
Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 116, Packets Received: 110, Packets Error: 0
    Neighbor 1:  Aging Time: 174(s)
       MAC Address : 0018-8203-39d8
       Port Name   : GigabitEthernet0/0/1
       Software Version: VRP 5.70 V100R006C00
       Device Name : AC6605
       Port Duplex : FULL
       Product Ver : AC6605
```

如果 NTDP 邻居正常建立，执行命令 **display ntdp**，可以看到 NTDP 的配置信息。

```
<Quidway> display ntdp
 Network topology discovery protocol is enabled
 Hops      : 3
 Timer     : 10 min
 Hop Delay : 200 ms
 Port Delay: 20 ms
 Total time for last collection:462ms
```

如果 NTDP 协议收集设备信息成功，执行命令 **display ntdp device-list** [**verbose**]，可以看到所有设备的信息列表。

```
<Quidway> display ntdp device-list
```


版权所有 © 华为技术有限公司

```
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                       AC6605
 0003-0003-0003  1                       AC6605
 0002-0002-0002  1                       AC6605
 0001-0001-0001  0                       AC6605
```

如果集群建立成功，执行命令 **display cluster**，可以看到本设备所属 HGMP 集群的信息，例如集群名称，管理 VLAN ID 等。

```
<HUAWEI_0.Quidway> display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.1.1.1/24
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 2 member(s) in the cluster, and 0 of them are down.
```

如果集群建立成功，执行命令 **display cluster candidates**，可以看到候选交换机的信息，例如：MAC 地址，设备类型等。

```
<HUAWEI_0.Quidway> display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

如果集群建立成功，执行命令 **display cluster members**，可以看到成员交换机的信息，例如：MAC 地址，设备类型等，并且成员交换机的状态为“Up”。

```
<HUAWEI_0.Quidway> display cluster members
The list of cluster member:
--------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
--------------------------------------------------------------------------------
0    AC6605                   00e0-fcb8-d6b6  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0018-8267-7f7d  Up     HUAWEI_1.Member-1
2    AC6605                   00e0-0003-0003  Up     HUAWEI_2.Member-2
```

10.3.4 配置 HGMP 的高级功能

介绍在建立基本的 HGMP 集群后，配置 HGMP 的一些可选特性，以进一步简化 HGMP 的管理与维护。

建立配置任务

在配置 HGMP 的高级功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

当用户已经建立和管理一个集群后，需要对集群的性能参数进行优化，以进一步简化HGMP 的管理与维护，更好的管理集群中的成员交换机，此时可以配置 HGMP 的高级功能。

前置任务

在配置 HGMP 集群的高级功能之前，需完成以下任务：

- 设备正确上电，且工作正常
- 配置设备接口的基本属性
- **配置 HGMP 的基本功能**

数据准备

在配置 HGMP 的高级功能之前，需要准备以下数据。

序号	数据
1	握手报文定时发送的时间间隔
2	设备的有效保留时间
3	成员交换机的老化时间
4	集群的组播地址
5	集群公用的 FTP 服务器、SFTP 服务器、日志主机，网管主机地址
6	配置集群默认的 FTP 服务器信息，包括 IP 地址，用户名称和密码

调整集群参数

为了更好的完成对集群设备的管理，可以根据需要来调整 HGMP 的参数。可以调整的参数包括：握手报文发送的时间间隔；配置有效保留时间；使能候选交换机自动加入集群的功能；配置成员交换机的老化时间；配置集群的组播地址；配置集群接口加入 VLAN 方式；配置集群公用服务器和主机。

操作步骤

- 配置握手报文发送的时间间隔

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **timer** *interval*，配置握手报文定时发送的时间间隔。

     缺省情况下，握手报文定时发送的时间间隔为 10 秒。该取值必须小于或等于有效保留时间的三分之一。

- 配置有效保留时间

  请在命令交换机上执行下面的命令。

版权所有 © 华为技术有限公司

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **holdtime** *hold-time*，配置设备的有效保留时间。

   缺省情况下，设备的有效保留时间为 60 秒。该取值必须大于或等于握手报文发送时间间隔的三倍。

- 使能候选交换机自动加入集群的功能

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **cluster-autojoin**，使能候选交换机自动加入集群的功能。

- 配置成员交换机的老化时间

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **cluster-discagingtime** *disconnect-aging-time*，配置成员交换机的老化时间。

     缺省情况下，没有配置老化时间，表示不进行老化处理。

- 配置集群的组播地址

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **cluster-multimac** *mac-address*，配置集群的组播地址。

     该组播地址的取值范围请参见《AC6605 命令参考》，缺省情况下，集群的组播地址是 01-80-C2-00-00-0A。

     建立集群前，需要先设置集群的组播 MAC 地址或者使用默认的组播 MAC 地址，然后再建立集群。 如果默认的组播 MAC 地址已被网络中的其他业务所使用或者为了增强网络的安全性，此时可以在允许范围内，重新设置集群的组播 MAC 地址。 集群一旦建立后，那么就不能再修改集群的组播 MAC 地址。 同一个集群内的设备，需要配置相同的集群组播地址。

- 配置集群接口加入 VLAN 方式

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **port-tagged vlan**，配置集群通信接口以 trunk 方式加入管理 VLAN。

- 配置集群公用服务器和主机

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。

版权所有 © 华为技术有限公司

3. 执行命令 **ftp-server** *ip-address*，配置集群公用的 FTP 服务器。

   说明

   集群内的成员交换机可以采用 2 种方式与集群外的 FTP 服务器互通。

   - 非 NAT（Network Address Translation）方式：这种方式下需要保证集群内的成员交换机与集群外的 FTP 服务器之间有可达的路由。
   - NAT（Network Address Translation）方式：这种方式下需要在命令交换机上的 Cluster 视图下同时配置命令 **cluster-ftp-nat enable**，来使能命令交换机的 FTP NAT 功能。集群使用的 NAT 规则由命令交换机自动配置，成员交换机会自动获取 NAT 映射端口。

   缺省情况下，命令交换机的 FTP NAT 功能处于禁止状态。即集群内的成员交换机采用非 NAT 方式与集群外的 FTP 服务器互通。

   集群公用的 FTP 服务器配置成功后，集群内的成员交换机可以使用命令 **cluster-ftp** 访问集群外的 FTP 服务器。

4. 执行命令 **sftp-server** *ip-address*，配置集群公用的 SFTP 服务器。
5. 执行命令 **snmp-host** *ip-address*，配置集群公用的 SNMP 主机。

   说明

   集群内的成员交换机可以采用 2 种方式与集群外的 SNMP 互通。

   - 非 NAT（Network Address Translation）方式：这种方式下需要保证集群内的成员交换机与 SNMP 之间有可达的路由。
   - NAT（Network Address Translation）方式：这种方式下需要在命令交换机上的 Cluster 视图下同时配置命令 **cluster-snmp-nat enable**，来使能命令交换机的 SNMP NAT 功能。集群使用的 NAT 规则由命令交换机自动配置，成员交换机会自动获取 NAT 映射端口。

   缺省情况下，命令交换机的 SNMP NAT 功能处于使能状态。即集群内的成员交换机采用 NAT 方式与集群外的 SNMP 互通。

6. 执行命令 **logging-host** *ip-address*，配置集群公用的日志主机。

   成员交换机将通过命令交换机来访问通过步骤 3 ～ 6 配置的服务器和主机。

   步骤 3 ～ 6 是可选配置，在执行时没有先后顺序。

   缺省情况下，集群没有公用服务器和主机。

----结束

利用 HGMP 管理集群中的设备

可以使用如下命令管理 HGMP 集群中的设备：配置批量下发、批量重启、即插即用，添加增量配置，同步配置文件，配置安全特性。

操作步骤

- 配置批量下发

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. （可选）执行命令 **cluster-plug-play ip** *ftp-ip-address* **username** *user-name* **password** *password* [**path-separator** *pathseparator*]，配置默认的 FTP 登录信息

     配置该命令后，批量下发会默认使用该配置中的信息。

版权所有 © 华为技术有限公司

4. （可选）执行命令 **cluster-member ftp-timeout** *time*，配置成员交换机通过 FTP 下载配置文件、版本文件或者补丁文件的超时时间。
5. 执行命令 **cluster-member** [**group-by** { **device-type** *device-type* | **ip** {*ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }] **get** { **configuration-file** | **system-software** | **patch** | **paf** | **license** } *file-name* [**ip** *ftp-ip-address* **username** *user-name* **password** *password*] [**path-separator** *pathseparator*]，执行批量下发。
   - 使用 **group-by** 可在批量下发时根据不同类型筛选出指定的成员交换机组。
   - 如果没有执行步骤 3，则命令中必须输入 IP 地址、用户名和密码。
   - 如果执行了步骤 3，在命令中可以不输入 IP 地址、用户名和密码，命令会默认使用步骤 3 配置的 IP 地址、用户名和密码。
   - 批量下发使用的 IP 地址为集群内部的 IP 地址。

- 配置批量重启

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. （可选）执行命令 **cluster-member reboot-timeout** *time*，配置成员交换机重启的超时时间。
  4. 执行命令 **cluster-member reboot** [**group-by** { **device-type** *device-type* | **ip** {*ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }]，执行批量重启。

     执行批量重启时不会保存设备当前配置。

- 配置即插即用

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. （可选）执行命令 **cluster-plug-play ip** *ftp-ip-address* **username** *user-name* **password** *password* [**path-separator** *pathseparator*]，配置默认的 FTP 登录信息。
  4. 执行命令 **cluster-plug-play enable**，配置即插即用。
     - 使用 **cluster-plug-play enable** 命令前，配置命令交换机接口的管理 VLAN（此接口用于直连候选交换机），需要使用 **port trunk allow-pass vlan** 命令，而不能使用 **port default vlan** 命令。
     - 步骤 3 仅用于替换设备的场景，新设备自动下载旧设备的配置文件。前提是 FTP Server 上有旧设备的配置文件，并且新设备和旧设备的物理拓扑以及设备类型相同。

- 配置与友商互通

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **cluster-packet-extend enable**，配置与友商互通。

版权所有 © 华为技术有限公司

- 使用 **cluster-packet-extend enable** 命令前，配置命令交换机接口的管理VLAN（此接口用于直连候选交换机），需要使用 **port trunk allow-pass vlan** 命令，而不能使用 **port default vlan** 命令。

- 添加增量配置

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **increment**，进入集群增量配置视图。
  4. 执行命令 **increment-command** [**command-number** *command-number*] **command-text** *command-text*，编辑命令列表。
  5. 执行命令 **increment-run** [**group-by** { **device-type** *device-type* | **ip** { *ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }]，确认命令下发到指定成员设备。
     - 执行增量配置只保存最后一次执行结果。
     - 成员组选方式可以是根据成员 ID，设备类型，IP 地址或者所有。
     - 编辑命令列表时，如果使用已存在的命令编号，那么会覆盖此命令编号对应的命令。
     - 可以通过 **undo increment-command** { **command-number** *command-number* | **all** }命令，删除已存在的增量配置命令。
     - 可以通过 **display increment-command** 命令，查看当前已编辑的增量配置命令列表。

- 同步配置文件

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **increment-config synchronization** [**group-by** { **device-type** *device-type* | **ip** {*ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }]，把成员交换机的配置文件同步到FTP 服务器。
     - 成员组选方式可以是根据成员 ID，设备类型，IP 地址或者所有。
     - 必须集群使能后才能执行本命令。

- 配置安全特性

  请在命令交换机上执行下面的命令。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **cluster**，进入集群视图。
  3. 执行命令 **cluster-member unrelated-port** [**group-by** { **device-type** *device-type* | **ip** {*ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }] { **ndp** | **ntdp** }，关闭不相关端口 NDP/NTDP 协议状态。
     - 执行此命令只保存最后一次执行的结果。
     - 成员组选方式可以是根据成员 ID，设备类型，IP 地址或者所有。

版权所有 © 华为技术有限公司

- 必须集群使能后才能执行本命令。

----结束

检查配置结果

前提条件

已经完成 HGMP 的高级功能的所有配置。

操作步骤

- 使用命令 **display cluster-increment-result**，查看下发增量配置的结果。
- 使用命令 **display cluster-license**，查看集群 License 的内容。
- 使用命令 **display cluster-topology-info**，查看集群拓扑信息。
- 使用命令 **display increment-command**，查看增量配置信息。
- 使用命令 **display increment-synchronization-result**，查看成员交换机的配置文件同步到 FTP 服务器的结果。
- 使用命令 **display member-getfile-state**，查看成员交换机获取配置文件、版本文件或者补丁文件的状态。
- 使用命令 **display member-interface-state { ndp | ntdp }**，查看成员交换机不相关端口 NDP 或 NTDP 的状态。
- 使用命令 **display member-reboot-state**，查看成员交换机重启的状态。
- 使用命令 **display member-save-state**，查看成员交换机保存当前配置的状态。
- 使用命令 **display synchronization-result**，查看成员交换机同步配置文件的结果。

----结束

任务示例

如果成员交换机下发增量配置成功，执行命令 **display cluster-increment-result**，可以看到结果为“success”。

```
<HUAWEI_0.Quidway> display cluster-increment-result
The result of member switchs executing increment commands:
--------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      Result    CommandId
--------------------------------------------------------------------------------
2    AC6605               0003-0003-0003 10.0.0.3       success   -

3    AC6605               0004-0004-0004 10.0.0.4       success   -
```

执行命令 **display cluster-license**，可以查看集群 License 的内容，包括命令交换机最多可以管理成员交换机的数量以及成员交换机最多可以级联的层数。

```
<Quidway> display cluster-license
The max numbers and hops of manage member switch:
-------------------------------------------------------------
Max numbers of manage member switch: 255
Max hops of manage member switch   : 16
```

执行命令 **display cluster-topology-info**，可以查看集群拓扑信息，包括正常链路、候选链路和问题链路。

```
<Quidway> display cluster-topology-info
<-->:normal device         <++>:candidate device         <??>:lost device
```


版权所有 © 华为技术有限公司

```
-------------------------------------------------------------------------
Total topology node number is 5.
[HUAWEI_0.Administrator: Root-00e0-ad14-c600]
|-(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/1)[HUAWEI_3.Member-3: 00e0-da1c-4c00]
| |-(GigabitEthernet0/0/2)<-->(GigabitEthernet0/0/1)[HUAWEI_2.Member-2: 00e0-875b-8f00]
| | |-(GigabitEthernet0/0/2)<-->(GigabitEthernet0/0/1)[HUAWEI_1.Member-1: 00e0-0f68-6f00]
|-(GigabitEthernet0/0/2)<-->(GigabitEthernet0/0/1)[HUAWEI_4.Member-4: 00e0-9f7e-0b00]
```

执行命令 **display increment-command**，可以查看集群增量配置信息，包括增量配置的编号和内容。

```
<Quidway> display increment-command
The content of increment commands:
-------------------------------------------------------------------------------
SN        Content
-------------------------------------------------------------------------------
10        vlan batch 10 to 20
20        ip route-static 2.0.0.0 8 10.0.0.1
```

如果成员交换机的配置文件同步到 FTP 服务器成功，执行命令 **display increment-synchronization-result**，可以看到结果为“success”。

```
<Quidway> display increment-synchronization-result
The result of member switchs' synchronization:
-------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      result
-------------------------------------------------------------------------------
1    AC6605               0002-0002-0002 10.0.0.2       success
2    AC6605               0003-0003-0003 10.0.0.3       success
3    AC6605               0004-0004-0004 10.0.0.4       success
```

如果成员交换机获取配置文件、版本文件或者补丁文件成功，执行命令 **display member-getfile-state**，可以看到结果为“success”。

```
<Quidway> display member-getfile-state
The status of member switchs getting file:
-------------------------------------------------------------------------
SN    Device              MacAddress        IPAddress        Result
-------------------------------------------------------------------------
2     AC6605               0002-0002-0002    10.0.0.2         success
3     AC6605               0003-0003-0003    10.0.0.3         success
```

成员交换机上不需要运行 NDP 和 NTDP 协议的接口，如果使能/禁止 NDP 和 NTDP 功能成功，执行命令 **display member-interface-state**，可以看到结果为“success”。

```
<HUAWEI_0.Quidway> display member-interface-state ndp
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         AC6605          0004-0004-0004      10.0.0.4            success
2         AC6605          0003-0003-0003      10.0.0.3            success
1         AC6605          0002-0002-0002      10.0.0.2            success
<HUAWEI_0.Quidway> display member-interface-state ntdp
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         AC6605          0004-0004-0004      10.0.0.4            success
2         AC6605          0003-0003-0003      10.0.0.3            success
1         AC6605          0002-0002-0002      10.0.0.2            success
```

如果成员交换机重启成功，执行命令 **display member-reboot-state**，可以看到结果为“success”。

```
<Quidway> display member-reboot-state
The result of member switchs rebooting:
-------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
SN    Device              MacAddress        IPAddress        Result
------------------------------------------------------------------------------
1     AC6605               0002-0002-0002    10.0.0.2         success
2     AC6605               0003-0003-0003    10.0.0.3         success
------------------------------------------------------------------------------
```

如果成员交换机保存当前配置成功，执行命令 **display member-save-state**，可以看到结果为“success”。

```
<Quidway> display member-save-state
The result of member switchs saving:
------------------------------------------------------------------------------
SN    Device              MacAddress        IPAddress        Result
------------------------------------------------------------------------------
1     AC6605               0002-0002-0002    10.0.0.2         success
2     AC6605               0003-0003-0003    10.0.0.3         success
------------------------------------------------------------------------------
```

如果成员交换机同步配置文件到 FTP 服务器成功，执行命令 **display synchronization-result**，可以看到结果为“success”。

```
<Quidway> display synchronization-result
The result of member switchs' synchronization:
------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      result
------------------------------------------------------------------------------
1    AC6605               0002-0002-0002 10.0.0.2       success
2    AC6605               0003-0003-0003 10.0.0.3       success
3    AC6605               0004-0004-0004 10.0.0.4       success
```

10.3.5 维护 HGMP

介绍如何清除 NDP 统计信息和监控 HGMP 集群的运行状况。

清除 NDP 统计信息

通过命令 reset ndp statistics 清除 NDP 的统计信息。

背景信息



注意

清除 NDP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除 NDP 的统计信息后，请在用户视图下执行 **reset ndp statistics** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>] 命令。

----结束

监控 HGMP 集群的运行状况

通过 display 命令监控 HGMP 的运行情况。

版权所有 © 华为技术有限公司

前提条件

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 HGMP 的运行状况。

操作步骤

- 使用命令 **display ndp** 查看系统 NDP 配置信息。
- 使用命令 **display ntdp** 显示全局 NTDP 信息。
- 使用命令 **display cluster** 查看本设备所属 HGMP 集群的信息。
- 使用命令 **display ntdp device-list** [**verbose**]查看通过 NTDP 收集到的设备信息。
- 使用命令 **display cluster-topology-info** 查看集群拓扑信息。
- 使用命令 **display cluster candidates** [**mac-address** *mac-address* | **verbose**]查看候选交换机的信息。

----结束

调试 HGMP

在出现 NDP、NTDP 或者集群运行故障时，请在用户视图下执行下面的 debugging 命令 对 NDP、NTDP 或者集群进行调试，查看调试信息，定位故障并分析故障原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 NDP、NTDP 或者集群运行故障时，请在用户视图下执行下面的 **debugging** 命令对 NDP、NTDP 或者集群进行调试，查看调试信息，定位故障并分析故障原因。

有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 Debugging 参考》。

操作步骤

- 使用命令 **debugging ndp packet** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]，打开 NDP 调试开关。
- 使用命令 **debugging ntdp** {**all** |**data** |**error** |**message** |**packet** [**verbose**] }，打开 NTDP 调试开关。
- 使用命令 **debugging cluster** { **all** | **event** | **handshake** | **member** | **mrc** | **nat** | **packet** | **state** }或者命令 **debugging cluster** { **packet** | **handshake** | **mrc** } [**verbose**] ，打开集群调试开关。

----结束

10.3.6 配置举例

介绍 HGMP 的各种组网举例。

版权所有 © 华为技术有限公司

配置 HGMP 集群基本功能示例

组网需求

如图 10-18 所示，用户通过二层设备建立一个二层网络。本网络内的二层设备较多，不便于到现场进行维护和管理。并且，为避免浪费大量的公网 IP 地址，则不能给本网络内的每台二层设备配置一个公网 IP 地址。

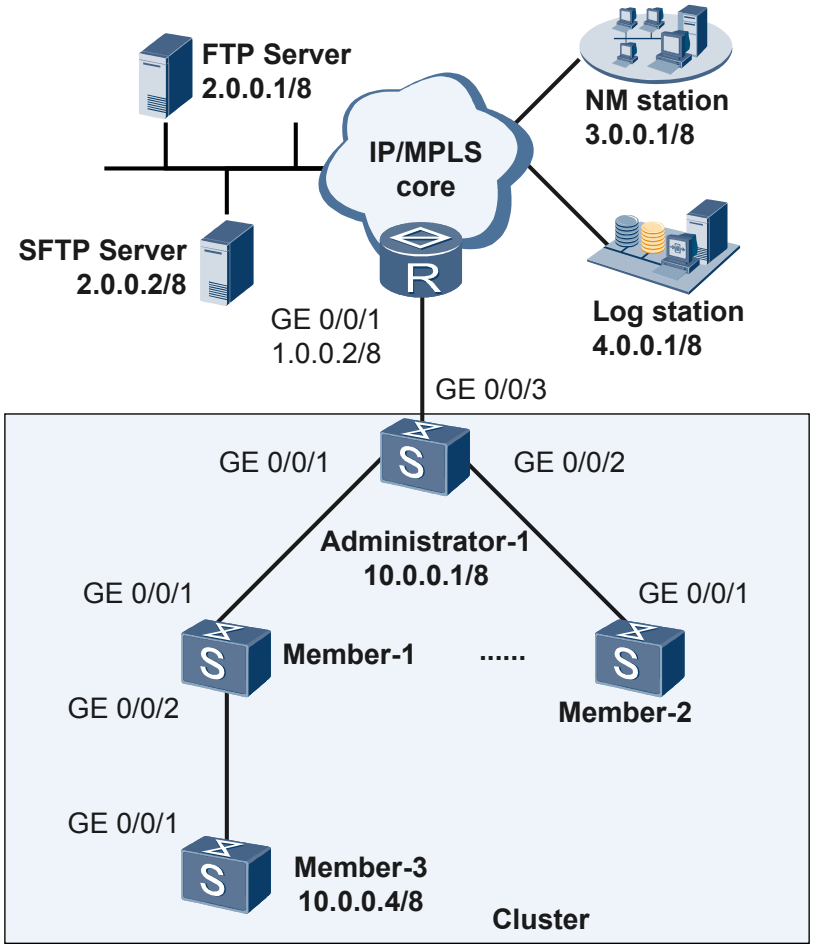
因此，为了有效的管理这个二层网络，可以将这个二层网络创建为一个集群，通过 HGMP 进行管理。

在本例中，从网络结构来说，Administrator-1 是距离管理员最近的一台设备，因此，将这台设备选为命令交换机。

说明

为方便描述，本例只选取了这个二层网络中的 4 台设备进行描述。

图 10-18 配置 HGMP 集群基本功能的组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 HGMP 集群基本功能：

1. 在所有的设备上创建管理 VLAN，并使能 NDP 和 NTDP，保证各台设备能够通过 NTDP 发现本网络的拓扑结构。
2. 选取命令交换机，并在此设备上创建集群“HUAWEI”。
3. 将本二层网络内所有支持 HGMP 的设备都加入这个集群。
4. 指定 VLANIF10 接口的 IP 地址，以便于集群内成员交换机与集群外设备的通信。
5. 配置集群公用的服务器和主机。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- 各台设备的 MAC 地址见**图 10-18**。
- 各台服务器和主机的 IP 地址见**图 10-18**。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

```
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                      AC6605
 0003-0003-0003  1                      AC6605
 0002-0002-0002  1                      AC6605
 0001-0001-0001  0                      AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
```


版权所有 © 华为技术有限公司

```
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002  AC6605
Member-2                      1     0003-0003-0003  AC6605
Member-3                      2     0004-0004-0004  AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```


版权所有 © 华为技术有限公司

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
```


版权所有 © 华为技术有限公司

```
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
```


版权所有 © 华为技术有限公司

```
return
```

配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）

组网需求

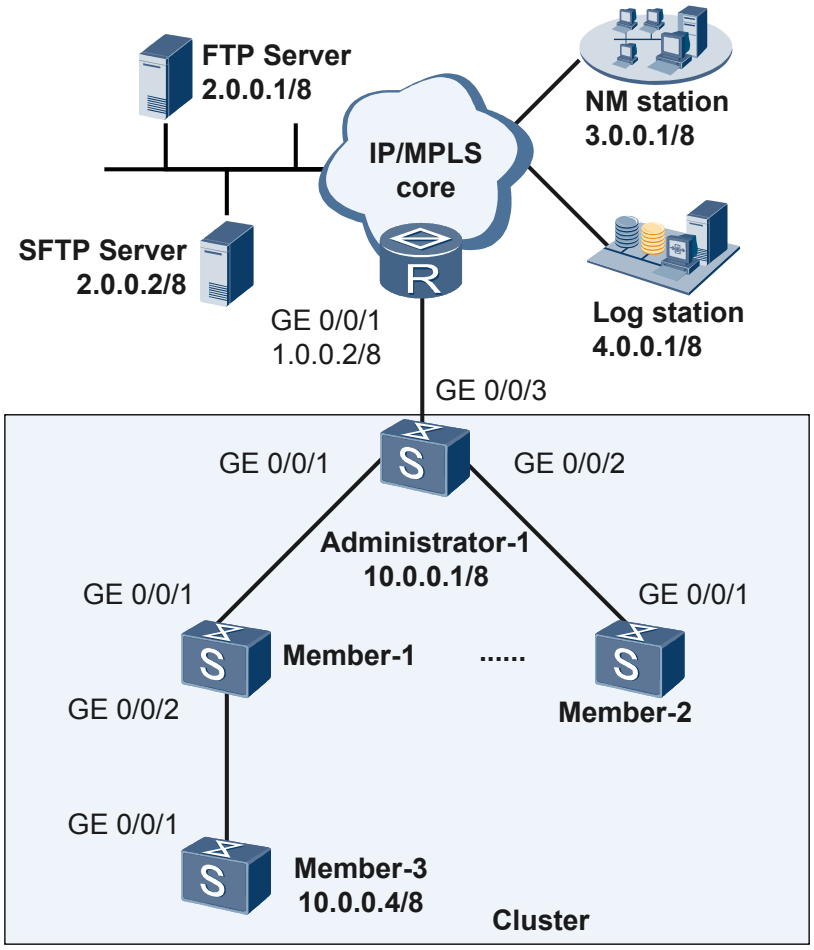
如图 10-19 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-1 的成员编号是 1，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要向 Member-1、Member-2 和 Member-3 上传文件，或从它们下载文件。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

说明

本例中采用 NAT 方式，分别以集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8），和集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）为例进行说明。

图 10-19 配置 HGMP 集群内外设备互通（NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通（NAT 方式）的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建和配置集群基本功能。
2. 对于集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8）：
   在成员交换机上执行 **cluster-ftp** 命令与集群公用的 FTP 服务器建立连接。
3. 对于集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）：
   - 计算成员交换机 FTP 协议所使用的集群保留接口号。
   - 在 PC 上通过 FTP 客户端与成员交换机建立 FTP 连接。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，配置为集群内的 FTP 服务器。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
```


版权所有 © 华为技术有限公司

```
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                      AC6605
 0003-0003-0003  1                      AC6605
 0002-0002-0002  1                      AC6605
 0001-0001-0001  0                      AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
```


版权所有 © 华为技术有限公司

```
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   AC6605
Member-2                      1     0003-0003-0003   AC6605
Member-3                      2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```


版权所有 © 华为技术有限公司

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
```


版权所有 © 华为技术有限公司

```
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 检查配置结果

- 成员交换机通过 NAT 方式访问 FTP 服务器。

```
<HUAWEI_3.Member-3> cluster-ftp
Trying 10.0.0.1 ...
Press CTRL+K to abort
Connected to 10.0.0.1.
220 FTP service ready.
User(10.0.0.1:(none)):hgmp
331 Password required for hgmp.
Enter password:
230 User logged in.
[ftp]
```

- 集群外设备通过 NAT 方式访问集群内 FTP 服务器。

  # 在对应的成员交换机（Member-2）上，配置 FTP 服务器。具体配置过程略，详见配置文件。

  # 计算成员交换机 FTP 协议所使用的集群保留端口号。

  Member-2 的成员编号是 2，根据“集群保留端口号的计算公式（集群保留接口号=接口号基数+成员编号*2）”，计算出 Member-2 开启 FTP 服务器时，所使用的集群保留端口号是：53248+2*2=53252。

  # 在 PC 上执行 FTP 客户端程序，通过 NAT 方式与 Member-2 建立 FTP 连接。

  说明

  NAT 方式下，集群外设备访问集群内 FTP 服务器。FTP 服务器的地址为命令交换机的管理 VLANIF 接口地址，端口号是集群保留端口号，而不是 FTP 服务通常的 21 端口。

```
ftp> open 1.0.0.1 53252
Connected to 1.0.0.1.
220 FTP service ready.
User (1.0.0.1:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
```


版权所有 © 华为技术有限公司

```
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
```


版权所有 © 华为技术有限公司

```
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）

组网需求

如图 10-20 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

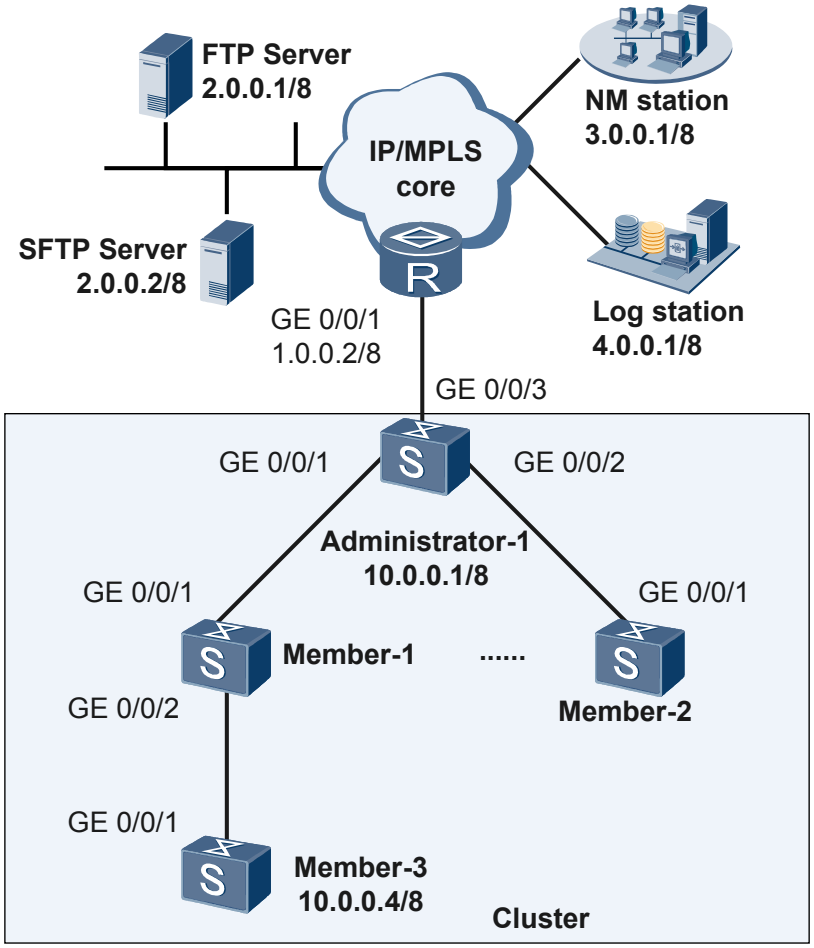
现在需要向 Member-1、Member-2 和 Member-3 上传文件，或从它们下载文件。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

说明

本例中采用非 NAT 方式，分别以集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8），和集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）为例进行说明。

版权所有 © 华为技术有限公司

图 10-20 配置 HGMP 集群内外设备互通（非 NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建和配置集群基本功能。
2. 取消命令交换机的 FTP NAT 功能（设备默认没有使能）。

   说明

   集群 NAT 相关配置，必须在命令交换机上进行。
3. 在命令交换机和成员交换机上分别配置路由，使 FTP 服务器与成员交换机之间存在可达的路由。
4. 对于集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8）：
   - 在成员交换机上执行 **ftp** 命令与集群公用的 FTP 服务器建立连接。
5. 对于集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）：

版权所有 © 华为技术有限公司

- 在 PC 上通过 FTP 客户端与成员交换机建立 FTP 连接。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，配置为集群内的 FTP 服务器。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
```


版权所有 © 华为技术有限公司

```
      Port Duplex : FULL
      Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : GigabitEthernet0/0/1
      Software Version: Version 5.70 V100R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
```


版权所有 © 华为技术有限公司

```
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
```


版权所有 © 华为技术有限公司

```
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   AC6605
Member-2                      1     0003-0003-0003   AC6605
Member-3                      2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```


版权所有 © 华为技术有限公司

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置成员交换机的路由，使成员交换机与 FTP 服务器之间存在可达的路由

配置成员交换机 1。

```
[HUAWEI_1.Member-1] ip route-static 2.0.0.0 8 10.0.0.1
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] ip route-static 2.0.0.0 8 10.0.0.1
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] ip route-static 2.0.0.0 8 10.0.0.1
```

说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见**配置 HGMP 集群增量配置功能示例**。

步骤 10 检查配置结果

- 成员交换机通过非 NAT 方式访问 FTP 服务器。

```
< HUAWEI_3.Member-3> ftp 2.0.0.1
Trying 2.0.0.1 ...
Press CTRL+K to abort
Connected to 2.0.0.1.
220 FTP service ready.
User(2.0.0.1:(none)):hgmp
331 Password required for hgmp.
Enter password:
230 User logged in.
[ftp]
```

- 集群外设备通过非 NAT 方式访问集群内 FTP 服务器。

  # 在对应的成员交换机（Member-2）上，配置 FTP 服务器。具体配置过程略，详见配置文件。

  # 在 PC 上执行 FTP 客户端程序，通过非 NAT 方式与 Member-2 建立 FTP 连接。

  说明

  非 NAT 方式下，集群外设备访问集群内 FTP 服务器。FTP 服务器的地址为成员交换机的管理 VLANIF 接口地址，端口号是 FTP 服务通常的 21 端口。

```
ftp> open 10.0.0.2
Connected to 10.0.0.2
220 FTP service ready.
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
User (10.0.0.2:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
```


版权所有 © 华为技术有限公司

```
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
```


版权所有 © 华为技术有限公司

```
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

配置 HGMP 集群内外设备 SNMP 互通示例（NAT 方式）

组网需求

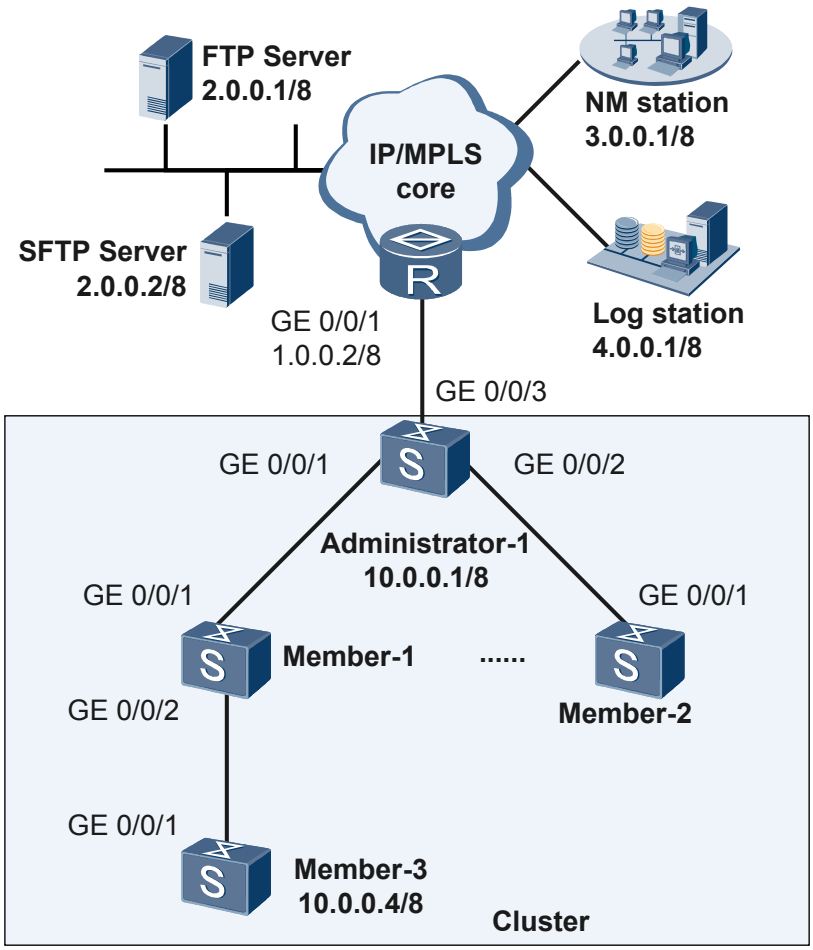
如图 10-21 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要 Member-1、Member-2 和 Member-3 向 SNMP 主机发送信息。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

说明

本例中采用 NAT 方式，以集群中的成员交换机 Member-3 访问集群外的 SNMP 主机（3.0.0.1/8）为例进行说明。

图 10-21 配置 HGMP 集群内外 SNMP 互通（NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 HGMP 集群内外设备 SNMP 互通（NAT 方式）的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建和配置集群基本功能。
2. 使能命令交换机的 SNMP NAT 功能（设备默认是使能的）。

   说明

   集群 NAT 相关配置，必须在命令交换机上进行。
3. 配置 SNMP 主机地址。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- SNMP 主机地址是 3.0.0.1/8。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 SNMP 主机之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                      AC6605
 0003-0003-0003  1                      AC6605
 0002-0002-0002  1                      AC6605
 0001-0001-0001  0                      AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
```


版权所有 © 华为技术有限公司

```
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   AC6605
Member-2                      1     0003-0003-0003   AC6605
Member-3                      2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```


版权所有 © 华为技术有限公司

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
```


版权所有 © 华为技术有限公司

```
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
```


版权所有 © 华为技术有限公司

```
#
return
```

配置 HGMP 集群内外设备 SNMP 互通示例（非 NAT 方式）

组网需求

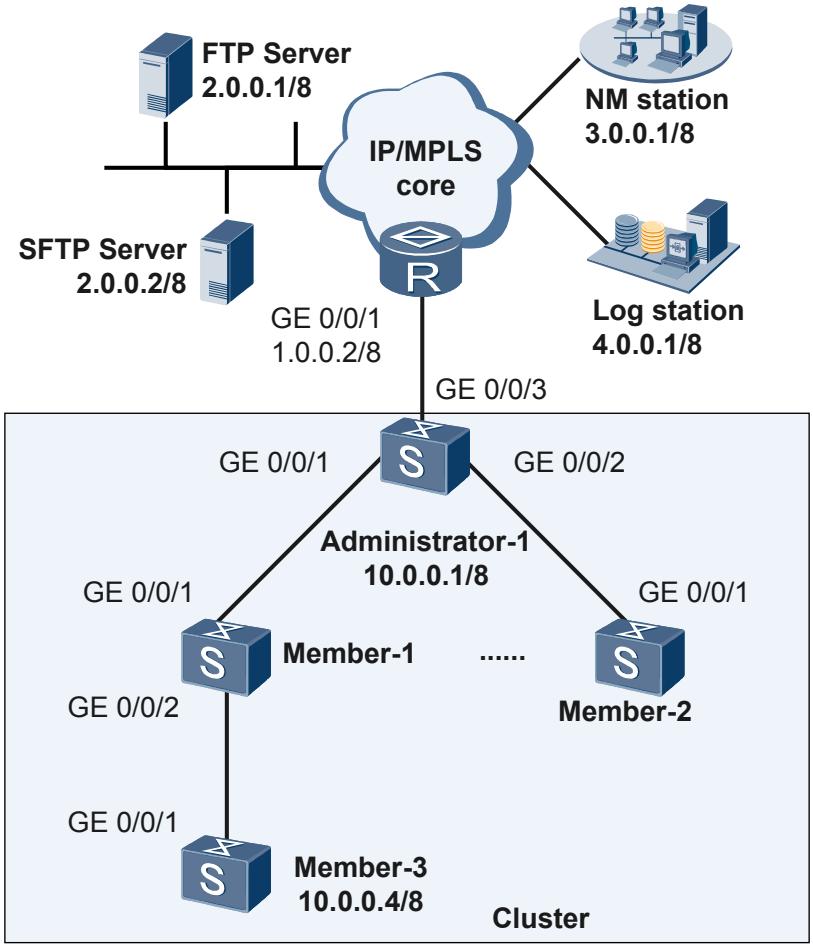
如图 10-22 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要 Member-1、Member-2 和 Member-3 向 SNMP 主机发送信息。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

说明

本例中采用非 NAT 方式，以集群中的成员交换机 Member-3 访问集群外的 SNMP 主机（3.0.0.1/8）为例进行说明。

图 10-22 配置 HGMP 集群内外 SNMP 互通（非 NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

版权所有 © 华为技术有限公司

配置思路

采用如下的思路配置 HGMP 集群内外设备 SNMP 互通的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建和配置集群基本功能。
2. 去使能命令交换机的 SNMP NAT 功能（设备默认是使能的）。

   说明

   集群 NAT 相关配置，必须在命令交换机上进行。
3. 在命令交换机和成员交换机上分别配置路由，使 SNMP 主机与成员交换机之间存在可达的路由。
4. 配置 SNMP 主机地址。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- SNMP 主机地址是 3.0.0.1/8。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
```


版权所有 © 华为技术有限公司

```
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
```


版权所有 © 华为技术有限公司

```
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

版权所有 © 华为技术有限公司

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   AC6605
Member-2                      1     0003-0003-0003   AC6605
Member-3                      2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
0    AC6605                  0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                  0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                  0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                  0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
```


版权所有 © 华为技术有限公司

```
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 取消命令交换机的 SNMP NAT 功能。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-snmp-nat enable
```

步骤 11 配置成员交换机的路由，使成员交换机与 SNMP 主机之间存在可达的路由。

配置成员交换机 1。

```
[HUAWEI_1.Member-1] ip route-static 3.0.0.0 8 10.0.0.1
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] ip route-static 3.0.0.0 8 10.0.0.1
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] ip route-static 3.0.0.0 8 10.0.0.1
```

说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见**配置 HGMP 集群增量配置功能示例**。

步骤 12 配置成员交换机的 SNMP 代理功能。

配置成员交换机 1。

```
[HUAWEI_1.Member-1] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
```

说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见**配置 HGMP 集群增量配置功能示例**。

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
```


版权所有 © 华为技术有限公司

```
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 undo cluster-snmp-nat enable
       cluster-ftp-nat enable
       ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
```


版权所有 © 华为技术有限公司

```
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return
```


版权所有 © 华为技术有限公司

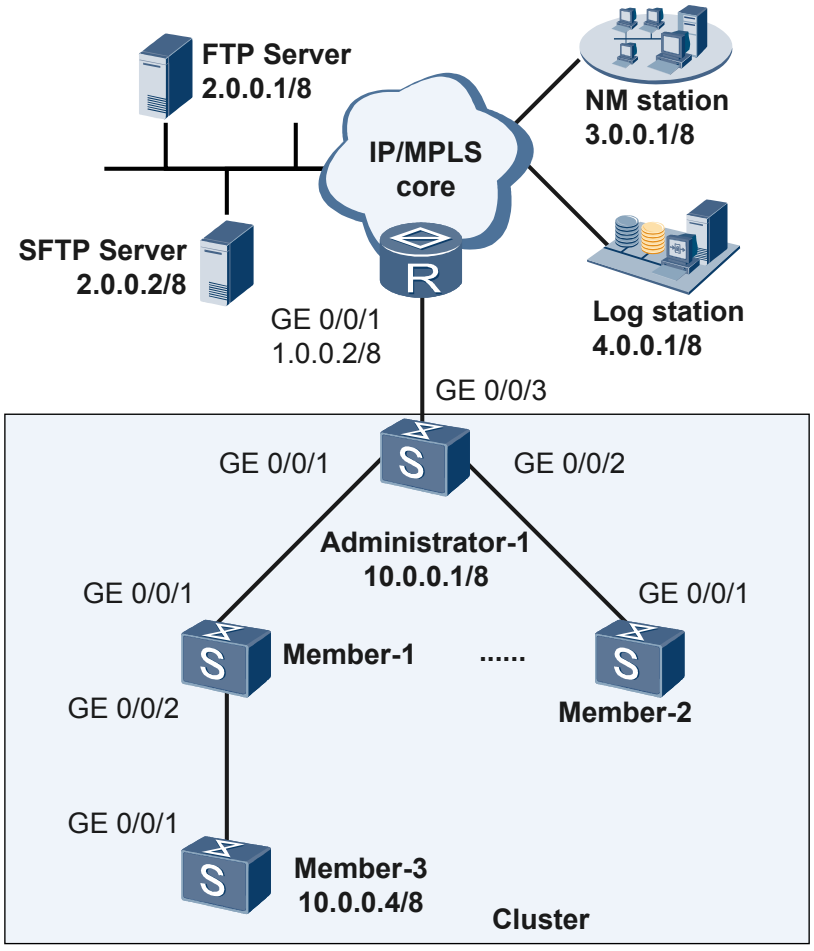
配置 HGMP 集群批量下发功能示例

组网需求

如图 10-23 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要控制成员交换机 Member-2、Member-3 从 FTP 服务器上批量下发配置文件。

图 10-23 配置 HGMP 集群批量下发功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通（NAT 方式）的基本功能：

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建集群。

版权所有 © 华为技术有限公司

2. **配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）**。

   说明

   - 配置 HGMP 集群内外设备 FTP 互通，可以采用 NAT 方式也可以采用非 NAT 方式。本例中采用 NAT 方式进行举例说明。
   - 如果不需要通过访问集群外部的 FTP 服务器来批量下发系统软件、补丁或者配置文件，那么此步骤可省略。

3. 在命令交换机上配置批量下发。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLAN 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
```


版权所有 © 华为技术有限公司

```
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

版权所有 © 华为技术有限公司

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

版权所有 © 华为技术有限公司

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
```


版权所有 © 华为技术有限公司

```
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join     : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002  AC6605
Member-2                      1     0003-0003-0003  AC6605
Member-3                      2     0004-0004-0004  AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

版权所有 © 华为技术有限公司

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```


版权所有 © 华为技术有限公司

步骤 10 执行批量下发

在命令交换机上执行批量下发命令，成员交换机通过 NAT 方式从 FTP 服务器（2.0.0.1）下载配置文件，并自动设置为下次启动的配置文件。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plug-play ip 2.0.0.1 username user1 password 123
[HUAWEI_0.Administrator-1-cluster] cluster-member group-by member-number 2 to 3 get configuration-file vrpcfg-hgmp.zip
```

步骤 11 检查配置结果

在命令交换机上执行 **display member-getfile-stat** 命令，查看成员交换机获取配置文件、系统软件或者补丁文件的状态。可以看到结果是“success”。

```
[HUAWEI_0.Administrator-1] display member-getfile-stat
The status of member switchs getting file:
-------------------------------------------------------------------------
SN    Device              MacAddress        IPAddress        Result
-------------------------------------------------------------------------
2     AC6605              0003-0003-0003    10.0.0.3         success
3     AC6605              0004-0004-0004    10.0.0.4         success
```

在成员交换机上执行 **dir** 命令，可以看到成员交换机已经成功下载到了指定的配置文件。以 Member-2 为例。

```
<HUAWEI_2.Member-2> dir *.zip
Directory of flash:/
  Idx  Attr  Size(Byte)  Date        Time       FileName
   0   -rw-       1,491  Sep 03 2008 17:43:52   vrpcfg.zip
   1   -rw-         752  Aug 05 2008 15:04:36   vrpcfg-hgmp.zip
506,880 KB total (35,920 KB free)
```

在成员交换机上执行 **display startup** 命令，可以看到成员交换机下次启动的配置文件的名称已改变。以 Member-2 为例。

```
<HUAWEI_2.Member-2> display startup
MainBoard:
  Configured startup system software:        flash:/AC6605.cc
  Startup system software:                   flash:/AC6605.cc
  Next startup system software:              flash:/AC6605.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg-hgmp.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
```


版权所有 © 华为技术有限公司

```
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
```


版权所有 © 华为技术有限公司

```
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

配置 HGMP 集群批量重启功能示例

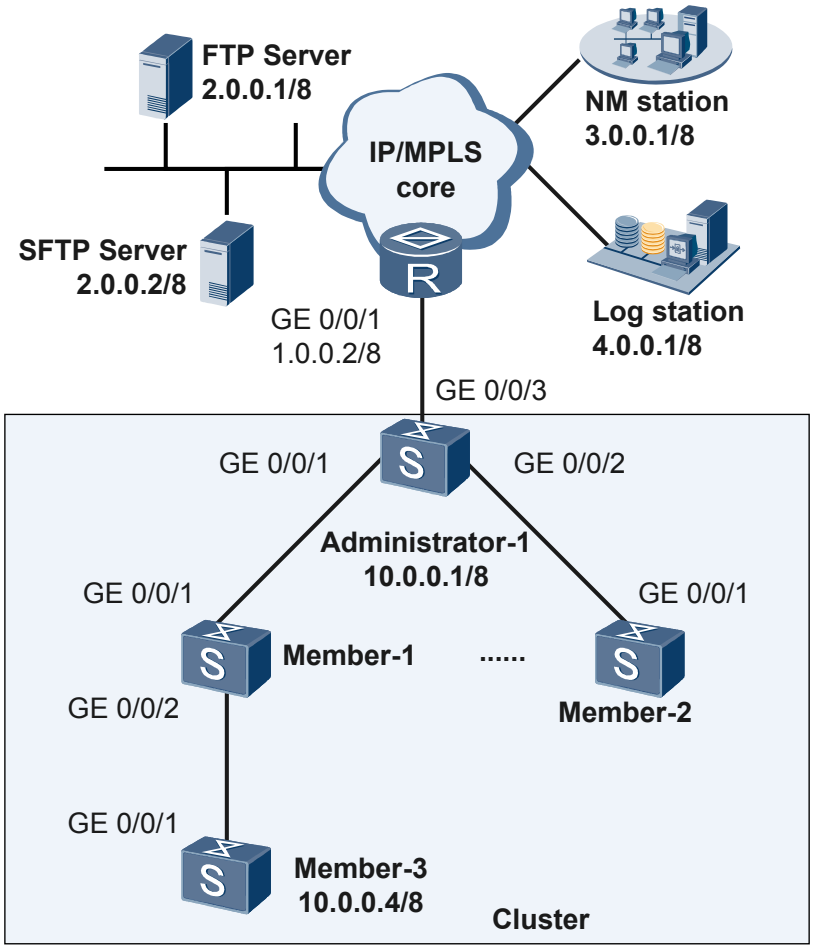
组网需求

如图 10-24 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要控制成员交换机 Member-2、Member-3 重启。

版权所有 © 华为技术有限公司

图 10-24 配置 HGMP 集群批量重启功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群批量重启的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建集群。
2. 在命令交换机上配置批量重启。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。

版权所有 © 华为技术有限公司

- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```


版权所有 © 华为技术有限公司

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

版权所有 © 华为技术有限公司

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
```


版权所有 © 华为技术有限公司

```
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   AC6605
Member-2                        1     0003-0003-0003   AC6605
Member-3                        2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
```


版权所有 © 华为技术有限公司

```
Input bandwidth utilization  : --
Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 执行批量重启

在命令交换机上执行批量重启命令，重新启动设备 Member-2 和 Member-3。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-member reboot group-by member-number 2 to 3
Info: This command will take members reboot.
Are you sure?[Y/N]y
```

步骤 11 检查配置结果

在成员交换机上执行 **display member-reboot-stat** 命令，查看成员交换机重启的状态。可以看到结果是“success”。此时指定的成员交换机已经重启。

```
[HUAWEI_2.Member-2] display member-reboot-stat
```


版权所有 © 华为技术有限公司

```
The result of member switchs rebooting:
-------------------------------------------------------------------------
SN    Device              MacAddress         IPAddress        Result
-------------------------------------------------------------------------
1     AC6605              0003-0003-0003     10.0.0.3         success
2     AC6605              0004-0004-0004     10.0.0.4         success
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
```


版权所有 © 华为技术有限公司

```
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
```


版权所有 © 华为技术有限公司

```
return
```

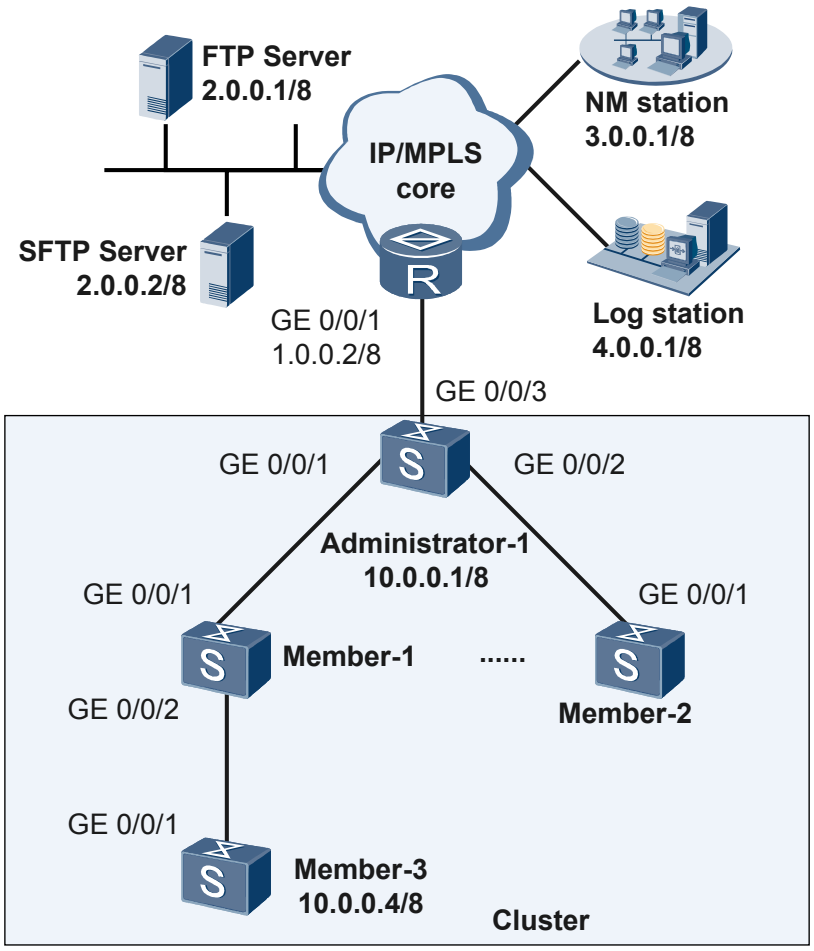
配置 HGMP 集群增量配置功能示例

组网需求

如图 10-25，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要在成员交换机 Member-2 和 Member-3 上创建 VLAN100 ～ VLAN200，并且配置下一跳地址为命令交换机的静态路由，此时可以使用 HGMP 集群增量配置功能。

图 10-25 配置 HGMP 集群增量配置功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群增量配置的基本功能：

版权所有 © 华为技术有限公司

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建集群。
2. 在命令交换机上编辑增量配置命令列表。
3. 给指定的成员交换机下发增量配置命令列表。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
```


版权所有 © 华为技术有限公司

```
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
```


版权所有 © 华为技术有限公司

```
      Port Name   : GigabitEthernet0/0/1
      Software Version: Version 5.70 V100R006C00
      Device Name : Member-1
      Port Duplex : FULL
      Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : GigabitEthernet0/0/1
      Software Version: Version 5.70 V100R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
```


版权所有 © 华为技术有限公司

```
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

版权所有 © 华为技术有限公司

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        AC6605
0003-0003-0003  1                        AC6605
0002-0002-0002  1                        AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   AC6605
Member-2                      1     0003-0003-0003   AC6605
Member-3                      2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
```


版权所有 © 华为技术有限公司

```
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 在命令交换机上编辑增量配置命令列表

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] increment
```


版权所有 © 华为技术有限公司

```
[HUAWEI_0.Administrator-1-cluster-increment] increment - command command-number 10 command-text vlan batch 100 to 200
[HUAWEI_0.Administrator-1-cluster-increment] increment - command command-number 20 command-text ip route-static 2.0.0.0 8 10.0.0.1
```

完成上述配置后，在命令交换机上执行 **display increment-command** 命令，可以查看增量配置命令列表。

```
[HUAWEI_0.Administrator-1] display increment-command
The content of increment commands:
-------------------------------------------------------------------------------
SN        Content
-------------------------------------------------------------------------------
10        vlan batch 100 to 200
20        ip route-static 2.0.0.0 8 10.0.0.1
```

步骤 11 下发增量配置命令列表

```
[HUAWEI_0.Administrator-1-cluster-increment] increment-run group-by member-number 2 to 3
```

步骤 12 检查配置结果

在成员交换机上执行 **display cluster-increment-result** 命令，查看给指定的成员交换机下发增量配置的结果。可以看到结果是“success”。

```
[HUAWEI_0.Administrator-1] display cluster-increment-result
The result of member switch executing increment commands:
-------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      Result    CommandId
-------------------------------------------------------------------------------
2    AC6605               0003-0003-0003 10.0.0.3       success   -

3    AC6605               0004-0004-0004 10.0.0.4       success   -
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
```


版权所有 © 华为技术有限公司

