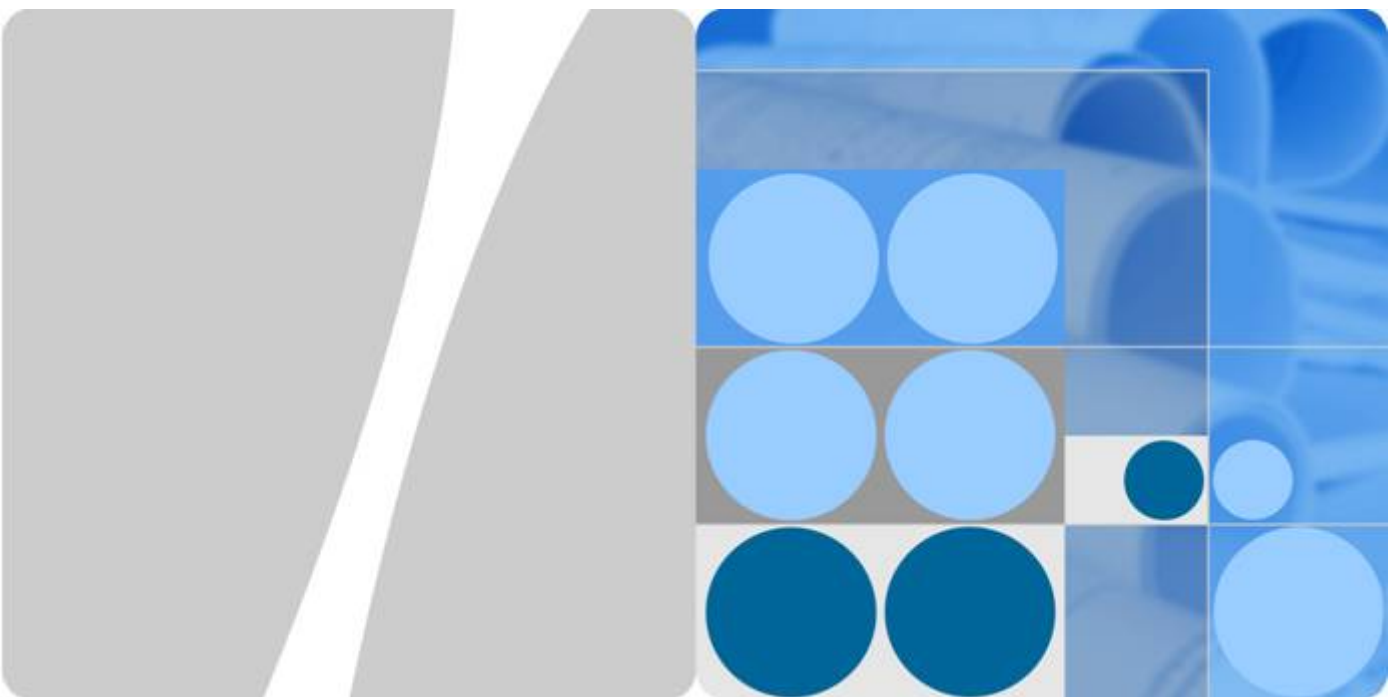




HUAWEI NetEngine20E-X6 高端业务路由器

V600R003C00

配置指南-系统管理

文档版本 01
发布日期 2011-05-15

版权所有 © 华为技术有限公司 2011。保留一切权利。

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

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：<http://www.huawei.com>

客户服务邮箱：support@huawei.com

客户服务电话：0755-28560000 4008302118

客户服务传真：0755-28560111

前言

概述

本手册介绍了 NE20E-X6 支持的系统管理协议和各种配置。主要内容包括系统管理的基础知识、各种系统管理协议的配置和各种配置案例。本手册最后提供了系统管理协议中常用的术语和缩略语。阅读本手册有助于用户系统掌握系统管理协议和各种配置信息。

读者对象

本文档（本指南）主要适用于以下工程师：

- 调测工程师
- 数据配置工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

修订记录

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

文档版本 01 (2011-05-15)

第一次正式发布。

目录

前言.....	iii
1 信息中心配置.....	1-1
1.1 信息中心简介.....	1-2
1.1.1 信息中心概述.....	1-2
1.1.2 NE20E-X6 支持的信息中心特性.....	1-2
1.2 配置日志信息的输出.....	1-7
1.2.1 建立配置任务.....	1-8
1.2.2 （可选）开启信息中心.....	1-9
1.2.3 （可选）命名信息通道.....	1-9
1.2.4 （可选）配置日志 ID 过滤功能.....	1-9
1.2.5 （可选）配置生成数据字典的功能.....	1-10
1.2.6 （可选）配置海量日志抑制功能.....	1-10
1.2.7 （可选）配置连续重复日志的统计输出功能.....	1-10
1.2.8 配置日志信息输出到日志缓冲区.....	1-11
1.2.9 配置日志信息输出到日志文件.....	1-11
1.2.10 配置日志信息输出到控制台.....	1-12
1.2.11 配置日志信息输出到终端.....	1-12
1.2.12 配置日志信息输出到日志主机.....	1-13
1.2.13 配置日志信息输出到 CF 卡.....	1-13
1.2.14 检查配置结果.....	1-14
1.3 配置告警信息的输出.....	1-16
1.3.1 建立配置任务.....	1-17
1.3.2 （可选）开启信息中心.....	1-18
1.3.3 （可选）命名信息通道.....	1-18
1.3.4 配置告警信息输出到告警缓冲区.....	1-18
1.3.5 配置告警信息输出到日志文件.....	1-19
1.3.6 配置告警信息输出到控制台.....	1-20
1.3.7 配置告警信息输出到终端.....	1-20
1.3.8 配置告警信息输出到 SNMP 代理.....	1-21
1.3.9 检查配置结果.....	1-21
1.4 配置调试信息的输出.....	1-23
1.4.1 建立配置任务.....	1-24

1.4.2 (可选) 开启信息中心.....	1-24
1.4.3 (可选) 命名信息通道.....	1-25
1.4.4 配置调试信息输出到日志文件.....	1-25
1.4.5 配置调试信息输出到控制台.....	1-26
1.4.6 配置调试信息输出到终端.....	1-26
1.4.7 配置调试信息输出到日志主机.....	1-27
1.4.8 检查配置结果.....	1-27
1.5 维护信息中心.....	1-28
1.6 信息中心配置举例.....	1-29
1.6.1 配置向日志文件输出日志信息示例.....	1-29
1.6.2 配置向日志主机输出日志信息示例.....	1-31
1.6.3 配置使用管理 VPN 实例时向公网日志主机输出日志信息示例.....	1-34
1.6.4 配置向日志主机发送二进制日志.....	1-37
1.6.5 配置向 SNMP Agent 输出告警信息示例.....	1-39
1.6.6 配置向控制台输出调试信息示例.....	1-41
2 SNMP 配置.....	2-1
2.1 SNMP 简介.....	2-2
2.1.1 SNMP 概述.....	2-2
2.1.2 NE20E-X6 支持的 SNMP 特性.....	2-4
2.2 配置设备使用 SNMPv1 与网管通信.....	2-6
2.2.1 建立配置任务.....	2-7
2.2.2 配置 SNMPv1 的基本功能.....	2-8
2.2.3 (可选) 限制网管对设备的访问权限.....	2-10
2.2.4 (可选) 配置 SNMP 扩展错误码功能.....	2-11
2.2.5 (可选) 配置向网管发送告警.....	2-11
2.2.6 (可选) 配置接口索引固定特性.....	2-12
2.2.7 检查配置结果.....	2-13
2.3 配置设备使用 SNMPv2c 与网管通信.....	2-15
2.3.1 建立配置任务.....	2-15
2.3.2 配置 SNMPv2c 的基本功能.....	2-16
2.3.3 (可选) 限制网管对设备的访问权限.....	2-18
2.3.4 (可选) 配置 SNMP 扩展错误码功能.....	2-20
2.3.5 (可选) 配置向网管发送告警.....	2-20
2.3.6 (可选) 配置接口索引固定特性.....	2-22
2.3.7 检查配置结果.....	2-22
2.4 配置设备使用 SNMPv3 与网管通信.....	2-25
2.4.1 建立配置任务.....	2-25
2.4.2 配置 SNMPv3 的基本功能.....	2-26
2.4.3 (可选) 限制网管对设备的访问权限.....	2-28
2.4.4 (可选) 配置 SNMP 扩展错误码功能.....	2-30
2.4.5 (可选) 配置向网管发送告警.....	2-30
2.4.6 (可选) 配置接口索引固定特性.....	2-31

2.4.7 检查配置结果.....	2-31
2.5 SNMP 配置举例.....	2-33
2.5.1 配置设备使用 SNMPv1 与网管通信示例.....	2-33
2.5.2 配置设备使用 SNMPv2c 与网管通信示例.....	2-37
2.5.3 配置设备使用 SNMPv3 与网管通信示例.....	2-40
3 RMON 和 RMON2 配置.....	3-1
3.1 RMON 和 RMON2 简介.....	3-2
3.1.1 RMON 和 RMON2 概述.....	3-2
3.1.2 NE20E-X6 支持的 RMON 和 RMON2 特性.....	3-3
3.2 配置 RMON.....	3-4
3.2.1 建立配置任务.....	3-5
3.2.2 使能接口的 RMON 统计功能.....	3-6
3.2.3 配置统计表.....	3-6
3.2.4 配置历史控制表.....	3-7
3.2.5 配置事件表.....	3-7
3.2.6 配置告警表.....	3-8
3.2.7 配置扩展告警表.....	3-8
3.2.8 检查配置结果.....	3-9
3.3 配置 RMON2.....	3-10
3.3.1 建立配置任务.....	3-11
3.3.2 配置主机控制表.....	3-11
3.3.3 配置协议目录表.....	3-12
3.3.4 检查配置结果.....	3-12
3.4 维护 RMON 和 RMON2.....	3-13
3.5 RMON 和 RMON2 配置举例.....	3-14
3.5.1 配置 RMON 示例.....	3-14
3.5.2 配置 RMON2 示例.....	3-18
4 HGMP 配置.....	4-1
4.1 HGMP 简介.....	4-2
4.1.1 HGMP 概述.....	4-2
4.1.2 NE20E-X6 支持的 HGMP 特性.....	4-4
4.2 配置 HGMP 的基本功能.....	4-7
4.2.1 建立配置任务.....	4-7
4.2.2 配置 NDP.....	4-8
4.2.3 配置 NTDP.....	4-9
4.2.4 创建集群.....	4-10
4.2.5 添加成员交换机.....	4-12
4.2.6 （可选）删除或退出集群.....	4-12
4.2.7 （可选）删除成员交换机.....	4-13
4.2.8 检查配置结果.....	4-14
4.3 配置 HGMP 的高级功能.....	4-16

4.3.1 建立配置任务.....	4-16
4.3.2 调整集群参数.....	4-17
4.3.3 利用 HGMP 管理集群中的设备.....	4-19
4.3.4 检查配置结果.....	4-21
4.4 维护 HGMP.....	4-24
4.4.1 清除 NDP 统计信息.....	4-24
4.4.2 监控 HGMP 集群的运行状况.....	4-24
4.4.3 调试 HGMP.....	4-25
4.5 配置举例.....	4-25
4.5.1 配置 HGMP 集群基本功能示例.....	4-26
4.5.2 配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）.....	4-36
4.5.3 配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）.....	4-46
4.5.4 配置 HGMP 集群内外设备 SNMP 互通示例（NAT 方式）.....	4-56
4.5.5 配置 HGMP 集群内外设备 SNMP 互通示例（非 NAT 方式）.....	4-66
4.5.6 配置 HGMP 集群批量下发功能示例.....	4-77
4.5.7 配置 HGMP 集群批量重启功能示例.....	4-88
4.5.8 配置 HGMP 集群增量配置功能示例.....	4-98
4.5.9 配置 HGMP 集群同步配置文件功能示例.....	4-108
4.5.10 配置 HGMP 集群安全特性示例.....	4-118
5 NTP 配置.....	5-1
5.1 NTP 简介.....	5-2
5.1.1 NTP 概述.....	5-2
5.1.2 NE20E-X6 支持的 NTP 特性.....	5-4
5.2 配置 NTP 基本功能.....	5-5
5.2.1 建立配置任务.....	5-6
5.2.2 配置 NTP 主时钟.....	5-7
5.2.3 配置更新客户端时钟的时间间隔.....	5-7
5.2.4 配置单播服务器/客户端模式.....	5-8
5.2.5 配置对等体模式.....	5-9
5.2.6 配置广播模式.....	5-10
5.2.7 配置组播模式.....	5-10
5.2.8 禁止指定接口接收 NTP 报文.....	5-11
5.2.9 检查配置结果.....	5-12
5.3 配置 NTP 安全机制.....	5-12
5.3.1 建立配置任务.....	5-13
5.3.2 配置 NTP 访问控制权限.....	5-15
5.3.3 使能 NTP 验证.....	5-15
5.3.4 在单播服务器/客户端模式下配置 NTP 验证.....	5-16
5.3.5 在对等体模式下配置 NTP 验证.....	5-16
5.3.6 在广播模式下配置 NTP 验证.....	5-17
5.3.7 在组播模式下配置 NTP 验证.....	5-17
5.3.8 在多播模式下配置 NTP 验证.....	5-18

5.3.9 检查配置结果.....	5-18
5.3.10 配置 KOD.....	5-19
5.3.11 在服务器端配置 KOD.....	5-19
5.3.12 客户端-服务器模式下在客户端配置 KOD.....	5-19
5.3.13 多播模式下在客户端配置 KOD.....	5-20
5.3.14 在对等体模式下为客户端配置 KOD.....	5-20
5.3.15 检查配置结果.....	5-20
5.4 维护 NTP.....	5-21
5.5 NTP 配置举例.....	5-21
5.5.1 配置带验证的单播 NTP 服务器/客户端模式示例.....	5-22
5.5.2 配置 NTP 对等体模式的示例.....	5-26
5.5.3 配置带验证的 NTP 广播模式示例.....	5-28
5.5.4 配置 NTP 组播模式示例.....	5-31
5.5.5 配置 NTP 多播模式示例.....	5-33
5.5.6 使用私有方案在客户端/服务器模式下配置 NTP 自动密钥的示例.....	5-36
5.5.7 使用可信方案在对等体模式下配置 NTP 自动密钥的示例.....	5-40
5.5.8 使用 IFF 方案在广播模式下配置 NTP 自动密钥的示例.....	5-43
5.5.9 使用 GQ 方案在组播模式下配置自动密钥的示例.....	5-46
5.5.10 使用 MV 方案在多播模式下配置 NTP 自动密钥的示例.....	5-49
5.5.11 在单播服务器/客户端模式下配置 NTP 验证的示例.....	5-52
5.5.12 在 NTP 对等体模式下配置 KOD 的示例.....	5-56
5.5.13 在 NTP 多播模式下配置 KOD 的示例.....	5-59
6 NQA 配置.....	6-1
6.1 NQA 简介.....	6-5
6.1.1 NQA 概述.....	6-5
6.1.2 NQA 与 Ping 的比较.....	6-5
6.1.3 NQA 客户端和服务端.....	6-6
6.1.4 NE20E-X6 支持的 NQA 特性.....	6-6
6.2 配置 ICMP 测试.....	6-8
6.2.1 建立配置任务.....	6-8
6.2.2 配置 ICMP 测试参数.....	6-9
6.2.3 检查配置结果.....	6-10
6.3 配置 DHCP 测试.....	6-11
6.3.1 建立配置任务.....	6-11
6.3.2 配置 DHCP 测试参数.....	6-12
6.3.3 检查配置结果.....	6-13
6.4 配置 FTP 下载测试.....	6-14
6.4.1 建立配置任务.....	6-14
6.4.2 配置 FTP 下载测试参数.....	6-15
6.4.3 检查配置结果.....	6-16
6.5 配置 FTP 上载测试.....	6-16
6.5.1 建立配置任务.....	6-17

6.5.2 配置 FTP 上载测试参数.....	6-17
6.5.3 检查配置结果.....	6-18
6.6 配置 HTTP 测试.....	6-19
6.6.1 建立配置任务.....	6-19
6.6.2 配置 HTTP 测试参数.....	6-20
6.6.3 检查配置结果.....	6-21
6.7 配置 DNS 测试.....	6-22
6.7.1 建立配置任务.....	6-22
6.7.2 配置 DNS 测试参数.....	6-23
6.7.3 检查配置结果.....	6-24
6.8 配置 Traceroute 测试.....	6-24
6.8.1 建立配置任务.....	6-24
6.8.2 配置 Traceroute 测试参数.....	6-25
6.8.3 检查配置结果.....	6-26
6.9 配置 SNMP 查询测试.....	6-27
6.9.1 建立配置任务.....	6-27
6.9.2 配置 SNMP 测试参数.....	6-27
6.9.3 检查配置结果.....	6-28
6.10 配置 TCP 测试.....	6-29
6.10.1 建立配置任务.....	6-29
6.10.2 配置 TCP 服务器端.....	6-30
6.10.3 配置 TCP 客户端.....	6-30
6.10.4 检查配置结果.....	6-31
6.11 配置 UDP 测试.....	6-32
6.11.1 建立配置任务.....	6-32
6.11.2 配置 UDP 测试服务器端.....	6-33
6.11.3 配置 UDP 测试客户端.....	6-33
6.11.4 检查配置结果.....	6-34
6.12 配置 Jitter 测试.....	6-35
6.12.1 建立配置任务.....	6-36
6.12.2 配置 Jitter 测试服务器端.....	6-37
6.12.3 配置 Jitter 测试客户端.....	6-37
6.12.4 检查配置结果.....	6-39
6.13 配置基于接口板发包的 Jitter 测试.....	6-40
6.13.1 建立配置任务.....	6-40
6.13.2 配置 Jitter 测试服务器端.....	6-41
6.13.3 配置 Jitter 测试客户端.....	6-42
6.13.4 检查配置结果.....	6-43
6.14 配置 LSP Ping 测试.....	6-44
6.14.1 建立配置任务.....	6-44
6.14.2 配置对 LSP 隧道的 LSP Ping 测试参数.....	6-45
6.14.3 配置对 TE 隧道的 LSP Ping 测试参数.....	6-46

6.14.4 配置对 CR-LSP 热备份隧道的 LSP Ping 测试参数.....	6-47
6.14.5 检查配置结果.....	6-48
6.15 配置 LSP Jitter 测试.....	6-49
6.15.1 建立配置任务.....	6-50
6.15.2 配置对 LDP 隧道的 LSP 抖动测试.....	6-50
6.15.3 配置对 MPLS TE 隧道的抖动测试.....	6-51
6.15.4 检查配置结果.....	6-52
6.16 配置 LSP Traceroute 测试.....	6-53
6.16.1 建立配置任务.....	6-54
6.16.2 配置对 LSP 隧道的 LSP Traceroute 测试参数.....	6-55
6.16.3 配置对 TE 隧道的 LSP Traceroute 测试参数.....	6-56
6.16.4 配置对 CR-LSP 热备份隧道的 LSP Traceroute 测试参数.....	6-57
6.16.5 检查配置结果.....	6-58
6.17 配置 ICMP Jitter 测试.....	6-59
6.17.1 建立配置任务.....	6-59
6.17.2 配置 ICMP Jitter 测试参数.....	6-60
6.17.3 检查配置结果.....	6-61
6.18 配置基于接口板发包的 ICMP Jitter 测试.....	6-62
6.18.1 建立配置任务.....	6-62
6.18.2 配置 ICMP Jitter 测试服务器端.....	6-63
6.18.3 配置 ICMP Jitter 测试客户端.....	6-64
6.18.4 检查配置结果.....	6-65
6.19 配置 Path Jitter 测试.....	6-66
6.19.1 建立配置任务.....	6-66
6.19.2 配置 PathJitter 测试参数.....	6-67
6.19.3 检查配置结果.....	6-68
6.20 配置 Path MTU 测试.....	6-69
6.20.1 建立配置任务.....	6-69
6.20.2 配置 Path MTU 测试参数.....	6-70
6.20.3 检查配置结果.....	6-71
6.21 配置 NQA 测试例实现 MPing 保留组地址.....	6-71
6.21.1 建立配置任务.....	6-72
6.21.2 创建 NQA MPing 测试例.....	6-72
6.21.3 配置 NQA MPing 测试例基本功能.....	6-73
6.21.4 （可选）调整 NQA MPing 测试例性能.....	6-73
6.21.5 启动 NQA MPing 测试例.....	6-74
6.21.6 检查配置结果.....	6-74
6.22 配置 NQA 测试例实现 MPing 普通组地址.....	6-75
6.22.1 建立配置任务.....	6-76
6.22.2 创建 NQA MPing 测试例.....	6-76
6.22.3 配置 NQA MPing 测试例基本功能.....	6-77
6.22.4 （可选）调整 NQA MPing 测试例性能.....	6-77

6.22.5 启动 NQA MPing 测试例.....	6-78
6.22.6 检查配置结果.....	6-78
6.23 通过 NQA 检测从组播源到查询者的 RPF 路径.....	6-79
6.23.1 建立配置任务.....	6-79
6.23.2 创建 NQA MTrace 测试例.....	6-80
6.23.3 配置 NQA MTrace 测试例基本功能.....	6-80
6.23.4 （可选）调整 NQA MTrace 测试例性能.....	6-81
6.23.5 启动 NQA MTrace 测试例.....	6-81
6.23.6 检查配置结果.....	6-82
6.24 通过 NQA 检测从组播源到查询者的组播路径.....	6-82
6.24.1 建立配置任务.....	6-83
6.24.2 创建 NQA MTrace 测试例.....	6-84
6.24.3 配置 NQA MTrace 测试例基本功能.....	6-84
6.24.4 （可选）调整 NQA MTrace 测试例性能.....	6-84
6.24.5 启动 NQA MTrace 测试例.....	6-85
6.24.6 检查配置结果.....	6-85
6.25 通过 NQA 检测从组播源到目的主机的 RPF 路径.....	6-86
6.25.1 建立配置任务.....	6-86
6.25.2 创建 NQA MTrace 测试例.....	6-87
6.25.3 配置 NQA MTrace 测试例基本功能.....	6-87
6.25.4 （可选）调整 NQA MTrace 测试例性能.....	6-88
6.25.5 启动 NQA MTrace 测试例.....	6-89
6.25.6 设置查询者过滤策略.....	6-89
6.25.7 检查配置结果.....	6-90
6.26 通过 NQA 检测从组播源到目的主机的组播路径.....	6-90
6.26.1 建立配置任务.....	6-91
6.26.2 创建 NQA MTrace 测试例.....	6-91
6.26.3 配置 NQA MTrace 测试例基本功能.....	6-92
6.26.4 （可选）调整 NQA MTrace 测试例性能.....	6-93
6.26.5 启动 NQA MTrace 测试例.....	6-93
6.26.6 设置查询者过滤策略.....	6-94
6.26.7 检查配置结果.....	6-94
6.27 配置单跳 PW 的 PWE3 Ping 测试.....	6-95
6.27.1 建立配置任务.....	6-95
6.27.2 配置单跳 PW 的 PWE3 Ping 测试参数.....	6-96
6.27.3 检查配置结果.....	6-97
6.28 配置多跳 PW 的 PWE3 Ping 测试.....	6-98
6.28.1 建立配置任务.....	6-98
6.28.2 配置多跳 PW 的 PWE3 Ping 测试参数.....	6-99
6.28.3 检查配置结果.....	6-100
6.29 配置单跳 PW 的 PWE3 Trace 测试.....	6-101
6.29.1 建立配置任务.....	6-101

6.29.2 配置单跳 PW 的 PWE3 Trace 测试参数.....	6-102
6.29.3 检查配置结果.....	6-103
6.30 配置多跳 PW 的 PWE3 Trace 测试.....	6-104
6.30.1 建立配置任务.....	6-104
6.30.2 配置多跳 PW 的 PWE3 Trace 测试参数.....	6-105
6.30.3 检查配置结果.....	6-106
6.31 配置多跳跨域 Kompella VLL 的 VC Trace 测试.....	6-107
6.31.1 建立配置任务.....	6-107
6.31.2 配置多跳跨域 Kompella VLL 的 VC Trace 测试参数.....	6-108
6.31.3 检查配置结果.....	6-109
6.32 配置 NQA 测试组.....	6-110
6.32.1 建立配置任务.....	6-111
6.32.2 创建 NQA 测试组.....	6-111
6.32.3 检查配置结果.....	6-112
6.33 配置 NQA 测试例的通用参数.....	6-113
6.33.1 建立配置任务.....	6-113
6.33.2 配置测试例的通用参数.....	6-113
6.33.3 检查配置结果.....	6-118
6.34 配置 NQA 双向传输延迟阈值.....	6-118
6.34.1 建立配置任务.....	6-118
6.34.2 配置双向传输延迟阈值.....	6-119
6.34.3 检查配置结果.....	6-119
6.35 配置 NQA 单向传输延迟阈值.....	6-120
6.35.1 建立配置任务.....	6-120
6.35.2 配置单向传输延迟阈值.....	6-121
6.35.3 检查配置结果.....	6-121
6.36 配置 NQA 测试的 Trap 开关.....	6-122
6.36.1 建立配置任务.....	6-122
6.36.2 配置发送测试失败发送 Trap.....	6-123
6.36.3 配置探测失败发送 Trap.....	6-124
6.36.4 配置探测完成发送 Trap.....	6-124
6.36.5 配置超过阈值发送 Trap.....	6-125
6.36.6 检查配置结果.....	6-125
6.37 配置测试结果发送到 FTP 服务器.....	6-126
6.37.1 建立配置任务.....	6-126
6.37.2 配置连接 FTP 服务器需要的参数.....	6-127
6.37.3 使能通过 FTP 保存 NQA 测试结果功能.....	6-128
6.37.4 （可选）配置通过 FTP 保存测试结果的条数.....	6-128
6.37.5 （可选）配置通过 FTP 保存的测试结果的时间.....	6-128
6.37.6 （可选）配置 FTP 传送成功向网管端发送 Trap.....	6-128
6.37.7 启动测试例.....	6-129
6.37.8 检查配置结果.....	6-129

6.38 配置上下限 NQA 阈值告警.....	6-130
6.38.1 建立配置任务.....	6-130
6.38.2 配置阈值告警相关事件.....	6-131
6.38.3 配置阈值告警.....	6-131
6.38.4 启动测试例.....	6-132
6.38.5 检查配置结果.....	6-132
6.39 配置 VPLS 组播 Ping 检测 VPLS 网络测试.....	6-133
6.39.1 建立配置任务.....	6-133
6.39.2 配置 VPLS 组播 Trace 检测组播转发.....	6-134
6.39.3 检查配置结果.....	6-135
6.40 配置 VPLS 组播 Ping 检测 Kompella VPLS 网络测试.....	6-136
6.40.1 建立配置任务.....	6-136
6.40.2 配置 VPLS 组播 Ping 检测组播转发.....	6-137
6.40.3 检查配置结果.....	6-138
6.41 配置 MAC Trace 测试.....	6-139
6.41.1 建立配置任务.....	6-139
6.41.2 配置 MAC Trace 测试参数.....	6-140
6.41.3 检查配置结果.....	6-140
6.42 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性.....	6-141
6.42.1 建立配置任务.....	6-141
6.42.2 配置 GMAC Ping 测试参数.....	6-142
6.42.3 配置 GMAC Trace 测试参数.....	6-143
6.42.4 检查配置结果.....	6-143
6.43 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性.....	6-145
6.43.1 建立配置任务.....	6-145
6.43.2 配置 GMAC Ping 测试参数.....	6-145
6.43.3 配置 GMAC Trace 测试参数.....	6-146
6.43.4 检查配置结果.....	6-147
6.44 配置 VPLS PW Ping 和 PW Trace 测试.....	6-148
6.44.1 建立配置任务.....	6-148
6.44.2 配置 VPLS PW Ping 测试参数.....	6-149
6.44.3 配置 VPLS PW Trace 测试参数.....	6-150
6.44.4 检查配置结果.....	6-151
6.45 配置 VPLS 组播 Trace 检测 VPLS 网络测试.....	6-153
6.45.1 建立配置任务.....	6-153
6.45.2 配置 VPLS 组播 Trace 检测组播转发.....	6-154
6.45.3 检查配置结果.....	6-155
6.46 配置 VPLS MAC Ping 测试.....	6-155
6.46.1 建立配置任务.....	6-156
6.46.2 配置 VPLS MAC Ping 测试参数.....	6-156
6.46.3 检查配置结果.....	6-157
6.47 配置 VPLS MAC Trace 测试.....	6-158

6.47.1 建立配置任务.....	6-158
6.47.2 配置 VPLS MAC Trace 测试参数.....	6-158
6.47.3 检查配置结果.....	6-159
6.48 配置 NQA 报文改写检查功能.....	6-160
6.49 维护 NQA.....	6-161
6.49.1 重新启动测试例.....	6-161
6.49.2 清除统计信息.....	6-162
6.49.3 调试 NQA.....	6-162
6.50 NQA 配置举例.....	6-163
6.50.1 配置 ICMP 测试示例.....	6-165
6.50.2 配置 DHCP 测试示例.....	6-167
6.50.3 配置 FTP 下载速度测试示例.....	6-169
6.50.4 配置 FTP 上载速度测试示例.....	6-171
6.50.5 配置 HTTP 测试示例.....	6-173
6.50.6 配置 DNS 测试示例.....	6-175
6.50.7 配置 Traceroute 测试示例.....	6-176
6.50.8 配置 SNMP Query 测试示例.....	6-178
6.50.9 配置 TCP 测试示例.....	6-180
6.50.10 配置 UDP 测试示例.....	6-182
6.50.11 配置 Jitter 测试示例.....	6-184
6.50.12 配置基于接口板发包的 Jitter 测试例.....	6-187
6.50.13 配置普通隧道 LSP Ping 测试示例.....	6-189
6.50.14 配置普通隧道 LSP Jitter 测试示例.....	6-192
6.50.15 配置 TE 隧道 LSP Jitter 测试示例.....	6-195
6.50.16 配置 ICMP Jitter 测试示例.....	6-198
6.50.17 配置基于接口板发包的 ICMP Jitter 测试例.....	6-199
6.50.18 配置 Path Jitter 测试示例.....	6-202
6.50.19 配置 Path MTU 测试示例.....	6-204
6.50.20 配置 TE 隧道 LSP Traceroute 测试示例.....	6-206
6.50.21 配置检测网段中的保留组成员示例.....	6-209
6.50.22 配置检测网络承载组播业务的性能示例.....	6-212
6.50.23 配置检测从组播源到当前路由器的 RPF 路径的测试例示例.....	6-217
6.50.24 配置检测从组播源到当前路由器的组播路径的测试例示例.....	6-222
6.50.25 配置检测从组播源到目的主机的 RPF 路径的测试例示例.....	6-226
6.50.26 配置检测从组播源到目的主机的组播路径的测试例示例.....	6-230
6.50.27 配置单跳 PW 的 PWE3 Ping 测试示例.....	6-233
6.50.28 配置多跳 PW 的 PWE3 Ping 测试示例.....	6-237
6.50.29 配置单跳 PW 的 PWE3 Trace 测试示例.....	6-242
6.50.30 配置多跳 PW 的 PWE3 Trace 测试示例.....	6-246
6.50.31 配置多跳跨域 Kompella L2VPN 的 VC Trace 测试示例.....	6-252
6.50.32 配置 NQA 测试组示例.....	6-258
6.50.33 配置向网管端发送 NQA 阈值告警示例.....	6-261

6.50.34 配置测试结果发送到 FTP 服务器示例.....	6-264
6.50.35 配置 NQA 上下限阈值告警示例.....	6-267
6.50.36 配置 Martini VPLS 的 VPLS 组播 Ping 测试示例.....	6-269
6.50.37 配置 Kompella VPLS 的 VPLS 组播 Ping 测试示例.....	6-273
6.50.38 配置 Martini VPLS 的 VPLS 组播 Trace 测试示例.....	6-277
6.50.39 配置 VPLS MAC Ping 测试示例.....	6-281
6.50.40 配置 VPLS MAC Trace 测试示例.....	6-285
6.50.41 配置 VPLS PW Ping 和 PW Trace 测试示例.....	6-289
6.50.42 配置 MAC Trace 测试 VLAN 示例.....	6-293
6.50.43 配置 MAC Trace 测试 VPLS 示例.....	6-296
6.50.44 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 示例.....	6-301
6.50.45 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 示例.....	6-305
6.50.46 配置 VPLS PW Ping 和 PW Trace 测试示例.....	6-309
6.50.47 配置对指定的组播 VPN 网络进行从组播源到目的主机的 RPF 路径检测.....	6-314
6.50.48 配置 NQA 上下限阈值告警、联动测试例事件示例.....	6-321
6.50.49 配置 CR-LSP 热备份隧道 LSP Traceroute 测试示例.....	6-324
7 NetStream 配置.....	7-1
7.1 NetStream 简介.....	7-2
7.1.1 NetStream 概述.....	7-2
7.1.2 NE20E-X6 支持的 NetStream 特性.....	7-3
7.2 配置 IPv4 网络的流量统计.....	7-5
7.2.1 建立配置任务.....	7-6
7.2.2 （可选）调整设备的 AS 域和接口索引模式.....	7-7
7.2.3 配置 NetStream 业务的处理方式.....	7-8
7.2.4 使能接口的 NetStream 功能.....	7-8
7.2.5 （可选）配置原始流 TCP-flag 的统计功能.....	7-9
7.2.6 （可选）配置模板刷新参数.....	7-10
7.2.7 配置 NetStream 报文的输出.....	7-10
7.2.8 配置 NetStream 的采样方式和采样比.....	7-12
7.2.9 检查配置结果.....	7-13
7.3 配置 MPLS 网络的流量统计.....	7-14
7.3.1 建立配置任务.....	7-15
7.3.2 （可选）调整设备的 AS 域和接口索引模式.....	7-16
7.3.3 配置 NetStream 采样的处理方式.....	7-17
7.3.4 使能接口的 NetStream 统计功能.....	7-17
7.3.5 配置 MPLS 报文的统计功能.....	7-17
7.3.6 （可选）配置模板刷新参数.....	7-18
7.3.7 配置 NetStream 报文的输出.....	7-18
7.3.8 配置 NetStream 的采样.....	7-18
7.3.9 检查配置结果.....	7-19
7.4 配置聚合流的流量统计.....	7-20
7.4.1 建立配置任务.....	7-21

7.4.2 配置聚合功能.....	7-21
7.4.3 （可选）配置 NetStream 报文输出的格式.....	7-22
7.4.4 （可选）配置聚合流模板刷新参数.....	7-22
7.4.5 （可选）配置老化时间.....	7-23
7.4.6 配置 NetStream 报文的输出.....	7-23
7.4.7 检查配置结果.....	7-24
7.5 配置 NetStream 多地址输出.....	7-25
7.5.1 建立配置任务.....	7-25
7.5.2 使能接口的 NetStream 功能.....	7-25
7.5.3 配置 NetStream 的采样比.....	7-26
7.5.4 配置 NetStream 的采样模式.....	7-26
7.5.5 配置报文的输出格式.....	7-26
7.5.6 配置统计信息的多地址输出.....	7-27
7.5.7 检查配置结果.....	7-27
7.6 维护 NetStream.....	7-28
7.6.1 强制老化原始流.....	7-28
7.7 配置举例.....	7-29
7.7.1 配置 IPv4 网络用户侧异常流量统计分析示例.....	7-29
7.7.2 配置 IPv4 网络 VLANIF 流量统计示例.....	7-32
7.7.3 配置 IPv4 网络 GRE 流量统计示例.....	7-35
7.7.4 配置 MPLS 网络的流量统计示例.....	7-39
7.7.5 配置聚合流的流量统计示例.....	7-43
7.7.6 配置统计信息输出主机备份示例.....	7-46
7.7.7 配置 VLAN 聚合流量统计示例.....	7-48
7.7.8 配置 NetStream 接口索引映射示例.....	7-52
7.7.9 配置 NetStream 的多地址输出.....	7-55
8 Ping 和 Tracert.....	8-1
8.1 ping 和 tracert 简介.....	8-3
8.1.1 ping 和 tracert.....	8-3
8.2 配置 ping 和 tracert 检测网络.....	8-3
8.2.1 建立配置任务.....	8-3
8.2.2 使用 ping 检测网络连接是否正常.....	8-4
8.2.3 使用 tracert 检测网络发生故障的位置.....	8-5
8.3 使用 Ping 和 Trace 检测 LDP LSP.....	8-5
8.3.1 建立配置任务.....	8-6
8.3.2 使用 Ping 检测 LDP LSP.....	8-6
8.3.3 使用 Tracert 检测 LDP LSP 连通性.....	8-7
8.4 使用 Ping 和 Tracert 检测 TE Tunnel.....	8-7
8.4.1 建立配置任务.....	8-8
8.4.2 使用 Ping 检测 TE Tunnel 连通性.....	8-8
8.4.3 使用 Trace 检测 TE Tunnel 连通性.....	8-9
8.5 使用 Ping 和 Tracert 检测 VLL 网络.....	8-9

8.5.1 建立配置任务.....	8-10
8.5.2 使用 Ping 检测 VLL 网络连通性.....	8-10
8.5.3 使用 Tracert 检测 VLL 网络连通性.....	8-11
8.6 使用 Ping 和 Tracert 检测 PWE3 网络.....	8-12
8.6.1 建立配置任务.....	8-12
8.6.2 使用 Ping 检测 PWE3 网络连通性.....	8-13
8.6.3 使用 Tracert 检测 PWE3 网络连通性.....	8-14
8.7 使用 Ping 和 Tracert 检测 VPLS 网络.....	8-15
8.7.1 建立配置任务.....	8-15
8.7.2 使用 Ping 检测 VPLS 网络连通性.....	8-16
8.7.3 使用 Tracert 检测 VPLS 网络连通性.....	8-17
8.8 使用 Ping 和 Tracert 检测 BGP/MPLS IP VPN 网络.....	8-17
8.8.1 建立配置任务.....	8-17
8.8.2 使用 Ping 检测 BGP/MPLS IP VPN 网络的连通性.....	8-18
8.9 使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络.....	8-19
8.9.1 建立配置任务.....	8-19
8.9.2 使用 MAC Ping 检测 VPLS 网络连通性.....	8-20
8.9.3 使用 MAC Trace 检测 VPLS 网络连通性.....	8-20
8.10 使用 Ping 和 Tracert 检测 TE Tunnel 叶子节点故障.....	8-21
8.10.1 建立配置任务.....	8-21
8.10.2 使用 Ping 检测 TE Tunnel 叶子节点故障.....	8-22
8.10.3 使用 Tracert 检测 TE Tunnel 叶子节点故障.....	8-23
8.11 使用 Ping 检测 MPLS 网络.....	8-23
8.11.1 建立配置任务.....	8-24
8.11.2 使用 Ping 检测 MPLS 网络 IP 转发是否正常.....	8-24
8.12 使用 Ping 检测 Trunk 链路.....	8-25
8.12.1 建立配置任务.....	8-25
8.12.2 使用 Ping 检测三层 Trunk 成员接口连通性.....	8-26
8.13 使用 Ping 和 Trace 检测多跳 PW.....	8-26
8.13.1 建立配置任务.....	8-27
8.13.2 使用 Ping 检测 MH-PW 连通性.....	8-30
8.13.3 使用 Trace 检测 MH-PW 连通性.....	8-30
8.14 使用 Service Ping 检测 PWE3 网络.....	8-31
8.14.1 建立配置任务.....	8-31
8.14.2 使用 Service Ping 检测 PWE3 网络.....	8-32
8.15 使用 Service Ping 检测 VLL 接入 VPLS 网络.....	8-33
8.15.1 建立配置任务.....	8-33
8.15.2 使用 Service Ping 检测 VLL 接入 VPLS 网络连通性.....	8-34
8.16 配置智能 ping 检测网络.....	8-35
8.16.1 建立配置任务.....	8-35
8.16.2 使用智能 ping 检测网络连接是否正常.....	8-36
9 LLDP 配置.....	9-1

9.1 LLDP 简介.....	9-2
9.1.1 LLDP 概述.....	9-2
9.1.2 NE20E-X6 支持的 LLDP 特性.....	9-2
9.2 配置 LLDP 功能.....	9-4
9.2.1 建立配置任务.....	9-4
9.2.2 （可选）使能 LLDP 告警.....	9-6
9.2.3 使能全局 LLDP 功能.....	9-6
9.2.4 （可选）去使能接口 LLDP 功能.....	9-6
9.2.5 （可选）配置 LLDP 管理地址.....	9-7
9.2.6 （可选）配置 LLDP 属性.....	9-7
9.2.7 检查配置结果.....	9-9
9.3 维护 LLDP.....	9-10
9.3.1 清除 LLDP 统计信息.....	9-10
9.3.2 监控 LLDP 运行状态.....	9-10
9.4 配置举例.....	9-11
9.4.1 配置 LLDP 功能示例.....	9-11
9.4.2 配置有 Eth-Trunk 的网络的 LLDP 功能示例.....	9-14
9.4.3 配置一个接口有多邻居的网络的 LLDP 功能示例.....	9-18
10 故障管理.....	10-1
10.1 故障管理简介.....	10-2
10.1.1 故障管理.....	10-2
10.2 配置告警管理.....	10-2
10.2.1 建立配置任务.....	10-2
10.2.2 配置告警级别.....	10-3
10.2.3 配置告警延迟上报.....	10-3
10.2.4 配置告警相关性抑制.....	10-4
10.2.5 检查配置结果.....	10-4
10.3 配置事件管理.....	10-5
10.3.1 建立配置任务.....	10-6
10.3.2 配置事件延迟上报.....	10-6
10.3.3 检查配置结果.....	10-7
10.4 配置实体故障隔离.....	10-8
10.5 维护.....	10-8
10.5.1 清除告警信息.....	10-8
10.5.2 清除事件信息.....	10-9
10.6 配置举例.....	10-9
10.6.1 配置告警管理示例.....	10-10
A 术语.....	A-1
B 缩略语.....	B-1

插图目录

图 1-1 信息中心的功能.....	1-4
图 1-2 日志输出格式.....	1-5
图 1-3 告警输出格式.....	1-6
图 1-4 配置向日志文件输出日志信息组网图.....	1-29
图 1-5 配置向日志主机输出信息组网图.....	1-31
图 1-6 配置使用管理 VPN 实例时向公网日志主机输出日志信息组网图.....	1-35
图 1-7 配置向日志主机发送二进制日志示例.....	1-38
图 1-8 输出告警到 SNMP Agent 组网图.....	1-40
图 1-9 向控制台输出信息组网图.....	1-42
图 2-1 SNMP 结构示意图.....	2-3
图 2-2 MIB 树结构.....	2-3
图 2-3 SNMP 操作示意图.....	2-4
图 2-4 配置使用 SNMPv1 与网管通信组网图.....	2-34
图 2-5 配置使用 SNMPv2c 管通信组网图.....	2-37
图 2-6 配置使用 SNMPv3 网管通信组网图.....	2-41
图 3-1 配置 RMON 组网图.....	3-14
图 3-2 RMON2 典型配置组网图.....	3-18
图 4-1 集群基本组网图（树型）.....	4-3
图 4-2 集群基本组网图（RRPP）.....	4-4
图 4-3 配置 HGMP 集群基本功能的组网图.....	4-27
图 4-4 配置 HGMP 集群内外设备互通（NAT 方式）的典型组网图.....	4-36
图 4-5 配置 HGMP 集群内外设备互通（非 NAT 方式）的典型组网图.....	4-47
图 4-6 配置 HGMP 集群内外 SNMP 互通（NAT 方式）的典型组网图.....	4-57
图 4-7 配置 HGMP 集群内外 SNMP 互通（非 NAT 方式）的典型组网图.....	4-67
图 4-8 配置 HGMP 集群批量下发功能的典型组网图.....	4-78
图 4-9 配置 HGMP 集群批量重启功能的典型组网图.....	4-89
图 4-10 配置 HGMP 集群增量配置功能的典型组网图.....	4-99
图 4-11 配置 HGMP 集群同步配置文件功能的典型组网图.....	4-109
图 4-12 配置 HGMP 集群安全特性的典型组网图.....	4-119
图 5-1 NTP 基本原理图.....	5-3
图 5-2 单播 NTP 服务器/客户端模式组网图.....	5-22
图 5-3 配置 NTP 对等体模式的组网图.....	5-26
图 5-4 配置 NTP 广播模式的组网图.....	5-29

图 5-5 配置 NTP 组播模式的组网图.....	5-31
图 5-6 NTP 多播模式的组网图.....	5-34
图 5-7 使用私有方案在服务器/客户端模式下配置 NTP 自动密钥的组网图.....	5-36
图 5-8 使用可信方案在对等体模式下配置 NTP 自动密钥的组网图.....	5-40
图 5-9 NTP 广播模式的组网图.....	5-43
图 5-10 使用 GQ 方案在组播模式下配置 NTP 自动密钥的组网图.....	5-46
图 5-11 使用 MV 方案在多播模式下配置 NTP 自动密钥的组网图.....	5-49
图 5-12 单播 NTP 服务器/客户端模式组网图.....	5-52
图 5-13 配置 NTP 对等体模式的组网图.....	5-57
图 5-14 配置 NTP 多播模式的组网图.....	5-60
图 6-1 NQA 测试示意图.....	6-5
图 6-2 NQA 客户端和服务器的关系.....	6-6
图 6-3 ICMP 测试组网图.....	6-166
图 6-4 DHCP 测试组网图.....	6-167
图 6-5 FTP 测试组网图.....	6-169
图 6-6 FTP 测试组网图.....	6-171
图 6-7 HTTP 测试组网图.....	6-173
图 6-8 DNS 测试组网图.....	6-175
图 6-9 Traceroute 测试组网图.....	6-177
图 6-10 SNMP Query 测试组网图.....	6-179
图 6-11 TCP 测试组网图.....	6-181
图 6-12 UDP 测试组网图.....	6-183
图 6-13 Jitter 测试组网图.....	6-185
图 6-14 Jitter 测试组网图.....	6-187
图 6-15 LSP Ping 测试组网图.....	6-190
图 6-16 ICMP Jitter 测试组网图.....	6-198
图 6-17 基于接口板发包的 ICMP Jitter 测试组网图.....	6-200
图 6-18 ICMP Jitter 测试组网图.....	6-202
图 6-19 Path MTU 测试组网图.....	6-204
图 6-20 LSP Traceroute 测试组网图.....	6-206
图 6-21 mping 保留组地址组网图.....	6-210
图 6-22 MPing 普通组地址组网图.....	6-212
图 6-23 MTrace 组网图.....	6-218
图 6-24 单跳 PW 的 PWE3 Ping 测试组网示例.....	6-234
图 6-25 多跳 PW 的 PWE3 Ping 测试组网示例.....	6-238
图 6-26 单跳 PW 的 PWE3 Trace 测试组网示例.....	6-243
图 6-27 多跳 PW 的 PWE3 Trace 测试组网示例.....	6-247
图 6-28 多跳跨域 Kompella L2VPN 的 VC Trace 测试组网示例.....	6-252
图 6-29 NQA 测试组网图.....	6-258
图 6-30 配置 NQA 阈值组网图.....	6-261
图 6-31 测试结果发送到 FTP 服务器组网图.....	6-265
图 6-32 配置 NQA 阈值告警组网图.....	6-267

图 6-33 Martini 方式 VPLS 组网图.....	6-270
图 6-34 Kompella 方式 VPLS 组网图.....	6-274
图 6-35 Martini 方式 VPLS 组网图.....	6-278
图 6-36 配置 VPLS MAC Ping 测试组网图.....	6-282
图 6-37 配置 VPLS MAC Trace 测试组网.....	6-285
图 6-38 配置 VPLS PW Ping 和 PW Trace 测试组网.....	6-289
图 6-39 配置 MAC Trace 测试 VLAN 组网.....	6-293
图 6-40 配置 MAC Trace 测试 VPLS 组网.....	6-296
图 6-41 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 组网.....	6-302
图 6-42 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 组网.....	6-305
图 6-43 配置 VPLS PW Ping 和 PW Trace 测试组网.....	6-310
图 6-44 配置单自治域 MD VPN 组网图.....	6-315
图 6-45 配置 NQA 阈值告警组网图.....	6-322
图 6-46 LSP Traceroute 测试组网图.....	6-325
图 7-1 NetStream 的设备角色.....	7-3
图 7-2 IPv4 网络的流量统计示意图.....	7-6
图 7-3 配置 MPLS 网络的流量统计组网图.....	7-15
图 7-4 配置 IPv4 网络用户侧异常流量统计分析组网图.....	7-30
图 7-5 配置 IPv4 网络 VLANIF 流量统计组网图.....	7-33
图 7-6 配置 IPv4 网络 GRE 流量统计组网图.....	7-36
图 7-7 配置 MPLS 网络的流量统计组网图.....	7-39
图 7-8 配置聚合流的流量统计组网图.....	7-43
图 7-9 配置统计信息输出双主机备份组网图.....	7-46
图 7-10 配置 VLAN 聚合流量统计组网.....	7-48
图 7-11 配置 NetStream 接口索引映射示例组网图.....	7-52
图 7-12 配置 NetStream 的多地址输出组网.....	7-55
图 8-1 MS-PW 网络组网图.....	8-27
图 8-2 PWE3 典型组网图.....	8-32
图 8-3 VLL 接入 VPLS 典型组网图.....	8-34
图 9-1 LLDP 应用环境组网图.....	9-5
图 9-2 配置 LLDP 功能组网图.....	9-12
图 9-3 配置有 Eth-Trunk 的网络的 LLDP 功能组网图.....	9-15
图 9-4 配置一个接口有多邻居的网络的 LLDP 功能组网图.....	9-19

表格目录

表 1-1 信息严重等级的定义.....1-2

表 1-2 信息通道和输出方向.....1-4

表 1-3 日志记录格式说明.....1-5

表 1-4 告警记录格式说明.....1-6

表 2-1 SNMP 的操作.....2-4

表 2-2 SNMP 支持的特性功能介绍.....2-5

表 2-3 SNMP 各版本支持的特性概况.....2-5

表 2-4 SNMP 各版本的应用场景.....2-6

表 3-1 各表的生存时间.....3-4

表 5-1 NTP 访问控制权限配置.....5-15

1 信息中心配置

关于本章

介绍了信息中心的基本概念和工作方式、配置过程、维护命令，并提供配置举例。

1.1 信息中心简介

信息中心是控制日志、告警、调试信息输出的通道。

1.2 配置日志信息的输出

配置日志信息的输出可以配置指定模块的日志信息输出到日志文件、控制台、终端和日志主机中。

1.3 配置告警信息的输出

配置告警信息的输出可以配置指定模块的告警信息输出到日志文件、控制台、终端和SNMP代理中。

1.4 配置调试信息的输出

配置调试信息的输出可以配置指定模块的调试信息输出到日志文件、控制台、终端和日志主机中。

1.5 维护信息中心

当确认信息中心中的缓冲信息需要删除时，可以执行命令 `reset info-center statistics`、`reset logbuffer` 和 `reset trapbuffer` 进行清除。执行清除命令后，信息将无法恢复。

1.6 信息中心配置举例

以示例方式介绍信息中心的配置。

1.1 信息中心简介

信息中心是控制日志、告警、调试信息输出的通道。

1.1.1 信息中心概述

信息中心是路由器的信息枢纽，通过对系统输出信息进行分类和筛选，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供强有力的支持。

1.1.2 NE20E-X6 支持的信息中心特性

NE20E-X6 系统中可以支持将 3 种信息（日志、告警和调试信息），按照 8 个严重等级，分配到 10 个信息通道中，再输出到多个方向。

1.1.1 信息中心概述

信息中心是路由器的信息枢纽，通过对系统输出信息进行分类和筛选，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供强有力的支持。

1.1.2 NE20E-X6 支持的信息中心特性

NE20E-X6 系统中可以支持将 3 种信息（日志、告警和调试信息），按照 8 个严重等级，分配到 10 个信息通道中，再输出到多个方向。

信息的分类

信息中心可以接收和处理 3 类信息：

- log 类：日志信息
- debug 类：调试信息
- trap 类：告警信息

信息的严重等级

根据信息的严重等级或紧急程度，信息分为 8 个等级。信息越严重，其严重等级值越小。详细信息见[表 1-1](#)。

表 1-1 信息严重等级的定义

显示值	严重等级	描述
0	Emergency	设备致命的异常，系统已经无法恢复正常，必须重启设备。如程序异常导致设备重启，内存的使用被检测出错误等。
1	Alert	设备重大的异常，需要立即采取措施。如设备内存占用率达到极限等。
2	Critical	设备重大的异常，需要采取措施进行处理或原因分析。如设备内存占用率超过低界线，温度超过低温告警线，BFD 探测出设备不可达，检测出错误的消息（消息是由本设备内部生成）等。

显示值	严重等级	描述
3	Error	错误的操作或设备的异常流程，不会影响后续业务，但是需要关注和原因分析。如用户的错误指令，用户密码错误，检测出错误协议报文（报文是由其他设备获得）。
4	Warning	设备的异常运转的异常点，可能引起业务故障的流程，需要引起注意。如用户关闭路由进程，BFD 探测的一次报文丢失，检测出错误协议报文等。
5	Notice	用于设备正常运转的关键操作信息。如用户执行 shutdown 命令，邻居发现，协议状态机的正常跳转等。
6	Informational	用于设备正常运转的一般性操作信息。如用户使用 display 命令等。
7	Debugging	设备正常运转的一般性信息，用户无需关注。

根据严重等级过滤信息时，仅输出严重等级值小于或等于所配置的严重等级值的信息，即，输出所配置级别和比所配置级别更严重的信息。

例如，当配置严重等级阈值为 6 时，仅输出严重等级值为 0 ~ 6 的信息。

信息中心的工作过程

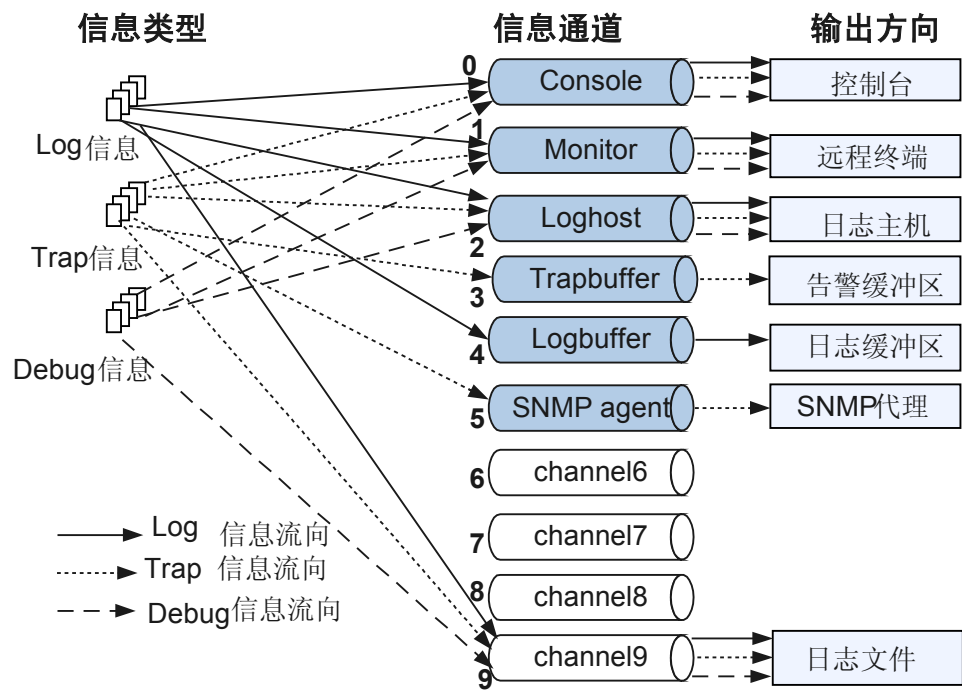
信息中心的工作过程如下：

- 接收各模块输出的日志信息（log）、告警信息（trap）和调试信息（debug）。
- 根据用户的设置，将不同重要程度的信息输出到不同的信息通道。
- 根据信息通道和输出方向的关联，将信息输出到不同方向。

概括来说，信息中心的主要工作就是将 3 种信息，按照 8 个严重等级，分配到 10 个信息通道中，再输出到多个方向。

如下图 1-1 所示。缺省情况下，日志、告警、调试信息都从缺省的信息通道输出。用户也可以指定从其他的通道进行输出，例如，用户配置发往日志缓存区的日志信息使用通道 6，则发送到日志缓存区的日志都会从通道 6 输出，不再从通道 4 输出。

图 1-1 信息中心的功能



信息通道和输出方向

信息中心支持 10 个通道，其中，通道 0 ~ 5 有缺省通道名。并且，这 6 个信息通道缺省与 6 个输出方向分别关联。设备上的 CF 卡缺省情况下，日志信息输出到日志文件使用通道 9，即，共支持 7 个缺省输出方向。

缺省通道和输出方向的对应关系请见表 1-2。

表 1-2 信息通道和输出方向

通道号	缺省通道名	输出方向	描述
0	console	console	本地控制台，可以接收日志、告警、调试信息。
1	monitor	monitor	VTY 终端，可以接收日志、告警、调试信息。方便远程维护。
2	loghost	loghost	日志主机，可以接收日志、告警、调试信息。信息在日志主机上以文件形式保存，供随时查看。
3	trapbuffer	trapbuffer	告警缓冲区，可以接收告警信息。在路由器内部分配，用于记录信息。
4	logbuffer	logbuffer	日志缓冲区，可以接收日志信息。在路由器内部分配，用于记录信息。
5	snmpagent	snmpagent	SNMP 代理，可以接收告警信息。

通道号	缺省通道名	输出方向	描述
6	未指定	未指定	保留，可由用户指定输出方向。
7	未指定	未指定	保留，可由用户指定输出方向。
8	未指定	未指定	保留，可由用户指定输出方向。
9	channel9	logfile	日志文件，可以接收日志、告警、调试信息。在设备的 CF 卡上以文件形式保存。

在配置多日志主机的情况下，用户可以配置日志信息通过一个通道或多个通道输出到不同的日志主机中。例如配置部分日志信息通过通道 2（loghost）输出到日志主机，部分日志信息从通道 6 输出到日志主机，还可以更改通道 6 的名称，便于对信息通道的管理。

日志信息的输出格式

Syslog 是信息中心（info-center）的一个子功能。Syslog 使用 UDP 进行传输，使用端口号 514 将日志信息输出到日志主机中。

日志格式如图 1-2 所示：

图 1-2 日志输出格式

<Int_16>TIMESTAMP HOSTNAME %%ddAAA/B/CCC(I):slot=XXX; YYYY

各字段的详细说明见表 1-3。

表 1-3 日志记录格式说明

字段	字段含义	说明
<Int_16>	前导符	在向日志主机发送的时候添加前导符。 在设备本机保存的日志不保存前导符。
TIMESTAMP	时间戳，信息输出的时间	时间戳有 5 种格式可供选择。 ● boot 型：相对时间类型。 ● date 型：系统时间类型。告警信息、日志信息和调试信息缺省采用 date 型时间戳。 ● short-date 型：与 date 型的唯一区别是，short-date 型时间戳不含年份。 ● format-date 型：另一种系统时间形式。 ● none 型：信息中不包含时间戳。 时间戳与主机名之间用一个空格隔开。
HOSTNAME	主机名	缺省是“HUAWEI”。

字段	字段含义	说明
%%	华为公司的标识	标识该日志是由华为公司的产品输出的。
dd	版本号	用来标识该日志格式的版本。
AAA	模块名	向信息中心输出信息的模块名称。
B	日志的级别	表示日志信息的级别。
CCC	简要描述	用以进一步说明信息的类型。
(l)	信息的类别	l: 用户日志标识。
slot=XXX	定位信息	slot: 表示发送定位信息的槽位号。
YYYY	描述符	各个模块向信息中心输出的信息的具体内容。由各个模块在每次输出时填充, 详细描述该日志的具体内容。

告警信息的输出格式

图 1-3 告警输出格式

TimeStamp HostName ModuleName/Severity/Brief:Description

各字段的详细说明见表 1-4。

表 1-4 告警记录格式说明

字段	字段含义	说明
TimeStamp	时间戳, 信息输出的时间	时间戳有 4 种格式可供选择。 ● boot 型: 相对时间类型。 ● date 型: 系统时间类型。告警信息、日志信息和调试信息缺省采用 date 型时间戳。 ● short-date 型: 与 date 型的唯一区别是, short-date 型时间戳不含年份。 ● none 型: 信息中不包含时间戳。 时间戳与主机名之间用一个空格隔开。
HostName	主机名	缺省是“HUAWEI”。主机名与模块名之间用一个空格隔开。
ModuleName	模块名	用来表示产生告警的模块名。

字段	字段含义	说明
Severity	严重级别	告警的严重级别。 ● Critical（紧急） ● Major（重要） ● Minor（次要） ● Warning（提示） ● Indeterminate（不确定） ● Cleared（已清除）
Brief	简要描述	告警信息的简要描述。
Description	描述信息	告警信息的描述信息。

1.2 配置日志信息的输出

配置日志信息的输出可以配置指定模块的日志信息输出到日志文件、控制台、终端和日志主机中。

1.2.1 建立配置任务

在配置日志信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

1.2.2（可选）开启信息中心

信息中心缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

1.2.3（可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道需要输出的内容。

1.2.4（可选）配置日志 ID 过滤功能

二进制日志提供了对于特定日志进行过滤的功能。

1.2.5（可选）配置生成数据字典的功能

当用户需要对日志服务器的日志进行解析时，需要使用数据字典生成完整的日志形式。

1.2.6（可选）配置海量日志抑制功能

用户可以通过手工配置所有日志的阈值。

1.2.7（可选）配置连续重复日志的统计输出功能

使能统计输出功能可以避免信息中心受到连续重复日志的冲击，保证业务正常运行。

1.2.8 配置日志信息输出到日志缓冲区

缺省情况从 channel4 向日志缓冲区输出信息，日志缓冲区的大小为 512 条。

1.2.9 配置日志信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析日志，为故障定位提供依据。

1.2.10 配置日志信息输出到控制台

通过配置日志信息输出到控制台，用户可以在控制台上查看到日志信息，了解到设备的运行情况。

1.2.11 配置日志信息输出到终端

通过配置日志信息输出到终端，用户可以在终端上查看到日志信息，了解到设备的运行情况。

1.2.12 配置日志信息输出到日志主机

通过配置日志信息输出到日志主机，用户可以在日志主机中查看到日志信息，了解到设备的运行情况。

1.2.13 配置日志信息输出到 CF 卡

用户可以配置日志信息输出到 CF 卡中，以保存或转移日志文件。

1.2.14 检查配置结果

检查信息中心配置结果。

1.2.1 建立配置任务

在配置日志信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

系统会通过日志的形式实时记录设备运行时出现的各种情况。日志信息可以输出到日志缓冲区、日志文件、控制台、终端屏幕、日志主机中以备存储和查阅。当遇到问题，需要了解设备在运行过程中发生的情况时，用户可以通过查询日志信息，为故障定位提供依据。

前置任务

在配置日志信息的输出之前，需完成以下任务：

- 路由器和日志主机连接正常
- 路由器和日志主机路由可达
- 配置 VPN 实例

数据准备

在配置日志信息输出之前，需准备以下数据：

序号	数据
1	● 信息通道号 channel-number ● 信息通道名 channel-name
2	模块名 module-name
3	日志主机地址
4	日志信息的级别 level
5	（可选）日志缓冲区的容量 size
6	（可选）VPN 实例名

1.2.2 （可选）开启信息中心

信息中心缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

背景信息

信息中心开启时，由于需要对信息进行分类、输出，尤其是待处理信息较多时，对系统性能有一定的影响。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心。

缺省情况下，信息中心处于开启状态。

----结束

1.2.3 （可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道需要输出的内容。

背景信息

在配置信息中心的路由器上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel channel-number name channel-name**，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

----结束

1.2.4 （可选）配置日志 ID 过滤功能

二进制日志提供了对于特定日志进行过滤的功能。

背景信息

二进制日志提供了对于特定日志进行过滤的功能，当用户需要过滤掉部分日志信息时，用户从日志解析工具中得到此部分日志对应的日志 ID。

配置过滤功能后，信息中心对此类信息就不进行发送处理，信息中心的各个输出方向上都无法获得此日志信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center filter-id { id } &<1-50>**，添加一个或多个 ID，ID 中间用空格隔开。



说明

目前只支持对 50 个不同的 ID 进行屏蔽，被屏蔽的 ID 集合称为 ID 过滤列表。ID 过滤列表根据 ID 的大小进行排列。

----结束

1.2.5 （可选）配置生成数据字典的功能

当用户需要对日志服务器的日志进行解析时，需要使用数据字典生成完整的日志形式。

背景信息

二进制日志文件根据数据字典将二进制日志还原为文本格式日志，所以数据字典是二进制日志文件用工具解析的基础。数据字典为日志 ID 以及日志级别、助记符、日志格式串等固定的信息的一个集合。生成数据字典主要供外部解析工具进行下载解析之用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center create-logbook { ftp ftp-address user-name user-name password password [file-name file-name | port-id port-number] * }**，生成数据字典命令。

----结束

1.2.6 （可选）配置海量日志抑制功能

用户可以通过手工配置所有日志的阈值。

背景信息

设备运行过程中，当连续产生具有相同日志 ID 的大量日志时，对信息中心的处理造成冲击，会影响其他日志的记录，严重时可能对运行业务带来影响。信息中心以单条日志为单位进行日志的流量监控，当监控周期内日志的流量持续超过阈值时，对该日志进行抑制，每秒内只处理阈值条日志，超过阈值的日志丢弃；当日志发送流量降低到阈值以下，经过 5 倍监控周期后，解除对日志的抑制。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center rate-limit threshold value [byinfoID infoID | bymodule-alias modname alias]**，设置信息中心每秒处理单条日志的阈值。

信息中心日志缺省采用统一阈值（30 条每秒），但是个别日志根据其使用场景选取的缺省值会高于 50 条。但是用户可以通过手工配置所有日志的阈值。



说明

- 如果阈值设置过小可能导致一些日志丢失
- 如果阈值设置过大可能导致信息中心不能分离出海量日志

----结束

1.2.7 （可选）配置连续重复日志的统计输出功能

使能统计输出功能可以避免信息中心受到连续重复日志的冲击，保证业务正常运行。

背景信息

在 HUAWEI NetEngine20E-X6 系统中，日志的触发由各个业务模块的处理流程控制，触发的信息量也在业务模块的流程中控制，信息中心负责对接收到的信息进行处理。

但是如 ARP、VRRP 等业务模块在某些场景下会短时间产生大量重复日志，这时可以使能连续重复日志的统计输出功能，避免信息中心受到冲击而影响其他日志的记录。

 说明

只有日志 ID 和全部参数完全相同，且中间无其它日志的两条日志，才可判定为连续重复日志。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center statistic-suppress enable**，使能连续重复日志的统计输出功能。

 说明

缺省情况下，连续重复日志的统计输出功能是使能的。

----结束

1.2.8 配置日志信息输出到日志缓冲区

缺省情况从 channel4 向日志缓冲区输出信息，日志缓冲区的大小为 512 条。

操作步骤

步骤 1 配置向通道中输出的日志信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source { module-name | default } channel { channel-number | channel-name } [log { state { off | on } | level severity } *]**，向信息通道中添加日志信息。

步骤 2 配置日志信息输出的通道

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center logbuffer [channel { channel-number | channel-name }]**，配置日志信息输出到日志缓存区所使用的通道。
3. （可选）执行命令 **info-center logbuffer [channel { channel-number | channel-name } | size buffersize] ***，配置日志缓冲区的容量。

缺省情况从 channel4 向日志缓冲区输出信息，日志缓冲区的大小为 512 条。

----结束

1.2.9 配置日志信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析日志，为故障定位提供依据。

操作步骤

步骤 1 配置向通道中输出的日志信息

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level severity** } *], 向信息通道中添加日志信息。

步骤 2 配置日志信息输出的通道

1. 执行命令 **info-center logfile channel** { *channel-number* | *channel-name* }, 配置向日志文件输出信息的通道。

步骤 3 (可选) 配置信息中心输出日志文件的大小

1. 执行命令 **info-center logfile size** *size* 命令, 配置日志文件的大小。

缺省情况下, 日志文件的大小为 8M。

----结束

1.2.10 配置日志信息输出到控制台

通过配置日志信息输出到控制台, 用户可以在控制台上查看到日志信息, 了解到设备的运行情况。

操作步骤

步骤 1 配置向通道中输出的日志信息

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level severity** } *], 向信息通道中添加 Log 信息。

步骤 2 配置日志信息输出的通道

1. 执行命令 **info-center console channel** { *channel-number* | *channel-name* }, 配置日志信息输出到控制台所使用的通道。
2. 执行命令 **quit**, 退回到用户视图。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**, 打开终端显示信息功能。
2. 执行命令 **terminal logging**, 打开终端显示日志信息功能。

----结束

1.2.11 配置日志信息输出到终端

通过配置日志信息输出到终端, 用户可以在终端上查看到日志信息, 了解到设备的运行情况。

操作步骤

步骤 1 配置向通道中输出的日志信息

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level severity** } *], 向信息通道中添加日志信息。

步骤 2 配置日志信息输出的通道

1. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置日志信息输出到终端所使用的通道。
2. 执行命令 **quit**，退回到用户视图。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**，使能终端显示信息的功能。
2. 执行命令 **terminal logging**，使能终端显示日志信息的功能。

----结束

1.2.12 配置日志信息输出到日志主机

通过配置日志信息输出到日志主机，用户可以在日志主机中查看到日志信息，了解到设备的运行情况。

操作步骤

步骤 1 配置向通道中输出的日志信息

1. 在配置信息中心的路由器上，执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加日志信息。

步骤 2 配置日志信息输出的通道

- 在 IPv4 网络中，执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置日志信息输出到日志主机所使用的通道。
缺省情况下，不向日志主机输出日志信息。
系统最多可配置 8 个日志主机，实现日志主机间相互备份的功能。
- 在 IPv6 网络中，执行命令 **info-center loghost ipv6** *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] }] *，配置日志信息输出到日志主机所使用的通道。
缺省情况下，不向日志主机输出日志信息。
系统最多可配置 8 个日志主机，实现日志主机间相互备份的功能。

----结束

1.2.13 配置日志信息输出到 CF 卡

用户可以配置日志信息输出到 CF 卡中，以保存或转移日志文件。

背景信息

在配置信息中心的路由器上进行下面的配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **set logfile-path slot slot-id { cfcard | cfcard2 }**，配置日志信息输出到指定的 CF 卡。

对于配有两块 CF 卡的主控板，日志缺省保存位置为 cfcard2:/log/；对于只有一块 CF 卡的主控板，日志缺省保存位置为 cfcard:/log/。

----结束

1.2.14 检查配置结果

检查信息中心配置结果。

前提条件

已经完成日志信息输出功能的所有配置。

操作步骤

- 使用命令 **display channel [channel-number | channel-name]**，查看通道配置的内容。
- 使用命令 **display info-center [statistics]**，查看信息中心记录的信息。
- 使用命令 **display logbuffer [level severity | size value | slot slot-id] ***，查看日志缓冲区记录的日志信息。
- 使用命令 **display info-center filter-id id**，查看单条日志 ID 的添加结果。
- 使用命令 **display info-center filter-id**，查看所有过滤日志 ID 的添加结果。
- 使用命令 **display info-center rate-limit threshold**，查看信息中心日志速率抑制的阈值。
- 使用命令 **display info-center rate-limit record**，查看信息中心日志速率抑制情况。

----结束

任务示例

执行命令 **display channel [channel-number | channel-name]** 显示信息通道的内容。

```
<HUAWEI> display channel
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      Y        debugging    Y        debugging

channel number:1, channel name:monitor
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      Y        debugging    Y        debugging
416c0000 BFD      Y        debugging    Y        debugging    Y        debugging

channel number:2, channel name:loghost
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        informational Y        debugging    N        debugging

channel number:3, channel name:trapbuffer
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  N        informational Y        warning      N        debugging

channel number:4, channel name:logbuffer
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      N        debugging    N        debugging

channel number:5, channel name:snmpagent
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  N        debugging    Y        warning      N        debugging
```

```
channel number:6, channel name:channel6
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y       debugging   Y       debugging   N       debugging

channel number:7, channel name:channel7
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y       debugging   Y       debugging   N       debugging

channel number:8, channel name:channel8
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y       debugging   Y       debugging   N       debugging

channel number:9, channel name:channel9
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y       debugging   Y       debugging   N       debugging
```

执行命令 **display info-center** 显示信息中心记录的信息。

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
    100.1.1.1, channel number 2, channel name loghost,
    language english , host facility local5

Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 9, channel number : 3, channel name : trapbuffer
    dropped messages 0, overwritten messages 0
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
    current messages 32, channel number:3, channel name:trapbuffer
    dropped messages 0, overwritten messages 0
logfile:
    channel number : 9, channel name : channel9, language : english
Information timestamp setting:
    log - date, trap - date, debug - boot
Sent messages = 2646, Received messages = 10395
IO Reg messages = 160 IO Sent messages = 7750
```

执行命令 **display logbuffer [level severity | size value | slot slot-id] ***显示日志缓冲区中记录的日志信息。

```
<HUAWEI> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 1
Feb 13 2007 20:05:46.523.1 HUAWEI %%01SHELL/4/CMDRECORD(1):task:vt0 ip:100.1.1.48 user:**
command:info-center timestamp log date precision-time millisecond
```

执行命令 **display info-center filter-id [id]**，查看过滤表中 ID 为 1098649600 的添加结果。

```
<HUAWEI> display info-center filter-id 1098649600
ID          : 1098649600
Module      : TE_TUNNEL
Alias       : NOTIFY_LSPM_FAIL
Content     : LSPM return error to TE when processing tunnel commit event! (TunnelName=[STRING],
ErrorCode=[ULONG])
Filtered Number : 0
```

执行命令 **display info-center filter-id**，查看过滤表中所有过滤 ID 所添加的结果。

```
<HUAWEI> display info-center filter-id
ID                : 1077481488
Module            : SHELL
Alias              : AUTHCMDSNDMSGFAIL
Content           : [string]
Filtered Number   : 0

ID                : 1079676930
Module            : VTY
Alias              : AUTHTIMEOUT
Content           : Refresh route to slot [ULONG].
Filtered Number   : 0
```

执行命令 **display info-center rate-limit threshold**，查看信息中心日志速率抑制的阈值。

```
<HUAWEI> display info-center rate-limit threshold
Rate limit threshold(per second):
Module      Alias                Default  Config
default     default                  50       50
SHELL       CMDRECORD                 4294967295 4294967295
SHELL       DISPLAY_CMDRECORD         4294967295 4294967295
SHELL       HIDECD                   4294967295 4294967295
SHELL       DISPLAY_HIDECD          4294967295 4294967295
TE_TUNNEL   NOTIFY_LSPM_FAIL         50       100
```

执行命令 **display info-center rate-limit record**，查看信息中心日志速率抑制情况。