```
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
```


版权所有 © 华为技术有限公司

```
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

配置 HGMP 集群同步配置文件功能示例

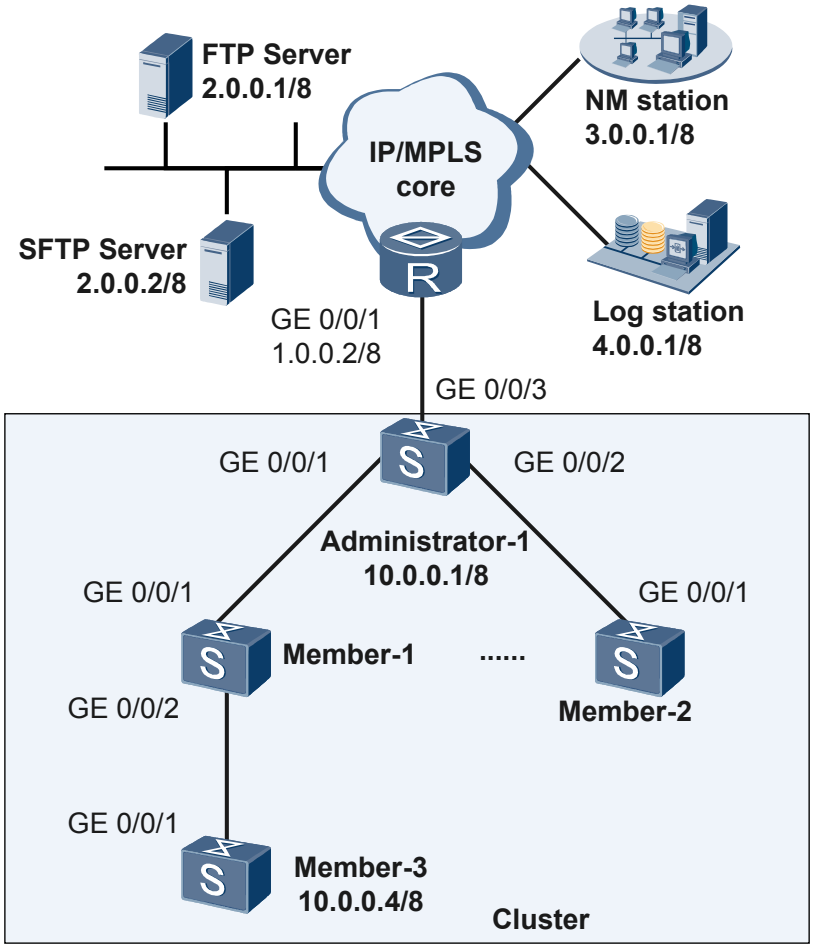
组网需求

如图 10-26，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要将所有成员交换机的配置文件同步到 FTP 服务器上，此时可以配置 HGMP 集群同步配置文件功能。

版权所有 © 华为技术有限公司

图 10-26 配置 HGMP 集群同步配置文件功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群同步配置文件的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建集群。
2. **配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）**。

   说明

   - 配置 HGMP 集群内外设备 FTP 互通，可以采用 NAT 方式也可以采用非 NAT 方式。本例中采用 NAT 方式进行举例说明。
   - 如果不需要通过访问集群外部的 FTP 服务器来完成 HGMP 集群同步配置文件功能，那么此步骤可省略。
3. 在命令交换机上执行同步配置命令。

版权所有 © 华为技术有限公司

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```


版权所有 © 华为技术有限公司

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
```


版权所有 © 华为技术有限公司

```
Port Name   : GigabitEthernet0/0/1
Software Version: Version 5.70 V100R006C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : AC6605
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
```


版权所有 © 华为技术有限公司

```
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
```


版权所有 © 华为技术有限公司

```
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   AC6605
Member-2                        1     0003-0003-0003   AC6605
Member-3                        2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
```


版权所有 © 华为技术有限公司

```
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 同步配置文件

在命令交换机上执行同步配置命令，成员交换机通过 NAT 方式同步配置文件到 FTP 服务器（2.0.0.1）上。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plug-play ip 2.0.0.1 username hgmp password hgmp
[HUAWEI_0.Administrator-1-cluster] increment-config synchronization
```

步骤 11 检查配置结果

版权所有 © 华为技术有限公司

完成上述配置后，在成员交换机上执行 **display increment-synchronization-result** 命令，查看成员交换机的配置文件同步到 FTP 服务器的结果。可以看到结果是“success”。

```
[HUAWEI_0.Administrator-1] display increment-synchronization-result
The result of member switchs' synchronization:
------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      result
------------------------------------------------------------------------------
1    AC6605               0002-0002-0002 10.0.0.2       success
2    AC6605               0003-0003-0003 10.0.0.3       success
3    AC6605               0004-0004-0004 10.0.0.4       success
```

在 FTP 服务器上可以看到以成员交换机 MAC 地址命名的配置文件，配置 HGMP 集群同步配置文件成功。

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

配置 HGMP 集群安全特性示例

组网需求

如图 10-27，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

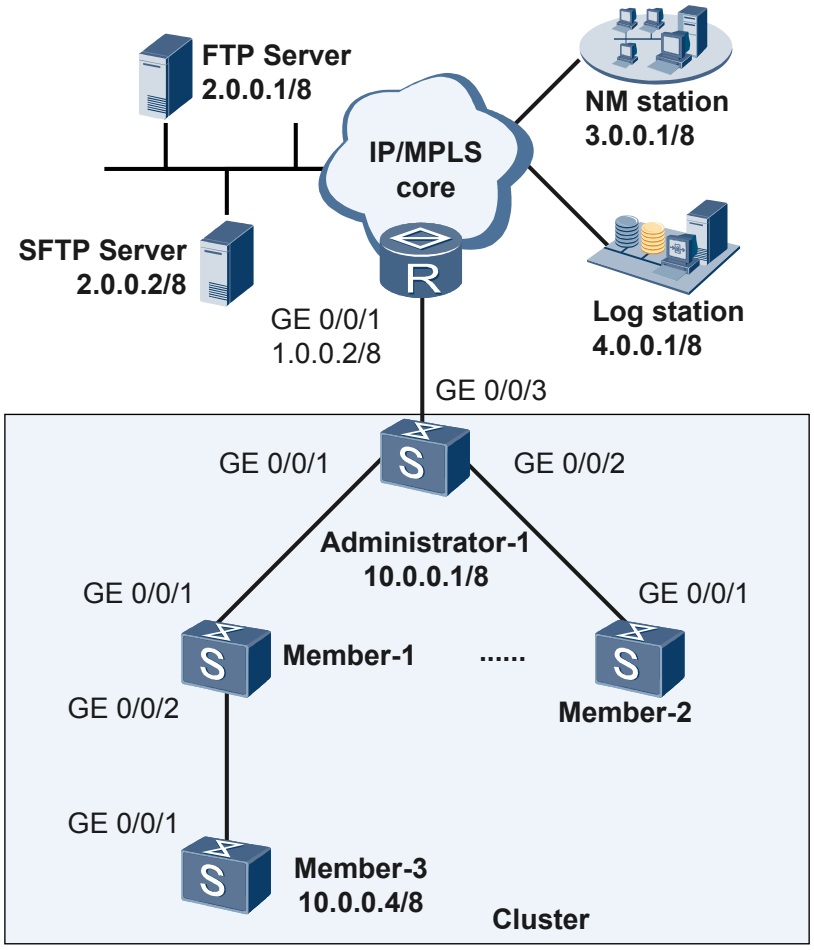
现在需要在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 和 NTDP 功能，以提高整个集群的安全性，此时可以配置 HGMP 集群安全特性。

说明

关闭成员交换机不相关端口的 NDP 或 NTDP 协议后，新的候选交换机接入成员交换机的不相关接口，新的候选交换机不能加入该集群。除非重新使能该成员交换机的不相关端口的 NDP 或 NTDP 协议。

版权所有 © 华为技术有限公司

图 10-27 配置 HGMP 集群安全特性的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群安全特性的基本功能：

1. 根据“**配置 HGMP 集群基本功能示例**”中的配置步骤创建集群。
2. 在命令交换机上运行关闭成员交换机不相关端口的 NDP 和 NTDP 协议的命令。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。

版权所有 © 华为技术有限公司

- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] port link-type trunk
[Administrator-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] port link-type trunk
[Administrator-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/2] quit
[Administrator-1] interface gigabitethernet 0/0/3
[Administrator-1-GigabitEthernet0/0/3] port link-type trunk
[Administrator-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-GigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] port link-type trunk
[Member-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] port link-type trunk
[Member-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-GigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] port link-type trunk
[Member-2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-GigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] port link-type trunk
[Member-3-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```


版权所有 © 华为技术有限公司

```
[Member-3-GigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ndp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ndp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ndp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ndp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ndp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ndp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 0/0/1 gigabitethernet 0/0/2
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : AC6605
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : AC6605
```

步骤 3 配置 NTDP

版权所有 © 华为技术有限公司

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 0/0/1
[Administrator-1-GigabitEthernet0/0/1] ntdp enable
[Administrator-1-GigabitEthernet0/0/1] quit
[Administrator-1] interface gigabitethernet 0/0/2
[Administrator-1-GigabitEthernet0/0/2] ntdp enable
[Administrator-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 0/0/1
[Member-1-GigabitEthernet0/0/1] ntdp enable
[Member-1-GigabitEthernet0/0/1] quit
[Member-1] interface gigabitethernet 0/0/2
[Member-1-GigabitEthernet0/0/2] ntdp enable
[Member-1-GigabitEthernet0/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 0/0/1
[Member-2-GigabitEthernet0/0/1] ntdp enable
[Member-2-GigabitEthernet0/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 0/0/1
[Member-3-GigabitEthernet0/0/1] ntdp enable
[Member-3-GigabitEthernet0/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
```


版权所有 © 华为技术有限公司

```
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------
 0004-0004-0004  2                        AC6605
 0003-0003-0003  1                        AC6605
 0002-0002-0002  1                        AC6605
 0001-0001-0001  0                        AC6605
```

步骤 5 创建集群

说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
```


版权所有 © 华为技术有限公司

```
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       AC6605
0003-0003-0003  1                       AC6605
0002-0002-0002  1                       AC6605
```

步骤 6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“**添加成员交换机**”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   AC6605
Member-2                        1     0003-0003-0003   AC6605
Member-3                        2     0004-0004-0004   AC6605
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    AC6605                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    AC6605                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    AC6605                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    AC6605                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```


版权所有 © 华为技术有限公司

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

说明

此处也可以使用动态路由协议。

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 禁止 NDP 功能和 NTDP 功能

在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 功能和 NTDP 功能。

```
# 禁止不相关接口的NDP功能
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ndp
# 禁止不相关接口的NTDP功能
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ntdp
```

步骤 11 检查配置结果

完成上述配置后，在命令交换机上执行 **display member-interface-state** 命令，查看成员交换机不相关接口的 NDP 或 NTDP 的状态。可以看到结果是“Success”。

```
[HUAWEI_0.Administrator-1] display member-interface-state ndp
```


版权所有 © 华为技术有限公司

```
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         AC6605          0004-0004-0004      10.0.0.4            success
2         AC6605          0003-0003-0003      10.0.0.3            success
1         AC6605          0002-0002-0002      10.0.0.2            success
[HUAWEI_0.Administrator-1] display member-interface-state ntdp
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         AC6605          0004-0004-0004      10.0.0.4            success
2         AC6605          0003-0003-0003      10.0.0.3            success
1         AC6605          0002-0002-0002      10.0.0.2            success
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet0/0/1
```


版权所有 © 华为技术有限公司

```
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

10.4 NTP 配置

通过配置 NTP，可以保持网络中各设备的时钟运行一致。

10.4.1 NTP 概述

本节描述了 NTP 的基本原理和与运行模式。

NTP（Network Time Protocol）的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用。

对于运行 NTP 的本地系统，既可以接收来自其他时钟源的同步，也可以作为时钟源去同步别的时钟，并且可以通过交换 NTP 报文互相同步。

NTP 报文封装在 UDP 报文中传输，使用端口号 123。

NTP 的应用

NTP 主要应用于需要网络中所有主机或交换机时钟保持一致的场景，比如：

- 网络管理：对从不同交换机采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
- 计费系统：要求所有设备的时钟保持一致。
- 完成某些功能：例如，定时重启网络中的所有交换机时，要求所有交换机的时钟保持一致。
- 多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟。
- 备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步。

对于网络中的众多设备，如果依靠管理员手工输入命令来修改系统时钟，不仅工作量巨大，也不能保证时钟的精确性。通过配置 NTP，可以很快将网络中设备的时钟同步，同时保证很高的精度。

NTP 的优势：

- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。
- 支持访问控制和 MD5 验证。
- 支持采用单播、组播或广播方式发送协议报文。

版权所有 © 华为技术有限公司

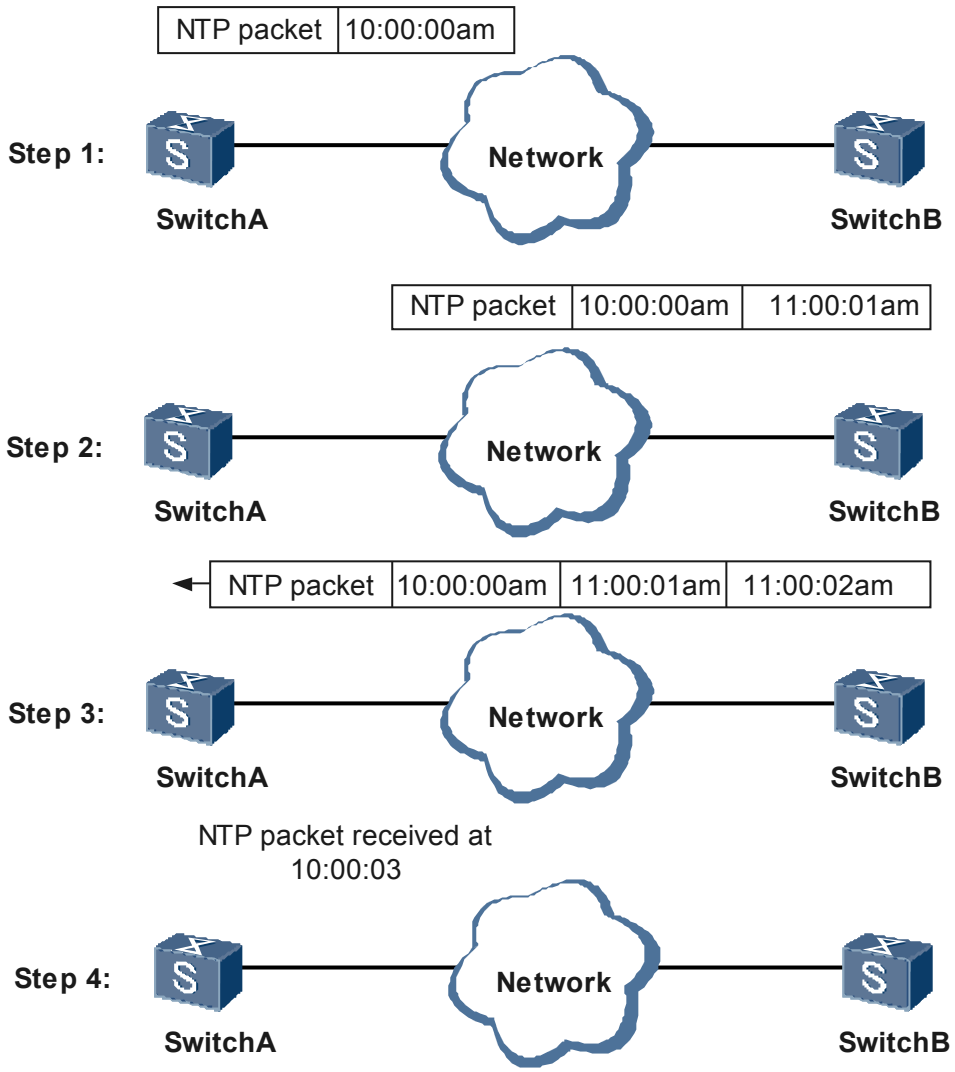
NTP 工作原理

NTP 基本工作原理如图 10-28 所示。Switch A 和 Switch B 通过广域网相连，它们都有自己独立的系统时钟，通过 NTP 实现系统时钟自动同步。

作如下假设：

- 在 Switch A 和 Switch B 的系统时钟同步之前，Switch A 的时钟设定为 10:00:00am，Switch B 的时钟设定为 11:00:00am。
- Switch B 充当 NTP 时间服务器。Switch A 的时钟与 Switch B 的时钟同步。
- 数据包在 Switch A 和 Switch B 之间单向传输需要 1 秒。
- Switch A 和 Switch B 处理 NTP 数据包的时间都是 1 秒。

图 10-28 NTP 基本原理图



系统时钟同步的工作过程如下：

版权所有 © 华为技术有限公司

1. Switch A 发送一个 NTP 消息包给 Switch B，该消息包带有它离开 Switch A 时的时间戳 10:00:00am（T1）。
2. 此 NTP 消息包到达 Switch B 时，Switch B 加上到达时间戳 11:00:01am（T2）。
3. 此 NTP 消息包离开 Switch B 时，Switch B 再加上离开时间戳 11:00:02am（T3）。
4. Switch A 接收到该响应消息包时，加上新的时间戳 10:00:03am（T4）。

   至此，Switch A 拥有足够信息来计算以下两个重要参数：

   - NTP 消息来回一个周期的时延：Delay=（T4-T1）-（T3-T2）。
   - Switch A 相对 Switch B 的时间差：Offset=（（T2-T1）+（T3-T4））/2。

   Switch A 根据时间差和时延来设定自己的时钟，实现与 Switch B 的时钟同步。

   以上是 NTP 工作原理的简略描述，在 RFC1305 中，NTP 使用复杂的算法来确保时钟同步的精确性。

   服务器和客户端的概念是相对而言的，提供时间标准的设备称为时间服务器，接收时间服务的设备称为客户端。

10.4.2 AC6605 支持的 NTP 特性

本节介绍 AC6605 支持的 NTP 运行模式。

AC6605 支持如下几种 NTP 工作模式：

- 单播服务器/客户端模式
- 对等体模式
- 广播模式
- 组播模式

单播服务器/客户端模式

这种模式只需要在客户端配置，服务器端除了配置 NTP 主时钟外，不需要进行其他专门配置。

注意只能是客户端同步到服务器，服务器不会同步到客户端。

配置完成后：

1. 客户端向服务器发送同步请求报文，报文中的 Mode 字段设置为 3（客户模式）。
2. 服务器端收到请求报文后，自动工作在服务器模式，并发送应答报文，报文中的 Mode 字段设置为 4（服务器模式）。
3. 客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器端。

对等体模式

在对等体模式中，NTP 只需要在主动对等体（Symmetric active）端进行配置。

对等体模式下，主动对等体和被动对等体可以互相同步，等级低（层数大）的对等体向等级高（层数小）的对等体同步。

配置完成后：

- 主动对等体向被动对等体发送同步请求报文，报文中的 Mode 字段设置为 1（主动对等体）。

版权所有 © 华为技术有限公司

- 被动对等体收到请求报文后，自动工作在被动对等体模式，并发送应答报文，报文中的 Mode 字段设置为 2（被动对等体）。

广播模式

在广播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向广播地址 255.255.255.255 发送时钟同步报文。
- 客户端侦听来自服务器的广播消息包。
- 客户端接收到第一个广播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。
- 客户端进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。

组播模式

在组播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向组播目的地址 224.0.1.1 发送时钟同步报文。
- 客户端侦听来自服务器的组播消息包。
- 当客户端接收到第一个组播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。
- 客户端进入组播客户端模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。

10.4.3 配置 NTP 基本功能

在 NTP 基本配置里，用户可以了解到如何配置 NTP 的基本功能，包括 NTP 的工作模式。

建立配置任务

在配置 NTP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 有 4 种工作模式：

- 服务器/客户端模式
- 对等体模式
- 广播模式
- 组播模式

在实际使用中，应根据网络部署情况选择适当的工作模式，以满足不同情况下的网络时钟同步需求。

版权所有 © 华为技术有限公司

对于单播服务器/客户端模式和对等体模式，还可以指定本地发送的所有 NTP 消息都使用同一接口的 IP 地址作为源 IP。

前置任务

在配置 NTP 基本功能之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网路层地址和路由协议，保证 NTP 报文可达

数据准备

在配置 NTP 基本功能之前，需要准备以下数据：

序号	数据
1	NTP 主时钟、主时钟的层数
2	收发 NTP 报文的接口
3	NTP 的版本
4	根据选用的工作模式，准备以下数据： ● 服务器/客户端模式：服务器的 IP 地址和服务器所属的 VPN 实例 ● 对等体模式：被动对等体的 IP 地址和被动对等体所属的 VPN 实例 ● 广播模式：发送和接收 NTP 广播包的接口、客户端允许建立的最大动态会话数目 ● 组播模式：NTP 组播消息包使用的组播组地址、组播消息包的生存周期 TTL、发送和接收 NTP 组播包的接口、客户端允许建立的最大动态会话数目
5	禁止接收 NTP 报文的接口

配置 NTP 主时钟

服务器端主时钟的层数一定要小于客户端时钟的层数，否则客户端无法跟服务器端的时钟进行同步。

背景信息

如果使用交换机提供 NTP 主时钟，请在作为 NTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service refclock-master** [*ip-address*] [*stratum*]配置 NTP 主时钟。

ip-address 是本地参考时钟的 IP 地址 127.127.t.u。t 的取值范围是 0 ～ 37。目前只能取 1，表示本地参考时钟；u 表示 NTP 进程号，取值范围是 0 ～ 3。

版权所有 © 华为技术有限公司

当不指定 IP 地址时，默认使用本地时钟 127.127.1.0 为 NTP 主时钟，层数为 8。

----结束

配置单播服务器/客户端模式

服务器/客户端服务方式下，客户端选择与服务器的主时钟进行同步。

背景信息

通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

如果在服务器端指定了发送 NTP 报文的源地址，该地址必须与在客户端配置的服务端 IP 地址相同。否则，客户端无法处理服务器端发送的 NTP 报文，进而时钟同步失败。

操作步骤

- 配置 NTP 客户端。

  请在作为客户端的交换机上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令：

     ntp-service source-interface vlanif *vlan-id*

     配置用来接收 NTP 报文的本地源接口。
  3. 执行命令:

     ntp-service unicast-server *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference**] *

     配置 NTP 服务器的 IP 地址。

     步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口（**source-interface**），优先选择步骤 3 指定的源接口。

     参数 *ip-address* 指定了 NTP 服务器的 IP 地址。该地址只能是一个主机 IP 地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。

     说明

     指定单播 NTP 服务器后，本地交换机自动充当客户端的角色。服务器上只能配置一个主时钟。

- （可选）配置 NTP 服务器上发送 NTP 报文的源接口

  请在作为客户端的交换机上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令:

     ntp-service source-interface vlanif *vlan-id*

     配置用来发送 NTP 报文的本地源接口。

     通常需要在客户端指定 NTP 服务器的源接口。之后，客户端与服务器端才能使用该接口交换 NTP 报文。

版权所有 © 华为技术有限公司

如果在服务器端指定了发送 NTP 报文的源接口，该接口必须与在客户端配置的服务端 IP 地址相同。否则，客户端无法处理服务器端发送的 NTP 报文，进而时钟同步失败。

----结束

配置对等体模式

介绍了如何配置 NTP 对等体模式。两个对等体上的时钟可以互相同步，一方既可以主动发送请求消息到对方请求时钟同步，又可以响应对方主动发送来的请求消息去同步对方。

操作步骤

- 配置 NTP 主动对等体
  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令：

     ntp-service source-interface vlanif *vlan-id*

     配置用来发送 NTP 报文的本地源接口。
  3. 执行命令:

     ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference**] *

     配置 NTP 对等体。

     步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口(**source-interface**)，优先使用步骤 3 中指定的源接口。

     参数 *ip-address* 指定了 NTP 对等体的 IP 地址。该地址只能是一个主机 IP 地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。

     说明

     指定 NTP 对等体后，本地交换机进入对称主动模式。对称被动端不需要配置。
- （可选）配置 NTP 被动对等体的源接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令:

     ntp-service source-interface vlanif *vlan-id*

     配置用来发送 NTP 报文的本地源接口。

     通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

     如果在主动对等体端指定了发送 NTP 报文的源接口，该接口必须与在被动对等体端配置的源接口相同。否则，主动对等体无法处理被动对等体发送的 NTP 报文，进而时钟同步失败。

----结束

配置广播模式

介绍了如何在局域网中配置 NTP 广播模式，实现局域网中的时钟同步。

版权所有 © 华为技术有限公司

操作步骤

- 配置一个 NTP 广播服务器

  请在作为 NTP 广播服务器的交换机上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。
  3. 执行命令 **interface vlanif** *vlan-id*，指定发送 NTP 广播报文的接口。
  4. 执行命令:

     ntp-service broadcast-server [**authentication-keyid** *key-id* | **version** *number*]*

     配置本地交换机作为 NTP 广播服务器。

     配置完成后，本地交换机周期性地向广播地址 255.255.255.255 发送时钟同步报文。

     说明

     广播模式只能在同一局域网中使用。

- 配置一个 NTP 广播客户端

  请在作为 NTP 广播客户端的交换机上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。
  3. 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。
  4. 执行命令 **interface vlanif** *vlan-id*，指定接收 NTP 广播报文的接口。
  5. 执行命令 **ntp-service broadcast-client**，将本地交换机配置为 NTP 广播客户端。

     步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

     配置完成后，本地交换机接收来自 NTP 服务器的广播 NTP 报文，并同步本地时钟。

     执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

配置组播模式

介绍如何配置 NTP 组播模式对域内的设备进行时钟同步。

操作步骤

- 配置一个 NTP 组播服务器

  请在作为 NTP 服务器的交换机上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，创建 VLAN 并接进入 VLAN 视图。
  3. 执行命令 **interface vlanif** *vlan-id*，指定发送 NTP 组播报文的接口。
  4. 执行命令:

版权所有 © 华为技术有限公司

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **version** *number*] *

配置本地交换机作为一个 NTP 组播服务器。

配置完成后，本地交换机周期性地向组播地址 224.0.1.1 发送时钟同步报文。

- 配置一个 NTP 组播客户端

请在作为客户端的交换机上,执行以下配置：

1. 执行命令 **system-view**，进入系统视图。
2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。
3. 执行命令 **vlan** *vlan-id*，创建 VLAN 并接进入 VLAN 视图。
4. 执行命令 **interface vlanif** *vlan-id*，指定接受 NTP 组播报文的接口。
5. 执行命令:

   ntp-service multicast-client [*ip-address*]

   配置本地交换机作为一个 NTP 组播客户端。

   步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

   配置完成后，本地交换机侦听来自 NTP 服务器的组播 NTP 报文，并同步本地时钟。

   执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

禁止指定接口接收 NTP 报文

当局域网中的某台主机不需要同步指定服务器的时钟时，可以禁止该主机的指定接口接收 NTP 报文。

背景信息

在需要禁止某个接口接收 NTP 报文的交换机上，请进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并接进入 VLAN 视图。

步骤 3 执行命令 **interface vlanif** *vlan-id*，指定接收 NTP 报文的接口。

步骤 4 执行命令:

```
ntp-service in-interface disable
```

禁止交换机上的接口接收 NTP 报文。

----结束

版权所有 © 华为技术有限公司

（可选）配置 NTP 的最大动态会话数

背景信息

当需要在作为 NTP 客户端的 AC6605 上配置 NTP 的最大动态会话数时，请进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service max-dynamic-sessions** *number*，配置 NTP 的最大动态会话数。

----结束

检查配置结果

在配置 NTP 基本功能成功后，可以查看到 NTP 的基本功能的配置情况。

前提条件

已经完成配置 NTP 基本功能的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。
- 执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<Quidway> display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 10.00 ms
 reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions** [**verbose**]查看 NTP 会话的状态。

```
<Quidway> display ntp-service sessions
              source          reference       stra reach poll  now offset delay disper
********************************************************************************
        [12345]127.127.1.0     LOCAL(0)          7    1   64    2      -    0.0   15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

版权所有 © 华为技术有限公司

```
<Quidway> display ntp-service trace
server 127.0.0.1,stratum 5, offset 0.024099, synch distance 0.06337
server 171.1.1.2,stratum 4, offset 0.028786, synch distance 0.04575
server 201.1.1.2,stratum 3, offset 0.035199, synch distance 0.03075
server 200.1.7.1,stratum 2, offset 0.039855, synch distance 0.01096
refid 127.127.1.0
```

10.4.4 配置 NTP 安全机制

本节介绍如何配置 NTP 安全模式，从而在对安全要求比较高的网络中，实现可靠的时钟同步。

建立配置任务

在配置 NTP 安全机制前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 提供访问权限和 NTP 验证两种安全机制。

- 访问权限

  通过设置访问权限保护本地 NTP 服务是 AC6605 提供的一种比较简单的安全措施。

  AC6605 提供 4 个等级的访问限制。当一个 NTP 访问请求报文到达本地时，按照最小访问限制到最大访问限制对报文进行依次匹配，以第 1 个匹配的为准，匹配顺序如下：

  - **peer**: 表示最小访问限制。远端设备可以给本地设备发送时间请求和控制查询，本地时钟也可以同步到远端服务器。
  - **server**: 远端设备可以对本地设备进行时间请求和控制查询，但本地时钟不会同步到远端服务器。
  - **synchronization**: 只允许远端设备对本地设备提出时间请求。
  - **query**: 表示最大访问限制。只允许远端设备对本地设备进行控制查询。
- NTP 验证

  在安全性要求较高的网络中，可以启用 NTP 验证功能。

  配置 NTP 验证功能分为两部分：配置客户端、配置服务器端。

  在配置 NTP 验证功能时，应注意以下原则：

  - 客户端和服务器端均需要配置 NTP 验证功能。否则，NTP 验证功能不生效。
  - 如果使能了 NTP 验证功能，应同时配置一个可信的密钥。
  - 在服务器端和客户端上配置的密钥必须相同。
  - 在 NTP 对等体模式下，主动对等体相当于客户端，被动对等体相当于服务器端。

前置任务

在配置 NTP 安全机制之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网络层地址和路由协议，保证客户端和交换机端路由可达
- 如果配置访问权限，需要配置用于进行访问控制的 ACL

版权所有 © 华为技术有限公司

数据准备

在配置 NTP 安全机制之前，需要准备以下数据：

序号	数据
1	ACL 规则
2	NTP 验证使用的密钥 ID 和密钥
3	NTP 主时钟、主时钟的层数
4	收发 NTP 报文的接口
5	NTP 的版本
6	根据选用的 NTP 工作模式，准备以下数据： ● 服务器/客户端模式：服务器的 IP 地址服务器所属的 VPN 实例 ● 对等体模式：被动对等体的 IP 地址被动对等体所属的 VPN 实例 ● 广播模式：发送和接收 NTP 广播包的接口、客户端允许建立的最大动态会话数目 ● 组播模式：NTP 组播消息包使用的组播组地址、组播消息包的生存周期 TTL

配置 NTP 访问控制权限

在接收到一个访问请求报文后，NTP 服务器按照降序（peer, server, synchronization to query）对报文的访问限制进行匹配，以第一个匹配的访问权限为准。

背景信息

请在交换机上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

ntp-service access { **peer** | **query** | **server** | **synchronization** } *acl-number*

在本地交换机上配置 NTP 服务的访问控制权限。

用户需要根据实际需求决定在哪台设备上配置 **ntp-service access** 命令。

具体描述见**表 10-5**。

表 10-5 NTP 访问控制权限配置

NTP 工作模式	限制的 NTP 请求类型	进行配置的设备
单播 NTP 服务器/客户端模式	限制客户端同步到服务器端	客户端

版权所有 © 华为技术有限公司

NTP 工作模式	限制的 NTP 请求类型	进行配置的设备
单播 NTP 服务器/客户端模式	限制服务器端处理客户端发送的时钟同步请求	服务器端
NTP 对等体模式	限制客户端和服务器端进行时钟同步	主动对等体端
NTP 对等体模式	限制被动对等体端处理主动对等体发送的时钟请求	被动对等体端
NTP 组播模式	限制客户端同步到服务器端	NTP 组播客户端
NTP 广播模式	限制客户端同步到服务器端	NTP 广播客户端

----结束

使能 NTP 验证

该部分描述了如何配置 NTP MD5 认证。

背景信息

为了确保网络中时间服务器的可靠性，客户端必须同已通过认证的 NTP 服务器进行同步，防止恶意攻击造成的时钟报文数据的更改。

请在交换机上进行以下配置。

操作步骤

- 配置 NTP MD5 认证

  说明

  - 客户端与服务器端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。
  - 必须先使能 NTP 验证功能，否则不会进行验证。

  1. 执行 **system-view** 命令，进入系统视图。
  2. 执行 **ntp-service authentication enable** 命令，使能 NTP 验证功能。
  3. 执行 **ntp-service authentication-keyid** *key-id* **authentication-mode md5** *password* 命令，配置 NTP 验证密钥。
  4. 执行 **ntp-service reliable authentication-keyid** *key-id* 命令，声明密钥可信。

----结束

在单播服务器/客户端模式下配置 NTP 验证

通过在 NTP 客户端配置与指定 NTP 服务器同步时使用的密钥 ID，可以在 NTP 服务器/客户端模式下应用 NTP 验证。

背景信息

请在作为 NTP 单播客户端的交换机上,执行以下配置：

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

ntp-service unicast-server *ip-address* [[**authentication-keyid** *key-id*] | [**version** *number*] | [**source-interface** *interface-type interface-number*] | [**preference**]]*

配置用来进行服务器和客户端时钟同步的验证密钥 ID。

----结束

在对等体模式下配置 NTP 验证

通过在本端配置与对等体端同步时使用的密钥 ID，可以在对等体模式下应用 NTP 验证。

背景信息

请在作为主动对等体端的交换机上,执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference**] *

配置用来进行 NTP 对等体时钟同步的验证密钥 ID。

----结束

在广播模式下配置 NTP 验证

通过在本地交换机配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在广播模式下应用 NTP 验证。

背景信息

请在作为 NTP 广播服务器的交换机上，执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **interface vlanif** *vlan-id*，指定发送 NTP 广播报文的接口。

步骤 4 执行命令 **ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*] *配置本地交换机作为 NTP 广播服务器时使用的密钥 ID。

对于广播客户端的配置，参见“**配置广播模式**”。

----结束

版权所有 © 华为技术有限公司

在组播模式下配置 NTP 验证

通过在本地交换机配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在组播模式下应用 NTP 验证。

背景信息

请在作为 NTP 组播服务器的交换机上，执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **interface vlanif** *vlan-id*，指定发送 NTP 组播包的接口。

步骤 4 执行命令:

ntp-service multicast-server [**authentication-keyid** *key-id* | **version** *number*]*

配置 NTP 组播服务器使用的验证密钥 ID。

对于组播客户端的配置，参见“配置组播模式”。

----结束

检查配置结果

在成功配置 NTP 安全机制后，可以查看到 NTP 安全机制的配置情况。

前提条件

已经完成 NTP 安全机制的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<Quidway> display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 10.00 ms
 reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

版权所有 © 华为技术有限公司

```
<Quidway> display ntp-service sessions
              source          reference       stra reach poll  now offset delay disper
**********************************************************************************
       [12345]127.127.1.0     LOCAL(0)          7    1   64    2      -    0.0   15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

10.4.5 维护 NTP

本节介绍在出现 NTP 运行故障时，如何运行 debugging 命令对 NTP 进行调试。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 NTP 运行故障时，请在用户视图下执行中的 **debugging** 命令对 NTP 进行调试，查看调试信息，定位故障并分析故障原因。

有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 命令手册》。

操作步骤

步骤 1 执行命令 **debugging ntp-service** { **access** | **adjustment** | **all** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }打开 NTP 的调试开关。

----结束

10.4.6 配置举例

介绍 NTP 的各种组网举例。

配置带验证的单播 NTP 服务器/客户端模式示例

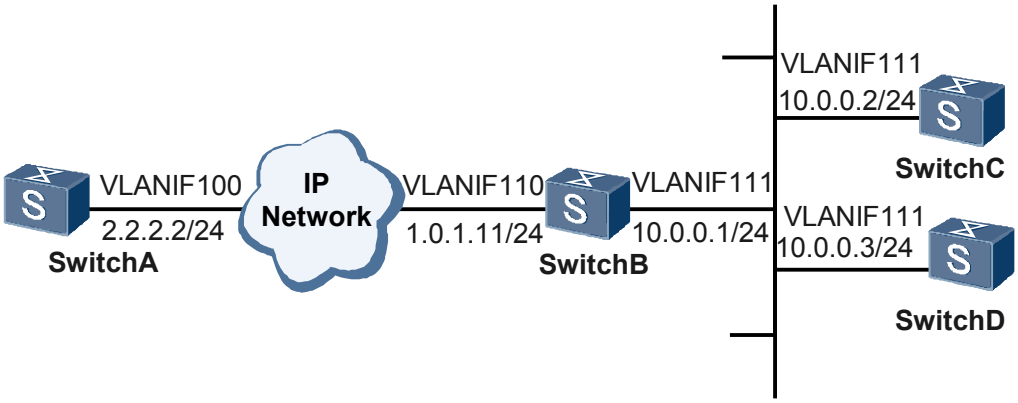
组网需求

如图 10-29 所示。

- SwitchA 作为 NTP 单播服务器，其本地时钟作为 NTP 主时钟，层数为 2。
- SwitchB 作为 NTP 客户端，同步远端服务器 SwitchA 的时钟。
- SwitchC 和 SwitchD 作为 NTP 客户端，把 SwitchB 作为自己的 NTP 服务器。
- 启用 NTP 验证。

版权所有 © 华为技术有限公司

图 10-29 单播 NTP 服务器/客户端模式组网图



配置思路

采用如下思路进行此案例的配置：

1. 配置 SwitchA 作为服务器，提供主时钟。
2. 配置 SwitchB 作为 NTP 客户端，同步 SwitchA 的时钟。
3. 配置 SwitchC、SwitchD 作为 NTP 客户端，同步 SwitchB 的时钟。
4. 在 SwitchA 和 SwitchB、SwitchC 和 SwitchD 上配置 NTP 验证。

说明

配置带验证的单播 NTP 服务器/客户端模式时：

- 客户端必须先使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。
- 客户端和服务器端都需要进行完整的配置，才能验证通过。

数据准备

为完成此配置，需准备如下数据：

- 参考时钟的 IP 地址
- NTP 主时钟的层次数
- 密钥编号
- 密码

操作步骤

步骤 1 配置各 Switch 的 IP 地址并路由可达。

如图 10-29，配置 IP 地址，配置 SwitchA 和 SwitchB 路由可达；配置 SwitchB 和 SwitchC，SwitchB 和 SwitchD 路由可达。

具体配置过程略。

步骤 2 在 SwitchA 配置 NTP 主时钟并启动验证功能。

在 SwitchA 上指定使用自己的本地时钟作为参考时钟，层数为 2。

版权所有 © 华为技术有限公司

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

在 SwitchA 上使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchA] ntp-service reliable authentication-keyid 42
```

注意服务器端与客户端必须配置相同的验证密钥。

步骤 3 在 SwitchB 指定 NTP 服务器并启动验证功能。

在 SwitchB 上使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
<SwitchB> system-view
[SwitchB] ntp-service authentication enable
[SwitchB] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchB] ntp-service reliable authentication-keyid 42
```

SwitchB 指定 SwitchA 为 NTP 服务器，并使用已配置的验证密钥。

```
[SwitchB] ntp-service unicast-server 2.2.2.2 authentication-keyid 42
```

步骤 4 在 SwitchC 指定 NTP 服务器。

SwitchC 指定 SwitchB 作为自己的 NTP 服务器。

```
<SwitchC> system-view
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchC] ntp-service reliable authentication-keyid 42
[SwitchC] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 5 在 SwitchD 指定 NTP 服务器。

SwitchD 指定 SwitchB 作为自己的 NTP 服务器。

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchD] ntp-service reliable authentication-keyid 42
[SwitchD] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 6 验证配置结果。

完成上述配置后，SwitchB 可以同步到 SwitchA 的时间。

查看 SwitchB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 SwitchA 低 1 级。

```
[SwitchB] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 2.2.2.2
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

完成上述配置后，SwitchC 可以同步到 SwitchB 的时间。

查看 SwitchC 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 SwitchB 低 1 级。

版权所有 © 华为技术有限公司

```
[SwitchC] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 SwitchD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 SwitchB 低 1 级。

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 SwitchA 的 NTP 状态。

```
[SwitchA] display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 26.50 ms
 peer dispersion: 10.00 ms
 reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 2.2.2.2 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
```


版权所有 © 华为技术有限公司

```
ntp-service refclock-master 2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#

vlan batch 110 111
#
interface Vlanif110
 ip address 1.0.1.11 255.255.255.0
#
interface Vlanif111
 ip address 10.0.0.1 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
interface  GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 2.2.2.2 authentication-keyid 42
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 111
#
interface Vlanif111
 ip address 10.0.0.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 111
#
interface Vlanif111
 ip address 10.0.0.3 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
```


版权所有 © 华为技术有限公司

```
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

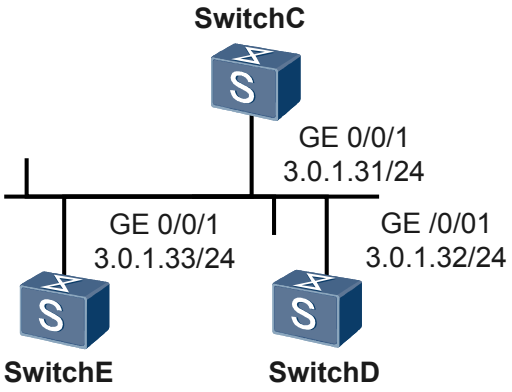
配置普通 NTP 对等体模式示例

组网需求

如图 10-30 所示。在同一个局域网中有 3 台 Switch。

- SwitchC 将自己的本地时钟设为 NTP 主时钟，层数为 2。
- SwitchD 将 SwitchC 设为自己的 NTP 服务器。即，SwitchD 作为客户端。
- SwitchE 将 SwitchD 设为自己的被动对等体。即，SwitchE 作为主动对等体。

图 10-30 NTP 对等体模式组网图



配置思路

采用如下思路进行此案例的配置：

1. 配置 SwitchC 的本地主时钟，SwitchD 向 SwitchC 请求时钟同步。
2. 配置 SwitchE 和 SwitchD 为对等体，SwitchE 向 SwitchD 发起时钟同步请求。
3. 最终实现 SwitchC、SwitchD、SwitchE 这 3 台 Switch 的时钟同步。

数据准备

为完成此配置例，需准备如下数据：

- SwitchC 的 IP 地址
- SwitchD 的 IP 地址
- NTP 主时钟的层次数

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 3 台 Switch 之间网络层可达。

按图 10-30 配置各接口的 IP 地址，配置完成后，3 台 Switch 可以相互 ping 通。

具体配置过程略。

步骤 2 配置 NTP 单播服务器/客户端模式。

在 SwitchC 上指定使用自己的本地时钟作为参考时钟，层数为 2。

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

在 SwitchD 上指定 SwitchC 作为自己的 NTP 服务器。

```
<SwitchD> system-view
[SwitchD] ntp-service unicast-server 3.0.1.31
```

配置完成后，SwitchD 的时钟同步到 SwitchC。

查看 SwitchD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 SwitchC 低 1 级。

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 3.0.1.31
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 62.50 ms
 root dispersion: 0.20 ms
 peer dispersion: 7.81 ms
 reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
```

步骤 3 配置 NTP 单播对等体模式。

在 SwitchE 上指定 SwitchD 作为自己的被动对等体。

```
<SwitchE> system-view
[SwitchE] ntp-service unicast-peer 3.0.1.32
```

SwitchE 没有配置主时钟，层数低于 SwitchD，所以 SwitchE 向 SwitchD 同步。

步骤 4 验证配置结果。

同步后观测 SwitchE 的状态。

查看 SwitchE 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。SwitchE 的时钟层数为 4，比被动对等体 SwitchD 低 1 级。

```
[SwitchE] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 3.0.1.32
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 124.98 ms
 root dispersion: 0.15 ms
 peer dispersion: 10.96 ms
 reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
```

----结束

版权所有 © 华为技术有限公司

配置文件

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.31 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ntp-service refclock-master 2
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.32 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
 ntp-service unicast-server 3.0.1.31
#
return
```

- SwitchE 的配置文件

```
#
 sysname SwitchE
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.33 255.255.255.0
#
interface  GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
 ntp-service unicast-peer 3.0.1.32
#
return
```

配置带验证的 NTP 广播模式示例

组网需求

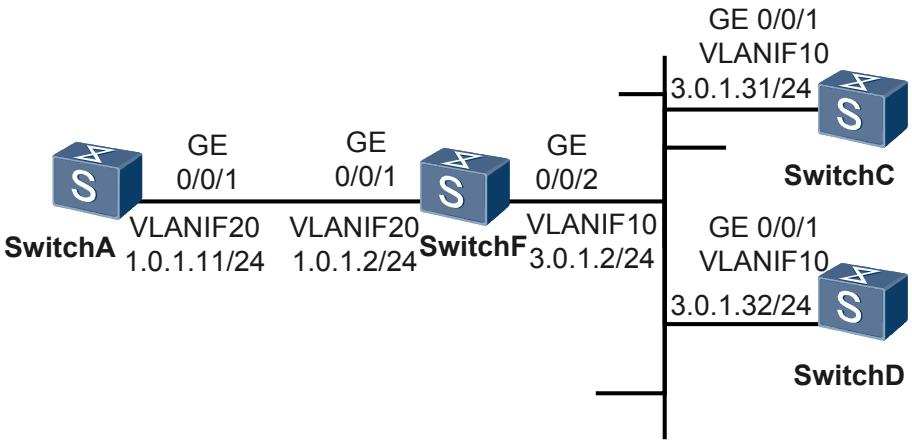
如图 10-31 所示。

- SwitchC 和 SwitchD 在同一个网段，SwitchA 在另一个网段。SwitchF 连接这两个网段。
- SwitchC 作为 NTP 广播服务器，使用本地时钟作为 NTP 主时钟，层数为 3，从接口 VLANIF10(对应的物理接口为 GigabitEthernet0/0/1)向外发送广播消息包。

版权所有 © 华为技术有限公司

- SwitchD 使用 VLANIF10(对应的物理接口为 GigabitEthernet0/0/1)接口监听广播消息。
- SwitchA 使用 VLANIF20(对应的物理接口为 GigabitEthernet0/0/1)接口监听广播消息。
- 启用 NTP 验证。

图 10-31 NTP 广播模式组网图



配置思路

采用如下思路进行此案例的配置：

1. 配置 SwitchC 为 NTP 广播服务器
2. 配置 SwitchA 和 SwitchD 为 NTP 广播客户端
3. 在 SwitchA、SwitchC 和 SwitchD 上配置 NTP 验证

数据准备

为完成此配置例，需准备如下数据：

- 各 Switch 的接口 IP 地址
- 各接口所属的 VLAN ID
- NTP 主时钟的层次数
- 验证密钥和密钥 ID

操作步骤

步骤 1 配置各 Switch 的 IP 地址。

按图 10-31 配置各接口的 IP 地址。

#配置 SwitchC 的 VLANIF 接口的和 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 10
[SwitchC-Vlan10] quit
[SwitchC] interface gigabitethernet 0/0/1
```


版权所有 © 华为技术有限公司

```
[SwitchC-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchC-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10]ip address 3.0.1.31 24
[SwitchC-Vlanif10]quit
```

#配置 SwitchD 接口的 VLANIF 和 IP 地址。

```
<SwitchD> system-view
[SwitchD] vlan 10
[SwitchD-Vlan10] quit
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] ip address 3.0.1.32 24
[SwitchD-Vlanif10] quit
```

#配置 SwitchF 接口的 VLANIF 和 IP 地址。

```
<SwitchF> system-view
[SwitchF] vlan 10
[SwitchF-Vlan10] quit
[SwitchF] interface gigabitethernet 0/0/2
[SwitchF-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchF-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchF-GigabitEthernet0/0/2] quit
[SwitchF] interface vlanif 10
[SwitchF-Vlanif10] ip address 3.0.1.2 24
[SwitchF-Vlanif10] quit
[SwitchF] vlan 20
[SwitchF-Vlan20] quit
[SwitchF] interface gigabitethernet 0/0/1
[SwitchF-GigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchF-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchF-GigabitEthernet0/0/1] quit
[SwitchF] interface vlanif 20
[SwitchF-vlanif20] ip address 1.0.1.2 24
[SwitchF-vlanif20] quit
```

#配置 SwitchA 接口的 VLANIF 和 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-Vlan20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 20
[SwitchA-vlanif20] ip address 1.0.1.11 24
[SwitchA-vlanif20] quit
```

步骤 2 配置 Switch 之间路由可达（略）。

步骤 3 配置 NTP 广播服务器，并启用验证。

配置 SwitchC 使用本地时钟作为 NTP 主时钟，层数为 3。

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 3
```

启用 NTP 验证。

```
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchC] ntp-service reliable authentication-keyid 16
```


版权所有 © 华为技术有限公司

配置 SwitchC 为 NTP 广播服务器，从 VLANIF10 发送 NTP 广播消息包，并指定使用密钥 ID 16 加密。

```
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] ntp-service broadcast-server authentication-keyid 16
[SwitchC-Vlanif10] quit
```

步骤 4 配置与服务器在同一网段的 NTP 广播客户端 SwitchD。

启用 NTP 验证。

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchD] ntp-service reliable authentication-keyid 16
```

配置 SwitchD 为 NTP 广播客户端，从接口 VLANIF10 侦听 NTP 广播消息包。

```
[SwitchD]interface vlanif 10
[SwitchD-vlanif10] ntp-service broadcast-client
[SwitchD-vlanif10] quit
```

配置完成后，SwitchD 的时钟同步到 SwitchC。

步骤 5 配置与服务器在不同网段的 NTP 广播客户端 SwitchA。

启用 NTP 验证。

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchA] ntp-service reliable authentication-keyid 16
```

配置 SwitchA 为 NTP 广播客户端，从接口 VLANIF20 侦听 NTP 广播消息包。

```
[SwitchA]interface vlanif 20
[SwitchA-vlanif20] ntp-service broadcast-client
[SwitchA-vlanif20] quit
```

步骤 6 验证配置结果。

完成以上配置后，SwitchD 能够同步到 SwitchC，而 SwitchA 不能同步到 SwitchC。

这是因为 SwitchA 和 SwitchC 不在同一个网段，收不到 SwitchC 发出的广播包；而 SwitchD 和 SwitchC 在同一个网段，能够收到 SwitchC 发出的广播包。

查看 SwitchD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 SwitchC 低 1 级。

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 3.0.1.31
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.42 ms
 peer dispersion: 0.00 ms
 reference time: 12:17:21.773 UTC Mar 7 2006(C7B7F851.C5EAF25B)
```

----结束

配置文件

- SwitchA 的配置文件

版权所有 © 华为技术有限公司

```
#
sysname SwitchA
#
vlan batch 20
#
interface Vlanif20
 ip address 1.0.1.11 255.255.255.0
 ntp-service broadcast-client
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
#
 ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 16
#
return
```

SwitchC 的配置文件

```
#
sysname SwitchC
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.31 255.255.255.0
 ntp-service broadcast-server authentication-keyid 16
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
ntp-service refclock-master 3
#
return
```

- SwitchD 的配置文件

```
#
sysname SwitchD
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.32 255.255.255.0
 ntp-service broadcast-client
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
#
return
```

- SwitchF 的配置文件

```
#
sysname SwitchF
#
vlan batch 10 20
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif10
 ip address 3.0.1.2 255.255.255.0
#
interface Vlanif20
 ip address 1.0.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 3.0.1.0 0.0.0.255
#
return
```

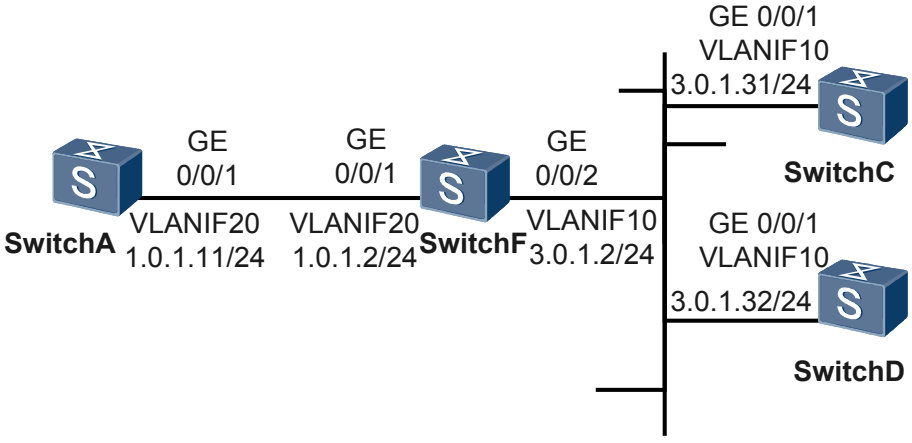
配置普通 NTP 组播模式示例

组网需求

如图 10-32 所示。

- SwitchC 和 SwitchD 在同一个网段，SwitchA 在另一个网段。SwitchF 连接这两个网段。
- SwitchC 作为 NTP 组播服务器，使用本地时钟作为 NTP 主时钟，层数为 2，从接口 VLANIF 10(对应的物理接口为 GigabitEthernet0/0/1)发送组播消息包。
- SwitchD 使用接口 VLANIF10(对应的物理接口为 GigabitEthernet0/0/1)监听组播消息。
- SwitchA 使用接口 VLANIF20(对应的物理接口为 GigabitEthernet0/0/1)监听组播消息。

图 10-32 NTP 组播模式组网图



版权所有 © 华为技术有限公司

配置思路

采用如下思路进行此案例的配置：

1. 配置 SwitchC 为 NTP 组播服务器
2. 配置 SwitchA 和 SwitchD 为 NTP 组播客户端

数据准备

为完成此配置例，需准备如下数据：

- 各 Switch 的接口 IP 地址
- NTP 主时钟的层次数

操作步骤

步骤 1 配置各 Switch 的 IP 地址。

按图 10-32 配置各接口的 IP 地址。

#配置 SwitchC 的 VLANIF 接口的和 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 10
[SwitchC-Vlan10] quit
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchC-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10]ip address 3.0.1.31 24
[SwitchC-Vlanif10]quit
```

#配置 SwitchD 接口的 VLANIF 和 IP 地址。

```
<SwitchD> system-view
[SwitchD] vlan 10
[SwitchD-Vlan10] quit
[SwitchD] interface gigabitethernet 0/0/1
[SwitchD-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-GigabitEthernet0/0/1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] ip address 3.0.1.32 24
[SwitchD-Vlanif10] quit
```

#配置 SwitchF 接口的 VLANIF 和 IP 地址。

```
<SwitchF> system-view
[SwitchF] vlan 10
[SwitchF-Vlan10] quit
[SwitchF] interface gigabitethernet 0/0/2
[SwitchF-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchF-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchF-GigabitEthernet0/0/2] quit
[SwitchF] interface vlanif 10
[SwitchF-Vlanif10] ip address 3.0.1.2 24
[SwitchF-Vlanif10] quit
[SwitchF] vlan 20
[SwitchF-Vlan20] quit
[SwitchF] interface gigabitethernet 0/0/1
[SwitchF-GigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchF-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchF-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

```
[SwitchF] interface vlanif 20
[SwitchF-vlanif20] ip address 1.0.1.2 24
[SwitchF-vlanif20] quit
```

#配置 SwitchA 接口的 VLANIF 和 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-Vlan20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 20
[SwitchA-vlanif20] ip address 1.0.1.11 24
[SwitchA-vlanif20] quit
```

步骤 2 配置 Switch 之间路由可达（略）。

步骤 3 配置 NTP 组播服务器。

配置 SwitchC 使用本地时钟作为 NTP 主时钟，层数为 2。

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

配置 SwitchC 为 NTP 组播服务器，从接口 VLANIF10 发送 NTP 组播消息包。

```
[SwitchC] interface vlanif 10
[SwitchC-vlanif10] ntp-service multicast-server
[SwitchC-vlanif10] quit
```

步骤 4 配置与服务器在同一网段的 NTP 组播客户端 SwitchD。

配置 SwitchD 为 NTP 组播客户端，使用接口 VLANIF10 监听 NTP 组播消息包。

```
<SwitchD> system-view
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] ntp-service multicast-client
[SwitchD-Vlanif10] quit
```

步骤 5 配置与服务器在不同网段的 NTP 组播客户端 SwitchA。

配置 SwitchA 为 NTP 组播客户端，从接口 VLANIF20 侦听 NTP 组播消息包。

```
<SwitchA> system-view
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ntp-service multicast-client
[SwitchA-Vlanif20] quit
```

步骤 6 验证配置结果。

完成以上配置后，SwitchD 能够同步到 SwitchC，而 SwitchA 不能同步到 SwitchC。

这是因为 SwitchA 和 SwitchC 不在同一个网段，收不到 SwitchC 发出的组播包；而 SwitchD 和 SwitchC 在同一个网段，能够收到 SwitchC 发出的组播包。

查看 SwitchD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 SwitchC 低 1 级。

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 3.0.1.31
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.66 ms
```


版权所有 © 华为技术有限公司

```
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005(C61734FD.800303C0)
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
vlan batch 20
#
interface Vlanif20
 ip address 1.0.1.11 255.255.255.0
 ntp-service multicast-client
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
sysname SwitchC
#
vlan batch 10
#
 ntp-service refclock-master  2
#
interface Vlanif10
 ip address 3.0.1.31 255.255.255.0
 ntp-service multicast-server
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchD 的配置文件

```
#
sysname SwitchD
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.32 255.255.255.0
 ntp-service multicast-client
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
Return
```

SwitchF 的配置文件