```
<HUAWEI> display info-center rate-limit record
Record No. 1
InfoID          : 1098731520
Module          : 6OVER4
Alias            : DESTFAIL
Rate limit threshold : 50
Total receive number : 1872
Total drop number   : 922
Total send number   : 950
Begin timestamp    : 2009-12-21 11:41:28
Record No. 2
InfoID          : 1098731521
Module          : 6OVER4
Alias            : SRCFAIL
Rate limit threshold : 50
Total receive number : 1872
Total drop number   : 922
Total send number   : 950
Begin timestamp    : 2009-12-21 11:41:28
```

1.3 配置告警信息的输出

配置告警信息的输出可以配置指定模块的告警信息输出到日志文件、控制台、终端和 SNMP 代理中。

1.3.1 建立配置任务

在配置告警信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

1.3.2 （可选）开启信息中心

信息中心缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

1.3.3 （可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道输出的内容。

1.3.4 配置告警信息输出到告警缓冲区

告警信息缺省情况是向告警缓冲区中发送的，并且有缺省的通道，通过配置可以指定告警信息从其他的通道发送。

1.3.5 配置告警信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析其中的告警信息，为故障定位提供依据。

1.3.6 配置告警信息输出到控制台

通过配置告警信息输出到控制台，用户可以在控制台上查看到告警信息，了解到设备的运行情况。

1.3.7 配置告警信息输出到终端

通过配置告警信息输出到终端，用户可以在终端上查看到告警信息，了解到设备的运行情况。

1.3.8 配置告警信息输出到 SNMP 代理

通过配置告警信息输出到 SNMP 代理，用户可以在网管上查看到告警信息，了解到设备的运行情况。

1.3.9 检查配置结果

完成告警信息输出的配置后，应使用相关命令确认配置结果正确。

1.3.1 建立配置任务

在配置告警信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

设备在遇到需要相关管理人员关注的情况时，会产生告警信息。告警信息会发送到告警缓冲区、日志文件、控制台、终端和网管端。管理人员通过查询相关告警信息，进行故障定位和对故障进行及时处理故障。

前置任务

在配置告警信息输出之前，需完成以下任务：

- 路由器和网管站接正常
- 路由器和网管站路由可达

数据准备

在配置告警信息输出之前，需准备以下数据：

序号	数据
1	● 信息通道号 channel-number ● 信息通道名 channel-name
2	模块名 module-name
3	告警信息的级别 level
4	（可选）告警缓冲区的容量

序号	数据
5	网管端地址

1.3.2 （可选）开启信息中心

信息中心缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

背景信息

在配置信息中心的路由器上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心。

缺省情况下，信息中心处于开启状态。

信息中心开启时，由于需要对信息进行分类、输出，尤其是待处理信息较多时，对系统性能有一定的影响。

----结束

1.3.3 （可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道输出的内容。

背景信息

在配置信息中心的路由器上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel channel-number name channel-name**，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

----结束

1.3.4 配置告警信息输出到告警缓冲区

告警信息缺省情况是向告警缓冲区中发送的，并且有缺省的通道，通过配置可以指定告警信息从其他的通道发送。

背景信息

在配置信息中心的路由器上进行以下的配置。

操作步骤

步骤 1 配置向通道中输出的告警信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**trap** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加告警信息。

缺省情况下，告警信息的时间戳格式为 **date**。

步骤 2 配置告警信息输出的通道

1. 执行命令 **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* }]，配置向告警缓冲区输出信息。
2. （可选）执行命令 **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size buffersize**] *，配置向告警缓冲区输出信息的所使用的通道。

缺省情况下，从 **channel3** 向告警缓冲区输出信息。告警缓冲区可以容纳 256 条信息。

----结束

1.3.5 配置告警信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析其中的告警信息，为故障定位提供依据。

背景信息

在配置信息中心的路由器上进行以下的配置。

操作步骤

步骤 1 配置向通道输出的告警信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**trap** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加告警信息。

缺省情况下，告警信息的时间戳格式为 **date**。

步骤 2 配置告警信息输出的通道

1. 执行命令 **info-center logfile channel** { *channel-number* | *channel-name* }，配置向日志文件输出告警信息的所使用的通道。

缺省情况下，从 **channel9** 输出到日志文件。

步骤 3 （可选）配置信息中心输出日志文件的大小

1. 执行命令 **info-center logfile size size** 命令，配置日志文件的大小。

缺省情况下，日志文件的大小为 8M。

----结束

1.3.6 配置告警信息输出到控制台

通过配置告警信息输出到控制台，用户可以在控制台上查看到告警信息，了解到设备的运行情况。

背景信息

在配置信息中心的路由器上进行以下的配置。

操作步骤

步骤 1 配置向通道输出的告警信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**trap** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加告警信息。

缺省情况下日志信息的时间戳格式为 **date**。

步骤 2 配置告警信息输出的通道

1. 执行命令 **info-center console channel** { *channel-number* | *channel-name* }，配置向控制台输出告警信息所使用的通道。

缺省情况下从 **channel0** 向控制台输出信息。

2. 执行命令 **quit**，退回到用户视图。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**，使能终端显示信息的功能。
2. 执行命令 **terminal trapping**，使能终端显示告警信息。

----结束

1.3.7 配置告警信息输出到终端

通过配置告警信息输出到终端，用户可以在终端上查看到告警信息，了解到设备的运行情况。

背景信息

在配置信息中心的路由器上进行以下的配置。

操作步骤

步骤 1 配置向通道输出的告警信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**trap** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加告警信息。

缺省情况下，告警信息的时间戳格式为 **date**。

步骤 2 配置告警信息输出的通道

1. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }, 配置向 VTY 终端输出信息所使用的通道。
缺省情况下, 从 channel1 向终端输出信息。
2. 执行命令 **quit**, 退回到用户视图。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**, 使能终端显示信息的功能。
2. 执行命令 **terminal trapping**, 使能终端显示 Trap 信息。

----结束

1.3.8 配置告警信息输出到 SNMP 代理

通过配置告警信息输出到 SNMP 代理, 用户可以在网管上查看到告警信息, 了解到设备的运行情况。

背景信息

在配置信息中心的路由器上进行如下的配置。

操作步骤

步骤 1 配置向通道中输出的告警信息

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**trap** { **state** { **off** | **on** } | **level severity** } *], 向信息通道中添加告警信息。
缺省情况下, 告警信息的时间戳格式为 date。

步骤 2 配置告警信息输出的通道

1. 执行命令 **info-center snmp channel** { *channel-number* | *channel-name* }, 配置告警信息输出到 SNMP 代理所使用的通道。
2. 执行命令 **snmp-agent**, 启动 SNMP 代理功能。
缺省情况下, 从 channel5 向 SNMP 代理输出信息。

----结束

1.3.9 检查配置结果

完成告警信息输出的配置后, 应使用相关命令确认配置结果正确。

前提条件

已经完成告警信息输出功能的所有配置。

操作步骤

- 执行 **display channel** [*channel-number* | *channel-name*] 命令查看通道配置的内容。
- 执行 **display info-center** [**statistics**] 命令查看信息中心记录的信息。

- 执行 **display trapbuffer** [size value]命令查看告警缓冲区记录的信息。

----结束

任务示例

执行命令 **display channel** 显示信息通道的内容。

```
<HUAWEI> display channel
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      Y        debugging  Y        debugging

channel number:1, channel name:monitor
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      Y        debugging  Y        debugging
416c0000 BFD      Y        debugging   Y        debugging  Y        debugging

channel number:2, channel name:loghost
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        informational Y        debugging  N        debugging

channel number:3, channel name:trapbuffer
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  N        informational Y        warning      N        debugging

channel number:4, channel name:logbuffer
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        warning      N        debugging  N        debugging

channel number:5, channel name:snmpagent
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  N        debugging   Y        warning      N        debugging

channel number:6, channel name:channel6
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        debugging   Y        debugging  N        debugging

channel number:7, channel name:channel7
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        debugging   Y        debugging  N        debugging

channel number:8, channel name:channel8
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        debugging   Y        debugging  N        debugging

channel number:9, channel name:channel9
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y        debugging   Y        debugging  N        debugging
```

执行命令 **display info-center** 显示信息中心记录的信息。

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
current messages 92, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 0
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
```

```
current messages 30, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
logfile:
    channel number : 9, channel name : channel9, language : english
Information timestamp setting:
    log - date, trap - date, debug - boot
Sent messages = 425, Received messages = 634
IO Reg messages = 160 IO Sent messages = 210
```

执行命令 **display trapbuffer** 显示告警缓冲区中记录的告警信息。

```
<HUAWEI> display trapbuffer
Trapping Buffer Configuration and contents:enabled
allowed max buffer size : 1024

actual buffer size : 256
channel number : 3 , channel name : trapbuffer
dropped messages : 0
overwritten messages : 0
current messages : 250
#May 12 2009 22:43:10 HUAWEI IFNET/4/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Interface
201326849 turned into UP state.
```

1.4 配置调试信息的输出

配置调试信息的输出可以配置指定模块的调试信息输出到日志文件、控制台、终端和日志主机中。

背景信息



注意

调试会对系统的运行造成影响，因此，在调试之后，要立即执行 **undo debugging all** 命令去使能调试。当 CPU 的使用率接近 100% 时，调试 ARP 可能会引起主板重启，因此，在使用调试命令前一定要谨慎操作。

1.4.1 建立配置任务

在配置调试信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

1.4.2 （可选）开启信息中心

信息中缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

1.4.3 （可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道需要输出的内容。

1.4.4 配置调试信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析其中的调试信息，为故障定位提供依据。

1.4.5 配置调试信息输出到控制台

当使用控制台登录设备时，可以将调试信息输出到控制台，便于实时了解调试信息。

1.4.6 配置调试信息输出到终端

当使用终端登录设备时，可以将调试信息输出到终端，便于实时了解调试信息。

1.4.7 配置调试信息输出到日志主机

通过配置调试信息输出到日志主机，方便用户查看调试信息。

1.4.8 检查配置结果

配置信息中心输出调试信息的功能成功后，用户可以查看到信息中心的配置情况。

1.4.1 建立配置任务

在配置调试信息的输出前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在设备遇到故障，需要对设备的运行情况进行分析，可以通过信息中心输出的 debug 信息，为故障定位提供依据。

前置任务

在配置调试信息输出功能之前，需完成以下任务：

- 路由器和 PC 连接正常
- 路由器和 PC 路由可达

数据准备

在配置调试输出之前，需准备以下数据：

序号	数据
1	● 信息通道号 channel-number ● 信息通道名 channel-name
2	模块名 module-name
3	调试信息的级别 level
4	PC 地址

1.4.2 （可选）开启信息中心

信息中缺省情况是开启的，如果信息中心处于未开启状态，可以通过此步骤来开启信息中心功能。

背景信息

信息中心开启时，由于需要对信息进行分类、输出，尤其是待处理信息较多时，对系统性能有一定的影响。

在配置信息中心的路由器上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center enable**，开启信息中心。

缺省情况下，信息中心处于开启状态。

----结束

1.4.3 （可选）命名信息通道

通过命名通道名，可以使用户清楚的知道每一个通道需要输出的内容。

背景信息

在配置信息中心的路由器上进行下面的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **info-center channel channel-number name channel-name**，将编号为 *channel-number* 的信息通道命名为 *channel-name*。

----结束

1.4.4 配置调试信息输出到日志文件

在设备遇到问题时，从设备中导出日志文件，通过分析其中的调试信息，为故障定位提供依据。

背景信息

在配置信息中心的路由器上，进行以下的配置。

操作步骤

步骤 1 配置向通道输出的信息调试信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source { module-name | default } channel { channel-number | channel-name } [debug { state { off | on } | level severity } *]**，向信息通道中添加调试信息。

缺省情况下日志信息的时间戳格式为 **date**，精度为毫秒。

步骤 2 配置调试信息输出的通道

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center logfile channel { channel-number | channel-name }**，配置调试信息输出到日志文件的通道。

步骤 3 （可选）配置信息中心输出日志文件的大小

1. 执行命令 **info-center logfile size size** 命令，配置日志文件的大小。

缺省情况下，调试信息将不会被保存在日志文件中。如果需要保存调试信息到日志文件，可以执行命令 **info-center source default channel 9 debug state on level severity**，向信息通道中添加记录。

----结束

1.4.5 配置调试信息输出到控制台

当使用控制台登录设备时，可以将调试信息输出到控制台，便于实时了解调试信息。

背景信息

在配置信息中心的路由器上，进行以下的配置。

操作步骤

步骤 1 配置向通道输出的信息调试信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source { module-name | default } channel { channel-number | channel-name } [debug { state { off | on } | level severity } *]**，向信息通道中添加调试信息。

缺省情况下日志信息的时间戳格式为 **date**，精度为毫秒。

步骤 2 配置调试信息输出的通道

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center console channel { channel-number | channel-name }**，配置向控制台输出调试信息的通道。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**，使能终端显示信息的功能。
2. 执行命令 **terminal debugging**，使能终端显示调试信息。

----结束

1.4.6 配置调试信息输出到终端

当使用终端登录设备时，可以将调试信息输出到终端，便于实时了解调试信息。

背景信息

在配置信息中心的路由器上，进行以下的配置。

操作步骤

步骤 1 配置向通道输出的信息调试信息

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source { module-name | default } channel { channel-number | channel-name } [debug { state { off | on } | level severity } *]**，向信息通道中添加调试信息。

缺省情况下日志信息的时间戳格式为 **date**，精度为毫秒。

步骤 2 配置调试信息输出的通道

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center monitor channel** { *channel-number* | *channel-name* }，配置向终端输出调试信息所使用的通道。
3. 执行命令 **quit**，退回到用户视图。

步骤 3 配置终端显示功能

1. 执行命令 **terminal monitor**，使能终端显示信息的功能。
2. 执行命令 **terminal debugging**，使能终端显示调试信息。

----结束

1.4.7 配置调试信息输出到日志主机

通过配置调试信息输出到日志主机，方便用户查看调试信息。

操作步骤

步骤 1 配置向通道输出的信息调试信息

1. 在配置信息中心的路由器上，执行命令 **system-view**，进入系统视图。
2. 执行命令 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **state** { **off** | **on** } | **level severity** } *]，向信息通道中添加调试信息。

步骤 2 配置调试信息输出的通道

- 在 IPv4 网络中，执行命令 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置向日志主机输出信息所使用的通道。

缺省情况下，不向日志主机输出调试信息。

系统最多可配置 8 个日志主机，实现日志主机间相互备份的功能。

- 在 IPv6 网络中，执行命令 **info-center loghost ipv6** *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] }] *，配置向日志主机输出信息所使用的通道。

缺省情况下，不向日志主机输出调试信息。

系统最多可配置 8 个日志主机，实现日志主机间相互备份的功能。

----结束

1.4.8 检查配置结果

配置信息中心输出调试信息的功能成功后，用户可以查看到信息中心的配置情况。

前提条件

已经完成调试信息输出功能的所有配置。

操作步骤

- 执行 **display channel** [*channel-number* | *channel-name*] 命令查看通道配置的内容。

- 执行 **display info-center [statistics]** 命令查看信息中心记录的信息。

----结束

任务示例

执行 **display channel** 命令显示配置的通道信息。

```
<HUAWEI> display channel 0
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning      Y      debugging  Y      debugging
416e0000 ARP       Y      warning      Y      debugging  Y      debugging
```

执行 **display info-center** 命令显示信息中心的配置信息。

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
current messages 512, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 411
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
current messages 256, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 12
logfile:
    channel number : 9, channel name : channel9, language : English
Information timestamp setting:
    log - date, trap - date, debug - boot

Sent messages = 7922, Received messages = 22927

IO Reg messages = 92 IO Sent messages = 15006
```

1.5 维护信息中心

当确认信息中心中的缓冲信息需要删除时，可以执行命令 **reset info-center statistics**、**reset logbuffer** 和 **reset trapbuffer** 进行清除。执行清除命令后，信息将无法恢复。

背景信息



注意

清除信息中心的统计信息后，以前的统计信息将无法恢复，请务必仔细确认。

操作步骤

- 在确认需要清除信息中心的统计信息后，请在用户视图下执行命令 **reset info-center statistics**。

- 在确认需要清除日志缓存区的统计信息后，请在用户视图下执行命令 **reset logbuffer**。
- 在确认需要清除告警缓冲区的统计信息后，请在用户视图下执行命令 **reset trapbuffer**。

----结束

1.6 信息中心配置举例

以示例方式介绍信息中心的配置。

1.6.1 配置向日志文件输出日志信息示例

配置指定模块的、指定级别的日志信息输出到日志文件中。维护人员可以通过查询日志信息，了解到设备的运行情况，在设备出现故障时，进行故障定位。

1.6.2 配置向日志主机输出日志信息示例

配置不同模块和级别的日志分别输出到不同的日志主机中，同时配置备份日志主机，实现对日志信息的备份。

1.6.3 配置使用管理 VPN 实例时向公网日志主机输出日志信息示例

配置不同类型和严重级别的日志信息，从信息中心发送到不同日志主机中。

1.6.4 配置向日志主机发送二进制日志

配置二进制日志发送到日志主机。由于发送的日志信息是二进制的形式，可以有效的减少日志发送给网络造成的负担。

1.6.5 配置向 SNMP Agent 输出告警信息示例

配置向 SNMP Agent 输出告警信息后，网管可以接收到设备发送的告警信息。

1.6.6 配置向控制台输出调试信息示例

在配置向控制台输出调试信息后，在设备遇到问题时，可以通过控制台登录设备执行调试命令，查看调试信息。

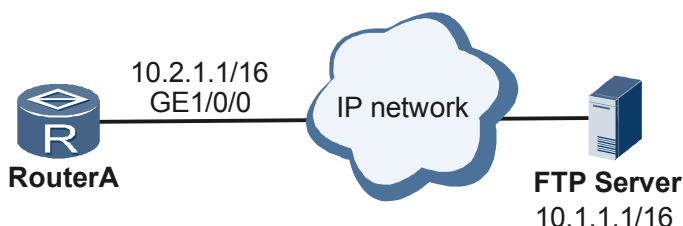
1.6.1 配置向日志文件输出日志信息示例

配置指定模块的、指定级别的日志信息输出到日志文件中。维护人员可以通过查询日志信息，了解到设备的运行情况，在设备出现故障时，进行故障定位。

组网需求

如图 1-4 所示，RouterA 中日志文件传送到 FTP Server。维护人员可以通过查询日志信息，了解到 RouterA 的运行情况，在 RouterA 出现故障时，进行故障定位。

图 1-4 配置向日志文件输出日志信息组网图



配置思路

采用如下思路进行本例的配置：

1. 开启信息中心。
2. 配置日志信息输出的内容。
3. 配置日志信息输出的通道。
4. 配置日志文件发送到 FTP Server。

数据准备

为完成此配置例，需准备如下的数据：

- 配置各接口的 IP 地址
- 信息通道号
- 允许日志输出的模块
- 信息的严重级别
- 日志信息输出语言
- FTP Server 地址
- FTP Server 用户名和密码

操作步骤

步骤 1 配置路由协议，使路由器和日志服务器之间有可达路由（略）

步骤 2 配置日志信息输出的通道

开启信息中心。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] info-center enable
```

步骤 3 配置通道输出的日志信息

配置通道允许输出日志信息的模块和严重级别。

```
[RouterA] info-center source ip channel channel19 log level warnings
```

步骤 4 配置日志信息输出的通道

配置日志信息输出到日志文件所使用的通道。

```
[RouterA] info-center logfile channel channel19
[RouterA] quit
```

步骤 5 配置日志文件传输到 FTP Server

配置登录到 FTP Server。

```
<RouterA> ftp 10.1.1.1
```

配置将传输日志文件到 FTP Server。

```
[RouterA-ftp] put 2007_07.log
[RouterA-ftp] quit
<RouterA>
```

步骤 6 验证配置结果

查看通道输出的日志文件通道信息。

```
<RouterA> display info-center
Information Center:enabled
logfile:
channel number : 9, channel name : channel9, language : english
Information timestamp setting:
log - date, trap - date, debug - boot
Sent messages = 5753, Received messages = 5866
IO Reg messages = 124 IO Sent messages = 114
```

在 FTP 服务器端查看传送到的日志文件。（略）

----结束

配置文件

```
#
sysname RouterA
#
info-center source IP channel 9 log level warnings
info-center logfile channel 9
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.2.1.1 255.255.0.0
#
ip route-static 10.1.0.0 255.255.0.0 10.2.1.2
#
return
```

1.6.2 配置向日志主机输出日志信息示例

配置不同模块和级别的日志分别输出到不同的日志主机中，同时配置备份日志主机，实现对日志信息的备份。

组网需求

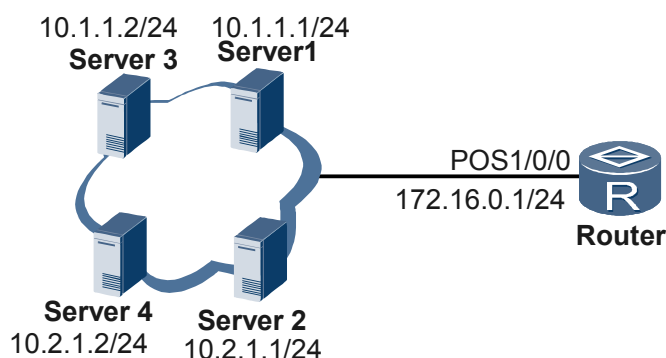
如图 1-5 所示，不同类型和严重级别的日志信息，从信息中心发送到不同日志主机中。

路由器向日志主机 Server1 发送由 FIB 模块和 IP 模块产生、严重等级为 notification 的日志信息；Server3 作为 Server1 的备份路由器。

路由器向日志主机 Server2 发送由 PPP 模块和 AAA 模块产生、严重等级为 warning 的日志信息；Server4 作为 Server2 的备份路由器。

需要在路由器侧和日志主机侧分别进行配置。

图 1-5 配置向日志主机输出信息组网图



配置思路

采用如下思路进行本例的配置：

1. 开启信息中心功能。
2. 命名通道名。
3. 配置允许输出的模块日志信息。
4. 配置日志信息输出的通道。
5. 配置发送日志信息的源接口。
6. 配置日志主机。

数据准备

为完成此配置例，需准备如下的数据：

- 日志主机的 IP 地址
- 信息通道号
- 输出日志的通道名称
- 允许日志输出的模块
- 信息的严重级别
- 日志信息输出语言

操作步骤

步骤 1 配置 IP 地址和路由协议，使路由器和日志服务器之间有可达路由（略）

步骤 2 开启信息中心

开启信息中心。

```
<HUAWEI> system-view  
[HUAWEI] info-center enable
```

步骤 3 命名通道名

为输出日志的通道命名。

```
[HUAWEI] info-center channel 6 name loghost1
```

步骤 4 配置日志信息输出的通道

配置通道允许输出日志信息的模块和严重级别。

```
[HUAWEI] info-center source fib channel loghost log level notifications  
[HUAWEI] info-center source ip channel loghost log level notifications  
[HUAWEI] info-center source ppp channel loghost1 log level warnings  
[HUAWEI] info-center source aaa channel loghost1 log level warnings
```

步骤 5 配置发送日志信息的源接口

配置发送日志信息的源接口。

```
[HUAWEI] info-center loghost source pos1/0/0
```

步骤 6 配置日志信息输出到指定的日志主机

指定 Server1 作为日志服务器、Server3 作为备份日志服务器，接收模块为 FIB 和 IP 的日志信息，输出语言为英文，使用日志记录工具为 Local2。

```
[HUAWEI] info-center loghost 10.1.1.1 channel loghost facility local2 language english
[HUAWEI] info-center loghost 10.1.1.3 channel loghost facility local2 language english
```

指定 Server2 作为日志服务器、Server4 作为备份日志服务器，接收模块为 PPP 和 AAA 的日志信息，输出语言为英文，使用日志记录工具为 Local4。

```
[HUAWEI] info-center loghost 10.2.1.2 channel loghost1 facility local4 language english
[HUAWEI] info-center loghost 10.2.1.4 channel loghost1 facility local4 language english
```

步骤 7 配置日志服务器

路由器会产生大量的日志信息，而路由器本身的存储空间相对有限，就需要配置日志服务器实现对设备日志的收集。

日志服务器可以是安装 UNIX 或 LINUX 操作系统的主机，也可以是安装第三方日志软件的主机。

在安装 UNIX 或 LINUX 的操作系统的主机中，可以通过在系统中启用 Syslog 后，通过 Syslog 机制在主机中记录设备的日志信息，实现日志信息的收集功能。

以安装 LINUX 系统主机为例，进行配置举例：

- 建立日志文件，在/var/log 目录中通过使用 **touch loghost.info** 命令，建立记录路由器信息的 loghost.info 文件。
- 编辑配置文件，编辑 etc/syslog.conf 内容为：loghost.info /var/log/router.log，表示主机名称为 loghost，把信息等级为 info 的日志记录到系统下的/var/log/loghost.log 中。
- 配置 etc/sysconfig/syslog 文件，将 syslogd_options="-m o"修改为：syslogd_option="-l -m o"，使系统可以记录远端设备的日志。
- 启动 Syslog 服务，使用命令 **service syslog restart** 来启动 Syslog 服务。

在安装第三方日志软件的主机中，可以通过在第三方软件中进行配置，实现对日志的收集功能。如华为网管软件 HUAWEI iManager N2000，此软件中有设备日志管理的功能，可以实现对设备发送的 Syslog 报文信息进行接收、过滤、存储、转发、动作触发。

在华为网管软件 HUAWEI iManager N2000 上配置日志服务的过程，请参见《HUAWEI iManager N2000 DMS-组合包 用户手册 第一分册》。

步骤 8 检测配置结果

查看已经配置的日志主机。

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
the interface name of the source address:pos1/0/0
    10.1.1.1, channel number 2, channel name loghost,
                                   language english , host facility local2
    10.1.1.3, channel number 2, channel name loghost,
                                   language english , host facility local2
    10.2.1.2, channel number 6, channel name loghost1
                                   language english , host facility local4
    10.2.1.4, channel number 6, channel name loghost1
                                   language english , host facility local4
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
```

```

        channel number : 5, channel name : snmpagent
Log buffer:
        enabled,max buffer size 1024, current buffer size 512,
current messages 50, channel number : 4, channel name : logbuffer
dropped messages 13, overwritten messages 3
Trap buffer:
        enabled,max buffer size 1024, current buffer size 256,
current messages 2, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
Information timestamp setting:
        log - date, trap - date, debug - boot

Sent messages = 683, Received messages = 682

IO Reg messages = 0 IO Sent messages = 0

# 在网管端查看接收到的日志信息。（略）

```

----结束

配置文件

```

#
info-center channel 6 name loghost1
info-center source FIB channel loghost channel 2 log level notification
info-center source IP channel 2 log level notification
info-center source PPP channel 6 log level warning
info-center source AAA channel 6 log level warning
info-center loghost source Pos1/0/0
info-center loghost 10.1.1.1 channel loghost facility local2
info-center loghost 10.1.1.3 channel loghost facility local2
info-center loghost 10.2.1.2 channel 6 facility local4
info-center loghost 10.2.1.4 channel 6 facility local4
#interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 172.16.0.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 172.16.0.2
ip route-static 10.2.1.0 255.255.255.0 172.16.0.2
#
return

```

1.6.3 配置使用管理 VPN 实例时向公网日志主机输出日志信息示例

配置不同类型和严重级别的日志信息，从信息中心发送到不同日志主机中。

组网需求

如图 1-6 所示，不同类型和严重级别的日志信息，从信息中心发送到不同日志主机中。

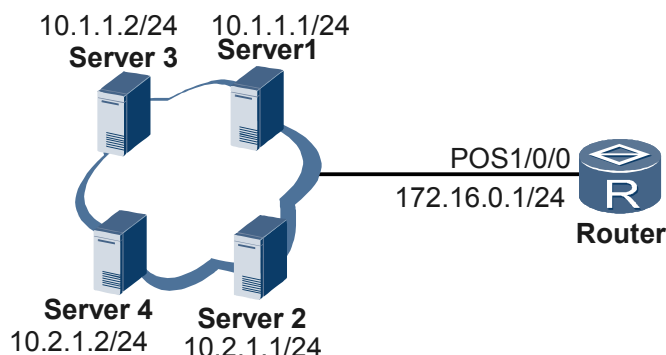
路由器向日志主机 Server1 发送由 FIB 模块和 IP 模块产生、严重等级为 notification 的日志信息；Server3 作为 Server1 的备份日志主机。

路由器向日志主机 Server2 发送由 PPP 模块和 AAA 模块产生、严重等级为 warning 的日志信息；Server4 作为 Server2 的备份日志主机。

需要在路由器侧和日志主机侧分别进行配置。

路由器上配置了管理 VPN 实例。

图 1-6 配置使用管理 VPN 实例时向公网日志主机输出日志信息组网图



配置思路

采用如下思路进行本例的配置：

1. 开启信息中心功能。
2. 命名通道名。
3. 配置允许输出的模块日志信息。
4. 配置日志信息输出的通道。
5. 配置发送日志信息的源接口。
6. 配置日志主机。

数据准备

为完成此配置例，需准备如下的数据：

- 日志主机的 IP 地址
- 信息通道号
- 输出日志的通道名称
- 允许日志输出的模块
- 信息的严重级别
- 日志信息输出语言

操作步骤

步骤 1 配置 IP 地址和路由协议，使路由器和日志服务器之间有可达路由（略）

步骤 2 开启信息中心

开启信息中心。

```
<HUAWEI> system-view  
[HUAWEI] info-center enable
```

步骤 3 命名通道名

为输出日志的通道命名。

```
[HUAWEI] info-center channel 6 name loghost1
```

步骤 4 配置日志信息输出的通道

配置通道允许输出日志信息的模块和严重级别。

```
[HUAWEI] info-center source fib channel loghost log level notifications
[HUAWEI] info-center source ip channel loghost log level notifications
[HUAWEI] info-center source ppp channel loghost1 log level warnings
[HUAWEI] info-center source aaa channel loghost1 log level warnings
```

步骤 5 配置发送日志信息的源接口

配置发送日志信息的源接口。

```
[HUAWEI] info-center loghost source pos1/0/0
```

步骤 6 配置日志信息输出到指定的日志主机

指定 Server1 作为日志服务器、Server3 作为备份日志服务器，接收模块为 FIB 和 IP 的日志信息，输出语言为英文，使用日志记录工具为 Local2。

```
[HUAWEI] info-center loghost 10.1.1.1 public-net facility local2 language english
[HUAWEI] info-center loghost 10.1.1.3 public-net facility local2 language english
```

指定 Server2 作为日志服务器、Server4 作为备份日志服务器，接收模块为 PPP 和 AAA 的日志信息，输出语言为英文，使用日志记录工具为 Local4。

```
[HUAWEI] info-center loghost 10.2.1.2 public-net channel loghost1 facility local4 language english
[HUAWEI] info-center loghost 10.2.1.4 public-net channel loghost1 facility local4 language english
```

步骤 7 配置日志服务器

路由器会产生大量的日志信息，而路由器本身的存储空间相对有限，就需要配置日志服务器实现对设备日志的收集。

日志服务器可以是安装 UNIX 或 LINUX 操作系统的主机，也可以是安装第三方日志软件的主机。

在安装 UNIX 或 LINUX 的操作系统的主机中，可以通过在系统中启用 Syslog 后，通过 Syslog 机制在主机中记录设备的日志信息，实现日志信息的收集功能。

以安装 LINUX 系统主机为例，进行配置举例：

- 建立日志文件，在/var/log 目录中通过使用 **touch loghost.info** 命令，来建立记录路由器信息的 loghost.info 文件。
- 编辑配置文件，编辑 etc/syslog.conf 内容为：loghost.info /var/log/router.log，表示主机名称为 loghost，把信息等级为 info 的日志记录到系统下的/var/log/loghost.log 中。
- 配置 etc/sysconfig/syslog 文件，将 syslogd_options="-m o",修改为：syslogd_option="-l -m o"，使系统可以记录远端设备的日志。
- 启动 Syslog 服务，使用命令 **service syslog restart** 来启动 Syslog 服务。

在安装第三方日志软件的主机中，可以通过在第三方软件中进行配置，实现对日志的收集功能。如华为网管软件 HUAWEI iManager N2000，此软件中有设备日志管理的功能，可以实现对设备发送的 Syslog 报文信息进行接收、过滤、存储、转发、动作触发。

在华为网管软件 HUAWEI iManager N2000 上配置日志服务的过程，请参见《HUAWEI iManager N2000 DMS-组合包 用户手册 第一分册》。

步骤 8 检测配置结果

查看已经配置的日志主机

```
<HUAWEI> display info-center
Information Center:enabled
```



```
Log host:
the interface name of the source address:pos1/0/0
    10.1.1.1, channel number 2, channel name loghost,
        language english , host facility local2
    10.1.1.3, channel number 2, channel name loghost,
        language english , host facility local2
    10.2.1.2, channel number 6, channel name loghost1
        language english , host facility local4
    10.2.1.4, channel number 6, channel name loghost1
        language english , host facility local4

Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
current messages 50, channel number : 4, channel name : logbuffer
dropped messages 13, overwritten messages 3
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
current messages 2, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
Information timestamp setting:
    log - date, trap - date, debug - boot

Sent messages = 683, Received messages = 682

IO Reg messages = 0 IO Sent messages = 0

# 在网管端查看接收到的日志信息。（略）

----结束
```

配置文件

```
#
info-center channel 6 name loghost1
info-center source FIB channel loghost channel 2 log level notification
info-center source IP channel 2 log level notification
info-center source PPP channel 6 log level warning
info-center source AAA channel 6 log level warning
info-center loghost source Pos1/0/0
info-center loghost 10.1.1.1 public-net facility local2
info-center loghost 10.1.1.3 public-net facility local2
info-center loghost 10.2.1.2 public-net channel 6 facility local4
info-center loghost 10.2.1.4 public-net channel 6 facility local4
#interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 172.16.0.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 172.16.0.2
ip route-static 10.2.1.0 255.255.255.0 172.16.0.2
#
return
```

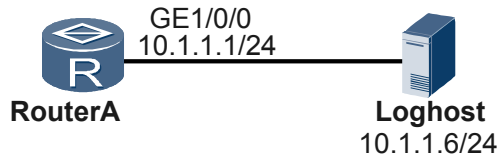
1.6.4 配置向日志主机发送二进制日志

配置二进制日志发送到日志主机。由于发送的日志信息是二进制的形式，可以有效的减少日志发送给网络造成的负担。

组网需求

如图 1-7 所示，RouterA 上产生的二进制日志信息，实时的传送到日志主机中。用户或维护人员通过日志解析工具对日志进行解析，通过查看日志信息，为故障定位提供依据。

图 1-7 配置向日志主机发送二进制日志示例



配置思路

采用如下思路进行本例的配置：

1. 在路由器上开启信息中心功能。
2. 添加一条日志 ID。
3. 生成数据字典并发送到日志服务器。
4. 配置二进制日志发送到日志主机。

数据准备

为完成此配置例，需准备如下的数据：

- 需要过滤的日志 ID
- 生成的数据字典的文件名
- FTP 服务器的 IP 地址
- 登录 FTP 服务器需要的用户名和密码
- 日志主机的 IP 地址

操作步骤

步骤 1 配置 RouterA 和 Loghost 的 IP 地址，并且路由可达（略）。

步骤 2 开启信息系统

开启信息中心。

```
<HUAWEI> system-view
[HUAWEI] info-center enable
```

步骤 3 添加一条日志 ID

配置日志信息输出的通道及模块信息。

```
[HUAWEI] info-center filter-id 1077514264
```

步骤 4 生成数据字典并发送到日志服务器

配置告警信息输出到 SNMP Agent。

```
[HUAWEI] info-center create-logbook ftp 10.1.1.6 user-name ftp password ftp file-name dicx.xml
```

在出现发送数据字典成功的提示信息 “Info: Succeeded in creating a data dictionary.” 后，在日志服务器查看数据字典是否已经传送成功。

步骤 5 配置二进制日志发送到日志主机

```
[HUAWEI] info-center loghost 10.1.1.6 binary
```

步骤 6 验证配置结果

查看添加得日志过滤 ID 信息。

```
[HUAWEI] display info-center filter-id 1077514264
ID: 1077514264
Content: task: [string] ip: [string] user: [string] command: [string]
Filtered Number: 3
```

查看 SNMP 输出信息所使用的通道。

```
[HUAWEI] display info-center
Information Center:enabled
Log host:
10.1.1.1, channel number 2, channel name loghost,
language english , host facility local7, binary
loghost
Console:
channel number : 0, channel name : console
Monitor:
channel number : 1, channel name : monitor
SNMP Agent:
channel number : 5, channel name : snmpagent
Log buffer:
enabled,max buffer size 1024, current buffer size 512,
current messages 512, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 14
Trap buffer:
enabled,max buffer size 1024, current buffer size 256,
current messages 256, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 238
logfile:
channel number : 9, channel name : channel9, language : english
Information timestamp setting:
log - formate-date millisecond, trap - date, debug - date
Sent messages = 49890, Received messages = 50171
IO Reg messages = 123 IO Sent messages = 282
```

----结束

配置文件

```
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
info-center filter-id 1077514264
info-center loghost 10.1.1.6 binary
#
return
```

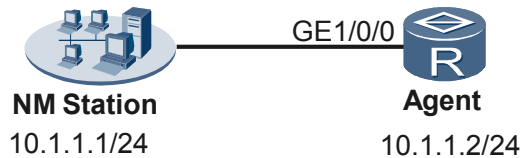
1.6.5 配置向 SNMP Agent 输出告警信息示例

配置向 SNMP Agent 输出告警信息后，网管可以接收到设备发送的告警信息。

组网需求

如图 1-8 所示，告警信息通过信息中心输出到 SNMP Agent，之后通过 SNMP Agent 发送到网管端。

图 1-8 输出告警到 SNMP Agent 组网图



配置思路

采用如下思路进行本例的配置：

1. 在路由器上开启信息中心功能。
2. 配置告警信息输出的通道及输出的模块。
3. 配置向 SNMP Agent 输出告警信息。
4. 配置告警信息输出到网管站。

数据准备

为完成此配置例，需准备如下的数据：

- 信息通道号
- 允许告警输出的模块
- 信息级别

操作步骤

步骤 1 开启信息中心

```
<HUAWEI> system-view
[HUAWEI] info-center enable
```

步骤 2 配置告警信息输出的通道及模块信息

配置告警信息输出的通道及模块信息。

```
[HUAWEI] info-center source ip channel channel7 trap level informational state on
```

说明

缺省情况下，告警信息通过 SNMP Agent 输出，并输出所有模块的信息。

步骤 3 配置向 SNMP Agent 输出告警信息

配置告警信息输出到 SNMP Agent。

```
[HUAWEI] info-center snmp channel channel7
```

步骤 4 配置 SNMP Agent 输出告警信息到网管

启动 SNMP Agent，配置版本为 SNMPv2c。

```
[HUAWEI] snmp-agent sys-info version v2c
```

配置 Trap 功能。

```
[HUAWEI] snmp-agent trap enable standard
```

```
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

步骤 5 验证配置结果

查看 SNMP Agent 输出信息所使用的通道。

```
[HUAWEI] display info-center
```

```
Information Center:enabled
```

```
SNMP Agent:
```

```
channel number : 7, channel name : channel7
```

查看 SNMP Agent 选用通道输出的信息。

```
[HUAWEI] display channel 7
```

```
channel number:7, channel name:channel7
```

MODU_ID	NAME	ENABLE	LOG_LEVEL	ENABLE	TRAP_LEVEL	ENABLE	DEBUG_LEVEL
ffff0000	default	Y	debugging	Y	debugging	N	debugging
416a0000	IP	Y	debugging	Y	informational	N	debugging

查看 SNMP Agent 输出网管的信息。

```
[HUAWEI] display snmp-agent target-host
```

```
Target-host NO. 1
```

```
-----
IP-address      : 10.1.1.1
VPN instance    : -
Security name   : public
Port            : 3000
Type            : trap
Version         : v1
Level           : No authentication and privacy
NMS type        : NMS
-----
```

----结束

配置文件

```
#
info-center source IP channel 7 trap level informational
info-center snmp channel 7
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100003598
snmp-agent community write write
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version v2c v3
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
snmp-agent trap enable standard
#
return
```

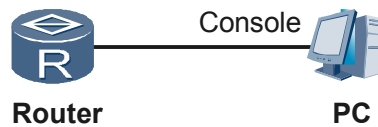
1.6.6 配置向控制台输出调试信息示例

在配置向控制台输出调试信息后，在设备遇到问题时，可以通过控制台登录设备执行调试命令，查看调试信息。

组网需求

如图 1-9 所示，PC 机与路由器 Console 口相连。要求配置向控制台输出 ARP 模块的调试信息。

图 1-9 向控制台输出信息组网图



配置思路

采用如下思路进行本例的配置：

1. 在路由器上开启信息中心功能。
2. 配置允许调试信息输出的模块。
3. 配置调试信息输出的通道。
4. 打开屏幕显示开关，显示调试信息。

数据准备

为完成此配置例，需准备如下的数据：

- 信息通道号
- 允许日志输出的模块
- 信息级别

操作步骤

步骤 1 开启信息系统

```
<HUAWEI> system-view
[HUAWEI] info-center enable
```

步骤 2 配置允许 ARP 模块的调试信息从控制台输出，并且严重等级限制为 debugging

```
[HUAWEI] info-center source arp channel console debug level debugging
[HUAWEI] info-center console channel console
[HUAWEI] quit
```

步骤 3 打开屏幕显示开关，显示调试信息

```
<HUAWEI> terminal monitor
<HUAWEI> terminal debugging
```

步骤 4 打开 ARP 模块的调试开关

```
<HUAWEI> debugging arp packet
```

步骤 5 验证配置结果

查看配置的通道信息。

```
<HUAWEI> display channel 0
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
```

ffff0000	default	Y	warning	Y	debugging	Y	debugging
416e0000	ARP	Y	warning	Y	debugging	Y	debugging

----结束

配置文件

```
#
info-center source ARP channel 0
#
return
```


2 SNMP 配置

关于本章

简单网络管理协议 SNMP（Simple Network Management Protocol）是广泛用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站 NMS）来管理网元的方法。共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3，用户可以根据情况选择同时配置一个或多个版本。

2.1 SNMP 简介

SNMP 为网管和设备间的通信提供一套标准协议，保证网管能够正常的管理设备和接收设备的告警。

2.2 配置设备使用 SNMPv1 与网管通信

配置 SNMPv1 功能后，网管和设备之间将使用 SNMPv1 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

2.3 配置设备使用 SNMPv2c 与网管通信

配置 SNMPv2c 功能后，网管和设备之间将使用 SNMPv2c 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

2.4 配置设备使用 SNMPv3 与网管通信

配置 SNMPv3 功能后，网管和设备之间将使用 SNMPv3 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

2.5 SNMP 配置举例

介绍 SNMP 的配置。请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

2.1 SNMP 简介

SNMP 为网管和设备间的通信提供一套标准协议，保证网管能够正常的管理设备和接收设备的告警。

2.1.1 SNMP 概述

网管通过在被管理设备中运行的 Agent 客户端上执行 GET-SET 操作来管理设备上的节点，设备上的节点由 MIB（Management Information Base）来唯一标识。

2.1.2 NE20E-X6 支持的 SNMP 特性

通过对 SNMP 协议各个版本特性支持情况的对比，以及各个版本适用的应用场景介绍，为用户进行网络部署时选取 SNMP 协议的版本提供参考依据。

2.1.1 SNMP 概述

网管通过在被管理设备中运行的 Agent 客户端上执行 GET-SET 操作来管理设备上的节点，设备上的节点由 MIB（Management Information Base）来唯一标识。

随着网络业务的日益发展，现有的网络中，设备数量日益庞大，且这些设备与网络管理员所在的中心机房距离较远。当这些设备发生故障时，由于设备无法主动上报故障，导致网络管理员无法及时感知、及时定位和排除故障，从而导致网络的维护效率降低，维护工作量大大增加。

为了解决这个问题，设备制造商已经在一些设备中提供了网络管理的功能，这样网管就可以远程询问设备的状态，同样设备能够在特定类型的事件发生时向网络管理工作站发出警告。

SNMP 就是规定网管站和设备之间如何传递管理信息的应用层协议。SNMP 定义了网管管理设备的几种操作，以及设备故障时能向网管主动发送告警。

网管使用 SNMP 协议管理设备时，存在网管站、Agent 和被管理设备三个角色。网管通过管理信息库 MIB 来唯一标识和管理设备上的节点。网管管理设备的操作包括：GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest、以及设备主动发送告警。关于角色、MIB 和操作的定义和作用请参考下面的具体内容。

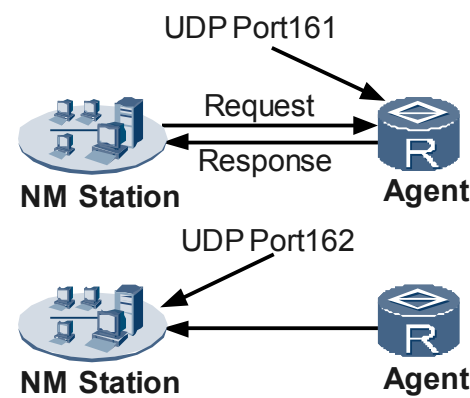
SNMP 定义三类角色

在网管通过 SNMP 协议管理设备过程中，定义了三类角色：

- 网管站：向被管理设备发送各种查询报文，以及接收被管理设备发送的告警。
- Agent：驻留在被管理设备上的一个进程。Agent 的作用如下：
 - 接收、解析来自网管站的查询报文。
 - 根据报文类型对管理变量进行 Read 或 Write 操作，并生成响应报文，返回给网管站。
 - 根据各协议模块对告警触发条件的定义，在达到触发条件后，如进入、退出系统视图或设备重新启动等，相应的模块通过 Agent 主动向网管站发送告警，报告所发生的事件。
- 被管理设备：接受网管的管理，产生和主动上报告警。

网管站与 Agent 的关系如图 2-1 所示。

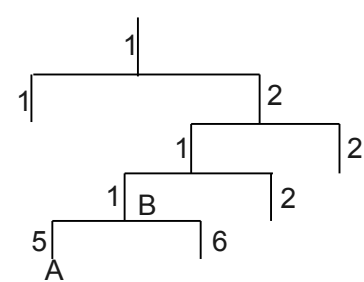
图 2-1 SNMP 结构示意图



MIB

为了在 SNMP 报文中唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象，整个层次结构就象一棵树，树的节点表示管理对象，如图 2-2 所示，它可以用从根开始的一条路径进行识别。

图 2-2 MIB 树结构



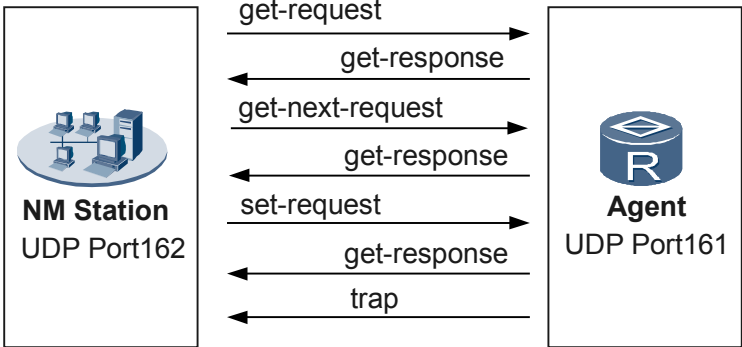
在图 2-2 中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的客体标识符（Object Identifier）。而 MIB 的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。

用户可以采用管理信息库标准 MIB，也可以按标准方式定义自己的 MIB。使用标准 MIB 能够降低部署代理部件的成本，从而降低整个网管系统的成本。

SNMP 操作

SNMP 以 GET-SET 操作方式替代复杂的命令集，利用如图 2-3 的操作实现全部功能。

图 2-3 SNMP 操作示意图



SNMP 的操作如表 2-1 所示。

表 2-1 SNMP 的操作

操作	功能
GetRequest	从某变量中取值，获取设备某功能节点状态，是网管向设备发出的请求。
GetNextRequest	在 MIB 表项中取下一项值，获取设备某功能的另一节点状态，是网管向设备发出的请求。
GetResponse	对 GetRequest、GetNextRequest、SetRequest 的响应，设备向网管的回应。
GetBulk	该操作相当于连续执行多次 GetNext 操作，是网管向设备发出的请求。
SetRequest	设置具体变量的值，对设备功能节点状态进行调整，是网管向设备发出的指令。
Trap	报告事件信息，是设备主动向网管报告事件。

说明

SNMP 协议用于网管对网络设备自身进行监控和管理，不能对网络整体运行情况进行监控和管理。如需要对网络整体运行情况进行监控和管理，比如了解网络性能情况、统计网络数据等，请参考《高端业务路由器 配置指南 系统管理》中 RMON 和 RMON2 配置、Netstream 配置、故障和性能管理配置。

2.1.2 NE20E-X6 支持的 SNMP 特性

通过对 SNMP 协议各个版本特性支持情况的对比，以及各个版本适用的应用场景介绍，为用户进行网络部署时选取 SNMP 协议的版本提供参考依据。

NE20E-X6 系统中支持 SNMPv1、SNMPv2c 和 SNMPv3 三个协议版本。各特性的功能如表 2-2 所示，各版本支持的特性列表如表 2-3 所示。SNMP 各版本的应用场景如表 2-4 所示，用户可以根据现网的运营情况，选择需要的版本使网管和被管理设备之间进行通信。

 说明

在网络中存在多个网管管理同一设备的情况，各网管站可能选用不同的 SNMP 协议版本与设备进行通信。为了满足这些网管和设备的正常通信，可以在设备上同时部署 SNMPv1、v2c、v3。

表 2-2 SNMP 支持的特性功能介绍

特性	功能描述
访问控制	访问控制主要用来限制管理设备的用户的权限。通过该功能可以限制指定的用户管理设备上的指定节点，从而提升精细化管理。
认证加密	认证加密主要是通过对网管和被管理设备传送的报文进行认证和加密，避免数据报文被窃取或篡改，从而提升数据传输的安全性。
错误码	错误码用来标识特定的故障现象，有助于管理员快速定位和解决故障，因此错误码越丰富越有利于管理员对设备进行管理。
Trap 告警	Trap 告警是被管理设备主动向网管发送告警。以便管理员能够及时发现设备的异常。 被管理设备发送 Trap 告警后，不需要网管进行接收确认。
Inform 告警	Inform 告警也是被管理设备向网管主动发送告警。 被管理设备发送 Inform 告警后，需要网管进行接收确认，被管理设备没有收到确认信息时会重复发送该告警，并且生成相应的告警日志，方便网管重启后，能够同步重启时间内发送的告警。 系统没有收到 inform 告警的确认信息时，将告警暂时保存在内存中，因此使用 Inform 告警可能会占用较多的系统资源。
Get-Bulk	Get-Bulk 主要方便管理员进行批量的 Get-next 操作。网络规模较大时，以节省管理员的工作量，提升管理效率。

表 2-3 SNMP 各版本支持的特性概况

特性列表	SNMPv1	SNMPv2c	SNMPv3
访问控制	基于团体名进行访问控制	基于团体名进行访问控制	基于用户和用户组进行访问控制

特性列表	SNMPv1	SNMPv2c	SNMPv3
认证加密	不支持	不支持	支持认证和加密， 认证和加密的方式如下： 认证： ● MD5 ● SHA 加密：DES56
错误码	支持 6 个错误码	支持 16 个错误码	支持 16 个错误码
Trap 告警	支持	支持	支持
Inform 告警	不支持	支持	不支持
Get-Bulk	不支持	支持	支持

表 2-4 SNMP 各版本的应用场景

版本	应用场景
SNMPv1	适用于小型网络，组网简单，对网络安全性要求不高或者网络环境本身比较安全，且比较稳定的网络，比如校园网，小型企业网。
SNMPv2c	适用于大中型网络，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞的网络。 通过配置 Inform 告警可以确保被管理设备发送的告警能够被网管收到。
SNMPv3	适用于各种规模的网络，尤其是对网络的安全性要求较高，确保合法的管理员才能对网络设备进行管理的网络。比如网管和被管理设备间的通信数据需要在公网上进行传输。

如果用户是统一规划建设新网络，建议根据上面的应用场景选择 SNMP 协议的版本。如果用户是网络扩建或升级，建议用户根据网管使用的版本选择在设备上配置对应的 SNMP 协议版本，保证设备和网管的通信。

2.2 配置设备使用 SNMPv1 与网管通信

配置 SNMPv1 功能后，网管和设备之间将使用 SNMPv1 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

2.2.1 建立配置任务

在配置网管使用 SNMPv1 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

2.2.2 配置 SNMPv1 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

2.2.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

2.2.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

2.2.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

2.2.6 （可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

2.2.7 检查配置结果

配置 SNMPv1 成功后，用户可以查看到 SNMPv1 的配置情况。

2.2.1 建立配置任务

在配置网管使用 SNMPv1 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较小，网络设备较少，且网络设备环境本身比较安全时（比如校园网、小型企业网），可以选择使用 SNMPv1 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv1 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv1 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方式和位置、SNMP 报文的尺寸
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间
4	（可选）固定索引的接口数目

2.2.2 配置 SNMPv1 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 3、4、5 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 **snmp-agent sys-info version v1**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。

使能 SNMPv1 后，被管理设备将同时支持 SNMPv1 和 SNMPv3，能同时满足使用 SNMPv1 和 SNMPv3 的网管对设备进行监控和管理。

步骤 4 执行命令 **snmp-agent community { read | write } community-name**，配置设备的读写团体名。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

步骤 5 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

- 如果是 IPv4 网络，请执行命令 **snmp-agent target-host trap address udp-domain ip-address [udp-port port-number] [public-net | vpn-instance vpn-instance-name] params securityname security-string [v1] [private-netmanager]**，配置设备发送告警和错误码的目的主机。
- 如果是 IPv6 网络，请执行命令 **snmp-agent target-host trap ipv6 address udp-domain ip-address [udp-port port-number] params securityname security-string [v1] [private-netmanager]**，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance vpn-instance-name**，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。

步骤 6 （可选）执行命令 **snmp-agent sys-info { contact contact | location location }**，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置网络管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

步骤 7 （可选）执行命令 **snmp-agent packet max-size byte-count**，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该团体名的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。比如：FM、NQA、DATASYNC、PM、SINDEX、L2IF(hwMacUsageRaisingThreshold、hwMacUsageFallingThreshold)、HGMP、RRPP、FR、HDLC、RMON、MP、VRRP、FIB、SNMP（coldStart、warmStart）、DHCPSPNP 模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考[限制网管对设备的访问权限](#)进行配置。

- 需要被管理设备上指定模块的告警发送到网管，请参考[配置向网管系统发送告警](#)进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择[配置 SNMP 扩展错误码功能](#)，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择[配置接口索引固定特性](#)，保证设备重启、接口重启等不会变更接口索引。

2.2.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 5 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，步骤 2、3、4 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl acl-number**，创建一个基本访问控制列表，过滤管理设备的网管用户。

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

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view { excluded | included } view-name oid-tree**，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community { read | write } { community-name | cipher community-name } [mib-view view-name | acl acl-number]***，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 为了加强安全性，用户可以选择配置 **cipher** 参数，使团体名以密文形式显示。该形式下，需要管理员妥善保管团体名称，否则忘记团体名时将无法通过设备查看获得。
- 如果需要使用该团体名的某些网管拥有视图 **viewdefault**（即 1.3.6.1）的权限，参数 **mib-view view-name** 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl acl-number** 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

2.2.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

2.2.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。



说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name feature-name trap-name trap-name**，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 4 执行命令 **snmp-agent notify-filter-profile { excluded | included } profile-name oid-tree**，创建或更新告警过滤信息。

对于使用 **snmp-agent notify-filter-profile** 命令用来更新或创建过滤视图，目前该命令不仅支持以变量 OID 的字符串作为参数输入，同时还支持以节点名作为参数输入。对于 OID 的字符串输入，支持采用“*”作为掩码进行设置。“*”只能放在字符串中间位置，不能放在字符串的头部或尾部。

步骤 5 执行命令 **snmp-agent trap source interface-type interface-number**，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 6 执行命令 **snmp-agent trap queue-size size**，设置发往目的主机的 Trap 报文的队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 7 执行命令 **snmp-agent trap life seconds**，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

2.2.6 （可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

----结束

2.2.7 检查配置结果

配置 SNMPv1 成功后，用户可以查看到 SNMPv1 的配置情况。

前提条件

已经完成 SNMPv1 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** 命令查看当前配置的团体名。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl acl-number** 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display current-configuration | include max-size** 命令查看 SNMP 报文的最大尺寸。
- 执行 **display current-configuration | include trap** 命令查看 Trap 配置信息。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。
- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

任务示例

在配置成功时，执行 **display snmp-agent community** 命令，查看配置的团体名信息。

```
<HUAWEI> display snmp-agent community
Community name:public
Group name:public
Storage-type: nonVolatile
Community name:private
Group name:private
Storage-type: nonVolatile
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<HUAWEI> display snmp-agent sys-info version
SNMP version running in the system:
SNMPv1 SNMPv3
```

执行 **display acl acl-number** 命令，查看配置的访问控制列表的规则。

```
<HUAWEI> display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
rule 5 permit source 1.1.1.1 0 (0 times matched)
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view
View name:ViewDefault
MIB Subtree:internet
Subtree mask:
Storage-type: nonVolatile
View Type:included
View status:active
View name:ViewDefault
MIB Subtree:snmpUsmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
View name:ViewDefault
MIB Subtree:snmpVacmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
View name:ViewDefault
MIB Subtree:snmpModules.18
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<HUAWEI> display snmp-agent sys-info contact
The contact person for this managed node:
R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<HUAWEI> display snmp-agent sys-info location
The physical location of this node:
Beijing China
```

执行 **display current-configuration | include max-size** 命令查看 SNMP 报文的最大尺寸。

```
<HUAWEI> display current-configuration | include max-size
snmp-agent packet max-size 1800
```

执行 **display current-configuration | include trap** 命令，查看 trap 配置信息。

```
<HUAWEI> display current-configuration configuration | include trap
snmp-agent trap enable standard
```

执行 **display snmp-agent extend error-code status** 命令，查看 SNMP 扩展错误码的使能情况。

```
<HUAWEI> display snmp-agent extend error-code status
Extend error-code status:enabled
```

执行 **display constant-ifindex configuration** 命令，查看接口索引固定的状态和配置信息。

```
<HUAWEI> display constant-ifindex configuration
ifindex constant : Enable
ifindex max-number : 65535
current ifindex subinterface mode : sparse-mode
next ifindex subinterface mode : sparse-mode
current ifindex allocation : no multi-chassis
```


2.3 配置设备使用 SNMPv2c 与网管通信

配置 SNMPv2c 功能后，网管和设备之间将使用 SNMPv2c 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

2.3.1 建立配置任务

在配置网管使用 SNMPv2c 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

2.3.2 配置 SNMPv2c 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

2.3.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

2.3.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

2.3.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

2.3.6 （可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

2.3.7 检查配置结果

配置 SNMPv2c 成功后，用户可以查看到 SNMPv2c 的配置情况。

2.3.1 建立配置任务

在配置网管使用 SNMPv2c 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较大，网络设备较多，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞时，可以选择使用 SNMPv2c 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv2c 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv2c 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方式和位置、SNMP 报文的尺寸
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间、Inform 告警的超时时间、重复发送次数、待确认的最大条数、告警日志的老化时间、日志缓冲区中最多能保存的告警日志条数
4	（可选）固定索引的接口数目

2.3.2 配置 SNMPv2c 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 3、4、5 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 （可选）执行命令 `snmp-agent`，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 `snmp-agent` 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 `snmp-agent sys-info version v2c`，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。

使能 SNMPv2c 后，被管理设备将同时支持 SNMPv2c 和 SNMPv3，能同时满足使用 SNMPv2c 和 SNMPv3 的网管对设备进行监控和管理。

步骤 4 执行命令 **snmp-agent community { read | write } community-name**，配置设备的读写团体名。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

步骤 5 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

- 如果是 IPv4 网络，请根据需要选择配置 Trap 方式告警或 Inform 方式告警：

 说明

Trap 方式告警和 Inform 方式告警的区别如下：

- 被管理设备发送 Trap 方式告警时，不需要告警主机回应确认信息。
- 被管理设备发送 Inform 方式告警时，需要告警主机回应确认消息，在超时时间范围内没有收到告警主机的回应消息时，被管理设备将重新发送该告警，直至发送的告警个数达到配置的重复发送最大次数。

被管理设备发送 Inform 告警时，同时记录告警日志，方便告警主机故障或链路故障恢复后，告警主机能够同步故障时间内产生的告警。

因此，Inform 告警相比 Trap 方式告警更加可靠，但由于重传机制的存在，可能导致设备需要缓存大量的告警信息，占用设备较多内存资源。

建议用户在网络比较稳定时选择 Trap 方式告警；在设备资源充足且网络不太稳定的环境下，选择配置 Inform 方式告警。

- Trap 告警：执行命令 **snmp-agent target-host trap address udp-domain ip-address [udp-port port-number] [public-net | vpn-instance vpn-instance-name] params securityname security-string [v2c] [private-netmanager]**，配置设备发送 Trap 告警和错误码的目的主机。
- Inform 告警：执行命令 **snmp-agent target-host inform address udp-domain ip-address [udp-port port-number] [vpn-instance vpn-instance-name] params securityname security-string v2c**，配置设备发送 Inform 告警和错误码的目标主机。
- 如果是 IPv6 网络，请执行命令 **snmp-agent target-host trap ipv6 address udp-domain ip-address [udp-port port-number] params securityname security-string [v2c] [private-netmanager]**，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance vpn-instance-name**，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。



说明

IPv6 网络只支持 Trap 方式告警，不支持 Inform 方式告警。

步骤 6 （可选）执行命令 **snmp-agent sys-info { contact contact | location location }**，配置设备管理员的联系方式和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置网络管理员的联系方式和位置，请执行两次该命令分别配置管理员的联系方式和位置。

步骤 7 （可选）执行命令 **snmp-agent packet max-size byte-count**，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该团体名的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。比如：FM、NQA、DATASYNC、PM、SINDEX、L2IF(hwMacUsageRaisingThreshold、hwMacUsageFallingThreshold)、HGMP、RRPP、FR、HDLC、RMON、MP、VRRP、FIB、SNMP（coldStart、warmStart）、DHCPSPNP 模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考[限制网管对设备的访问权限](#)进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考[配置向网管系统发送告警](#)进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择[配置 SNMP 扩展错误码功能](#)，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择[配置接口索引固定特性](#)，保证设备重启、接口重启等不会变更接口索引。

2.3.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 5 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，步骤 2、3、4 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl acl-number**，创建一个基本访问控制列表，过滤管理设备的网管用户。

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

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view { excluded | included } view-name oid-tree**，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community { read | write } { community-name | cipher community-name } [mib-view view-name | acl acl-number]***，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 为了加强安全性，用户可以选择配置 **cipher** 参数，使团体名以密文形式显示。该形式下，需要管理员妥善保管团体名称，否则忘记团体名时将无法通过设备查看获得。
- 如果需要使用该团体名的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **mib-view view-name** 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl acl-number** 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

2.3.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

2.3.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

 说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name feature-name trap-name trap-name**，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name feature-name trap-name trap-name** 命令一次关闭一个告警开关。

步骤 4 根据配置 SNMPv2c 的基本功能中选择的告警方式，配置对应的告警参数：

Trap 告警参数请参考 [Trap 告警参数配置](#)，Inform 告警参数配置请参考 [Inform 告警参数配置](#)

Trap 告警参数配置：

1. 执行命令 **snmp-agent notify-filter-profile { excluded | included } profile-name oid-tree**，创建或更新告警过滤信息。

对于使用 **snmp-agent notify-filter-profile** 命令用来更新或创建过滤视图，目前该命令不仅支持以变量 OID 的字符串作为参数输入，同时还支持以节点名作为参数输

入。对于 OID 的字符串输入，支持采用 “*” 作为掩码进行设置。“*” 只能放在字符串中间位置，不能放在字符串的头部或尾部。

2. 执行命令 **snmp-agent trap source interface-type interface-number**，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

3. 执行命令 **snmp-agent trap queue-size size**，设置发往目的主机的 Trap 报文的队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

4. 执行命令 **snmp-agent trap life seconds**，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

Inform 告警参数配置：

1. 执行命令 **snmp-agent inform { timeout seconds | resend-times times | pending number } ***，配置确认告警的超时时间、重复发送告警的次数和待确认告警的最大条数。

如果当前网络不稳定，那么增加告警确认的超时时间的同时，需要增加告警重复发送的次数和待确认告警的最大条数，缺省情况下，告警确认的超时时间为 15 秒，告警重复发送的次数为 3 次，待确认告警的最大条数为 39 条。

Inform 方式告警重复发送次数建议配置为小于等于 10 次，否则将影响设备性能。

2. 执行命令 **snmp-agent inform { timeout seconds | resend-times times } * address udp-domain ip-address [vpn-instance vpn-instance-name] params securityname security-string**，配置指定目标主机的告警确认超时时间和告警重复发送的次数。

如果当前网络不稳定，那么增加告警确认的超时时间的同时，需要增加告警重复发送的次数和待确认告警的最大条数，缺省情况下，告警确认的超时时间为 15 秒，告警重复发送的次数为 3 次。

Inform 方式告警重复发送次数建议配置为小于等于 10 次，否则将影响设备性能。

3. 执行命令 **snmp-agent notification-log enable**，使能告警日志功能。

如果路由器与目标主机之间的链路发生故障，导致路由不可达。路由器不再发送 Inform 告警，但是继续记录告警日志。当链路恢复正常，路由变为可达后，目标主机将同步路由器在链路故障期间记录的告警日志。

使能告警日志功能后，系统只记录 Inform 方式的告警，不记录 Trap 方式的告警。

缺省情况下，告警日志功能关闭。

4. 执行命令 **snmp-agent notification-log { global-ageout ageout | global-limit limit } ***，配置告警日志的老化时间和日志缓冲区中最多能保存的告警日志条数。

缺省情况下，告警日志的老化时间为 24 小时。超过 24 小时，告警日志被自动删除。

缺省情况下，日志缓冲区中最多能保存的告警日志为 500 条。超出这个限制，将从最早的一条告警日志开始删除。

----结束

2.3.6 （可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

----结束

2.3.7 检查配置结果

配置 SNMPv2c 成功后，用户可以查看到 SNMPv2c 的配置情况。

前提条件

已经完成 SNMPv2c 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** 命令查看当前配置的团体名。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl acl-number** 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display current-configuration | include max-size** 命令查看 SNNP 报文的最大尺寸。
- 执行命令 **display current-configuration | include trap**，查看 Trap 配置信息。
- 执行 **display snmp-agent target-host** 命令查看目标主机的信息。
- 执行 **display snmp-agent inform [address udp-domain ip-address [vpn-instance vpn-instance-name] params securityname security-string]** 命令查看全局或指定目标主机的 Inform 参数、主机统计信息。
- 执行 **display snmp-agent notification-log info** 命令查看告警日志缓冲区中的告警日志信息。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。

- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

任务示例

在配置成功后，执行 **display snmp-agent community** 命令，查看配置的团体名信息。

```
<HUAWEI> display snmp-agent community
Community name:public
  Group name:public
  Storage-type: nonVolatile
Community name:private
  Group name:private
  Storage-type: nonVolatile
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<HUAWEI> display snmp-agent sys-info version
SNMP version running in the system:
  SNMPv2c SNMPv3
```

执行 **display acl acl-number** 命令，查看配置的访问控制列表的规则。

```
<HUAWEI> display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
rule 5 permit source 1.1.1.1 0 (0 times matched)
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view
View name:ViewDefault
  MIB Subtree:internet
  Subtree mask:
  Storage-type: nonVolatile
  View Type:included
  View status:active
View name:ViewDefault
  MIB Subtree:snmpUsmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
View name:ViewDefault
  MIB Subtree:snmpVacmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
View name:ViewDefault
  MIB Subtree:snmpModules.18
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active

Total number is 1
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<HUAWEI> display snmp-agent sys-info contact
The contact person for this managed node:
  R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<HUAWEI> display snmp-agent sys-info location
The physical location of this node:
  Beijing China
```

执行 **display current-configuration | include max-size** 命令查看 SNMP 报文的最大尺寸。

```
<HUAWEI> display current-configuration | include max-size
snmp-agent packet max-size 1800
```

执行 **display current-configuration | include trap** 命令查看 trap 配置信息。

```
<HUAWEI> display current-configuration configuration | include trap
snmp-agent trap enable standard
```

执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码的使能情况。

```
<HUAWEI> display snmp-agent extend error-code status
Extend error-code status:enabled
```

执行 **display snmp-agent target-host** 命令查看目标主机的信息。

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
```

```
-----
IP-address      : 2.2.2.2
VPN instance    : -
Security name   : abc
Port            : 23
Type            : inform
Version         : v2c
Level           : No authentication and privacy
NMS type        : NMS
-----
```

```
Target-host NO. 2
```

```
-----
IP-address      : 1.1.1.1
VPN instance    : -
Security name   : aaa
Port            : 22
Type            : trap
Version         : v2c
Level           : No authentication and privacy
NMS type        : HW NMS
-----
```

执行 **display snmp-agent inform** 命令可查看 Inform 方式发送告警的配置信息的显示。

```
<HUAWEI> display snmp-agent inform
Global config: resend-times 3, timeout 15s, pending 39
Global status: current notification count 0
Target-host ID: VPN instance/IP-Address/Security name
a/1.1.1.1/public:
  Config: resend-times 3, timeout 15s
  Status: retries 0, pending 0, sent 0, dropped 0, failed 0, confirmed 0
```

执行 **display snmp-agent notification-log info** 命令查看告警日志缓冲区中的告警日志信息。

```
<HUAWEI> display snmp-agent notification-log info
Notification log information :
Notifications Admin Status: enable
GlobalNotificationsLogged: 0
GlobalNotificationsBumped: 0
GlobalNotificationsLimit: 500
GlobalNotificationsAgeout: 24
Total number of notification log: 0
```

执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

```
<HUAWEI> display constant-ifindex configuration
ifindex constant : Enable
ifindex max-number : 65535
current ifindex subinterface mode : sparse-mode
next ifindex subinterface mode : sparse-mode
current ifindex allocation : no multi-chassis
```


2.4 配置设备使用 SNMPv3 与网管通信

配置 SNMPv3 功能后，网管和设备之间将使用 SNMPv3 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

2.4.1 建立配置任务

在配置网管使用 SNMPv3 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

2.4.2 配置 SNMPv3 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

2.4.3（可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强使用 SNMPv3 进行通信的网管和被管理设备的安全性。

2.4.4（可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

2.4.5（可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

2.4.6（可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

2.4.7 检查配置结果

配置 SNMPv3 成功后，用户可以查看到 SNMPv3 的配置情况。

2.4.1 建立配置任务

在配置网管使用 SNMPv3 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络对安全性要求较高，只有合法的管理员才能对网络设备进行管理，并且传输的网络数据需要保证其安全性和准确性时，比如网管和被管理设备间的通信数据需要

在公网上进行传输，可以部署 SNMPv3，通过 SNMPv3 的认证和加密功能确保数据传输的安全性，保证网管和被管理设备之间的正常通信。

前置任务

在完成配置网管使用 SNMPv3 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv3 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、用户和用户组的名称、告警目的主机地址、管理员的联系方法和位置、SNMP 报文的尺寸
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间
4	（可选）固定索引的接口数目

2.4.2 配置 SNMPv3 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 4、5、6 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 （可选）执行命令 **snmp-agent sys-info version v3**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv3。故该步骤可选。

步骤 4 执行命令 **snmp-agent group v3 group-name [authentication | privacy]**，配置 SNMP 用户组。

当网管和设备处在不安全的网络环境中时，比如容易遭受攻击等，建议用户配置参数 **authentication** 或 **privacy**，使能数据的认证和加密功能。

用户可以选择的认证加密模式如下：

- 不配置 **authentication** 和 **privacy** 参数：不认证不加密。适用于网络环境安全，且管理员比较固定的情况下。
- 配置 **authentication** 参数：只认证不加密。适用于网络环境安全，但管理员比较多，管理员对设备交叉操作比较频繁的情况下。通过认证可以限制拥有权限的管理员才可以访问该设备。
- 配置 **privacy** 参数：既认证又加密。适用于网络环境不太安全，管理员交叉操作多的情况下。通过认证和加密既可以限制特定的管理员访问设备，并且使网络数据以加密形式发送，避免网络数据被窃取，造成关键数据泄露。

步骤 5 执行命令 **snmp-agent usm-user v3 user-name group-name [authentication-mode { md5 | sha } password [privacy-mode des56 password]**，配置 SNMP 用户信息。

用户组和用户配置完成后，使用该用户名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

用户组使能认证和加密功能后，用户可以选择认证和加密的方式，对网络传输的数据进行认证和加密。

- 认证方式
 - MD5（Message Digest 5）：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
 - SHA-1（Secure Hash Algorithm）：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

- 加密方式
 - DES 使用 56bit 的密钥对一个 64bit 的明文块进行加密。

步骤 6 执行下面的命令配置设备发送告警和错误码的目的主机，请根据网络需要选择下面的命令进行配置：

- 如果是 IPv4 网络，请执行命令 **snmp-agent target-host trap address udp-domain ip-address [udp-port port-number] [public-net | vpn-instance vpn-instance-name] params securityname security-string [v3] [private-netmanager]**，配置设备发送告警和错误码的目的主机。
- 如果是 IPv6 网络，请执行命令 **snmp-agent target-host trap ipv6 address udp-domain ip-address [udp-port port-number] params securityname security-string [v3] [private-netmanager]**，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance vpn-instance-name**，指定告警需要穿越的 VPN 实例。
- **securityname** 用来在网管上标识和区别发送告警的源设备，方便用户识别告警的发送方。
- 当网管和被管理设备是华为设备时，可以选择配置 **private-netmanager**，使告警中携带更丰富的信息，比如告警的类型、发送告警的序号和告警发送的时间，以便能更加快速的定位和解决问题。
- 设备产生过多的告警会影响用户对故障根因的排查，为了减少无关告警对用户定位故障造成的影响，用户可以选择配置 **notify-filter-profile** 参数，筛选出用户关心的告

警，这些告警将被发送至告警主机，其他无关告警将被设备过滤掉，不再发送至告警主机。要使告警的过滤策略生效，用户还需要在[配置用户组](#)时选取 **notify-view** 参数。

步骤 7 （可选）执行命令 **snmp-agent sys-info { contact *contact* | location *location* }**，配置设备管理员的联系方式和位置。

当网管管理较多设备时，为了方便网管管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置网络管理员的联系方式和位置，请执行两次该命令分别配置管理员的联系方式和位置。

步骤 8 （可选）执行命令 **snmp-agent packet max-size *byte-count***，配置设备接收或发送的 SNMP 消息包的最大值。

缺省情况下，SNMP 报文最大尺寸为 12000 字节。

配置 SNMP 报文的最大尺寸后，当 SNMP 报文尺寸大于配置的最大尺寸时，设备将丢弃该报文。该报文尺寸根据网管能够处理的最大报文尺寸进行设定，否则将导致网管无法处理该报文。

----结束

后续处理

以上任务配置完成后，网管就可以和被管理设备之间进行正常的基本通信。其中：

- 访问控制是使用该用户组的网管都可以对设备上的所有节点进行监控和管理。
- 被管理设备向网管发送缺省状态是打开的模块的告警。比如：FM、NQA、DATASYNC、PM、SINDEX、L2IF(hwMacUsageRaisingThreshold、hwMacUsageFallingThreshold)、HGMP、RRPP、FR、HDLC、RMON、MP、VRRP、FIB、SNMP（coldStart、warmStart）、DHCPSPNP 模块的告警。

如果需要进行更精细化的管理，比如：

- 需要使用该用户组中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考[限制网管对设备的访问权限](#)进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考[配置向网管系统发送告警](#)进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择[配置 SNMP 扩展错误码功能](#)，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。
- 为了使网管和被管理设备通信过程中，某些特定的功能能够和指定的接口绑定，比如计费、故障定位，可以选择[配置接口索引固定特性](#)，保证设备重启、接口重启等不会变更接口索引。

2.4.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强使用 SNMPv3 进行通信的网管和被管理设备的安全性。

背景信息

当有多个网管使用同一个用户组名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用用户组名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 5 可以省略。
- 如果需要使用用户组名的所有网管管理设备上的指定节点，步骤 2、3、4 可以省略。
- 如果需要使用用户组名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl acl-number**，创建一个基本访问控制列表，过滤管理设备的网管用户。

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

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view { excluded | included } view-name oid-tree**，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **excluded**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **included**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent group v3 group-name [authentication | privacy] [read-view read-view | write-view write-view | notify-view notify-view]* [acl acl-number]**，配置用户组的读写权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read-view** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write-view** 参数。
- 用户希望筛选部分重要告警，过滤掉无关告警时，选择配置 **notify-view notify-view** 参数，限制被管理设备向网管发送告警的 MIB 节点。配置该参数后，设备产生的告警中匹配 **notify-view** 指定的 MIB 节点的告警才能发送到该用户的网管。为了使告警过滤策略生效，还需要在[配置告警主机](#)中选取 **notify-filter-profile** 参数。
- 为了加强安全性，用户可以选择配置 **authentication** 或 **privacy** 参数，**authentication** 对用户只认证不加密，**privacy** 对用户既认证又加密，具体请参考[认证和加密选取原则](#)。
- 如果需要使用该用户组的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **[read-view read-view | write-view write-view | notify-view notify-view]** 可以省略。
- 如果需要使用该用户组的所有网管管理设备上的某些节点，参数 **acl acl-number** 可以省略。
- 如果需要使用该用户组的某些网管管理设备上的某些节点，ACL 和 MIB 视图都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

2.4.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

2.4.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

 说明

使用 **snmp-agent trap enable** 命令打开所有模块的告警开关，或者使用 **snmp-agent trap enable feature-name** 打开三个或三个以上的告警开关时。

- 如果需要一次性关闭所有打开的告警开关，需使用 **snmp-agent trap disable** 关闭所有打开的告警开关。
- 如果需要一次性恢复所有的告警开关至缺省状态，需使用 **undo snmp-agent trap enable**、或者 **undo snmp-agent trap disable** 恢复所有的告警开关至缺省状态。
- 如果需要关闭其中某一个告警开关时，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 3 执行命令 **snmp-agent trap enable feature-name feature-name trap-name trap-name**，使能向网管发送指定特性下的某条告警信息。

如果需要关闭某一个告警开关，可以使用 **undo snmp-agent trap enable feature-name** 命令一次关闭一个告警开关。

步骤 4 执行命令 **snmp-agent notify-filter-profile { excluded | included } profile-name oid-tree**，创建或更新告警过滤信息。

对于使用 **snmp-agent notify-filter-profile** 命令用来更新或创建过滤视图，目前该命令不仅支持以变量 OID 的字符串作为参数输入，同时还支持以节点名作为参数输入。对于 OID 的字符串输入，支持采用 “*” 作为掩码进行设置。“*” 只能放在字符串中间位置，不能放在字符串的头部或尾部。

步骤 5 执行命令 **snmp-agent trap source interface-type interface-number**，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 6 执行命令 **snmp-agent trap queue-size size**，设置发往目的主机的 Trap 报文的队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当地把队列长度加长，减少告警丢失的发生。

步骤 7 执行命令 **snmp-agent trap life seconds**，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

2.4.6 （可选）配置接口索引固定特性

配置接口索引固定特性可以使接口的索引值固定，不受接口的增加、删除、系统重启或者软硬件配置变化的影响而改变，从而满足一些需要固定接口的功能的需求，比如计费、故障诊断等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ifindex constant**，使能接口索引固定特性。

在配置接口索引固定后，当前所有接口及新创建的接口索引的值都是固定的。在系统需要重新启动前，需要先执行 **save** 命令，保存接口的配置信息，否则接口的索引值在系统启动后，会发生变化。

----结束

2.4.7 检查配置结果

配置 SNMPv3 成功后，用户可以查看到 SNMPv3 的配置情况。

前提条件

已经完成 SNMPv3 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent usm-user [engineid engineid | group group-name | username user-name]*** 命令查看用户信息。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl acl-number** 命令显示配置的访问控制列表的规则。

- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display current-configuration | include max-size** 命令查看 SNMP 报文的最大尺寸。
- 执行 **display current-configuration | include trap** 命令查看 Trap 配置信息。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。
- 执行 **display constant-ifindex configuration** 命令查看接口索引固定的状态和配置信息。

----结束

任务示例

执行 **display snmp-agent usm-user** 命令，查看 SNMP 用户信息。