```
#
sysname SwitchF
#
vlan batch 10 20
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif10
 ip address 3.0.1.2 255.255.255.0
#
interface Vlanif20
 ip address 1.0.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 3.0.1.0 0.0.0.255
#
return
```

10.5 Ping 和 Tracert 配置

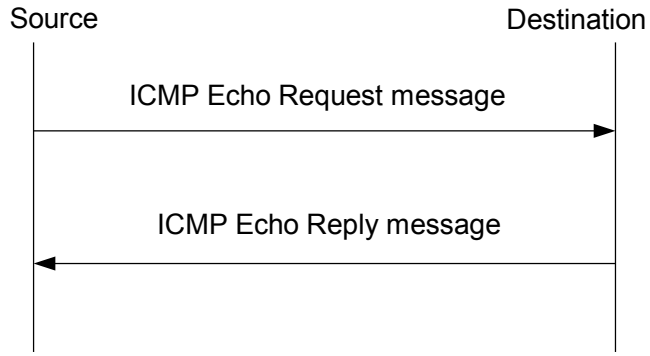
介绍 Ping 和 Tracert 命令的基本概念和使用。

10.5.1 Ping

ping 命令主要用于检查网络连接及主机是否可达。“Ping”这个词源于声纳定位操作，指来自声纳设备的脉冲信号。

如图 10-33 所示，**ping** 基于 ICMP 报文，即源端向目的端发送 ICMP Echo Request 报文，目的端收到此报文后立即回送 ICMP Echo Reply 报文。

图 10-33 Ping 原理



通过判断目的端是否回送 ICMP Echo Reply 报文，以及源端从发送 ICMP Echo Request 报文到接收到 ICMP Echo Reply 报文之间的时间差，可以检测源端和目的端在 IP 层的可达性，以及两端之间的链路状态。

版权所有 © 华为技术有限公司

图 10-34 ICMP Echo Request 和 ICMP Echo Reply 报文格式

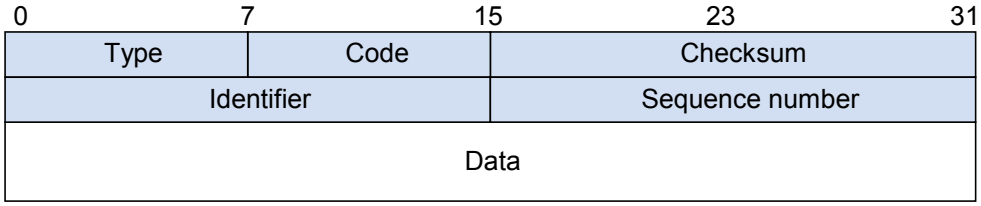


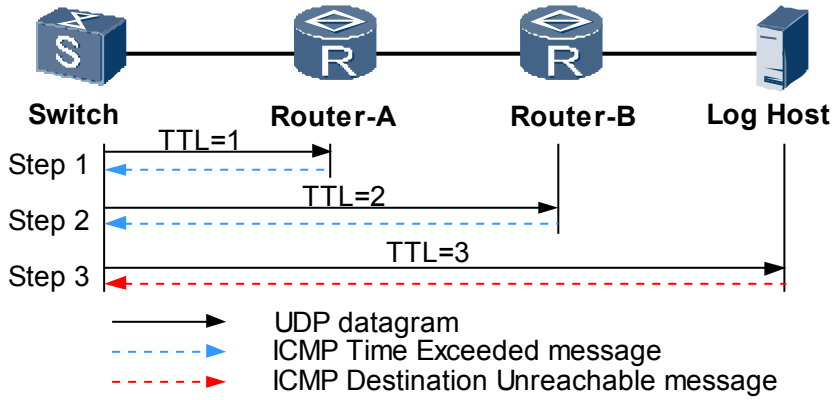
图 10-34 显示了 ICMP Echo Request 报文和 ICMP Echo Reply 报文的格式。其中，Data 字段是可变长度的字段。用户可以在 **ping** 命令中指定该字段的长度。

10.5.2 Tracert

“Tracert”的全称是“Trace Route”，主要用于检测源端到目的端之间的网关的数量和 IP 地址，检查网络连接是否可达，以及分析网络什么地方发生了故障。

AC6605 基于 ICMP 协议实现了 Trace Route 功能，记录报文从发送主机到目的地所经过的网关，检查网络连接是否可达，分析网络发生了故障的位置。

图 10-35 Trace Route 原理



以图 10-35 为例，介绍 AC6605 上 **tracert** 命令的实现原理。在 AC6605 上执行 **tracert** 命令，目的 IP 地址是日志主机的 IP 地址，采用缺省参数。

1. AC6605 首先发送一个目的 IP 地址是日志主机 IP 地址的 UDP 报文，此报文的 TTL 等于 1，且目的 UDP 端口号是 33434。
2. Router-A 收到 AC6605 发出的 UDP 报文后，判断目的 IP 地址不是本机 IP 地址。然后将 TTL 减 1，判断 TTL 等于 0，则向 AC6605 发送 ICMP Time Exceeded 报文。
3. AC6605 收到 Router-A 的 ICMP Time Exceeded 后，修改步骤 1 中的 UDP 报文，将此报文的 TTL 和目的 UDP 端口号各加 1，再次发送此报文。
4. 重复步骤 2 和步骤 3，直到日志主机接收到 AC6605 发送的 UDP 报文。
5. 日志主机收到 AC6605 发送的 UDP 报文后，判断目的 IP 地址是本机 IP 地址，则处理此报文。日志主机根据此报文中的目的 UDP 端口号寻找占用此端口号的上层协

版权所有 © 华为技术有限公司

议，在大多数情况下，大于 30000 的 UDP 端口号都没有被占用。因此，日志主机向 AC6605 发送 ICMP Destination Unreachable 报文，标识目的端口不可达。

6. AC6605 收到日志主机发送的 ICMP Destination Unreachable 后，判断出 UDP 报文已经到达目的端，则停止 Tracert 程序。

在上述步骤中，源端的 Tracert 程序根据步骤 3 中收到的 ICMP Time Exceeded 报文来记录源端与目的端之间的网关的 IP 地址。

10.5.3 配置 Ping 和 Tracert

介绍 Ping 和 Tracert 命令的使用。

建立配置任务

应用环境

连接 AC6605 的客户端无法正常上网，需要通过 **ping** 和 **tracert** 命令检测网络连接是否正常。

前置任务

- 确保客户端与 AC6605 之间的物理连接正常。
- 确保客户端正确配置了 IP 地址。

数据准备

在配置 Ping 和 Tracert 之前，需要准备以下数据。

序号	数据
1	客户端的 IP 地址。
2	网关的 IP 地址。

使用 Ping 检测网络连接是否正常

背景信息

请在连接异常客户端的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **ping** [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-f** | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-n** | **-p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host*，测试网络连接是否正常。

以上 **ping** 命令只列出了部分参数，各选项及参数的意义请参见《AC6605 无线接入控制器 命令参考》。

执行本命令输出的结果包括：

版权所有 © 华为技术有限公司

- 对每一个本端发出的 ICMP Echo Request 报文的响应情况，如果超时仍未收到响应报文，则输出“Request time out”，否则显示响应报文中数据字节数、报文序号、TTL和响应时间。
- 最终统计信息：发送报文总数、接收报文总数、未响应报文百分比和响应时间的最小值、平均值和最大值。

```
<Quidway> ping 202.38.160.244
PING 202.38.160.244 : 56 data bytes, press CTRL_C to break
  Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
  Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
  Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
  Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
  Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/2/3 ms
```

----结束

使用 Tracert 检测网络发生故障的位置

背景信息

请在连接异常客户端的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **tracert** [**-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *nqueries* | **-w** *timeout*]* *host*，测试故障发生的位置。

以上 **tracert** 命令只列出了部分参数，各选项及参数的意义请参见《AC6605 无线接入控制器 命令参考》。

执行本命令输出的结果可以表明从源主机到目的主机经过了哪些网关。

```
<Quidway> tracert 18.26.0.115
traceroute to 18.26.0.115 (18.26.0.115), max hops: 30 ,packet length: 40
1  128.3.112.1 (128.3.112.1)  0 ms  0 ms  0 ms
2  128.32.216.1 (128.32.216.1)  19 ms  19 ms  19 ms
3  128.32.216.1 (128.32.216.1)  39 ms  19 ms  19 ms
4  128.32.136.23 (128.32.136.23)  19 ms  39 ms  39 ms
5  128.32.168.22 (128.32.168.22)  20 ms  39 ms  39 ms
6  128.32.197.4 (128.32.197.4)  59 ms  119 ms  39 ms
7  131.119.2.5 (131.119.2.5)  59 ms  59 ms  39 ms
8  129.140.70.13 (129.140.70.13)  80 ms  79 ms  99 ms
9  129.140.71.6 (129.140.71.6)  139 ms  139 ms  159 ms
10  129.140.81.7 (129.140.81.7)  199 ms  180 ms  300 ms
11  129.140.72.17 (129.140.72.17)  300 ms  239 ms  239 ms
12  * * *
13  128.121.54.72 (128.121.54.72)  259 ms  499 ms  279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  18.26.0.115 (18.26.0.115)  339 ms  279 ms  279 ms
```

----结束

版权所有 © 华为技术有限公司

10.5.4 调试

介绍通过调试 ICMP 报文来定位故障的方法。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

对于在两台 AC6605 之间执行 **ping** 或 **tracert** 命令测试不通的情况，在排除物理连接的故障后，可以在两台设备上分别执行以下命令来作进一步定位。

操作步骤

步骤 1 使用命令 **debugging ip icmp** 打开 ICMP 报文的调试开关。

该命令可以查看在设备执行 **ping** 或 **tracert** 命令的过程中，ICMP 报文的收发情况，从而可以判断具体是哪台设备发生故障。

----结束

10.5.5 配置举例

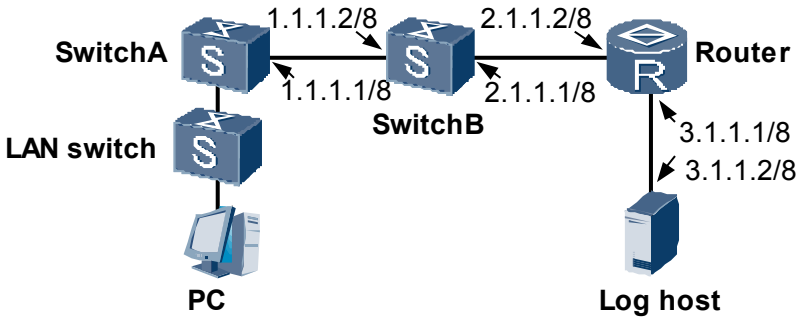
介绍 Ping 和 Tracert 命令使用的配置举例。

Ping 和 Tracert 的应用示例

配置需求

如图 10-36 所示，用户在结束了对 SwitchA 的配置之后，需要检查 SwitchA 与日志主机之间的链路是否通畅。如果发现不通，由于 SwitchA 和日志主机之间存在其他的网络设备，用户还需要定位具体是在哪段链路上发生问题。

图 10-36 ping 命令与 tracert 命令应用的组网图



版权所有 © 华为技术有限公司

配置思路

采用如下的思路检查链路状况。

1. 在 SwitchA 上执行 **ping** 命令检测其与日志主机之间的连通性。
2. 发现链路不通时，执行 **tracert** 命令确定具体在哪段链路上存在故障。

数据准备

为完成此配置例，需准备如下的数据。

- SwitchB 的 IP 地址为 1.1.1.2/8 和 2.1.1.1/8。
- Router 的 IP 地址为 2.1.1.2/8 和 3.1.1.1/8。
- 日志主机的 IP 地址为 3.1.1.2/8。

操作步骤

步骤 1 执行 **ping** 命令

在 SwitchA 上执行 **ping** 命令，测试与主机之间的连通性。

```
<Quidway> ping 3.1.1.2
  PING 3.1.1.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 3.1.1.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

SwitchA 显示无法 ping 通日志主机，表明两者之间有某段链路发生故障。

步骤 2 执行 **tracert** 命令

在 SwitchA 上执行 **tracert** 命令，定位具体是哪段链路产生故障。

```
<Quidway> tracert 3.1.1.2
 traceroute to 3.1.1.2(3.1.1.2), max hops: 30 ,packet length: 40
 1 1.1.1.2            4 ms  5 ms  5 ms
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
...
```

反馈的信息表明，数据包经由 SwitchB 后无法达到 Router，由此可以判断出 SwitchB 和 Router 之间的链路发生了故障。当 SwitchB 和 Router 之间的链路修复正常后，再次执行步骤 1 和步骤 2，确认后续链路的通畅，直至 SwitchA 与日志主机之间能够正常通信。

----结束

配置文件

无

版权所有 © 华为技术有限公司

10.6 NQA 配置

通过配置 NQA，可以有效的检测网络运行的状态，使用户能够实时采集到各种网络运行指标。

10.6.1 NQA 概述

通过 NQA 概述，用户可以了解到 NQA 的引入及其实现的功能。

随着网络增值业务的开展，用户对 QoS 的相关要求越来越高。为了让用户看到承诺的带宽是否达到需求，网络管理员需要设备侧提供相关的时延、抖动、丢包率等相关的统计参数，以及时了解网络的性能状况。

AC6605 提供 NQA（Network Quality Analysis）功能满足上述需求。

NQA 可以测量网络上运行的各种协议的性能，使网络管理员能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、文件传输速率、FTP 连接时延、DNS 解析时延、DNS 解析错误率等。通过对这些指标进行控制，可以为用户提供不同等级的网络服务。

同时，NQA 也是网络故障诊断和定位的有效工具。

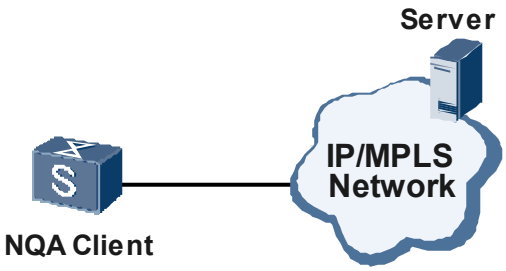
10.6.2 NQA 与 Ping 的比较

通过 NQA 与 Ping 的比较，用户可以了解到 NQA 与 Ping 在测试方式方面的区别。

NQA 是对 Ping 功能的扩展和增强。

Ping 使用 ICMP（Internet Control Message Protocol）测试数据包测试本端和指定目的端之间的往返时间，NQA 不但可以完成这项功能，还可以探测 TCP、UDP、FTP、HTTP、SNMP 服务是否打开，以及测试各种服务的响应时间。如图 10-37 所示。

图 10-37 NQA 测试示意图



与 Ping 不同，NQA 不在控制台终端实时显示每个包的往返时间或是否超时，而是在测试结束后通过 **display nqa results** 命令来查看 NQA 的测试结果。

用户也可以通过网管来设置 NQA 各项操作的参数，并启动测试。

10.6.3 NQA 客户端和服务器

本节介绍到 NQA 客户端、服务器和 NQA 测试例之间的关系。

版权所有 © 华为技术有限公司

NQA 测试例和 NQA 客户端

NQA 可以对多个项目进行测试，每个项目都需要创建一个测试例，且每个测试例只能是某一种类型的 NQA 测试。

NQA 测试例在客户端创建。每个测试例都有一个管理员名称和一个操作标签，管理员名称和操作标签可以唯一确定一个测试例。

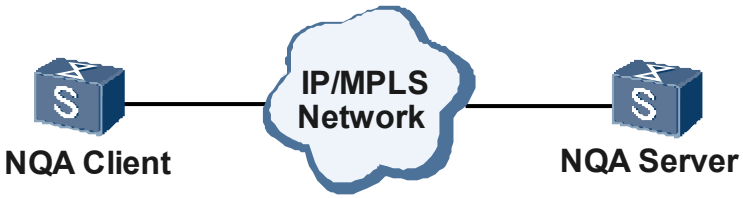
在测试例视图下，需要配置相关的测试参数。其中，有些参数只适用于某种类型的测试例，另外一些则适用于所有类型的测试例。

NQA 服务器

在大多数的测试项中，只需要配置 NQA Client 端。但在进行 TCP、UDP 和 Jitter 类型测试时，必须配置 NQA 服务器。

NQA 服务器负责处理 NQA 客户端发来的测试包，如图 10-38 所示，NQA 服务器通过监听功能对客户端发起的测试进行响应。

图 10-38 NQA 客户端和服务器的关系



可以在一个 NQA 服务器上创建多个 TCP 或 UDP 监听服务，每个监听服务对应一组指定的目的地址和端口号，目的地址和端口号可以重复。

NQA 测试执行

只有在 NQA 服务器上配置了相应的监听地址和端口号后，客户端发起的请求才能得到服务器的响应。并且，服务器监听服务中指定的 IP 地址、端口号要和客户端配置的参数一致。

创建测试例并配置好相关测试项参数之后，必须通过命令 **start** 启动 NQA 测试，并使用 **display nqa results** 命令查看测试结果。

10.6.4 AC6605 支持的 NQA 特性

介绍了 AC6605 支持的 NQA 测试例类型及调度方式。

NQA 提供的特性

- 与网管的配合：
  - 网管可以完全管理 NQA 的所有功能
  - 支持 NQA MIB 用户接口
  - 支持 Disman-traceroute-MIB 用户接口
  - 支持 Disman-NSLookUp-MIB 用户接口

版权所有 © 华为技术有限公司

- 支持 Disman-ping-MIB 用户接口

- Jitter 类型的测试例支持最大连续发送报文数目 3000，可模拟语音业务流量。
- 支持毫秒级统计。
- 支持热备份：

  实现主控板和备板上 NQA 测试例的配置信息同步，发生主备倒换后时，NQA 测试例能正常测试，避免了主备倒换时主控板和备板上的数据不一致。
- 支持测试例的任务调度：

  实现对测试例的调度，降低设备的并发负担。

  对单个测试例，支持多种启动时间、结束时间的设置：

  - 支持立即启动、延迟启动、定时启动
  - 支持报文发送完后自动结束、立即结束、延迟结束、定时结束、生命周期结束

  多个任务同时启动时，设备主动合理分布启动时间和测试间隔。
- 支持自动延时功能。可以最大限度的利用系统的资源，在规定的时间内完成测试例。
- 支持单向延迟统计和双向延迟统计，并且可以通过设定阈值，对测试结果中超过阈值的报文进行统计。
- 支持单向丢包统计。
- 支持灵活告警机制。即，根据被测对象的 OID，为被测对象设置上限和下限阈值，监控被测对象的性能。当测试结果超过阈值时，根据当前事件触发告警。

10.6.5 配置 ICMP 测试

介绍使用 ICMP 测试检测 IP 网络的连通性。

建立配置任务

在配置 ICMP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

ICMP 测试提供类似于普通 **ping** 命令的功能，但输出信息更为丰富。

前置任务

在配置 ICMP 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

数据准备

在配置 ICMP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	目的地址

版权所有 © 华为技术有限公司

序号	数据
3	（可选）VPN 实例名、发送测试报文的源接口、源 IP 地址、Echo Request 报文大小、TTL、ToS、填充字符、测试报文发送间隔、NQA 测试的失败百分比
4	启动方式和结束方式

配置 ICMP 测试参数

在 ICMP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下述配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type icmp**，配置测试例类型为 ICMP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 ICMP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-interface** *interface-type interface-number*，配置发送测试报文的源接口。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。该参数相当于 **ping** 命令中的“**-a**”选项。
- 执行命令 **datasize** *size*，配置 Echo Request 报文的大小，不包括 IP 头。该参数相当于 **ping** 命令中的“**-s**”选项。
- 执行命令 **ttl** *number*，配置 TTL 值。该参数相当于 **ping** 命令中的“**-h**”选项。
- 执行命令 **tos** *value*，配置服务类型，即 IP 报文头中 ToS 字段的值。该参数相当于 **ping** 命令中的“**-tos**”选项。
- 执行命令 **datafill** *fillstring*，配置填充字符。该参数相当于 **ping** 命令中的“**-p**”选项。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。该参数相当于 **ping** 命令中的“**-m**”选项。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

版权所有 © 华为技术有限公司

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在配置 ICMP 测试成功后，可以查看到测试的结果数据。

前提条件

已经完成 ICMP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

执行 **display nqa results** 命令，如果测试已经成功结束，可以看到以下信息。

- testFlag is inactive
- The test is finished
- Completion:success

对于 ICMP 类型的测试，还可以看到接收到响应报文的最小时间、最大时间、RTT（往返时延）。

```
<Quidway> display nqa results
 NQA entry(admin, test) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                 RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.112.58.3
   Min/Max/Average Completion Time: 2/5/3
   Sum/Square-Sum  Completion Time: 9/33
   Last Good Probe Time: 2010-06-21 15:33:09.2
   Lost packet ratio: 0 %
```

10.6.6 配置 FTP 下载测试

介绍使用 NQA 测试 FTP 下载的主要性能指标。

版权所有 © 华为技术有限公司

建立配置任务

在配置 FTP 下载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在 NQA 的 FTP 下载测试中，本地作为 FTP 客户端，从 FTP 服务器下载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

前置任务

在配置 FTP 下载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA FTP 客户端与 FTP 服务器之间路由可达

数据准备

在配置 FTP 下载测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	FTP 服务器的 IP 地址
3	（可选）FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号
4	FTP 用户名和密码
5	要下载的文件名
6	启动方式和结束方式

配置 FTP 下载测试参数

在配置 FTP 下载测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type ftp**，配置测试例类型为 FTP。

版权所有 © 华为技术有限公司

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 FTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置测试例的源地址。
- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **ftp-operation get**，配置操作类型为 Get。

缺省情况下，FTP 操作类型为 Get 操作。

步骤 7 执行命令 **ftp-username** *name*，配置 FTP 用户名。

步骤 8 执行命令 **ftp-password** *password*，配置 FTP 密码。

步骤 9 执行命令 **ftp-filename** *file-name*，配置 FTP 操作文件名。

说明

在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

步骤 10 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 FTP 下载成功后，可以查看到 FTP 下载测试的结果数据。

前提条件

已经完成 FTP 下载测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

版权所有 © 华为技术有限公司

任务示例

对于 FTP 下载测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<Quidway> display nqa results
 NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                                  ResponseProbe:1
   Completion :success                          RTD OverThresholds number: 0
   MessageBodyOctetsSum: 448                    Stats errors number: 0
   Operation timeout number: 0                  System busy operation number:0
   Drop operation number:0                      Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 438/438/438
   DataConnTime Min/Max/Average: 218/218/218
   SumTime Min/Max/Average: 656/656/656
   Average RTT:380
   Lost packet ratio: 0 %
```

10.6.7 配置 FTP 上载测试

介绍使用 NQA 测试 FTP 上载的主要性能指标。

建立配置任务

在配置 FTP 上载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在 NQA 的 FTP 上载测试中，本地作为 FTP 客户端，向 FTP 服务器上载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

进行上载测试时，可以指定要上载的文件，也可以指定要上载的字节数，NQA 客户端自动构造测试文件上载。

前置任务

在配置 FTP 上载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA 客户端与 FTP 服务器之间路由可达

数据准备

在配置 FTP 上载测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	FTP 服务器的 IP 地址

版权所有 © 华为技术有限公司

序号	数据
3	FTP 用户名和密码
4	（可选）FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号
5	要上载的文件名或文件大小
6	启动方式和结束方式

配置 FTP 上载测试参数

在配置 FTP 上载测试参数时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type ftp**，配置测试例类型为 FTP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 FTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置测试例的源地址。
- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **ftp-operation put**，配置操作类型为 Put。

缺省情况下,FTP 的操作类型是 GET。

步骤 7 执行命令 **ftp-username** *name*，配置 FTP 用户名。

步骤 8 执行命令 **ftp-password** *password*，配置 FTP 密码。

步骤 9 指定要上载的文件，有两种方式可以选择。

- 如果要上载指定名称的文件，使用命令 **ftp-filename** *file-name*。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

- 可以不指定文件路径，系统会在当前路径下查找该文件。如果指定的文件名不存在，则按照指定文件名来构造一个文件，上载文件的大小为 1M。
- 文件名不能包含字符：“~、*、/、\、'、"、，”，文件路径可以包含这些字符。
- 文件名中可以包含扩展名，但不能只有扩展名。如.txt。

- 如果要上载指定大小的文件，使用命令 **ftp-filesize** *size*。客户端将自动构建一个名为“nqa-ftp-test.txt”的文件上载。

  说明

  在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

步骤 10 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 FTP 上载测试成功后，可以查看到 FTP 上载测试的结果数据。

前提条件

已经完成 FTP 上载测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** 命令查看测试结果。

----结束

任务示例

对于 FTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<Quidway> display nqa results
```


版权所有 © 华为技术有限公司

```
NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
 1 . Test 1 result   The test is finished
  SendProbe:1                                  ResponseProbe:1
  Completion :success                          RTD OverThresholds number: 0
  MessageBodyOctetsSum: 448                    Stats errors number: 0
  Operation timeout number: 0                  System busy operation number:0
  Drop operation number:0                      Disconnect operation number: 0
  CtrlConnTime Min/Max/Average: 438/438/438
  DataConnTime Min/Max/Average: 218/218/218
  SumTime Min/Max/Average: 656/656/656
  Average RTT:380
  Lost packet ratio: 0 %
```

10.6.8 配置 HTTP 测试

介绍使用 NQA 测试 HTTP 服务各阶段的响应速度。

建立配置任务

在配置 HTTP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 的 HTTP 测试提供三个阶段的响应速度：

- DNS 解析时间：客户端发送 DNS 报文给名字解析器，将 HTTP 服务器名字解析为 IP 地址，DNS 解析报文返回的时间。
- TCP 建立连接时间：客户端与 HTTP 服务器通过 TCP“三次握手”建立连接所用的时间。
- 交易时间：客户端发送 Get 或 Post 报文给 HTTP 服务器，响应报文到达 HTTP 服务器的时间。

前置任务

在配置 HTTP 测试之前，需完成以下任务：

- 配置 HTTP 服务器
- 配置 NQA 客户端与 HTTP 服务器之间路由可达

数据准备

在配置 HTTP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	HTTP 服务器名
3	●（可选）源地址、源端口号 ●（可选）目的端口号 ●（可选）NQA 测试的失败百分比
4	HTTP 操作类型

版权所有 © 华为技术有限公司

序号	数据
5	HTTP 测试所访问的页面和版本信息
6	启动方式和结束方式

配置 HTTP 测试参数

在配置 HTTP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 HTTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type http**，配置测试例类型为 HTTP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 HTTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **http-operation** { **get** | **post** }，配置 HTTP 操作类型。

缺省情况下，HTTP 操作类型为 Get 操作。

步骤 7 执行命令 **http-url** *deststring* [*verstring*]，配置 HTTP 测试所访问的页面以及 HTTP 版本信息。

说明

在不配置 HTTP 版本信息的情况下，缺省情况下支持 HTTP1.0。通过配置可以支持 HTTP1.1。

步骤 8 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。

版权所有 © 华为技术有限公司

- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 HTTP 测试成功后，可以查看到 HTTP 测试的结果数据。

前提条件

已经完成 HTTP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 HTTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段的响应速度。

- DNS 查询时间：DNSRTT
- TCP 连接建立时间：TCPConnectRTT
- 服务器返回数据时间：TransactionRTT、RTT

```
<Quidway> display nqa results
NQA entry (admin, http) :testflag is inactive ,testtype is http
  1 . Test 1 result   The test is finished
    SendProbe:3                          ResponseProbe:3
    Completion:success                   RTD OverThresholdsnumber: 0
    MessageBodyOctetsSum: 411            TargetAddress: 100.2.1.200
    DNSQueryError number: 0              HTTPError number: 0
    TcpConnError number : 0              System busy operation number:0
    DNSRTT Sum/Min/Max:0/0/0             TCPConnectRTT Sum/Min/Max: 6/1/4
    TransactionRTT Sum/Min/Max: 3/1/1
    RTT Sum/Min/Max/Avg: 7/1/5/2
    DNSServerTimeout:0  TCPConnectTimeout:0  TransactionTimeout: 0
    Lost packet ratio:0%
```

10.6.9 配置 DNS 测试

介绍使用 NQA 测试 DNS 解析速度。

建立配置任务

在配置 DNS 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

DNS 测试用于检测将给定的 DNS 名称解析成 IP 地址的速度。

前置任务

在配置 DNS 测试之前，需完成以下任务：

- 配置 DNS 服务器
- 配置 NQA 客户端与 DNS 服务器之间路由可达

数据准备

在配置 DNS 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	DNS 服务器的 IP 地址
3	要解析的目的主机名
4	启动方式和结束方式

配置 DNS 测试参数

在配置 DNS 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 DNS 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能基于 DNS 的动态域名解析功能。

缺省情况下，动态域名解析功能被禁止。

步骤 3 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 4 执行命令 **test-type dns**，配置测试例类型为 DNS。

步骤 5 执行命令 **dns-server ipv4** *ip-address*，配置 DNS 服务器地址的 IPv4 地址。

说明

具体参数配置请参见**配置 NQA 测试例的通用参数**。

步骤 6 执行命令 **destination-address url** *urlstring*，配置目的主机名。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

版权所有 © 华为技术有限公司

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 DNS 测试成功后，可以查看到 DNS 测试的结果数据。

前提条件

已经完成 DNS 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 DNS 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is dns
  1 . Test 1 result   The test is finished
   Send operation times: 1              Receive response times: 1
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.82.55.191
   Min/Max/Average Completion Time: 4/4/4
   Sum/Square-Sum  Completion Time: 4/16
   Last Good Probe Time: 2010-06-21 15:40:12.6
   Lost packet ratio: 0 %
```

10.6.10 配置 Traceroute 测试

介绍使用 NQA 进行 Traceroute 测试，查看网络中每一跳的连通情况。

建立配置任务

在配置 Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

NQA 的 Trcaeroute 测试提供类似于普通 Traceroute 命令的功能，但输出信息更为丰富。

前置任务

在配置 Traceroute 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

数据准备

在配置 Trcaeroute 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	目的地址
3	（可选）：VPN 实例名、允许的最大跳失败数、报文的初始 TTL 和最大 TTL、源地址、目的端口
4	启动方式和结束方式

配置 Traceroute 测试参数

在配置 Traceroute 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type trace**，配置测试例类型为 Traceroute。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置 Traceroute 测试的目的地址。

步骤 5 （可选）根据需要，配置 Traceroute 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **tracert-hopfailtimes** *times*，配置 NQA 测试 Traceroute 测试例的跳失败数。
- 执行命令 **tracert-livetime first-ttl** *first-ttl* **max-ttl** *max-ttl*，配置报文的初始 TTL 和最大 TTL。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

版权所有 © 华为技术有限公司

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 Traceroute 测试成功后，可以查看到 Traceroute 测试的结果数据。

前提条件

已经完成 Traceroute 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 Traceroute 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到每一跳的统计信息。

```
<Quidway> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is trace
  1 . Test 1 result   The test is finished
   Completion:success                  Attempts number:1
   Disconnect operation number:0       Operation timeout number:0
   System busy operation number:0      Connection fail number:0
   Operation sequence errors number:0  RTT Stats errors number:0
   Drop operation number:0
   Last good path Time:2010-06-21 15:41:01.7
   1 . Hop 1
    Send operation times: 3             Receive response times: 3
    Min/Max/Average Completion Time: 1/2/1
    Sum/Square-Sum  Completion Time: 4/6
    RTD OverThresholds number: 0
    Last Good Probe Time: 2010-06-21 15:41:01.7
    Destination ip address:10.112.58.3
    Lost packet ratio: 0 %
```

10.6.11 配置 SNMP 查询测试

介绍使用 NQA 测试主机与 SNMP Agent 之间的通信状况。

版权所有 © 华为技术有限公司

建立配置任务

在配置 SNMP 查询测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

通过 SNMP 查询测试，可以了解主机与 SNMP Agent 之间通信的统计信息。

前置任务

在配置 SNMP 测试之前，需完成以下任务：

- 配置 SNMP Agent
- 配置 NQA 客户端与 SNMP Agent 之间路由可达

数据准备

在配置 SNMP 查询测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	SNMP Agent 的 IP 地址
3	（可选）源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
4	启动方式和结束方式

配置 SNMP 测试参数

在配置 SNMP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type snmp**，配置测试例类型为 SNMP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址，即 SNMP Agent 的地址。

说明

目的地址所指定的机器上必须启动网管功能，否则将收不到回应包。

版权所有 © 华为技术有限公司

步骤 5 （可选）根据需要，配置 SNMP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 SNMP 查询测试成功后，可以查看到 SNMP 查询测试的结果数据。

前提条件

已经完成 SNMP 查询测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 SNMP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results
 NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
  1 . Test 1 result   The test is finished
    Send operation times: 3              Receive response times: 3
    Completion:success                   RTD OverThresholds number: 0
    Attempts number:1                    Drop operation number:0
    Disconnect operation number:0        Operation timeout number:0
    System busy operation number:0       Connection fail number:0
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
Operation sequence errors number:0   RTT Stats errors number:0
Destination ip address:10.2.1.2
Min/Max/Average Completion Time: 63/172/109
Sum/Square-Sum  Completion Time: 329/42389
Last Good Probe Time: 2006-8-5 15:33:49.1
Lost packet ratio: 0 %
```

10.6.12 配置 TCP 测试

介绍使用 NQA 测试 TCP 端口的响应速度。

建立配置任务

在配置 TCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 支持对 TCP 连接指定端口的响应速度测试。

前置任务

在配置 TCP 测试之前，需配置 NQA 客户端与 TCP 服务器之间路由可达。

数据准备

在配置 TCP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	TCP 服务器端监听的 IP 地址和端口号
3	（可选）目的端口号、源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
4	启动方式和结束方式

配置 TCP 服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server tcpconnect** [**vpn-instance** *vpn-instance-name*] *ip-address port-number*，配置 TCP 监听服务。

版权所有 © 华为技术有限公司

----结束

配置 TCP 客户端

在 TCP 客户端配置测试例时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型为 TCP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 （可选）根据需要，配置 TCP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

测试类型 TCP Public 和 TCP Private 的不同之处在于：

- TCP Public 测试固定向目的地址的 7 号 TCP 端口发起连接建立请求，客户端不需要配置目的端口，但要在服务器端监听 7 号 TCP 端口。
- TCP Private 测试需要指定目的端口，并且服务器端要对应监听。

----结束

版权所有 © 华为技术有限公司

检查配置结果

在 TCP 测试成功后，可以查看到 TCP 测试的结果数据。

前提条件

已经完成 TCP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

任务示例

对于 TCP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results
 NQA entry(admin, tcp) :testflag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
    Send operation times: 3                Receive response times: 3
    Completion:success                     RTD OverThresholds number: 0
    Attempts number:0                      Drop operation number:0
    Disconnect operation number:0          Operation timeout number:0
    System busy operation number:0         Connection fail number:0
    Operation sequence errors number:0     RTT Stats errors number:0
    Destination ip address:10.2.1.2
    Min/Max/Average Completion Time: 31/62/51
    Sum/Square-Sum  Completion Time: 155/8649
    Last Good Probe Time: 2006-8-5 15:55:15.3
    Lost packet ratio: 0 %
```

执行 **display nqa-server** 命令，查看 NQA 测试的服务器端状态。

```
<Quidway> display nqa-server
 NQA Server Max: 100            NQA Server Num: 1
 NQA Concurrent TCP Server : 1   NQA Concurrent UDP Server: 0

 nqa-server tcpconnect 10.112.58.3 2000 ACTIVE
```

10.6.13 配置 UDP 测试

介绍使用 NQA 测试 UDP 端口的响应速度。

建立配置任务

在配置 UDP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 支持对 UDP 连接指定端口的响应速度测试。

版权所有 © 华为技术有限公司

前置任务

在配置 UDP 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

数据准备

在配置 UDP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	UDP 服务器端监听的 IP 地址和端口号
3	UDP 客户端发送探测报文的目的地址和目的端口号
4	（可选）：源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
5	启动方式和结束方式

配置 UDP 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server udpecho** [**vpn-instance** *vpn-instance-name*] *ip-address port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

配置 UDP 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

背景信息

请在 NQA 客户器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type udp**，配置测试例类型为 UDP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 （可选）根据需要，配置 UDP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 UDP 测试成功后，可以查看到 UDP 测试的结果数据。

前提条件

已经完成 UDP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

版权所有 © 华为技术有限公司

任务示例

对于 UDP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results
 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 32/109/67
   Sum/Square-Sum  Completion Time: 203/16749
   Last Good Probe Time: 2006-8-5 16:9:21.6
   Lost packet ratio: 0 %
```

执行 **display nqa-server** 命令，查看 NQA 测试的服务器端状态。

```
<Quidway> display nqa-server
 NQA Server Max: 100            NQA Server Num: 1
 NQA Concurrent TCP Server : 0   NQA Concurrent UDP Server: 1

 nqa-server udpecho 10.112.58.3 3000 ACTIVE
```

10.6.14 配置 Jitter 测试

介绍使用 NQA 测试网络的抖动情况。客户端和服务器端都必须是华为设备才能进行 Jitter 测试。

建立配置任务

在配置 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

Jitter 测试的过程如下：

1. 源端以一定的时间间隔向目的端发送数据包。
2. 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。
3. 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

说明

在客户端和服务器端配置 NTP，可以有效提高测试的精度。

版权所有 © 华为技术有限公司

前置任务

在配置 Jitter 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

数据准备

在配置 Jitter 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	UDP 服务器端监听的 IP 地址和端口号
3	UDP 客户端发送探测报文的目的地址和目的端口号
4	（可选）：VPN 实例名、UDP 客户端发送探测报文的源地址、UDP 客户端发送探测报文的源端口号、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号
5	启动方式和结束方式

配置 Jitter 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server udpecho** [**vpn-instance** *vpn-instance-name*] *ip-address port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

配置 Jitter 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

背景信息

说明

系统支持统计 Jitter 测试最大单向延时。

请在 NQA 客户端进行下列配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **nqa-jitter tag-version** *version-number*，配置 Jitter 报文的版本号。

在配置 Jitter 报文的版本号为 2 并配置单向丢包统计后，在测试结果中将可以看到，从源端到目的端、从目的端到源端和未知方向的丢包情况。为网络管理员定位网络故障、检测恶意对网络的攻击提供依据。

步骤 3 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 4 执行命令 **test-type jitter**，配置测试例类型为 Jitter。

步骤 5 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 6 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 7 （可选）根据需要，配置 Jitter 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **probe-count** *number*，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum** *number*，配置每次测试所发送的测试包个数。

  Jitter 测试是对 UDP 报文传输的延时变化进行统计分析。为了提高统计结果的准确性，每一次测试系统都会发送多个测试包。每次测试发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。

  说明

  Jitter 测试的次数取决于 **probe-count** 命令的配置，而每次测试所发送的测试包的个数由 **jitter-packetnum** 命令确定。实际配置时，**probe-count** 命令设置的测试次数与 **jitter-packetnum** 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置发送测试包的时间间隔。

  Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 8 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。

版权所有 © 华为技术有限公司

- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

前提条件

已经完成 Jitter 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

任务示例

对于 Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   Min/Max/Avg/Sum RTT:1/1/1/60          RTT  Square Sum:60
   NumOfRTT:60                           Drop operation number:60
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:1                     Max Positive DS:1
   Positive SD Number:15                 Positive DS Number:1
   Positive SD Sum:15                    Positive DS Sum:1
   Positive SD Square Sum:15             Positive DS Square Sum:1
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:1                     Max Negative DS:1
   Negative SD Number:15                 Negative DS Number:1
   Negative SD Sum:15                    Negative DS Sum:1
   Negative SD Square Sum:15             Negative DS Square Sum:1
   Min Delay SD:0                        Min Delay DS:0
   Avg Delay SD:27                       Avg Delay DS:1
   Max Delay SD:1                        Max Delay DS:1
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 jitter out value:0.0312500
   jitter in value:0.0020833             NumberOfOWD:60
   OWD SD Sum:27                         OWD DS Sum:1
   TimeStamp unit: ms
```

10.6.15 配置 ICMP Jitter 测试

介绍使用 ICMP Jitter 测试测试 IP 网络的抖动情况。

版权所有 © 华为技术有限公司

说明

AC6605 支持 ICMP Jitter 测试。

建立配置任务

在配置 ICMP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

Jitter 测试的过程如下：

- 源端以一定的时间间隔向目的端发送数据包。
- 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。
- 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

在服务器端是非华为设备时，可以通过配置 ICMP Jitter 测试例，测试网络的抖动情况。

前置任务

在配置 ICMP Jitter 测试之前，需配置 NQA 客户端与服务器之间路由可达。

数据准备

在配置 Jitter 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	目的 IP 地址
3	（可选）：VPN 实例名、客户端发送探测报文的源地址、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、超时时间、NQA 测试的失败百分比
4	启动方式和结束方式

配置 ICMP Jitter 测试参数

在配置 ICMP Jitter 测试时，需要配置的相关参数。

版权所有 © 华为技术有限公司

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type icmpjitter**，配置测试例类型为 ICMP Jitter。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 ICMP Jitter 测试其他参数。

- 执行命令 **icmp-jitter-mode** { **icmp-echo** | **icmp-timestamp** }
- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **probe-count** *number*，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum** *number*，配置每次测试所发送的测试包个数。

  说明

  Jitter 测试的次数取决于 probe-count 命令的配置，而每次测试所发送的测试包的个数由 jitter-packetnum 命令确定。实际配置时，probe-count 命令设置的测试次数与 jitter-packetnum 命令设置的测试包个数的乘积不能超过 3000。
- 执行命令 **interval milliseconds** *interval*，配置发送测试包的时间间隔。

  Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

检查配置结果

在 ICMP Jitter 测试成功后，可以查看到 ICMP Jitter 测试的结果数据。

前提条件

已经完成 ICMP Jitter 测试的所有配置。

版权所有 © 华为技术有限公司

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。

操作步骤

- 使用命令 **display nqa results** [**test-instance** *admin-name test-name*]，在 NQA 客户端查看测试结果。

----结束

任务示例

对于 ICMP Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Quidway> display nqa results test-instance admin icmpjitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
 1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion :success                   RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:1/144/12/709      RTT  Square Sum:61007
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:138                   Max Positive DS:3
   Positive SD Number:7                  Positive DS Number:19
   Positive SD Sum:152                   Positive DS Sum:21
   Positive SD Square Sum :19116         Positive DS Square Sum :27
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:21                    Max Negative DS:4
   Negative SD Number:14                 Negative DS Number:19
   Negative SD Sum:152                   Negative DS Sum:22
   Negative SD Square Sum :2796          Negative DS Square Sum :34
   Min Delay SD:1                        Min Delay DS:0
   Max Delay SD:72                       Max Delay DS:71
   Delay SD Square Sum:15111             Delay DS Square Sum:14728
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:5
   Average of Jitter SD:14               Average of Jitter DS:1
   jitter out value:4.7604818            jitter in value:0.5399519
   NumberOfOWD:60                        Packet Loss Ratio: 0%
   OWD SD Sum:339                        OWD DS Sum:310
   ICPIF value: 0                        MOS-CQ value: 0
   TimeStamp unit: ms
```

10.6.16 配置 NQA 测试例的通用参数

介绍一些 NQA 测试常用的测试参数，并说明各个参数都可以应用到哪些测试例中。

建立配置任务

在配置 NQA 测试例的通用参数前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

除了不同测试类型的具体配置参数外，NQA 还提供测试例的通用配置项。

对于本节介绍的通用配置，通常情况下，使用缺省值即可。

版权所有 © 华为技术有限公司

前置任务

在配置 NQA 通用参数之前，需正确创建 NQA 测试例。

配置测试例的通用参数

指明各个测试在具体测试例中的应用。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入已建立的 NQA 测试例的测试例视图。

步骤 3 根据需要，配置测试例通用参数。

- 执行命令 **agetime** *hh:mm:ss*，配置 NQA 测试例的老化时间。
- 执行命令 **datafill** *fillstring*，配置 NQA 测试例的填充字符。

  说明

  不能对 SNMP、TCP、FTP、HTTP、DNS 测试例配置此参数。
- 执行命令 **datasize** *size*，配置 NQA 测试例的报文大小。

  说明

  不能对 SNMP、TCP、FTP、HTTP、DNS 测试例配置此参数。
- 执行命令 **description** *string*，配置测试例描述。
- 执行命令 **destination-address ipv4** *ip-address*，配置 NQA 测试例的目的 IP 地址。
- 执行命令 **destination-address url** *urlstring*，配置 NQA 测试例的目的 url 地址。

  说明

  只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的目的 url 地址。
- 执行命令 **destination-port** *port-number*，配置 NQA 测试例的目的端口号。

  说明

  只能对 UDP、Jitter、TCP、Trace、FTP 和 HTTP 类型的测试例，配置 NQA 测试例的目的端口号。
- 执行命令 **dns-server ipv4** *ip-address*，配置 NQA 测试中 DNS 测试例的 DNS 服务器地址。

  说明

  只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的 DNS 服务器地址。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。

  说明

  不能对 Trace、FTP、DNS 测试配置此参数。
- 执行命令 **frequency** *interval*，配置 NQA 测试例的测试周期。
- 执行命令 **ftp-filename** *file-name*，配置 NQA 测试 FTP 测试例的文件名和文件路径。

版权所有 © 华为技术有限公司

说明

只能对 FTP 类型的测试例，配置 NQA 测试 FTP 测试例的文件名和文件路径。

- 执行命令 **ftp-filesize** *size*，配置 NQA 测试中 FTP 测试例测试的文件大小。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例测试的文件大小。

- 执行命令 **ftp-operation** { **get** | **put** }，配置 NQA 测试中 FTP 测试例的操作类型。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的操作类型。

- 执行命令 **ftp-password** *password*，配置 NQA 测试中 FTP 测试例的用户密码。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的用户密码。

- 执行命令 **ftp-username** *name*，配置 NQA 测试的 FTP 测试例使用的用户名。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试的 FTP 测试例使用的用户名。

- 执行命令 **http-operation** { **get** | **post** }，配置 NQA 测试 HTTP 测试例的测试类型。

  说明

  只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的测试类型。

- 执行命令 **http-url** *deststring* [*verstring*]，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。

  说明

  只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。

- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置 NQA 测试例的报文间隔。

  说明

  只能对 ICMP、UDP、SNMP、Jitter、TCP 类型的测试例，配置 NQA 测试例的报文间隔。

- 执行命令 **jitter-packetnum** *number*，配置 NQA 测试例的测试报文个数。
- 执行命令 **probe-count** *number*，配置一次测试的探针数。

  说明

  不能对 FTP 和 DNS 测试配置此参数。

- 执行命令 **probe-failtimes** *times*，用来配置 NQA 测试例的报文失败数，即，发送 Trap 的阈值。
- 执行命令 **records history** *number*，配置 NQA 测试的最大历史记录数目。
- 执行命令 **records result** *number*，配置 NQA 测试的最大测试结果记录数目。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

  说明

  不能对 DNS 测试配置此参数。

- 执行命令 **set-df**，不允许对报文分片。

  说明

  只能对 Trace 类型的测试例，配置不允许对报文分片。

- 执行命令 **send-trap** { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** } * }，配置 Trap 消息的发送条件。
- 执行命令 **source-address ipv4** *ip-address*，配置 NQA 测试例的源 IP 地址。
- 执行命令 **source-interface** *interface-type interface-number*，配置 NQA 测试例的源接口。

版权所有 © 华为技术有限公司

说明

只能对 ICMP 类型的测试例，配置 NQA 测试例的源接口。

- 执行命令 **source-port** *port-number*，配置本次测试的源端口号。

  说明

  只能对 UDP、SNMP、TCP、FTP 和 HTTP 测试配置此参数。

- 执行命令 **test-failtimes** *times*，配置当 NQA 测试连续测试失败达到一定的次数以后，需要向网管发送 Trap 信息。
- 执行命令 **timeout** *time*，配置测试超时时间。
- 执行命令 **ttl** *number*，配置 NQA 测试例报文中的 TTL 值。

  说明

  不能对 DNS、Trace 测试配置此参数。

- 执行命令 **tos** *value*，配置测试包的服务类型 TOS。

  说明

  不能对 DNS、Trace 测试配置此参数。

- 执行命令 **tracert-hopfailtimes** *times*，配置 NQA 测试 Trace route 测试例的跳失败数。

  说明

  只能对 Trace 测试例配置此参数。

- 执行命令 **tracert-livetime first-ttl** *first-ttl* **max-ttl** *max-ttl*，配置 NQA 测试 Trace 测试例的生存时间。

  说明

  只能对 Trace 测试例配置生存时间。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置 NQA 测试例的 VPN 实例名。

  说明

  不能对 DNS 测试配置此参数。

----结束

检查配置结果

在配置 NQA 测试例的通用参数成功后，可以查看到测试的结果数据。

前提条件

已经完成 NQA 测试例通用参数功能的所有配置。

操作步骤

步骤 1 执行 **display nqa-agent** [*admin-name test-name*] [**verbose**]查看 NQA 测试例配置的通用参数。

----结束

任务示例

```
<Quidway> display nqa-agent
nqa test-instance a a
 test-type pwe3trace
 local-pw-id 1
```


版权所有 © 华为技术有限公司

```
 vc-type bgp
 nqa status : normal
nqa test-instance a b
 test-type icmpjitter
 destination-address ipv4 100.1.1.201
 source-address ipv4 100.1.1.200
 hardware-based enable
 ttl 100
 tos 100
 timeout 20
 nqa status : normal
```

10.6.17 配置 NQA 双向传输延迟阈值

介绍配置 NQA 双向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

建立配置任务

在配置 NQA 双向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

配置测试例的双向传输阈值后，在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

前置任务

在配置 NQA 阈值之前，需完成以下任务：

- 设备运行正常
- 正确创建 NQA 测试例并配置相关参数

数据准备

在配置阈值功能之前，需要准备以下数据。

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	测试例的双向传输延迟阈值

配置双向传输延迟阈值

配置双向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

背景信息

在运行 NQA 测试例的交换机上进行如下配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 视图。

步骤 3 执行命令 **test-type** *test-type*，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5（可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **threshold rtd** *rtd-value*，配置双向传输延迟阈值。

步骤 7 执行命令 **send-trap rtd**，打开阈值 Trap 开关。

----结束

检查配置结果

在配置 NQA 双向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

前提条件

已经完成 NQA 双向传输延迟阈值测试功能的所有配置。

操作步骤

步骤 1 执行 **display nqa-agent** [*admin-name test-name*] [**verbose**]命令查看 NQA 测试例阈值配置。

----结束

任务示例

执行命令 **display nqa-agent verbose**，可以查看 NQA 阈值的配置信息。例如：

```
<Quidway> display nqa-agent verbose
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 100.1.1.201
 destination-port 80
 threshold rtd 2000
 send-trap rtd
 nqa status : normal
```

10.6.18 配置 NQA 测试的 Trap 开关

通过配置 NQA 测试的 Trap 开关可以实现 NQA 测试成功或者失败产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

建立配置任务

在配置 NQA 测试的 Trap 开关前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

版权所有 © 华为技术有限公司

应用环境

NQA 测试成功或者失败都会产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

NQA 支持 DISMAN-PING-MIB 中定义的 3 类 TRAP。

NQA 支持超过单向延迟阈值或超过双向延迟阈值向网管发送 Trap。

- 对于所有的测试例如果双向传输延迟超过设置的阈值时，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。
- 对于 Jitter 类型的测试例如果从源到目的或从目的到源，任意一个方向的传输延迟超过设置的阈值，且 Trap 使能标志为真，则根据配置的网管地址向网管发送 Trap 信息。

Trap 报文包含目的 IP 地址信息、操作状态信息、结果地址信息、最小和最大 RTT、时间总和、已发送探测数、接收到的相应报文数、RTT 平方和，以及最后一次探测成功的时间。

前置任务

在配置 NQA 测试的 Trap 开关之前，需完成以下任务：

- NQA 客户端与网管站之间路由可达
- 正确创建 NQA 测试例并配置相关参数

数据准备

在配置 NQA 测试的 Trap 开关之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	触发 Trap 发送的 NQA 事件类型
3	● 触发 Trap 发送的测试失败次数（可选） ● 触发 Trap 发送的探测失败次数（可选）

配置发送测试失败发送 Trap

在 NQA 测试报文失败后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type** { **jitter** | **icmpjitter** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

版权所有 © 华为技术有限公司

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap testfailure**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

步骤 7 执行命令 **test-failtimes** *times*，配置发送 Trap 的测试失败次数。

缺省情况下，测试失败一次就会发送一条 Trap 信息。

----结束

配置探测失败发送 Trap

在 NQA 测试失败后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type** { **jitter** | **icmpjitter** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap probefailure**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

步骤 7 执行命令 **probe-failtimes** *times*，配置发送 Trap 的探测失败次数。

缺省情况下，探测失败一次就会发送一条 Trap 信息。

----结束

配置探测完成发送 Trap

在 NQA 测试完成后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type** { **jitter** | **icmpjitter** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap testcomplete**，发送 Trap 开关。

版权所有 © 华为技术有限公司

缺省情况下，不发送 Trap 消息。

----结束

配置超过阈值发送 Trap

在 NQA 测试结果超过阈值后，发送 Trap。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type** { **jitter** | **icmpjitter** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap rtd**，打开超过阈值发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

检查配置结果

在配置 NQA 测试的 Trap 开关成功后，可以在 Trapbuffer 中看到告警信息。

前提条件

已经完成 NQA 测试 Trap 开关测试功能的所有配置。

操作步骤

步骤 1 执行命令 **display trapbuffer** [**size** *value*] 查看 NQA 测试例发送的 Trap。

----结束

任务示例

执行命令 **display trapbuffer** [**size** *value*] ，查看产生的告警信息。

例如：

```
<Quidway> display trapbuffer size 2
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
```


版权所有 © 华为技术有限公司

```
Current messages : 11
#May  6 2009 12:54:17 CBB6-PE3 SINDEX/4/INDEXMAP:OID 1.3.6.1.4.1.2011.5.25.110.2.0.1
ShortIFIndexMapTable changed.
#May  6 2009 11:02:37 CBB6-PE3 SRM_BASE/4/ENTITYREGSUCCESS: OID 1.3.6.1.4.1.2011.5.25.129.2.1.18
Physical entity register succeeded.
 (EntityPhysicalIndex=17367040, BaseTrapSeverity=2, BaseTrapProbableCause=70144,
BaseTrapEventType=5, EntPhysicalContainedIn=1677721
6, EntPhysicalName="SRU slot 9", RelativeResource="", ReasonDescription="MPU9")
```

10.6.19 维护 NQA

在测试中需要对测试进行维护时，可以通过重新启动测试例，清空测试结果信息实现对测试例的维护。

重新启动测试例

在测试不成功时，可以在下一个时间段重新启动测试来尝试。

前提条件

在确认需要重新启动测试例的情况下，请在 NQA 视图下执行以下命令。

背景信息



注意

重新启动测试例，将终止正在运行的测试例。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 测试例视图。

步骤 3 执行命令 **restart** 重新启动一条 NQA 测试例。

----结束

清除统计信息

当前的测试统计信息已经保存到 FTP 服务器，可以把相关的测试结果清除。

前提条件

在确认需要清除统计信息时，请在 NQA 视图下执行以下的命令。

背景信息



注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 测试例视图。

步骤 3 使用 **clear-records** 命令清除 NQA 测试例的所有历史统计和结果统计。

----结束

调试 NQA

在测试中遇到问题时，可以针对测试例进行调试。

前提条件

在出现运行故障时，请在用户视图下执行下面的 **debugging** 命令对 NQA 进行调试，查看调试信息，并定位故障的原因。

背景信息

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

操作步骤

步骤 1 使用 **debugging nqa all** 命令打开 NQA 的调试开关。

----结束

10.6.20 配置举例

介绍具体的配置案例。

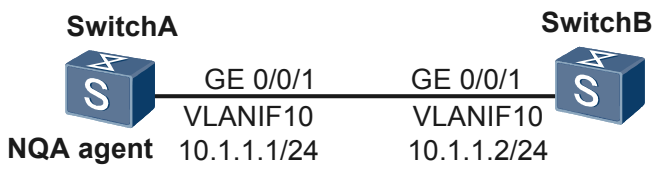
配置 ICMP 测试示例

组网需求

如图 10-39 所示。SwitchA 和 SwitchB 通过 Vlanif 接口实现三层互通。

SwitchA 作为 NQA 客户端，测试 SwitchB 是否可达。

图 10-39 ICMP 测试组网图



版权所有 © 华为技术有限公司

配置思路

1. 使用 NQA ICMP 测试功能，测试报文在本端（SwitchA）和指定的目的端（SwitchB）之间是否可达，以及报文的往返时间。

数据准备

为完成此配置例，需准备如下的数据：

- SwitchB 的主机地址

操作步骤

步骤 1 配置 VLAN，将接口加入到 VLAN

配置 SwitchA

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-Vlan10] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

配置 SwitchB

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 10
[SwitchB-Vlan10] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
```

步骤 2 配置 VLANIF 接口，并且配置 VLANIF 接口的 IP 地址

配置 SwitchA

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
```

配置 SwitchB

```
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 10.1.1.2 24
```

步骤 3 使能 NQA 客户端，配置 ICMP 类型的 NQA 测试例

```
[SwitchA] nqa test-instance admin icmp
[SwitchA-nqa-admin-icmp] test-type icmp
[SwitchA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

步骤 4 立即启动测试

```
[SwitchA-nqa-admin-icmp] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-icmp] display nqa results test-instance admin icmp

 NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
```


版权所有 © 华为技术有限公司

```
Send operation times: 3              Receive response times: 3
Completion:success                   RTD OverThresholds number: 0
Attempts number:1                    Drop operation number:0
Disconnect operation number:0        Operation timeout number:0
System busy operation number:0       Connection fail number:0
Operation sequence errors number:0   RTT Stats errors number:0
Destination ip address:10.1.1.2
Min/Max/Average Completion Time: 1/30/17
Sum/Square-Sum  Completion Time: 51/1301
Last Good Probe Time: 2010-06-09 19:27:48.1
Lost packet ratio: 0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置 FTP 下载速度测试示例

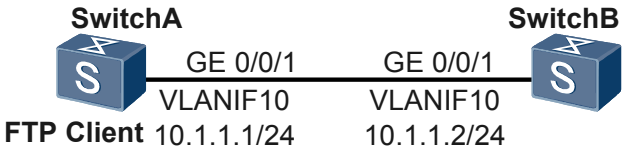
组网需求

如图 10-40 所示。

- SwitchB 作为 FTP Server。
- 登录 FTP 服务器的用户名为 user1，密码为 hello，要下载的文件名为 test.txt。

版权所有 © 华为技术有限公司

图 10-40 FTP 测试组网图



配置思路

为完成此配置例，需准备如下的数据：

1. SwitchA 作为 NQA 客户端。
2. 在 SwitchA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及从 FTP 服务器得到一个文件的时间。

数据准备

为完成 FTP 下载速度测试，需准备如下数据：

- FTP 服务器的 IP 地址
- 进行测试的源 IP 地址
- FTP 用户名和密码
- FTP 测试操作文件

操作步骤

步骤 1 配置 SwitchA 和 SwitchB 的 IP 地址（略）

步骤 2 配置 SwitchB 作为 FTP 服务器

```
<SwitchB> system-view
[SwitchB] ftp server enable
[SwitchB] aaa
[SwitchB-aaa] local-user user1 password cipher hello
[SwitchB-aaa] local-user user1 service-type ftp
[SwitchB-aaa] local-user user1 ftp-directory flash:
[SwitchB-aaa] quit
```

步骤 3 在 SwitchA 上配置 FTP 类型的 NQA 测试例

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin ftp
[SwitchA-nqa-admin-ftp] test-type ftp
[SwitchA-nqa-admin-ftp] destination-address ipv4 10.1.1.2
[SwitchA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[SwitchA-nqa-admin-ftp] ftp-operation get
[SwitchA-nqa-admin-ftp] ftp-username user1
[SwitchA-nqa-admin-ftp] ftp-password hello
[SwitchA-nqa-admin-ftp] ftp-filename test.txt
```

步骤 4 启动测试操作

```
[SwitchA-nqa-admin-ftp] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
```


版权所有 © 华为技术有限公司