```
<HUAWEI> display snmp-agent usm-user
User name: ul
Engine ID: 000007DB7F00000100000772 active
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<HUAWEI> display snmp-agent sys-info version
SNMP version running in the system:
SNMPv3
```

执行 **display acl acl-number** 命令，查看配置的访问控制列表的规则。

```
<HUAWEI> display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
rule 5 permit source 1.1.1.1 0 (0 times matched)
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view
View name:ViewDefault
MIB Subtree:internet
Subtree mask:
Storage-type: nonVolatile
View Type:included
View status:active
View name:ViewDefault
MIB Subtree:snmpUsmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
View name:ViewDefault
MIB Subtree:snmpVacmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
View name:ViewDefault
MIB Subtree:snmpModules.18
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active

Total number is 1
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<HUAWEI> display snmp-agent sys-info contact
```



```
The contact person for this managed node:
    R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<HUAWEI> display snmp-agent sys-info location
    The physical location of this node:
        Beijing China
```

执行 **display current-configuration | include max-size** 命令查看 SNMP 报文的最大尺寸。

```
<HUAWEI> display current-configuration | include max-size
    snmp-agent packet max-size 1800
```

执行 **display current-configuration | include trap** 命令，查看 trap 配置信息。

```
<HUAWEI> display current-configuration configuration | include trap
    snmp-agent trap enable standard
```

执行 **display snmp-agent extend error-code status** 命令，查看 SNMP 扩展错误码的使能情况。

```
<HUAWEI> display snmp-agent extend error-code status
    Extend error-code status:enabled
```

执行 **display constant-ifindex configuration** 命令，查看接口索引固定的状态和配置信息。

```
<HUAWEI> display constant-ifindex configuration
    ifindex constant : Enable
    ifindex max-number : 65535
    current ifindex subinterface mode : sparse-mode
    next ifindex subinterface mode : sparse-mode
    current ifindex allocation : no multi-chassis
```

2.5 SNMP 配置举例

介绍 SNMP 的配置。请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

2.5.1 配置设备使用 SNMPv1 与网管通信示例

网管在管理设备时使用 SNMPv1 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

2.5.2 配置设备使用 SNMPv2c 与网管通信示例

网管在管理设备时使用 SNMPv2c 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

2.5.3 配置设备使用 SNMPv3 与网管通信示例

网管在管理设备时使用 SNMPv3 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

2.5.1 配置设备使用 SNMPv1 与网管通信示例

网管在管理设备时使用 SNMPv1 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

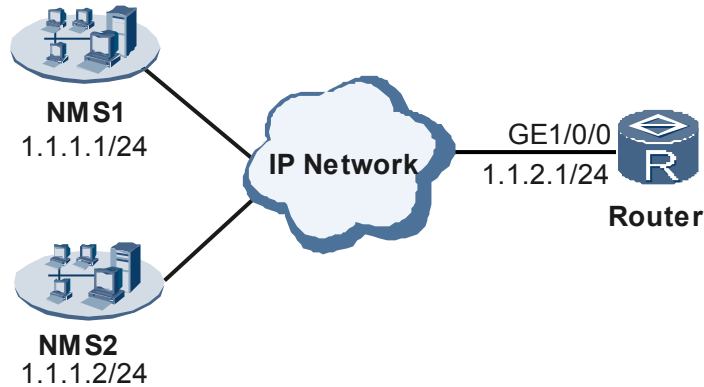
组网需求

如图 2-4 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理该设备上除 HGMP 之外的所有节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上该设备管理员，以便对故障进行快速定位和排除，故要求在设备上配置设备管理员的联系方法。

图 2-4 配置使用 SNMPv1 与网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv1。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称
- ACL 号
- NMS 地址
- 管理员联系方式

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<HUAWEI> system-view
```

```
[HUAWEI] snmp-agent
```

步骤 3 配置 SNMP 的版本为 v1

```
[HUAWEI] snmp-agent sys-info version v1
```

查看配置的 SNMP 的版本信息。

```
[HUAWEI] display snmp-agent sys-info version
SNMP version running in the system:
    SNMPv1 SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[HUAWEI-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[HUAWEI-acl-basic-2001] quit
```

配置 MIB 视图，限制 NMS2 可以管理设备上除 HGMP 之外的节点。

```
[HUAWEI] snmp-agent mib-view excluded allethgmp 1.3.6.1.4.1.2011.6.7
```

配置团体名引用 ACL 和 MIB 视图。

```
[HUAWEI] snmp-agent community write adminnms2 mib-view allethgmp acl 2001
```

步骤 5 配置告警功能

```
[HUAWEI] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname 1.1.3.1
[HUAWEI] snmp-agent trap source loopbak0
[HUAWEI] snmp-agent trap queue-size 200
[HUAWEI] snmp-agent trap life 60
```

步骤 6 配置管理员联系方式

```
[HUAWEI] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<HUAWEI> display snmp-agent community
Community name:adminnms2
Group name:adminnms2
Acl:2001
Storage-type: nonVolatile
```

查看 ACL 配置。

```
<HUAWEI> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
rule 5 permit source 1.1.1.2 0 (0 times matched)
rule 6 deny source 1.1.1.1 0 (0 times matched)
```

查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view viewname allethgmp
View name:allethgmp
MIB Subtree:hwCluster
Subtree mask:FF80 (Hex)
Storage-type: nonVolatile
```

```
View Type:excluded
View status:active
```

查看告警的目标主机。

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
```

```
-----
IP-address      : 1.1.1.2
VPN instance    : -
Security name   : 1.1.3.1
Port            : 162
Type            : trap
Version         : v1
Level           : No authentication and privacy
NMS type        : NMS
-----
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方式。

```
<HUAWEI> display snmp-agent sys-info contact
The contact person for this managed node:
      call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
snmp-agent trap type base-trap
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 1.1.2.1 255.255.255.0
#
interface loopback0
 ip address 1.1.3.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 1.1.2.0 0.0.0.255
 network 1.1.3.1 0.0.0.0
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
snmp-agent community write adminnms2 mib-view allxthgmp acl 2001
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v1 v3
```

```
snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname 1.1.3.1

snmp-agent mib-view excluded allxthgmp hwCluster
snmp-agent trap source loopback0
snmp-agent trap queue-size 200
snmp-agent trap life 60
#
return
```

2.5.2 配置设备使用 SNMPv2c 与网管通信示例

网管在管理设备时使用 SNMPv2c 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

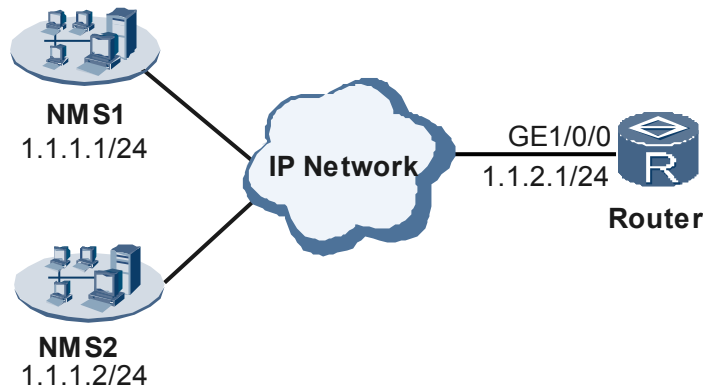
组网需求

如图 2-5 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备上除 HGMP 之外的所有节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。由于设备发送的告警需要经过公网才能被网管接收，为了保证告警接收的可靠性，采用 Inform 方式告警。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方式。

图 2-5 配置使用 SNMPv2c 管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv2c。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点。
4. 配置设备的 Inform 告警功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方式。

6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称
- ACL 号
- NMS 地址
- 管理员联系方式

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<HUAWEI> system-view
[HUAWEI] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v2c

```
[HUAWEI] snmp-agent sys-info version v2c
```

查看配置的 SNMP 的版本信息。

```
[HUAWEI] display snmp-agent sys-info version
SNMP version running in the system:
    SNMPv2c SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[HUAWEI-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[HUAWEI-acl-basic-2001] quit
```

配置 MIB 视图。

```
[HUAWEI] snmp-agent mib-view excluded allextgmp 1.3.6.1.4.1.2011.6.7
```

配置团体名引用 ACL 和 MIB 视图。

```
[HUAWEI] snmp-agent community write adminnms2 mib-view allextgmp acl 2001
```

步骤 5 配置告警功能

```
[HUAWEI] snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname 1.1.2.1
[HUAWEI] snmp-agent inform timeout 15 resend-times 3 pending 39
[HUAWEI] snmp-agent notification-log enable
[HUAWEI] snmp-agent notification-log global-ageout 8
```

步骤 6 配置管理员联系方式

```
[HUAWEI] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<HUAWEI> display snmp-agent community
Community name:adminnms2
Group name:adminnms2
Acl:2001
Storage-type: nonVolatile
```

查看 ACL。

```
<HUAWEI> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
rule 5 permit source 1.1.1.2 0 (0 times matched)
rule 6 deny source 1.1.1.1 0 (0 times matched)
```

查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view viewname allxthgmp
View name:allxthgmp
MIB Subtree:hwCluster
Subtree mask:FF80(Hex)
Storage-type: nonVolatile
View Type:excluded
View status:active
```

查看告警的目标主机。

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
-----
IP-address      : 1.1.1.2
VPN instance    : -
Security name   : 1.1.2.1
Port            : 162
Type            : trap
Version         : v1
Level           : No authentication and privacy
NMS type        : NMS
-----
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<HUAWEI> display snmp-agent sys-info contact
The contact person for this managed node:
call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
snmp-agent trap type base-trap
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 01.1.1.1 0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 1.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 1.1.2.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
snmp-agent community write adminnms2 mib-view allxthgmp acl 2001
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v2c v3
snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname 1.1.2.1

snmp-agent mib-view excluded allxthgmp hwCluster
snmp-agent inform timeout 15 resend-times 3 pending 39
snmp-agent notification-log enable
snmp-agent notification-log global-ageout 8
#
return
```

2.5.3 配置设备使用 SNMPv3 与网管通信示例

网管在管理设备时使用 SNMPv3 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

组网需求

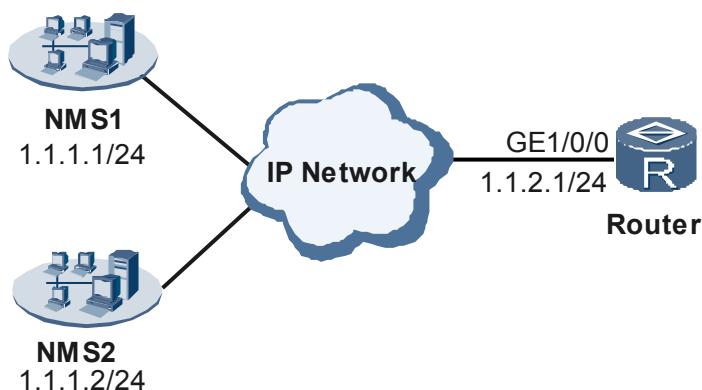
如图 2-6 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备上除 HGMP 之外的所有节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于 NMS2 和设备间的数据需要穿越公网，对用户的数据进行认证和加密。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方式。

图 2-6 配置使用 SNMPv3 网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv3。
3. 配置用户访问权限，限制 NMS2 可以管理设备上 HGMP 之外的节点，并对用户进行数据加密。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 用户组名称
- 用户名和密码
- 认证和加密算法
- ACL 号
- NMS 地址
- 管理员联系方式

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 配置 SNMP Agent

```
<HUAWEI> system-view
[HUAWEI] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v3

```
[HUAWEI] snmp-agent sys-info version v3
```

查看配置的 SNMP 的版本信息。

```
[HUAWEI] display snmp-agent sys-info version
SNMP version running in the system:
    SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[HUAWEI-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[HUAWEI-acl-basic-2001] quit
```

配置 MIB 视图。

```
[HUAWEI] snmp-agent mib-view included testview iso
```

配置用户组和用户，对用户的数据进行认证和加密。

```
[HUAWEI] snmp-agent usm-user v3 testuser testgroup authentication-mode md5 87654321 privacy-mode
des56 87654321
[HUAWEI] snmp-agent group v3 testgroup privacy write-view testview notify-view testview acl 2001
```

步骤 5 配置告警功能

```
[HUAWEI] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname testuser
[HUAWEI] snmp-agent trap source loopback0
[HUAWEI] snmp-agent trap queue-size 200
[HUAWEI] snmp-agent trap life 60
```

步骤 6 配置管理员联系方法

```
[HUAWEI] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置 NMS

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看用户组。

```
<HUAWEI> display snmp-agent group testgroup
```

```
Group name: testgroup
Security model: v3 noAuthnoPriv
Readview: ViewDefault
Writeview: testview
Notifyview: testview
Storage-type: nonVolatile
Acl:2001
```

查看用用户。

```
<HUAWEI> display snmp-agent usm-user
```

```
User name: testuser
Engine ID: 000007DB7F00000100004C3F active
Group name:testgroup
```

查看 ACL。

```
<HUAWEI> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
```

```
rule 5 permit source 1.1.1.2 0 (0 times matched)
rule 6 deny source 1.1.1.1 0 (0 times matched)
```

查看 MIB 视图。

```
<HUAWEI> display snmp-agent mib-view viewname testview
View name:testview
MIB Subtree:iso
Subtree mask:
Storage-type: nonVolatile
View Type:included
View status:active
```

查看告警的目标主机。

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
```

```
-----
IP-address       : 1.1.1.2
Source interface : -
VPN instance     : -
Security name    : testuser
Port             : 162
Type             : trap
Version          : v1
Level            : No authentication and privacy
NMS type         : NMS
-----
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方式。

```
<HUAWEI> display snmp-agent sys-info contact
The contact person for this managed node:
      call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
snmp-agent trap type base-trap
#
acl number 2001
rule 5 permit source 1.1.1.2 0
rule 6 deny source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 1.1.2.1 255.255.255.0
#
interface loopback0
ip address 1.1.3.1 255.255.255.255
```

```
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
  network 1.1.3.1 0.0.0.0
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF000004A7
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v3
snmp-agent group v3 testgroup write-view testview notify-view testview acl 2001
snmp-agent group v3 testgroup privacy
snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname testuser
snmp-agent mib-view included testview iso
snmp-agent usm-user v3 testuser testgroup authentication-mode md5 `,+VK;'MYJF=,/<97^aP^1!! privacy-
mode des56 `,+VK;'MYJF=,/<97^aP^1!!
snmp-agent trap source loopback0
snmp-agent trap queue-size 200
#
return
```

3 RMON 和 RMON2 配置

关于本章

通过 RMON(Remote Network Monitoring)和 RMON2 可以实现对以太接口的监控。

3.1 RMON 和 RMON2 简介

通过 RMON 和 RMON2 的简介，用户可以了解到 RMON 和 RMON2 的工作原理。

3.2 配置 RMON

通过配置 RMON 可以实现对于网络状况和流量进行监控。

3.3 配置 RMON2

通过 RMON2 可以实现对网络上某一接口进行流量监控，分析所有进出该接口的数据来自于哪些主机，去向哪些主机，并分别对网络上每台主机流经该接口的数据进行统计。

3.4 维护 RMON 和 RMON2

在出现 RMON 运行故障时，请在用户视图下执行中的 **debugging** 命令对 RMON 进行调试，查看调试信息，定位故障并分析故障原因。

3.5 RMON 和 RMON2 配置举例

介绍 RMON 和 RMON2 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

3.1 RMON 和 RMON2 简介

通过 RMON 和 RMON2 的简介，用户可以了解到 RMON 和 RMON2 的工作原理。

3.1.1 RMON 和 RMON2 概述

介绍 RMON 和 RMON2 的工作原理及 RMON 和 RMON2 的区别。

3.1.2 NE20E-X6 支持的 RMON 和 RMON2 特性

本节介绍了 NE20E-X6 对 RMON 和 RMON2 的支持。

3.1.1 RMON 和 RMON2 概述

介绍 RMON 和 RMON2 的工作原理及 RMON 和 RMON2 的区别。

RMON 概述

RMON 基于简单网络管理协议 SNMP 体系结构实现，与现存 SNMP 框架兼容，包括网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分。

RMON Agent 跟踪统计网络中的各种流量信息，例如，某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。它使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效手段。减少了网管站与代理 Agent 间的通讯流量，从而实现更简单有效地管理大型网络。

RMON 允许有多个监控者，它可用两种方法收集数据。

- 通过专用的 RMON Probe（探测器）。NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将 RMON Agent 直接嵌入网络设备（例如路由器）中，使它们成为带 RMON Probe 功能的网络设备。NMS 是用 SNMP 基本命令与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。

目前只能对网络设备的以太网接口进行监控和统计。

RMON2 概述

RMON2 是 RMON MIB 规范的一部分，是对原始 RMON 的简单扩充，并添加了一些新组。

RMON 和 RMON2 都是针对于以太网链路的监控，RMON 只在 MAC 层监视流量，RMON2 可以监视 MAC 层以上协议流量。

RMON2 从 OSI 模型第 3 层到第 7 层对数据包进行解码。它包括两个重要含义：

- RMON 代理能基于网络层协议和地址监视流量，包括 IP 协议。这使代理能够看到与之相连的外部 LAN 网段，查看通过路由器进入 LAN 的流量。
- RMON 代理可以对应用程序流量解码和监视，例如 E-mail、FTP 和 WWW，所以，代理能够记录进出特定应用程序的流量。

RFC2021 中定义的 RMON2 包含 MIB 组：protocolDir、protocolDist、addressMap、nlHost、nlMatrix、alHost、alMatrix、usrHistory、probeConfig、rmonConformance。

3.1.2 NE20E-X6 支持的 RMON 和 RMON2 特性

本节介绍了 NE20E-X6 对 RMON 和 RMON2 的支持。

RMON 特性

NE20E-X6 通过把 RMON Agent 模块直接嵌入网络设备中，与其它模块形成一个完整的系统来实现 RMON。网管工作站 NMS 可以完全利用 SNMP NMS，网络管理人员无须进行额外的学习。

NE20E-X6 RMON 支持 RFC2819 规定的统计、历史、告警和事件四个组以及华为规定的私有扩展告警组（PERFORMANCE-MIB）。下面对这几个组分别进行介绍。

- 统计组

统计组统计被监控的每个子网的基本统计信息。它能统计某一网段的流量和各种类型包的分布，还能统计各种类型的错误帧数、碰撞次数等。

统计组包含一个以太网统计表（ethernetStatsTable）。



说明

RMON 统计结果与 **display interface** 的显示结果不完全一致，虽然两者都是从底层获取数据，但 RMON 搜集的信息更全面。

- 历史组

历史组定期收集网络状态统计信息并存储，以便后续的处理。

历史组包含两个表：

- 历史控制表（historyControlTable）：主要用来设置采样间隔时间等控制信息。
- 以太网历史表（ethernetHistoryTable）：为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

历史控制表中的每一项控制信息在以太网历史表中最多可以有 10 条历史数据相对应，如果超过指定条数，将循环覆盖。

- 告警组

告警组允许针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值，如果采样数据在相应的方向上越过阈值，监视器会记录日志或者把告警发往网管站。

按照 RFC2819，告警功能采用一种滞后机制限制告警事件的产生。应用这个机制后，当采样数据以某方向跨过阈值时，将会产生一个事件。直到相反方向的阈值被跨过以前，不会产生更多的事件。

NE20E-X6 在实现时没有采取这种方式，因为滞后机制可能长时间不会产生告警。在 NE20E-X6 中，只要采样值回到正常阈值后就可以重新告警。

告警组包括一个告警表（alarmTable）。

- 事件组

事件组提供关于 RMON 代理所产生的所有事件的表。当某事件发生时，可以记录日志或发送 TRAP 到网管站。

事件组主要实现 Log、Trap 以及 Log-Trap 三种事件输出，每个日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

事件组包括事件表（eventTable）和日志表（logTable）。

- 扩展告警组

扩展告警组在 RFC2819 基础上增加了用表达式设定告警对象和告警生存时间的功能。它包括一个扩展告警表（prialarmTable）。

各表项在 NE20E-X6 中，为节约系统资源，每个表记录都有自己的生存时间，规定了当此行状态不是有效状态 VALID 时，此行可以存在的时间。对于一直处于非 VALID 状态的行，其生存时间将递减。当生存时间为 0 时，行被删除。各表的容量和最大生存时间如表 3-1 所示。

表 3-1 各表的生存时间

表名称	表项容量(Byte)	最大生存时间 (s)
统计表	100	600
历史控制表	100	600
告警表	60	6000
事件表	60	600
事件日志表	600	-
扩展告警表	50	6000

 说明

事件日志表没有最大生存时间，日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

当有接口板或接口卡被拔出时，接口对应的统计表和历史控制表状态会变成 INVALID 状态，此时，对应的统计表和历史控制表的生存时间被设置为 1200s。如果表记录的生存时间到达 0，该表记录将被删除。

当接口插入时，如果存在对应的表记录，则把对应表记录的行状态变为 VALID，这一表记录成为有效的正常表记录。

RMON2 特性

NE20E-X6 目前只支持 RMON2 中的两个 MIB 组：protocolDir 和 nlHost。

其中，nlHost 只支持网络层主机组，不支持应用层主机组，即不实现主机控制表中对应应用层主机组的控制部分和 alHostTable 表，因此，协议目录组中只能设置 IP 协议，设置其它协议无效。

3.2 配置 RMON

通过配置 RMON 可以实现对于网络状况和流量进行监控。

3.2.1 建立配置任务

在配置 RMON 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

3.2.2 使能接口的 RMON 统计功能

需要进行流量统计的接口使能统计功能。如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

3.2.3 配置统计表

统计表中记录 RMON 收集到的接口流量信息。

3.2.4 配置历史控制表

历史数据管理功能可以设定对某个接口进行采样、保存数量和采样参数（时间间隔），定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

3.2.5 配置事件表

通过配置事件表后，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

3.2.6 配置告警表

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

3.2.7 配置扩展告警表

RMON 扩展告警表与 RMON 告警表相比增加了用表达式设定告警对象的功能。

3.2.8 检查配置结果

在配置 RMON 功能成功后，可以查看到 RMON 采集的流量信息。

3.2.1 建立配置任务

在配置 RMON 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

如果要对某一网段的网络状况进行监控、流量统计，可以配置 RMON。

对 RMON 功能的启动时间没有特殊要求，可以预先启动该功能，也可以在怀疑某个接口所连接子网的流量异常时进行配置。

推荐的做法是：预先配置好统计表，对流量有异常的端口配置两条历史控制策略，对某项指标或某几项指标有怀疑时进行告警配置，设定上下阈值，查看告警信息。

说明

RMON 只能提供一些流量统计和异常等信息，并不能防止这些信息尤其是异常情况，要消除异常还需要其它管理手段。

前置任务

在配置 RMON 之前，需完成以下任务：

- 配置以太网接口的参数
- 配置 SNMP 基本功能

数据准备

在配置 RMON 之前，需要准备以下数据：

序号	数据
1	确定要使能统计功能的接口
2	确定要使用的统计表及相关参数
3	确定要使用的历史控制表及相关参数

序号	数据
4	确定要使用的事件表及相关参数
5	确定要使用的告警表及相关参数
6	确定要使用的扩展告警表及相关参数

3.2.2 使能接口的 RMON 统计功能

需要进行流量统计的接口使能统计功能。如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

背景信息

请在需要进行流量统计的接口进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface { ethernet | gigabitethernet } interface-number**，进入接口视图。

步骤 3 执行命令 **rmon-statistics enable**，使能接口的 RMON 统计功能。

如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

----结束

3.2.3 配置统计表

统计表中记录 RMON 收集到的接口流量信息。

背景信息

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface { ethernet | gigabitethernet } interface-number**，进入接口视图。

步骤 3 执行命令 **rmon statistics entry-number [owner owner-name]**，配置统计表。

网络管理员监控设备接口的统计信息时，要为相应的接口创建一（表）行，给出接口的 OID、行索引和行的状态。此后，网络管理员可以通过读取本行的方式获取最新统计数据。

----结束

3.2.4 配置历史控制表

历史数据管理功能可以设定对某个接口进行采样、保存数量和采样参数（时间间隔），定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

背景信息

RMON 规范建议每个被监视的接口可以有 2 个以上历史控制条目，间隔 30 秒依次采样一次。

短周期取样使监视器能够探测到流量模式的突变，长周期取样则监视接口的稳定状态行为。

目前，NE20E-X6 为每个历史控制条目最多保留 10 条最近的记录，超过 10 条将循环覆盖。

说明

为减少 RMON 对系统性能的影响，历史表的采样间隔应在 10 秒以上，且不要对同一端口配置过多的历史控制表项和告警表项。

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface { ethernet | gigabitethernet } interface-number**，进入接口视图。

步骤 3 执行命令 **rmon history entry-number buckets number interval sampling-interval [owner owner-name]**，配置历史控制表。

----结束

3.2.5 配置事件表

通过配置事件表后，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

背景信息

请在需要进行监控的设备上进行如下的配置。

RMON 事件管理在事件表的指定行添加事件，并定义事件的处理方式：

- **log**: 只发送日志
- **log-trap**: 既发送日志同时也向 NMS 发送 Trap 消息
- **none**: 标记为没有事件发生
- **trap**: 只向 NMS 发送 Trap 消息

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon event** *entry-number* [**description string**] { **log** | **trap object** | **log-trap object** | **none** } [**owner owner-name**], 配置事件表。

----结束

3.2.6 配置告警表

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

背景信息

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。事件通常会记录在设备的日志表中，或向 NMS 发送 Trap。

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警（此时告警记录的状态为 **undercreation**，不是有效状态 **VALID**）。

只要事件表中配置了上限和下限其中一个事件，符合条件便会触发相应的告警（告警记录的状态为 **VALID**）。同理，如果告警变量设置错误，例如设置成一个不存在的 OID，告警记录的状态也为 **undercreation**，不会正常告警。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon alarm** *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner owner-name**], 配置告警表。

----结束

3.2.7 配置扩展告警表

RMON 扩展告警表与 RMON 告警表相比增加了用表达式设定告警对象的功能。

背景信息

在 RFC2819 的告警表基础上，RMON 扩展告警管理增加了用表达式设定告警对象的功能，并且可以限定扩展告警行的总生存时间。

扩展告警表比告警表多了以下几项：

- 扩展告警变量的表达式字符串，可以是若干简单告警变量 OID 组成的四则表达式（+，-，*，/和小括号）。
- 扩展告警行的描述字符串。
- 采样类型为变化率。
- 扩展告警状态类型，包括两种类型：永远（Forever）和限定时间（cycle）。对于 cycle 类型，当经过了扩展告警状态周期指定时间后，不再产生告警并且此表行被删除。

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警。告警记录的状态为 *undercreation*，不是有效状态 *VALID*。

只要上限和下限其中一个事件在事件表中配置了，符合条件便会触发相应的告警，告警记录的状态为 *VALID*。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon prialarm entry-number prialarm-formula description-string sampling-interval { absolute | changeratio | delta } rising-threshold threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2 entrytype { cycle entry-period | forever } [owner owner-name]**，配置扩展告警表。

----结束

3.2.8 检查配置结果

在配置 RMON 功能成功后，可以查看到 RMON 采集的流量信息。

前提条件

已经完成 RMON 功能的所有配置。

操作步骤

- 执行 **display rmon alarm [entry-number]** 命令查看 RMON 告警信息。
- 执行 **display rmon event [entry-number]** 命令查看 RMON 事件。
- 执行 **display rmon eventlog [entry-number]** 命令查看 RMON 事件日志。
- 执行 **display rmon history [ethernet interface-number | gigabitethernet interface-number]** 命令查看 RMON 历史信息。
- 执行 **display rmon prialarm [entry-number]** 命令查看 RMON 扩展告警表。
- 执行 **display rmon statistics [ethernet interface-number | gigabitethernet interface-number]** 命令查看 RMON 统计消息。

----结束

任务示例

配置成功后，执行命令 **display rmon alarm**，查看告警表的信息。

```
<HUAWEI> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
Samples absolute value : 1. 3. 6. 1. 2. 1. 16. 1. 1. 1. 6. 1 <etherStatsBroadcastPkts.1>
Sampling interval      : 30(sec)
Rising threshold       : 500(linked with event 1)
Falling threshold      : 100(linked with event 1)
When startup enables   : risingOrFallingAlarm
Latest value           : 1975
```

执行命令 **display rmon event**，查看事件表信息。

```
<HUAWEI> display rmon event
Event table 1 owned by Test300 is VALID.
```

```

Description: null.
Will cause log when triggered, last triggered at 0days 00h:24m:10s.
Event table 2 owned by Test300 is VALID.
Description: forUseofPrialarm.
Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.

```

执行命令 **display rmon eventlog**，查看事件记录的日志信息。

```

<HUAWEI> display rmon eventlog
Event table 1 owned by Test300 is VALID.
Generates eventLog 1.1 at 0days 00h:39m:30s.
Description: The 1.3.6.1.2.1.16.1.1.1.6.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.

```

执行命令 **display rmon history**，查看 RMON 历史信息。

```

<HUAWEI> display rmon history
History control entry 1 owned by Test300 is VALID,
Samples interface      : GigabitEthernet3/0/0<ifEntry.402653698>
Sampling interval      : 30(sec) with 10 buckets max.
Last Sampling time     : 0days 00h:09m:43s
Latest sampled values :
octets                 :645           , packets                 :7
broadcast packets      :7             , multicast packets      :0
undersize packets      :6             , oversize packets      :0
fragments packets      :0             , jabbers packets       :0
CRC alignment errors   :0             , collisions             :0
Dropped packet:        :0             , utilization            :0

```

执行命令 **display rmon prialarm**，查看 RMON 扩展告警表信息。

```

<HUAWEI> display rmon prialarm 1
Prialarm table 1 owned by Test300 is VALID.
Samples delta value    : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
Sampling interval      : 30(sec)
Rising threshold       : 1000(linked with event 2)
Falling threshold      : 0(linked with event 2)
When startup enables   : risingOrFallingAlarm
This entry will exist   : forever.
Latest value           : 16

```

执行命令 **display rmon statistics**，查看 RMON 统计信息。

```

<HUAWEI> display rmon statistics
Statistics entry 1 owned by Test300 is VALID.
Interface : GigabitEthernet3/0/0<ifEntry.402653698>
Received :
octets           :142915224 , packets           :1749151
broadcast packets :11603     , multicast packets :756252
undersized packets :0         , oversized packets :0
fragments packets :0         , jabbers packets   :0
CRC alignment errors:0       , collisions         :0
Dropped packet (insufficient resources):1795
Packets received according to length (octets):
64 :150183 , 65-127 :150183 , 128-255 :1383
256-511:3698 , 512-1023:0 , 1024-1518:0

```

3.3 配置 RMON2

通过 RMON2 可以实现对网络上某一接口进行流量监控，分析所有进出该接口的数据来自于哪些主机，去向哪些主机，并分别对网络上每台主机流经该接口的数据进行统计。

3.3.1 建立配置任务

在配置 RMON2 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

3.3.2 配置主机控制表

通过配置主机控制表可以实现对指定主机流量的监控。

3.3.3 配置协议目录表

RMON2 只支持以太网口的 IP 协议包的流量统计。

3.3.4 检查配置结果

在配置 RMON2 功能成功后，可以查看到 RMON2 采集的流量信息。

3.3.1 建立配置任务

在配置 RMON2 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

如果要对网络上某一接口进行流量监控，分析所有进出该接口的数据来自于哪些主机、去向哪些主机，并分别对网络上每台主机流经该接口的数据进行统计，可以通过配置 RMON2 来实现。

前置任务

在配置 RMON2 之前，需完成以下任务。

- 配置以太网接口的参数

数据准备

在配置 RMON2 之前，需要准备以下数据：

序号	数据
1	主机控制表中 hlHostControlDataSource、hlHostControlStatus 的值
2	协议目录表中 protocolDirDescr、protocolDirHostConfig 的值

3.3.2 配置主机控制表

通过配置主机控制表可以实现对指定主机流量的监控。

背景信息

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon2 hlhostcontroltable index ctrl-index [datasource interface { interface-type interface-number }] [maxentry maxentry-value] [owner owner-name] [status { active | inactive }]**，配置主机控制表。

对某一个接口进行流量统计，必须创建该接口的主机控制表条目。

索引用来判断是创建一个条目还是对已存在的条目进行修改。

创建条目时必须配置参数 **datasource interface**（即 **hlHostControlDataSource**）。每个接口在主机控制表中只能创建一行条目，不能重复创建。

当设置 **hlHostControlStatus** 的值为 **inactive** 时，会自动删除主机表中所有与其相关的条目。

当 **hlHostControlStatus** 的值是 **active** 时，不能修改 **hlHostControlDataSource** 和 **hlHostControlNIMaxDesiredEntries** 的值。

当 **hlHostControlDataSource** 对应的接口物理状态为 **Down** 时，如果 **hlHostControlStatus** 的值是 **active**，则会自动转换为 **notinservice**，在命令行下显示为 **Plug-out** 状态，在 NMS 上看到的状态为 **notinservice**。此时该行不允许用户修改，只能被删除。当接口状态变为 **UP** 时，主机控制表的状态又将恢复为 **active**。

当某行中 **hlHostControlDataSource** 对应的接口被删除时，该行也被删除。

----结束

3.3.3 配置协议目录表

RMON2 只支持以太网口的 IP 协议包的流量统计。

背景信息

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon2 protocoldir table protocol-dirid protocol-id parameter parameter-value [descr description-string] [host { notsupported | supportedon | supportedoff }] [owner owner-name] [status { active | inactive }]**，配置协议目录表。

目前，RMON2 只支持以太网口的 IP 协议包的流量统计，一种协议占一个条目，所以这个表最多只有一行。

- 当创建一个条目或将一个条目的状态（**protocolDirStatus**）设置为 **active** 时，必须同时设置 **parameter**（相当于 **protocolDirDescr**）和 **host**（相当于 **protocolDirHostConfig**）参数。
- 当 **protocolDirStatus** 设为 **active** 时，不能修改 **protocolDirDescr** 中的值。
 - 如果这时对象 **protocolDirHostConfig** 的值为 **notsupported** 时，也不能被修改为其他值。
 - 如果为非 **notsupported**，则可以在 **supportedon** 和 **supportedoff** 之间切换。
 - 当 **protocolDirHostConfig** 的值从 **supportedon** 变成 **supportedoff** 时，将删除主机控制表中对应的条目。
- 当 **protocolDirStatus** 设置为 **inactive** 时，将删除主机表中的相关条目。

----结束

3.3.4 检查配置结果

在配置 RMON2 功能成功后，可以查看到 RMON2 采集的流量信息。

前提条件

已经完成 RMON2 功能的所有配置。

操作步骤

- 执行 **display rmon2 protocoldirtable** 命令查看协议目录表信息。
- 执行 **display rmon2 hlhostcontroltable [index ctrl-index]** 命令查看控制表信息。
- 执行 **display rmon2 nlhosttable [hostcontrolindex ctrl-index] [timemark time-value] [protocoldirlocalindex protocol-local-index] [hostaddress ip-address]** 命令查看主机表信息。

----结束

任务示例

配置成功后，执行命令 **display rmon2 protocoldirtable**，查看协议目录表信息。

```
<HUAWEI> display rmon2 protocoldirtable
Info: The protocol directory table changed at time : 3days 18h:59m:49s (32758966), last time
protocolDirId      : 8.0.0.0.1.0.0.8.0
protocolDirParameters : 2.0.0
protocolDirLocalIndex : 1
protocolDirDescr    : aaa
protocolDirAddressMapConfig: notsupported
protocolDirHostConfig : supportedon
protocolDirMatrixConfig : notsupported
protocolDirOwner      :
protocolDirStatus     : active
```

执行命令 **display rmon2 hlhostcontroltable**，查看主机控制表信息。

```
<HUAWEI> display rmon2 hlhostcontroltable
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus
index datasource droppedfrm inserts Deletes maxentries owner status
123 GigabitEthernet2/2/0 0 19 0 100 China active
```

执行命令 **display rmon2 nlhosttable**，查看主机表信息。

```
<HUAWEI> display rmon2 nlhosttable hostcontrolindex 123 timemark 1000 hostaddress 10.110.99.2
Abbreviation:
HIIdx - hlHostControlIndex
PIIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIIdx PIIdx Addr InPkts OutPkts InOctes OutOctes OutMac ChgTm CrtTm
123 1 10.110.99.2 0 78 0 10046 78 81489 40859
```

3.4 维护 RMON 和 RMON2

在出现 RMON 运行故障时，请在用户视图下执行中的 **debugging** 命令对 RMON 进行测试，查看调试信息，定位故障并分析故障原因。

背景信息



说明

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 RMON 运行故障时，请在用户视图下执行中的 **debugging** 命令对 RMON 进行测试，查看调试信息，定位故障并分析故障原因。打开调试开关的操作步骤请参考《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》中“系统维护配置”的内容。有关 **debugging** 命令的解释请参考《HUAWEI NetEngine20E-X6 高端业务路由器 debugging 参考》。

操作步骤

- 在用户视图下执行命令 **debugging rmon**，打开 RMON 调试开关。
- 在用户视图下执行命令 **debugging rmon2**，打开 RMON2 调试开关。

----结束

3.5 RMON 和 RMON2 配置举例

介绍 RMON 和 RMON2 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

3.5.1 配置 RMON 示例

统计接口的流量信息，当流量超过设定值时，记录日志。

3.5.2 配置 RMON2 示例

通过配置 RMON2，实现对接口进行 IP 协议包的流量统计。

3.5.1 配置 RMON 示例

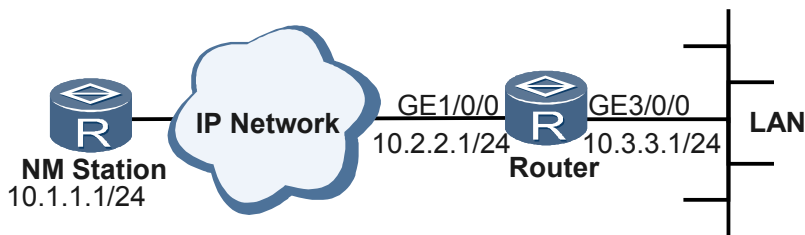
统计接口的流量信息，当流量超过设定值时，记录日志。

组网需求

如图 3-1 所示，要求对 Router 的接口 GE3/0/0 连接的子网进行监控，包括：

- 有关流量和各种类型包数量的实时和历史统计信息。
- 对此接口流量的字节数设置告警监控，当每分钟的流量超过设定值时，记录日志。
- 监控此子网的广播和组播信息流量，对该子网的组播和广播总数进行告警设置，当超过设定值时，主动向网管站 NM Station 上报告警信息。

图 3-1 配置 RMON 组网图



配置思路

采用如下的思路配置 RMON:

1. 使用 SNMP 配置命令允许发送 Trap 报文并设置相应的团体名。
2. 使能统计功能并配置统计表。
3. 配置历史控制表。
4. 配置事件表。
5. 配置告警表及扩展告警表。

数据准备

为完成此配置例，需准备如下的数据：

- 信息采样时间间隔
- 触发告警事件阈值

操作步骤

步骤 1 配置路由器和网管站路由可达（略）

步骤 2 配置允许向网管站发送 Trap

使能 SNMP 发送 Trap 的功能。

```
<HUAWEI> system-view
<HUAWEI> sysname Router
[Router] snmp-agent trap enable
[Router] snmp trap enable feature-name rmon non-excessive all
```

配置向指定的网管站发送 Trap。

```
[Router] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

步骤 3 配置统计功能

使能 RMON 接口统计功能。

```
<Router> system-view
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] rmon-statistics enable
```

配置统计表。

```
[Router-GigabitEthernet3/0/0] rmon statistics 1 owner Test300
```

步骤 4 配置历史控制表

设置 RMON 对子网中的流量信息采样，采样间隔为 30 秒钟，并保存最近 10 次数据。

```
[Router-GigabitEthernet3/0/0] rmon history 1 buckets 10 interval 30 owner Test300
```

步骤 5 配置事件表

设置 RMON 的 1 号事件处理方式为记录日志，2 号事件处理方式为向网管站发送 Trap 消息。

```
<Router> system-view
```

```
[Router] rmon event 1 log owner Test300
[Router] rmon event 2 description forUseofPriAlarm trap public owner Test300
```

步骤 6 配置告警表

设置采样间隔时间和触发告警事件 1 的阈值。

```
[Router] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold 100 1 owner Test300
```

步骤 7 配置扩展告警表

设置 RMON 对统计表中广播和组播总数每 30 秒钟进行 1 次采样，当采样变化值高于最大阈值 1000 或低于最小阈值 0 时触发事件 2，向网管站发送 Trap 信息。

```
[Router] rmon priAlarm 1 1.3.6.1.2.1.16.1.1.1.6.1+1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 30 delta rising-threshold 1000 2 falling-threshold 0 2 entrytype forever owner Test300
```

步骤 8 检测配置结果

查看配置效果。可以随时查看子网的数据流量信息。

```
<Router> display rmon statistics gigabitethernet 3/0/0
Statistics entry 1 owned by Test300 is VALID.
Interface : GigabitEthernet3/0/0<ifEntry.402653698>
Received :
octets          :142915224 , packets          :1749151
broadcast packets :11603      , multicast packets:756252
undersized packets :0          , oversized packets:0
fragments packets :0          , jabbers packets :0
CRC alignment errors:0          , collisions      :0
Dropped packet (insufficient resources):1795
Packets received according to length (octets):
64      :150183 , 65-127 :150183 , 128-255 :1383
256-511:3698   , 512-1023:0   , 1024-1518:0
```

查看配置效果。命令行方式只显示最后一次采样记录，如果要查看所有历史记录，需要使用特定网管站软件。

```
<Router> display rmon history gigabitethernet 3/0/0
History control entry 1 owned by Test300 is VALID,
Samples Interface : GigabitEthernet3/0/0<ifEntry.402653698>
Sampling interval : 30(sec) with 10 buckets max.
Last Sampling time : 0days 00h:19m:43s
Latest sampled values :
octets          :645      , packets          :7
broadcast packets :7      , multicast packets :0
undersize packets :6      , oversize packets :0
fragments packets :0      , jabbers packets :0
CRC alignment errors :0    , collisions      :0
Dropped packet: :0      , utilization      :0
History record:
Record No.1 (Sample time: 0days 00h:02m:30s)
octets          :0        , packets          :0
broadcast packets :0      , multicast packets :0
undersize packets :0      , oversize packets :0
fragments packets :0      , jabbers packets :0
CRC alignment errors :0    , collisions      :0
Dropped packet: :0        , utilization      :0
```

查看时间信息。

```
<Router> display rmon event
Event table 1 owned by Test300 is VALID.
Description: null.
Will cause log when triggered, last triggered at 0days 00h:24m:10s.
Event table 2 owned by Test300 is VALID.
Description: forUseofPriAlarm.
Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.
```

查看告警信息。

```
<Router> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
Samples absolute value : 1.3.6.1.2.1.16.1.1.1.6.1 <etherStatsBroadcastPkts.1>
Sampling interval      : 30(sec)
Rising threshold       : 500(linked with event 1)
Falling threshold      : 100(linked with event 1)
When startup enables   : risingOrFallingAlarm
Latest value           : 1975
```

查看扩展告警表信息。

```
<Router> display rmon prialarm 1
Prialarm table 1 owned by Test300 is VALID.
Samples delta value    : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
Sampling interval      : 30(sec)
Rising threshold       : 1000(linked with event 2)
Falling threshold      : 0(linked with event 2)
When startup enables   : risingOrFallingAlarm
This entry will exist   : forever.
Latest value           : 16
```

查看事件日志信息。

```
<Router> display rmon eventlog
Event table 1 owned by Test300 is VALID.
Generates eventLog 1.1 at 0days 00h:39m:30s.
Description: The 1.3.6.1.2.1.16.1.1.1.6.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

如果所设置的扩展告警变量超过预定范围，网管站可以接受到告警 Trap 信息。

----结束

配置文件

```
#
sysname Router
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.2.2.1 255.255.255.0
interface GigabitEthernet3/0/0
undo shutdown
ip address 10.3.3.1 255.255.255.0
rmon-statistics enable
rmon statistics 1 owner Test300
rmon history 1 buckets 10 interval 30 owner Test300
#
rmon event 1 description null log owner Test300
rmon event 2 description forUseofPrialarm trap public owner Test 300
rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold 100 1
owner Test300
rmon prialarm 1 .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 30 delta
rising-threshold 1000 2 falling-threshold 0 2 entrytype forever owner Test300
#
ip route-static 10.1.1.0 255.255.255.0 10.2.2.2
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF0000017C
snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
#
return
```

3.5.2 配置 RMON2 示例

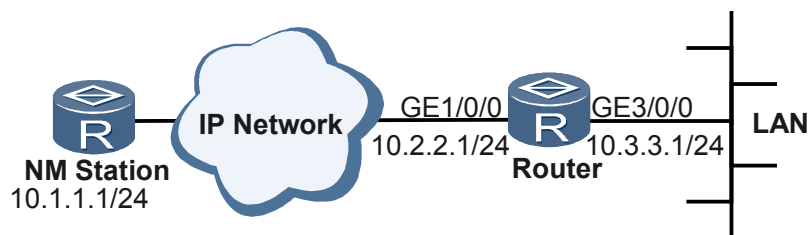
通过配置 RMON2，实现对接口进行 IP 协议包的流量统计。

组网需求

如图 3-2 所示，通过配置 RMON2，对 Router 的 GE3/0/0 接口进行 IP 协议包的流量统计。

RMON2 可以通过 NM Station 进行远程监视，也可以通过命令行配置方式进行流量监视。本例主要通过命令行配置来进行流量监视。

图 3-2 RMON2 典型配置组网图



配置思路

采用如下的思路配置 RMON2：

1. 配置主机控制表。
2. 配置协议目录表。

数据准备

为完成此配置例，需准备如下的数据：

- 主机控制表索引和主机表最大表项
- 协议 ID

操作步骤

步骤 1 配置 RMON2

配置主机控制表。设置索引为 123，并将主机表的最大条目数设为 100。

```
<HUAWEI> system-view
<HUAWEI> sysname Router
[Router] rmon2 hlhostcontroltable index 123 datasource interface gigabitethernet 3/0/0 maxentry 100
owner china status active
```

配置协议目录表。协议 ID 目前只支持 8.0.0.0.1.0.0.8.0，parameter 只支持 2.0.0，host 的值设置为 supportedon（即对该协议进行流量统计）。

```
[Router] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 descr ip host
supportedon owner china status active
```

步骤 2 检验配置结果

查看整个主机表的信息。

```
<Router> display rmon2 nlhosttable hostcontrolindex 123
Abbreviation:
HIdx - hlHostControlIndex
PIIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIIdx Addr      InPkts  OutPkts  InOctes  OutOctes  OutMac  ChgTm  CrtTm
123   1    10.110.99.2  0       78       0         10046    78      81489  40859
123   1    10.110.99.255 78      0        10046    0        0       81489  40859
```

指定 IP 地址来查看特定主机的流量。

```
<Router> display rmon2 nlhosttable hostcontrolindex 123 hostaddress 10.110.99.2
Abbreviation:
HIdx - hlHostControlIndex
PIIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIIdx Addr      InPkts  OutPkts  InOctes  OutOctes  OutMac  ChgTm  CrtTm
123   1    10.110.99.2  0       78       0         10046    78      81489  40859
```

设置时间过滤器的值，只查看符合过滤条件的条目。

```
<Router> display rmon2 nlhosttable hostcontrolindex 123 timemark 1000 hostaddress 10.110.99.2
Abbreviation:
HIdx - hlHostControlIndex
PIIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIIdx Addr      InPkts  OutPkts  InOctes  OutOctes  OutMac  ChgTm  CrtTm
123   1    10.110.99.2  0       78       0         10046    78      81489  40859
```

查看主机控制表信息，可以看到该接口上的增加主机条目数、删除的主机条目数和主机表的最大条目数。

```
<Router> display rmon2 hlhostcontroltable
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus
index datasource      droppedfrm inserts  eletes  maxentries owner  status
```

```
123  GigabitEthernet3/0/0  0          19          0          100        China  active
```

----结束

配置文件

```
#
sysname Router
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.2.1 255.255.255.0
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.3.3.1 255.255.255.0
#
rmon2 protocoltable protocolid 8.0.0.1.0.0.8.0 parameter 2.0.0 descr ip host supported on owner
china status active
rmon2 hlhostcontroltable index 123 datasource interface GigabitEthernet3/0/0 maxentry 100 owner
china status active
#
return
```


4 HGMP 配置

关于本章

通过配置 HGMP 协议，利用一台命令交换机建立集群，对加入集群的大量以太网交换机进行集中管理和配置，可以减轻工程和维护的工作量。

4.1 HGMP 简介

介绍 HGMP 的基本原理、典型组网和 NE20E-X6 系统对 HGMP 的支持。

4.2 配置 HGMP 的基本功能

通过配置 HGMP 的基本功能，可以建立或者管理一个集群。

4.3 配置 HGMP 的高级功能

介绍在建立基本的 HGMP 集群后，配置 HGMP 的一些可选特性，以进一步简化 HGMP 的管理与维护。

4.4 维护 HGMP

介绍如何清除 NDP 统计信息和监控 HGMP 集群的运行状况。

4.5 配置举例

介绍 HGMP 配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

4.1 HGMP 简介

介绍 HGMP 的基本原理、典型组网和 NE20E-X6 系统对 HGMP 的支持。

4.1.1 HGMP 概述

通过 HGMP 概述您可以了解到 HGMP 的引入原因和典型组网。

4.1.2 NE20E-X6 支持的 HGMP 特性

您可以了解到 NE20E-X6 对 HGMP 的支持情况。

4.1.1 HGMP 概述

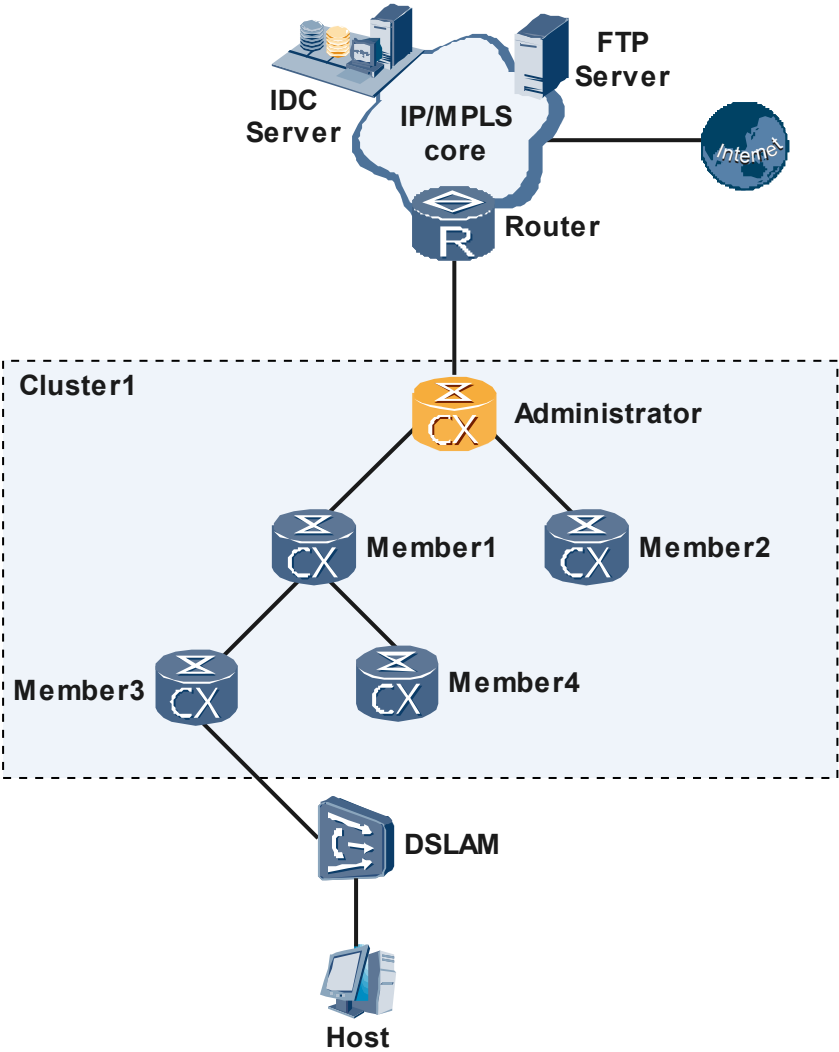
通过 HGMP 概述您可以了解到 HGMP 的引入原因和典型组网。

目前无论在城域网还是企业网中都广泛采用了以太网技术，随着网络规模的增大，在网络边缘使用大量的接入设备，由于这些设备数量巨大，又需要逐一管理维护，使管理工作非常繁琐，同时要为这些设备逐一配置 IP 地址，在目前 IP 地址资源比较紧张的情况下无疑是一种浪费。

HGMP（Huawei Group Management Protocol）即华为组管理协议，该协议是华为公司自主开发的用于管理一组以太网交换机的协议。通过 HGMP 协议，利用一台命令交换机建立集群，对加入集群的大量以太网交换机进行集中管理和配置，可以减轻工程和维护的工作量。此外由于一个集群对外只使用一个 IP 地址，这种管理方式还可以节约 IP 地址，缓解目前 IP 地址资源比较紧张的情况。

集群的基本组网图如图 4-1 和图 4-2 所示。

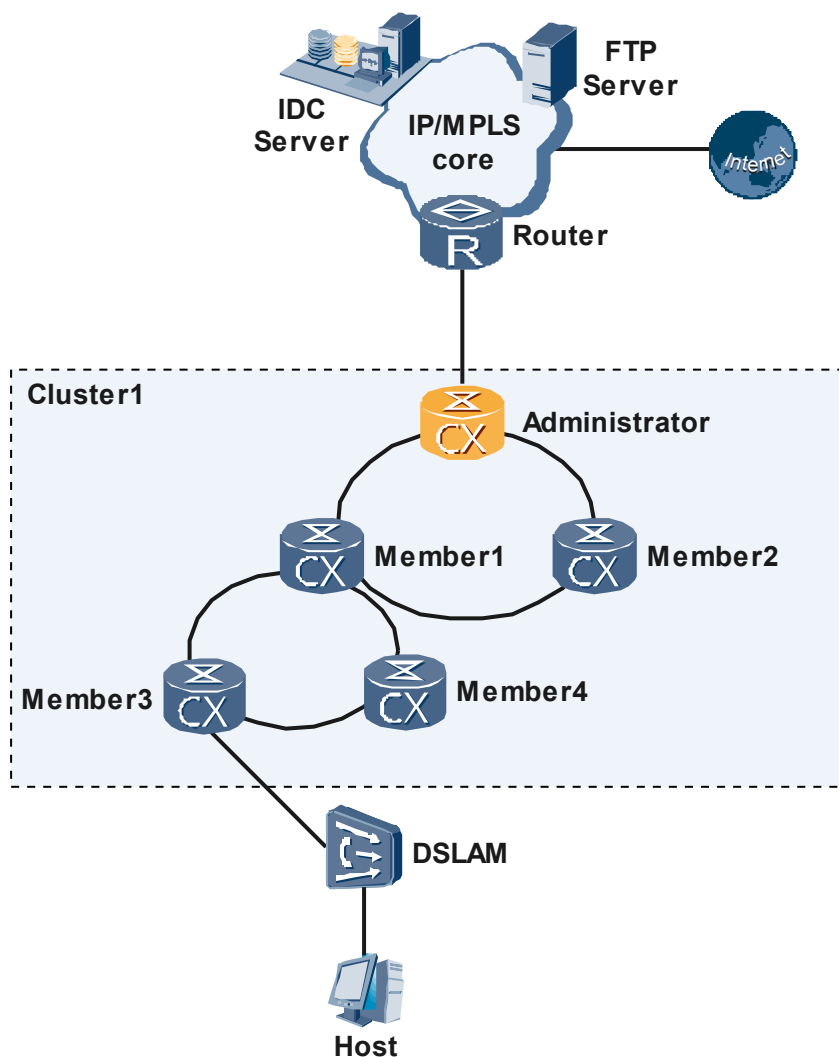
图 4-1 集群基本组网图（树型）



Administrator: 命令交换机

Member: 成员交换机

图 4-2 集群基本组网图 (RRPP)



Administrator: 命令交换机

Member: 成员交换机

4.1.2 NE20E-X6 支持的 HGMP 特性

您可以了解到 NE20E-X6 对 HGMP 的支持情况。

NDP

NDP (Neighbor Discovery Protocol) 是 HGMP 定义的邻居发现报文, 用于收集直接相连的邻居站点信息。NDP 报文收集的邻居站点信息包括设备类型、软件版本、硬件版本、连接接口、成员编号、用于集群通信的私有 IP 地址、硬件平台等信息。

说明

任何支持 HGMP 的设备都不转发 NDP 报文。

设备在本机中建立 NDP 表, 用于存储邻居站点信息。

当设备从邻居站点接收到 NDP 报文时，设备对报文内容和 NDP 表进行比较，更新相应的表项信息。

NTDP

NTDP（Network Topology Discovery Protocol）是 HGMP 定义的拓扑收集报文，用于收集网络拓扑信息。设备根据 NDP 表提供的邻居站点信息，发送和转发拓扑收集请求，在一定网络范围内收集每台设备中 NDP 表的表项。

当设备收到 NTDP 拓扑请求报文后，会立即发送 NTDP 拓扑响应报文。同时，设备根据 NTDP 转发原则，向其它接口转发接收到的 NTDP 报文。

集群角色

HGMP 定义了 4 种集群角色：命令交换机、成员交换机、候选交换机和备份交换机。

说明

目前 NE20E-X6 暂不支持备份交换机的角色。

- 命令交换机是集群中的管理设备。为保证集群内部设备与集群外部设备的正常通信，命令交换机需要设置公网 IP 地址。
- 成员交换机是集群中的成员设备。对成员交换机的管理是通过命令交换机的代理来完成的。成员交换机可以不设置公网 IP 地址。
- 候选交换机是指具有集群功能，但未加入任何集群的设备。
- 备份交换机是指集群中为命令交换机提供备份功能的设备。当命令交换机失效时，备份交换机能够自动转换为命令交换机。

用户可以通过配置来指定设备的角色，各种角色可以按一定的规则进行切换。

基本集群管理

基本集群管理主要包括以下内容：

- 建立集群管理域
- 加入成员/删除成员
- 成员状态迁移
- 集群内部通讯
- 命令交换机/候选交换机的切换
- 拓扑显示
- 修改集群管理配置
- SNMP 自动配置

NAT

HGMP 通过 NAT 实现集群内成员与公网设备的互通，并可以通过开关控制是否通过 NAT 实现互通。

- 命令交换机是集群中的管理设备。为保证集群内部设备与集群外部设备的正常通信，命令交换机需要设置公网 IP 地址。
- 为保证集群内外设备通过 NAT 互通，命令交换机上要打开指定协议的 NAT 开关。

- 集群使用的 NAT 规则由命令交换机自动配置，对从集群内访问集群外设备，成员交换机会自动获取 NAT 映射端口，对从集群外访问集群内设备，需要计算成员设备指定服务的端口号。

批量下发

HGMP 提供对所管理的成员交换机批量下发的操作，批量下发的范围包括产品大包、设备配置文件、补丁、PAF 文件和 license 文件。

- 只有命令交换机可以执行批量下发命令。
- 命令交换机上可以配置即插即用使用的 ip 地址、用户名和密码，当命令中不指定 ip 地址、用户名和密码时，将使用即插即用的 ip 地址、用户名和密码。当这两者都未配置时，命令不能执行。
- 成员交换机使用 FTP 从服务器上下载指定的文件，下载完成后，自动将文件设置为下次启动的默认值。
- 可以配置成员交换机同时进行 FTP 下载的数量，避免拥塞。

批量重启

HGMP 提供对指定的一组成员交换机批量重启。

- 批量重启时，成员交换机不会保存当前配置。
- 成员交换机收到批量重启命令后，会等待 1 秒保证控制报文在集群内充分扩散。

增量配置

在集群范围内，通常有一些成员设备有相同的配置，如创建 VLAN，打开某一特性。增量配置功能，是针对组选成员设备进行批量远程控制，1ToN 方式操作简单快捷，只需在命令设备上编辑控制命令列表，一次下发完成，并可查询各个成员设备各个控制命令的执行状况。组选方式可以是全选，根据设备类型，根据成员 ID 或根据 IP 地址。

- 增量配置只能在命令交换机上操作。
- 增量配置适应于批量成员设备统一操作场景，针对组选设备一次执行完成。
- 增量配置返回结果列表报告各成员执行情况，如遇到执行错误可针对序号找到具体执行错误的命令。
- 增量配置只保存最后一次执行结果，下一次执行下发后自动清除上次结果。
- 增量配置视图下编辑配置命令列表，命令执行和具体视图密切相关，执行顺序方法与单台设备上的一致。

同步配置文件

集群建立，并且配置好基本功能后，可以通过同步配置命令，将集群成员的配置文件保存到指定的 FTP 服务器上。

- 同步配置，需要预先指定 FTP Server。

安全特性

集群建立完成，并配置好基本功能后，可根据需求将集群网络边界关闭，将集群的可管理范围确定下来。在打开即插即用功能以及 PAF 控制 HGMP 能力设备自动打开二层口 NDP 和 NTDP 协议后，成员设备上大量二层口自动配置了 NDP 和 NTDP 协议使能，在

一些集群不相关的端口上，可不必开启这些功能。关闭不相关端口 NDP/NTDP 协议状态减少报文负担，也确保集群拓扑不再轻易变化。

- 在命令交换机上执行集群内不相关端口 NDP/NTDP 协议状态关闭开启。
- 关闭集群不相关端口 NDP 协议状态，端口上 NDP 报文不再上送。
- 关闭集群不相关端口 NTDP 协议状态，端口上 NTDP 报文不再上送。
- 在集群范围确定之后，集群的不相关端口定义为没有 NDP 邻居的端口。

即插即用

一台将要加入集群的设备，需要人工完成一些集群相关的配置。在设备数量巨大的情况下，将及其耗费人力，即插即用可以解决这个问题。预先通过 PAF 控制设备做一些集群必须的基本配置，然后，物理接入集群设备，该设备就可以自动加入集群。

- 即插即用需要 PAF 控制设备，做一些基本配置。
- 命令交换机需要使能即插即用功能。
- 命令交换机和成员相连接的端口配置，需要以 TRUNK 方式加入管理 VLAN。
- 命令交换机需要启用 NTDP 定时收集功能。

4.2 配置 HGMP 的基本功能

通过配置 HGMP 的基本功能，可以建立或者管理一个集群。

4.2.1 建立配置任务

在配置 HGMP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

4.2.2 配置 NDP

通过配置 NDP 来收集设备直接相连的邻居站点信息。

4.2.3 配置 NTDP

通过配置 NTDP 来收集网络拓扑信息。

4.2.4 创建集群

当用户需要通过集群来管理设备时，需要先创建集群。

4.2.5 添加成员交换机

当用户希望通过集群来管理某台设备，而该设备并不是该集群的成员交换机时，就可以配置增加成员交换机。

4.2.6（可选）删除或退出集群

4.2.7（可选）删除成员交换机

当用户不再需要通过集群来管理某个管理域中的某台设备时，就可以配置删除成员交换机。

4.2.8 检查配置结果

在配置 HGMP 的基本功能成功后，可以查看到已经完成的 HGMP 基本功能的配置。

4.2.1 建立配置任务

在配置 HGMP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当用户需要建立或管理一个集群时，此时可以配置 HGMP 的基本功能。

前置任务

在配置 HGMP 集群的基本功能之前，需完成以下任务：

- 设备正确上电，且工作正常
- 配置设备接口的基本属性

数据准备

在配置 HGMP 集群的基本功能之前，需要准备以下数据。

序号	数据
1	集群使用的私有 IP 地址范围
2	集群的名称
3	成员交换机的 MAC 地址
4	(可选) NDP 信息有效保留时间、NDP 报文的发送时间间隔
5	(可选) 拓扑收集范围、NTDP 拓扑请求报文转发时的跳数延迟时间和接口延迟时间、定时收集拓扑的时间间隔
6	(可选) 管理 VLAN 的 VLAN 编号、有效保留时间、握手机制定时发送时间、网管主机地址、FTP 服务器和 SFTP 服务器地址

4.2.2 配置 NDP

通过配置 NDP 来收集设备直接相连的邻居站点信息。

操作步骤

- 使能系统 NDP

请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ndp enable**，使能系统 NDP。

缺省情况下，系统 NDP 未使能。

- 使能接口 NDP

请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 这时可有两种选择：
 - 执行命令 **ndp enable interface** { *interface-type interface-number* [**to interface-type interface-number**] } <1-10>，在系统视图下使能接口 NDP。

- 执行命令 **interface interface-type interface-number**, 进入接口视图后, 再执行命令 **ndp enable**, 使能接口 NDP。
- (可选) 配置 NDP 信息的有效保留时间
请在命令交换机和成员交换机上执行下面的命令。
 1. 执行命令 **system-view**, 进入系统视图。
 2. 执行命令 **ndp timer aging aging-time**, 配置 NDP 信息的有效保留时间。
缺省情况下, NDP 信息的有效保留时间为 180 秒。NDP 信息的有效保留时间必须比 NDP 报文发送的时间间隔长。
- (可选) 配置 NDP 报文发送的时间间隔
请在命令交换机和成员交换机上执行下面的命令。
 1. 执行命令 **system-view**, 进入系统视图。
 2. 执行命令 **ndp timer hello interval**, 配置 NDP 报文发送的时间间隔。
缺省情况下, NDP 报文发送时间间隔为 60 秒。NDP 报文发送的时间间隔必须比 NDP 信息的有效保留时间短。

----结束

4.2.3 配置 NTDP

通过配置 NTDP 来收集网络拓扑信息。

操作步骤

- 使能系统 NTDP
请在命令交换机和成员交换机上执行下面的命令。
 1. 执行命令 **system-view**, 进入系统视图。
 2. 执行命令 **ntdp enable**, 使能系统 NTDP。
缺省情况下, 系统 NTDP 未使能。
- 使能接口 NTDP
请在命令交换机和成员交换机上执行下面的命令。
 1. 执行命令 **system-view**, 进入系统视图。
 2. 执行命令 **interface interface-type interface-number**, 进入接口视图。
 3. 执行命令 **ntdp enable**, 使能接口 NTDP。
- (可选) 配置拓扑收集范围
请在命令交换机和成员交换机上执行下面的命令。
 1. 执行命令 **system-view**, 进入系统视图。
 2. 执行命令 **ntdp hop max-hop-value**, 配置拓扑收集范围。
缺省情况下, 拓扑收集范围为 3。拓扑收集范围越大, 占用拓扑收集设备的内存越多。
- (可选) 配置转发 NTDP 报文的延迟时间
请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ntdp timer hop-delay hop-delay-time**，配置转发 NTDP 报文的跳数延迟时间。
3. 执行命令 **ntdp timer port-delay port-delay-time**，配置转发 NTDP 报文的接口延迟时间。

缺省情况下，NTDP 的跳数延迟时间为 200ms，NTDP 的接口延迟时间为 20ms。

- （可选）配置定时拓扑收集的时间间隔

请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ntdp timer interval**，配置定时拓扑收集的时间间隔。

缺省情况下，定时拓扑收集的时间间隔为 0 分钟，即不进行定时拓扑收集。

- （可选）启动拓扑信息收集

请在命令交换机和成员交换机上执行下面的命令。

1. 在用户视图下，执行命令 **ntdp explore**，启动拓扑信息的收集。

用户可以通过此命令随时收集网络拓扑。

----结束

4.2.4 创建集群

当用户需要通过集群来管理设备时，需要先创建集群。

操作步骤

- 配置管理 VLAN

请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan vlan-id**，创建 VLAN 并进入 VLAN 视图。

缺省情况下，设备的管理 VLAN 是 VLAN 1，且需要手工创建。

- 如果不需要更改缺省的管理 VLAN，则可不执行步骤 6 和步骤 7。此时步骤 2 中的 **vlan-id** 是“1”。
- 如果需要更改管理 VLAN 的 VLAN 编号，则步骤 2、步骤 4 和步骤 7 中的 **vlan-id** 必须相同。

3. 执行命令 **quit**，退出 VLAN 视图。
4. 执行命令 **interface vlanif vlan-id**，创建 VLANIF 并进入 VLANIF 视图。
5. 执行命令 **quit**，退出 VLANIF 视图。
6. 执行命令 **cluster**，进入集群视图。
7. 执行命令 **mngvlanid vlan-id**，配置管理 VLAN。

在命令交换机上更改管理 VLAN 的 VLAN 编号或者删除管理 VLAN 及相应的 VLANIF，则集群自动被删除。

在成员交换机上更改管理 VLAN 的 VLAN 编号或者删除管理 VLAN 及相应的 VLANIF，则成员交换机自动退出集群。

- 使能集群功能

请在命令交换机和成员交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster enable**，使能集群功能。

缺省情况下，设备上的集群功能未使能。

- 创建集群

NE20E-X6 设备提供了手动创建集群和自动创建集群两种方式。

 说明

创建 HGMP 集群后，如果重启命令交换机，那么成员交换机重新加入集群，其编号可能发生变化。

手动创建集群

下面的配置步骤只需要在一台设备上执行配置，该设备是命令交换机或者是 HGMP 集群建立后的命令交换机。

通过这种方式创建集群时，需要用户手动添加成员交换机。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **ip-pool administrator-ip-address { mask-length | mask }**，配置集群使用的 IP 地址范围。

该步骤只能在集群还没有建立时才能执行。如果集群已经建立，系统不允许修改集群使用的私有 IP 地址范围。

4. 执行命令 **build cluster-name**，设置命令交换机及集群名称并创建集群。

自动创建集群

下面的配置步骤只需要在一台设备上执行，该设备是命令交换机或者是 HGMP 集群建立后的命令交换机。

通过这种方式创建集群时，命令交换机会提示用户是否将已发现的所有的候选交换机加入集群。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **ip-pool administrator-ip-address { mask-length | mask }**，配置集群使用的 IP 地址范围。

该步骤只能在集群还没有创建时才能执行。如果集群已经创建，系统不允许修改集群 IP 地址范围。

4. 执行命令 **auto-build [recover]**，自动建立集群。

auto-build 命令还可以用于自动添加成员交换机，具体配置过程请参见“**添加成员交换机**”。

----结束

4.2.5 添加成员交换机

当用户希望通过集群来管理某台设备，而该设备并不是该集群的成员交换机时，就可以配置增加成员交换机。

背景信息

创建集群后，可以通过以下两种方法来增加成员交换机。

操作步骤

- 手动增加成员交换机

通过这种方式增加成员交换机时，需要用户手动指定成员交换机的 MAC 地址。

本配置只能在命令交换机上执行。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **add-member** [*member-number*] **mac-address** *mac-address* [**password** *password*]，增加成员交换机。

- 自动增加成员交换机

通过这种方式增加成员交换机时，命令交换机会提示用户是否将已发现的所有的候选交换机加入集群。但如果增加成员交换机的方式为验证方式时，命令交换机将退回自动增加成员交换机的操作。

本配置只能在命令交换机上执行。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **auto-build** [**recover**]，自动增加成员交换机。

auto-build 命令还可以用于自动创建集群，具体配置过程请参见“[创建集群](#)”。

recover 用来将所有成员交换机重新加入 HGMP 集群，包括在命令交换机上丢失的成员交换机。



说明
如果 HGMP 集群 A 的命令交换机认为交换机 N 不属于集群 A，但交换机 N 却认为自己属于集群 A，则交换机 N 被称为在命令交换机上丢失的成员交换机。

----结束

4.2.6 （可选）删除或退出集群

背景信息

当用户不需要通过集群来管理设备，但之前又已经创建过集群时，可以将该设备删除或退出集群。

操作步骤

- 删除集群

请在命令交换机上执行下面的命令，实现删除集群的功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入 HGMP 集群视图。
3. 执行命令 **undo build**，删除集群。

在命令交换机上执行本命令后，HGMP 集群视图下 **mngvlanid** 命令和 **ip-pool** 命令相关的配置仍存在，其它与命令交换机相关的配置将被删除。此外所有的成员交换机将自动退出集群。

- 禁用集群

请在命令交换机或者成员交换机上执行下面的命令，实现禁用集群的功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **undo cluster enable**，禁用集群。
 - 在命令交换机上执行本命令后，HGMP 集群视图下 **mngvlanid** 命令相关的配置仍存在，其它与 HGMP 集群相关的配置将被删除。此外所有的成员交换机将自动退出集群。
 - 在成员交换机上执行本命令后，该成员交换机将自动退出集群，对其他的成员交换机和命令交换机无影响。

- 退出集群

请在成员交换机上执行下面的命令，实现退出集群的功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入 HGMP 集群视图。
3. 执行命令 **undo administrator-address**，退出集群。

 说明

在成员交换机上使用 **undo administrator-address** 命令，只会使成员交换机短暂地退出集群，而不会导致命令交换机将该成员删除。如果要从一个 HGMP 集群中彻底删除成员交换机，建议用户使用 **delete-member** 命令。

----结束

4.2.7 （可选）删除成员交换机

当用户不再需要通过集群来管理某个管理域中的某台设备时，就可以配置删除成员交换机。

背景信息

当用户不再需要通过集群来管理某个管理域中的某台设备时，就可以配置删除成员交换机。

本配置只能在命令交换机上执行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cluster**，进入集群视图。

步骤 3 执行命令 **delete-member member-number**，删除成员交换机。

----结束

4.2.8 检查配置结果

在配置 HGMP 的基本功能成功后，可以查看到已经完成的 HGMP 基本功能的配置。

前提条件

已经完成 HGMP 的基本功能的所有配置。

操作步骤

- 使用命令 **display ndp**，查看系统 NDP 配置信息。
- 使用命令 **display ndp interface { interface-type interface-number [to interface-type interface-number] } <1-10>**，查看指定接口 NDP 发现的邻居信息。
- 使用命令 **display ntdp**，查看全局 NTDP 信息。
- 使用命令 **display ntdp device-list [verbose]**，查看 NTDP 收集到的设备信息。
- 使用命令 **display cluster**，查看集群状态和统计信息。
- 使用命令 **display cluster candidates [mac-address mac-address | verbose]**，查看候选交换机信息。
- 使用命令 **display cluster members [member-number | verbose]**，查看集群成员信息。

----结束

任务示例

如果 NDP 邻居正常建立，执行命令 **display ndp**，可以看到邻居节点的 MAC 地址和邻居节点的与本接口相连的接口号等信息。