```
SendProbe:1                              ResponseProbe:1
Completion :success                      RTD OverThresholds number: 0
MessageBodyOctetsSum: 448                Stats errors number: 0
Operation timeout number: 0              System busy operation number:0
Drop operation number:0                  Disconnect operation number: 0
CtrlConnTime Min/Max/Average: 438/438/438
DataConnTime Min/Max/Average: 218/218/218
SumTime Min/Max/Average: 656/656/656
Average RTT:656
Lost packet ratio:0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.1.1.2
 source-address ipv4 10.1.1.1
 ftp-username user1
 ftp-password hello
 ftp-filename test.txt
 ftp-operation get
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
 FTP server enable
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
 #
return
```

配置 FTP 上载速度测试示例

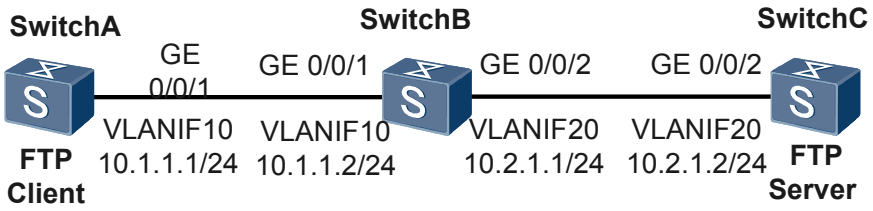
组网需求

如图 **10-41** 所示。

版权所有 © 华为技术有限公司

测试向 FTP Server，即 SwitchC 上载文件的速度。

图 10-41 FTP 测试组网图



配置思路

采用如下思路进行 FTP 上载速度的测试：

1. SwitchA 作为 NQA 客户端和 FTP Client。在 SwitchA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及向 FTP 服务器上载一个文件的时间。
2. 登录 FTP 服务器的用户名为 user1，密码为 hello，构造大小为 10k 的文件上载。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器的 IP 地址
- 进行测试的 FTP 客户端源 IP 地址
- FTP 用户名和密码
- FTP 上载的文件大小

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 配置 SwitchC 作为 FTP 服务器

```
<SwitchC> system-view
[SwitchC] ftp server enable
[SwitchC] aaa
[SwitchC-aaa] local-user user1 password cipher hello
[SwitchC-aaa] local-user user1 service-type ftp
[SwitchC-aaa] local-user user1 ftp-directory flash:
[SwitchC-aaa] quit
```

步骤 3 在 SwitchA 上配置 FTP 类型的 NQA 测试例，构造一个大小为 10k 字节的文件上载

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin ftp
[SwitchA-nqa-admin-ftp] test-type ftp
[SwitchA-nqa-admin-ftp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[SwitchA-nqa-admin-ftp] ftp-operation put
[SwitchA-nqa-admin-ftp] ftp-username user1
[SwitchA-nqa-admin-ftp] ftp-password hello
[SwitchA-nqa-admin-ftp] ftp-filename nqa-ftp-test.txt
[SwitchA-nqa-admin-ftp] ftp-filesize 10
```


版权所有 © 华为技术有限公司

步骤 4 启动测试操作

```
[SwitchA-nqa-admin-ftp] start now
```

步骤 5 验证测试结果

在 SwitchA 上查看 NQA 测试结果。

```
[SwitchA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                          ResponseProb:1
   Completion :success                  RTD OverThresholds number: 0
   MessageBodyOctetsSum: 10240          Stats errors number: 0
   Operation timeout number: 0          System busy operation number:0
   Drop operation number:0              Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 657/657/657
   DataConnTime Min/Max/Average: 500/500/500
   SumTime Min/Max/Average: 1157/1157/1157
   Average RTT:1157
   Lost packet ratio:0 %
```

在 SwitchC 上可以看到增加了一个名为“nqa-ftp-test.txt”的文件。

```
<SwitchC> dir
Directory of flash:

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
   0   -rw-            331  Feb 06 2009 18:34:34   private-data.txt
   1   -rw-          10240  Feb 06 2009 18:37:06   nqa-ftp-test.txt

2540 KB total (1536 KB free)
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.2.1.2
 source-address ipv4 10.1.1.1
 ftp-filesize 10
 ftp-username user1
 ftp-password hello
 ftp-filename nqa-ftp-test.txt
 ftp-operation put
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
```


版权所有 © 华为技术有限公司

```
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

- SwitchC 的配置文件

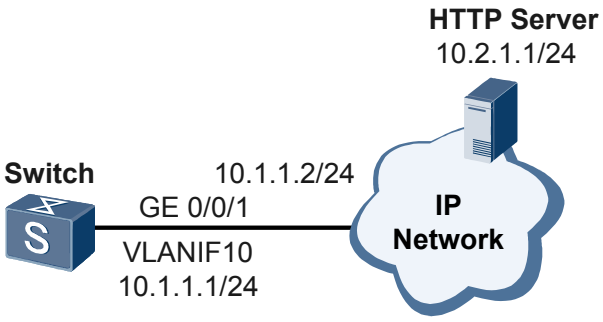
```
#
 sysname SwitchC
#
 FTP server enable
#
vlan batch 20
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

配置 HTTP 测试示例

组网需求

如图 10-42 所示。Switch 通过广域网和 HTTP Server 相连。

图 10-42 HTTP 测试组网图



版权所有 © 华为技术有限公司

配置思路

采用如下思路进行 HTTP 响应速度的测试：

1. Switch 做为 NQA 客户端。
2. 在 Switch 上配置并启动 HTTP 测试例，使用 NQA HTTP 功能测试是否可以和指定的 HTTP 服务器建立连接，以及它们之间传输一个文件的时间。

数据准备

为完成此配置例，需准备如下的数据：

- HTTP Server 的主机地址
- HTTP 测试操作类型

操作步骤

步骤 1 配置 Switch 和 HTTP Server 之间路由可达（略）。

步骤 2 使能 NQA 客户端，配置 HTTP 类型的 NQA 测试例

```
<Quidway> system-view
[Quidway] nqa test-instance admin http
[Quidway-nqa-admin-http] test-type http
[Quidway-nqa-admin-http] destination-address ipv4 10.2.1.1
[Quidway-nqa-admin-http] http-operation get
[Quidway-nqa-admin-http] http-url www.huawei.com
```

步骤 3 启动测试操作

```
[Quidway-nqa-admin-http] start now
```

步骤 4 验证测试结果

```
[Quidway-nqa-admin-http] display nqa results test-instance admin http
 NQA entry(admin, http) :testflag is inactive ,testtype is http
  1 . Test 1 result   The test is finished
   SendProbe:3                          ResponseProbe:3
   Completions: success                 RTD OverThresholdsnumber: 0
   MessageBodyOctetsSum: 0              TargetAddress: 10.2.1.1
   DNSQueryError number: 0              HTTPError number: 0
   TcpConnError number : 3              System busy operation number:0
   DNSRTT Sum/Min/Max:0/0/0             TCPConnectRTT Sum/Min/Max: 0/0/0
   TransactionRTT Sum/Min/Max: 11/3/4
   RTT Sum/Min/Max/Avg: 18/5/7/6
   DNSServerTimeout:0  TCPConnectTimeout:0  TransactionTimeout: 0
   Lost packet ratio:0%
```

----结束

配置文件

Switch 的配置文件

```
#
sysname Quidway
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
```


版权所有 © 华为技术有限公司

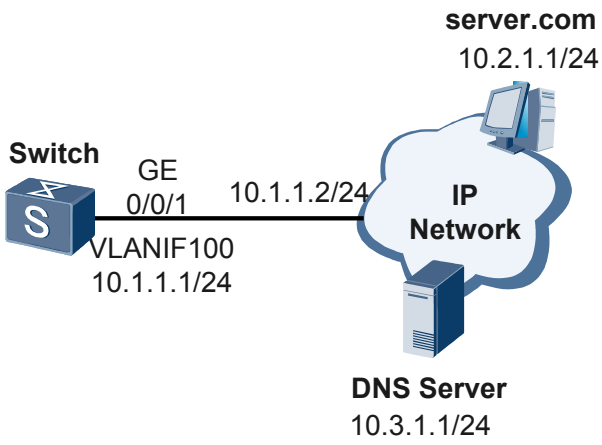
```
 port hybrid untagged vlan 10
#
nqa test-instance admin http
 test-type http
 destination-address ipv4 10.2.1.1
 http-operation get
 http-url www.huawei.com
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

配置 DNS 测试示例

组网需求

如图 10-43 所示，Switch 作为 DNS Client 端，通过域名（server.com）访问 IP 地址为 10.2.1.1/24 的主机。

图 10-43 DNS 测试组网图



配置思路

采用如下思路进行 DNS 解析速度的测试：

1. Switch 作为 NQA 客户端。
2. 在 Switch 上配置并启动 DNS 测试例，测试是否可以和指定的 DNS 服务器建立连接，以及 DNS 地址解析的响应速度。

数据准备

为完成此配置例，需准备如下的数据：

- DNS Server 的 IP 地址
- 要访问的主机名

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 Switch、DNS Server 及所要访问的主机之间网络层可达（略）

步骤 2 配置 DNS 类型的 NQA 测试例

```
<Quidway> system-view
[Quidway] dns server 10.3.1.1
[Quidway] nqa test-instance admin dns
[Quidway-nqa-admin-dns] test-type dns
[Quidway-nqa-admin-dns] dns-server ipv4 10.3.1.1
[Quidway-nqa-admin-dns] destination-address url server.com
```

步骤 3 启动测试操作

```
[Quidway-nqa-admin-dns] start now
```

步骤 4 验证测试结果

```
[Quidway] display nqa results test-instance admin dns

 NQA entry(admin, dns) :testflag is inactive ,testtype is dns
  1 . Test 1 result   The test is finished
   Send operation times: 1              Receive response times: 1
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address: 10.3.1.1
   Min/Max/Average Completion Time: 1/1/1
   Sum/Square-Sum  Completion Time: 1/1
   Last Good Probe Time: 2009-2-3 10:52:5.7
   Lost packet ratio: 0 %
```

----结束

配置文件

Switch 的配置文件

```
#
 sysname Quidway
#
 dns server 10.3.1.1
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin dns
 test-type dns
 destination-address url server.com
 dns-server ipv4 10.3.1.1
#
 ip route-static 10.3.1.0 255.255.255.0 10.1.1.2
#
return
```


版权所有 © 华为技术有限公司

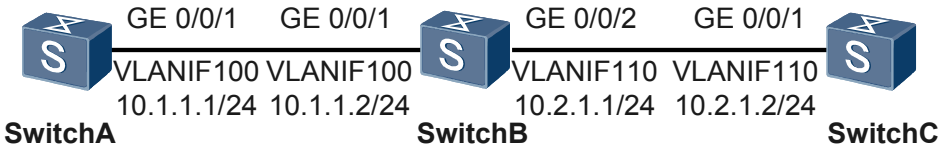
配置 Traceroute 测试示例

组网需求

如图 10-44 所示。

在 SwitchA 上对 SwitchC 接口 Vlanif110 接口的 IP 地址进行 Traceroute 测试。

图 10-44 Traceroute 测试组网图



配置思路

采用如下思路进行 Traceroute 测试：

1. SwitchA 作为 NQA 客户端。
2. 在 SwitchA 上配置并启动 Traceroute 测试例，测试到 SwitchC 的每一跳统计信息。

数据准备

为完成此配置例，需准备如下的数据：

- Traceroute 测试的目的地址。

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 配置在 SwitchA 上 Traceroute 类型的 NQA 测试例，目的地址为 10.2.1.2

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin trace
[SwitchA-nqa-admin-trace] test-type trace
[SwitchA-nqa-admin-trace] destination-address ipv4 10.2.1.2
```

步骤 3 启动测试操作

```
[SwitchA-nqa-admin-trace] start now
```

步骤 4 验证测试结果

在 SwitchA 上查看 NQA 测试结果。

```
[SwitchA-nqa-admin-trace] display nqa results test-instance admin trace
 NQA entry(admin, trace) :testflag is inactive ,testtype is trace
  1 . Test 1 result   The test is finished
   Completion:success                   Attempts number:1
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Drop operation number:0
   Last good path Time:2006-8-5 14:38:58.5
   1 . Hop 1
```


版权所有 © 华为技术有限公司

```
  Send operation times: 3              Receive response times: 3
  Min/Max/Average Completion Time: 46/47/41
  Sum/Square-Sum  Completion Time: 125/5349
  RTD OverThresholds number: 0
  Last Good Probe Time: 2006-8-5 14:38:58.3
  Destination ip address:10.1.1.2
  Lost packet ratio: 0 %
 2 . Hop 2
  Send operation times: 3              Receive response times: 3
  Min/Max/Average Completion Time: 31/79/62
  Sum/Square-Sum  Completion Time: 188/13286
  RTD OverThresholds number: 0
  Last Good Probe Time: 2006-8-5 14:38:58.5
  Destination ip address:10.2.1.2
  Lost packet ratio: 0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin trace
 test-type  trace
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 110
```


版权所有 © 华为技术有限公司

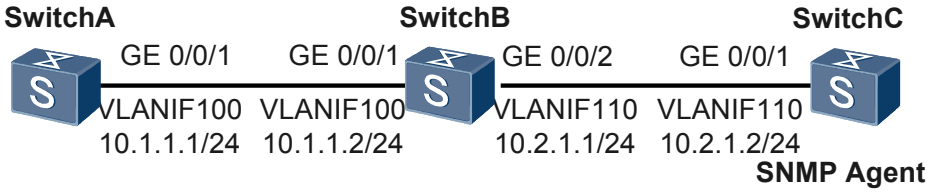
```
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

配置 SNMP Query 测试示例

组网需求

如图 10-45 所示。SwitchC 使能 SNMP Agent，使用 NQA SNMP Query 功能测试从 SwitchA 发出一个 SNMP 协议查询报文到收到响应报文所用的时间。

图 10-45 SNMP Query 测试组网图



配置思路

采用如下思路进行 SNMP Query 测试：

1. SwitchA 作为 NQA 客户端。
2. 在 SwitchA 上创建并启动 SNMP Query 类型的测试例。
3. 在 SwitchC 上使能 SNMP Agent。

数据准备

为完成此配置例，需准备如下的数据：

- SNMP Agent 的主机地址

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 在 SwitchC 上启动 SNMP Agent 功能

```
<SwitchC> system-view
[SwitchC] snmp-agent
```

步骤 3 在 SwitchA 上创建 SNMP 类型的测试例

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin snmp
```


版权所有 © 华为技术有限公司

```
[SwitchA-nqa-admin-snmp] test-type snmp
[SwitchA-nqa-admin-snmp] destination-address ipv4 10.2.1.2
```

步骤 4 启动测试操作

```
[SwitchA-nqa-admin-snmp] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-snmp] display nqa results test-instance admin snmp
 NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
  1 . Test 1 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                      RTD OverThresholds number: 0
   Attempts number:1                       Drop operation number:0
   Disconnect operation number:0          Operation timeout number:0
   System busy operation number:0         Connection fail number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 63/172/109
   Sum/Square-Sum  Completion Time: 329/42389
   Last Good Probe Time: 2006-8-5 15:33:49.1
   Lost packet ratio: 0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin snmp
 test-type snmp
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
```


版权所有 © 华为技术有限公司

```
#
return
```

- SwitchC 的配置文件

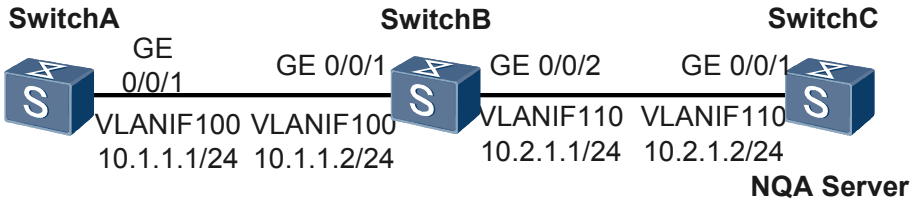
```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100006294
 snmp-agent sys-info version all
#
return
```

配置 TCP 测试示例

组网需求

如图 10-46 所示。使用 NQA TCP Private 功能测试 SwitchA 到 SwitchC 之间建立 TCP 连接的时间。

图 10-46 TCP 测试组网图



配置思路

采用如下思路进行 TCP 测试的配置：

1. SwitchA 做为 NQA 客户端，SwitchC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 TCP 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器主机地址
- 服务器端 TCP 服务的监听端口号

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 在 SwitchC 上配置 NQA 服务器

配置 NQA 服务器 TCP 连接监听的 IP 地址和端口号。

```
<SwitchC> system-view
[SwitchC] nqa-server tcpconnect 10.2.1.2 9000
```

步骤 3 配置 SwitchA

使能 NQA 客户端，配置 TCP Private 类型的测试例。

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin tcp
[SwitchA-nqa-admin-tcp] test-type tcp
[SwitchA-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-tcp] destination-port 9000
```

步骤 4 启动测试

```
[SwitchA-nqa-admin-tcp] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-tcp] display nqa results test-instance admin tcp
 NQA entry(admin, tcp) :testFlag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                     RTD OverThresholds number: 0
   Attempts number:1                      Drop operation number:0
   Disconnect operation number:0          Operation timeout number:0
   System busy operation number:0         Connection fail number:0
   Operation sequence errors number:0     RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 46/63/52
   Sum/Square-Sum  Completion Time: 156/8294
   Last Good Probe Time: 2006-8-5 15:53:17.8
   Lost packet ratio: 0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```


版权所有 © 华为技术有限公司

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- SwitchC 的配置文件

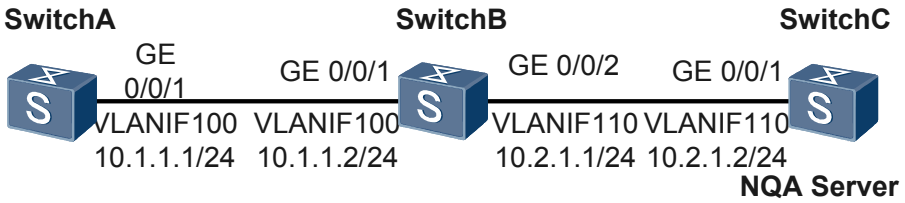
```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 110
 prot trunk allow-pass vlan 110
#
 nqa-server tcpconnect 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

配置 UDP 测试示例

组网需求

如图 10-47 所示。使用 NQA UDP Public 功能测试 SwitchA 与 SwitchC 之间 UDP 协议报文的往返时间。

图 10-47 UDP 测试组网图



版权所有 © 华为技术有限公司

配置思路

1. SwitchA 做为 NQA 客户端，SwitchC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 UDP Public 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端主机地址
- 服务器端 UDP 服务的监听端口号

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 在 SwitchC 上配置 NQA 服务器

配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 10.2.1.2 6000
```

步骤 3 配置 SwitchA

使能 NQA 客户端，配置 UDP Public 类型的测试例。

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin udp
[SwitchA-nqa-admin-udp] test-type udp
[SwitchA-nqa-admin-udp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-udp] destination-port 6000
```

步骤 4 启动测试

```
[SwitchA-nqa-admin-udp] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-udp] display nqa results test-instance admin udp
 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 32/109/67
   Sum/Square-Sum  Completion Time: 203/16749
   Last Good Probe Time: 2006-8-5 16:9:21.6
   Lost packet ratio: 0 %
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 100
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-port 6000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 nqa-server udpecho 10.2.1.2 6000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

配置 Jitter 测试示例

组网需求

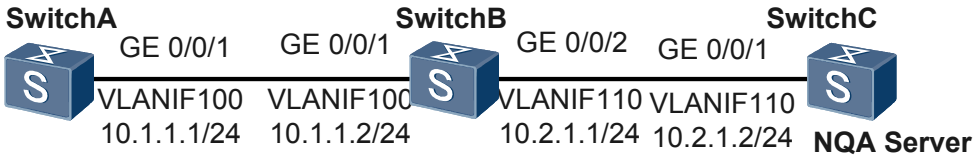
如图 10-48 所示。使用 NQA Jitter 功能测试 SwitchA 与 SwitchC 之间传送报文的抖动时间。SwitchA、SwitchC 通过同步 SwitchB 的时钟来保持时间的同步，从而提升测试精度。

版权所有 © 华为技术有限公司

说明

关于时钟同步介绍请参见《AC6605 无线接入控制器 特性描述 网络管理》的“NTP”。

图 10-48 Jitter 测试组网图



配置思路

采用如下思路进行 Jitter 测试的配置：

1. SwitchC 配置为 NTP 客户端，SwitchB 为 NTP 服务器端。
2. SwitchA 做为 NQA 客户端，SwitchC 做为 NQA 服务器端。
3. 在 NQA 服务器上配置监听服务类型和监听端口号。
4. 在 NQA 客户端配置 Jitter 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址
- 服务器端 UDP 服务的监听端口号

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 在 SwitchC 上配置 NQA 服务器

配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 10.2.1.2 9000
```

步骤 3 配置 SwitchA

使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] test-type jitter
[SwitchA-nqa-admin-jitter] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-jitter] destination-port 9000
```

步骤 4 启动测试操作

```
[SwitchA-nqa-admin-jitter] start now
```

步骤 5 验证测试结果

```
[SwitchA-nqa-admin-jitter] display nqa results test-instance admin jitter

 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
```


版权所有 © 华为技术有限公司

```
1 . Test 1 result   The test is finished
 SendProbe:60                            ResponseProbe:60
 Completion:success                      RTD OverThresholds number:0
 Min/Max/Avg/Sum RTT:1/98/8/461          RTT  Square Sum:23037
 NumOfRTT:60                             Drop operation number:0
 Operation sequence errors number:0      RTT Stats errors number:0
 System busy operation number:0          Operation timeout number:0
 Min Positive SD:1                       Min Positive DS:1
 Max Positive SD:96                      Max Positive DS:8
 Positive SD Number:15                   Positive DS Number:8
 Positive SD Sum:172                     Positive DS Sum:18
 Positive SD Square Sum :9868            Positive DS Square Sum :86
 Min Negative SD:1                       Min Negative DS:1
 Max Negative SD:20                      Max Negative DS:10
 Negative SD Number:18                   Negative DS Number:8
 Negative SD Sum:163                     Negative DS Sum:28
 Negative SD Square Sum :2519            Negative DS Square Sum :194
 Min Delay SD:0                          Min Delay DS:0
 Avg Delay SD:3                          Avg Delay DS:3
 Max Delay SD:49                         Max Delay DS:48
 Packet Loss SD:0                        Packet Loss DS:0
 Packet Loss Unknown:0                   jitter out value:5.1291060
 jitter in value:0.6602845               NumberOfOWD:60
 OWD SD Sum:206                          OWD DS Sum:195
 TimeStamp unit: ms
```

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
  nqa-server udpecho 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

配置 ICMP Jitter 测试示例

组网需求

如图 10-49 所示。

SwitchA 作为 NQA 客户端，测试与 SwitchB 之间网络的抖动情况。

图 10-49 ICMP Jitter 测试组网图



配置思路

采用如下思路进行 ICMP Jitter 测试的配置：

1. SwitchA 做为 NQA 客户端，在 SwitchA 上建立 ICMP Jitter 测试用例。
2. SwitchB 做为 NQA 服务器端。

数据准备

为完成此配置例，需准备如下数据：

- SwitchB 的 IP 地址

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 SwitchA 和 SwitchB 之间可达（略）

步骤 2 配置 SwitchA 的 NQA 测试例

使能 NQA 客户端，配置 ICMP Jitter 测试例。

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin icmpjitter
[SwitchA-nqa-admin-icmpjitter] test-type icmpjitter
[SwitchA-nqa-admin-icmpjitter] destination-address ipv4  10.1.1.2
```

步骤 3 启动测试操作

```
[SwitchA-nqa-admin-icmpjitter] start now
```

步骤 4 验证测试结果

```
[SwitchA-nqa-admin-icmpjitter] display nqa results test-instance admin icmpjitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion :success                   RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:1/3/1/65          RTT  Square Sum:77
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:3                     Max Positive DS:1
   Positive SD Number:18                 Positive DS Number:15
   Positive SD Sum:22                    Positive DS Sum:15
   Positive SD Square Sum :32            Positive DS Square Sum :15
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:2                     Max Negative DS:1
   Negative SD Number:21                 Negative DS Number:14
   Negative SD Sum:22                    Negative DS Sum:14
   Negative SD Square Sum :24            Negative DS Square Sum :14
   Min Delay SD:0                        Min Delay DS:0
   Max Delay SD:1                        Max Delay DS:1
   Delay SD Square Sum:4                 Delay DS Square Sum:1
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:1
   Average of Jitter SD:1                Average of Jitter DS:1
   jitter out value:0.5599658            jitter in value:0.3574005
   NumberOfOWD:60                        Packet Loss Ratio: 0%
   OWD SD Sum:4                          OWD DS Sum:1
   ICPIF value: 0                        MOS-CQ value: 0
   TimeStamp unit: ms
```

----结束

配置文件

- SwitchA 的配置文件

```
#
sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
```


版权所有 © 华为技术有限公司

```
nqa test-instance admin icmpjitter
 test-type icmpjitter
#
return
```

- SwitchB 的配置文件

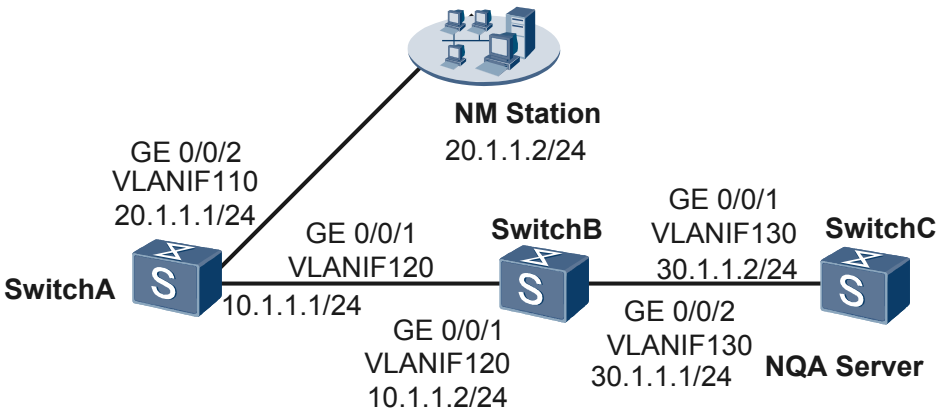
```
#
 sysname SwitchB
#
 vlan batch 10
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

配置向网管端发送 NQA 阈值告警示例

组网需求

如图 10-50 所示在配置 Jitter 测试例时，配置阈值并启动告警功能。启动 Jitter 测试例，在测试结束后，当从 SwitchA 到 SwitchC 或从 SwitchC 到 SwitchA 的测试报文中，有超过设定的单向传输告警阈值，或测试报文的往返时间超过设定的双向传输阈值时，SwitchA 会向网管端发送一次 Trap 消息。通过 NM Station 接收到的 Trap 消息，网络管理人员可以清晰的看到产生告警的原因。

图 10-50 配置 NQA 阈值组网图



说明

关于时钟同步介绍请参见《AC6605 无线接入控制器 特性描述 网络管理》的“NTP”。

配置思路

采用如下思路进行阈值的配置：配置一个 Jitter 测试例

1. 配置 NQA 阈值功能
2. 开启 Trap 发送开关

版权所有 © 华为技术有限公司

3. 配置向网管端发送 Trap

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址及端口号
- 监听服务类型及监听端口号
- RTD 阈值和 OWD 阈值
- 网管端地址

操作步骤

步骤 1 配置 SwitchA、SwitchB 和 SwitchC 之间路由可达（略）

步骤 2 配置一个 Jitter 测试例

在 SwitchC 上配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 30.1.1.2 9000
```

在 SwitchA 上使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] test-type jitter
[SwitchA-nqa-admin-jitter] destination-address ipv4 30.1.1.2
[SwitchA-nqa-admin-jitter] destination-port 9000
```

步骤 3 配置 NQA 阈值功能

在 SwitchA 上配置 RTD 阈值。

```
[SwitchA-nqa-admin-jitter] threshold rtd 20
```

步骤 4 开启发送 Trap 的功能

```
[SwitchA-nqa-admin-jitter] send-trap rtd
[SwitchA-nqa-admin-jitter] quit
```

步骤 5 配置向网管发送 Trap 的功能

```
[SwitchA] snmp-agent trap enable
[SwitchA] snmp-agent sys-info version v2c
[SwitchA] snmp-agent target-host trap address udp-domain 20.1.1.2 params securityname public v2c
```

步骤 6 启动测试操作

```
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] start now
[SwitchA-nqa-admin-jitter] quit
[SwitchA] quit
```

步骤 7 检查配置结果

显示各 Switch 的 NQA 测试结果信息。

```
<SwitchA> display nqa results

NQA entry(test, jitter) :testflag is inactive ,testtype is jitter
 1 . Test 1 result   The test is finished
   Send operation times:3000            Receive response times:3000
   Completion :success                  RTD RTD OverThresholds number:25
   Min/Max/Avg/Sum RTT:1/26/1/3143      RTT  Square Sum:5665
   NumOfRTT:3000                        Drop operation number:0
```


版权所有 © 华为技术有限公司

```
Operation sequence errors number:0   RTT Stats errors number:0
System busy operation number:0       Operation timeout number:0
Min Positive SD:1                    Min Positive DS:0
Max Positive SD:27                   Max Positive DS:0
Positive SD Number:1890              Positive DS Number:0
Positive SD Sum:2128                 Positive DS Sum:0
Positive SD Square Sum :4864         Positive DS Square Sum :0
Min Negative SD:1                    Min Negative DS:1
Max Negative SD:16                   Max Negative DS:2
Negative SD Number:38                Negative DS Number:1936
Negative SD Sum:129                  Negative DS Sum:1998
Negative SD Square Sum :1445         Negative DS Square Sum :2122
Min Delay SD:0                       Min Delay DS:0
Avg Delay SD:0                       Avg Delay DS:0
Max Delay SD:13                      Max Delay DS:12
Packet Loss SD:0                     Packet Loss DS:0
Packet Loss Unknown:0                Average of Jitter:1
Packet Loss Unknown:0                jitter out value:0.7489559
jitter in value:0.6627117            NumberOfOWD:0
OWD SD Sum:81                        OWD DS Sum:62
TimeStamp unit: ms
```

在告警缓冲区检查是否产生 Trap 消息。

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 3

#Jul  9 00:28:34 2009 Quidway  NQA/4/RTDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.16 NQA entry RTD
over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Quidway NQA/4/SDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.17 NQA entry OWD-SD
over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Quidway  NQA/4/DSTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.
18 NQA entry OWD-DS over threshold. (OwnerIndex=admin, TestName=jitter)
```

在网管端查看是否可以正确接收到 Trap 消息。(略)

----结束

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
vlan batch 110 120
#
interface Vlanif110
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 120
 port hybrid untagged vlan 120
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
ospf 1
 area 0.0.0.0
```


版权所有 © 华为技术有限公司

```
  network 10.1.1.0 0.0.0.0
#
nqa test-instance test jitter
 test-type jitter
 destination-address ipv4 30.1.1.2
 destination-port 9000
 threshold rtd 20
 send-trap rtd
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100007B29
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain 20.1.1.2 params securityname public v2c
 snmp-agent trap enable
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
vlan batch 120 130
#
interface Vlanif120
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif130
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 120
 port hybrid untagged vlan 120
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 130
 port hybrid untagged vlan 130
#
ospf 1
 area 0.0.0.1
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
vlan batch 130
#
interface Vlanif130
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 130
 port hybrid untagged vlan 130
#
  nqa-server udpecho 30.1.1.2 9000
#
ospf 1
 area 0.0.0.1
  network 30.1.1.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

10.7 RMON 配置

通过 RMON(Remote Network Monitoring)可以实现对以太接口的监控。

10.7.1 RMON 概述

介绍 RMON 的工作原理。

RMON 概述

RMON 基于简单网络管理协议 SNMP 体系结构实现，与现存 SNMP 框架兼容，包括网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分。

RMON Agent 跟踪统计网络中的各种流量信息，例如，某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。它使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效手段。减少了网管站与代理 Agent 间的通讯流量，从而实现更简单有效地管理大型网络。

RMON 允许有多个监控者，它可用两种方法收集数据。

- 通过专用的 RMON Probe（探测仪）。NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将 RMON Agent 直接嵌入网络设备（例如交换机）中，使它们成为带 RMON Probe 功能的网络设备。NMS 是用 SNMP 基本命令与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。

目前只能对网络设备的以太网接口进行监控和统计。

10.7.2 AC6605 支持的 RMON 特性

本节介绍了 AC6605 对 RMON 的支持。

RMON 特性

AC6605 通过把 RMON Agent 模块直接嵌入网络设备中，与其它模块形成一个完整的系统来实现 RMON。网管工作站 NMS 可以完全利用 SNMP NMS，网络管理人员无须进行额外的学习。

AC6605 RMON 支持 RFC2819 规定的统计、历史、告警和事件四个组以及华为规定的私有扩展告警组（PERFORMANCE-MIB）。下面对这几个组分别进行介绍。

- 统计组

  统计组统计被监控的每个子网的基本统计信息。它能统计某一网段的流量和各种类型包的分布，还能统计各种类型的错误帧数、碰撞次数等。

  统计组包含一个以太网统计表（ethernetStatsTable）。

  说明

  RMON 统计结果与 **display interface** 的显示结果不完全一致，虽然两者都是从底层获取数据，但 RMON 搜集的信息更全面。

- 历史组

  历史组定期收集网络状态统计信息并存储，以便后续的处理。

版权所有 © 华为技术有限公司

历史组包含两个表：

- 历史控制表（historyControlTable）：主要用来设置采样间隔时间等控制信息。
- 以太网历史表（ethernetHistoryTable）：为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

历史控制表中的每一项控制信息在以太网历史表中最多可以有 10 条历史数据相对应，如果超过指定条数，将循环覆盖。

- 告警组

  告警组允许针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值，如果采样数据在相应的方向上越过阈值，监视器会记录日志或者把告警发往网管站。

  按照 RFC2819，告警功能采用一种滞后机制限制告警事件的产生。应用这个机制后，当采样数据以某方向跨过阈值时，将会产生一个事件。直到相反方向的阈值被跨过以前，不会产生更多的事件。

  AC6605 在实现时没有采取这种方式，因为滞后机制可能长时间不会产生告警。在 AC6605 中，只要采样值回到正常阈值后就可以重新告警。

  告警组包括一个告警表（alarmTable）。

- 事件组

  事件组提供关于 RMON 代理所产生的所有事件的表。当某事件发生时，可以记录日志或发送 TRAP 到网管站。

  事件组主要实现 Log、Trap 以及 Log-Trap 三种事件输出，每个日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

  事件组包括事件表（eventTable）和日志表（logTable）。

- 扩展告警组

  扩展告警组在 RFC2819 基础上增加了用表达式设定告警对象和告警生存时间的功能。它包括一个扩展告警表（prialarmTable）。

各表项在 AC6605 中，为节约系统资源，每个表记录都有自己的生存时间，规定了当此行状态不是有效状态 VALID 时，此行可以存在的时间。对于一直处于非 VALID 状态的行，其生存时间将递减。当生存时间为 0 时，行被删除。各表的容量和最大生存时间如**表 10-6** 所示。

表 10-6 各表的生存时间

表名称	表项容量(Byte)	最大生存时间（s）
统计表	100	600
历史控制表	100	600
告警表	60	6000
事件表	60	600
事件日志表	600	-
扩展告警表	50	6000

说明

事件日志表没有最大生存时间，日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

版权所有 © 华为技术有限公司

当有接口板或接口卡被拔出时，接口对应的统计表和历史控制表状态会变成 INVALID 状态，此时，对应的统计表和历史控制表的生存时间被设置为 1200s。如果表记录的生存时间到达 0，该表记录将被删除。

当接口插入时，如果存在对应的表记录，则把对应表记录的行状态变为 VALID，这一表记录成为有效的正常表记录。

10.7.3 配置 RMON

通过配置 RMON 可以实现对于网络状况和流量进行监控。

建立配置任务

在配置 RMON 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

如果要对某一网段的网络状况进行监控、流量统计，可以配置 RMON。

对 RMON 功能的启动时间没有特殊要求，可以预先启动该功能，也可以在怀疑某个接口所连接子网的流量异常时进行配置。

推荐的做法是：预先配置好统计表，对流量有异常的端口配置两条历史控制策略，对某项指标或某几项指标有怀疑时进行告警配置，设定上下阈值，查看告警信息。

说明

RMON 只能提供一些流量统计和异常等信息，并不能防止这些信息尤其是异常情况，要消除异常还需要其它管理手段。

前置任务

在配置 RMON 之前，需完成以下任务：

- 配置以太网接口的参数
- 配置 SNMP 基本功能

数据准备

在配置 RMON 之前，需要准备以下数据：

序号	数据
1	确定要使能统计功能的接口
2	确定要使用的统计表及相关参数
3	确定要使用的历史控制表及相关参数
4	确定要使用的事件表及相关参数
5	确定要使用的告警表及相关参数
6	确定要使用的扩展告警表及相关参数

版权所有 © 华为技术有限公司

使能接口的 RMON 统计功能

需要进行流量统计的接口使能统计功能。如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

背景信息

请在需要进行流量统计的接口进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon-statistics enable**，使能接口的 RMON 统计功能。

如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

----结束

配置统计表

统计表中记录 RMON 收集到的接口流量信息。

背景信息

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon statistics** *entry-number* [**owner** *owner-name*]，配置统计表。

网络管理员监控设备接口的统计信息时，要为相应的接口创建一（表）行，给出接口的 OID、行索引和行的状态。此后，网络管理员可以通过读取本行的方式获取最新统计数据。

----结束

配置历史控制表

历史数据管理功能可以设定对某个接口进行采样、保存数量和采样参数（时间间隔），定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

背景信息

RMON 规范建议每个被监视的接口可以有 2 个以上历史控制条目，间隔 30 秒依次采样一次。

短周期取样使监视器能够探测到流量模式的突变，长周期取样则监视接口的稳定状态行为。

版权所有 © 华为技术有限公司

目前，AC6605 为每个历史控制条目最多保留 10 条最近的记录，超过 10 条将循环覆盖。

说明

为减少 RMON 对系统性能的影响，历史表的采样间隔应在 10 秒以上，且不要对同一端口配置过多的历史控制表项和告警表项。

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]，配置历史控制表。

----结束

配置事件表

通过配置事件表后，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

背景信息

请在需要进行监控的设备上进行如下的配置。

RMON 事件管理在事件表的指定行添加事件，并定义事件的处理方式：

- **log**：只发送日志
- **log-trap**：既发送日志同时也向 NMS 发送 Trap 消息
- **none**：标记为没有事件发生
- **trap**：只向 NMS 发送 Trap 消息

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon event** *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*]，配置事件表。

----结束

配置告警表

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

背景信息

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。事件通常会记录在设备的日志表中，或向 NMS 发送 Trap。

版权所有 © 华为技术有限公司

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警（此时告警记录的状态为 undercreation，不是有效状态 VALID）。

只要事件表中配置了上限和下限其中一个事件，符合条件便会触发相应的告警（告警记录的状态为 VALID）。同理，如果告警变量设置错误，例如设置成一个不存在的 OID，告警记录的状态也为 undercreation，不会正常告警。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon alarm** *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*]，配置告警表。

----结束

配置扩展告警表

RMON 扩展告警表与 RMON 告警表相比增加了用表达式设定告警对象的功能。

背景信息

在 RFC2819 的告警表基础上，RMON 扩展告警管理增加了用表达式设定告警对象的功能，并且可以限定扩展告警行的总生存时间。

扩展告警表比告警表多了以下几项：

- 扩展告警变量的表达式字符串，可以是若干简单告警变量 OID 组成的四则表达式（＋，－，*，/和小括号）。
- 扩展告警行的描述字符串。
- 采样类型为变化率。
- 扩展告警状态类型，包括两种类型：永远（Forever）和限定时间（cycle）。对于 cycle 类型，当经过了扩展告警状态周期指定时间后，不再产生告警并且此表行被删除。

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警。告警记录的状态为 undercreation，不是有效状态 VALID。

只要上限和下限其中一个事件在事件表中配置了，符合条件便会触发相应的告警，告警记录的状态为 VALID。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon prialarm** *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1*

版权所有 © 华为技术有限公司

falling-threshold *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*]，配置扩展告警表。

----结束

检查配置结果

在配置 RMON 功能成功后，可以查看到 RMON 采集的流量信息。

前提条件

已经完成 RMON 功能的所有配置。

操作步骤

- 执行 **display rmon alarm** [*entry-number*]命令查看 RMON 告警信息。
- 执行 **display rmon event** [*entry-number*]命令查看 RMON 事件。
- 执行 **display rmon eventlog** [*entry-number*]命令查看 RMON 事件日志。
- 执行 **display rmon history** [**gigabitethernet** *interface-number*]命令查看 RMON 历史信息。
- 执行 **display rmon prialarm** [*entry-number*]命令查看 RMON 扩展告警表。
- 执行 **display rmon statistics** [**gigabitethernet** *interface-number*]命令查看 RMON 统计消息。

----结束

任务示例

配置成功后，执行命令 **display rmon alarm**，查看告警表的信息。

```
<Quidway> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
Samples  absolute value   : 1.3.6.1.2.1.16.1.1.1.6.1 <etherStatsBroadcastPkts.1>
Sampling interval         : 30(sec)
Rising threshold          : 500(linked with event 1)
Falling threshold         : 100(linked with event 1)
When startup enables      : risingOrFallingAlarm
Latest value              : 1975
```

执行命令 **display rmon event**，查看事件表信息。

```
<Quidway> display rmon event
Event table 1 owned by Test300 is VALID.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.
Event table 2 owned by Test300 is VALID.
  Description: forUseofPrialarm.
  Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.
```

执行命令 **display rmon eventlog**，查看事件记录的日志信息。

```
<Quidway> display rmon eventlog
Event table 1 owned by Test300 is VALID.
  Generates eventLog 1.1 at 0days 00h:39m:30s.
  Description: The 1.3.6.1.2.1.16.1.1.1.6.1 defined in alarm table 1,
     less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

执行命令 **display rmon history**，查看 RMON 历史信息。

```
<Quidway> display rmon history
History control entry 1 owned by Creator is VALID,
  Samples interface     : GigabitEthernet0/0/1<ifEntry.402653698>
  Sampling interval     : 30(sec) with 10 buckets max.
```


版权所有 © 华为技术有限公司

```
  Last Sampling time    : 0days 00h:09m:43s
  Latest sampled values :
  octets              :645       , packets           :7
  broadcast packets   :7         , multicast packets :0
  undersize packets   :6         , oversize packets  :0
  fragments packets   :0         , jabbers packets   :0
  CRC alignment errors :0        , collisions        :0
  Dropped packet:     :0         , utilization       :0
```

执行命令 **display rmon prialarm**，查看 RMON 扩展告警表信息。

```
<Quidway> display rmon prialarm 1
Prialarm table 1 owned by Test300 is VALID.
  Samples delta value       : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 2)
  Falling threshold         : 0(linked with event 2)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever.
  Latest value              : 16
```

执行命令 **display rmon statistics**，查看 RMON 统计信息。

```
<Quidway> display rmon statistics
Statistics entry 1 owned by Test300 is VALID.
  Interface : GigabitEthernet<ifEntry.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersized packets  :0         , oversized packets:0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

10.7.4 维护 RMON

在出现 RMON 运行故障时，请在用户视图下执行中的 **debugging** 命令对 RMON 进行调试，查看调试信息，定位故障并分析故障原因。

背景信息

说明

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 RMON 运行故障时，请在用户视图下执行中的 **debugging** 命令对 RMON 进行调试，查看调试信息，定位故障并分析故障原因。有关 **debugging** 命令的解释请参考《AC6605 无线接入控制器 debugging 参考》。

操作步骤

- 在用户视图下执行命令 **debugging rmon**，打开 RMON 调试开关。

----结束

10.7.5 配置举例

介绍 RMON 和 RMON2 的配置举例。

版权所有 © 华为技术有限公司

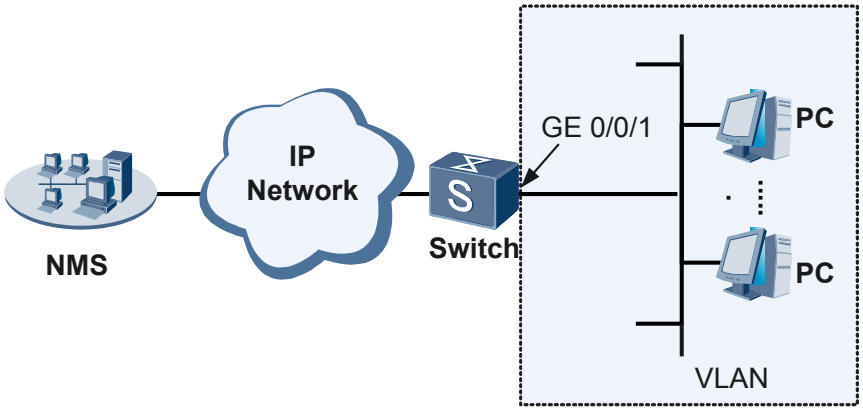
配置 RMON 示例

组网需求

如图 10-51 所示，Switch 设备的 GigabitEthernet0/0/1 接口属于某个 VLAN。要求对以太网接口 GigabitEthernet0/0/1 所连接的网络进行监控，得到广播报文、组播报文和未知单播报文的实时报文数量和历史统计信息。

并且，当 VLAN 内的广播报文、组播报文或未知单播报文的数量异常时，Switch 设备自动向 NMS 上报 Trap 信息。

图 10-51 配置 RMON 组网图



配置思路

本例中需要向网管站发送 Trap 信息，因此需要使用 SNMP 配置命令允许发送 Trap 报文并设置相应的团体名。相关信息请参见“SNMP 配置”。

在 Switch 上需要进行如下配置：使能统计功能并配置统计表、配置历史控制表、配置事件表、配置告警表。

数据准备

为完成此配置例，需准备如下的数据：

- 信息采样时间间隔
- 触发告警事件阈值
- 和网管站之间通信的团体名

配置步骤

1. 配置 Switch 和网管站之间路由可达（略）
2. 配置统计功能

   # 使能 RMON 接口统计功能。

```
<Switch> system-view
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] rmon-statistics enable
```


版权所有 © 华为技术有限公司

配置以太网统计表。

```
[Switch-GigabitEthernet0/0/1] rmon statistics 1 owner User01
```

查看配置效果，了解网络上的数据流量信息。

```
[Switch-GigabitEthernet0/0/1] display rmon statistics gigabitethernet 0/0/1
Statistics entry 1 owned by User01 is VALID.Received  :
  Interface : GigabitEthernet0/0/1<ifEntry.514>
  Received  :
  octets              :156       , packets          :1
  broadcast packets   :0         , multicast packets:1
  undersized packets  :0         , oversized packets:0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):0
  Packets received according to length (octets):
  64     :0         ,  65-127  :0         ,  128-255  :1
  256-511:0         ,  512-1023:0         ,  1024-1518:0
```

3. 配置历史控制表

设置 RMON 对子网中的流量信息进行采样，采样间隔为 30 秒钟，并保存最近 10 次数据。

```
[Switch-GigabitEthernet0/0/1] rmon history 1 buckets 10 interval 30 owner User01
```

查看配置效果。命令行方式只会显示最后一次采样记录，如果要查看所有历史记录，需要使用特定网管站软件。

```
[Switch-GigabitEthernet0/0/1] quit
[Switch] display rmon history gigabitethernet 0/0/1
History control entry 1 owned by User01 is VALID
  Samples interface     : GigabitEthernet0/0/1<ifEntry.514>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 01h:56m:21s
  Latest sampled values :
  octets               :11385     , packets           :0
  broadcast packets    :0         , multicast packets :9
  undersize packets    :0         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
  History record:
  Record No.1 (Sample time: 1days 07h:37m:29s)
  octets               :11182     , packets           :0
  broadcast packets    :0         , multicast packets :8
  undersize packets    :0         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
```

4. 配置事件表

设置 RMON 的 1 号事件处理方式为记录日志。

```
[Switch] rmon event 1 description logevent log owner User01
```

配置 RMON 的 2 号事件处理方式为向网管站发送 Trap 报文，团体名为 public。

```
[Switch] rmon event 2 description prialarmevent trap public owner User01
```

查看配置结果。

```
[Switch] display rmon event
Event table 1 owned by User01 is VALID.
  Description: logevent.
  Will cause log when triggered, last triggered at 0days 00h:00m:00s.
Event table 2 owned by User01 is VALID.
  Description: prialarmevent.
  Will cause snmp-trap when triggered, last triggered at 0days 00h:00m:00s.
```

5. 配置广播报文的告警表

版权所有 © 华为技术有限公司

设置采样广播报文（对应 alarm-OID 为 1.3.6.1.2.1.16.1.1.1.6.1）的时间间隔是 30 秒，当接收到大于或等于 10000 个广播报文时触发事件 1；当接收到小于或等于 100 个广播报文时，触发事件 2。

```
[Switch] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 10000 1 falling-threshold 100 2 owner User01
```

查看配置结果。

```
<Switch> display rmon alarm 1
Alarm table 1 owned by User01 is VALID.
  Samples  absolute value : 1.3.6.1.2.1.16.1.1.1.6.1<etherStatsBroadcastPkts.1>
  Sampling interval       : 30(sec)
  Rising threshold        : 10000(linked with event 2)
  Falling threshold       : 100(linked with event 1)
  When startup enables    : risingOrFallingAlarm
  Latest value            : 0
```

6. 配置组播报文的告警表

设置采样组播报文（对应 alarm-OID 为 1.3.6.1.2.1.16.1.1.1.7.1）的时间间隔是 30 秒，当接收到大于或等于 50000 个组播报文时触发事件 1；当接收到小于或等于 100 个组播报文时，触发事件 2。

```
[Switch] rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold 50000 1 falling-threshold 100 2 owner User01
```

查看配置结果。

```
<Switch> display rmon alarm 2
Alarm table 2 owned by User01 is VALID.
  Samples  absolute value : 1.3.6.1.2.1.16.1.1.1.7.1<etherStatsMulticastPkts.1>
  Sampling interval       : 30(sec)
  Rising threshold        : 50000(linked with event 2)
  Falling threshold       : 100(linked with event 1)
  When startup enables    : risingOrFallingAlarm
  Latest value            : 0
```

7. 配置未知单播报文的告警表

设置采样未知单播报文（对应 alarm-OID 为 1.3.6.1.2.1.2.2.1.12.898）的时间间隔是 30 秒，当接收到大于或等于 1000 个未知单播报文时触发事件 1；当接收到小于或等于 10 个未知单播报文时，触发事件 2。

```
[Switch] rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold 1000 1 falling-threshold 10 2 owner User01
```

查看配置结果。

```
<Switch> display rmon alarm 3
Alarm table 3 owned by User01 is VALID.
  Samples    absolute value : 1.3.6.1.2.1.2.2.1.12.898<ifInNUcastPkts.898>
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 2)
  Falling threshold         : 10(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  Latest value              : 0
```

配置文件

```
#
sysname Switch
#
snmp-agent
 snmp-agent local-engineid 000007DB7F000001000071B6
#
interface GigabitEthernet0/0/1
 rmon-statistics enable
 rmon statistics 1 owner user01
 rmon history 1 buckets 10 interval 30 owner user01
#
 rmon event 1 description logevent log owner User01
```


版权所有 © 华为技术有限公司

```
 rmon event 2 description prialarmeven trap public owner User01
 rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 10000 2 falling-threshold 100 1
owner User01
 rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold 50000 2 falling-threshold 100 1
owner User01
 rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold 1000 2 falling-threshold 10 1
owner User01
#
return
```


版权所有 © 华为技术有限公司

11 无线侧系统管理配置

关于本章

介绍无线侧系统管理配置过程。

11.1 配置用户登录
用户可以通过 Console 口或 Telnet 方式登录交换机，实现对交换机本地或远程维护。

11.2 配置用户界面
配置 Console 用户界面和 VTY 用户界面，实现在本地和远程维护 AC。

11.3 设置启动文件

11.4 重新启动
介绍 AC6605 的重新启动。

11.5 设备升级
介绍 AC6605 设备和 AP 设备的升级。

11.6 查看设备状态
介绍 display 命令以及如何使用 display 命令查看设备运行状态。

11.7 （可选）激活 License
介绍 AC6605 设备 License 的激活方式。

版权所有 © 华为技术有限公司

11.1 配置用户登录

用户可以通过 Console 口或 Telnet 方式登录交换机，实现对交换机本地或远程维护。

11.1.1 用户通过 Console 口登录系统

当用户需要配置第一次上电的 AC6605 或在本地维护 AC6605 时，可以通过 Console 口登录。

背景信息

用户需要根据设备上所配置的 Console 口的物理属性（包括传输速率、数据位、校验方式、停止位、流控方式），来配置终端登录时的相关参数。首次登录设备时，终端属性的各参数值均为设备的缺省值。

操作步骤

步骤 1 在 PC 上打开终端仿真程序（如 Windows XP 的超级终端），如图 11-1 新建一个连接。

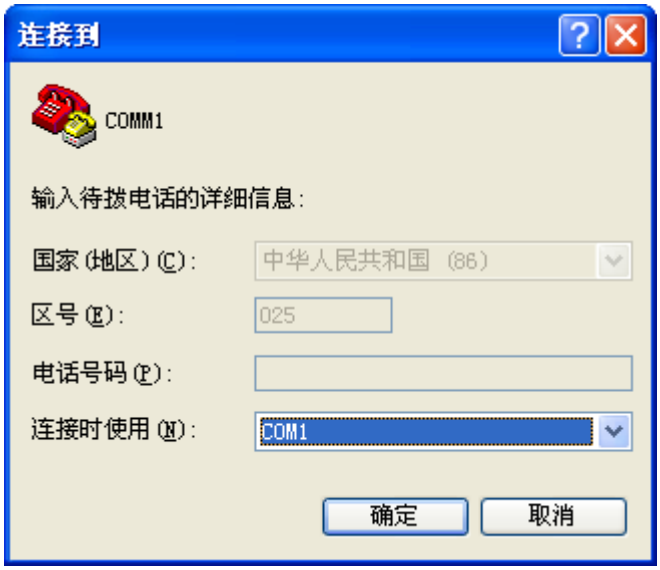
图 11-1 新建连接



步骤 2 设置连接端口，如图 11-2。

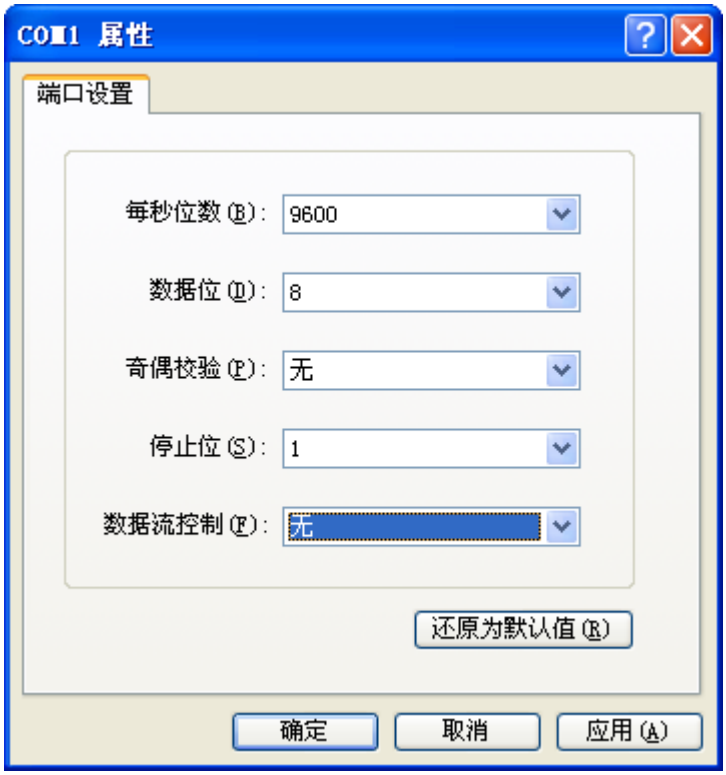
版权所有 © 华为技术有限公司

图 11-2 连接端口设置



步骤 3 设置端口通信参数，与设备的缺省值保持一致，如图 11-3。

图 11-3 端口通信参数设置



步骤 4 按 Enter 键，直到出现用户视图的命令行提示符，如<Quidway>，至此用户进入了用户视图配置环境。

版权所有 © 华为技术有限公司

此时用户可以键入命令，对设备进行配置，需要帮助可以随时键入“?”。

----结束

后续处理

进入用户视图后，可以使用 **display device** 命令来查看登录的是有线侧界面还是无线侧界面。

```
<Quidway> display device
AC6605-26-PWR's Device status:
Slot  Sub Type         Online    Power      Register       Status     Role
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     -   AC6605-26    Present   PowerOn    Registered     Normal     Master
      4   POWER        Present   PowerOn    Registered     Normal     NA
```

如果显示信息如上，表示登录有线侧界面；如果显示信息如下，表示登录无线侧界面。

```
<Quidway> display device
AC6605-AC's Device status:
Slot  Sub Type     Online    Power      Register       Alarm      Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     -   AC6605   Present   PowerOn    Registered     Normal     Master
```

AC6605 的有线侧和无线侧共用一个物理串口。串口登录后按快捷键 Ctrl+Y 可以在无线侧界面和有线侧界面之间切换。快捷键 Ctrl+Y 只能在 Console 口登录时才起作用。按下快捷键 Ctrl+Y 后，显示以下信息：

- Info: Switch console to AC.表示登录到无线侧界面；
- Info: Switch console to LSW.表示登录到有线侧界面。

说明

使用 Console 口登录设备时，登录到有线侧还是无线侧，依赖于设备状态。设备刚刚启动后，默认登录到有线侧；如果在使用过程中有切换，断开过 Console 口的连接，下次重新连接时，登录的还是断开前停留的那一侧。如果无线侧有过单独重启，Console 口会自动切换至与有线侧相连。

11.1.2 用户通过终端 Telnet 登录到系统

当通过 Console 口登录设备完成相关配置后，用户可以使用 Telnet 协议从终端登录到远端设备，实现对设备的远程维护。

操作步骤

步骤 1 配置 VTY 用户界面的用户级别和验证方式。

配置的具体步骤请参见 **11.2.2 配置 VTY 用户界面**

步骤 2 配置客户端登录。

在 PC 上运行 Telnet，如下图所示。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 11-4 PC 上的 Telnet 界面



单击<确定>。

在登录窗口输入用户名和口令，验证通过后，出现用户视图的命令行提示符，如<Quidway>。至此用户进入了用户视图配置环境。

说明

登录交换机前，需要保证 PC 和交换机能够 ping 通，否则无法登录交换机。

----结束

11.1.3 检查配置结果

前提条件

已完成用户通过 Console 口或 Telnet 登录系统的所有配置。

操作步骤

- 用户通过 Console 口登录系统。
  - 使用 **display users** [**all**]命令显示用户界面的使用信息。
  - 使用 **display user-interface console** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。
  - 使用 **display local-user** 命令查看本地用户列表。
  - 使用 **display access-user** 命令查看在线用户。
- 用户通过 Telnet 登录系统。
  - 使用 **display users** [**all**]命令查看用户界面连接情况。
  - 使用 **display telnet server status** 命令查看 Telnet 服务器的状态和配置信息。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

任务示例

- 用户通过 Console 口登录系统。

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Quidway> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  0   CON 0   00:00:44                                 pass           no
Username : Unspecified
```

执行命令 **display user-interface console** *ui-number1* [**summary**]，查看用户界面的物理属性和配置。

```
<Quidway> display user-interface console 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600       -     3     -           N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

执行命令 **display local-user**，可以查看本地用户列表。

```
<Quidway> display local-user
 ------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  admin                          A      H         -
  ------------------------------------------------------------------------------
  Total 1 user(s)
```

- 用户通过 Telnet 登录系统。

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Quidway> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  34  VTY 0   00:00:12  TEL    10.138.77.38                        no
Username : Unspecified
+ 35  VTY 1   00:00:00  TEL    10.138.77.57                        no
Username : Unspecified
```

执行命令 **display telnet server status**，可以看到 Telnet 服务器的状态和配置信息。

```
<Quidway> display telnet server status
Telnet IPV4 server                    :Enable
Telnet IPV6 server                    :Enable
Telnet server port                    :23
```

11.2 配置用户界面

配置 Console 用户界面和 VTY 用户界面，实现在本地和远程维护 AC。

11.2.1 配置 Console 用户界面

配置 Console 用户界面，实现在本地维护 AC。

版权所有 © 华为技术有限公司

操作步骤

- 配置 Console 接口属性。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 console 用户界面视图。
  3. （可选）执行命令 **speed** *speed-value*，设置传输速率。

     缺省情况下，传输速率为 9600bit/s。
  4. （可选）执行命令 **flow-control** { **hardware** | **none** | **software** }，设置流控方式。

     缺省情况下，流控方式为 None。
  5. （可选）执行命令 **parity** { **even** | **mark** | **none** | **odd** | **space** }，设置校验位。

     缺省情况下，校验位为 None。
  6. （可选）执行命令 **stopbits** { **1.5** | **1** | **2** }，设置停止位。

     缺省情况下，停止位为 1bit。
  7. （可选）执行命令 **databits** { **5** | **6** | **7** | **8** }，设置数据位。

     缺省情况下，数据位为 8。

  说明

  当用户通过 Console 接口登录 AC6605 无线侧时，超级终端的上述属性要和 AC6605 无线侧的接口属性保持一致，否则不能登录到 AC6605 无线侧。
- 配置 Console 终端属性。

  用户可以配置 Console 接口的用户超时断连功能、终端屏幕的显示长度或宽度以及历史命令缓冲区大小。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number* ，进入 console 用户界面视图。
  3. 执行命令 **shell**，启动终端服务。
  4. 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

     缺省情况下，用户界面断连的超时时间为 10 分钟。
- 配置用户的优先级。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 console 用户界面视图。
  3. 执行命令 **user privilege level** *level*，设置用户的优先级。

     用户的优先级和命令的优先级是相对应的，即用户只能使用和自己级别相对应的命令。

     命令优先级请参见**命令级别**。
- 配置用户验证方式。

  设置 AAA 验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **quit**，退出 Console 用户界面视图。
  5. 执行命令 **aaa**，进入 AAA 视图。

华为专有和保密信息
版权所有 © 华为技术有限公司

6. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

设置密码验证。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证。
4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置 password 验证的口令。

设置不对用户验证。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
3. 执行命令 **authentication-mode none**，设置用户验证方式为不验证。

----结束

11.2.2 配置 VTY 用户界面

配置 VTY 用户界面，实现在远程维护 AC。

操作步骤

- 配置 VTY 用户界面的最大个数。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface maximum-vty** *number*，配置可以同时登录到交换机的 VTY 类型用户界面的最大个数。

     说明

     当配置 VTY 用户界面最大个数为 0 时，任何用户（包括网管用户）都无法登录到交换机。

     如果要配置的 VTY 用户接口的最大数小于当前的最大数量，则不需要其它配置。

     如果要配置的 VTY 用户接口的最大数量大于当前的最大数量，就需要为新增加的用户接口配置验证方式和密码。因为对于新增用户接口系统默认为使用密码验证。
- 配置 VTY 终端属性。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。
  3. 执行命令 **shell**，启用 VTY 终端服务。
  4. 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。
- 配置用户验证方式。

  设置 AAA 验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **quit**，退出 Console 用户界面视图。

版权所有 © 华为技术有限公司

5. 执行命令 **aaa**，进入 AAA 视图。
6. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

设置密码验证。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证。
4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置 password 验证的口令。

设置不对用户验证。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
3. 执行命令 **authentication-mode none**，设置用户验证方式为不验证。

----结束

11.2.3 检查配置结果

前提条件

已完成 Console 用户界面或 VTY 用户界面的所有配置。

操作步骤

- 配置 Console 用户界面。
  - 使用 **display users** [**all**]命令显示用户界面的使用信息。
  - 使用 **display user-interface console** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。
  - 使用 **display local-user** 命令查看本地用户列表。
  - 使用 **display access-user** 命令查看在线用户。
- 配置 VTY 用户界面。
  - 使用 **display users** [**all**]命令查看用户界面的使用信息。
  - 使用 **display user-interface maximum-vty** 命令查看 VTY 类型用户界面的最大个数。
  - 使用 **display user-interface** [[*ui-type*] *ui-number1* | *ui-number*] [**summary**]命令查看用户界面的物理属性和配置。

----结束

11.3 设置启动文件

11.3.1 配置交换机下次启动时加载的系统软件

用户在升级 AC6605 系统软件等情况时，需要指定 AC6605 下次启动时加载的系统软件。

版权所有 © 华为技术有限公司

背景信息

如果不配置 AC6605 下次启动时加载的系统软件，则 AC6605 下次启动时将默认启动此次加载的系统软件。当需要更改下次启动的系统文件（如设备升级）时，则需要指定下次启动时加载的系统软件。

系统软件文件名必须以“.cc”作为扩展名，而且必须存放在存储设备的根目录下。

说明

此配置只能在有线侧执行。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *system-file* [**slave-board**]，配置 AC6605 下次启动时加载的系统软件。

系统软件的文件名必须以“.cc”作为扩展名，而且必须存放在 Flash 的根目录下。

指定 AC6605 下次启动加载的系统文件时，如果待升级的软件对应的 BOOTROM 版本和当前设备 BOOTROM 版本不一致，设备会自动提醒升级设备 BOOTROM。

----结束

11.3.2 配置交换机下次启动时加载的配置文件

用户在重启设备之前，可以指定 AC6605 无线侧下次启动时加载的配置文件。

背景信息

可以使用 **display startup** 命令查看 AC6605 无线侧是否配置了下次启动时加载的配置文件。如果没有配置，则下次启动采用缺省配置文件。

配置文件的文件名必须以.cfg 或.zip 作为扩展名，而且必须存放在存储设备的根目录下。

AC6605 上电时，默认从 Flash 存储器中读取配置文件进行初始化，因此该配置文件中的配置称为初始配置。如果 Flash 中尚没有配置文件，则交换机用缺省参数初始化。

操作步骤

- 执行 **startup saved-configuration** *configuration-file* 命令，配置 AC6605 无线侧下次启动时加载的配置文件。

----结束

11.3.3 检查配置结果

设置系统启动文件配置成功后，可以查看 AC6605 下次启动时加载的配置文件的内容和设备启动时使用的文件信息。

前提条件

已完成设置系统启动文件的相关配置。

版权所有 © 华为技术有限公司

操作步骤

- 使用 **display current-configuration** [**configuration** [*configuration-type* [*configuration-instance*]] | **controller** | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name* [**filter** *filter-expression*] | **filter** *filter-expression*]命令查看当前配置信息。
- 使用 **display saved-configuration** [**last** | **time** | **configuration**]命令查看交换机下次启动时加载的配置文件的内容。
- 使用 **display startup** 命令查看设备启动时使用的文件信息。

----结束

任务示例

执行命令 **display startup**，可以查看设备启动时使用的文件信息。

```
<Quidway> display startup
MainBoard:
  Configured startup system software:        NULL
  Startup system software:                   NULL
  Next startup system software:              NULL
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg.zip
  Startup paf file:                          default
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

11.4 重新启动

介绍 AC6605 的重新启动。

11.4.1 （可选）通过按键立即重新启动 AC6605

介绍通过按键立即重新启动 AC6605 的注意事项和操作步骤。

背景信息

注意

一般情况下，不要轻易执行此操作，因为它将导致网络在短时间内瘫痪。在通过此操作重新启动 AC6605 时，请确认是否需要保存配置文件，同时确保重新启动时的文件信息正确。有关保存配置文件的操作，请参见《AC6605 无线接入控制器 配置指南-基础配置》。通过按键立即重新启动时，会同时重新启动无线侧和有线侧设备。

请在需要立即重新启动的 AC6605 上进行以下操作。

操作步骤

步骤 1 按动 AC6605 上的“RST”重启按钮，重新启动 AC6605。

----结束

版权所有 © 华为技术有限公司

11.4.2 （可选）通过命令行定时重新启动 AC6605

介绍通过命令行定时重新启动 AC6605 的注意事项和操作步骤。

背景信息

注意

一般情况下，不要轻易使用 **schedule reboot** 命令，因为它将导致网络在短时间内瘫痪。

在通过 **schedule reboot** 命令定时重新启动 AC6605 时，请确认是否需要保存配置文件，同时确保重新启动时的文件信息正确。有关保存配置文件的操作，请参见《AC6605 无线接入控制器 配置指南-基础配置》。

请在需要定时重新启动的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令，使能定时重新启动功能，根据 type 参数取值不同，来设置重新启动时间。

- at time：设置 AC6605 定时重新启动的具体时间。
- delay interval：设置 AC6605 在定时重新启动前等待的时间。

该命令在缺省情况下，只能由级别 3 的用户执行。缺省情况下，未配置重新启动 AC6605 的时间，即未使能定时重新启动功能。

----结束

11.4.3 检查配置结果

通过命令行配置定时重新启动 AC6605 后，可以查看 AC6605 定时重新启动的设置信息。

前提条件

已经完成命令行定时重新启动的配置。

操作步骤

步骤 1 执行命令 **display schedule reboot**，查看 AC6605 定时重新启动的设置信息。

----结束

任务示例

在配置成功时，执行 **display schedule reboot** 命令，可以查看正确配置的 AC6605 定时重新启动的设置信息。

```
<Quidway> display schedule reboot
Info:System will reboot at 00:00:00 2007/10/30 (in 23 hours and 53 minutes).
```


版权所有 © 华为技术有限公司

11.5 设备升级

介绍 AC6605 设备和 AP 设备的升级。

11.5.1 AC 设备升级

介绍 AC6605 升级的注意事项和操作步骤。

背景信息

说明

AC6605 的设备升级只能在有线侧进行。

操作步骤

步骤 1 升级前准备

1. 查看正在运行的系统软件的版本。

```
<Quidway> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.70 (AC6605 V200R001C00)
Copyright (C) 2003-2012 HUAWEI TECH CO., LTD
Quidway AC6605-PWR Routing Switch uptime is 0 week, 1 day, 23 hours, 33 minutes

H852V26S 0(Master) : uptime is 0 week, 1 day, 23 hours, 33 minutes
512M bytes DDR Memory
128M bytes FLASH
Pcb      Version :  VER A
Basic  BOOTROM  Version :  000 Compiled at Feb 10 2012, 17:00:24
CPLD   Version : 258
Software Version : VRP (R) Software, Version 5.70 (V200R001C00)
PWRCARD I information
Pcb      Version : PWR VER A
```

2. 3.3 检查设备运行状态。

```
<Quidway> display device
AC6605-26-PWR's Device status:
Slot  Sub Type         Online    Power      Register       Status     Role
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     -   AC6605-26    Present   PowerOn    Registered     Normal     Master
      4   POWER        Present   PowerOn    Registered     Normal     NA
```

步骤 2 加载系统软件和 Bootrom。

1. 使用 FTP、TFTP 或 Bootrom 系统菜单方式，将 Bootrom 程序和系统软件拷贝到设备存储介质的根目录下。
2. 指定设备启动时加载的系统软件。

```
<Quidway> startup system-software s-s6605-b018.cc
```

说明

如果执行 startup system-software file 命令行时有下面的提示，请选择 Y 更新 BOOTROM，更新成功直接跳到步骤 c，否则需要继续步骤 b 操作。

```
<Quidway> startup system-software s-s6605-b018.cc
Warning: Basic BOOTROM will be upgraded. Continue?(Y/N)[N]: y
Upgrading BOOTROM,please wait for a moment

Info: BOOTROM UPGRADE OK
Info: Succeeded in setting the software for booting system
```


版权所有 © 华为技术有限公司

3. （可选）升级设备启动时加载的 Bootrom

```
<Quidway> upgrade basic-bootrom s-s6605-b018.cc
Warning: Basic BOOTROM will be upgraded. Continue?(Y/N)[N]: y
Upgrading BOOTROM,please wait for a moment

[Slot 0]:
Info: BOOTROM UPGRADE OK.
```

步骤 3 重新启动交换机。

对于是否需要保存配置，请根据需要选择 y 或者 n，设置完成后提示是否需要重新启动设备，请选择 y 重新启动设备。

```
<Quidway> reboot
Info: The system is now comparing the configuration, please wait.
Warning: All the configuration will be saved to the configuration file for the next startup:flash:/
vrpcfg.zip, Continue?[Y/N]:y
Now saving the current configuration to the slot 0.
Info: Save the configuration successfully.
System will reboot! Continue?[Y/N]:      y
Info: system is rebooting ,please wait…
```

----结束

11.5.2 升级 AP 设备

AP 在正常运行之前或 AC 版本变更后，AP 和 AC 协商决定与当前 AC 版本对应的 AP 运行版本，如果版本不匹配，AP 开始升级。

背景信息

AP 支持两种版本升级模式：

- ac-mode：AP 升级时从 AC 上下载升级版本。
- ftp-mode：AC 通过 ap-update ftp-server 命令下发 FTP 配置信息后，由 AP 到 FTP 服务器下载升级版本。

说明

- 预先设置升级模式控制 AP 版本升级方式，ac-mode、ftp-mode 二选一。且处在同时支持同类 AP 最大 128 个并行加载的限制下。
- AP 升级时采用 FTP 模式，须保证版本文件名与版本号一致，否则会导致 AP 不停换包重启。

操作步骤

- 配置 ac-mode 升级模式。

  说明

  使用 TFTP 或者 FTP 方式将指定的升级文件加载到 AC 设备上。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **wlan**，进入 WLAN 视图。
  3. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式为“ac-mode”。
  4. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置与 AP 类型对应的升级文件名。
- 配置 ftp-mode 升级模式。
  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftpusername* | **ftp-password** *ftppassword*] *，配置 FTP 服务器 IP、FTP 客户端用户名、密码。

   说明

   将 AP 升级所需的升级文件存放在 FTP 服务目录下，并确保 AP 与 FTP 服务器网络互通。
4. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式为“ftp-mode”。
5. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置与 AP 类型对应的升级文件名。

----结束

后续处理

- 后续可执行命令 **ap-update multi-load ap-type** *type-id*，按照 AP 类型进行批量 AP 在线升级。
- 升级完成后，需要执行命令 **ap-update multi-reset ap-type** *type-id*，批量复位升级完成的 AP。

11.5.3 检查配置结果

前提条件

已完成用户对 AC6605 或 AP 的升级。

操作步骤

- AC6605 升级
  - 使用 **display startup** 命令查看系统软件是否为目标版本。
  - 使用 **display device** 命令查看单板是否注册正常。
- AP 升级
  - 使用 **display ap all** 命令查看 AP 的状态是否为 normal。

----结束

任务示例

- AC6605 升级

执行命令 **display startup**，可以查看系统软件是否为目标版本。

```
<Quidway> display startup
MainBoard:
  Configured startup system software:        flash:/s-s6605-b018.cc
  Startup system software:                   flash:/s-s6605-b018.cc
  Next startup system software:              flash:/s-s6605-b018.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     flash:/increment_coreln.pat
  Next startup patch package:                flash:/increment_coreln.pat
```


版权所有 © 华为技术有限公司

执行命令 **display device** 命令查看单板是否注册正常。

```
<Quidway> display device
Slot  Sub Type         Online    Power      Register       Status     Role
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     -   AC6605-26    Present   PowerOn    Registered     Normal     Master
      4   POWER        Present   PowerOn    Registered     Normal     NA
```

- AP 升级

执行命令 **display ap all** 命令查看 AP 的状态是否为 normal。

```
<Quidway> display ap all
 AP 0 detail information:
  All AP information:
  ------------------------------------------------------------------------------
  AP     AP                                  Profile  Region  AP
  ID     Type                                ID       ID      State
  ------------------------------------------------------------------------------
  0      WA603SN                             0        0       fault
  1      WA603DN                             0        0       fault
  2      WA633SN                             0        0       normal
  3      WA603SN                             0        0       normal
  4      WA603DN                             0        0       fault
  100    WA603DN                             0        0       fault
  1022   WA603SN                             0        0       fault
  1023   WA603SN                             0        0       fault
  ------------------------------------------------------------------------------
  Total number: 8
```

11.6 查看设备状态

介绍 display 命令以及如何使用 display 命令查看设备运行状态。

11.6.1 查看设备信息

通过 display 命令查看 AC6605 的部件信息。

操作步骤

步骤 1 执行命令 **display device**，查看部件类型及状态信息。

在实际操作中，在任意视图下使用该命令查看设备的部件信息。显示信息包括：部件类型、是否在线、是否加电、是否注册、是否告警以及主备状态。

----结束

11.6.2 查看版本信息

通过 display 命令查看 AC6605 的软件版本、机架类型、主控板及接口板的相关信息。

背景信息

请在需要查看版本信息的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **display version**，查看版本信息。

----结束

版权所有 © 华为技术有限公司

11.6.3 查看诊断信息

通过 display 命令查看多条常用 display 命令的输出信息，可用于系统出现故障时的故障定位。

背景信息

请在需要查看诊断信息的 AC6605 上进行以下配置。

操作步骤

步骤 1 执行命令 **display diagnostic-information**，查看设备上的诊断信息。

诊断信息包括时钟、版本、当前配置文件、保存的配置文件、接口上的物理信息和协议信息、收发报文的统计信息、内存使用状况、系统日志等信息。

说明

由于诊断信息显示内容较多，且不同的设备诊断信息不一样，故这里省略示例。

----结束

11.6.4 显示系统配置信息

当用户需要查看系统配置信息时，可以使用以下命令查看到系统版本、系统时钟、起始配置信息、当前配置信息等信息。

操作步骤

- 执行命令 **display version**，显示系统版本。
- 执行命令 **display clock** ，显示系统时钟。
- 执行命令 **display saved-configuration**，显示起始配置信息。
- 执行命令 **display current-configuration**，显示当前配置信息。

  说明

  - 用户通过查看版本信息可以获知系统当前使用的软件版本相关信息。
  - 起始配置信息是设备上电时进行设备初始化工作的配置文件的信息。当前配置信息是设备运行过程中正在生效的配置信息。具体配置请参见《AC6605 基础配置-配置系统启动》

----结束

11.6.5 显示系统运行状态

当用户需要查看系统运行状态时，可以使用以下命令查看当前视图的运行配置等信息。

操作步骤

- 执行命令 **display this**，显示当前视图的运行配置。

----结束

11.7 （可选）激活 License

介绍 AC6605 设备 License 的激活方式。

版权所有 © 华为技术有限公司

背景信息

License 文件指控制软件版本的容量、功能和时间的授权文件，该文件根据合同信息生成，通过专门的加密工具生成，以电子件形式发放。

AC6605 的 License 是用于控制设备允许接入的最大 AP 数量。用户需要根据实际业务需求购买对应数量资源的 License 文件。

说明

- AC6605 默认开启 License 功能。
- AC6605 默认支持管理 4 个调试 AP，通过购买 License，可支持最多管理 512 个 AP。License 中管理 AP 的数量不会与 4 个调试 AP 叠加。例如 License 支持管理 N 个 AP，加载 License 后 AC6605 只支持 N 个 AP 而不是 N+4 个 AP。
- License 正确激活后，进入 Normal 或 Demo 状态。Normal 或 Demo 状态过期后，进入 Trial 状态。设备在 Trial 状态时可以支持上线最大 AP 数与 Normal 或 Demo 状态相同。Trial 默认为 60 天，60 天后，License 失效，此时强制默认值 4 个 AP 外的其它 AP 下线。Normal 状态对应的是商用 License，Demo 状态对应的是非商用 License。
- 设备正确加载了 License 文件后，允许最大 AP 上线数量按照 License 实际授权数控制。

操作步骤

- 将 License 文件上传到 AC6605 的无线侧。上传方式有三种，具体方式请参考《AC6605 V200R001C00 License 使用指导书》。
  - AC6605 作为 FTP Server；
  - AC6605 作为 FTP Client；
  - AC6605 作为 TFTP Client。
- 执行命令 **license active** *file-name*，激活 License 文件。
- 执行命令 **display license state** ，显示 AC6605 License 状态。

----结束

任务示例

执行命令 **license active** *file-name*，激活 AC 的 License 文件 license.dat。

```
<Quidway> license active license.dat
Info: The License is being activated. Please wait for a
moment.
Info: Succeeded in activating the License file on the master board.
```

执行命令 **display license**，显示 AC 的 License 文件。

```
<Quidway> display license
Info: Active License on master board: flash:/LIC_ON190223_A018409856C_AC6605.dat

 R&D of Huawei Technologies Co., Ltd.

 Product name      : AC6605
 Product version   : V200R001
 License Serial No : LIC20120423008110
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2012-04-23 14:31:53
 Feature name      : ACCESS
 Authorize type    : DEMO
 Expired date      : 2012-07-01
 Trial days        : 60
 Configure items :
 Item name : H85SWLANAC00        value : 1024
```

执行命令 **display license state**，可以查看激活 License 后的信息。

版权所有 © 华为技术有限公司

```
<Quidway> display license state
 Info: Master board license state: Trial. The remain days is 59.
```


版权所有 © 华为技术有限公司

12 WLAN 配置

关于本章

12.1 WLAN 基本业务配置
介绍 AC+瘦 AP 组网模式下的 WLAN 基本业务配置过程。

12.2 WLAN WDS 配置
介绍 WLAN WDS 业务配置过程。

12.3 WLAN 安全配置
介绍 AC+瘦 AP 组网模式下 WLAN 安全特性的配置过程。

12.4 WLAN QoS 配置
介绍 AC+瘦 AP 组网模式下的 QoS 业务配置过程。

版权所有 © 华为技术有限公司

12.1 WLAN 基本业务配置

介绍 AC+瘦 AP 组网模式下的 WLAN 基本业务配置过程。

12.1.1 WLAN 业务简介

本节主要介绍了 WLAN 的概述和组网应用。

WLAN 概述

WLAN(Wireless Local Area Network)无线局域网是指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。它是一种利用无线技术实现快速接入以太网的技术。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。和传统的有线接入方式相比，无线局域网的启动和实施相对简单，维护的成本低廉，一般只要安放一个或多个接入点设备就可建立覆盖整个建筑或地区的局域网络。

WLAN 以无线多址信道作为传输媒介，利用电磁波完成数据交互，实现传统有线局域网的功能。WLAN 技术现在已经广泛的应用在商务区，大学，机场，及其他公共区域。

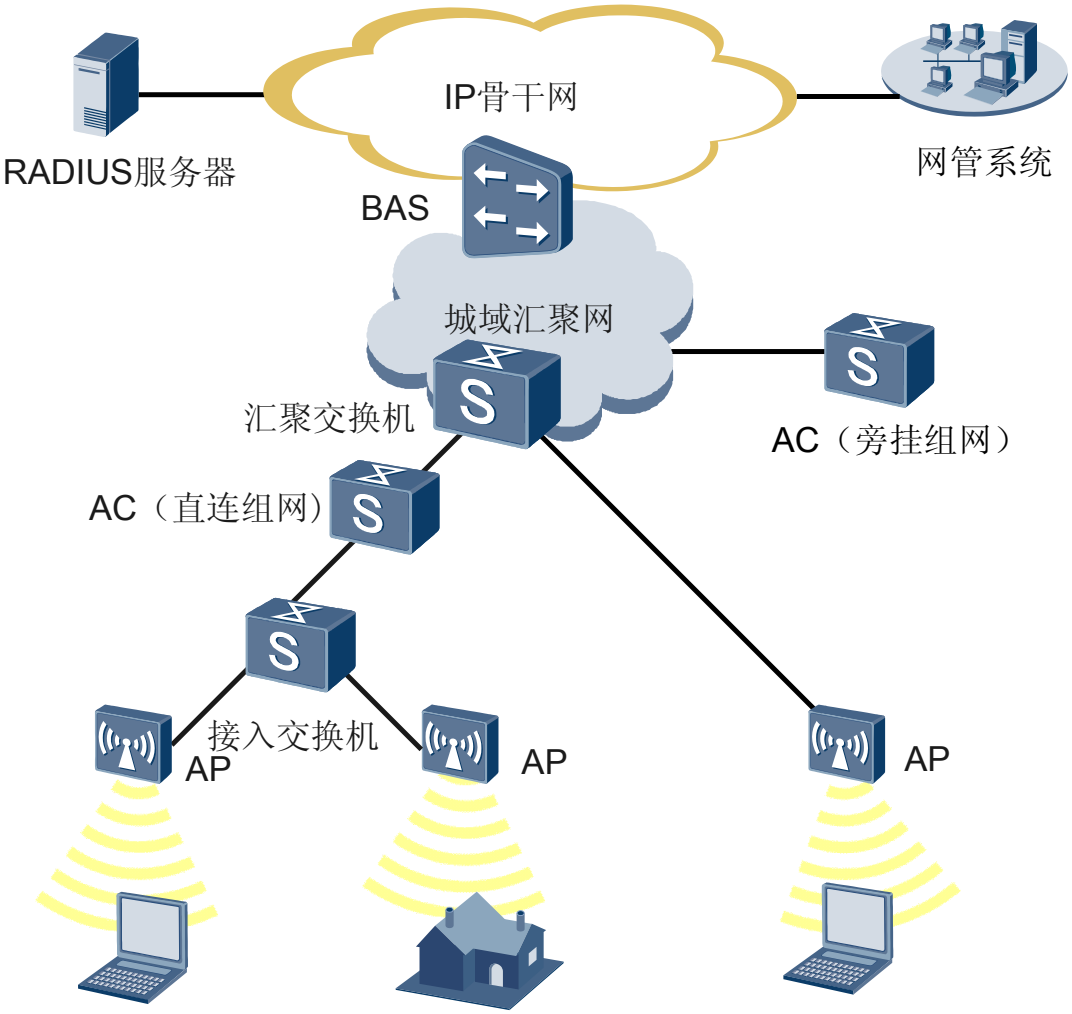
WLAN 组网应用

WLAN 系统不是完全的无线系统，它的服务器和骨干网仍然安置在固定网络，只是用户可以通过无线方式接入网络。

WLAN(AC+瘦 AP)组网模式如图 **12-1** 所示。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 12-1 AC+瘦 AP 组网模式



AP	无线信道数据加密、解密由 AP 完成。 AP 监测无线信息汇聚到 AC，AC 对无线信道进行集中智能管理。
AC	AC 角色由 AC6605 承担。 WLAN 用户关联，无线接入控制和安全由 AC 集中管理。 AP、AC 间建立管理通道，AC 对 AP 集中配置管理，降低维护工作量。
BAS	用户认证计费一般由功能强大的 BAS 负责。
网管系统	通过网管系统管理 AC。
RADIUS 服务器	认证、授权、计费服务器。

无线终端通过 WLAN 接入互联网的数据流主要传输在两段不同传输媒介，即无线终端与 AP 之间的无线链路以及 AP 与 AC 之间的有线链路:

- AP 与 AC 之间的有线链路建立过程可以分为 AP 发现 AC、AP 与 AC 建立 CAPWAP 隧道、AP 加入 AC、AP 版本更新过程、AP 配置更新过程、数据检查过程以及运行状态确定七个步骤。

版权所有 © 华为技术有限公司

1. AP 启动后，通过三种方式发现 AC：分别是单播、组播和广播方式。一般情况下单播方式的 AC 发现可以采用三种方法：DHCP 发现、DNS 发现和静态配置。
   - DHCP 方式：AP 通过 DHCP 报文从 AC 的 IP 地址池中分到 IP 地址。AC 在分配给 AP IP 地址时，采用 OPTION43 携带 AC 的 IP 地址。
   - DNS 方式：AP 通过 DNS 的域名解析获得 AC 的 IP 地址。
   - 静态配置：在 AP 上静态配置 AC 的 IP 地址。
2. AP 根据此 IP 地址与 AC 协商，AP 接收到响应消息后开始与 AC 建立 CAPWAP 隧道，该隧道是采用 DTLS 加密传输 UDP 数据报文。
3. CAPWAP 隧道建立后，AP 与 AC 之间通过发送加入请求消息和加入响应消息进行协商。在协商过程中，AC 会判决是否允许该 AP 加入。
4. AP 根据协商参数判断当前版本是否是最新版本，如果不是最新版本，则 AP 将在 CAPWAP 隧道上开始更新软件版本。AP 在软件版本更新完成后重新启动，重复进行 AC 发现、建立 CAPWAP 隧道、加入过程。
5. 版本更新完成后，AP 向 AC 发送配置状态请求消息，向 AC 通告当前本地配置（天线、射频配置、速率、信道、功率），AC 会立即响应配置状态响应消息，立即更新 AP 请求的配置。
6. 配置更新完成后，AP 会将配置更新的结果通过改变状态请求消息反馈给 AC，AC 根据这个消息获得 AP 上更新结果，并反馈改变状态响应消息。
7. 在以上步骤完成后，AP 进入“normal”状态，开始正常工作。

- 无线终端与 AP 之间的无线链路建立过程可以分为终端扫描 AP、终端在 AP 上认证和终端与 AP 进行关联三个步骤。

1. 无线局域网中多个 AP 定期发送 BEACON 帧，无线终端在每个信道上检测多个设备定期发送的 BEACON 帧后，选择一台 AP 作为 WLAN 接入设备。
2. 无线终端在通过 AP 的 802.11 链路认证后，发送关联请求给 AP。AP 会将关联请求帧转发给 AC，由 AC 决定是否允许此无线终端加入，并发送站点配置请求消息给 AP。
3. 无线终端开始拨号进行 802.1x 认证，与 AP 建立关联关系。

WLAN 基本概念

- STA（无线终端）

  带有无线网卡的 PC 或便携式笔记本电脑等终端。

- AP（Access Point，接入点）

  AP 提供无线终端到局域网的桥接功能，在无线终端与无线局域网之间进行无线到有线和有线到无线的帧转换。

- AC（Access Controller，无线控制器）

  无线控制器对无线局域网中的所有 AP 进行控制和管理。无线控制器还可以通过同认证服务器交互信息，来为 WLAN 用户提供认证服务。

- SSID

  SSID（Service Set Identifier，服务组合识别码），无线终端可以先扫描所有网络，然后选择特定的 SSID 接入某个指定无线网络。

- 无线介质

  无线介质是用于在无线用户间传输帧的介质。WLAN 系统使用无线射频作为传输介质。

版权所有 © 华为技术有限公司

- 服务集（Service-Set）

  服务集是 WLAN 业务参数的集合，用户可以预先配置多个服务集，然后将其绑定到 AP 的某个射频上，实现 WLAN 业务的快速配置和下发。

- VAP（Virtual Access Point，虚拟接入点）

  VAP 是 AP 上的业务功能实体。用户可以在 AP 的每个射频上创建不同的 VAP，通过为 AP 的指定射频绑定服务集，就可以创建 VAP。

12.1.2 AC6605 支持的 WLAN 特性

AC6605 支持的特性包括 AC 管理、AP 管理、WLAN 射频管理、WLAN 用户接入安全管理和 WLAN QoS 管理。

AP 管理

AP 上电后缺省配置为空，AC6605 作为 AC，下发 WLAN 业务配置至 AP。

AC6605 支持三种方式建立 AP 与 AC 互通，分别为：

- 离线增加 AP：AP 离线，在 AC 上预先配置好 AP 的各项属性（AP ID、AP 类型、AP MAC/SN、AP 模板、AP 域等），AP 就能够自动上线。
- 自动发现 AP 并正常上线：用户配置好 AP 白名单和 AP 认证方式，当 AP 与 AC 连接时，合法的 AP 能够正常上线。
- 自动发现 AP 并确认上线：用户配置好 AP 认证方式，一个不在白名单中的 AP 上线后，会被记录到未授权的 AP 列表中。需要用户手工确认后，此 AP 才能正常上线。

WLAN 射频管理

成功部署 WLAN 网络后，由于无线环境的不断变化，移动障碍物的存在，或者其他射频信号的干扰都会对无线信号传播质量造成影响。

此时，AP 的信道、发射功率必须能够动态调整以适应用户环境的变化。而人工完成这个调整过程成本太高，所以在 WLAN 系统中，AC 负责完成无线射频资源管理。

AC6605 支持通过射频模板进行 WLAN 射频管理。

WLAN 用户接入安全管理

无线局域网由于信道开放的特点，使得攻击者能够很容易的进行窃听，恶意修改并转发。为了更好的防止未授权用户接入网络，WLAN 提供了一些安全策略。根据安全级别的不同，可以选择不同的安全策略。

AC6605 支持通过安全模板进行用户接入安全管理，支持 WEP、WPA/WPA2、WAPI 四种安全策略。

WLAN QoS 管理

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

AC6605 支持通过创建 WMM 模板，流量模板和配置用户优先级、用户 CAR 进行 QoS 控制。

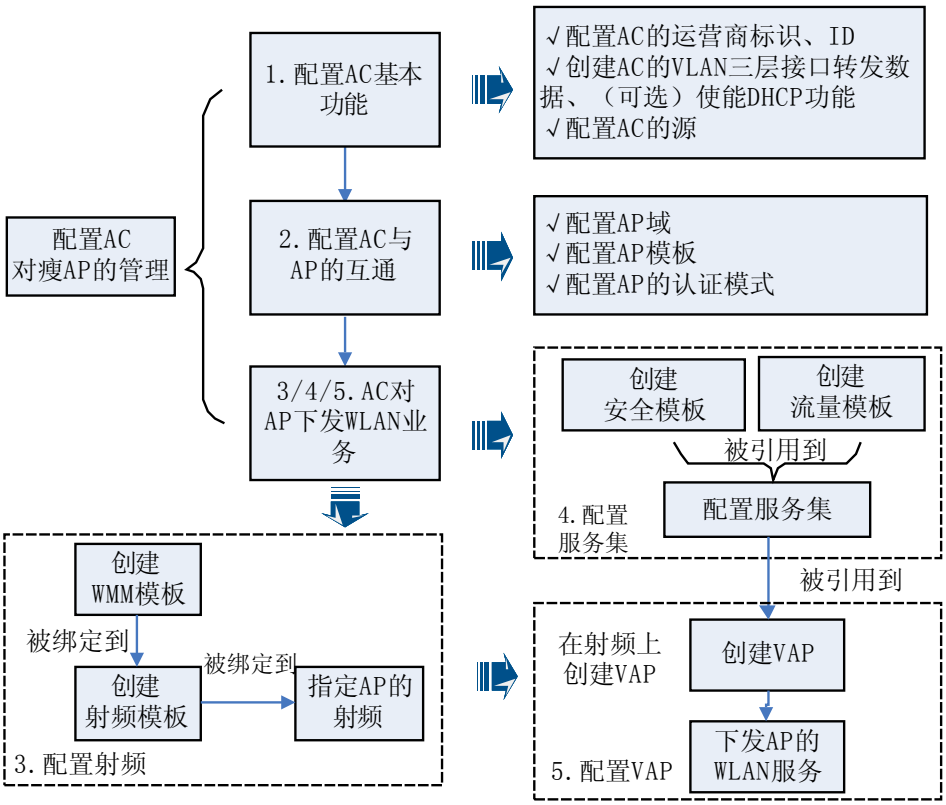
版权所有 © 华为技术有限公司

WLAN 业务配置流程

WLAN 业务的配置流程如图 12-2 所示，可以分为 5 个部分：

1. AC 基础配置
2. 配置 AC 与 AP 的互通
3. 配置 AP 的射频
4. 配置 AP 的服务集
5. 配置 VAP，下发 WLAN 服务

图 12-2 WLAN 业务的配置流程



12.1.3 配置 AC 基本功能

配置 AC 的基本功能，包括 AC ID、运营商标识、国家码标识和 AC 的源接口等。

应用环境

AC 作为无线控制器，负责 AP 的集中管理及 WLAN 用户的无线接入和安全控制。配置 AC 基本功能完成后，AP 才可以与 AC 互通，从而进行后续的 WLAN 业务部署。

数据准备

在配置 AC 基本功能之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	AC ID、AC 的运营商标识、国家码标识
2	（可选）配置 AC 作为 DHCP 服务器：VLANIF 接口编号、地址池网段
3	AC 的源接口编号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan ac-global ac id** *ac-id* **[carrier id** { **cmcc** | **ctc** | **cuc** |**other** }]，配置 AC ID，同时可以配置 AC 的运营商标识。

在实际应用中，为了便于管理，用户需要为每个 AC 配置 AC ID 和运营商标识。

缺省情况下，AC ID 为 0，运营商标识为 **other**。

说明

如果此命令中已经配置了运营商标识，则跳过步骤**步骤 3**。

步骤 3 执行命令 **wlan ac-global carrier id** { **cmcc** | **ctc** | **cuc** | **other** } [**ac id** *ac-id*]，配置 AC 的运营商标识。

目前运营商标识有四家：cmcc/中国移动、ctc/中国电信、cuc/中国联通、other/其他。

步骤 4 执行命令 **wlan ac-global country-code** *country-code*，配置 AC 的国家码标识。

步骤 5 （可选）执行以下命令，配置 AC 作为 DHCP 服务器，AP 从 AC 上获取 IP 地址功能。

1. 执行命令 **dhcp enable**，使能 DHCP 功能。
2. 执行命令 **interface vlanif vlanif** *vlan-id*，创建 VLANIF 接口；或者执行命令 **interface loopback number**，创建 Loopback 接口。

   说明

   执行本命令前，需要确认该 VLAN 已存在。
3. 执行命令 **ip address**，配置给 AP 分配地址的地址池网段。
4. 执行命令 **quit**，返回系统视图。

AP 需要获取一个 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。此处配置 AC 为 DHCP 服务器，AP 从 AC 上获取 IP 地址。

步骤 6 执行命令 **wlan**，进入 WLAN 视图。

步骤 7 执行命令 **wlan ac source interface** { **LoopBack** *loopback-num* | **Vlanif** *vlan-id* }，配置 AC 的源接口。

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

----结束

版权所有 © 华为技术有限公司

操作结果

执行命令 **display wlan ac-global**，查看配置的 AC 信息。

12.1.4 配置 AP 与 AC 互通

配置 WLAN 业务前，AP 与 AC 能够互通是基础。AP 上线有三种方式：离线增加 AP 并配置上线、自动发现 AP 并正常上线和自动发现 AP 并确认上线。

建立配置任务

在配置 AP 与 AC 互通前了解 AP 与 AC 互通的应用环境、前置任务和数据准备。

应用环境

AP 与 AC 能够互通是 WLAN 业务可以部署的基础。AP 与 AC 间可以是直接连接，也可以是二、三层网络拓扑。

AP 上线有三种方式：离线增加 AP 并配置上线、自动发现 AP 并正常上线和自动发现 AP 并确认上线。

AP 离线增加上线和自动发现上线的区别在于：

- 离线增加 AP 时，需要提前知道 AP 的 MAC 或 SN 等信息，可以修改 AP 的缺省配置，这样 AP 上线后将采用离线配置的数据进行工作。
- 自动发现 AP 时，不需要提前知道 AP 的 MAC 或 SN 等信息，AP 采用缺省的配置上线。

前置任务

在配置 AP 与 AC 互通之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

数据准备

在配置 AP 与 AC 互通之前，需准备以下数据。

序号	数据
1	（可选）AP 新类型的名称、AP 新类型 ID
2	AP 升级文件名称、升级文件对应的 AP 类型 ID
3	（可选）FTP 服务器 IP 地址、FTP 客户端用户名/密码
4	AP ID、AP 类型 ID 或 AP 类型名称、AP MAC 地址、AP SN 编号
5	（可选）AP 域 ID
6	（可选）AP 模板名称、AP 模板 ID、MTU 值、日志服务器 IP 地址

版权所有 © 华为技术有限公司

离线增加 AP 并配置上线

离线添加 AP 后，合法的 AP 将正常上线。

前提条件

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

背景信息

离线增加的 AP，可以预先配置 AP 的类型、SN 或 MAC，当实际 AP 上线后，如果和离线增加的 AP 的类型、SN 或 MAC 匹配，则 AP 直接进入工作状态，能够正常提供 WLAN 业务。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* } *，配置新的 AP 类型。

缺省情况下，系统预置了几种缺省支持的 AP 设备类型，包括：WA601、WA631、WA603SN、WA603DN、WA653SN、WA633SN、WA603DE、WA653DE、SRG1201GW、AP6010SN-GN、AP6010DN-AGN、AP6310SN-GN、AP6510DN-AGN、AP6610DN-AGN、WA705DN-AGN、AP7110DN-AGN。

步骤 4 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式。

预先设置升级模式控制 AP 版本升级方式，ac-mode、ftp-mode 二选一。系统缺省升级模式为 ac-mode。

步骤 5 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id* ，配置 AP 升级对应的升级文件。

- 当升级模式为 ac-mode 时，需要将 AP 升级文件上载到 AC 中。
- 当升级模式为 ftp-mode 时，执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftpusername* | **ftp-password** *ftppassword*] *，配置 FTP 服务器 IP、客户端用户名、密码。

步骤 6 执行命令 **ap id** *ap-id* [{ **type-id** *type-id* | **ap-type** *ap-type* } { **mac** *ap-mac* | **sn** *ap-sn* } *]，离线增加一个 AP。

离线增加 AP 时，需要指定 AP 设备类型、MAC 或 SN。

步骤 7 （可选）执行命令 **region-id** *region-id*，将增加的 AP 加入指定域。

通过执行命令 **ap-region id** *region-id* 新建 AP 域，便于管理，如果不新建，则使用系统缺省域。

步骤 8 （可选）执行命令 **profile-id** *profile-id*，将增加的 AP 绑定指定 AP 模板。

通过执行命令 **ap-profile** { **id** *profile-id* | **name** *profile-name* } *，新建 AP 模板并配置模板参数（MTU、日志服务器地址、备份模式）。

版权所有 © 华为技术有限公司

如果不新建，则使用系统缺省模板。

----结束

操作结果

执行命令 **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* }，查看离线增加的 AP。

自动发现 AP 并正常上线

用户配置好 AP 白名单和 AP 认证方式，当 AP 与 AC 连接时，合法的 AP 将自动发现并正常上线。

前提条件

- AC 设备的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* } *，配置新的 AP 类型。

缺省情况下，系统预置了几种缺省支持的 AP 设备类型，包括：WA601、WA631、WA603SN、WA603DN、WA653SN、WA633SN、WA603DE、WA653DE、SRG1201GW、AP6010SN-GN、AP6010DN-AGN、AP6310SN-GN、AP6510DN-AGN、AP6610DN-AGN、WA705DN-AGN、AP7110DN-AGN。

步骤 4 执行命令 **ap-auth-mode** *auth-mode*，配置 AP 的认证方式（MAC、SN 或不检测）。

缺省情况下，AP 认证方式为 MAC 地址认证。

步骤 5 执行命令 **ap-whitelist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加合法 AP 的 MAC 或者 SN 到白名单里，可以批量增加。

说明

- 如果 AP 认证方式为“no-auth”，上线 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。
- 如果 AP 认证方式为“sn-auth”或“mac-auth”，AP 连接到 AC，且该 AP 的 MAC 或 SN 在白名单中，该 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。

----结束

操作结果

因为实际上线 AP 的 MAC 地址或 SN 与 AC 上白名单中配置匹配，此时 AP 将直接进入“normal”状态。

执行命令 **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* }，查看到自动发现的 AP 状态为正常。

版权所有 © 华为技术有限公司

自动发现 AP 并确认上线

用户配置好 AP 认证方式，一个不在白名单中的 AP 上线后，会被记录到未授权的 AP 列表中。需要用户手工确认后，此 AP 才能正常上线。

前提条件

- AC 设备的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* } *，配置新的 AP 类型。

缺省情况下，系统预置了几种缺省支持的 AP 设备类型，包括：WA601、WA631、WA603SN、WA603DN、WA633SN、WA603DE、WA653DE、WA653SN、AP6010SN-GN、AP6010DN-AGN、AP6310SN-GN、AP6510DN-AGN、AP6610DN-AGN。

步骤 4 执行命令 **ap-auth-mode** { **mac-auth** | **no-auth** | **sn-auth** }命令修改 AP 的认证方式（MAC 或 SN 认证）。

缺省情况下，AP 认证方式为 MAC 地址认证。

步骤 5 如确认此 AP 为合法，执行命令 **ap-confirm** { **all** | { **mac** *ap-mac* | **sn** *ap-sn* } [**id** *ap-id*] }，对 AP 进行确认。

AP 确认成功后，其 MAC 或 SN 将自动加入白名单，此 AP 自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，AP 正常工作。

----结束

（可选）配置 AP 数据缓存功能

配置 AP 数据缓存功能，用于网管定时查询 AP 的相关统计数据。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 （可选）执行命令 **ap-collect-time enable**，使能 AC 上的 AP 数据缓存功能。

缺省情况下，AC 上的 AP 数据缓存功能是关闭的。

步骤 4 执行命令 **ap collect-time** *timevalue*，用于使能 AC 上的 AP 数据缓存功能，并设置 AC 上缓存 AP 数据的缓存时长。

缺省情况下，AC 上缓存 AP 数据的缓存时间为 15 分钟。

----结束

版权所有 © 华为技术有限公司

检查配置结果

AP 与 AC 互通配置成功后，可以在 AC 上查看 AP 信息。

操作步骤

步骤 1 执行命令 **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* }，查看 AP 信息。

步骤 2 执行命令 **display ap-auth-mode**，查看 AP 的认证模式。

步骤 3 执行命令 **display ap-profile** { **all** | **default** | **id** *profile-id* | **name** *profile-name* }，查看 AP 模板信息。

步骤 4 执行命令 **display ap-region** { **default** | **all** | **id** *region-id* }，查看 AP 域信息。

步骤 5 执行命令 **display ap-run-info id** *ap-id*，查看 AP 运行信息。

步骤 6 执行命令 **display ap-type** { **all** | **id** *type-id* | **type** *ap-type* }，查看 AP 类型信息。

步骤 7 执行命令 **display ap-update mode**，查看 AP 升级模式。

步骤 8 执行命令 **display ap-update update-filename ap-type** *type-id*，查看 AP 升级文件名。

步骤 9 执行命令 **display ap-update ftp-server** ，查看用于 AP 升级的 FTP 服务器信息。

步骤 10 执行命令 **display ap-whitelist** { **mac** | **sn** } | [{ **begin** | **exclude** | **include** } *regular-expression*]，查看 AP 白名单信息。

步骤 11 执行命令 **display wlan commit status**，查看当前 Service-set 的配置是否下发到 AP。

----结束

12.1.5 配置 WLAN 射频

AP 上线后，需要给 AP 配置射频模板。AP 开始工作后系统缺省为其创建 Radio，最多可以创建 4 个 Radio，无需手工创建。

建立配置任务

在配置 WLAN 射频前了解 WLAN 射频的应用环境、前置任务和数据准备。

应用环境

WLAN 系统使用无线射频作为传输介质，且无线通讯通过抢占信道来传输数据。为了保证不同质量的无线接入服务，需要创建 WMM 模板并配置相应参数。另外，WLAN 系统使用射频模板对射频参数进行配置。WMM 模板创建后需绑定到射频模板，随绑定的射频模板应用到射频中。

前置任务

在配置 WLAN 射频之前，需完成以下任务：

AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。

数据准备

在配置 WLAN 射频之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	WMM 模板名称、（可选）WMM 模板 ID
2	（可选）WMM EDCA Client：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）
3	（可选）WMM EDCA AP：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）、ack-policy （ACK 策略）。
4	射频模板名称、（可选）射频模板 ID
5	AP ID、射频 ID、绑定的射频模板名称/或射频 ID
6	（可选）射频参数调优周期、调优的 AP 域 ID、定时调优时间
7	（可选）负载均衡组名称、负载均衡组 ID、AP ID/射频 ID、流量门限、会话门限、最大关联次数

配置 WMM 模板

不同的应用需求对于网络的要求是不同的，通过配置 WMM 模板，可以为不同的应用提供不同质量的接入服务。

背景信息

WMM 协议是一种无线 QoS 协议，用于保证优先级高的报文抢占无线信道的能力越高，从而保证语音、视频等应用在无线网络中有更好的质量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* } *，配置 WMM 模板。

WMM 模板创建成功后，模板内的参数均自动配置为缺省值。使用命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

#创建 WMM 模板“wp”，所有配置均为缺省值。

```
[Quidway-wlan-view] display wmm-profile name wp
  Profile ID      : 2
  Profile name    : wp
  WMM switch      : enable
  Mandatory switch: disable
  Client EDCA parameters:
  ------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit
  AC_VO  3       2       2      47
  AC_VI  4       3       2      94
  AC_BE  10      4       3      0
```


版权所有 © 华为技术有限公司

```
AC_BK  10      4       7       0
-------------------------------------------------
AP EDCA parameters:
-------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  3       2       1      47         normal
AC_VI  4       3       1      94         normal
AC_BE  6       4       3      0          normal
AC_BK  10      4       7      0          normal
-------------------------------------------------
```

说明

终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同报文获得不同级别的服务，我们将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样。

四个优先级队列的名称和优先级顺序缺省为：AC_VO(语音) > AC_VI(视频) > AC_BE(尽力而为) > AC_BK(背景)。

四个优先级队列的优先级顺序并不是绝对的，可以通过参数修改来调整优先级顺序，这些参数称为 EDCA 参数(Enhanced Distributed Channel Access)。包括 AIFSN（arbitration inter Frame spacing number 仲裁帧间隙数）、ECWmin（exponetn form of CWmin 最小竞争窗口指数形式）、ECWmax (exponent form of CWmax 最大竞争窗口指数形式)、TXOPlimit（transmission opportunity limit 传输机会限制）以及 ack-policy （ACK 策略）。

- AIFSN：WMM 针对不同 AC 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。
- ECWmin 和 ECWmax：这两个数值决定了平均退避时间值，数值越大，用户的平均退避时间越长。
- TXOPLimit：用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用的信道时长越大，如果是 0，则每次占用信道后，只能发送一个报文。
- ack-policy：有 normal ack(应答)和 no ack(不应答)两种策略，缺省为 noraml ack。

占用信道发送报文的原理：终端在占用信道发送报文前，先监听信道，当信道空闲时间大于或等于空闲等待时间时，在竞争窗口范围内随即选择退避时间进行退避，最先结束退避的终端竞争到信道，开始发送报文。

----结束

配置射频模板

射频模板中可以配置射频类型、射频速率、射频功率模式、射频信道模式和绑定 WMM 模板，且只有绑定了 WMM 模板的射频模板才可以被射频绑定。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* } *，配置射频模板。

射频模板创建成功后，模板内的参数均自动配置为默认值。

执行命令 **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看射频模板配置的各项属性。

```
[Quidway-wlan-radio-prof-radio-profile-1] display radio-profile name huawei
-------------------------------------------------------------------------
  Profile ID                          :1
  Profile name                        :huawei
  Radio type                          :802.11b/g
  Rate mode                           :auto
  Rate(Mbps)                          :54
  Channel mode                        :auto
```


版权所有 © 华为技术有限公司