```
<HUAWEI> display ndp
Neighbor discovery protocol is enabled.
Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
Interface: GigabitEthernet1/0/1
    Status: Disabled, Packets Sent: 0, Packets Received: 0, Packets Error: 0
Interface: GigabitEthernet1/0/2
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0
    Neighbor 1: Aging Time: 174(s)
        MAC Address : 0018-8203-39d8
        Port Name   : GigabitEthernet1/0/1
        Software Version: Version
        Device Name : NE20E-X6
        Port Duplex : FULL
        Product Ver : NE20E-X6
```

如果 NDP 邻居正常建立，执行命令 **display ndp interface**，可以看到邻居节点的 MAC 地址和邻居节点的与本接口相连的接口号等信息。

```
<HUAWEI> display ndp interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
    Status: Enabled, Packets Sent: 116, Packets Received: 110, Packets Error: 0
    Neighbor 1: Aging Time: 174(s)
        MAC Address : 0018-8203-39d8
        Port Name   : GigabitEthernet1/0/1
        Software Version: Version
        Device Name : NE20E-X6
        Port Duplex : FULL
        Product Ver : NE20E-X6
```

如果 NTDP 邻居正常建立，执行命令 **display ntdp**，可以看到 NTDP 的配置信息。

```
<HUAWEI> display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:462ms
```

如果 NTDP 协议收集设备信息成功，执行命令 **display ntdp device-list [verbose]**，可以看到所有设备的信息列表。

```
<HUAWEI> display ntdp device-list
The device-list of NTDP:
-----
MAC              HOP  IP              PLATFORM
-----
0004-0004-0004   2                NE20E-X6
0003-0003-0003   1                NE20E-X6
0002-0002-0002   1                NE20E-X6
0001-0001-0001   0                NE20E-X6
```

如果集群建立成功，执行命令 **display cluster**，可以看到本设备所属 HGMP 集群的信息，例如集群名称，管理 VLAN ID 等。

```
<HUAWEI_0. HUAWEI> display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.1.1.1/24
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 2 member(s) in the cluster, and 0 of them are down.
```

如果集群建立成功，执行命令 **display cluster candidates**，可以看到候选交换机的信息，例如：MAC 地址，设备类型等。

```
<HUAWEI_0. HUAWEI> display cluster candidates
MAC              HOP  IP              PLATFORM
-----
0004-0004-0004   2                NE20E-X6
0003-0003-0003   1                NE20E-X6
0002-0002-0002   1                NE20E-X6
```

如果集群建立成功，执行命令 **display cluster members**，可以看到成员交换机的信息，例如：MAC 地址，设备类型等，并且成员交换机的状态为“Up”。

```
<HUAWEI_0. HUAWEI> display cluster members
The list of cluster member:
-----
SN   Device Type      MAC Address      Status Device Name
-----
0    NE20E-X6           00e0-fcb8-d6b6   Admin  HUAWEI_0. Administrator-1
1    NE20E-X6           0018-8267-7f7d   Up      HUAWEI_1. Member-1
2    NE20E-X6           00e0-0003-0003   Up      HUAWEI_2. Member-2
```


4.3 配置 HGMP 的高级功能

介绍在建立基本的 HGMP 集群后，配置 HGMP 的一些可选特性，以进一步简化 HGMP 的管理与维护。

4.3.1 建立配置任务

在配置 HGMP 的高级功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

4.3.2 调整集群参数

为了更好的完成对集群设备的管理，可以根据需要来调整 HGMP 的参数。可以调整的参数包括：握手机制发送的时间间隔；配置有效保留时间；使能候选交换机自动加入集群的功能；配置成员交换机的老化时间；配置集群的组播地址；配置集群接口加入 VLAN 方式；配置集群公用服务器和主机。

4.3.3 利用 HGMP 管理集群中的设备

可以使用如下命令管理 HGMP 集群中的设备：配置批量下发、批量重启、即插即用，添加增量配置，同步配置文件，配置安全特性。

4.3.4 检查配置结果

4.3.1 建立配置任务

在配置 HGMP 的高级功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当用户已经建立和管理一个集群后，需要对集群的性能参数进行优化，以进一步简化 HGMP 的管理与维护，更好的管理集群中的成员交换机，此时可以配置 HGMP 的高级功能。

前置任务

在配置 HGMP 集群的高级功能之前，需完成以下任务：

- 设备正确上电，且工作正常
- 配置设备接口的基本属性
- **配置 HGMP 的基本功能**

数据准备

在配置 HGMP 的高级功能之前，需要准备以下数据。

序号	数据
1	握手机制定时发送的时间间隔
2	设备的有效保留时间
3	成员交换机的老化时间

序号	数据
4	集群的组播地址
5	集群公用的 FTP 服务器、SFTP 服务器、日志主机，网管主机地址
6	配置集群默认的 FTP 服务器信息，包括 IP 地址，用户名称和密码

4.3.2 调整集群参数

为了更好的完成对集群设备的管理，可以根据需要来调整 HGMP 的参数。可以调整的参数包括：握手机报文发送的时间间隔；配置有效保留时间；使能候选交换机自动加入集群的功能；配置成员交换机的老化时间；配置集群的组播地址；配置集群接口加入 VLAN 方式；配置集群公用服务器和主机。

操作步骤

- 配置握手机报文发送的时间间隔

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **timer interval**，配置握手机报文定时发送的时间间隔。

缺省情况下，握手机报文定时发送的时间间隔为 10 秒。该取值必须小于或等于有效保留时间的三分之一。

- 配置有效保留时间

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **holdtime hold-time**，配置设备的有效保留时间。

缺省情况下，设备的有效保留时间为 60 秒。该取值必须大于或等于握手机报文发送时间间隔的三倍。

- 使能候选交换机自动加入集群的功能

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **cluster-autojoin**，使能候选交换机自动加入集群的功能。

- 配置成员交换机的老化时间

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **cluster-discagingtime disconnect-aging-time**，配置成员交换机的老化时间。

缺省情况下，没有配置老化时间，表示不进行老化处理。

- 配置集群的组播地址

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **cluster-multimac mac-address**，配置集群的组播地址。

该组播地址的取值范围请参见《NE20E-X6 命令参考》，缺省情况下，集群的组播地址是 01-80-C2-00-00-0A。

建立集群前，需要先设置集群的组播 MAC 地址或者使用默认的组播 MAC 地址，然后再建立集群。如果默认的组播 MAC 地址已被网络中的其他业务所使用或者为了增强网络的安全性，此时可以在允许范围内，重新设置集群的组播 MAC 地址。集群一旦建立后，那么就不能再修改集群的组播 MAC 地址。同一个集群内的设备，需要配置相同的集群组播地址。

- 配置集群接口加入 VLAN 方式

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **port-tagged vlan**，配置集群通信接口以 trunk 方式加入管理 VLAN。

- 配置集群公用服务器和主机

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **ftp-server ip-address**，配置集群公用的 FTP 服务器。

 说明

集群内的成员交换机可以采用 2 种方式与集群外的 FTP 服务器互通。

- 非 NAT (Network Address Translation) 方式：这种方式下需要保证集群内的成员交换机与集群外的 FTP 服务器之间有可达的路由。
- NAT (Network Address Translation) 方式：这种方式下需要在命令交换机上的 Cluster 视图下同时配置命令 **cluster-ftp-nat enable**，来使能命令交换机的 FTP NAT 功能。集群使用的 NAT 规则由命令交换机自动配置，成员交换机会自动获取 NAT 映射端口。

缺省情况下，命令交换机的 FTP NAT 功能处于禁止状态。即集群内的成员交换机采用非 NAT 方式与集群外的 FTP 服务器互通。

集群公用的 FTP 服务器配置成功后，集群内的成员交换机可以使用命令 **cluster-ftp** 访问集群外的 FTP 服务器。

4. 执行命令 **sftp-server ip-address**，配置集群公用的 SFTP 服务器。
5. 执行命令 **snmp-host ip-address**，配置集群公用的 SNMP 主机。



说明

集群内的成员交换机可以采用 2 种方式与集群外的 SNMP 互通。

- 非 NAT (Network Address Translation) 方式: 这种方式下需要保证集群内的成员交换机与 SNMP 之间有可达的路由。
- NAT (Network Address Translation) 方式: 这种方式下需要在命令交换机上的 Cluster 视图下同时配置命令 **cluster-snmp-nat enable**, 来使能命令交换机的 SNMP NAT 功能。集群使用的 NAT 规则由命令交换机自动配置, 成员交换机会自动获取 NAT 映射端口。

缺省情况下, 命令交换机的 SNMP NAT 功能处于使能状态。即集群内的成员交换机采用 NAT 方式与集群外的 SNMP 互通。

6. 执行命令 **logging-host ip-address**, 配置集群公用的日志主机。

成员交换机将通过命令交换机来访问通过步骤 3 ~ 6 配置的服务器和主机。

步骤 3 ~ 6 是可选配置, 在执行时没有先后顺序。

缺省情况下, 集群没有公用服务器和主机。

---结束

4.3.3 利用 HGMP 管理集群中的设备

可以使用如下命令管理 HGMP 集群中的设备: 配置批量下发、批量重启、即插即用, 添加增量配置, 同步配置文件, 配置安全特性。

操作步骤

- 配置批量下发

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **cluster**, 进入集群视图。
3. (可选) 执行命令 **cluster-plug-play ip ftp-ip-address username user-name password password [path-separator pathseparator]**, 配置默认的 FTP 登录信息
配置该命令后, 批量下发会默认使用该配置中的信息。
4. (可选) 执行命令 **cluster-member ftp-timeout time**, 配置成员交换机通过 FTP 下载配置文件、版本文件或者补丁文件的超时时间。
5. 执行命令 **cluster-member [group-by { device-type device-type | ip { ip-address [to ip-address] } &<1-10> | member-number { member-number [to member-number] } &<1-10> }] get { configuration-file | system-software | patch | paf | license } file-name [ip ftp-ip-address username user-name password password] [path-separator pathseparator]**, 执行批量下发。
 - 使用 **group-by** 可在批量下发时根据不同类型筛选出指定的成员交换机组。
 - 如果没有执行步骤 3, 则命令中必须输入 IP 地址、用户名和密码。
 - 如果执行了步骤 3, 在命令中可以不输入 IP 地址、用户名和密码, 命令会默认使用步骤 3 配置的 IP 地址、用户名和密码。
 - 批量下发使用的 IP 地址为集群内部的 IP 地址。

- 配置批量重启

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. （可选）执行命令 **cluster-member reboot-timeout time**，配置成员交换机重启的超时时间。
4. 执行命令 **cluster-member reboot [group-by { device-type device-type | ip { ip-address [to ip-address] } &<1-10> | member-number { member-number [to member-number] } &<1-10> }]**，执行批量重启。

执行批量重启时不会保存设备当前配置。

- 配置即插即用

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. （可选）执行命令 **cluster-plug-play ip ftp-ip-address username user-name password password [path-separator pathseparator]**，配置默认的 FTP 登录信息。
4. 执行命令 **cluster-plug-play enable**，配置即插即用。
 - 使用 **cluster-plug-play enable** 命令前，配置命令交换机接口的管理 VLAN（此接口用于直连候选交换机），需要使用 **port trunk allow-pass vlan** 命令，而不能使用 **port default vlan** 命令。
 - 步骤 3 仅用于替换设备的场景，新设备自动下载旧设备的配置文件。前提是 FTP Server 上有旧设备的配置文件，并且新设备和旧设备的物理拓扑以及设备类型相同。

- 配置与友商互通

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **cluster-packet-extend enable**，配置与友商互通。
 - 使用 **cluster-packet-extend enable** 命令前，配置命令交换机接口的管理 VLAN（此接口用于直连候选交换机），需要使用 **port trunk allow-pass vlan** 命令，而不能使用 **port default vlan** 命令。

- 添加增量配置

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **increment**，进入集群增量配置视图。
4. 执行命令 **increment-command [command-number command-number] command-text command-text**，编辑命令列表。
5. 执行命令 **increment-run [group-by { device-type device-type | ip { ip-address [to ip-address] } &<1-10> | member-number { member-number [to member-number] } &<1-10> }]**，确认命令下发到指定成员设备。
 - 执行增量配置只保存最后一次执行结果。

- 成员组选方式可以根据成员 ID，设备类型，IP 地址或者所有。
- 编辑命令列表时，如果使用已存在的命令编号，那么会覆盖此命令编号对应的命令。
- 可以通过 **undo increment-command** { **command-number** *command-number* | **all** } 命令，删除已存在的增量配置命令。
- 可以通过 **display increment-command** 命令，查看当前已编辑的增量配置命令列表。

- 同步配置文件

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **increment-config synchronization** [**group-by** { **device-type** *device-type* | **ip** { *ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }]，把成员交换机的配置文件同步到 FTP 服务器。
 - 成员组选方式可以根据成员 ID，设备类型，IP 地址或者所有。
 - 必须集群使能后才能执行本命令。

- 配置安全特性

请在命令交换机上执行下面的命令。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cluster**，进入集群视图。
3. 执行命令 **cluster-member unrelated-port** [**group-by** { **device-type** *device-type* | **ip** { *ip-address* [**to** *ip-address*] } &<1-10> | **member-number** { *member-number* [**to** *member-number*] } &<1-10> }] { **ndp** | **ntdp** }，关闭不相关端口 NDP/NTDP 协议状态。
 - 执行此命令只保存最后一次执行的结果。
 - 成员组选方式可以根据成员 ID，设备类型，IP 地址或者所有。
 - 必须集群使能后才能执行本命令。

----结束

4.3.4 检查配置结果

前提条件

已经完成 HGMP 的高级功能的所有配置。

操作步骤

- 使用命令 **display cluster-increment-result**，查看下发增量配置的结果。
- 使用命令 **display cluster-license**，查看集群 License 的内容。
- 使用命令 **display cluster-topology-info**，查看集群拓扑信息。
- 使用命令 **display increment-command**，查看增量配置信息。
- 使用命令 **display increment-synchronization-result**，查看成员交换机的配置文件同步到 FTP 服务器的结果。

- 使用命令 **display member-getfile-state**，查看成员交换机获取配置文件、版本文件或者补丁文件的状态。
- 使用命令 **display member-interface-state { ndp | ntdp }**，查看成员交换机不相关端口 NDP 或 NTDP 的状态。
- 使用命令 **display member-reboot-state**，查看成员交换机重启的状态。
- 使用命令 **display member-save-state**，查看成员交换机保存当前配置的状态。
- 使用命令 **display synchronization-result**，查看成员交换机同步配置文件的结果。

----结束

任务示例

如果成员交换机下发增量配置成功，执行命令 **display cluster-increment-result**，可以看到结果为“success”。

```
<HUAWEI_0.HUAWEI> display cluster-increment-result
The result of member switchs executing increment commands:
```

SN	Device	MacAddress	IpAddress	Result	CommandId
2	NE20E-X6	0003-0003-0003	10.0.0.3	success	—
3	NE20E-X6	0004-0004-0004	10.0.0.4	success	—

执行命令 **display cluster-license**，可以查看集群 License 的内容，包括命令交换机最多可以管理成员交换机的数量以及成员交换机最多可以级联的层数。

```
<HUAWEI> display cluster-license
The max numbers and hops of manage member switch:
```

```
Max numbers of manage member switch: 255
Max hops of manage member switch : 16
```

执行命令 **display cluster-topology-info**，可以查看集群拓扑信息，包括正常链路、候选链路和问题链路。

```
<HUAWEI> display cluster-topology-info
The topology information about the cluster:
<-->:normal device      <+>:candidate device      <??>:lost device
```

```
Total topology node number is 5.
[HUAWEI_0.Administrator: Root-00e0-ad14-c600]
|-(GigabitEthernet1/0/2)<-->(GigabitEthernet1/0/1) [HUAWEI_3.Member-3: 00e0-dalc-4c00]
| |-(GigabitEthernet1/0/3)<-->(GigabitEthernet1/0/1) [HUAWEI_2.Member-2: 00e0-875b-8f00]
| | |-(GigabitEthernet1/0/0)<-->(GigabitEthernet1/0/0) [HUAWEI_1.Member-1: 00e0-0f68-6f00]
|-(GigabitEthernet1/0/1)<-->(GigabitEthernet1/0/2) [HUAWEI_4.Member-4: 00e0-9f7e-0b00]
```

执行命令 **display increment-command**，可以查看集群增量配置信息，包括增量配置的编号和内容。

```
<HUAWEI> display increment-command
The content of increment commands:
```

SN	Content
10	vlan batch 10 to 20
20	ip route-static 2.0.0.0 8 10.0.0.1

如果成员交换机的配置文件同步到 FTP 服务器成功，执行命令 **display increment-synchronization-result**，可以看到结果为“success”。

```
<HUAWEI> display increment-synchronization-result
```


The result of member switches' synchronization:

SN	Device	MacAddress	IpAddress	result
1	NE20E-X6	0002-0002-0002	10.0.0.2	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
3	NE20E-X6	0004-0004-0004	10.0.0.4	success

如果成员交换机获取配置文件、版本文件或者补丁文件成功，执行命令 **display member-getfile-state**，可以看到结果为“success”。

```
<HUAWEI> display member-getfile-state
The status of member switchs getting file:
```

SN	Device	MacAddress	IPAddress	Result
2	NE20E-X6	0002-0002-0002	10.0.0.2	success
3	NE20E-X6	0003-0003-0003	10.0.0.3	success

成员交换机上不需要运行 NDP 和 NTDP 协议的接口，如果使能/禁止 NDP 和 NTDP 功能成功，执行命令 **display member-interface-state**，可以看到结果为“success”。

```
<HUAWEI_0.HUAWEI> display member-interface-state ndp
The result of member switches executed disable member interface command:
```

SN	Device	MacAddress	IpAddress	result
3	NE20E-X6	0004-0004-0004	10.0.0.4	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
1	NE20E-X6	0002-0002-0002	10.0.0.2	success

```
<HUAWEI_0.HUAWEI> display member-interface-state ntdp
The result of member switches executed disable member interface command:
```

SN	Device	MacAddress	IpAddress	result
3	NE20E-X6	0004-0004-0004	10.0.0.4	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
1	NE20E-X6	0002-0002-0002	10.0.0.2	success

如果成员交换机重启成功，执行命令 **display member-reboot-state**，可以看到结果为“success”。

```
<HUAWEI> display member-reboot-state
The result of member switchs rebooting:
```

SN	Device	MacAddress	IPAddress	Result
1	NE20E-X6	0002-0002-0002	10.0.0.2	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success

如果成员交换机保存当前配置成功，执行命令 **display member-save-state**，可以看到结果为“success”。

```
<HUAWEI> display member-save-state
The result of member switchs saving:
```

SN	Device	MacAddress	IPAddress	Result
1	NE20E-X6	0002-0002-0002	10.0.0.2	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success

如果成员交换机同步配置文件到 FTP 服务器成功，执行命令 **display synchronization-result**，可以看到结果为“success”。

```
<HUAWEI> display synchronization-result
The result of member switchs' synchronization:
```

SN	Device	MacAddress	IpAddress	result
1	NE20E-X6	0002-0002-0002	10.0.0.2	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
3	NE20E-X6	0004-0004-0004	10.0.0.4	success

4.4 维护 HGMP

介绍如何清除 NDP 统计信息和监控 HGMP 集群的运行状况。

4.4.1 清除 NDP 统计信息

通过命令 `reset ndp statistics` 清除 NDP 的统计信息。

4.4.2 监控 HGMP 集群的运行状况

通过 `display` 命令监控 HGMP 的运行情况。

4.4.3 调试 HGMP

在出现 NDP、NTDP 或者集群运行故障时，请在用户视图下执行下面的 `debugging` 命令对 NDP、NTDP 或者集群进行调试，查看调试信息，定位故障并分析故障原因。

4.4.1 清除 NDP 统计信息

通过命令 `reset ndp statistics` 清除 NDP 的统计信息。

背景信息



注意

清除 NDP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 步骤 1** 在确认需要清除 NDP 的统计信息后，请在用户视图下执行 `reset ndp statistics` `[interface { interface-type interface-number [to interface-type interface-number] } <1-10>]` 命令。

----结束

4.4.2 监控 HGMP 集群的运行状况

通过 `display` 命令监控 HGMP 的运行情况。

前提条件

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 HGMP 的运行状况。

操作步骤

- 使用命令 `display ndp` 查看系统 NDP 配置信息。
- 使用命令 `display ntdp` 显示全局 NTDP 信息。

- 使用命令 **display cluster** 查看本设备所属 HGMP 集群的信息。
- 使用命令 **display ntdp device-list** [**verbose**]查看通过 NTDP 收集到的设备信息。
- 使用命令 **display cluster-topology-info** 查看集群拓扑信息。
- 使用命令 **display cluster candidates** [**mac-address mac-address** | **verbose**]查看候选交换机的信息。

----结束

4.4.3 调试 HGMP

在出现 NDP、NTDP 或者集群运行故障时，请在用户视图下执行下面的 **debugging** 命令对 NDP、NTDP 或者集群进行调试，查看调试信息，定位故障并分析故障原因。

背景信息



注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 NDP、NTDP 或者集群运行故障时，请在用户视图下执行下面的 **debugging** 命令对 NDP、NTDP 或者集群进行调试，查看调试信息，定位故障并分析故障原因。

打开调试开关的操作步骤请参考《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》中“信息中心”的内容。有关 **debugging** 命令的解释请参考《HUAWEI NetEngine20E-X6 高端业务路由器 Debugging 参考》。

操作步骤

- 使用命令 **debugging ndp packet** [**interface** { *interface-type interface-number* [*to interface-type interface-number*] } &<1-10>]，打开 NDP 调试开关。
- 使用命令 **debugging ntdp** { **all** | **data** | **error** | **message** | **packet** [**verbose**] }，打开 NTDP 调试开关。
- 使用命令 **debugging cluster** { **all** | **event** | **handshake** | **member** | **mrc** | **nat** | **packet** | **state** } 或者命令 **debugging cluster** { **packet** | **handshake** | **mrc** } [**verbose**]，打开集群调试开关。

----结束

4.5 配置举例

介绍 HGMP 配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

4.5.1 配置 HGMP 集群基本功能示例

为了有效的管理这个二层网络，可以将这个二层网络创建为一个集群，通过 HGMP 进行管理。

4.5.2 配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）

通过 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

4.5.3 配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）

可以通过非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

4.5.4 配置 HGMP 集群内外设备 SNMP 互通示例（NAT 方式）

通过 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

4.5.5 配置 HGMP 集群内外设备 SNMP 互通示例（非 NAT 方式）

通过非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

4.5.6 配置 HGMP 集群批量下发功能示例

当需要控制成员交换机从 FTP 服务器上批量下发配置文件时，进行此配置。

4.5.7 配置 HGMP 集群批量重启功能示例

在需要控制成员交换机重启时，进行此配置。

4.5.8 配置 HGMP 集群增量配置功能示例

现在需要在成员交换机创建集群，并且配置下一跳地址为命令交换机的静态路由，此时可以使用 HGMP 集群增量配置功能。

4.5.9 配置 HGMP 集群同步配置文件功能示例

需要将所有成员交换机的配置文件同步到 FTP 服务器上，此时可以配置 HGMP 集群同步配置文件功能。

4.5.10 配置 HGMP 集群安全特性示例

需要在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 和 NTDP 功能，以提高整个集群的安全性，此时可以配置 HGMP 集群安全特性。

4.5.1 配置 HGMP 集群基本功能示例

为了有效的管理这个二层网络，可以将这个二层网络创建为一个集群，通过 HGMP 进行管理。

组网需求

如图 4-3 所示，某运营商通过二层设备建立一个二层网络。本网络内的二层设备较多，不便于到现场进行维护和管理。并且，为避免浪费大量的公网 IP 地址，则不能给本网络内的每台二层设备配置一个公网 IP 地址。

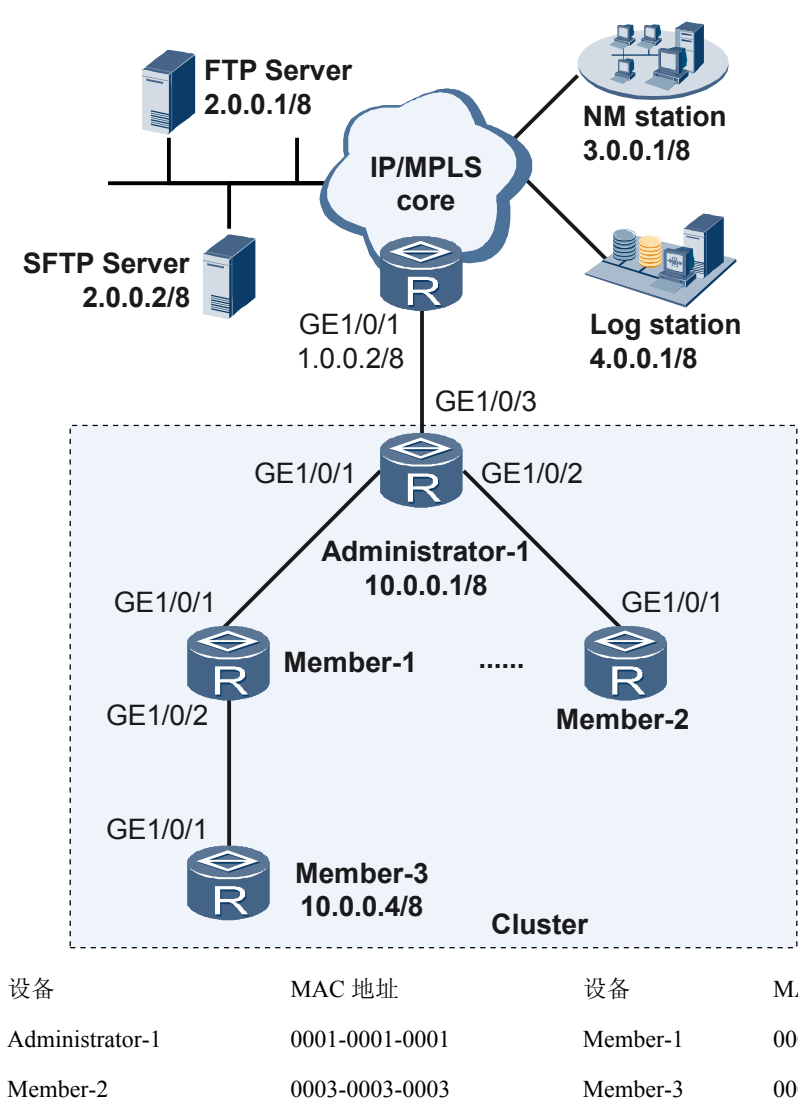
因此，为了有效的管理这个二层网络，可以将这个二层网络创建为一个集群，通过 HGMP 进行管理。

在本例中，从网络结构来说，Administrator-1 是距离管理员最近的一台设备，因此，将这台设备选为命令交换机。

说明

为方便描述，本例只选取了这个二层网络中的 4 台设备进行描述。

图 4-3 配置 HGMP 集群基本功能的组网图



配置思路

采用如下的思路配置 HGMP 集群基本功能：

1. 在所有的设备上创建管理 VLAN，并使能 NDP 和 NTDP，保证各台设备能够通过 NTDP 发现本网络的拓扑结构。
2. 选取命令交换机，并在此设备上创建集群 “HUAWEI”。
3. 将本二层网络内所有支持 HGMP 的设备都加入这个集群。
4. 指定 VLANIF10 接口的 IP 地址，以便于集群内成员交换机与集群外设备的通信。
5. 配置集群公用的服务器和主机。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- 各台设备的 MAC 地址见图 4-3。
- 各台服务器和主机的 IP 地址见图 4-3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
```

```
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
```

```

Device Name : Member-1
Port Duplex : FULL
Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。



说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```

[Administrator-1] display ntdp
Network topology discovery protocol is enabled

```

```
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004 2          NE20E-X6
0003-0003-0003 1          NE20E-X6
0002-0002-0002 1          NE20E-X6
```

步骤6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                Hops  MAC Address    DeviceType
Member-1            1     0002-0002-0002 NE20E-X6
Member-2            1     0003-0003-0003 NE20E-X6
Member-3            2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type      MAC Address      Status Device Name
-----
0    NE20E-X6          0001-0001-0001   Admin  HUAWEI_0.Administrator-1
1    NE20E-X6          0002-0002-0002   Up     HUAWEI_1.Member-1
2    NE20E-X6          0003-0003-0003   Up     HUAWEI_2.Member-2
3    NE20E-X6          0004-0004-0004   Up     HUAWEI_3.Member-3
```

步骤7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。


```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Last 0 seconds input rate 0 bits/sec, 0 packets/sec
    Last 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts
    Output:0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
```

```
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
cluster-ftp-nat enable
ftp-server 2.0.0.1
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
sysname Member-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
```

```
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-2 的配置文件

```
#
sysname Member-2
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
```

```

mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return

```

4.5.2 配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）

通过 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

组网需求

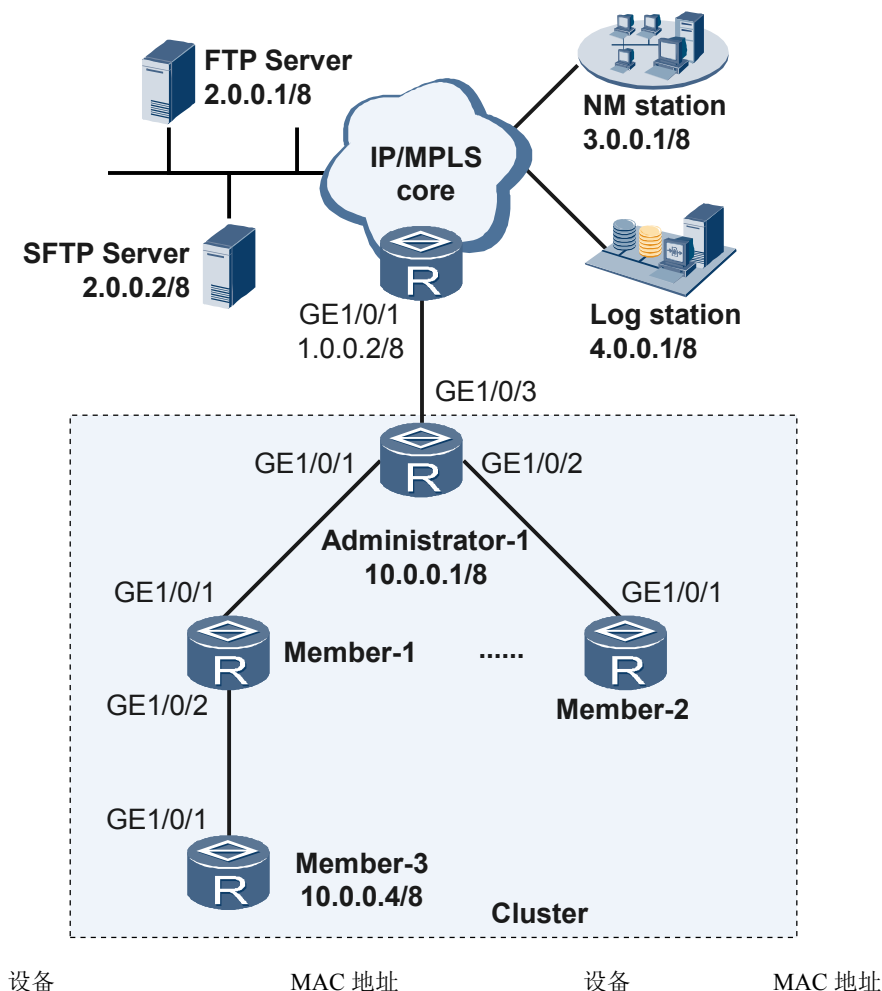
如图 4-4 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-1 的成员编号是 1，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要向 Member-1、Member-2 和 Member-3 上传文件，或从它们下载文件。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

说明

本例中采用 NAT 方式，分别以集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8），和集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）为例进行说明。

图 4-4 配置 HGMP 集群内外设备互通（NAT 方式）的典型组网图



Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通（NAT 方式）的基本功能：

1. 根据“[配置 HGMP 集群基本功能示例](#)”中的配置步骤创建和配置集群基本功能。
2. 对于集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8）：
在成员交换机上执行 **cluster-ftp** 命令与集群公用的 FTP 服务器建立连接。
3. 对于集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）：
 - 计算成员交换机 FTP 协议所使用的集群保留接口号。
 - 在 PC 上通过 FTP 客户端与成员交换机建立 FTP 连接。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，配置为集群内的 FTP 服务器。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
```

```
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
  Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
  Neighbor 1: Aging Time: 2(s)
    MAC Address : 0002-0002-0002
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
    Device Name : Member-1
    Port Duplex : FULL
    Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
  Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
  Neighbor 1: Aging Time: 5(s)
    MAC Address : 0003-0003-0003
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
    Device Name : Member-2
    Port Duplex : FULL
    Product Ver : NE20E-X6
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。



说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
```

```
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```


MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群



说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004  2          NE20E-X6
0003-0003-0003  1          NE20E-X6
0002-0002-0002  1          NE20E-X6
```

步骤 6 添加成员交换机



说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
```

```

Candidate list:
Name                Hops  MAC Address    DeviceType
Member-1            1     0002-0002-0002 NE20E-X6
Member-2            1     0003-0003-0003 NE20E-X6
Member-3            2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.