```
Power mode                              :auto
Calibrate interval(min)                 :720
PER threshold(%)                        :30
Conflict rate threshold(%)              :60
RTS/CTS threshold(Byte)                 :2347
Fragmentation threshold(Byte)           :2346
Short retry number limit                :7
Long retry number limit                 :4
Support short preamble                  :support
DTIM interval (Beacon interval numbers):3
Beacon interval(ms)                     :100
WMM profile ID                          :1
WMM profile name                        :huawei
Interference detect switch              :disable
Calibrate switch                        :enable
Common frequency disturb threshold(%)   :50
Adjacent frequency disturb threshold(%):50
Station disturb threshold               :32
Radio device report duration(second)    :60
RTS/CTS mode                            :CTS-TO-SELF
Wifi-light mode                         :traffic
Beamforming Switch                      :disable
------------------------------------------------------------------------
```

步骤 4 （可选）执行命令 **radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。

如果绑定了该模板的某个射频不支持新修改的射频类型，修改会失败。

步骤 5 （可选）执行命令 **rate auto max-rate rate-value** { **rate_1** | **rate_2** | **rate_5_5** | **rate_6** | **rate_9** | **rate_11** | **rate_12** | **rate_18** | **rate_22** | **rate_24** | **rate_33** | **rate_36** | **rate_48** | **rate_54** }，配置射频模板的速率参数。

步骤 6 （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。

缺省情况下，功率模式为“auto”，即射频能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

步骤 7 （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。

缺省情况下，信道模式为“auto”，即射频能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

步骤 8 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* } ，为射频模板绑定 WMM 模板。

说明

只有绑定了 WMM 模板的射频模板才可以被射频绑定。

步骤 9 （可选）执行命令 **wifi-light** { **signal-strength** | **traffic** }，配置 AP 的 wifi 灯闪烁表示的状态信息。

说明

该命令只对开启 WDS 功能的 AP 适用，未开启 WDS 功能的 AP，无论配置为哪种方式，wifi 灯的闪烁都表示为流量状态。

步骤 10 （可选）执行命令 **rts-cts-mode** { **cts-to-self** | **disable** | **rts-cts** }，配置指定射频模板中 RTS-CTS 的工作模式。

说明

配置 RTS-CTS 的工作模式会影响传输速率，如果需要降低网络延时，可以关闭 RTS-CTS 的工作模式。

----结束

版权所有 © 华为技术有限公司

在射频上绑定射频模板

为指定射频绑定射频模板，绑定成功后，射频模板参数会应用到该射频中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。

步骤 4 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }，为指定射频绑定射频模板。

----结束

（可选）配置 AP 射频资源管理

AP 的射频资源管理包括动态信道分配和发射功率控制。

背景信息

当 WLAN 网络中的 AP 设备丢失，或者障碍物的阻挡会造成覆盖黑洞，AC 会周期性检测网络中是否有覆盖黑洞的存在并进行纠正。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* } *，配置射频模板。

射频模板创建成功后，模板内的参数均自动配置为缺省值。

步骤 4 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，这样 AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

在 WLAN 网络运行期间，AC 会周期性触发 AP 测量网络环境，以判断是否调整 AP 信道以及如何调整 AP 信道。

步骤 5 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，这样 AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

在 WLAN 网络运行期间，AC 会周期性触发 AP 采集邻居信息，判断是否需要调整 AP 的传输功率，以完整覆盖 WLAN 区域。



注意

用户修改信道或配套天线增益，以及射频调优自动触发信道/功率调整情况下，可能触发最大发射功率超限告警（如果用户选用的外置天线增益过高，有可能超出 AP 软件可调范围（即使软件将功率控制到最低也无法满足当地法规）。

步骤 6 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。

版权所有 © 华为技术有限公司

调优的目的是为了使射频下用户之间发射功率不受干扰。配置调优周期后，将按调优周期定时检测周围信号环境，如果信号环境恶化则启动局部调优。

步骤 7 手工启动全局调优：

- 执行命令 **quit**，返回 WLAN 视图。
- 执行命令 **calibrate startup region** *region-id* [**listen-uncontrol-neighbor**]，启动指定域的全局调优。
- 执行命令 **calibrate auto-startup region** *region-id* **time** *time* [**listen-uncontrol-neighbor**]，定时启动调优。

----结束

（可选）配置 AP 负载均衡组

AC 根据配置策略控制 AP 接入的无线用户，以保证 WLAN 网络实现负载均衡，优化网络性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **load-balance-group** { **name** *group-name* | **id** *group-id* } *，配置负载均衡组。

1. 执行命令 **member ap-id** *ap-id* **radio-id** *radio-id*，向负载均衡组内添加射频。

   添加后当有 STA 关联这个射频时，会先比较该射频和组内其他已正常工作射频的负载均衡情况，来决定是否让 STA 关联这个射频。

2. （可选）执行命令 **traffic gap** *gap-threshold*，配置负载均衡组的负载均衡模式为流量模式。

   负载均衡组内各射频的流量（上下行之和）差值超过 *gap-threshold* 门限时，AC 认为组内射频间出现负载不均衡，后续的 STA 关联请求会被自动负载到相对空闲的射频上。

   缺省情况下，负载均衡模式为会话模式。

3. （可选）执行命令 **session gap** *gap-threshold*，配置负载均衡组的负载均衡模式为会话模式。

   负载均衡组内各射频下的 STA 数目差值超过 *gap-threshold* 门限时，AC 认为组内射频间出现负载不均衡，后续的 STA 关联请求会被自动负载到相对空闲的射频上。

4. 执行命令 **associate-threshold** *associate-threshold*，配置负载均衡组的最大关联次数。

   STA 请求关联组内的某射频超过最大关联次数后，无论是否满足负载均衡的条件，STA 都允许被关联。

----结束

（可选）设置流量调度开关

前提条件

VAP 已经配置完成。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**， 进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*,进入指定射频的配置视图。

步骤 4 执行命令 **users-traffic-scheduler enable**,打开流量调度开关。

----结束

（可选）设置射频工作模式

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**,进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*,进入指定射频的配置视图。

步骤 4 执行命令 **work-mode** { **hybrid** | **monitor** | **normal** },设置射频工作模式。

步骤 5 执行命令 **quit**,返回到 WLAN 视图。

步骤 6 执行命令 **commit ap** *ap-id*,下发配置到指定 AP。

----结束

检查配置结果

WLAN 射频配置成功后，可查看 WLAN 射频的相关信息。

操作步骤

步骤 1 执行命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板信息。

步骤 2 执行命令 **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看射频模板信息。

步骤 3 执行命令 **display binding radio-profile** { **id** *profile-id* | **name** *profile-name* }，查看指定射频模板的绑定关系。

步骤 4 执行命令 **display load-balance-group** { **all** | **id** *group-id* | **name** *group-name* }，查看负载均衡组信息。

步骤 5 执行命令 **display actual channel-power ap-id** *ap-id* **radio-id** *radio-id*，查看指定射频上当前实际的信道和功率值。

步骤 6 执行命令 **display calibrate auto-startup info region** *region-id*，查看指定域上周期性自动启动全局调优信息。

步骤 7 执行命令 **display radio config ap-id** *ap-id* **radio-id** *radio-id*，查看单个射频的当前配置信息。

----结束

版权所有 © 华为技术有限公司

12.1.6 配置无线用户接入

AP 正常工作后，AP 根据 VAP 的参数配置提供给用户不同的业务。

建立配置任务

在配置 WLAN 业务前了解 WLAN 业务的应用环境、前置任务和数据准备。

应用环境

用户想通过无线方式接入以太网络时，需要配置 WLAN 业务。WLAN 业务的配置流程请参见 **12.1.2 AC6605 支持的 WLAN 特性**一节的“WLAN 业务配置流程”介绍。

前置任务

在配置 WLAN 业务之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。
- WLAN 射频已经配置完成，具体请参见 **12.1.5 配置 WLAN 射频**。

数据准备

在配置 WLAN 业务之前，需准备以下数据。

序号	数据
1	WLAN-ESS 接口编号、 Guest-Vlan VLAN ID、Restrict-Vlan VLAN ID、QoS Car 名称
2	安全模板名称、（可选）安全模板 ID。根据选择的安全策略，进行不同的数据准备： ● WEP 共享密钥认证：密钥值、密钥索引 ● WPA/WPA2 共享密钥认证：密钥值 ● WAPI 认证：AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件、ASU 服务器的 IP 地址、（可选）BK 更新间隔/生存期百分比、（可选）MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数、（可选）证书认证鉴别报文的重传次数
3	流量模板名称、（可选）流量模板 ID、（可选）up-map-8021p 映射值、（可选）8021p-map-up 映射值、（可选）报文限速速率、（可选）隧道优先级映射值
4	服务集名称、（可选）服务集 ID，绑定的安全模板名称/ID、绑定的流量模板名称/ID
5	AP ID/射频 ID、绑定的服务集名称/ID、（可选）WLAN 索引

版权所有 © 华为技术有限公司

配置 WLAN-ESS 接口

WLAN-ESS 接口下可以配置 QoS 流策略、接口优先级和接口下的认证方式等参数。

背景信息

WLAN-ESS 是一种虚拟的二层接口，类似于 hybrid 类型的二层以太网接口，具有二层属性，并可配置多种二层协议。

创建 WLAN-ESS 接口后，需要在服务集下绑定该接口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface wlan-ess** *wlan-ess-number*，创建 WLAN-ESS 接口。

步骤 3 执行命令 **port link-type hybrid**,配置接口的链路类型为 Hybrid。

缺省情况下，接口的链路类型为 Hybrid。可以不配置本命令。

步骤 4 执行命令 **port hybrid pvid vlan** *vlan-id*，配置 Hybrid 类型接口的缺省 VLAN ID。

缺省情况下，所有接口的缺省 VLAN 为 VLAN1。

步骤 5 执行命令 **port hybrid untagged vlan**，配置 Hybrid 类型接口加入的 VLAN。这些 VLAN 的帧以 Untagged 方式通过接口。

缺省情况下，Hybrid 接口以 Untagged 方式加入 VLAN1。

步骤 6 执行命令**{ dot1x-authentication | mac-authentication | web-authentication } enable**，配置 WLAN-ESS 接口下接入用户的认证方式。

说明

- 如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在接口下执行 **dot1x-authentication enable** 。
- 如果接入安全策略采用 WPA/WPA2 PSK 认证，无需执行 **dot1x-authentication enable** 命令。
- **mac-authentication** 可以且只能和 WPA/WPA2 PSK 结合起来用，即 WLAN 用户上线后，先进行 MAC 认证，再进行 WPA/WPA2 PSK 认证。
- **web-authentication** 可以且只能和 WEP 结合起来用，即 WLAN 用户通过 WEP 认证后，再访问 Web 服务器进行后续的业务认证。

步骤 7 执行命令 **dot1x authentication-method** { **chap** | **pap** | **eap** }，配置 dot1x 的认证方式。

缺省情况下，使用 **chap** 认证方式。

说明

dot1x 的认证方式为 **chap** 或者 **pap** 时，不支持配置端口所在的 guest-vlan 和 restrict-vlan。

步骤 8 （可选）执行命令 **dot1x guest-vlan** *vlan-id*，配置端口所在的 guest-vlan。

为了让某些用户在 Dot1x 认证前就能够访问一些网络资源，可以把该接口加入 guest-vlan 中。

步骤 9 （可选）执行命令 **dot1x restrict-vlan** *vlan-id*，配置端口所在的 restrict-vlan。

为了让某些用户在 Dot1x 认证失败后也能访问某些受限网络资源，可以把该接口加入 restrict-vlan 中。

版权所有 © 华为技术有限公司

步骤 10 （可选）执行命令 **qos car** { **inbound** | **outbound** }*car-name*，配置接口下的 QoS CAR 模板。

步骤 11 （可选）执行命令 **dot1x authentication domain** *domain-name*,用于在 WLAN-ESS 接口上绑定 AAA 域。

步骤 12 （可选）执行命令 **port-isolate enable** ,用于使能 AC 设备上的端口隔离功能。

步骤 13 （可选）执行命令 **port priority** ,用于设置接口为不带 VLAN tag 的报文添加的缺省 802.1p 优先级值。

步骤 14 （可选）执行命令 **traffic-policy** ,用于在接口上配置一个流策略。

步骤 15 （可选）执行命令 **trust** ,用于指定报文按照某类优先级进行映射。

步骤 16 （可选）执行命令 **trust upstream** ,用于在接口上绑定 DiffServ 域，配置后，系统会根据 DiffServ 域中的映射关系将流经该接口的报文优先级与 PHB 行为和报文颜色进行映射。

----结束

配置安全模板

配置用户接入 WLAN 网络使用的安全策略。

背景信息

WLAN 接入安全策略有 4 种，分别为 WEP 认证、WPA 认证、WPA2 认证和 WAPI 认证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* } *，配置用户的接入安全模板。

模板创建后，缺省配置如下：

- 对于 WEP：缺省配置为开放系统认证方式+空密钥。
- 对于 WPA1：缺省配置为 802.1x+PEAP 认证方式+TKIP 数据加密方式。
- 对于 WPA2：缺省配置为 802.1x+PEAP 认证方式+CCMP 数据加密方式。
- 对于 WAPI：缺省配置为 WAI 认证方式+WPI 数据加密方式。

步骤 4 配置各种安全策略：

- WEP 开放系统认证
  1. 执行命令 **security-policy wep** ，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method open-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
- WEP 共享密钥认证
  1. 执行命令 **security-policy wep** ，配置安全策略为 **wep** 方式。

版权所有 © 华为技术有限公司

2. 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
3. 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。

   WEP-40 方式下：10 个十六进制或者 5 个 ASCII 字符；WEP-104 方式下：26 个十六进制或者 13 个 ASCII 字符。
4. 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

   WEP 的密钥可以配置 4 个，在认证或者加密时只使用一个，使用此命令来指定使用哪一个密钥。

- WPA/WPA2 认证
  1. 执行命令 **security-policy wpa** ，配置安全策略为 **wpa** 方式。
  2. 执行命令**{ wpa | wpa2 } authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 dot1x 认证方式和相应的加密方式。

     说明

     如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在 WLAN-ESS 接口下执行 **dot1x-authentication enable** 。
  3. 执行命令**{ wpa | wpa2 } authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
- WAPI 认证
  1. 执行命令 **security-policy wapi** ，配置安全策略为 **wapi** 方式。
  2. 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。

     WAPI 的认证方式支持基于证书和基于预共享密钥两种，当用户选择基于预共享密钥时，需要输入共享密钥。
  3. 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file_name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
  4. 执行命令 **wapi import private-key file-name** *file_name*，导入 AC 的私钥文件。
  5. 执行命令 **wapi asu ip** *ip-address*，配置 ASU 服务器的 IP 地址。

     WAPI 证书方式下，AC 会将证书发送到该 IP 地址所在的 ASU 服务器。
  6. （可选）执行如下命令修改 WAPI 的参数：
     - 执行命令 **wapi** { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-interval* }，配置 BK 更新间隔、生存期百分比。

       缺省情况下，BK 的更新间隔为 43200s，生存期百分比为 70%。
     - 执行命令 **wapi** { **msk-update-interval** *msk-interval* | **msk-update-packet** *msk-packet* | **msk-retrans-count** *msk-count* }，配置 MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数。

       缺省情况下，MSK 更新间隔为 86400s，MSK 更新报文数为 10000，MSK 密钥协商报文重传次数为 3 次。
     - 执行命令 **wapi cert-retrans-count** *cert-count*，配置证书认证鉴别报文的重传次数。

       缺省情况下，重传次数为 3 次。
     - 执行命令 **wapi** { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }，配置 WAPI 的 USK 和 MSK 的更新方式。

版权所有 © 华为技术有限公司

缺省情况下，USK 和 MSK 都是基于时间更新。

----结束

配置流量模板

当需要为某个 VAP 定制特定的优先级映射、流量抑制等功能时，创建相应的流量模板并绑定到服务集中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，配置流量模板。

流量模板创建成功后，模板内的参数均为缺省值。执行命令 **display traffic-profile** { **id** *profile-id* | **name** *profile-name* }，查看各项属性的缺省配置。

#查看 Traffic 模板“traffic-profile-1”的各项属性。

```
[Quidway-wlan-view] display traffic-profile name traffic-profile-1
  Profile ID         : 3
  Profile name       : traffic-profile-1
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
  802.1p to User-priority Mapping List:
  ----------------------------
  802.1p  User-priority
  0       0
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  ----------------------------
  Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)
  ----------------------------
  ToS(inner)     ToS(outer)
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
```


版权所有 © 华为技术有限公司

说明

STA 发出的 802.11 报文要通过 AP 进入以太网时，需要转换成 802.3 报文，这期间可以不进行优先级映射，也可以按照不同的 VAP 设置不同的优先级，或按照 UP（用户优先级）映射到优先级。

802.3 报文通过 AP 转发给 STA 时，被转换成 802.11 报文，其中的 UP 域可以根据 DSCP、CoS 映射而来，或者由流分类设置。

----结束

配置 WLAN 服务集

服务集（service-set）是业务层面的关键参数集，服务集应绑定安全模板和流量模板。

前提条件

安全模板和流量模板已经配置完成。

背景信息

服务集是一个业务参数集合。当它被绑定到指定 AP 的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP（Virtual Access Point）上。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } *，配置服务集。

步骤 4 执行命令 **ssid** *ssid*，指定服务集的 SSID。

步骤 5 （可选）执行命令 **ssid-hide**，配置 Beacon 帧中隐藏 SSID。

步骤 6 执行命令 **security-profile** { **name** *profile-name* | **id** *profile-id* } *，服务集下绑定安全模板。

步骤 7 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，服务集下绑定流量模板。

说明

服务集下绑定的安全模板和流量模板，对使用该服务集的所有用户起作用。

步骤 8 执行命令 **wlan-ess**，服务集下绑定 wlan-ess 接口。

步骤 9 执行命令 **service-vlan**，用于指定绑定 service-set 服务集的 VAP 的业务 VLAN ID。

步骤 10 执行命令 **association-timeout** *association-timeout*，用于配置 STA（无线客户端）用户关联老化时间。

步骤 11 执行命令 **max-user-number** *max-user-number*，用于配置服务集的最大接入用户数目。

步骤 12 （可选）执行命令 **ip source guard enable**,使能 AP 的 IPSG(Ip Source Guard)功能。

缺省情况下，AP 的 IPSG 功能处于未使能状态。

步骤 13 （可选）执行命令 **tunnel-forward protocol dot1x**,使能 eap 报文的隧道转发功能。

缺省情况下，eap 报文的隧道转发功能未使能。

版权所有 © 华为技术有限公司

步骤 14 （可选）执行命令 **dai enable**,使能动态 arp 检测功能。

缺省情况下，动态 arp 检测功能未使能。

步骤 15 （可选）执行命令 **arp-attack threshold** *threshold-value*,配置 ARP 攻击告警门限值。

缺省情况下，arp 攻击告警门限值为 15。

步骤 16 （可选）执行命令 **dhcp trust port**,使能 AP 的 dhcp 信任功能。

缺省情况下，AP 的 dhcp 信任功能处于关闭状态。

----结束

配置 VAP

VAP 下发 AP 时，与 VAP 绑定的服务集参数作为 VAP 的参数一起下发到 AP，AP 根据 VAP 配置的参数提供给用户不同的业务。

前提条件

- 指定射频上已经绑定了射频模板，具体请参见**在射频上绑定射频模板**。
- 服务集已经创建并配置好参数，具体请参见**配置 WLAN 服务集**。

背景信息

VAP 是 AP 上的业务功能实体。用户可以在 AP 的每个射频上创建不同的 VAP，通过为 AP 的指定射频绑定服务集，就可以创建 VAP。执行命令 **commit** { **all** | **ap** *ap-id* }提交配置，将 VAP 下发到 AP。

说明

在 AC 上执行的关于 AP 的 WLAN 业务配置命令，必须执行 **commit** 命令下发到 AP 后才能真正生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 创建单个 VAP。

1. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。
2. 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } [**wlan** *wlan-id*]，绑定服务集。
3. 执行命令 **quit**，返回 WLAN 视图
4. 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

步骤 4 批量创建 VAP。

1. 执行命令 **batch ap** { *ap-id* [**to** *ap-id*] } &<0-1023> **radio** { *radio-id* [**to** *radio-id*] } &<1-4> **service-set** { *service-set-id* [**to** *service-set-id*] } &<0-1023> [**radio-profile** { **id** *profile-id* | **name** *profile-name* } *]，批量创建 VAP。
2. 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

----结束

版权所有 © 华为技术有限公司

配置用户组

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-group** *group-name*，创建用户组并进入用户组视图。

步骤 3 执行命令 **acl-id** *acl-id*，绑定用户组的访问控制列表。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **aaa**，进入 AAA 视图。

步骤 6 执行命令 **cut access-user user-group** *group-name*，删除所有使用该用户组的上线用户。

----结束

配置 VLAN Mapping

介绍配置 VLAN Mapping 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface eth-trunk** *trunk-id*，创建 Eth-Trunk 接口并进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **inner-vlan** *vlan-id3* **map-vlan** *vlan-id4* [**to** *vlan-id5*] **delete-inner-vlan**，配置当前接口的 VLAN Mapping 功能。

说明

QinQ 映射后的 VLAN 不能与 PVID 的 VLAN 相同。

----结束

检查配置结果

WLAN 业务配置完成后，可以查看 WLAN 业务相关的配置信息。

操作步骤

步骤 1 执行命令 **display vap** { **all** [**type** { **service-set** | **bridge-profile** }] | **ap** *ap-id* [**radio** *radio-id* | **type** { **service-set** | **bridge-profile** }] | **service-set** { **id** *service-set-id* | **name** *service-set-name* } | **bridge-profile** { **id** *bridge-profile-id* | **name** *bridge-profile-name* } }，查看 VAP 信息。

步骤 2 执行命令 **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] }，查看安全模板信息。

步骤 3 执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看流量模板信息。

步骤 4 执行命令 **display service-set** { **all** | **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* }，查看服务集信息。

版权所有 © 华为技术有限公司

步骤 5 执行命令 **display interface wlan-ess** [*wlan-ess-number*]，查看 WLAN-ESS 接口运行状态和统计信息。

----结束

12.1.7 管理 AP

介绍 AC+瘦 AP 组网模式下配置 LLDP、AP 光模块告警阈值、AP 动态节能、双链路备份过程。

配置 LLDP 功能

LLDP（Link Layer Discovery Protocol，链路层发现协议）是 IEEE802.1AB 中定义的二层发现协议。通过采用 LLDP 技术，在网络规模迅速扩大时，网管系统可以快速掌握二层网络拓扑、拓扑变化信息。

背景信息

通过 LLDP 协议，可以将本端设备的设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等信息组织成不同的 TLV（Type Length Value）,并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己相邻的邻居，邻居收到这些信息后将其保存在 LLDP 远端系统 MIB（Management Information Base，管理信息库）库中，供 AC 查询和判断链路的通信状况。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wlan ap lldp enable**,使能全局的 LLDP 功能。

缺省情况下，全局的 LLDP 功能处于未使能状态。

步骤 4 执行命令 **ap id** *ap-id*，进入 AP 视图。

步骤 5 执行命令 **lldp enable**,使能 AP 的 LLDP 功能。

缺省情况下，AP 的 LLDP 功能处于使能状态。

步骤 6 执行命令 **lldp admin-status** { **rx** | **tx** | **txrx** }，使能 AP 的报文发送或接收功能。

缺省情况下，AP 的 LLDP 报文发送和接收功能都使能。

步骤 7 （可选）执行命令 **lldp tlv-enable basic-tlv** { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }，配置 AP 发布的 TLV 类型。

缺省情况下，LLDP 发布所有基本类型 TLV。

步骤 8 （可选）执行命令 **lldp message-transmission** { **delay** *delay-time* | **hold-multiplier** *multiplier-id* | **interval** *interval-time* }，配置 AP 设备 LLDP 协议的时间参数。

缺省情况下，AP 设备 LLDP 协议时间参数如下：

- **delay** *delay-time*：2 秒

版权所有 © 华为技术有限公司

- **hold-multiplier** *multiplier-id*：4 倍
- **interval** *interval-time*：30 秒

步骤 9 （可选）执行命令 **lldp report-interval** *interval-time*，配置 AP 向 AC 上报邻居信息的最小时间间隔。

缺省情况下，AP 向 AC 上报邻居信息的最小时间间隔为 30 秒。

步骤 10 （可选）执行命令 **lldp restart-delay** *delay-time*，配置 AP 的 LLDP 模块从禁用状态重新使能的延迟时间。

缺省情况下，AP 的 LLDP 模块从禁用状态重新使能的延迟时间为 2 秒。

----结束

配置 AP 光模块告警阈值

本章节主要描述如何配置 AP 光模块告警阈值。

背景信息

光模块的告警主要包括光模块接收功率过高告警/恢复、光模块接收功率过低告警/恢复、光模块温度过高告警/恢复、光模块温度过低告警/恢复。针对这四种告警，必须设置 4 个阈值，以判断 4 种告警和恢复的临界点。设置光模块的告警阈值后，当 AP 检测到实际值不在设定的阈值范围内时，AP 产生告警信息上报给 AC，方便用户的维护。

说明
目前，支持光模块的 AP 类型只有 WA653SN、AP6610DN-AGN 两种。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap id** *ap-id*，进入 AP 视图。

步骤 4 执行命令 **optical** { **high-rx-power** | **low-rx-power** | **high-temperature** | **low-temperature** } **threshold** *value*，配置光模块告警阈值。

缺省情况下，光模块告警阈值如下：

- high-rx-power：100uw
- low-rx-power：2.5uw
- high-temperature：70°C
- low-temperature：-5°C

----结束

配置 AP 动态节能

配置 AP 动态节能功能，可降低 AP 设备的功耗，从而降低用户的运营成本。

版权所有 © 华为技术有限公司

背景信息

打开 AP 动态节能开关后，如果当 AP 上没有报文通过的时候，设备会自动进入节能模式；如果当 AP 检测到有报文通过时，设备会自动恢复正常的工作状态。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ap id** *ap-id*，进入 AP 视图。

步骤 3 执行命令 **save-mode enable**，打开 AP 的动态节能开关。

缺省情况下，AP 的动态节能开关关闭。

----结束

配置双链路备份

一台 AC 下面最大能关联 512 台 AP，如果 AC 出现故障，会导致其下所有 AP 上的接入用户业务全部中断，严重影响用户运营。配置双链路备份，能够保证业务的稳定。

背景信息

为了实现 AC 的备份，AP 需要与两个 AC 分别建立信道连接。这两个 AC 之间为主备的关系，处于主用状态的 AC 负责为 AP 提供服务，处于备份状态的 AC 为主用的 AC 提供备份，当 AP 检测到 AP 与主用 AC 之间的链路故障时，AP 发送报文通知备用 AC 切换为主用 AC，同时把 AP 上的接入用户的数据业务信息发往该 AC，保证业务的稳定。

注意

在配置双链路备份时，对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致。否则当 AC 的主备状态切换后，无法保证 AP 工作正常。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wlan ac protect { enable | disable }**，使能全局双链路功能。

缺省情况下，全局双链路功能未使能。

步骤 4 执行命令 **wlan ac protect { protect-ac | priority }**，配置全局备份 AC 的 IP 地址或 AC 的优先级。

缺省情况下，没有配置全局备份 AC 的 IP 地址或 AC 的优先级。

说明

如果在 WLAN 视图和 AP 视图下配置了相同参数，则 AP 视图下的配置将被优先采用。

步骤 5 执行命令 **wlan ac protect restore** { **enable** | **disable** }，打开全局回切功能开关。

缺省情况下，全局回切功能开关打开。

版权所有 © 华为技术有限公司

说明

如果关闭全局回切功能开关，则在备 AC 切换为主 AC 之后，即使原主 AC 与 AP 的链路恢复，也不会重新切换至原主 AC。

步骤 6 执行命令 **ap id** *ap-id*，进入 AP 视图。

步骤 7 执行命令 **protect-ac**，配置指定 AP 的备份 AC 的 IP 地址。

缺省情况下，没有配置指定 AP 的备份 AC 的地址。

说明

如果在 WLAN 视图和 AP 视图下配置了相同参数，则 AP 视图下的配置将被优先采用。

步骤 8 执行命令 **priority**，在 AP 视图下配置 AC 的优先级。

缺省情况下，没有在 AP 视图下配置 AC 的优先级。

说明

- 如果在 WLAN 视图和 AP 视图下配置了相同参数，则 AP 视图下的配置将被优先采用。
- 如果 AP 连接的两台 AC 都配置了优先级，则优先级高的成为主用 AC。如果全局回切功能开关已打开，则此 AC 的链路出现故障又恢复后，会重新与 AP 建立连接，切换为主 AC。

----结束

检查配置结果

前提条件

已完成 LLDP 功能、AP 光模块、AP 动态节能、双链路备份的配置。

操作步骤

- 执行 **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* }命令,查看 AP 信息,包括 AP 的动态节能功能是否使能、双链路备份中 AC 的优先级和备份 AC 的 IP 地址等信息。
- 执行 **display optical-info ap-id** *ap-id* 命令,查看指定 AP 的光模块信息。
- 执行 **display lldp ap-neighbor** [*ap-id* [**port** *portnum*]]命令,查看指定 AP 的 LLDP 邻居信息。

----结束

12.1.8 维护

介绍如何复位 AP、升级 AP、定位 AP 及用户位置。

复位 AP

当 AP 工作不正常时，可能需要对其复位。

版权所有 © 华为技术有限公司

背景信息

注意

AP 复位会中断业务，请谨慎使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap-reset** { **all** | **id** *ap-id* }，进行 AP 复位。

----结束

升级 AP 设备

AP 在正常运行之前或 AC 版本变更后，AP 和 AC 协商决定与当前 AC 版本对应的 AP 运行版本，如果版本不匹配，AP 开始升级。

背景信息

AP 支持两种版本升级模式：

- ac-mode：AP 升级时从 AC 上下载升级版本。
- ftp-mode：AC 通过 ap-update ftp-server 命令下发 FTP 配置信息后，由 AP 到 FTP 服务器下载升级版本。

说明

- 预先设置升级模式控制 AP 版本升级方式，ac-mode、ftp-mode 二选一。且处在同时支持同类 AP 最大 128 个并行加载的限制下。
- AP 升级时采用 FTP 模式，须保证版本文件名与版本号一致，否则会导致 AP 不停换包重启。

操作步骤

- 配置 ac-mode 升级模式。

  说明

  使用 TFTP 或者 FTP 方式将指定的升级文件加载到 AC 设备上。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **wlan**，进入 WLAN 视图。
  3. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式为“ac-mode”。
  4. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id* ，配置与 AP 类型对应的升级文件名。
- 配置 ftp-mode 升级模式。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **wlan**，进入 WLAN 视图。

版权所有 © 华为技术有限公司

3. 执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftpusername* | **ftp-password** *ftppassword*] *，配置 FTP 服务器 IP、FTP 客户端用户名、密码。

   说明

   将 AP 升级所需的升级文件存放在 FTP 服务目录下，并确保 AP 与 FTP 服务器网络互通。

4. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式为“ftp-mode”。
5. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id* ，配置与 AP 类型对应的升级文件名。

----结束

后续处理

- 后续可执行命令 **ap-update multi-load ap-type** *type-id*，按照 AP 类型进行批量 AP 在线升级。
- 升级完成后，需要执行命令 **ap-update multi-reset ap-type** *type-id*，批量复位升级完成的 AP。

定位 AP 位置

通过查询指定射频的邻居信息，便于分析 AP 的布放情况、相邻关系等，可用于网络规划。

背景信息

非法 AP 的存在，可能会对 WLAN 网络中其他 AP 产生信号干扰，导致 WLAN 网络的信号传输质量下降，WLAN 网络的数据传输也有可能被窃取。为了将非法 AP 从 WLAN 网络中剔除，保证 WLAN 网络的安全，往往需要分析 AP 的布放情况，定位出 AP 的网络拓扑位置。

操作步骤

步骤 1 执行命令 **display neighbor ap-id** *ap-id* **radio-id** *radio-id*，查询指定射频的邻居信息。

根据查询到的邻居信息，可以分析 AP 的布放情况、相邻关系等。

----结束

查询统计信息

通过 **display** 命令查看用户和报文的统计信息。

操作步骤

- 执行命令 **display statistics** { **arp** | **icmp** } **ap-id** *ap-id*,查看指定 AP 的 ARP 报文或 ICMP 报文的统计数。
- 执行命令 **display statistics ssid** *ssid-name* **ap** *ap-id* **radio** *radio-id*,查看指定 AP 的射频上某一个 SSID 的报文统计信息。
- 执行命令 **display statistics** { **mac** | **calibrate** } **ap-id** *ap-id* **radio-id** *radio-id*，查看指定射频上的 MAC 层统计信息，或者查看指定射频信道、功率调优相关的统计信息。
- 执行命令 **display station assoc-info** { **sta** *mac-address* | **ap** *ap-id* [**radio** *radio-id* | **radio** *radio-id* **service-set** *service-set-id*] } ，查看指定无线终端的接入信息，或者查

版权所有 © 华为技术有限公司

看指定 AP 上、指定 AP + Radio 上或指定 AP + Radio + ESS 上所有关联的无线终端接入信息。

- 执行命令 **display station assoc-num** { **service-set** *service-set-id* | **ap** *ap-id* [**radio** *radio-id*] }，查看指定 service-set 或指定 AP 上关联的无线终端数。
- **display station statistics** { **sta** *mac-address* | **ap** *ap-id* }，查看无线终端的相关统计信息，支持指定无线终端（STA）查看，可以获取无线终端的报文、字节和速率相关统计；指定 AP 查看时，可以获取该 AP 上无线终端关联、重关联和去关联次数统计。
- 执行命令 **display station status sta** *mac-address*，查看无线终端的相关状态信息，目前包括：接入的 SSID、在线时间、上行信噪比和上行接收功率。
- 执行命令 **display statistics sta** *mac-address*，查看在线 STA 的统计信息。

----结束

清除用户统计信息

介绍使用 reset 命令清除用户统计信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **reset aaa statistics authentication**，清除 AAA 用户认证相关统计信息。

步骤 3 执行命令 **reset access-user statistics**，清除接入用户认证相关统计信息。

----结束

12.1.9 配置举例

配置 WLAN 基本业务示例

组网需求

网络供应商为某两个临近区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 和 AP 组网图如图 12-3 所示。

- 由接入交换机分配业务 VLAN，并给 AP 管理报文打管理 VLAN tag。
- AC 同时作为 DHCP Server 给 AP 分配 IP 地址。
- AP1 和 AP2 上业务数据采用数据直接转发模式。

版权所有 © 华为技术有限公司

图 12-3 配置 WLAN 基本业务示例图

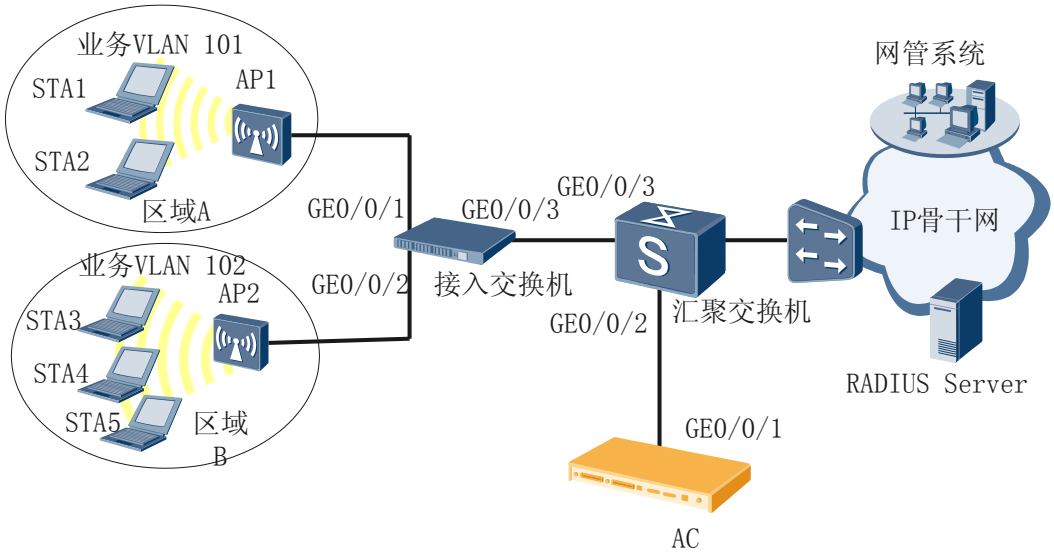


表 12-1 数据规划表

配置项	数据
WLAN 服务	WEP Open-System 认证，不加密。
AP 管理 VLAN	VLAN 100（接入交换机分配）
AP 域	AP1:101 AP2:102
服务集	● Name：Huawei-1 ● SSID：Huawei-1 ● WLAN 虚接口：WLAN-ESS 0 ● 数据转发模式：直接转发
	● Name：Huawei-2 ● SSID：Huawei-2 ● WLAN 虚接口：WLAN-ESS 1 ● 数据转发模式：直接转发
WLAN 用户 VLAN	AP1：VLAN 101 AP2：VLAN 102
AC Carrier ID/AC ID	CTC（中国电信）/1
AC 管理 IP 地址	Vlanif 接口：192.168.0.1/24
AP 地址池	192.168.0.2 ～ 192.168.0.254/24
AP 网关	192.168.0.1/24（AC）
DHCP 服务器	AC 作为 DHCP 服务器，为 AP 分配地址

版权所有 © 华为技术有限公司

配置思路

1. 配置接入交换机、汇聚交换机和 AC，实现 AP 和 AC 互通。
2. 配置 AC 的基本功能，包括配置 AC 运营商标识和 ID、AC 与 AP 之间通信的源接口，实现 AC 作为 DHCP Server 功能。
3. 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。
4. 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

   其中配置 VAP，需要：

   a. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。

   b. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。

   c. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。

   d. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。

操作步骤

步骤 1 配置接入交换机、汇聚交换机和 AC，使 AP 和 AC 互通。

#配置接入交换机连接 AP 的以太网端口（GE0/0/1 和 GE0/0/2）类型为 trunk 类型，PVID 为 100。配置接入交换机上连接汇聚交换机的 GE0/0/3 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 102
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 102
[Quidway-GigabitEthernet0/0/3] quit
```

#配置汇聚交换机上连接 AC 的 GE0/0/2 接口透传所有业务和管理 VLAN。配置汇聚交换机上连接接入交换机的 GE0/0/3 接口透传所有业务和管理 VLAN。

```
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 102
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 102
```

#配置 AC 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname LSW
[LSW] vlan batch 100 to 102
[LSW] interface GigabitEthernet 0/0/1
[LSW-GigabitEthernet0/0/1] port link-type trunk
[LSW-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
```


版权所有 © 华为技术有限公司

```
[LSW-GigabitEthernet0/0/1] quit
[LSW] interface XGigabitEthernet 0/0/27
[LSW-XGigabitEthernet0/0/27] port link-type trunk
[LSW-XGigabitEthernet0/0/27] port trunk allow-pass vlan 100 to 102
[LSW-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[AC-XGigabitEthernet0/0/1] quit
```

步骤 2 配置 AC 的基本功能。

#配置 AC 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC] wlan ac-global ac id 1 carrier id  ctc
[AC] wlan ac-global country-code cn
```

#创建 VLANIF 接口，配置其 IP 地址作为数据转发的三层接口，使能 DHCP 服务功能。

Vlanif 100 为 AP 分配 IP 地址，Vlanif 101 为区域 A 的 STA 分配 IP 地址，Vlanif 102 为区域 B 的 STA 分配 IP 地址。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

说明

AP 需要获取一个 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。此处配置 AC 为 DHCP 服务器，AP 从 AC 上获取 IP 地址。

#配置 AC 的源接口，用于 AP 和 AC 之间建立隧道通信。

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
```

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

步骤 3 配置 AP 并上线。

#配置 AP 的认证方式为“no-auth”。

```
[AC-wlan-view] ap-auth-mode no-auth
```

说明

如果 AP 认证模式为“no-auth”，上线 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。

#配置 AP 域 ID 分别为 101 和 102。

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```


版权所有 © 华为技术有限公司

```
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```

#配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

步骤 4 配置 WLAN-ESS 虚接口。

```
[AC] interface wlan-ess 0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] quit
```

步骤 5 配置 AP 对应的射频。

#创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm-1 id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

#创建名为“radio-1”的射频模板，绑定 WMM 模板“wmm-1”。

```
[AC-wlan-view] radio-profile name radio-1
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[AC-wlan-radio-prof-radio-1] quit
```

#将 AP1 和 AP2 对应的射频绑定射频模板“radio-1”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] radio-profile name radio-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name radio-1
[AC-wlan-radio-1/0] quit
```

步骤 6 配置 AP 对应的服务集。

#创建安全模板。

安全模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
[AC-wlan-view] security-profile name security-1 id 1
[AC-wlan-sec-prof-security-1] wep authentication-method open-system
[AC-wlan-sec-prof-security-1] security-policy wep
[AC-wlan-sec-prof-security-1] quit
```

#配置 QoS 策略，创建流量模板。

流量模板名为“traffic-1”，参数采用缺省配置。

```
[AC-wlan-view] traffic-profile name traffic-1
[AC-wlan-traffic-prof-traffic-1] quit
```

#分别创建与 AP1 及 AP2 对应的服务集，并绑定流量模板及安全模板、WLAN-ESS 接口。

```
[AC-wlan-view] service-set name huawei-1
[AC-wlan-service-set-huawei-1] ssid huawei-1
```


版权所有 © 华为技术有限公司

```
[AC-wlan-service-set-huawei-1] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-1] security-profile name security-1
[AC-wlan-service-set-huawei-1] wlan-ess 0
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] forward-mode direct-forward
[AC-wlan-service-set-huawei-1] quit
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-2] security-profile name security-1
[AC-wlan-service-set-huawei-2] wlan-ess 1
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] forward-mode direct-forward
[AC-wlan-service-set-huawei-2] quit
```

步骤 7 配置 AP 对应的 VAP，下发 WLAN 服务。

#将 AP1 和 AP2 对应的射频绑定服务集“Huawei-1”和“Huawei-2”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] service-set name huawei-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
```

#下发 AP 的 WLAN 服务。

```
[AC-wlan-view] commit ap 0
[AC-wlan-view] commit ap 1
```

步骤 8 验证配置结果

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-1 和 huawei-2 的 WLAN 网络并正常上线。

----结束

配置文件

- AC 上的配置文件

```
#
 sysname AC
#
 vlan batch 100 to 102
#
 dhcp enable
#
 wlan ac-global carrier id ctc ac id 1
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select
interface
#
interface WLAN-ESS0
 port hybrid untagged vlan 101
#
```


版权所有 © 华为技术有限公司

```
interface WLAN-ESS1
 port hybrid untagged vlan 102
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 to
102
#
wlan
 wlan ac source interface Vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 0 type-id 7 mac 80fb-0616-31d1 sn AB34002078
  region-id 101
 ap id 1 type-id 6 mac 5489-9849-8265 sn AB36015000
  region-id 102
 wmm-profile name wmm-1 id
1
 traffic-profile name traffic-1 id
1
 security-profile name security-1 id
1
 service-set name huawei-1 id 1
  wlan-ess 0
  ssid huawei-1
  traffic-profile id 1
  service-vlan 101
 service-set name huawei-2 id 2
  wlan-ess 1
  ssid huawei-2
  traffic-profile id 2
  service-vlan
102
 radio-profile name radio-1 id 1
  wmm-profile id 1
 ap 0 radio 0
  radio-profile name radio-1
  service-set id 0 wlan 1
 ap 1 radio 0
  radio-profile name radio-1
  service-set id 1 wlan 1
#
return
```

- 接入交换机上的配置文件

```
#
 vlan batch 100 to 102
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 102
#
```

- 汇聚交换机上的配置文件

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 to 102
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 102
#
```

配置 AP 双链路备份示例

组网需求

为了实现 AP 双链路备份，AP 需要与 AC1 和 AC2 分别建立隧道链接。建立好 CAPWAP 隧道后，AP 与 AC1、AC2 之间都会有 CAPWAP 握手报文检测隧道状态，当 AP 检测到 AP 与 AC1 之间隧道故障时，进行主备倒换，避免 CAPWAP 重新建立连接导致的业务中断。

AC 和 AP 组网图如图 12-4 所示。

- 由接入交换机分配业务 VLAN，并给 AP 管理报文打管理 VLAN tag。
- 接入交换机同时作为 DHCP Server 给 AP 和 STA 分配 IP 地址。
- AP 上业务数据采用数据直接转发模式。

图 12-4 配置 AP 双链路备份示例图

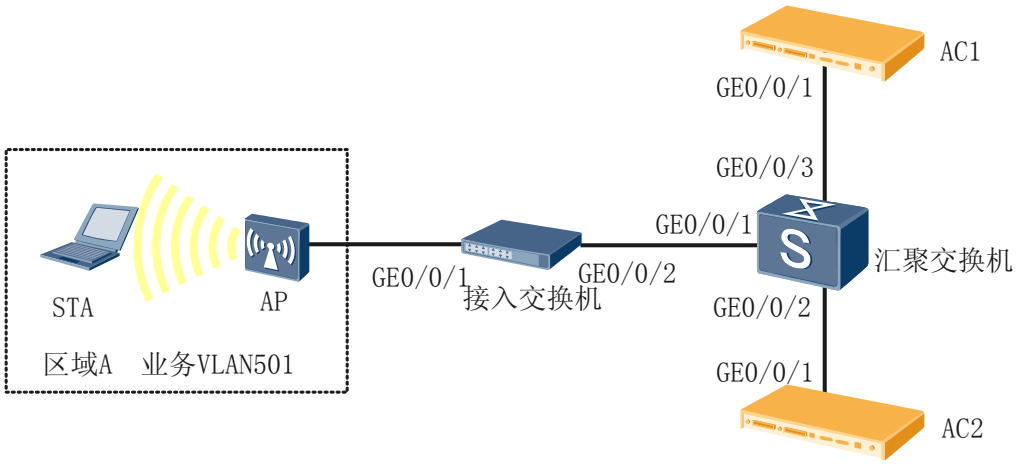


表 12-2 数据规划表

配置项	数据
WLAN 服务	WEP Open-System 认证，不加密。
AP 管理 VLAN	VLAN 500（接入交换机分配）
AP 域	101
服务集	● Name：Huawei ● SSID：Huawei ● WLAN 虚接口：WLAN-ESS 0 ● 数据转发模式：直接转发
WLAN 业务 VLAN	501

版权所有 © 华为技术有限公司

配置项	数据
SwitchVLAN	VLAN 500/501
AC Carrier ID/AC ID	CTC（中国电信）/1
AC1 管理 IP 地址	Vlanif 接口：60.1.1.2/24
AC2 管理 IP 地址	Vlanif 接口：60.1.1.3/24
AP 地址池	60.1.1.4 ～ 60.1.1.254/24
AP 网关	60.1.1.1/24（Switch）
DHCP 服务器	接入交换机作为 DHCP 服务器，为 AP 和 STA 分配地址

配置思路

1. 配置接入交换机、汇聚交换机、AC1 和 AC2，实现 AP 和 AC1 和 AC2 的互通。
2. 配置 AC1 的基本功能，包括配置 AC1 运营商标识和 ID、AC1 与 AP 之间通信的源接口，实现 Switch 作为 DHCP Server 功能。
3. 配置 AC1 的优先级和备份 AC 的 IP 地址。
4. 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。
5. 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

   其中配置 VAP，需要：

   a. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
   b. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。
   c. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
   d. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。
6. 配置 AC2。

操作步骤

步骤 1 配置接入交换机、汇聚交换机和 AC，使 AP 和 AC 互通。

#配置接入交换机连接 AP 的以太网端口（GE0/0/1）类型为 trunk 类型，PVID 为 500。配置接入交换机连接汇聚交换机的 GE0/0/2 接口透传管理和业务 VLAN。

```
<Quidway> system-view
[Quidway] vlan batch 500 501
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk pvid vlan 500
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

配置汇聚交换机连接 AC1 的 GE0/0/3 接口透传管理和业务 VLAN。

```
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/3] quit
```

配置汇聚交换机连接 AC2 的 GE0/0/2 接口透传管理和业务 VLAN。

```
[Quidway] interface XGigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/2] quit
```

配置汇聚交换机连接接入交换机的 GE0/0/1 接口透传管理和业务 VLAN。

```
[Quidway] interface XGigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/1] quit
```

创建 VLANIF 接口，使能 DHCP 服务功能，vlanif 500 为 AP 分配地址，vlanif 501 为 STA 分配 IP 地址。

```
[Quidway] dhcp enable
Quidway] interface vlanif500
[Quidway-vlanif500] ip address 60.1.1.1 255.255.255.0
[Quidway-vlanif500] dhcp select interface
[Quidway-vlanif500] quit
[Quidway] dhcp enable
[Quidway] interface vlanif501
[Quidway-vlanif501] ip address 60.1.2.1 255.255.255.0
[Quidway-vlanif501] dhcp select interface
[Quidway-vlanif501] quit
```

步骤 2 配置 AC1。

配置 AC1 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC1
[AC1] interface GigabitEthernet 0/0/1
[AC1-GigabitEthernet0/0/1] port link-type trunk
[AC1-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-GigabitEthernet0/0/1] quit
[AC1] interface XGigabitEthernet 0/0/27
[AC1-XGigabitEthernet0/0/27] port link-type trunk
[AC1-XGigabitEthernet0/0/27] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
[AC1] interface XGigabitEthernet 0/0/1
[AC1-XGigabitEthernet0/0/1] port link-type trunk
[AC1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/1] quit
```

配置 AC1 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC1] wlan ac-global ac id 1 carrier id  ctc
[AC1] wlan ac-global country-code cn
```

配置 AC1 的源接口，用于 AP 和 AC1 之间建立隧道通信。

```
[AC1] interface vlanif500
[AC1-vlanif500] ip address 60.1.1.2 255.255.255.0
[AC1-vlanif500] quit
[AC1] wlan
```


版权所有 © 华为技术有限公司

```
[AC1-wlan-view] wlan ac source interface vlanif 500
[AC1-wlan-view] quit
```

全局配置备份 AC2 的 IP 地址，AC1 的优先级，用于双链路备份。

```
[AC1-wlan-view] wlan ac protect enable protect-ac 60.1.1.5 priority 2
[AC1-wlan-view] wlan ac protect restore enable
```

说明

- 全局配置 AC 的优先级和备份 AC 的 IP 地址。
- 为了和 AP 视图下配置区分，全局配置的备份 AC 的 IP 地址不是 AC2 的源接口地址。

AP 视图下配置备份 AC2 的 IP 地址，AC1 的优先级，用于双链路备份。

```
[AC1-wlan-view] ap id 0
[AC1-wlan-ap-0] priority 3 protect 60.1.1.3
[AC1-wlan-ap-0] quit
```

说明

- AP 视图下配置 AC 的优先级和备份 AC 的 IP 地址。
- AP 优先选取 AP 视图下配置的 AC 优先级和备份 AC 的 IP 地址，即优先级为 3，备份 AC 的 IP 地址为 60.1.1.3。

配置 AC1 上 AP 的认证方式为“no-auth”。

```
[AC1-wlan-view] ap-auth-mode no-auth
```

配置 AP 域 ID 为 101。

```
[AC1-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```

配置 AP 加入 AP 域 101。

```
[AC-wlan-view] ap id 0
[AC1-wlan-ap-0] region-id 101
[AC1-wlan-ap-0] quit
```

配置 WLAN-ESS 虚接口。

```
[AC1] interface wlan-ess 0
[AC1-WLAN-ESS0] port link-type hybrid
[AC1-WLAN-ESS0] port hybrid untagged vlan 501
[AC1-WLAN-ESS0] quit
```

创建名为“wmm”的 WMM 模板，参数采用默认配置。

```
[AC1] wlan
[AC1-wlan-view] wmm-profile name wmm id 1
[AC1-wlan-wmm-prof-wmm] quit
```

创建名为“radio”的射频模板，绑定 WMM 模板“wmm”。

```
[AC1-wlan-view] radio-profile name radio
[AC1-wlan-radio-prof-radio] wmm-profile name wmm
[AC1-wlan-radio-prof-radio] quit
```

将 AP 对应的射频绑定射频模板“radio”。

```
[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] radio-profile name radio
[AC1-wlan-radio-0/0] quit
```

创建安全模板,安全模板名为“security”，认证模式为 WEP 认证，开放认证，不加密。

```
[AC1-wlan-view] security-profile name security id 1
[AC1-wlan-sec-prof-security] wep authentication-method open-system
[AC1-wlan-sec-prof-security] security-policy wep
[AC1-wlan-sec-prof-security] quit
```


版权所有 © 华为技术有限公司

配置 QoS 策略，创建流量模板。流量模板名为“traffic”，参数采用缺省配置。

```
[AC1-wlan-view] traffic-profile name traffic
[AC1-wlan-traffic-prof-traffic] quit
```

创建 AP 对应的服务集，并绑定流量模板及安全模板、WLAN-ESS 接口。

```
[AC1-wlan-view] service-set name huawei
[AC1-wlan-service-set-huawei] ssid huawei
[AC1-wlan-service-set-huawei] traffic-profile name traffic
[AC1-wlan-service-set-huawei] security-profile name security
[AC1-wlan-service-set-huawei] wlan-ess 0
[AC1-wlan-service-set-huawei] service-vlan 501
[AC1-wlan-service-set-huawei] forward-mode direct-forward
[AC1-wlan-service-set-huawei] quit
```

将 AP 对应的射频绑定服务集“Huawei”。

```
[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] service-set name huawei
[AC1-wlan-radio-0/0] quit
```

#下发 AP 的 WLAN 服务。

```
[AC1-wlan-view] commit ap 0
```

步骤 3 配置 AC2

配置 AC1 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC2
[AC2] interface GigabitEthernet 0/0/1
[AC2-GigabitEthernet0/0/1] port link-type trunk
[AC2-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-GigabitEthernet0/0/1] quit
[AC2 interface XGigabitEthernet 0/0/27
[AC2-XGigabitEthernet0/0/27] port link-type trunk
[AC2-XGigabitEthernet0/0/27] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
[AC2] interface XGigabitEthernet 0/0/1
[AC2-XGigabitEthernet0/0/1] port link-type trunk
[AC2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/1] quit
```

配置 AC2 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC2] wlan ac-global ac id 2 carrier id  ctc
[AC2] wlan ac-global country-code cn
```

配置 AC2 的源接口，用于 AP 和 AC2 之间建立隧道通信。

```
[AC2] interface vlanif500
[AC2-vlanif500] ip address 60.1.1.3 255.255.255.0
[AC2-vlanif500] quit
[AC2] wlan
[AC2-wlan-view] wlan ac source interface vlanif 500
[AC2-wlan-view] quit
```

全局使能双链路备份和回切功能。

```
[AC2-wlan-view] wlan ac protect enable
[AC2-wlan-view] wlan ac protect restore enable
```

AP 视图下配置主用 AC1 的 IP 地址，AC2 的优先级，用于双链路备份。

版权所有 © 华为技术有限公司

```
[AC1-wlan-view] ap id 0
[AC1-wlan-ap-0] priority 6 protect 60.1.1.2
[AC1-wlan-ap-0] quit
```

说明

AC2 其他基本业务的配置请参考 AC1 的配置过程。

步骤 4 验证配置结果

执行命令 **display wlan ac protect**，查看 AC1 的优先级和备份 AC 的 IP 地址。

AP 下的无线接入用户可以搜索到 SSID 标识为 huawei 的 WLAN 网络并正常上线。

当 AP 与 AC1 的链路中断后，AC2 切换为主 AC，保证业务的稳定。

----结束

配置文件

- 接入交换机的配置文件

```
#
 vlan batch 500 to 501
#
 dhcp enable
#
interface Vlanif500
 ip address 60.1.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif501
 ip address 60.1.2.1 255.255.255.0
 dhcp select interface
#
 interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 500
 port trunk allow-pass vlan 500 to 501
#
 interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
```

- 汇聚交换机的配置文件

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
```

- AC1 的配置文件

```
#
 sysname AC1
#
 vlan batch 500 to 501
#
 wlan ac-global carrier id ctc ac id 1
#
interface Vlanif500
```


版权所有 © 华为技术有限公司

```
 ip address 60.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface Wlan-Ess0
 port link-type hybrid
 port hybrid untagged vlan 501
#
wlan
 wlan ac source interface vlanif500
 wlan ac protect enable protect-ac 60.1.1.5 priority 2
 ap-region id 101
 ap-auth-mode no-auth
 ap id 0
  priority 3
  protect-ac 60.1.1.3
  region-id
101
  wmm-profile name wmm id 4
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name huawei id 6
  wlan-ess 0
  ssid huawei
  traffic-profile id 1
  security-profile id 1
  service-vlan 501
 radio-profile name radio id 4
  wmm-profile id 4
 ap 0 radio 0
  radio-profile id 4
  service-set id 6 wlan 1
 #
return
```

- AC2 的配置文件

```
#
 sysname AC2
#
 vlan batch 500 to
501
#
 wlan ac-global carrier id ctc ac id 2
#
interface Vlanif500
 ip address 60.1.1.3 255.255.255.0
#
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/1
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 500 to 501
#
interface Wlan-Ess0
 port link-type hybrid
 port hybrid untagged vlan 501
#
wlan
 wlan ac source interface vlanif500
 wlan ac protect enable
 ap-region id 101
 ap-auth-mode no-auth
 ap id 0
  priority 6
  protect-ac 60.1.1.2
  region-id
101
  wmm-profile name wmm id 4
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name huawei id 6
  wlan-ess 0
  ssid huawei
  traffic-profile id 1
  security-profile id 1
  service-vlan 501
 radio-profile name radio id 4
  wmm-profile id 4
 ap 0 radio 0
  radio-profile id 4
  service-set id 6 wlan 1
 #
return
```

配置全局双链路备份示例

组网需求

为了实现全局双链路备份，AP1、AP2 需要与 AC1 和 AC2 分别建立隧道链接。建立好 CAPWAP 隧道后，AP1、AP2 与 AC1、AC2 之间都会有 CAPWAP 握手报文检测隧道状态，当检测到 AP1、AP2 与 AC1 之间隧道故障时，进行主备倒换，避免 CAPWAP 重新建立连接导致的业务中断。

AC 和 AP 组网图如**图 12-5** 所示。

- 由 Switch 分配业务 VLAN，并给 AP 管理报文打管理 VLAN tag。
- Switch 同时作为 DHCP Server 给 AP 和 STA 分配 IP 地址。
- AP1 和 AP2 上业务数据采用数据直接转发模式。

版权所有 © 华为技术有限公司

图 12-5 配置全局双链路备份示例图

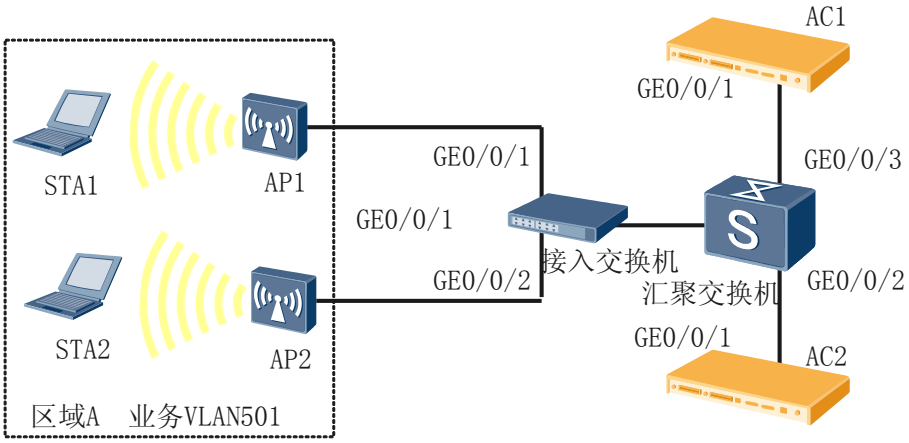


表 12-3 数据规划表

配置项	数据
WLAN 服务	WEP Open-System 认证，不加密。
AP 管理 VLAN	VLAN 500（Switch 分配）
AP 域	101
服务集	● Name：Huawei ● SSID：Huawei ● WLAN 虚接口：WLAN-ESS 0 ● 数据转发模式：直接转发
WLAN 业务 VLAN	501
SwitchVLAN	VLAN 500/501
AC Carrier ID/AC ID	CTC（中国电信）/1
AC1 管理 IP 地址	Vlanif 接口：60.1.1.2/24
AC2 管理 IP 地址	Vlanif 接口：60.1.1.3/24
AP 地址池	60.1.1.4 ～ 60.1.1.254/24
AP 网关	60.1.1.1/24（Switch）
DHCP 服务器	Switch 作为 DHCP 服务器，为 AP 和 STA 分配地址

配置思路

1. 配置接入交换机、汇聚交换机、AC1 和 AC2，实现 AP 和 AC1 和 AC2 的互通。
2. 配置 AC1 的基本功能，包括配置 AC1 运营商标识和 ID、AC1 与 AP 之间通信的源接口，实现 Switch 作为 DHCP Server 功能。
3. 配置 AC1 的优先级和备份 AC 的 IP 地址。

版权所有 © 华为技术有限公司

4. 配置 AP 上线的认证方式，并把 AP1 和 AP2 加入 AP 域中，实现 AP1 和 AP2 正常工作。
5. 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

   其中配置 VAP，需要：

   a. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
   b. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。
   c. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
   d. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。
6. 配置 AC2。

操作步骤

步骤 1 配置接入交换机

#配置接入交换机连接 AP1 的以太网端口（GE0/0/1）类型为 trunk 类型，PVID 为 500。

```
<Quidway> system-view
[Quidway] vlan batch 500 501
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk pvid vlan 500
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/1] quit
```

#配置接入交换机连接 AP2 的以太网端口（GE0/0/2）类型为 trunk 类型，PVID 为 500。

```
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk pvid vlan 500
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/2] quit
```

#配置接入交换机连接汇聚交换机的以太网端口（GE0/0/3）类型为 trunk 类型。

```
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/3] quit
```

步骤 2 配置汇聚交换机，使能 DHCE server

配置汇聚交换机连接接入交换机的 GE 接口透传管理和业务 VLAN。

```
[Quidway] interface XGigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/1] quit
```

配置汇聚交换机连接 AC1 的 GE 接口透传管理和业务 VLAN。

```
[Quidway] interface XGigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/3] quit
```

配置汇聚交换机连接 AC2 的 GE 接口（GE0/0/2）透传管理和业务 VLAN。

```
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
```


版权所有 © 华为技术有限公司

```
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet0/0/2] quit
```

创建 VLANIF 接口，使能 DHCP 服务功能，vlanif 500 为 AP 分配地址，vlanif 501 为 STA 分配 IP 地址。

```
[Quidway] dhcp enable
Quidway] interface vlanif500
[Quidway-vlanif500] ip address 60.1.1.1 255.255.255.0
[Quidway-vlanif500] dhcp select interface
[Quidway-vlanif500] quit
[Quidway] dhcp enable
[Quidway] interface vlanif501
[Quidway-vlanif501] ip address 60.1.2.1 255.255.255.0
[Quidway-vlanif501] dhcp select interface
[Quidway-vlanif501] quit
```

步骤 3 配置 AC1。

配置 AC1 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC1
[AC1] interface GigabitEthernet 0/0/1
[AC1-GigabitEthernet0/0/1] port link-type trunk
[AC1-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-GigabitEthernet0/0/1] quit
[AC1] interface XGigabitEthernet 0/0/27
[AC1-XGigabitEthernet0/0/27] port link-type trunk
[AC1-XGigabitEthernet0/0/27] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
[AC1] interface XGigabitEthernet 0/0/1
[AC1-XGigabitEthernet0/0/1] port link-type trunk
[AC1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/1] quit
```

配置 AC1 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC1] wlan ac-global ac id 1 carrier id  ctc
[AC1] wlan ac-global country-code cn
```

配置 AC1 的源接口，用于 AP 和 AC1 之间建立隧道通信。

```
[AC1] interface vlanif500
[AC1-vlanif500] ip address 60.1.1.2 255.255.255.0
[AC1-vlanif500] quit
[AC1] wlan
[AC1-wlan-view] wlan ac source interface vlanif 500
[AC1-wlan-view] quit
```

配置备份 AC2 的 IP 地址，AC1 的优先级，用于双链路备份。

```
[AC1-wlan-view] wlan ac protect enable protect-ac 60.1.1.3 priority 2
[AC1-wlan-view] wlan ac protect restore enable
```

配置 AC1 上 AP 的认证方式为“no-auth”。

```
[AC1-wlan-view] ap-auth-mode no-auth
```

配置 AP 域 ID 为 101。

```
[AC1-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```

配置 AP1 和 AP2 都加入 AP 域 101。

版权所有 © 华为技术有限公司

```
[AC-wlan-view] ap id 0
[AC1-wlan-ap-0] region-id 101
[AC1-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC1-wlan-ap-1] region-id 101
[AC1-wlan-ap-1] quit
```

配置 WLAN-ESS 虚接口。

```
[AC1] interface wlan-ess 0
[AC1-WLAN-ESS0] quit
```

创建名为“wmm”的 WMM 模板，参数采用默认配置。

```
[AC1] wlan
[AC1-wlan-view] wmm-profile name wmm id 1
[AC1-wlan-wmm-prof-wmm] quit
```

创建名为“radio”的射频模板，绑定 WMM 模板“wmm”。

```
[AC1-wlan-view] radio-profile name radio
[AC1-wlan-radio-prof-radio] wmm-profile name wmm
[AC1-wlan-radio-prof-radio] quit
```

将 AP1 和 AP2 对应的射频绑定射频模板“radio”。

```
[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] radio-profile name radio
[AC1-wlan-radio-0/0] quit
[AC1-wlan-view] ap 1 radio 0
[AC1-wlan-radio-1/0] radio-profile name radio
[AC1-wlan-radio-1/0] quit
```

创建安全模板,安全模板名为“security”，认证模式为 WEP 认证，开放认证，不加密。

```
[AC1-wlan-view] security-profile name security id 1
[AC1-wlan-sec-prof-security] wep authentication-method open-system
[AC1-wlan-sec-prof-security] security-policy wep
[AC1-wlan-sec-prof-security] quit
```

#配置 QoS 策略，创建流量模板。流量模板名为“traffic”，参数采用缺省配置。

```
[AC1-wlan-view] traffic-profile name traffic
[AC1-wlan-traffic-prof-traffic] quit
```

#创建与 AP1 及 AP2 对应的服务集，并绑定流量模板及安全模板、WLAN-ESS 接口。

```
[AC1-wlan-view] service-set name huawei
[AC1-wlan-service-set-huawei] ssid huawei
[AC1-wlan-service-set-huawei] traffic-profile name traffic
[AC1-wlan-service-set-huawei] security-profile name security
[AC1-wlan-service-set-huawei] wlan-ess 0
[AC1-wlan-service-set-huawei] service-vlan 501
[AC1-wlan-service-set-huawei] forward-mode direct-forward
[AC1-wlan-service-set-huawei] quit
```

#将 AP1 和 AP2 对应的射频绑定服务集“Huawei”。

```
[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] service-set name huawei
[AC1-wlan-radio-0/0] quit
[AC1-wlan-view] ap 1 radio 0
[AC1-wlan-radio-1/0] service-set name huawei
[AC1-wlan-radio-1/0] quit
```

#下发 AP 的 WLAN 服务。

```
[AC1-wlan-view] commit ap 0
[AC1-wlan-view] commit ap 1
```


版权所有 © 华为技术有限公司

步骤 4 配置 AC2

配置 AC1 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC2
[AC2] interface GigabitEthernet 0/0/1
[AC2-GigabitEthernet0/0/1] port link-type trunk
[AC2-GigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-GigabitEthernet0/0/1] quit
[AC2 interface XGigabitEthernet 0/0/27
[AC2-XGigabitEthernet0/0/27] port link-type trunk
[AC2-XGigabitEthernet0/0/27] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
[AC2] interface XGigabitEthernet 0/0/1
[AC2-XGigabitEthernet0/0/1] port link-type trunk
[AC2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/1] quit
```

配置 AC2 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC2] wlan ac-global ac id 2 carrier id  ctc
[AC2] wlan ac-global country-code cn
```

配置 AC2 的源接口，用于 AP 和 AC2 之间建立隧道通信。

```
[AC2] interface vlanif500
[AC2-vlanif500] ip address 60.1.1.3 255.255.255.0
[AC2-vlanif500] quit
[AC2] wlan
[AC2-wlan-view] wlan ac source interface vlanif 500
[AC2-wlan-view] quit
```

配置主用 AC2 的 IP 地址，AC2 的优先级，用于双链路备份。

```
[AC2-wlan-view] wlan ac protect enable protect-ac 60.1.1.2 priority 5
[AC2-wlan-view] wlan ac protect restore enable
```

说明

AC2 基本业务的配置请参考 AC1 的配置。

步骤 5 验证配置结果

执行命令 **display wlan ac protect**，查看 AC1 的优先级和备份 AC 的 IP 地址。

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei 的 WLAN 网络并正常上线。

当 AP 与 AC1 的链路中断后，AC2 切换为主 AC，保证业务的稳定。

----结束

配置文件

- 接入交换机的配置文件

```
#
 vlan batch 500 to 501
#
 dhcp enable
#
interface Vlanif500
 ip address 60.1.1.1 255.255.255.0
```


版权所有 © 华为技术有限公司

```
 dhcp select interface
#
interface Vlanif501
 ip address 60.1.2.1 255.255.255.0
 dhcp select interface
#
 interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 500
 port trunk allow-pass vlan 500 to 501
#
 interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 500
 port trunk allow-pass vlan 500 to 501
#
 interface GigabitEthernet0/0/3
 port link-type trunk
  port trunk allow-pass vlan 500 to 501
#
```

- 汇聚交换机的配置文件

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
```

- AC1 的配置文件

```
#
 sysname AC1
#
 vlan batch 500 to
501
#
 wlan ac-global carrier id ctc ac id 1
#
interface Vlanif500
 ip address 60.1.1.2 255.255.255.0
#
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#

interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface Wlan-Ess0
#
wlan
 wlan ac source interface vlanif500
 wlan ac protect enable protect-ac 60.1.1.3 priority 2
 ap-region id 101
 ap-auth-mode no-auth
```


版权所有 © 华为技术有限公司

```
 ap id 0
  region-id
101
  wmm-profile name wmm id 4
 ap id 1
  region-id
101
  wmm-profile name wmm id 4
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name huawei id 6
  wlan-ess 0
  ssid huawei
  traffic-profile id 1
  security-profile id 1
  service-vlan 501
 radio-profile name radio id 4
  wmm-profile id 4
 ap 0 radio 0
  radio-profile id 4
  service-set id 6 wlan 1
 ap 1 radio 0
  radio-profile id 4
  service-set id 6 wlan 1
 #
return
```

- AC2 的配置文件

```
#
 sysname AC2
#
 vlan batch 500 to
501
#
 wlan ac-global carrier id ctc ac id 2
#
interface Vlanif500
 ip address 60.1.1.3 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface Wlan-Ess0
#
wlan
 wlan ac source interface vlanif500
 wlan ac protect enable protect-ac 60.1.1.2 priority 5
 ap-region id 101
 ap-auth-mode no-auth
 ap id 0
   region-id
101
   wmm-profile name wmm id 4
 ap id 1
   region-id
101
   wmm-profile name wmm id
4
   traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name huawei id 6
```


版权所有 © 华为技术有限公司

```
 wlan-ess 0
 ssid huawei
 traffic-profile id 1
 security-profile id 1
 service-vlan 501
radio-profile name radio id 4
 wmm-profile id 4
ap 0 radio 0
 radio-profile id 4
 service-set id 6 wlan 1
ap 1 radio 0
 radio-profile id 4
 service-set id 6 wlan
1
#
return
```

12.2 WLAN WDS 配置

介绍 WLAN WDS 业务配置过程。

12.2.1 WDS 简介

WDS 概述

WDS（Wireless Distribution System，无线分布式系统）：通过无线虚链路连接两个或者多个独立的有线局域网或者无线局域网，组建一个互通的网络实现数据访问。

传统 WLAN 业务中，AP 必须连接到已有的有线网络才可以为无线用户提供网络访问服务。为了扩大无线网络的覆盖面积，需要用电缆、交换机、电源等设备将众多 AP 与 AC 相互建立起连接，这将导致最终的部署成本较高，且耗时较长。

使用 WLAN WDS 技术，AP 之间可以是无线连接的，易于在一些复杂的环境中方便快捷的建设无线局域网。另一方面，使用 WDS 技术将众多 AP 部署成 WDS 网络，则 AP 间可以建立起无线的、多跳的连接，进而 AP 就可以通过无线方式连接到 AC。 WDS 网络的优点包括：

- 低成本，高性能。
- 扩展性好，无需铺设新的有线连接即可部署更多的 AP。
- 易于在地铁、公司、大型仓储、制造、码头等较复杂的环境部署无线网络。

WDS 技术有关概念

如图 12-6 所示，对于 WDS 技术需要了解以下相关概念。

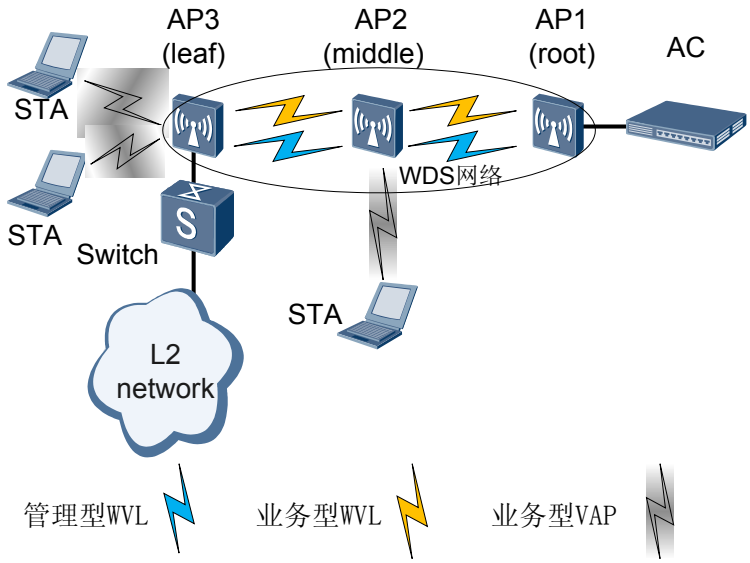
1. 在传统 WLAN 业务中，AP 通过创建业务型 VAP 以便 STA(Station,站点,即无线终端)接入。相似的，在 WDS 网络中，AP 通过创建网桥型 VAP 以便让邻居网桥接入，进而两者之间建立起无线虚链路。
   - 网桥：AP 射频上提供 WDS 业务的功能实体。
   - 业务型 VAP：AP 为 STA 提供的 WLAN 业务接入点。
   - 网桥型 VAP：AP 网桥上为邻居网桥提供的与之建立无线虚链路的接入点。网桥型 VAP 是成对出现的，分别称之 AP 型网桥和 STA 型网桥。其中，AP 型网桥是为 STA 型网桥提供与之建立连接的接入点。

版权所有 © 华为技术有限公司

- WVL（Wireless Virtual Link，无线虚链路）：两个分属不同 AP 网桥的网桥型 VAP 建立起的连接。
- 业务型 WVL：业务型无线虚链路，WDS 网络中的业务数据通道。
- 管理型 WVL：管理型无线虚链路，WDS 网络中的管理数据通道。在使能各 AP 的射频网桥功能后，AP 间会自动建立起管理型 WVL，该链路仅允许管理、配置报文通过。

2. 根据 AP 在 WDS 网络中的实际位置，AP 射频网桥的工作模式有三种，分别为 root 模式、middle 模式、leaf 模式。
   - root 模式：AP 作为根节点直接与 AC 通过有线相连，另以 AP 型网桥向下供 STA 型网桥接入。
   - middle 模式：AP 作为中间节点以 STA 型网桥向上连接 AP 型网桥、以 AP 型网桥向下供 STA 型网桥接入。
   - leaf 模式：AP 作为叶子节点以 STA 型网桥向上连接 AP 型网桥。
3. 在利用 WDS 技术部署的 WLAN 网络中的 AP 与传统 WLAN 网络中的 AP 有所不同，其有线口不仅仅只用于连接 AC，还可以连接交换机或主机。根据 AP 在 WDS 网络中的实际位置，AP 有线口的工作模式有两种，分别为 root 模式、endpoint 模式。
   - root 模式：用于连接 AC。
   - endpoint 模式：用于连接交换机或直接连接主机。

图 12-6 利用 WDS 技术部署的 WLAN 网络示意图

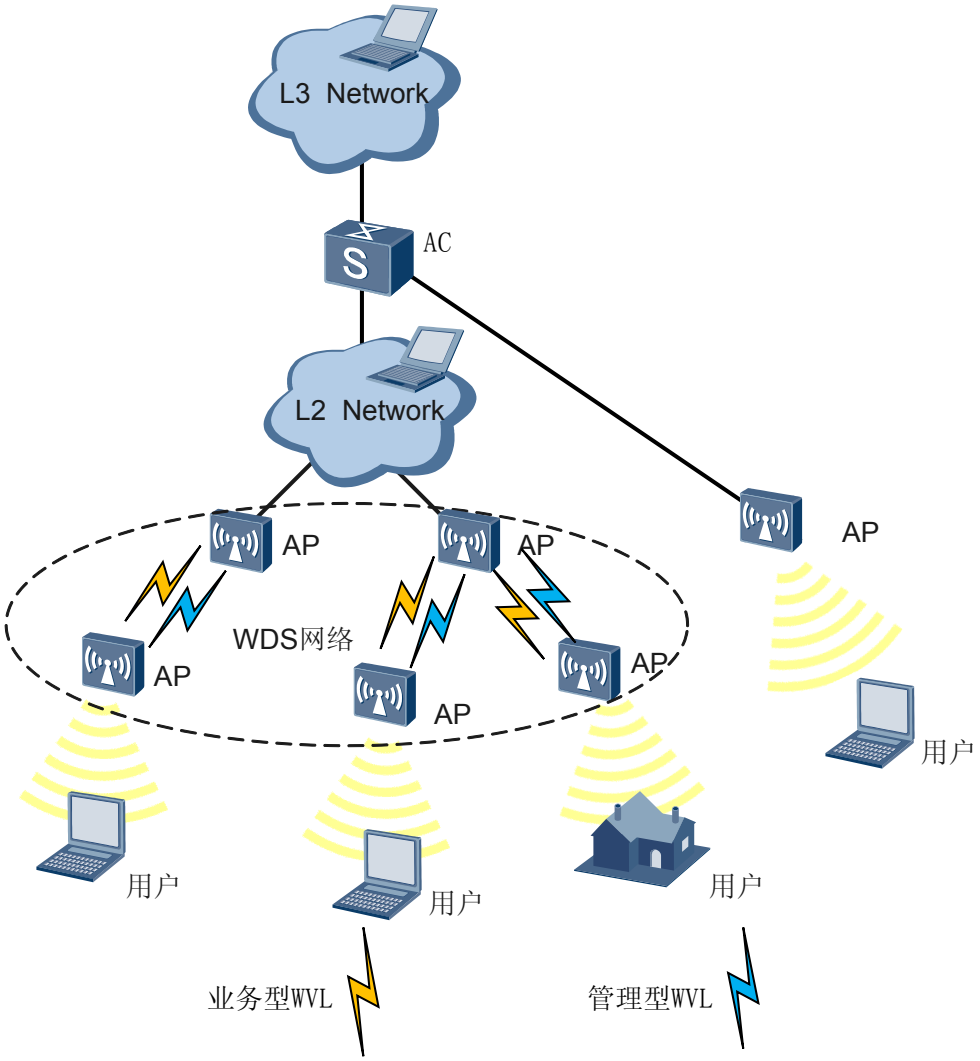


WDS 组网应用

如图 12-7 所示，使用 WDS 技术将众多 AP 部署成 WDS 网络，则 AP 间可以建立起无线的、多跳的连接，进而 AP 就可以通过无线方式连接到 AC。另一方面，对于终端用户而言，是感知不到传统 WLAN 网络与利用 WDS 技术部署的无线网络的区别，因为这两种网络只是在骨干网部分有所不同。

版权所有 © 华为技术有限公司

图 12-7 AP 通过 WDS 接入 AC 示意图



说明

AC 角色由 AC6605 承担。

12.2.2 AC6605 支持的 WLAN WDS 特性

AC6605 作为 AC，支持的有关 WDS 的特性包括射频网桥管理、网桥白名单管理、AP 有线口管理、WDS 网络的 STP 功能管理。同时需要注意，管理员在 AC6605 上配置的所有有关 AP 的参数只有下发到 AP 后才能真正的生效。

射频网桥管理

根据 AP 在 WDS 网络中的实际位置，AC6605 支持为 AP 射频网桥配置不同的工作模式。

网桥模板是 AP 与其邻居建立 WVL 的必备属性集。管理员通过在 AC6605 上配置网桥模板并将其绑定到 AP 射频，使得 AP 射频自动创建网桥型 VAP，进而 AP 射频依靠不同 VAP 的参数建立和维护与邻居间的 WVL。

版权所有 © 华为技术有限公司

网桥白名单管理

在 WDS 网络中，管理员通过 AC6605 为 AP 射频网桥配置网桥白名单后，则只有匹配该白名单中 MAC 地址的 AP 能够关联到此 AP 射频。

AP 有线口管理

根据 AP 在 WDS 网络中的实际位置，AC6605 支持为 AP 有线口配置不同的工作模式。

当 AP 有线口的工作模式配置为 endpoint 时，能够通过 AC6605 为其配置允许通过的 VLAN 数据。同时 AC6605 支持使能 AP 有线口的用户隔离功能。

WDS 网络的 STP 功能管理

AC6605 支持对射频网桥以及 AP 有线口下的 STP(Spanning Tree Protocol,生成树协议)功能进行管理。

WLAN WDS 业务配置流程

WLAN WDS 业务配置流程可以分为以下几个步骤：

1. 配置 AP 射频参数，并使能射频的网桥功能。
2. 配置网桥模板。
3. （可选）配置网桥白名单。
4. 配置网桥型 VAP 并将其下发到 AP。

说明

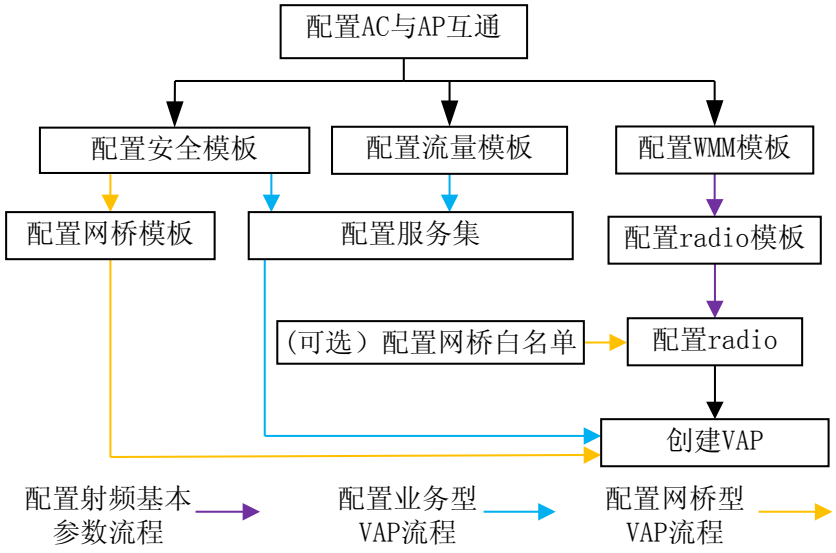
在配置 WDS 过程中，如果需要在 AP 有线口下直接连接主机或交换机，则需要配置 AP 有线口参数。同时，为了避免网桥间以及 AP 有线口下部署的网络间可能发生的环路现象，需要配置其 STP 功能。

图 12-8 为“利用 WDS 技术部署 WLAN 业务的配置流程”。配置网桥型 VAP 的过程即为配置 WLAN WDS 业务的过程，配置业务型 VAP 的过程即为配置传统 WLAN 业务的过程。从图中可以看出这两种 VAP 的配置有如下特点。

1. 网桥型 VAP 与业务型 VAP 类似，是由网桥模板绑定到射频上而自动创建的。
2. 网桥模板类似于传统 WLAN 业务中的服务集，两者区别是网桥模板只需要绑定安全模板即可。
3. 网桥型 VAP 与业务型 VAP 都是基于射频创建的，所以在配置两者之前都需要确保射频相关参数已配置完成。
4. 网桥白名单的配置是可选的，需要注意的是网桥白名单是绑定到射频上而不是绑定到网桥模板。

版权所有 © 华为技术有限公司

图 12-8 利用 WDS 技术部署 WLAN 业务的配置流程



说明

强烈建议无线桥接级联 AP 最多不要超过 3 台。

root，middle 和 leaf 模式下的各个 AP，最多可以带 6 台桥接 AP。

12.2.3 配置 WDS 业务

介绍 AC+瘦 AP 组网模式下的 WLAN WDS 业务配置过程。

配置网桥模式

背景信息

AP 射频之间建立 WVL 之前，需要使能 AP 射频的网桥功能。根据 AP 在 WDS 网络中的位置，可对射频网桥配置三种不同的工作模式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*，进入 AP 指定射频视图。

步骤 4 执行命令 **bridge enable** [**mode** { **root** | **middle** | **leaf** }]，配置射频网桥的工作模式。

缺省情况下，射频网桥工作模式为 disable。

说明

支持 WDS 功能的 AP 型号为：AP6010SN-GN、AP6010DN-AGN、AP6510DN-AGN、AP6610DN-AGN、WA615DN-AGN、WA615DSN-GN、WA655DN-AGN。

----结束

版权所有 © 华为技术有限公司

配置网桥模板

前提条件

安全模板已经成功创建。

背景信息

网桥模板的功能与传统 WLAN 业务中的服务集 service-set 相似，其用于绑定到 AP 指定射频上以创建网桥型 VAP。

网桥模板是一个属性集，包含了 AP 与其邻居建立 WVL 的必备参数。管理员将一个网桥模板和一个 radio 绑定后，该 radio 将继承所绑定的网桥模板的所有属性，进而自动创建网桥型 VAP。radio 依靠不同 VAP 的参数建立和维护与邻居间的 WVL。

通过配置网桥模板中加入的 VLAN，可以控制 WVL 允许通过的数据。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **bridge-profile** {**name** *profile-name* | **id** *profile-id* } *，创建并进入网桥模板。

步骤 4 执行命令 **bridge-name** *name*，指定网桥模板的标识。

缺省情况下，bridge-profile 无标识。

步骤 5 执行命令 **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，在网桥模板上以 Tagged 形式加入一个或一组 VLAN。

缺省情况下，bridge-profile 上没有配置 VLAN。

说明

一个网桥模板最多允许加入 256 个 VLAN。

步骤 6 执行命令 **security-profile** { **name** *profile-name* | **id** *profile-id* }，在网桥模板上绑定指定安全模板。

缺省情况下，bridge-profile 上没有绑定安全模板。

----结束

配置网桥型 VAP

前提条件

AP 指定射频已经绑定了射频模板，具体请参见《*WLAN 基本业务配置 配置 WLAN 射频*》中的“**在射频上绑定射频模板**”。

网桥模板已经创建并配置好参数，具体请参见**配置网桥模板**。

在 AP 指定射频上绑定网桥模板之前，需要与 VAP 的 wlan-id 做互斥检查，只有当前射频 VAP 的 13 和 14 两个 wlan-id 未被使用，才可以将网桥模板绑定到射频。

版权所有 © 华为技术有限公司

背景信息

网桥型 VAP 与业务型 VAP 类似，是 AP 无线物理端口上的逻辑单元，其有独立的 MAC 地址（bssid）和网桥标识（Bridge-Name）。AP 指定射频依靠网桥型 VAP 的参数建立和维护与邻居间的 WVL。

一个射频上仅支持绑定一个网桥模板，生成两个网桥型 VAP。系统自动为其分配 13、14 两个 wlan-id。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*，进入 AP 指定射频视图。

步骤 4 执行命令 **bridge-profile** { **name** *profile-name* | **id** *profile-id* } ，在射频上绑定网桥模板。

缺省情况下，radio 上没有绑定 bridge-profile。

----结束

检查配置结果

背景信息

WDS 基本业务配置完成后，可以查看已配置的信息。

操作步骤

步骤 1 执行命令 **display bridge-profile** { **all** | **name** *profile-name* | **id** *profile-id* | **bridge-name** *name* },查看配置的网桥模板信息。

步骤 2 执行命令 **display vap** { **all** | **ap** *ap-id* [**radio** *radio-id*] } **type bridge-profile**，查看配置的网桥型 VAP。

说明

根据实际需要，使用 **display vap** 命令，可以分别查看业务型 VAP、网桥型 VAP 等信息。

步骤 3 执行命令 **display bridge-link**，查看建立起无线虚链路的射频网桥信息。

----结束

12.2.4 配置网桥白名单

背景信息

在 AP 射频上配置网桥白名单后，则只有匹配该白名单中 MAC 地址的 AP 能够关联到此 AP 射频，进而如果通过安全认证，则双方建立起 WVL。

如果不为 AP 射频网桥配置网桥白名单，则所有的邻居 AP 都可以关联到此 AP 射频。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 创建并配置网桥白名单。

1. 执行命令 **bridge-whitelist** { **name** *whitelist-name* | **id** *whitelist-id* } *，创建并进入网桥白名单。

   缺省情况下，系统无网桥白名单模板。

2. 执行命令 **peer ap mac** *mac-address*，配置网桥白名单中允许接入的邻居 AP 的 MAC 地址。
3. 执行命令 **quit**，返回 WLAN 视图。

步骤 4 在 radio 上绑定网桥白名单。

1. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入 AP 指定射频视图。
2. 执行命令 **bridge-whitelist** { **name** *whitelist-name* | **id** *whitelist-id* }，在 radio 上绑定已配置的网桥白名单。

   缺省情况下，radio 上没有绑定 bridge-whitelist。

步骤 5 执行命令 **bridge whitelist enable**，使能射频上绑定的网桥白名单。

网桥白名单在绑定到 AP 射频后只有使能才能生效。

缺省情况下，不使能射频网桥的白名单。

----结束

检查配置结果

- 执行命令 **display bridge-whitelist** { **all** | **id** *whitelist-id* | **name** *whitelist-name* }，用以查看网桥白名单的配置信息。

12.2.5 配置 AP 有线口参数

背景信息

在 WLAN WDS 网络中 AP 可通过 WVL 接入 AC，所以在传统 WLAN 中 AP 用来连接 AC 的有线口就空闲下来。

在 WDS 网络部署中，必须有一个 AP 是通过有线口和 AC 相连，该 AP 有线口的工作模式即为 root。对于其他通过 WVL 连接到 AC 的 AP，其有线口在配置为 endpoint 模式后可以直接在其上连接主机或部署二层网络，这时有线口的作用就类似于交换机的 Hybrid 端口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap id** *ap-id* ，进入 AP 视图。

步骤 4 配置 AP 有线口参数。

版权所有 © 华为技术有限公司

1. 执行命令 **lineate-port mode** { **root** | **endpoint** }，配置 AP 有线口的工作模式。

   缺省情况下，AP 有线口的工作模式为 root。

   说明

   在更改 AP 有线口的工作模式后，需要使用命令 **ap-reset** 重置 AP 才能生效。

2. 执行命令 **lineate-port pvid vlan** *vlan-id*,配置 AP 有线口的 pvid VLAN。

   缺省情况下，AP 有线口没有 pvid VLAN。

3. 执行命令 **lineate-port vlan** { **tagged** | **untagged** } { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置 AP 有线口加入的 VLAN。

   AP 有线口下最多支持加入 256 个 VLAN。

   缺省情况下，AP 有线口没有加入任何 VLAN。

4. 执行命令 **lineate-port user-isolate enable**，使能 AP 有线口的用户隔离功能。

   AP 有线口只有在 endpoint 工作模式下才能够使能用户隔离功能。

   缺省情况下，AP 有线口的用户隔离功能不使能。

----结束

检查配置结果

执行命令 **display ap** { **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* }，查看 AP 有线口相关参数。

12.2.6 配置 STP 功能

背景信息

当 AP 有线口的工作模式为 endpoint 并在其下部署二层网络时，网络间可能会出现环路现象。在 WDS 网络部署中，AP 射频网桥之间也可能会出现网络环路。

通过使能射频网桥或 AP 有线口下的 STP 功能，能够有效的防止 WDS 网络中或 AP 有线口下部署的二层网络发生环路。

操作步骤

步骤 1 使能 AP 射频网桥的 STP 功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入 AP 指定射频视图。
4. 执行命令 **bridge stp enable**，使能射频网桥的 STP 功能。

   缺省情况下，射频网桥的 STP 功能不使能。

5. 执行命令 **quit**，返回 WLAN 视图。

步骤 2 使能 AP 有线口的 STP 功能。

1. 执行命令 **ap id** *ap-id*，进入 AP 视图。
2. 执行命令 **bridge stp enable**，使能 AP 有线口的 STP 功能。

版权所有 © 华为技术有限公司

缺省情况下，AP 有线口的 STP 功能不使能。

但是，华为交换机（包括 AC）端口的默认的 STP 开销按 802.1t 标准，而 AP 默认的为 802.1d 标准，如果和华为交换机对接且启用 WDS 的 STP 时，需要在系统视图下执行命令 **stp pathcost-standard dot1d-1998**，正确设置交换机（包括 AC）端口的开销，否则可能造成 WDS root AP 路径被 block。

----结束

12.2.7 配置参数下发

背景信息

在 WLAN WDS 业务配置过程中，在 AC 上配置的所有有关 AP 的参数，必须执行 **commit** 命令使参数下发到 AP 后才能真正的生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **commit** { **all** | **ap** *ap-id* }，将 AC 上配置的参数下发到 AP。

----结束

12.2.8 配置举例

配置利用 WDS 技术部署 WLAN 业务示例

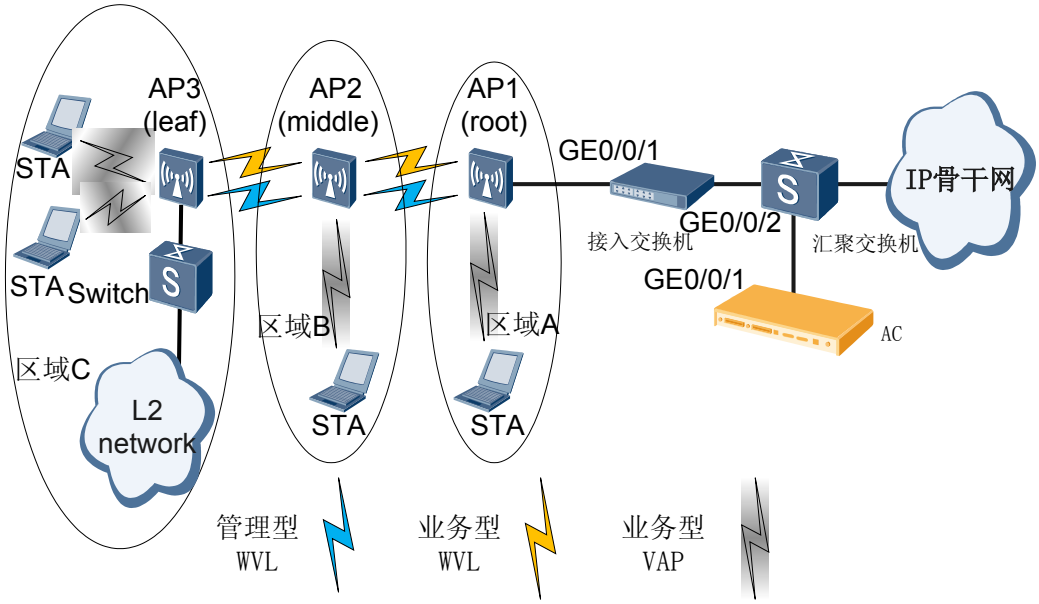
组网需求

如图 12-9 所示，某公司需要为三个临近办公区域（区域 A，区域 B，区域 C）提供 WLAN 上网服务，但是 AC 此时只余一个接口可用，该公司为了节省开支，利用 WDS 技术将区域 B、区域 C 中的 AP 通过无线方式接入 AC。

- AC6605 提供 AC 的功能。
- AC 同时作为 DHCP Server 给 AP 以及个区域内的 STA 分配 IP 地址。
- AP1 通过有线接入 AC，为区域 A 提供 WLAN 业务并且为 AP2 提供网桥接入。
- AP2 通过网桥接入 AC，为区域 B 提供 WLAN 业务并且为 AP3 提供网桥接入。
- AP3 通过网桥接入 AC，为区域 C 提供 WLAN 业务并且在有线口下部署二层网络。

版权所有 © 华为技术有限公司

图 12-9 配置 WLAN WDS 业务示意图



数据准备

表 12-4 为完成配置任务，需要获悉 AP 的以下数据。

AP	类型	MAC
AP1	WA603SN	0025-9e12-6667
AP2	WA603SN	5489-9845-9573
AP3	WA603SN	80fb-0689-81c3

表 12-5 为完成配置任务，需规划以下数据项。

配置项	数据
VLAN	管理 VLAN：100
	业务 VLAN：101、102、103、104、105、106 其中 ● 区域 A：无线业务的 VLAN 为 101 ● 区域 B：无线业务的 VLAN 为 102 ● 区域 C：无线业务的 VLAN 为 103 ● 区域 C：AP3 有线口下 VLAN 为 104、105、106
AP 的业务数据转发模式	直接转发
AC 的源接口 IP 地址	Vlanif 100：192.168.0.1/24
AP 域	AP1:101，AP2:102，AP3:103

版权所有 © 华为技术有限公司

配置项	数据
WMM 模板	名称：wp01
射频模板	名称：rp01
安全模板	● 名称：sp01 ● 安全与认证策略：WPA2+PSK ● 认证密钥：12345678 ● 加密方式：CCMP
流量模板	名称：tp01
网桥模板	● 名称：bp01 ● 网桥标识：ChinaNet01
服务集	● 名称：ss01 ● SSID：ChinaSer01 ● WLAN 虚接口：WLAN-ESS 1 ● 业务数据转发模式：直接转发
	● 名称：ss02 ● SSID：ChinaSer02 ● WLAN 虚接口：WLAN-ESS 2 ● 业务数据转发模式：直接转发
	● 名称：ss03 ● SSID：ChinaSer03 ● WLAN 虚接口：WLAN-ESS 3 ● 业务数据转发模式：直接转发
网桥白名单	名称：bw01

说明

在配置任务之前需确保 AP1、AP2、AP3 提供网桥功能的射频上没有配置 wlan id 为 13、14、15、16 的业务型 VAP。

配置思路

1. 配 AC 与 AP1 互通。
2. 配置 AP 指定射频参数，并配置射频的网桥工作模式。
3. 配置网桥模板与服务集。
4. 配置网桥白名单。
5. 创建 VAP。
6. 配置 AP 有线口参数。
7. 向 AP 下发参数。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配 AC 与 AP1 互通。

1. 配置接入交换机、汇聚交换机和 AC 的相关参数，使数据能够通过 Switch 透传到 AC。

   #配置接入交换机上与 AP1 相连的以太网端口 GE0/0/1 的类型为 trunk 类型，PVID 为 100。

   ```
   <Quidway> system-view
   [Quidway] vlan batch 100 to 105
   [Quidway] interface GigabitEthernet 0/0/1
   [Quidway-GigabitEthernet0/0/1] port link-type trunk
   [Quidway-GigabitEthernet0/0/1] port trunk pvid vlan 100
   [Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 106
   [Quidway-GigabitEthernet0/0/1] quit
   ```

   #配置接入交换机上与汇聚交换机相连的以太网端口 GE0/0/2 的类型为 trunk 类型。

   ```
   <Quidway> system-view
   [Quidway] vlan batch 100 to 105
   [Quidway] interface GigabitEthernet 0/0/1
   [Quidway-GigabitEthernet0/0/1] port link-type trunk
   [Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 106
   [Quidway-GigabitEthernet0/0/1] quit
   ```

   # 配置汇聚交换机连接 AC1 的 GE0/0/2 口透传管理和业务 VLAN。

   ```
   [Quidway] interface GigabitEthernet 0/0/2
   [Quidway-GigabitEthernet0/0/2] port link-type trunk
   [Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 106
   [Quidway-GigabitEthernet0/0/2] quit
   ```

   # 配置 AC1 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

   ```
   <Quidway> system-view
   [Quidway] sysname AC
   [AC] vlan batch 100 to 106
   [AC] interface GigabitEthernet 0/0/1
   [AC-GigabitEthernet0/0/1] port link-type trunk
   [AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 106
   [AC-GigabitEthernet0/0/1] quit
   [AC1] interface XGigabitEthernet 0/0/27
   [AC1-XGigabitEthernet0/0/27] port link-type trunk
   [AC1-XGigabitEthernet0/0/27] port trunk allow-pass vlan 100 to 106
   [AC1-XGigabitEthernet0/0/27] quit
   ```

   # 切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

   ```
   [AC1] interface XGigabitEthernet 0/0/1
   [AC1-XGigabitEthernet0/0/1] port link-type trunk
   [AC1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
   [AC1-XGigabitEthernet0/0/1] quit
   ```

2. 配置 AC 的基本功能。

   #配置 AC 的全局参数（运营商标识、ID、国家码）以方便识别和管理。

   ```
   [AC] wlan ac-global ac id 1 carrier id  ctc
   [AC] wlan ac-global country-code cn
   ```

   #在 AC 上创建 VLANIF 接口，为其配置 IP 地址以便作为数据转发的三层接口，并使能其 DHCP 服务功能。

版权所有 © 华为技术有限公司

AP 需要获取一个 IP 地址才能与 AC 建立连接，此处配置 AC 为 DHCP 服务器，AP 从 AC 上获取 IP 地址。

Vlanif 100 为 AP 分配 IP 地址，Vlanif 101 为区域 A 的 STA 分配 IP 地址，Vlanif 102 为区域 B 的 STA 分配 IP 地址，Vlanif 103 为区域 B 的 STA 分配 IP 地址。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
[AC] interface vlanif 103
[AC-Vlanif102] ip address 192.168.3.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

#配置 AC 的源接口以及 WLAN-ESS 虚接口。

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
[AC-wlan-view] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 101
[AC-WLAN-ESS1] quit
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port link-type hybrid
[AC-WLAN-ESS2] port hybrid untagged vlan 102
[AC-WLAN-ESS2] quit
[AC] interface wlan-ess 3
[AC-WLAN-ESS3] port link-type hybrid
[AC-WLAN-ESS3] port hybrid untagged vlan 103
[AC-WLAN-ESS3] quit
```

3. 离线增加 AP,并配置 AP 域以及 AP 的上线认证方式。

#离线增加 AP。

```
[AC-wlan-view] ap id 1 ap-type WA603SN mac 0025-9e12-6667
[AC-wlan-ap-1] quit
[AC-wlan-view] ap id 2 ap-type WA603SN mac 5489-9845-9573
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3 ap-type WA603SN mac 80fb-0689-81c3
[AC-wlan-ap-3] quit
```

#配置 AP 的上线认证方式为“no-auth”。

AP 认证模式配置为“no-auth”后，AP1 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。AP2 和 AP3 在管理型 WDS 通道建立后，以相同方式上线。

```
[AC-wlan-view] ap-auth-mode no-auth
```

说明

对于初次部放的 AP，根据 AP 型号不同，如果 AP 在上电后射频网桥功能即使能，则 AP 会自动建立起管理型 WVL 通道。如果 AP 在上电后射频网桥功能不使能，则需要手动使能其射频网桥功能。

#配置 AP 域 ID 分别为 101、102、103。

版权所有 © 华为技术有限公司

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
[AC-wlan-view] ap-region id 103
[AC-wlan-ap-region-103] quit
```

#配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102，AP3 加入 AP 域 103。

```
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 101
[AC-wlan-ap-1] quit
[AC-wlan-view] ap id 2
[AC-wlan-ap-2] region-id 102
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3
[AC-wlan-ap-3] region-id 103
[AC-wlan-ap-3] quit
```

步骤 2 配置 AP 指定射频参数，并配置射频的网桥工作模式。

#创建名称为 wp01 的 WMM 模板，采用其默认配置。

```
[AC-wlan-view] wmm-profile name wp01
[AC-wlan-wmm-prof-wp01] quit
```

#创建名称为 rp01 的 radio 模板，采用其默认配置并绑定 WMM 模板“wp01”。

```
[AC-wlan-view] radio-profile name rp01
[AC-wlan-radio-prof-rp01] wmm-profile name wp01
[AC-wlan-radio-prof-rp01] quit
```

#在各 AP 指定射频上绑定 radio 模板“rp01”，并配置射频的网桥工作模式。

1. 在 ap1_radio0（ID 为 1 的 AP 的射频 0 口）上绑定射频模板“rp01”，配置网桥工作模式为 root。

   ```
   [AC-wlan-view] ap 1 radio 0
   [AC-wlan-radio-1/0] radio-profile name rp01
   [AC-wlan-radio-1/0] bridge enable mode root
   [AC-wlan-radio-prof-rp01] quit
   ```

2. 在 ap2_radio0 上绑定射频模板“rp01”，配置网桥工作模式为 middle。

   ```
   [AC-wlan-view] ap 2 radio 0
   [AC-wlan-radio-2/0] radio-profile name rp01
   [AC-wlan-radio-2/0] bridge enable mode middle
   [AC-wlan-radio-prof-rp01] quit
   ```

3. 在 ap3_radio0 上绑定射频模板“rp01”，配置网桥工作模式为 leaf。

   ```
   [AC-wlan-view] ap 3 radio 0
   [AC-wlan-radio-3/0] radio-profile name rp01
   [AC-wlan-radio-3/0] bridge enable mode leaf
   [AC-wlan-radio-prof-rp01] quit
   ```

步骤 3 配置网桥模板与服务集。

#创建名称为 sp01 的安全模板，并配置其安全与认证策略为“WPA2－PSK”、认证密钥为“12345678”、加密方式为“CCMP”。

```
[AC-wlan-view] security-profile name sp01
[AC-wlan-sec-prof-sp01] security-policy wpa2
[AC-wlan-sec-prof-sp01] wpa2 authentication-method psk pass-phrase 12345678 encryption-method ccmp
[AC-wlan-sec-prof-sp01] quit
```

#创建名称为 tp01 的流量模板，采用其默认配置。

```
[AC-wlan-view] traffic-profile name tp01
[AC-wlan-traffic-prof-tp01] quit
```


版权所有 © 华为技术有限公司

#创建名称为 bp01、网桥标识为 ChinaNet01 的网桥模板，并绑定安全模板“sp01”。

```
[AC-wlan-view] bridge-profile name bp01
[AC-wlan-bridge-prof-bp01] bridge-name ChinaNet01
[AC-wlan-bridge-prof-bp01] vlan tagged 100 to 106
[AC-wlan-bridge-prof-bp01] security-profile name sp01
[AC-wlan-bridge-prof-bp01] quit
```

#配置服务集。

1. #创建并配置名称为 ss01、SSID 为 ChinaSer01 的服务集。

```
[AC-wlan-view] service-set name ss01
[AC-wlan-service-set-ss01] traffic-profile name tp01
[AC-wlan-service-set-ss01] security-profile name sp01
[AC-wlan-service-set-ss01] ssid ChinaSer01
[AC-wlan-service-set-ss01] service-vlan 101
[AC-wlan-service-set-ss01] wlan-ess 1
[AC-wlan-service-set-ss01] forward-mode direct-forward
[AC-wlan-service-set-ss01] quit
```

2. #创建并配置名称为 ss02、SSID 为 ChinaSer02 的服务集。

```
[AC-wlan-view] service-set name ss02
[AC-wlan-service-set-ss02] traffic-profile name tp01
[AC-wlan-service-set-ss02] security-profile name sp01
[AC-wlan-service-set-ss02] ssid ChinaSer02
[AC-wlan-service-set-ss02] service-vlan 102
[AC-wlan-service-set-ss02] wlan-ess 2
[AC-wlan-service-set-ss02] forward-mode direct-forward
[AC-wlan-service-set-ss02] quit
```

3. #创建并配置名称为 ss03、SSID 为 ChinaSer03 的服务集。

```
[AC-wlan-view] service-set name ss03
[AC-wlan-service-set-ss03] traffic-profile name tp01
[AC-wlan-service-set-ss03] security-profile name sp01
[AC-wlan-service-set-ss03] ssid ChinaSer03
[AC-wlan-service-set-ss03] service-vlan 103
[AC-wlan-service-set-ss03] wlan-ess 3
[AC-wlan-service-set-ss03] forward-mode direct-forward
[AC-wlan-service-set-ss03] quit
```

步骤 4 配置网桥白名单。

#创建名称为 bw01 的网桥白名单。

```
[AC-wlan-view] bridge-whitelist name bw01
[AC-wlan-br-whitelist-bw01] peer ap mac 0025-9e12-6667
[AC-wlan-br-whitelist-bw01] peer ap mac 5489-9845-9573
[AC-wlan-br-whitelist-bw01] peer ap mac 80fb-0689-81c3
[AC-wlan-br-whitelist-bw01] quit
```

步骤 5 创建 VAP。

#在 ap1_radio0 上创建网桥型 VAP 与业务型 VAP，并绑定网桥白名单。

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] bridge-profile name bp01
[AC-wlan-radio-1/0] bridge-whitelist name bw01
[AC-wlan-radio-1/0] bridge whitelist enable
[AC-wlan-radio-1/0] service-set name ss01
[AC-wlan-radio-prof-rp01] quit
```

#在 ap2_radio0 上创建网桥型 VAP 与业务型 VAP，并绑定网桥白名单。

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] bridge-profile name bp01
[AC-wlan-radio-2/0] bridge-whitelist name bw01
[AC-wlan-radio-2/0] bridge whitelist enable
[AC-wlan-radio-2/0] service-set name ss02
[AC-wlan-radio-prof-rp01] quit
```


版权所有 © 华为技术有限公司

#在 ap3_radio0 上创建网桥型 VAP 与业务型 VAP，并绑定网桥白名单。

```
[AC-wlan-view] ap 3 radio 0
[AC-wlan-radio-3/0] bridge-profile name bp01
[AC-wlan-radio-3/0] bridge-whitelist name bw01
[AC-wlan-radio-3/0] bridge whitelist enable
[AC-wlan-radio-3/0] service-set name ss03
[AC-wlan-radio-prof-rp01] quit
```

步骤 6 配置 AP 有线口参数。

#配置 AP1 有线口参数。

```
[AC-wlan-view] ap id 1
[AC-wlan-ap-1]] lineate-port mode root
[AC-wlan-ap-1]] quit
```

#配置 AP3 有线口参数。

```
[AC-wlan-view] ap id 3
[AC-wlan-ap-3] lineate-port pvid vlan 104
[AC-wlan-ap-3] lineate-port vlan tagged 105
[AC-wlan-ap-3] lineate-port vlan untagged 106
[AC-wlan-ap-3] lineate-port stp enable
[AC-wlan-ap-3] lineate-port mode endpoint
[AC-wlan-ap-3] lineate-port user-isolate enable
[AC-wlan-ap-3] quit
```

说明

更改 AP 有线口的工作模式后，需要重置 AP 才能生效。

步骤 7 向 AP 下发参数。

在 AC 上对 AP 的各项参数的配置只有下发到 AP 后才能生效。

```
[AC-wlan-view] commit ap 1
[AC-wlan-view] commit ap 2
[AC-wlan-view] commit ap 3
```

----结束

配置文件

- Switch 上的配置文件。

```
#
 vlan batch 100 to 105
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 106
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 106
```

- AC 上的配置文件

```
#
 sysname AC
#
 vlan batch 100 to 106
#
 wlan ac-global carrier id ctc ac id 1
#
dhcp enable
#
```


版权所有 © 华为技术有限公司

```
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
#
interface Vlanif103
 ip address 192.168.3.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 106
#
interface Wlan-Ess1
 port hybrid untagged vlan 101
#
interface Wlan-Ess2
 port hybrid untagged vlan 102
#
interface Wlan-Ess3
 port hybrid untagged vlan 103
#
wlan
 wlan ac source interface vlanif100
 ap-region id 101
 ap-region id 102
 ap-region id 103
 ap-auth-mode no-auth
 ap id 1 type-id 6 mac 0025-9e12-6667
  region-id 101
 ap id 2 type-id 6 mac 5489-9845-9573
  region-id 102
 ap id 3 type-id 6 mac 80fb-0689-81c3
  region-id 103
  lineate-port stp enable
  lineate-port mode endpoint
  lineate-port pvid vlan 104
  lineate-port user-isolate enable
  lineate-port vlan tagged 105
  lineate-port vlan untagged 106
 wmm-profile name wp01 id 0
 traffic-profile name tp01 id 0
 security-profile name sp01 id 0
  security-policy wpa2
  wpa2 authentication-method psk pass-phrase 12345678 encryption-method ccmp
 service-set name ss01 id 0
  wlan-ess 1
  ssid ChinaSer01
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 service-set name ss02 id 1
  wlan-ess 2
  ssid ChinaSer02
```


版权所有 © 华为技术有限公司

```
 traffic-profile id 0
 security-profile id 0
 service-vlan 102
service-set name ss03 id 2
 wlan-ess 3
 ssid ChinaSer03
 traffic-profile id 0
 security-profile id 0
 service-vlan 103
bridge-profile name bp01 id 0
 bridge-name ChinaNet01
 security-profile id 0
 vlan tagged 100 to 106
radio-profile name rp01 id 0
 wmm-profile id 0
bridge-whitelist name bw01 id 0
 peer ap mac 0025-9e12-6667
 peer ap mac 5489-9845-9573
 peer ap mac 80fb-0689-81c3
ap 1 radio 0
 radio-profile id 0
 bridge enable mode root
 bridge whitelist enable
 bridge-whitelist id 0
 service-set id 0 wlan 1
 bridge-profile id 0
ap 2 radio 0
 radio-profile id 0
 bridge enable mode middle
 bridge whitelist enable
 bridge-whitelist id 0
 service-set id 1 wlan 1
 bridge-profile id 0
ap 3 radio 0
 radio-profile id 0
 bridge enable mode leaf
 bridge whitelist enable
 bridge-whitelist id 0
 service-set id 2 wlan 1
 bridge-profile id 0
#
```

12.3 WLAN 安全配置

介绍 AC+瘦 AP 组网模式下 WLAN 安全特性的配置过程。

12.3.1 WLAN 安全简介

为了更好的防止未授权用户接入网络，需要实施性能高于 802.11 认证的高级安全机制。安全性高于 802.11 认证的 WLAN 安全机制有以下几种：链路认证方式、WLAN 服务的数据安全和用户接入认证。

链路认证方式

- 开放系统认证（Open System Authentication）

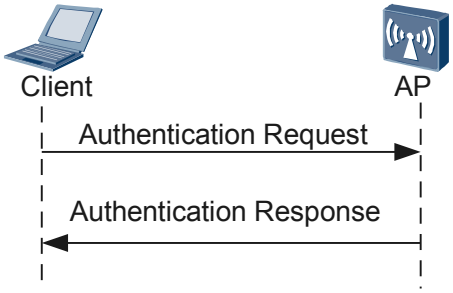
  开放系统认证是缺省使用的认证机制，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。开放系统认证包括两个步骤：

  1. 无线客户端发起认证请求；

版权所有 © 华为技术有限公司

2. AP 确定无线客户端可以通过无线链路认证，并向无线客户端回应认证结果为“成功”。

图 12-10 开放系统认证过程



- 共享密钥认证（Shared key authentication）

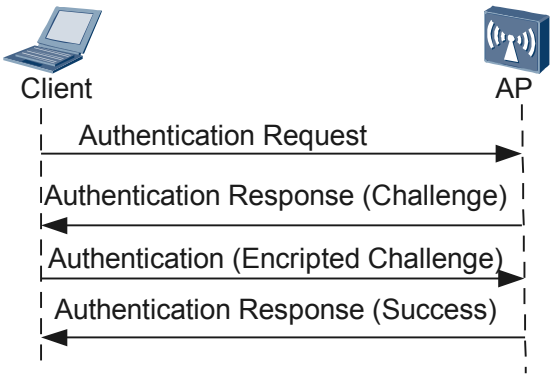
  共享密钥认证是除开放系统认证以外的另外一种认证机制。共享密钥认证需要无线客户端和无线设备端配置相同的共享密钥。

  共享密钥认证的认证过程为：

  1. 无线客户端先向无线设备端发送认证请求，无线设备端会随机产生一个 Challenge 包（即一个字符串）发送给客户端。
  2. 无线客户端会将接收到的字符串拷贝到新的消息中，用密钥加密后再发送给无线设备端。
  3. 无线设备端接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给客户端的字符串进行比较。

     如果相同，则说明客户端拥有无线设备端相同的共享密钥，即通过了 Shared Key 认证，否则 Shared Key 认证失败。

图 12-11 共享密钥认证过程



WLAN 服务的数据安全

相对于有线网络，WLAN 网络存在着与生俱来的数据安全问题。在一个区域内的所有的 WLAN 设备共享一个传输媒介，如果传输媒介和传输链路没有采取适当的加密保护，使用上的风险就会大幅增加，并直接威胁到 WLAN 接入数据的安全。

版权所有 © 华为技术有限公司

802.11 协议也在致力于解决 WLAN 的安全问题，主要的方法为对数据报文进行加密，保证只有特定的设备可以对接收到的报文成功解密。其他的设备虽然可以接收到数据报文,但是由于没有对应的密钥，无法对数据报文解密，从而实现了 WLAN 数据的安全性保护。

目前支持的加密方式有 RC4 加密、TKIP 加密和 CCMP 加密。

用户接入认证

- PSK 认证

  PSK 认证需要在无线客户端和设备端配置相同的预共享密钥，如果密钥相同，PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

- 802.1x 认证

  802.1x 协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指在 WLAN 接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

- MAC 接入认证

  MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。

12.3.2 AC6605 支持的 WLAN 安全特性

AC6605 支持的 WLAN 安全特性包括接入安全策略管理、STA(Station)黑白名单管理及用户隔离管理。

接入安全策略管理

接入安全策略管理即根据网络情况配置用户接入 WLAN 设备采用的认证方式。

AC6605 支持 WEP（Wired Equivalent Privacy）、WPA（Wi-Fi Protected Access）、WPA2 和 WAPI（WLAN Authentication and Privacy Infrastructure）四种接入安全策略。

STA 黑白名单

AC6605 通过将 STA 加入到黑白名单列表中，对 STA 的接入模式进行控制。

- 使能黑名单功能后，如果 STA 匹配黑名单列表，则该 STA 无法关联上 AP，从而无法访问无线网络。
- 使能白名单功能后，如果 STA 匹配白名单列表，则该 STA 可以关联上 AP，从而访问无线网络，而不在白名单内的 STA 将无法访问无线网络。

用户隔离

用户隔离功能是指关联到同一个 AP 上的所有无线用户之间的二层报文相互不能转发，从而使无线用户之间不能直接进行通讯。

AC6605 支持通过在服务集下配置用户隔离、及在 WLAN-ESS 口下配置端口隔离两种方式，实现关联到同一 AP 上的无线用户的二层隔离功能。

版权所有 © 华为技术有限公司

12.3.3 配置用户接入安全策略

配置接入安全策略即根据网络情况配置用户接入 WLAN 设备采用的认证方式。

应用环境

无线局域网由于信道开放的特点，使得攻击者能够很容易的进行窃听，用户信息被恶意的修改并转发。为了更好的防止未授权用户接入网络，WLAN 提供了一些安全策略。根据安全级别的不同，可以选择不同的安全策略。

- WEP 为早期的安全策略方案，存在一定的安全风险，可应用在安全要求不高的开放场合，如机场、车站等。
- WPA 和 WAPI 为安全性较高的安全策略，可为系统提供较高的安全保护。

前置任务

在配置用户接入安全策略之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

数据准备

在配置用户接入安全策略之前，需准备以下数据。

序号	数据
1	安全模板名称、（可选）安全模板 ID
2	WEP 共享密钥、密钥索引
3	WPA/WPA2 共享密钥
4	● （采用共享密钥认证）WAPI 共享密钥 ● （采用证书认证）AC 的证书文件和私钥文件、AC 证书颁布者的证书以及 ASU 的证书文件名、ASU 服务器的 IP 地址。
5	（可选）BK（Base Key）更新间隔、生存期百分比；MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数；证书认证鉴别报文的重传次数

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* } *，配置用户的接入安全模板。

模板创建后，缺省配置如下：

版权所有 © 华为技术有限公司

- 对于 WEP：缺省配置为开放系统认证方式+空密钥。
- 对于 WPA1：缺省配置为 802.1x+PEAP 认证方式+TKIP 数据加密方式。
- 对于 WPA2：缺省配置为 802.1x+PEAP 认证方式+CCMP 数据加密方式。
- 对于 WAPI：缺省配置为 WAI 认证方式+WPI 数据加密方式。

步骤 4 配置各种安全策略：

- WEP 开放系统认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method open-system [data-encrypt]**，配置使用 WEP 开放系统认证。
- WEP 共享密钥认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
  3. 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。

     WEP-40 方式下：10 个十六进制或者 5 个 ASCII 字符；WEP-104 方式下：26 个十六进制或者 13 个 ASCII 字符。
  4. 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

     WEP 的密钥可以配置 4 个，在认证或者加密时只使用一个，使用此命令来指定使用哪一个密钥。
- WPA/WPA2 认证
  1. 执行命令 **security-policy wpa**，配置安全策略为 **wpa** 方式。
  2. 执行命令**{ wpa | wpa2 } authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 dot1x 认证方式和相应的加密方式。

     说明

     如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在 WLAN-ESS 接口下执行 **dot1x-authentication enable**。

     WPA 与 WPA2 认证的不同点主要表现在协议报文格式上，安全性上几乎没有差别。
  3. 执行命令**{ wpa | wpa2 } authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
- WAPI 认证
  1. 执行命令 **security-policy wapi**，配置安全策略为 **wapi** 方式。
  2. 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。

     WAPI 的认证方式支持基于证书和基于预共享密钥两种，当用户选择基于预共享密钥时，需要输入共享密钥。
  3. 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file_name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
  4. 执行命令 **wapi import private-key file-name** *file_name*，导入 AC 的私钥文件。
  5. 执行命令 **wapi asu ip** *ip-address*，配置 ASU 服务器的 IP 地址。

版权所有 © 华为技术有限公司

WAPI 证书方式下，AC 会将证书发送到该 IP 地址所在的 ASU 服务器。

6. （可选）执行如下命令修改 WAPI 的参数：
   - 执行命令 **wapi** { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-interval* }，配置 BK 更新间隔、生存期百分比。

     缺省情况下，BK 的更新间隔为 43200s，生存期百分比为 70%。
   - 执行命令 **wapi** { **msk-update-interval** *msk-interval* | **msk-update-packet** *msk-packet* | **msk-retrans-count** *msk-count* }，配置 MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数。

     缺省情况下，MSK 更新间隔为 86400s，MSK 更新报文数为 10000，MSK 密钥协商报文重传次数为 3 次。
   - 执行命令 **wapi cert-retrans-count** *cert-count*，配置证书认证鉴别报文的重传次数。

     缺省情况下，重传次数为 3 次。
   - 执行命令 **wapi** { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }，配置 WAPI 的 USK 和 MSK 的更新方式。

     缺省情况下，USK 和 MSK 都是基于时间更新。

----结束

检查配置结果

执行命令 **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] }，查看配置的安全模板信息。

查询单个模板的详细信息。

```
<Quidway> display security-profile id 0 detail
  ------------------------------------------------------------
  Profile name                    : lw
  Profile ID                      : 0
  Authentication                  : Share key
  Encryption                      : WEP-40
  ------------------------------------------------------------
  Service-set ID                  SSID
  0                               l00129796_9300
  1                               l00129796_93002
  ------------------------------------------------------------
  WEP's configuration
  Authentication                  : Share key
  Encryption                      : WEP-40
  Key 0                           : *****
  Key 1                           : Empty
  Key 2                           : Empty
  Key 3                           : Empty
  Default key ID                  : 0
  ------------------------------------------------------------
  WPA's configuration
  Authentication                  : WPA  802.1x + PEAP
  Encryption                      : TKIP
  ------------------------------------------------------------
  WPA2's configuration
  Authentication                  : WPA2 802.1x + PEAP
  Encryption                      : CCMP
  ------------------------------------------------------------
  WAPI's configuration
  CA certificate filename         : -
  ASU certificate filename        : -
  AC certificate filename         : -
  AC private key filename         : -
```


版权所有 © 华为技术有限公司

```
Authentication server IP          : -
Authentication method             : WAPI PSK
WAI timeout(s)                    : 60
BK update interval(s)             : 43200
BK lifetime threshold(%)          : 70
USK update interval(s)            : 600
USK update packet(k)              : 10
MSK update interval(s)            : 86400
MSK update packet(k)              : 10
Cert auth retrans count           : 3
USK negotiate retrans count       : 3
MSK negotiate retrans count       : 3
USK update method                 : Time-based
MSK update method                 : Time-based
-------------------------------------------------------------
```

12.3.4 配置 STA 黑白名单

通过配置 STA 黑白名单功能，实现更简单、更灵活的控制某个 AP 下的 STA 接入 WLAN 网络。

应用环境

用户如果想让某些 STA 不能访问 WLAN 网络，可以将其加入 STA 黑名单列表中；如果仅想让某些 STA 访问 WLAN 网络，可以将其加入 STA 白名单列表中。

前置任务

在配置 STA 黑白名单之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

数据准备

在配置 STA 黑白名单之前，需准备以下数据。

序号	数据
1	AP ID 号、STA 的 MAC 地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 配置黑白名单

- 配置黑名单
  1. 执行命令 **sta-access-mode ap** *ap-id* { **blacklist** | **whitelist** | **disable** }，配置 STA 接入控制模式为 **blacklist**。

     缺省情况下，STA 接入控制模式为 **disable**。
  2. 执行命令 **sta-blacklist** *mac-address*，配置 STA 黑名单。

版权所有 © 华为技术有限公司

- 配置白名单

  1. 执行命令 **sta-access-mode ap** *ap-id* { **blacklist** | **whitelist** | **disable** }，配置 STA 接入控制模式为 **whitelist**。

     缺省情况下，STA 接入控制模式为 **disable**。

  2. 执行命令 **sta-whitelist** *mac-address*，配置 STA 白名单。

----结束

检查配置结果

- 执行命令 **display sta-access-mode ap** *ap-id*，查看 STA 接入控制模式。

  查询 STA 接入控制模式。

```
<Quidway> display sta-access-mode ap 0
  Station access control mode: disable
```

- 执行命令 **display sta-blacklist**，查看 STA 黑名单列表。

  查询黑名单信息。

```
<Quidway> display sta-blacklist
  Station mac global black list information:
  ------------------------------------------------------------------------------
  ID        MAC
  ------------------------------------------------------------------------------
  0         0026-0000-90a1
  1         0026-0000-909f
  ------------------------------------------------------------------------------
  Total number: 2
```

- 执行命令 **display sta-whitelist**，查看 STA 白名单列表。

  查询白名单信息。

```
<Quidway> display sta-whitelist
  Station mac global white list information:
  ------------------------------------------------------------------------------
  ID        MAC
  ------------------------------------------------------------------------------
  0         0025-9e26-b9bd
  1         001e-907a-b6a6
  2         0026-0000-90a1
  ------------------------------------------------------------------------------
  Total number: 3
```

12.3.5 配置用户隔离

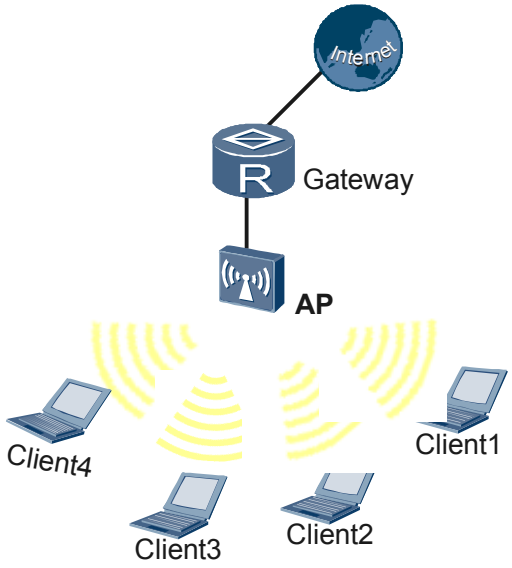
用户隔离功能是指关联到同一个 AP 上的所有无线用户之间的二层报文相互不能转发，从而使无线用户之间不能直接进行通讯，使得用户流量集中至网关转发，便于对该用户进行计费等管理。

应用环境

在各类公共场合以及网络运营商、大中型企业、金融机构等环境中，有些用户需要在热点公共地区（如机场、咖啡店等）通过无线接入 Internet，因此用户认证问题就显得至关重要。如果不能准确可靠地进行用户认证，非法用户就可以未经授权而擅自使用网络资源，不仅会占用宝贵的无线信道资源，增加带宽费用，还会降低合法用户的服务质量，并给无线接入服务提供商带来不可接受的损失。无线用户二层隔离功能结合 IEEE802.11i、RADIUS 的用户认证以及计费方式可以给用户提供专业级的安全保障。

版权所有 © 华为技术有限公司

图 12-12 用户隔离组网



如图 12-12 所示，配置用户隔离后，Cleint 1 ～ Client 4 之间不能直接互通。

前置任务

在配置用户隔离之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 12.1.3 配置 AC 基本功能。
- AP 和 AC 之间网络连接正常。

数据准备

在配置隔离之前，需准备以下数据。

序号	数据
1	服务集模板名称、（可选）服务集 ID
2	（可选）WLAN-ESS 接口编号

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 配置用户隔离

- 如果 AP 与 AC 之间采用数据直接转发方式，则仅需要在服务集下配置用户隔离。
  1. 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } *，配置服务集。
  2. 执行命令 **user-isolate**，配置用户隔离。

版权所有 © 华为技术有限公司

- 如果 AP 与 AC 之间采用数据隧道转发方式，则需要同时在服务集和 WLAN-ESS 接口下配置用户隔离。

  1. 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } *，配置服务集。
  2. 执行命令 **user-isolate** ，配置用户隔离。
  3. 执行命令 **quit**，返回到系统视图。
  4. 执行命令 **interface wlan-ess** *wlan-ess-number* 进入 WLAN-ESS 接口视图。
  5. 执行命令 **port-isolate enable**，使能端口隔离。

----结束

检查配置结果

执行命令 **display service-set** {**id** *service-set-id* | **name** *service-set-name* }，查看服务集下用户隔离是否使能。

12.3.6 配置示例

配置接入安全策略的业务示例

组网需求

如图 12-13 所示，AP1 和 AP2 为接入用户提供 WLAN 服务，用户可以搜索到 5 个无线网络，分别提供不同的用户接入安全策略，要求：

- SSID 为 huawei-1 的无线网络的 WLAN 服务采用开放式系统认证+不加密。
- SSID 为 huawei-2 的无线网络的 WLAN 服务采用共享密钥认证+WEP-40 加密。
- SSID 为 huawei-3 的无线网络采用 WPA1 认证+TKIP 加密。
- SSID 为 huawei-4 的无线网络采用 WPA2 认证+CCMP 加密。
- SSID 为 huawei-5 的无线网络采用 WAPI 认证。

此外，要求 STA3 和 STA4 用户连接到 Internet 时需要通过 RADIUS 服务器进行认证，其中 RADIUS 服务器 IP 地址为 10.10.10.100。STA5 用户使用 WAPI 认证的 ASU 服务器的 IP 地址为 10.10.10.1。

版权所有 © 华为技术有限公司

图 12-13 配置 WLAN 用户接入安全策略示例图

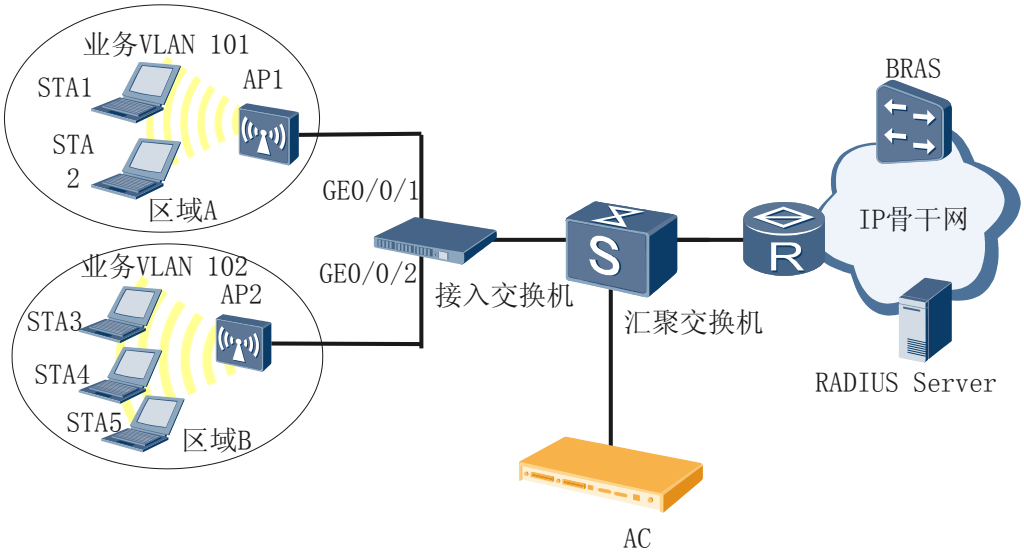


表 12-6 数据规划表

配置项	数据
WLAN 用户接入安全策略	● 安全模板:security-1 ● SSID：huawei-1 ● 认证模式：WEP 开放式系统认证
	● 安全模板:security-2 ● SSID：huawei-2 ● 认证模式：WEP 共享密钥认证 ● 加密方式：WEP-40 加密 密钥短语：12345
	● 安全模板:security-3 ● SSID：huawei-3 ● 认证模式：WPA1 认证（802.1x+PEAP） ● 加密方式：TKIP
	● 安全模板:security-4 ● SSID：huawei-4 ● 认证模式：WPA2 认证（802.1x+PEAP） ● 加密方式：CCMP
	● 安全模板:security-5 ● SSID：huawei-5 ● 认证模式：WAPI 认证（证书认证）
射频模板	radio-1，缺省配置
ASU 服务器 IP 地址	10.10.10.1

版权所有 © 华为技术有限公司

配置项	数据
RADIUS 服务器 IP 地址	10.10.10.100

前提条件

- 配置前请确保 AC 与 ASU Server 和 RADIUS Server 间路由可达。
- 配置安全模板 security-5 的安全策略时，请确保 AC 认证证书 huawei-ac.cer，ASU 认证证书 huawei-asu.cer，Issuer 认证证书 huawei-asu.cer，AC 的私钥证书 huawei-ac.cer 均已保存至 AC。

配置思路

1. 创建接入安全模板，并配置各种接入安全策略，实现各 SSID 网络下接入的 STA 采用不同的安全策略。
2. 创建服务集，并在服务集下绑定接入安全模板和 SSID，实现服务集和接入安全策略、SSID 的关联。
3. 创建 VAP 并下发，实现各 SSID 网络下接入的 STA，根据采用的不同安全策略均可正常访问 WLAN 网络。

说明

- 操作步骤中的前三步与 WLAN 基本业务的配置示例相同，不再赘述，具体请参见**配置 WLAN 基本业务示例**。
- 配置安全模板 security-3 的安全策略时，需配置 WPA 使用 dot1x 认证方式和相应的加密方式。
- 配置安全模板 security-4 的安全策略时，需配置 WPA2 使用 dot1x 认证方式和相应的加密方式。

操作步骤

步骤 1 配置 Switch 和 AC，使 AP 和 AC 互通。（略）

步骤 2 配置 AC 的基本功能。（略）

步骤 3 配置 AP 并上线。（略）

步骤 4 配置 AP 对应的射频。

#创建名为“wmm”的 WMM 模板，参数采用默认配置。

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

#创建名为“radio”的射频模板，绑定 WMM 模板“wmm”。

```
[AC-wlan-view] radio-profile name radio
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm
[AC-wlan-radio-prof-radio-1] quit
```

#将 AP1 和 AP2 对应的射频绑定射频模板“radio”。

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-0/0] radio-profile name radio
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 2 radio 0
```


版权所有 © 华为技术有限公司

```
[AC-wlan-radio-1/0] radio-profile name radio
[AC-wlan-radio-1/0] quit
```

步骤 5 配置 RADIUS Server 与 AAA 方案，并配置域名信息。

```
[AC] radius-server template peap.radius.com
[AC-radius-peap.radius.com] radius-server authentication 10.137.146.163 1812
[AC-radius-peap.radius.com] radius-server accounting 10.137.146.163 1813
[AC-radius-peap.radius.com] radius-server shared-key simple huawei
[AC-radius-peap.radius.com] quit
[AC] aaa
[AC-aaa] authentication-scheme radius
[AC-aaa-authen-radius] authentication-mode radius
[AC-aaa-authen-radius] quit
[AC-aaa] accounting-scheme radius
[AC-aaa-accounting-radius] accounting-mode radius
[AC-aaa-accounting-radius] quit
[AC-aaa] domain peap.radius.com
[AC-aaa-domain-peap.radius.com] authentication-scheme radius
[AC-aaa-domain-peap.radius.com] accounting-scheme radius
[AC-aaa-domain-peap.radius.com] radius-server peap.radius.com
[AC-aaa-domain-peap.radius.com] quit
```

步骤 6 配置 WLAN-ESS 虚接口。配置 WLAN-ESS 1 虚接口使用 802.1X 认证方式。

```
[AC] dot1x enable
[AC] interface wlan-ess 0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid pvid vlan 101
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid pvid vlan 102
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] dot1x-authentication enable
[AC-WLAN-ESS1] dot1x authentication-method eap
[AC-WLAN-ESS1] quit
```

步骤 7 创建接入安全模板 security-1、security-2、security-3、security-4、security-5。

```
[AC] wlan
[AC-wlan-view] security-profile name security-1
[AC-wlan-sec-prof-security-1] quit
[AC-wlan-view] security-profile name security-2
[AC-wlan-sec-prof-security-2] quit
[AC-wlan-view] security-profile name security-3
[AC-wlan-sec-prof-security-3] quit
[AC-wlan-view] security-profile name security-4
[AC-wlan-sec-prof-security-4] quit
[AC-wlan-view] security-profile name security-5
[AC-wlan-sec-prof-security-5] quit
```

步骤 8 配置 WLAN 用户的接入安全模板。

- 配置接入安全模板 security-1 的安全策略。

  #安全模板采用 WEP 开放系统认证。

  ```
  [AC-wlan-view] security-profile name security-1
  [AC-wlan-sec-prof-security-1] wep authentication-method open-system
  [AC-wlan-sec-prof-security-1] security-policy wep
  [AC-wlan-sec-prof-security-1] quit
  ```

- 配置接入安全模板 security-2 的安全策略。

  #安全模板采用 WEP 共享密钥认证，WEP-40 方式，密钥短语为 12345。

  ```
  [AC-wlan-view] security-profile name security-2
  [AC-wlan-sec-prof-security-2] wep authentication-method share-key
  [AC-wlan-sec-prof-security-2] wep key wep-40 pass-phrase 0 12345
  [AC-wlan-sec-prof-security-2] security-policy wep
  [AC-wlan-sec-prof-security-2] quit
  ```


版权所有 © 华为技术有限公司

- 配置接入安全模板 security-3 的安全策略。

  #安全模板的 WPA1 认证采用 802.1x+PEAP 方式，采用 TKIP 加密。

  ```
  [AC-wlan-view] security-profile name security-3
  [AC-wlan-sec-prof-security-3] wpa authentication-method dot1x peap encryption-method tkip
  [AC-wlan-sec-prof-security-3] security-policy wpa
  [AC-wlan-sec-prof-security-3] quit
  ```

- 配置接入安全模板 security-4 的安全策略。

  #安全模板的 WPA2 认证采用 802.1x+PEAP 方式，采用 CCMP 加密。

  ```
  [AC-wlan-view] security-profile name security-4
  [AC-wlan-sec-prof-security-4] wpa2 authentication-method dot1x peap encryption-method ccmp
  [AC-wlan-sec-prof-security-4] security-policy wpa2
  [AC-wlan-sec-prof-security-4] quit
  ```

- 配置接入安全模板 security-5 的安全策略。

  #安全模板的 WAPI 认证采用证书认证方式。

  ```
  [AC-wlan-view] security-profile name security-5
  [AC-wlan-sec-prof-security-5] wapi authentication-method certificate
  ```

  #配置 ASU 服务器的 IP 地址为 10.10.10.1，AC 认证证书为 huawei-ac.cer，ASU 认证证书为 huawei-asu.cer，Issuer 认证证书为 huawei-asu.cer，AC 的私钥证书为 huawei-ac.cer。

  ```
  [Quidway-wlan-sec-prof-security-5] wapi asu ip 10.10.10.1
  [Quidway-wlan-sec-prof-security-5] wapi import certificate ac file-name flash:/huawei-ac.cer
  [Quidway-wlan-sec-prof-security-5] wapi import certificate asu file-name flash:/huawei-
  asu.cer
  [Quidway-wlan-sec-prof-security-5] wapi import certificate issuer file-name flash:/huawei-
  asu.cer
  [Quidway-wlan-sec-prof-security-5] wapi import private-key file-name flash:/huawei-ac.cer
  [Quidway-wlan-sec-prof-security-5] security-policy wapi
  [Quidway-wlan-sec-prof-security-5] quit
  ```

步骤 9 创建服务集，并创建 VAP，下发 WLAN 业务。

- # 创建名为 SS-1 的 service-set，SSID 为 huawei-1，绑定 Traffic 模板 ctc，Security 模板 security-1。下发 WLAN 服务到 AP1 的射频 0 上。

  ```
  [AC-wlan-view] traffic-profile name ctc
  [AC-wlan-traffic-prof-ctc] quit
  [AC-wlan-view] service-set name ss-1
  [AC-wlan-service-set-ss-1] ssid huawei-1
  [AC-wlan-service-set-ss-1] traffic-profile name ctc
  [AC-wlan-service-set-ss-1] security-profile name security-1
  [AC-wlan-service-set-ss-1] service-vlan 101
  [AC-wlan-service-set-ss-1] wlan-ess 0
  [AC-wlan-service-set-ss-1] quit
  [AC-wlan-view]  ap 1 radio 0
  [AC-wlan-radio-1/0] service-set name ss-1
  [AC-wlan-radio-1/0] quit
  [AC-wlan-view] commit ap 1
  ```

- #创建名为 SS-2 的 service-set，SSID 为 huawei-2，绑定 Traffic 模板 ctc，Security 模板 security-2。下发 WLAN 服务到 AP1 的射频 0 上。

  ```
  [AC-wlan-view] service-set name ss-2
  [AC-wlan-service-set-ss-2] ssid huawei-2
  [AC-wlan-service-set-ss-2] traffic-profile name ctc
  [AC-wlan-service-set-ss-2] security-profile name security-2
  [AC-wlan-service-set-ss-2] service-vlan 101
  [AC-wlan-service-set-ss-2] wlan-ess 0
  [AC-wlan-service-set-ss-2] quit
  [AC-wlan-view] ap 1 radio 0
  [AC-wlan-radio-1/0] service-set name ss-2
  [AC-wlan-radio-1/0] quit
  [AC-wlan-view] commit ap 1
  ```

- #创建名为 SS-3 的 service-set，SSID 为 huawei-3，绑定 Traffic 模板 ctc，Security 模板 security-3。下发 WLAN 服务到 AP2 的射频 0 上。

版权所有 © 华为技术有限公司

```
[AC-wlan-view] service-set name ss-3
[AC-wlan-service-set-ss-3] ssid huawei-3
[AC-wlan-service-set-ss-3] traffic-profile name ctc
[AC-wlan-service-set-ss-3] security-profile name security-3
[AC-wlan-service-set-ss-3] service-vlan 102
[AC-wlan-service-set-ss-3] wlan-ess 1
[AC-wlan-service-set-ss-3] quit
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name ss-3
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

- #创建名为 SS-4 的 service-set，SSID 为 huawei-4，绑定 Traffic 模板 ctc，Security 模板 security-4。下发 WLAN 服务到 AP2 的射频 0 上。

```
[AC-wlan-view] service-set name ss-4
[AC-wlan-service-set-ss-4] ssid huawei-4
[AC-wlan-service-set-ss-4] traffic-profile name ctc
[AC-wlan-service-set-ss-4] security-profile name security-4
[AC-wlan-service-set-ss-4] service-vlan 102
[AC-wlan-service-set-ss-4] wlan-ess 1
[AC-wlan-service-set-ss-4] quit
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name ss-4
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

- #创建名为 SS-5 的 service-set，SSID 为 huawei-5，绑定 Traffic 模板 ctc，Security 模板 security-5。下发 WLAN 服务到 AP1 的射频 0 上。

```
[AC-wlan-view] service-set name ss-5
[AC-wlan-service-set-ss-5] ssid huawei-5
[AC-wlan-service-set-ss-5] traffic-profile name ctc
[AC-wlan-service-set-ss-5] security-profile name security-5
[AC-wlan-service-set-ss-5] service-vlan 101
[AC-wlan-service-set-ss-5] wlan-ess 0
[AC-wlan-service-set-ss-5] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-2/0] service-set name ss-5
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 1
```

步骤 10 验证配置结果

AP1 和 AP2 下的接入用户可以搜索到 5 个无线网络，其网络标识分别为 huawei-1、huawei-2、huawei-3、huawei-4、huawei-5。

- 选择 SSID 为 huawei-1 的网络时，用户无需验证即可以正常使用 WLAN 服务。
- 选择 SSID 为 huawei-2 的网络时，用户需要有共享密钥才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-3 和 huawei-4 的网络时，用户需要通过 802.1x 认证才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-5 的网络时，用户需要有匹配的证书才可以使用 WLAN 服务。

----结束

AC 上的配置文件

```
#
 sysname AC
#
 vlan batch 100 to 102
#
 wlan ac-global carrier id ctc ac id 1
#
dhcp enable
#
```


版权所有 © 华为技术有限公司

```
dot1x enable
#
radius-server template peap.radius.com
 radius-server shared-key simple huawei
 radius-server authentication 10.10.10.100 1812
 radius-server accounting 10.10.10.100 1813
#
aaa
 authentication-scheme radius
  authentication-mode radius
 accounting-scheme radius
  accounting-mode
radius
 domain peap.radius.com
  authentication-scheme radius
  accounting-scheme radius
  radius-server
peap.radius.com
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select
interface
#
interface WLAN-ESS0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#

interface Wlan-Ess1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
 dot1x-authentication enable
 dot1x authentication-method
eap
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 to
102
#
wlan
 wlan ac source interface vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 1 type-id 6 mac 5489-9849-8194 sn AB36014894
  region-id 101
 ap id 2 type-id 6 mac 5489-9849-8193 sn AB36014893
  region-id 102
 wmm-profile name wmm id 0
 traffic-profile name ctc id 1
 security-profile name security-1 id 0
 security-profile name security-2 id 1
  wep authentication-method share-key
  wep key wep-40 pass-phrase 0 12345
 security-profile name security-3 id 2
  security-policy wpa
 security-profile name security-4 id 3
  security-policy wpa2
```


版权所有 © 华为技术有限公司

```
security-profile name security-5 id 4
 security-policy wapi
 wapi asu ip 10.10.10.1
 wapi import certificate ac file-name flash:/huawei-ac.cer
 wapi import certificate asu file-name flash:/huawei-asu.cer
 wapi import certificate issuer file-name flash:/huawei-asu.cer
 wapi import private-key file-name flash:/huawei-ac.cer
service-set name ss-1 id 0
 wlan-ess 0
 ssid huawei-1
 traffic-profile id 1
 security-profile id 1
 service-vlan 101
service-set name ss-2 id 1
 wlan-ess 0
 ssid huwei-2
 traffic-profile id 1
 security-profile id 2
 service-vlan 101
service-set name ss-3 id 2
 wlan-ess 1
 ssid huawei-3
 traffic-profile id 1
 security-profile id 3
 service-vlan 102
service-set name ss-4 id 3
 wlan-ess 1
 ssid huawei-4
 traffic-profile id 1
 security-profile id 4
 service-vlan 102
service-set name ss-5 id 4
 wlan-ess 0
 ssid huawei-5
 traffic-profile id 1
 security-profile id 5
 service-vlan 101
radio-profile name radio id 2
 wmm-profile id 0
ap 1 radio 0
 radio-profile name radio
 service-set  id 1 wlan 1
 service-set  id 2 wlan 1
 service-set  id 5 wlan 1
ap 2 radio 0
 radio-profile name radio
 service-set  id 3 wlan 2
 service-set  id 4 wlan 2
```

12.4 WLAN QoS 配置

介绍 AC+瘦 AP 组网模式下的 QoS 业务配置过程。

12.4.1 WLAN QoS 简介

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

802.11 网络提供了基于竞争的无线接入服务，但是不同的应用需求对于网络的要求是不同的，而原始的网络不能为不同的应用提供不同质量的接入服务，所以已经不能满足实际应用的需要。

IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 特性，这个协议的标准化时间很长，在这个过程中，Wi-Fi 组织为了保证不同 WLAN 厂商提供 QoS 的设备之间可

版权所有 © 华为技术有限公司

以互通，定义了 WMM（Wi-Fi Multimedia，Wi-Fi 多媒体）标准。WMM 标准使 WLAN 网络具备了提供 QoS 服务的能力。

WMM

WMM 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。

EDCA

EDCA（Enhanced Distributed Channel Access，增强的分布式信道访问）是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。

AC

AC（Access Category，接入类），WMM 按照优先级从高到低的顺序分为 AC-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个优先级队列，保证越高优先级队列中的报文，抢占信道的能力越高。

12.4.2 AC6605 支持的 WLAN QoS 特性

AC6605 支持的 WLAN QoS 特性包括射频的 QoS 策略管理、VAP 的 QoS 策略管理、用户优先级和用户 CAR 管理。

射频的 QoS 策略

在 802.11 协议中分布式协调功能 DCF(Distributed Coordination Function)规定了 AP 和客户端使用载波监听/冲突避免 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)的接入方式。在占用信道发送数据前，AP 或客户端会监听信道。当信道空闲时间大于或等于规定的空闲等待时间，AP 或客户端在竞争窗口范围内随机选择退避时间进行退避。最先结束退避的设备竞争到信道。

WMM 协议将数据报文分为 4 个 AC 队列(AC_VO、AC_VI、AC_BE、AC_BK)，高优先级的 AC 占用信道的机会大于低优先级的 AC。每个 AC 队列定义了一套信道竞争 EDCA (Enhanced Distributed Channel Access)参数，该参数决定了队列占用信道的能力大小。

EDCA 参数包括：

- 仲裁帧间隙数 AIFSN(Arbitration Inter Frame Spacing Number)，AIFSN 数值越大，用户的空闲等待时间越长。
- 最小竞争窗口指数形式 ECWmin(Exponent form of CWmin)和最大竞争窗口指数形式 ECWmax(Exponent form of CWmax)，决定了平均退避时间值，这两个数值越大，用户的平均退避时间越长。
- 传输机会限制 TXOPLimit(Transmission Opportunity Limit)，用户一次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大，如果是 0，则每次占用信道后只能发送一个报文。
- ACK 策略：NORMAL ACK 是指对于每个发送的单播报文，接收者在成功接收到发送报文后，都要发送一个应答 ACK 进行确认。No ACK 指在通信质量很好、干扰很小的情况下，我们不进行应答 ACK，这样发送失败也不会重发，但是可以提高发送效率。

WLAN 特性中，将 EDCA 参数及其他的 WMM 参数集中在 WMM 模板中进行管理。WMM 模板创建后需绑定到射频模板中，随绑定的射频模板应用到射频中。

版权所有 © 华为技术有限公司

VAP 的 QoS 策略管理

报文上行时，AP 接收到无线客户端发送的 802.11 数据报文后，将其转换为 802.3 报文，可以通过隧道，也可以不通过隧道到达 AC，然后向网络侧继续转发。在整个传送过程中依据 802.3 报文优先级或隧道优先级进行调度。

报文下行时，AC 将网络侧收到的 802.3 报文，通过隧道或直接发送给 AP，通过隧道时在中间网络可依据隧道优先级进行调度。AP 接收到 802.3 报文后，将其转换为 802.11 报文，并依据报文中的 UP 优先级选择不同的 AC 队列发送给用户终端。

VAP 的 QoS 策略管理通过 Traffic 模板进行管理。Traffic 模板参数说明如表 12-7 所示。

表 12-7 Traffic 模板参数说明

参数名	说明
Client/VAP 的无线上行限速	限制无线客户端或整个 VAP 上行的无线报文速率。
802.3 报文优先级配置	配置 AP 上行 802.3 报文内层的 802.1p 优先级：采用指定值或依据无线客户端发送的 802.11 报文 UP 优先级映射。
上行隧道优先级配置	配置 AP 上行 802.3 报文外层的隧道优先级：采用指定值或依据内层优先级进行映射。
802.11 报文优先级配置	配置 AP 下行 802.11 报文的优先级。

Traffic 模板创建后需绑定到服务集 Sevice-Set 中，随着服务集应用到对应的 VAP 中。

12.4.3 配置射频的 QoS 策略

配置射频的 QoS 策略，提供不同的信道抢占能力，实现不同的服务质量。

应用环境

无线终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同无线用户获得不同级别的服务，可通过配置 WMM 模板参数来实现。

前置任务

在配置射频的 QoS 策略之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

数据准备

在配置射频的 QoS 策略之前，需准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	WMM 模板名称、（可选）WMM 模板 ID
2	（可选）WMM EDCA Client：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）
3	（可选）WMM EDCA AP：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* } *，配置 WMM 模板。

WMM 模板创建成功后，模板内的参数均自动配置为缺省值。使用命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

#创建 WMM 模板“wp”，所有配置均为缺省值。

```
[Quidway-wlan-view] display wmm-profile name wp
  Profile ID      : 2
  Profile name    : wp
  WMM switch      : enable
  Client EDCA parameters:
  ----------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit
  AC_VO  3       2       2      47
  AC_VI  4       3       2      94
  AC_BE  10      4       3      0
  AC_BK  10      4       7      0
  ----------------------------------------------------
  AP EDCA parameters:
  ----------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
  AC_VO  3       2       1      47         normal
  AC_VI  4       3       1      94         normal
  AC_BE  6       4       3      0          normal
  AC_BK  10      4       7      0          normal
  ----------------------------------------------------
```


版权所有 © 华为技术有限公司

说明

终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同报文获得不同级别的服务，我们将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样。

四个优先级队列的名称和优先级顺序缺省为：AC_VO(语音) > AC_VI(视频) > AC_BE(尽力而为) > AC_BK(背景)。

四个优先级队列的优先级顺序并不是绝对的，可以通过参数修改来调整优先级顺序，这些参数称为 EDCA 参数(Enhanced Distributed Channel Access)。包括 AIFSN（arbitration inter Frame spacing number 仲裁帧间隙数）、ECWmin（exponetn form of CWmin 最小竞争窗口指数形式）、ECWmax (exponent form of CWmax 最大竞争窗口指数形式)、TXOPlimit（transmission opportunity limit 传输机会限制）以及 ack-policy（ACK 策略）。

- AIFSN：WMM 针对不同 AC 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。
- ECWmin 和 ECWmax：这两个数值决定了平均退避时间值，数值越大，用户的平均退避时间越长。
- TXOPLimit：用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用的信道时长越大，如果是 0，则每次占用信道后，只能发送一个报文。
- ack-policy：有 normal ack(应答)和 no ack(不应答)两种策略，缺省为 noraml ack。

占用信道发送报文的原理：终端在占用信道发送报文前，先监听信道，当信道空闲时间大于或等于空闲等待时间时，在竞争窗口范围内随即选择退避时间进行退避，最先结束退避的终端竞争到信道，开始发送报文。

步骤 4 （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *，配置终端上四个 WMM 队列的 EDCA 参数。

步骤 5 （可选）执行命令 **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

检查配置结果

执行命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

12.4.4 配置 VAP 的 QoS 策略

当需要为某个 VAP 定制特定的优先级映射、流量抑制等功能时，创建相应的流量模板并绑定到服务集中。

应用环境

STA 发出的 802.11 报文要通过 AP 进入以太网时，需要转换成 802.3 报文，这期间可以不进行优先级映射，也可以按照不同的 VAP 设置不同的优先级，从而提供不同的 QoS 服务质量。

前置任务

在配置 VAP 的 QoS 策略之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。

版权所有 © 华为技术有限公司

数据准备

在配置 VAP 的 QoS 策略之前，需准备以下数据。

序号	数据
1	流量模板名称、（可选）流量模板 ID
2	（可选）up-map-8021p 映射值、8021p-map-up 映射值
3	（可选）报文限速速率
4	（可选）隧道优先级映射值

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，配置流量模板。

流量模板创建成功后，模板内的参数均为缺省值。执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看各项属性的缺省配置。

#查看 Traffic 模板“traffic-profile-1”的各项属性。

```
[Quidway-wlan-view] display traffic-profile name traffic-profile-1
  Profile ID         : 3
  Profile name       : traffic-profile-1
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
  802.1p to User-priority Mapping List:
  ----------------------------
  802.1p  User-priority
  0       0
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  ----------------------------
  Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)
  ----------------------------
  ToS(inner)     ToS(outer)
  0              0
  1              1
```


版权所有 © 华为技术有限公司

```
2               2
3               3
4               4
5               5
6               6
7               7
--------------------------
```

说明

802.3 报文通过 AP 转发给 STA 时，被转换成 802.11 报文，其中的 UP 域可以根据 DSCP、CoS 映射而来，或者由流分类设置。

步骤 4 （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。

STA 发送 802.11 报文后，在 AP 上终结，同时构造 802.3 报文上行。为保证报文在 AP 转发时能够得到一定的服务质量，需要填充其优先级值以便调度。

步骤 5 （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，配置下行时 802.1p 优先级值到用户优先级值的映射关系。

步骤 6 （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。

步骤 7 （可选）执行以下命令配置上行隧道优先级值。存在指定和映射两种模式，只能选择其一。

- **tunnel-priority up designate** { **tos** | **8021p** } *priority-value*
- **tunnel-priority up map** { **tos-tos** | **tos-8021p** | **8021p-tos** | **8021p-8021p** } *value0 value1 value2 value3 value4 value5 value6 value7*

----结束

检查配置结果

执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看流量模板配置的各项属性。

12.4.5 配置用户优先级和用户 CAR

通过创建用户模板，并在用户模板下配置用户优先级、用户 CAR 等属性来对用户业务进行 QoS 控制。

应用环境

用户终端发送 802.11 报文后，在 AP 上终结，同时构造 802.3 报文上行。为保证报文到达 AC 后转发时能够得到一定的服务质量，可以配置用户优先级、用户 CAR 进行流量控制。

前置任务

在配置用户优先级和用户 CAR 之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见 **12.1.3 配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。
- QoS Car 模板已经配置完成。

版权所有 © 华为技术有限公司

数据准备

在配置用户优先级和用户 CAR 之前，需准备以下数据。

序号	数据
1	用户模板名称、（可选）用户模板 ID
2	用户优先级
3	QoS CAR 名称

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **user-profile** { **name** *profile-name* | **id** *profile-id* } *，配置用户模板。

步骤 4 执行命令 **user-priority** { **downstream** | **upstream** }*user-priority*，配置用户报文到达 AC 后的优先级。

步骤 5 执行命令 **quit**，退出用户模板视图。

步骤 6 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } *，创建并进入服务集模板视图。

步骤 7 执行命令 **user-profile** { **name** *profile-name* | **id** *profile-id* }，在指定服务集中绑定用户模板。

----结束

检查配置结果

执行命令 **display user-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看用户模板信息。

查询所有用户模板。

```
<Quidway> display user-profile all
  -------------------------------------------------
   ID     Name
  -------------------------------------------------
   0      up
   1      kk
  -------------------------------------------------
   Total: 2
```

查询单个用户模板。

```
<Quidway> display user-profile name p1
  Profile name                 : p1
  Profile ID                   : 0
  QoS CAR inbound CAR-profile  : -
  QoS CAR outbound CAR-profile : -
  User-priority upstream       : -
  User-priority downstream     : -
```


版权所有 © 华为技术有限公司

12.4.6 通过 QoS 模板配置用户优先级和用户 CAR

通过创建 QoS 模板，并在 QoS 模板下配置用户优先级、用户 CAR 等属性来对用户进行 QoS 控制。

应用环境

用户终端发送 802.11 报文后，在 AP 上终结，同时构造 802.3 报文上行。为保证报文到达 AC 后转发时能够得到一定的服务质量，可以配置用户优先级、用户 CAR 进行流量控制。

说明

- QoS 模板与用户模板有相同的功能，同为通过设置用户优先级和 CAR 值来对用户进行 QoS 控制，但二者实现 QoS 控制的机制不一样，QoS 模板通过与用户组绑定的方式，将优先级和 CAR 配置作用于用户。当 AC 上同时在用户组下绑定了 QoS 模板和用户模板下配置了 QOS 时，优先使用 QoS 模板配置进行 QoS 控制。
- QoS 模板配置信息修改后，只对后续上线用户生效。

前置任务

在配置用户优先级和用户 CAR 之前，需完成以下任务：

- AC 的基本功能已经配置完成，具体请参见**配置 AC 基本功能**。
- AP 和 AC 之间网络连接正常。
- 用户组已建立，且信息下发到 AP。

数据准备

在配置用户优先级和用户 CAR 之前，需准备以下数据。

序号	数据
1	QoS 模板名称。
2	用户优先级。
3	用户 CAR 值。
4	QoS 模板描述信息（可选）。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **qos profile name** *profile-name*，配置 QoS 模板。

步骤 3 执行命令 **description** *description*，对 QoS 模板进行描述。

步骤 4 执行命令 **car** { **inbound** | **outbound** } **cir** *cir-value* [**pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]，配置用户的 CAR 值。

步骤 5 执行命令 **remark local-precedence** { *local-precedence-name* | *local-precedence-value* }，指定用户的优先级。

版权所有 © 华为技术有限公司

步骤 6 执行命令 **quit**，退出 QOS 模板视图。

步骤 7 执行命令 **user-group** *group-name*，创建用户组并进入用户组视图。

步骤 8 执行命令 **qos-profile** *name*，在用户组视图下绑定已创建的 QOS 模板。

步骤 9 执行命令 **quit**，退出用户组视图。

步骤 10 执行命令 **wlan**，进入 WLAN 视图。

步骤 11 执行命令 **commit** { **all** |**ap** *ap-id* }，下发配置信息到 AP，后续用户上线并加入用户组时，获得 QoS 模板配置。

----结束

检查配置结果

执行命令 **display qos-profile** { **all** | **name** *profile-name* } ，查看 QoS 模板信息。

查询名称为 name1 的用户 QoS profile 成员信息。

```
[Quidway] display qos-profile name name1
 Name                        :name1
 Description                 :global
 Local Precedence            :-
 Inbound  car cir - kbps, cbs - bytes, pir - kbps, pbs - bytes
 Outbound car cir - kbps, cbs - bytes, pir - kbps, pbs - bytes
```

查询所有 QoS profile 成员信息。

```
[Quidway] display qos-profile all
   index              QoS Profile Name
 ---------------------------------------
     0                 name1
 ---------------------------------------
 Total QoS Profile number is 1
```

12.4.7 配置示例

配置 QoS 策略的业务示例

组网需求

STA1、STA2 通过 AP1 连接到网络，STA3、STA4 和 STA5 通过 AP2 连接到网络。其中 STA5 为 VIP 客户。要求：

- AP1 下用户优先满足语音需求。
- AP2 下用户优先满足视频需求。
- 当网络带宽不足时，优先满足 VIP 客户的使用需求。

AC 和 AP 组网图如**图 12-14** 所示。

版权所有 © 华为技术有限公司

图 12-14 配置 WLAN 基本业务示例图

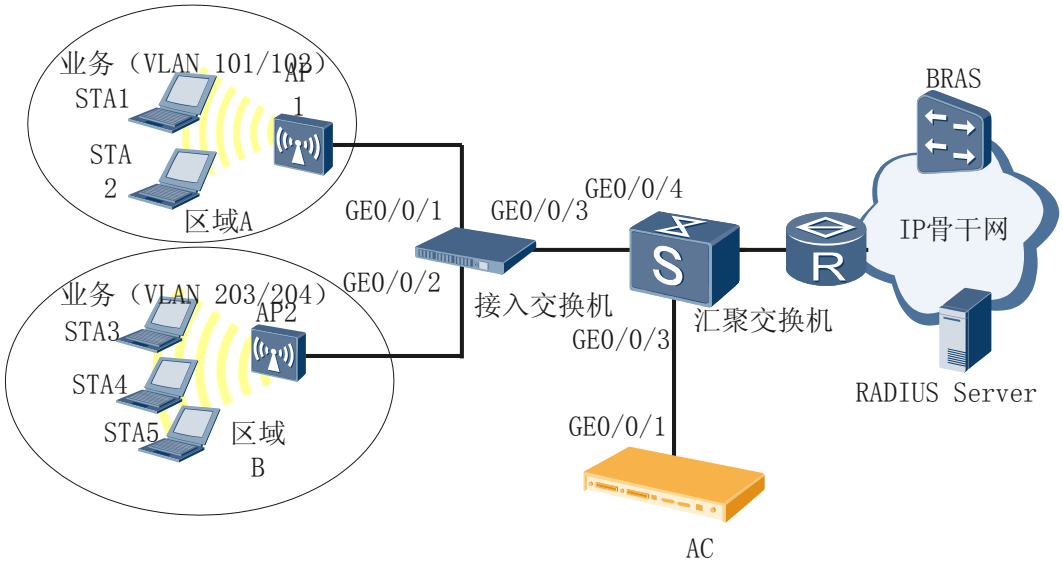


表 12-8 数据规划表

配置项	数据
WLAN 服务	● SSID：huawei-1 ● Traffic 模板：huawei ● VLAN:101
	● SSID：huawei-2 ● Traffic 模板：huawei ● VLAN:102
	● SSID：huawei-3 ● Traffic 模板：huawei ● VLAN:203
	● SSID：huawei-4 ● Traffic 模板：huawei ● VLAN:204
	● SSID：huawei-5 ● Traffic 模板：huawei-vip ● VLAN:205
AP 射频模板	● AP1 射频模板:huawei；WMM 模板：huawei ● AP2 射频模板:huawei-vi；WMM 模板：huawei-vi
AP 管理 VLAN	VLAN 100(由接入交换机分配）

版权所有 © 华为技术有限公司

配置项	数据
AP Region	● AP1：101 ● AP2：102
AP 业务 VLAN	● AP1：VLAN 101、VLAN 102 ● AP2：VLAN 203、VLAN 204、VLAN 205
Switch VLAN	VLAN 100/101/102/203/204/205
AC 管理 IP 地址	Vlanif100：192.168.0.1/24
AC Carrier ID/AC ID/国家码	CTC/1/CN

配置思路

1. 配置接入交换机、汇聚交换机和 AC，实现 AP 和 AC 互通。
2. 配置 AC 的基本功能，包括配置 AC 运营商标识和 ID、AC 与 AP 之间通信的源接口。
3. 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。
4. 配置相应 QoS 要求的 VAP，下发 WLAN 业务。其中配置相应 QoS 要求的 VAP，需要：
   - 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
   - 创建 WMM 模板并配置模板属性，创建射频模板，并在射频模板下绑定 WMM 模板，实现优先满足用户语音或视频通信的需求。
   - 创建流量模板并配置模板属性，实现当网络带宽不足时，优先满足 VIP 客户的通信需求。
   - 创建安全模板，实现 STA 接入网络的安全控制。
   - 创建服务集，并在服务集下绑定安全模板、流量模板。
   - 配置 VAP，下发 WLAN 业务，实现不同 STA 使用 WLAN 网络的 QoS 控制。

操作步骤

步骤 1 配置接入交换机、汇聚交换机和 AC，使 AP 和 AC 互通。

#配置接入交换机连接 AP 的以太网端口（GE0/0/1 和 GE0/0/2）类型为 trunk 类型，PVID 为 100。

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] vlan batch 203 to 205
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101 102
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 203 to 205
[Quidway-GigabitEthernet0/0/2] quit
```


版权所有 © 华为技术有限公司

#配置接入交换机上连接汇聚交换机的以太网端口（GE0/0/3）透传所有业务和管理VLAN。

```
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 102 203 to 205
[Quidway-GigabitEthernet0/0/3] quit
```

#配置汇聚交换机上连接接入交换机的以太网端口（GE0/0/4）透传所有业务和管理VLAN。

```
[Quidway] interface GigabitEthernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type trunk
[Quidway-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 102 203 to 205
[Quidway-GigabitEthernet0/0/4] quit
```

#配置汇聚交换机上连接 AC 的 GE 接口透传所有业务和管理 VLAN。

```
[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 102 203 to 205
[Quidway-GigabitEthernet0/0/3] quit
```

配置 AC 有线侧连接汇聚交换机的 GE0/0/1 接口和连接无线侧的 XGE0/0/27 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname LSW
[LSW] vlan batch 100 to 102
[LSW] vlan batch 203 to 205
[LSW] interface GigabitEthernet 0/0/1
[LSW-GigabitEthernet0/0/1] port link-type trunk
[LSW-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102 203 to 205
[LSW-GigabitEthernet0/0/1] quit
[LSW] interface XGigabitEthernet 0/0/27
[LSW-XGigabitEthernet0/0/27] port link-type trunk
[LSW-XGigabitEthernet0/0/27] port trunk allow-pass vlan 100 to 102 203 to 205
[LSW-XGigabitEthernet0/0/27] quit
```

切换到无线侧，配置无线侧连接有线侧的接口 XGE0/0/1 透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102 203 to 205
[AC-XGigabitEthernet0/0/1] quit
```

步骤 2 配置 AC 的基本功能。

#配置 AC 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC] wlan AC-global AC id 1 carrier id  ctc
[AC] wlan AC-global country-code cn
```

#创建 VLANIF 接口，配置其 IP 地址作为数据转发的三层接口。

```
[AC] interface vlanif100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
[AC] interface vlanif203
```


版权所有 © 华为技术有限公司

```
[AC-Vlanif203] ip address 192.168.3.1 24
[AC-Vlanif203] dhcp select interface
[AC-Vlanif203] quit
[AC] interface vlanif204
[AC-Vlanif204] ip address 192.168.4.1 24
[AC-Vlanif204] dhcp select interface
[AC-Vlanif204] quit
[AC] interface vlanif205
[AC-Vlanif205] ip address 192.168.5.1 24
[AC-Vlanif205] dhcp select interface
[AC-Vlanif205] quit
```

#配置 AC 的源接口，用于 AP 和 AC 之间建立隧道通信。

```
[AC] wlan
[AC-wlan-view] wlan AC source interface vlanif 100
[AC-wlan-view] quit
```

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

步骤 3 配置 AP 并上线。

#配置 AP 的认证方式为“no-auth”。

```
[AC-wlan-view] ap-auth-mode no-auth
```

说明

如果 AP 认证模式为“no-auth”，上线 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。

#配置 AP 域 ID 分别为 101 和 102。

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```

#配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

步骤 4 配置 WLAN-ESS 虚接口。

```
[AC] interface wlan-ess1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 101
[AC-WLAN-ESS1] quit
[AC] interface wlan-ess2
[AC-WLAN-ESS2] port link-type hybrid
[AC-WLAN-ESS2] port hybrid untagged vlan 102
[AC-WLAN-ESS2] quit
[AC] interface wlan-ess3
[AC-WLAN-ESS3] port link-type hybrid
[AC-WLAN-ESS3] port hybrid untagged vlan 203
[AC-WLAN-ESS3] quit
[AC] interface wlan-ess4
[AC-WLAN-ESS4] port link-type hybrid
[AC-WLAN-ESS4] port hybrid untagged vlan 204
[AC-WLAN-ESS4] quit
[AC] interface wlan-ess5
[AC-WLAN-ESS5] port link-type hybrid
```


版权所有 © 华为技术有限公司

```
[AC-WLAN-ESS5] port hybrid untagged vlan 205
[AC-WLAN-ESS5] quit
```

步骤 5 配置 AP 对应的各种模板。

- 创建 WMM 模板

  #创建 WMM 模板“huawei”，采用缺省配置，其中优先级队列顺序为缺省值：AC_VO(语音) > AC_VI(视频)。

  ```
  [AC-wlan-view] wmm-profile name huawei
  [AC-wlan-wmm-prof-huawei] quit
  ```

  #创建 WMM 模板“huawei-vi”，并修改队列优先级参数，使优先级队列顺序为：AC_VI(视频) >AC_VO(语音)。

  ```
  [AC-wlan-view] wmm-profile name huawei-vi
  [AC-wlan-wmm-prof-huawei-vi] wmm edca ap AC-vi ecw ecwmin 1 ecwmax 1 aifsn 1 txoplimit 36 ack-policy normal
  [AC-wlan-wmm-prof-huawei-vi] wmm edca client AC-vi ecw ecwmin 1 ecwmax 3 aifsn 1 txoplimit 36
  [AC-wlan-wmm-prof-huawei-vi] quit
  ```

- #创建 Radio 模板，并绑定 WMM 模板。

  ```
  [AC-wlan-view] radio-profile name huawei
  [AC-wlan-radio-prof-huawei] wmm-profile name huawei
  [AC-wlan-radio-prof-huawei] quit
  [AC-wlan-view] radio-profile name huawei-vi
  [AC-wlan-radio-prof-huawei-vi] wmm-profile name huawei-vi
  [AC-wlan-radio-prof-huawei-vi] quit
  ```

- #创建名为“huawei”的 Security 模板。

  ```
  [AC-wlan-view] security-profile name huawei
  [AC-wlan-sec-prof-huawei] quit
  ```

- 创建 Traffic 模板。

  #创建名为“huawei”的 Traffic 模板，设置 VAP 下行限速为 1024Kbps，STA 上行限速为 512Kbps。

  ```
  [AC-wlan-view] traffic-profile name huawei
  [AC-wlan-traffic-prof-huawei] rate-limit client up 512
  [AC-wlan-traffic-prof-huawei] rate-limit vap down 1024
  [AC-wlan-traffic-prof-huawei] quit
  ```

  #创建名为“huawei-vip”的 Traffic 模板。设置 VAP 限速为 2048Kbps，STA 限速为 1024Kbps。

  ```
  [AC-wlan-view] traffic-profile name huawei-vip
  [AC-wlan-traffic-prof-huawei-vi] rate-limit client up 1024
  [AC-wlan-traffic-prof-huawei-vi] rate-limit vap up 2048
  [AC-wlan-traffic-prof-huawei-vi] quit
  ```

步骤 6 配置 AP 对应的射频。

- #配置 AP1 的射频，绑定 Radio 模板“huawei”。

  ```
  [AC-wlan-view] ap 1 radio 0
  [AC-wlan-radio-1/0] radio-profile name huawei
  [AC-wlan-radio-1/0] quit
  ```

- #配置 AP2 的射频，绑定 Radio 模板“huawei-vi”。

  ```
  [AC-wlan-view] ap 2 radio 0
  [AC-wlan-radio-2/0] radio-profile name huawei-vi
  [AC-wlan-radio-2/0] quit
  ```

步骤 7 配置 AP 对应的服务集。

- #创建名为“huawei-1”的 service-set，SSID 为“huawei-1”，绑定 Traffic 模板“huawei”，Security 模板“huawei”， VLAN101。

  ```
  [AC-wlan-view] service-set name huawei-1
  [AC-wlan-service-set-huawei-1] ssid huawei-1
  [AC-wlan-service-set-huawei-1] traffic-profile name huawei
  [AC-wlan-service-set-huawei-1] security-profile name huawei
  ```


版权所有 © 华为技术有限公司

```
[AC-wlan-service-set-huawei-1] wlan-ess 1
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] quit
```

- #创建名为“huawei-2”的 service-set，SSID 为“huawei-2”，绑定 Traffic 模板“huawei”，Security 模板“huawei”， VLAN102。

```
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name huawei
[AC-wlan-service-set-huawei-2] security-profile name huawei
[AC-wlan-service-set-huawei-2] wlan-ess 2
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] quit
```

- #创建名为“huawei-3”的 service-set，SSID 为“huawei-3”，绑定 Traffic 模板“huawei”，Security 模板“huawei”， VLAN203。

```
[AC-wlan-view] service-set name huawei-3
[AC-wlan-service-set-huawei-3] ssid huawei-3
[AC-wlan-service-set-huawei-3] traffic-profile name huawei
[AC-wlan-service-set-huawei-3] security-profile name huawei
[AC-wlan-service-set-huawei-3] wlan-ess 3
[AC-wlan-service-set-huawei-3] service-vlan 203
[AC-wlan-service-set-huawei-3] quit
```

- #创建名为“huawei-4”的 service-set，SSID 为“huawei-4”，绑定 Traffic 模板“huawei”，Security 模板“huawei”， VLAN204。

```
[AC-wlan-view] service-set name huawei-4
[AC-wlan-service-set-huawei-4] ssid huawei-4
[AC-wlan-service-set-huawei-4] traffic-profile name huawei
[AC-wlan-service-set-huawei-4] security-profile name huawei
[AC-wlan-service-set-huawei-4] wlan-ess 4
[AC-wlan-service-set-huawei-4] service-vlan 204
[AC-wlan-service-set-huawei-4] quit
```

- #创建名为“huawei-5”的 service-set，SSID 为“huawei-5”，绑定 Traffic 模板“huawei-vip”，Security 模板“huawei”， VLAN205。

```
[AC-wlan-view] service-set name huawei-5
[AC-wlan-service-set-huawei-5] ssid huawei-5
[AC-wlan-service-set-huawei-5] traffic-profile name huawei-vip
[AC-wlan-service-set-huawei-5] security-profile name huawei
[AC-wlan-service-set-huawei-5] wlan-ess 5
[AC-wlan-service-set-huawei-5] service-vlan 205
[AC-wlan-service-set-huawei-5] quit
```

步骤 8 配置 AP 对应的 VAP，下发 WLAN 服务。

#将 AP1 对应的射频绑定服务集“huawei-1”和“huawei-2”，下发 VAP。

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-1
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```

#将 AP1 对应的射频绑定服务集“huawei-3”、“huawei-4”和“huawei-5”，下发 VAP。

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name huawei-3
[AC-wlan-radio-2/0] service-set name huawei-4
[AC-wlan-radio-2/0] service-set name huawei-5
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

步骤 9 验证配置结果

AP1 和 AP2 下用户可以搜索到 5 个 WLAN 网络，其网络标识分别为 huawei-1、huawei-2、huawei-3、huawei-4、huawei-5。STA1－STA5 分别选择 huawi-1 到 huawei-5 的 WLAN 网络。

版权所有 © 华为技术有限公司

- STA1、STA2、STA3 和 STA4 用户速率最大为 512Kbps。STA5 用户速率最大为 1024Kbps，当网络带宽不足时优先得到满足。
- AP1 下用户 STA1 和 STA2 的语音通信优先被满足。AP2 下用户 STA3、STA4 和 STA5 的视频通信优先被满足。

----结束

配置文件

- AC 上的配置文件

```
#
 sysname AC
#
 vlan batch 100 to 102
 vlan batch 203 to 205
#
dhcp enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/27
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 500 to 501
#
 wlan AC-global carrier id ctc AC id 1
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
#
interface Vlanif203
 ip address 192.168.3.1 255.255.255.0
 dhcp select interface
#
interface Vlanif204
 ip address 192.168.4.1 255.255.255.0
 dhcp select interface
#
interface Vlanif205
 ip address 192.168.5.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Ess1
 port hybrid untagged vlan 101
#
interface Wlan-Ess2
 port hybrid untagged vlan 102
#
interface Wlan-Ess3
 port hybrid untagged vlan 203
#
interface Wlan-Ess4
 port hybrid untagged vlan 204
```


版权所有 © 华为技术有限公司

```
#
interface Wlan-Ess5
 port hybrid untagged vlan 205
#
wlan
 wlan AC source interface Vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 1 type-id 6 mac 5489-9849-83e9 sn AB36014989
 ap id 2 type-id 8 mac 5489-9846-e19a sn AB35053258
 wmm-profile name huawei id 0
 wmm-profile name Huawei-vi id 1
  wmm edca ap AC-vi aifsn 1 ecw ecwmin 1 ecwmax 1 txoplimit 36
  wmm edca client AC-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
 traffic-profile name huawei id 0
  rate-limit client up 512
  rate-limit vap down 1024
 traffic-profile name huawei-vip id 1
  rate-limit client up 1024
  rate-limit vap up 2048
 security-profile name huawei id 0
 service-set name huawei-1 id 0
  wlan-ess 1
  ssid huawei-1
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 service-set name huawei-2 id 1
  wlan-ess 2
  ssid huawei-2
  traffic-profile id 0
  security-profile id 0
  service-vlan 102
service-set name huawei-3 id 2
  wlan-ess 3
  ssid huawei-3
  traffic-profile id 0
  security-profile id 0
  service-vlan 203
service-set name huawei-4 id 3
  wlan-ess 4
  ssid huawei-4
  traffic-profile id 0
  security-profile id 0
  service-vlan 204
service-set name huawei-5 id 4
  wlan-ess 5
  ssid huawei-5
  traffic-profile id 1
  security-profile id 0
  service-vlan 205
radio-profile name huawei id 0
  wmm-profile id 0
 radio-profile name huawei-vi id 1
  wmm-profile id 1
 ap 1 radio 0
  radio-profile name huawei
  service-set name huawei-1 wlan 1
  service-set name huawei-2 wlan 1
 ap 2 radio 0
  radio-profile name huawei-vi
  service-set name huawei-3 wlan 2
  service-set name huawei-4 wlan 2
  service-set name huawei-5 wlan 2
```

- 接入交换机上的配置文件

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
```


版权所有 © 华为技术有限公司

```
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 101 102
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 203 to 205
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 102 203 to 205
```

- 汇聚交换机上的配置文件

```
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 102 203 to 205
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 100 to 102 203 to 205
```


版权所有 © 华为技术有限公司