```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```

[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type      MAC Address      Status Device Name
-----
0    NE20E-X6         0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6         0002-0002-0002  Up     HUAWEI_1.Member-1
2    NE20E-X6         0003-0003-0003  Up     HUAWEI_2.Member-2
3    NE20E-X6         0004-0004-0004  Up     HUAWEI_3.Member-3

```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```

[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit

```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```

[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Last 0 seconds input rate 0 bits/sec, 0 packets/sec
Last 0 seconds output rate 0 bits/sec, 0 packets/sec
Input: 0 packets,0 bytes,
      0 unicast,0 broadcast,0 multicasts
Output:0 packets,0 bytes,
      0 unicast,0 broadcast,0 multicasts.

```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```

[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2

```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```

[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable

```

```
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
```

Cluster name:"HUAWEI"

Role:Administrator switch

management vlan id : 10

Cluster multicast MAC address : 0180-c200-000a(default)

Cluster auto-join : disabled

Handshake timer:10 sec

Handshake hold-time:60 sec

IP pool:10.0.0.1/8

Logging host:4.0.0.1

SNMP host:3.0.0.1

FTP server:2.0.0.1

SFTP server:2.0.0.2

cluster-member ftp-timeout: 300 sec(default)

Cluster SNMP NAT capability : enabled

Cluster FTP NAT capability : disabled

There are 4 member(s) in the cluster, and 0 of them are down.

步骤 10 检查配置结果

- 成员交换机通过 NAT 方式访问 FTP 服务器。

```
<HUAWEI_3.Member-3> cluster-ftp
```

```
Trying 10.0.0.1 ...
```

```
Press CTRL+K to abort
```

```
Connected to 10.0.0.1.
```

```
220 FTP service ready.
```

```
User(10.0.0.1:(none)):hgmp
```

```
331 Password required for hgmp.
```

```
Enter password:
```

```
230 User logged in.
```

```
[ftp]
```

- 集群外设备通过 NAT 方式访问集群内 FTP 服务器。

在对应的成员交换机（Member-2）上，配置 FTP 服务器。具体配置过程略，详见配置文件。

计算成员交换机 FTP 协议所使用的集群保留端口号。

Member-2 的成员编号是 2，根据“集群保留端口号的计算公式（集群保留接口号=接口号基数+成员编号*2）”，计算出 Member-2 开启 FTP 服务器时，所使用的集群保留端口号是：53248+2*2=53252。

在 PC 上执行 FTP 客户端程序，通过 NAT 方式与 Member-2 建立 FTP 连接。

 说明

NAT 方式下，集群外设备访问集群内 FTP 服务器。FTP 服务器的地址为命令交换机的管理 VLANIF 接口地址，端口号是集群保留端口号，而不是 FTP 服务通常的 21 端口。

```
ftp> open 1.0.0.1 53252
```

```
Connected to 1.0.0.1.
220 FTP service ready.
User (1.0.0.1:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
cluster-ftp-nat enable
ftp-server 2.0.0.1
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
sysname Member-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
```

```
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-2 的配置文件

```
#
sysname Member-2
#
FTP server enable
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
```

```
#
cluster
  mngvlanid 10
  administrator-address 0001-0001-0001 name HUAWEI
#
return
```

4.5.3 配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）

可以通过非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

组网需求

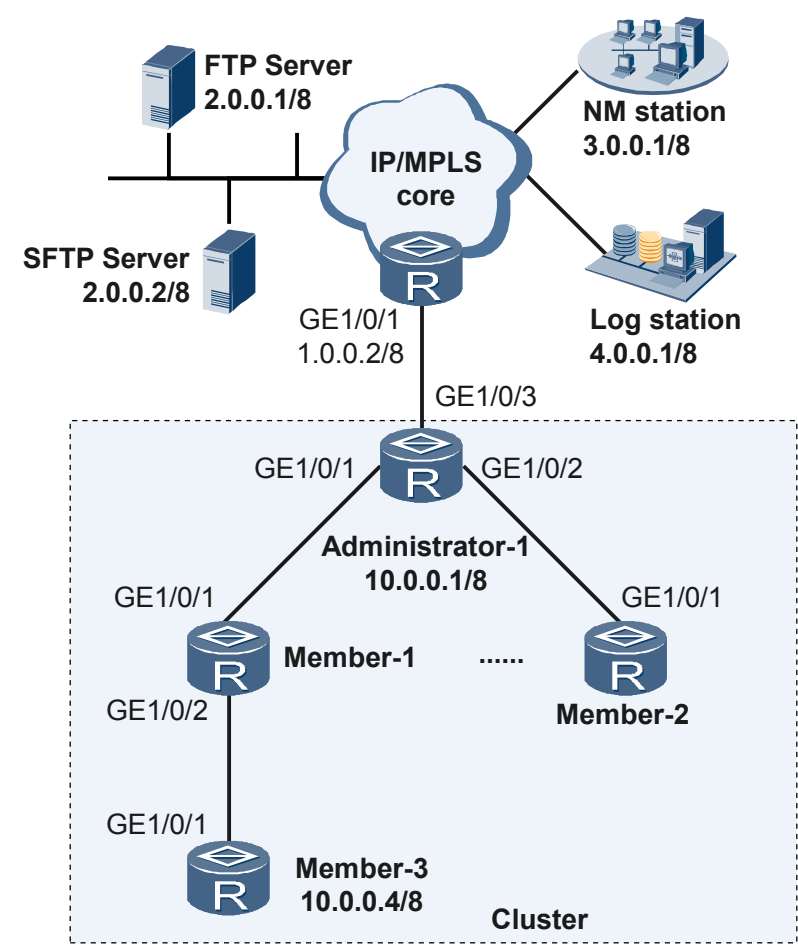
如图 4-5 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要向 Member-1、Member-2 和 Member-3 上传文件，或从它们下载文件。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外设备与成员交换机建立 FTP 连接。

说明

本例中采用非 NAT 方式，分别以集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8），和集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）为例进行说明。

图 4-5 配置 HGMP 集群内外设备互通（非 NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通示例（非 NAT 方式）的基本功能：

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建和配置集群基本功能。
2. 取消命令交换机的 FTP NAT 功能（设备默认没有使能）。

说明

集群 NAT 相关配置，必须在命令交换机上进行。

3. 在命令交换机和成员交换机上分别配置路由，使 FTP 服务器与成员交换机之间存在可达的路由。
4. 对于集群中的成员交换机 Member-3 访问集群外的 FTP 服务器（2.0.0.1/8）：
 - 在成员交换机上执行 **ftp** 命令与集群公用的 FTP 服务器建立连接。
5. 对于集群外的设备访问集群内的 FTP 服务器（成员交换机 Member-2）：

- 在 PC 上通过 FTP 客户端与成员交换机建立 FTP 连接。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，配置为集群内的 FTP 服务器。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
```



```
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
```

```

Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name   : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name   : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC              HOP  IP              PLATFORM
0004-0004-0004   2                NE20E-X6
0003-0003-0003   1                NE20E-X6
0002-0002-0002   1                NE20E-X6
```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name              Hops  MAC Address      DeviceType
Member-1          1     0002-0002-0002   NE20E-X6
Member-2          1     0003-0003-0003   NE20E-X6
Member-3          2     0004-0004-0004   NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
```

SN	Device Type	MAC Address	Status	Device Name
0	NE20E-X6	0001-0001-0001	Admin	HUAWEI_0.Administrator-1
1	NE20E-X6	0002-0002-0002	Up	HUAWEI_1.Member-1
2	NE20E-X6	0003-0003-0003	Up	HUAWEI_2.Member-2
3	NE20E-X6	0004-0004-0004	Up	HUAWEI_3.Member-3

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
  Input: 0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts
  Output:0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置成员交换机的路由，使成员交换机与 FTP 服务器之间存在可达的路由

配置成员交换机 1。

```
[HUAWEI_1.Member-1] ip route-static 2.0.0.0 8 10.0.0.1
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] ip route-static 2.0.0.0 8 10.0.0.1
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] ip route-static 2.0.0.0 8 10.0.0.1
```

 说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见[配置 HGMP 集群增量配置功能示例](#)。

步骤 10 检查配置结果

- 成员交换机通过非 NAT 方式访问 FTP 服务器。

```
< HUAWEI_3.Member-3> ftp 2.0.0.1
Trying 2.0.0.1 ...
Press CTRL+K to abort
Connected to 2.0.0.1.
220 FTP service ready.
User(2.0.0.1:(none)):hgmp
331 Password required for hgmp.
```

```
Enter password:
230 User logged in.
[ftp]
```

- 集群外设备通过非 NAT 方式访问集群内 FTP 服务器。

在对应的成员交换机（Member-2）上，配置 FTP 服务器。具体配置过程略，详见配置文件。

在 PC 上执行 FTP 客户端程序，通过非 NAT 方式与 Member-2 建立 FTP 连接。

说明

非 NAT 方式下，集群外设备访问集群内 FTP 服务器。FTP 服务器的地址为成员交换机的管理 VLANIF 接口地址，端口号是 FTP 服务通常的 21 端口。

```
ftp> open 10.0.0.2
Connected to 10.0.0.2
220 FTP service ready.
User (10.0.0.2:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 aaa
 local-user hgmp password simple hgmp
 local-user hgmp service-type ftp
 local-user hgmp ftp-directory cfcad:
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
```

```
ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

4.5.4 配置 HGMP 集群内外设备 SNMP 互通示例（NAT 方式）

通过 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

组网需求

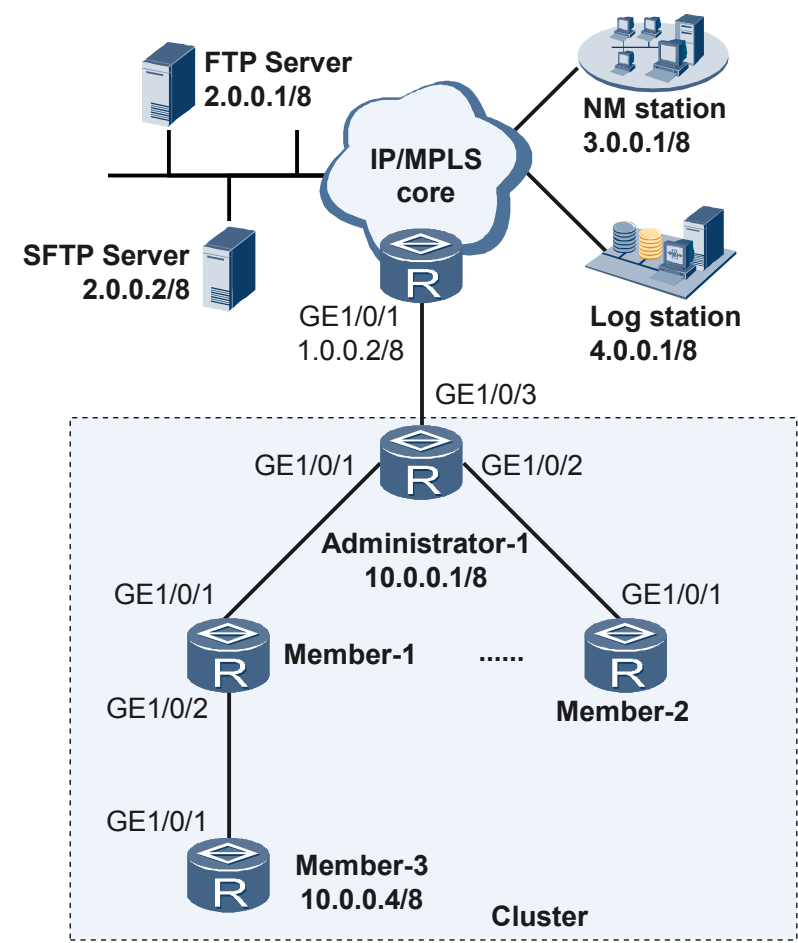
如图 4-6 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要 Member-1、Member-2 和 Member-3 向 SNMP 主机发送信息。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

说明

本例中采用 NAT 方式，以集群中的成员交换机 Member-3 访问集群外的 SNMP 主机（3.0.0.1/8）为例进行说明。

图 4-6 配置 HGMP 集群内外 SNMP 互通（NAT 方式）的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 SNMP 互通（NAT 方式）的基本功能：

- 1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建和配置集群基本功能。
- 2. 使能命令交换机的 SNMP NAT 功能（设备默认是使能的）。

说明

集群 NAT 相关配置，必须在命令交换机上进行。

- 3. 配置 SNMP 主机地址。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- SNMP 主机地址是 3.0.0.1/8。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 SNMP 主机之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
```

```
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 **Enable**。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
```

```

Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```

[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min

```

```
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
```

```

Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.

```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```

[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004  2          NE20E-X6
0003-0003-0003  1          NE20E-X6
0002-0002-0002  1          NE20E-X6

```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```

[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                      Hops  MAC Address  DeviceType
Member-1                  1     0002-0002-0002 NE20E-X6
Member-2                  1     0003-0003-0003 NE20E-X6
Member-3                  2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.

```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```

[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type          MAC Address      Status Device Name
-----
0    NE20E-X6             0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6             0002-0002-0002  Up     HUAWEI_1.Member-1
2    NE20E-X6             0003-0003-0003  Up     HUAWEI_2.Member-2
3    NE20E-X6             0004-0004-0004  Up     HUAWEI_3.Member-3

```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Last 0 seconds input rate 0 bits/sec, 0 packets/sec
    Last 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts
    Output:0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
```

```

FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.

```

步骤 10 检查配置结果

- 完成上述配置后，执行 **display current-configuration filter snmp** 命令，会看到 SNMP Agent 已经使能，其中命令交换机的 udp-domain 为 SNMP 主机的地址 3.0.0.1，成员交换机的 udp-domain 为命令交换机的地址 10.0.0.1。以命令交换机和成员交换机 3 的显示为例。

```

[HUAWEI_0.Administrator-1] display current-configuration filter snmp
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
[HUAWEI_3.Member-3] display current-configuration filter snmp
snmp-agent target-host trap address udp-domain 10.0.0.1 params securityname cluster

```

----结束

配置文件

- Administrator-1 的配置文件

```

#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return

```


- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-2 的配置文件

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
aaa
 local-user hgmp password simple hgmp
 local-user hgmp service-type ftp
 local-user hgmp ftp-directory cfcad:
#
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

4.5.5 配置 HGMP 集群内外设备 SNMP 互通示例（非 NAT 方式）

通过非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

组网需求

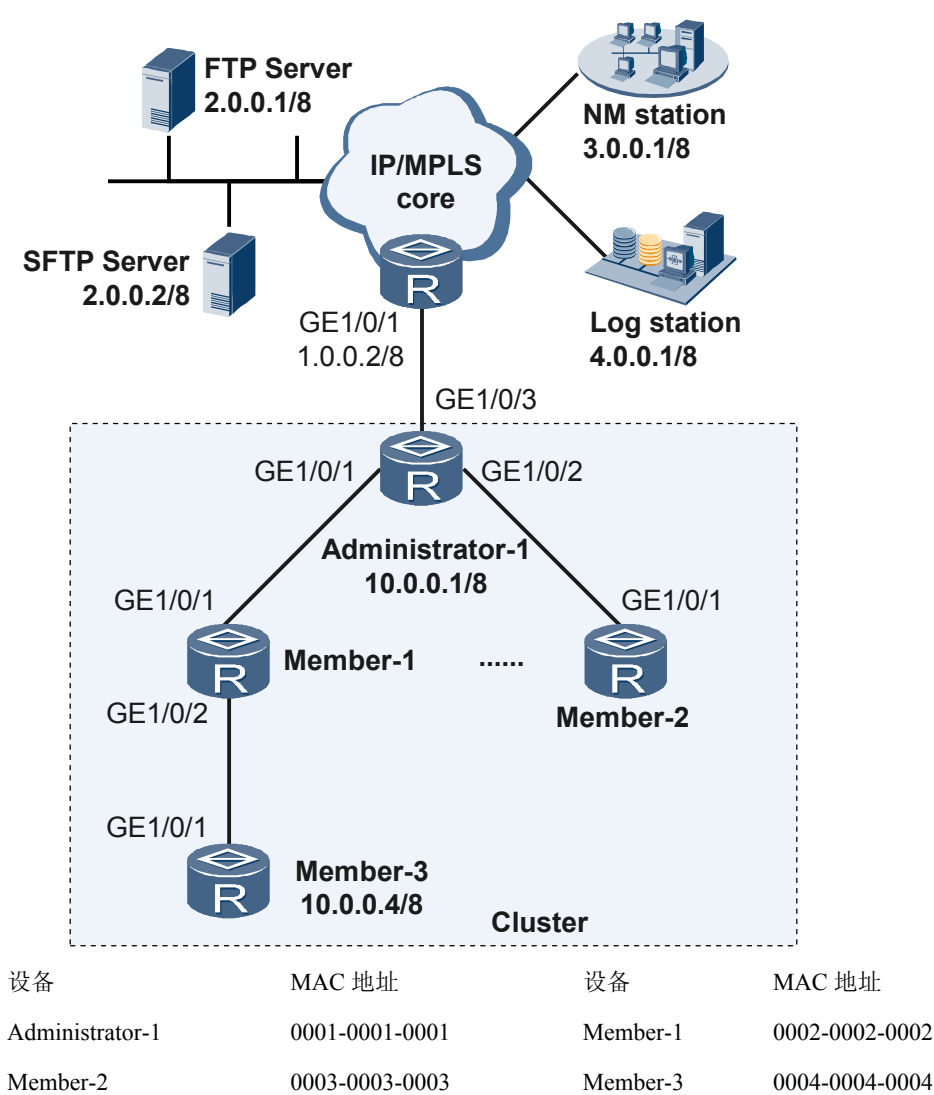
如图 4-7 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要 Member-1、Member-2 和 Member-3 向 SNMP 主机发送信息。此时，可以通过 NAT 方式或者非 NAT 方式，使集群外 SNMP 主机与成员交换机建立连接。

说明

本例中采用非 NAT 方式，以集群中的成员交换机 Member-3 访问集群外的 SNMP 主机（3.0.0.1/8）为例进行说明。

图 4-7 配置 HGMP 集群内外 SNMP 互通（非 NAT 方式）的典型组网图



配置思路

采用如下的思路配置 HGMP 集群内外设备 SNMP 互通的基本功能：

- 1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建和配置集群基本功能。
- 2. 去使能命令交换机的 SNMP NAT 功能（设备默认是使能的）。

说明

集群 NAT 相关配置，必须在命令交换机上进行。

- 3. 在命令交换机和成员交换机上分别配置路由，使 SNMP 主机与成员交换机之间存在可达的路由。
- 4. 配置 SNMP 主机地址。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- SNMP 主机地址是 3.0.0.1/8。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
```

```
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 **Enable**。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
```

```

Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```

[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min

```

```
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
```

```
Cluster name:"HUAWEI"  
Role:Administrator switch  
  
management vlan id      : 10  
Cluster multicast MAC address : 0180-c200-000a(default)  
Cluster auto-join        : disabled  
  
Handshake timer:10 sec  
Handshake hold-time:60 sec  
IP pool:10.0.0.1/8  
No logging host configured  
No SNMP host configured  
No FTP server configured  
No SFTP server configured  
cluster-member ftp-timeout: 300 sec(default)  
Cluster SNMP NAT capability : enabled  
Cluster FTP NAT capability : disabled  
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates  
MAC          HOP  IP          PLATFORM  
0004-0004-0004  2          NE20E-X6  
0003-0003-0003  1          NE20E-X6  
0002-0002-0002  1          NE20E-X6
```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build  
Collecting candidate list, please wait...  
Candidate list:  
Name              Hops  MAC Address  DeviceType  
Member-1          1     0002-0002-0002 NE20E-X6  
Member-2          1     0003-0003-0003 NE20E-X6  
Member-3          2     0004-0004-0004 NE20E-X6  
Add all to cluster?(Y/N) y  
Info: Cluster auto-build Finish!  
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members  
The list of cluster member:  
  
-----  
SN   Device Type          MAC Address      Status Device Name  
-----  
0    NE20E-X6              0001-0001-0001  Admin  HUAWEI_0.Administrator-1  
1    NE20E-X6              0002-0002-0002  Up     HUAWEI_1.Member-1  
2    NE20E-X6              0003-0003-0003  Up     HUAWEI_2.Member-2  
3    NE20E-X6              0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。


```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Last 0 seconds input rate 0 bits/sec, 0 packets/sec
    Last 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts
    Output:0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
```

```
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 取消命令交换机的 SNMP NAT 功能。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-snmp-nat enable
```

步骤 11 配置成员交换机的路由，使成员交换机与 SNMP 主机之间存在可达的路由。

配置成员交换机 1。

```
[HUAWEI_1.Member-1] ip route-static 3.0.0.0 8 10.0.0.1
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] ip route-static 3.0.0.0 8 10.0.0.1
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] ip route-static 3.0.0.0 8 10.0.0.1
```

 说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见[配置 HGMP 集群增量配置功能示例](#)。

步骤 12 配置成员交换机的 SNMP 代理功能。

配置成员交换机 1。

```
[HUAWEI_1.Member-1] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
```

配置成员交换机 2。

```
[HUAWEI_2.Member-2] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
```

配置成员交换机 3。

```
[HUAWEI_3.Member-3] snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
```

 说明

这里也可以通过增量配置，给多个成员交换机同时配置，具体配置方法请参见[配置 HGMP 集群增量配置功能示例](#)。

步骤 13 检查配置结果

完成上述配置后，执行 **display current-configuration filter snmp** 命令，会看到 SNMP Agent 已经使能，其中命令交换机和成员交换机的 udp-domain 都为 SNMP 主机的地址 3.0.0.1，以命令交换机和成员交换机 3 的显示为例。

```
[HUAWEI_0.Administrator-1] display current-configuration filter snmp
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
[HUAWEI_3.Member-3] display current-configuration filter snmp
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
```

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 undo cluster-snmp-nat enable
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
```

```

ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
snmp-agent
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return

```

- Member-2 的配置文件

```

#
sysname Member-2
#
FTP server enable
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
aaa
local-user hgmp password simple hgmp
local-user hgmp service-type ftp
local-user hgmp ftp-directory cfcad:
#
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
snmp-agent
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return

```

- Member-3 的配置文件

```

#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown

```

```
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
snmp-agent
snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname cluster
#
return
```

4.5.6 配置 HGMP 集群批量下发功能示例

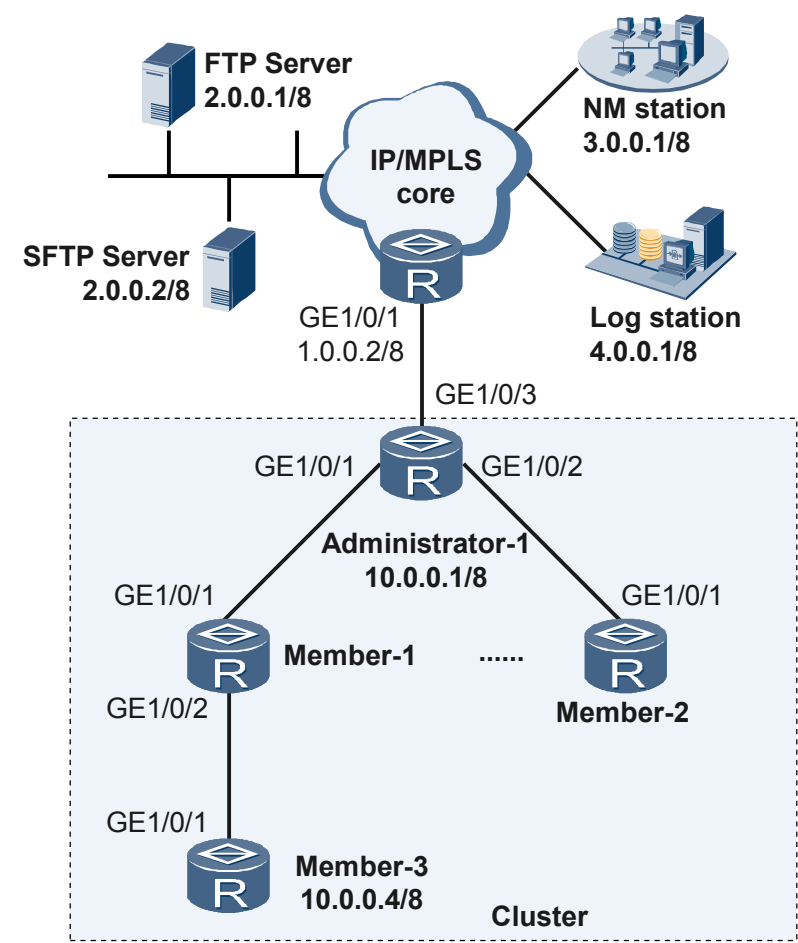
当需要控制成员交换机从 FTP 服务器上批量下发配置文件时，进行此配置。

组网需求

如图 4-8 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要控制成员交换机 Member-2、Member-3 从 FTP 服务器上批量下发配置文件。

图 4-8 配置 HGMP 集群批量下发功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群内外设备 FTP 互通（NAT 方式）的基本功能：

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建集群。
2. 配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）。

说明

- 配置 HGMP 集群内外设备 FTP 互通，可以采用 NAT 方式也可以采用非 NAT 方式。本例中采用 NAT 方式进行举例说明。
 - 如果不需要通过访问集群外部的 FTP 服务器来批量下发系统软件、补丁、PAF 文件、License 文件或者配置文件，那么此步骤可省略。
3. 在命令交换机上配置批量下发。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLAN 10 接口的 IP 地址是 10.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
```

```
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
```



```

MAC Address : 0002-0002-0002
Port Name   : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name   : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。



说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004 2          NE20E-X6
0003-0003-0003 1          NE20E-X6
0002-0002-0002 1          NE20E-X6
```

步骤 6 添加成员交换机



- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                Hops  MAC Address    DeviceType
Member-1            1     0002-0002-0002 NE20E-X6
Member-2            1     0003-0003-0003 NE20E-X6
Member-3            2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type          MAC Address      Status Device Name
-----
0    NE20E-X6              0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6              0002-0002-0002  Up      HUAWEI_1.Member-1
2    NE20E-X6              0003-0003-0003  Up      HUAWEI_2.Member-2
3    NE20E-X6              0004-0004-0004  Up      HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port, The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
  Input: 0 packets, 0 bytes,
        0 unicast, 0 broadcast, 0 multicasts
  Output: 0 packets, 0 bytes,
        0 unicast, 0 broadcast, 0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name: "HUAWEI"
Role: Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled
```

```
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 使能命令交换机的 FTP NAT 功能。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
```

步骤 11 执行批量下发

在命令交换机上执行批量下发命令，成员交换机通过 NAT 方式从 FTP 服务器（2.0.0.1）下载配置文件，并自动设置为下次启动的配置文件。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plugin-play ip 2.0.0.1 username user1 password 123
[HUAWEI_0.Administrator-1-cluster] cluster-member group-by member-number 2 to 3 get configuration-
file vrpcfg-hgmp.zip
```

步骤 12 检查配置结果

在命令交换机上执行 **display member-getfile-state** 命令，查看成员交换机获取配置文件、系统软件或者补丁文件的状态。可以看到结果是“Succeed”。

```
[HUAWEI_0.Administrator-1] display member-getfile-state
The status of member switchs getting file:
```

SN	Device	MacAddress	IPAddress	Result
2	NE20E-X6	0003-0003-0003	10.0.0.3	Succeed
3	NE20E-X6	0004-0004-0004	10.0.0.4	Succeed

在成员交换机上执行 **dir** 命令，可以看到成员交换机已经成功下载到了指定的配置文件。以 Member-2 为例。

```
<HUAWEI_2.Member-2> dir *.zip
Directory of cfcard:/
  Idx  Attr  Size(Byte)  Date      Time      FileName
    0   -rw-      1,491  Sep 03 2008 17:43:52  vrpcfg.zip
    1   -rw-       752  Aug 05 2008 15:04:36  vrpcfg-hgmp.zip
506,880 KB total (35,920 KB free)
<HUAWEI_2.Member-2> cd slave#cfcard:
<HUAWEI_2.Member-2> dir *.zip
Directory of slave#cfcard:/
  Idx  Attr  Size(Byte)  Date      Time      FileName
    0   -rw-      1,491  Sep 03 2008 17:43:54  vrpcfg.zip
    1   -rw-       752  Aug 05 2008 15:07:50  vrpcfg-hgmp.zip
503,544 KB total (34,776 KB free)
```

在成员交换机上执行 **display startup** 命令，可以看到成员交换机下次启动的配置文件的名称已改变。以 Member-2 为例。

```
<HUAWEI_2.Member-2> display startup
MainBoard:
  Configured startup system software:    cfcard:/vrpv500r006c01b100.cc
  Startup system software:               cfcard:/vrpv500r006c01b100.cc
  Next startup system software:          cfcard:/vrpv500r006c01b100.cc
  Startup saved-configuration file:      cfcard:/vrpcfg.zip
  Next startup saved-configuration file:  cfcard:/vrpcfg-hgmp.zip
```

```

Startup paf file:                cfc card:/paf.txt
Next startup paf file:          cfc card:/paf.txt
Startup license file:           cfc card:/license.txt
Next startup license file:      cfc card:/license.txt
Startup patch package:          NULL
Next startup patch package:     NULL
SlaveBoard:
Configured startup system software: cfc card:/vrpv500r006c01b100.cc
Startup system software:        cfc card:/vrpv500r006c01b100.cc
Next startup system software:    cfc card:/vrpv500r006c01b100.cc
Startup saved-configuration file: cfc card:/vrpcfg.zip
Next startup saved-configuration file: cfc card:/vrpcfg-hgmp.zip
Startup paf file:                cfc card:/paf.txt
Next startup paf file:          cfc card:/paf.txt
Startup license file:           cfc card:/license.txt
Next startup license file:      cfc card:/license.txt
Startup patch package:          NULL
Next startup patch package:     NULL

```

----结束

配置文件

- Administrator-1 的配置文件

```

#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
 return

```

- Member-1 的配置文件

```

#

```

```
sysname Member-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-2 的配置文件

```
#
sysname Member-2
#
FTP server enable
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
```

```
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

4.5.7 配置 HGMP 集群批量重启功能示例

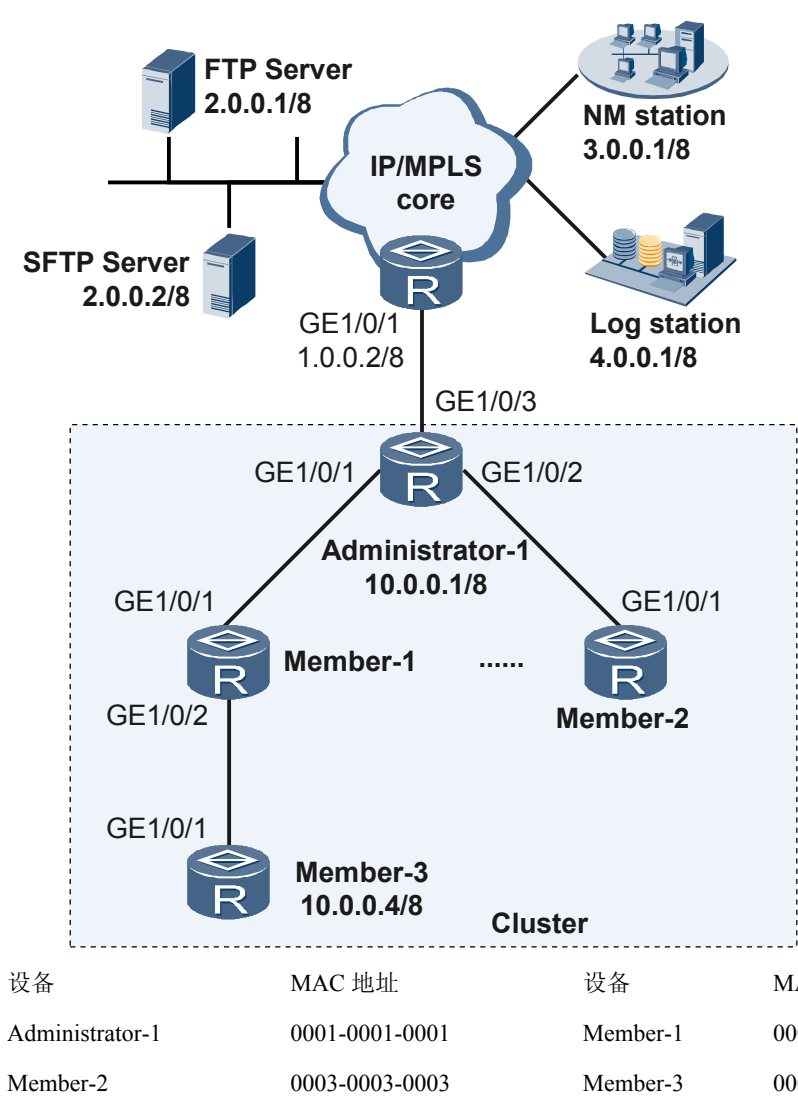
在需要控制成员交换机重启时，进行此配置。

组网需求

如图 4-9 所示，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要控制成员交换机 Member-2、Member-3 重启。

图 4-9 配置 HGMP 集群批量重启功能的典型组网图



配置思路

采用如下的思路配置 HGMP 集群批量重启的基本功能：

1. 根据“[配置 HGMP 集群基本功能示例](#)”中的配置步骤创建集群。
2. 在命令交换机上配置批量重启。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
  Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
  Neighbor 1: Aging Time: 2(s)
    MAC Address : 0002-0002-0002
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
    Device Name : Member-1
    Port Duplex : FULL
    Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
  Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
  Neighbor 1: Aging Time: 5(s)
    MAC Address : 0003-0003-0003
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
```

```
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled
```

```
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004  2          NE20E-X6
0003-0003-0003  1          NE20E-X6
0002-0002-0002  1          NE20E-X6
```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name          Hops  MAC Address  DeviceType
Member-1      1     0002-0002-0002 NE20E-X6
Member-2      1     0003-0003-0003 NE20E-X6
Member-3      2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type          MAC Address      Status Device Name
-----
0    NE20E-X6             0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6             0002-0002-0002  Up      HUAWEI_1.Member-1
2    NE20E-X6             0003-0003-0003  Up      HUAWEI_2.Member-2
3    NE20E-X6             0004-0004-0004  Up      HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
```

```
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
Input: 0 packets,0 bytes,
      0 unicast,0 broadcast,0 multicasts
Output:0 packets,0 bytes,
      0 unicast,0 broadcast,0 multicasts.
```

步骤8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 执行批量重启

在命令交换机上执行批量重启命令，重新启动设备 Member-2 和 Member-3。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-member reboot group-by member-number 2 to 3
Info: This command will take members reboot.
Are you sure?[Y/N]y
```

步骤 11 检查配置结果

等待一段时间后，在命令交换机上执行 **display member-reboot-state** 命令，查看成员交换机重启的状态。可以看到结果是“Succeed”。说明此时指定的成员交换机已经重启成功。

```
[HUAWEI_0.Administrator-1] display member-reboot-state
The result of member switchs rebooting:
```

SN	Device	MacAddress	IPAddress	Result
1	NE20E-X6	0003-0003-0003	10.0.0.3	Succeed
2	NE20E-X6	0004-0004-0004	10.0.0.4	Succeed

----结束

配置文件**● Administrator-1 的配置文件**

```
#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
cluster-ftp-nat enable
ftp-server 2.0.0.1
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
```



```
#  
return
```

- Member-1 的配置文件

```
#  
sysname Member-1  
#  
vlan batch 10  
#  
cluster enable  
ntdp enable  
ntdp hop 3  
ntdp timer 10  
ndp enable  
#  
interface Vlanif10  
#  
interface GigabitEthernet1/0/1  
undo shutdown  
portswitch  
port default vlan 10  
ntdp enable  
ndp enable  
#  
interface GigabitEthernet1/0/2  
undo shutdown  
portswitch  
port default vlan 10  
ntdp enable  
ndp enable  
#  
cluster  
mngvlanid 10  
administrator-address 0001-0001-0001 name HUAWEI  
#  
return
```

- Member-2 的配置文件

```
#  
sysname Member-2  
#  
vlan batch 10  
#  
cluster enable  
ntdp enable  
ntdp hop 3  
ntdp timer 10  
ndp enable  
#  
interface Vlanif10  
#  
interface GigabitEthernet1/0/1  
undo shutdown  
portswitch  
port default vlan 10  
ntdp enable  
ndp enable  
#  
cluster  
mngvlanid 10  
administrator-address 0001-0001-0001 name HUAWEI  
#  
return
```

- Member-3 的配置文件

```
#  
sysname Member-3  
#  
vlan batch 10
```

```
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

4.5.8 配置 HGMP 集群增量配置功能示例

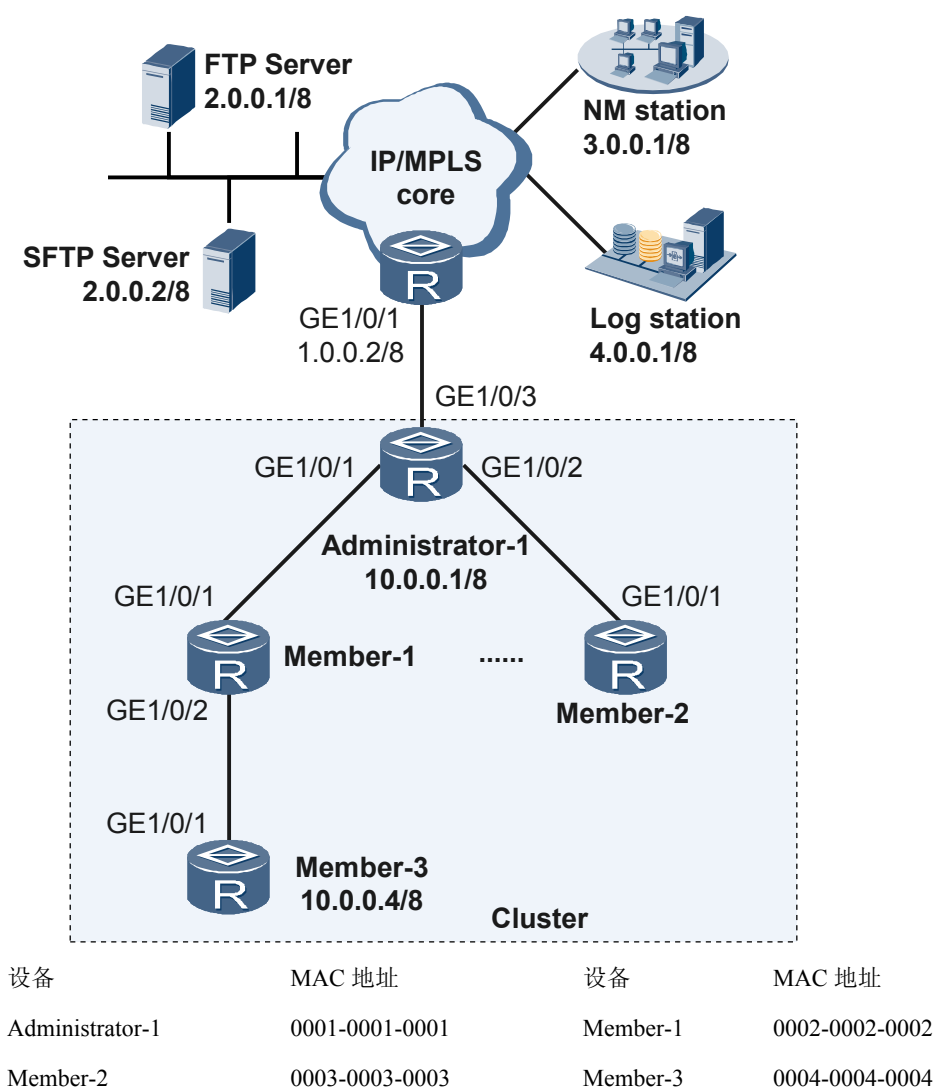
现在需要在成员交换机创建集群，并且配置下一跳地址为命令交换机的静态路由，此时可以使用 HGMP 集群增量配置功能。

组网需求

如[图 4-10](#)，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要在成员交换机 Member-2 和 Member-3 上创建 VLAN100 ~ VLAN200，并且配置下一跳地址为命令交换机的静态路由，此时可以使用 HGMP 集群增量配置功能。

图 4-10 配置 HGMP 集群增量配置功能的典型组网图



配置思路

采用如下的思路配置 HGMP 集群增量配置的基本功能：

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建集群。
2. 在命令交换机上编辑增量配置命令列表。
3. 给指定的成员交换机下发增量配置命令列表。

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8。
- 集群的地址池是 10.0.0.0/8。

- Administrator 的集群 IP 地址是 10.0.0.1/8。
- Member-2 的成员编号是 2，Member-3 的成员编号是 3。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name : GigabitEthernet1/0/1
```

```
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6
```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
```

```
Cluster auto-join      : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004  2          NE20E-X6
0003-0003-0003  1          NE20E-X6
0002-0002-0002  1          NE20E-X6
```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name              Hops  MAC Address  DeviceType
Member-1          1     0002-0002-0002  NE20E-X6
Member-2          1     0003-0003-0003  NE20E-X6
Member-3          2     0004-0004-0004  NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type      MAC Address      Status Device Name
-----
0    NE20E-X6          0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6          0002-0002-0002  Up      HUAWEI_1.Member-1
2    NE20E-X6          0003-0003-0003  Up      HUAWEI_2.Member-2
3    NE20E-X6          0004-0004-0004  Up      HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。


```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
  Input: 0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts
  Output:0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
```

There are 4 member(s) in the cluster, and 0 of them are down.

步骤 10 在命令交换机上编辑增量配置命令列表

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] increment
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number 10 command-text vlan
batch 100 to 200
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number 20 command-text ip
route-static 2.0.0.0 8 10.0.0.1
```

完成上述配置后，在命令交换机上执行 **display increment-command** 命令，可以查看增量配置命令列表。

```
[HUAWEI_0.Administrator-1] display increment-command
The content of increment commands:
```

SN	Content
10	vlan batch 100 to 200
20	ip route-static 2.0.0.0 8 10.0.0.1

步骤 11 下发增量配置命令列表

```
[HUAWEI_0.Administrator-1-cluster-increment] increment-run group-by member-number 2 to 3
```

步骤 12 检查配置结果

在命令交换机上执行 **display cluster-increment-result** 命令，查看给指定的成员交换机下发增量配置的结果。可以看到结果是“success”。

```
[HUAWEI_0.Administrator-1] display cluster-increment-result
The result of member switchs executing increment commands:
```

SN	Device	MacAddress	IpAddress	Result	CommandId
2	NE20E-X6	0003-0003-0003	10.0.0.3	success	-
3	NE20E-X6	0004-0004-0004	10.0.0.4	success	-

----结束

配置文件

● Administrator-1 的配置文件

```
#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
```

```
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
cluster-ftp-nat enable
ftp-server 2.0.0.1
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

● Member-1 的配置文件

```
#
sysname Member-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-2 的配置文件

```
#
sysname Member-2
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
```

```
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

4.5.9 配置 HGMP 集群同步配置文件功能示例

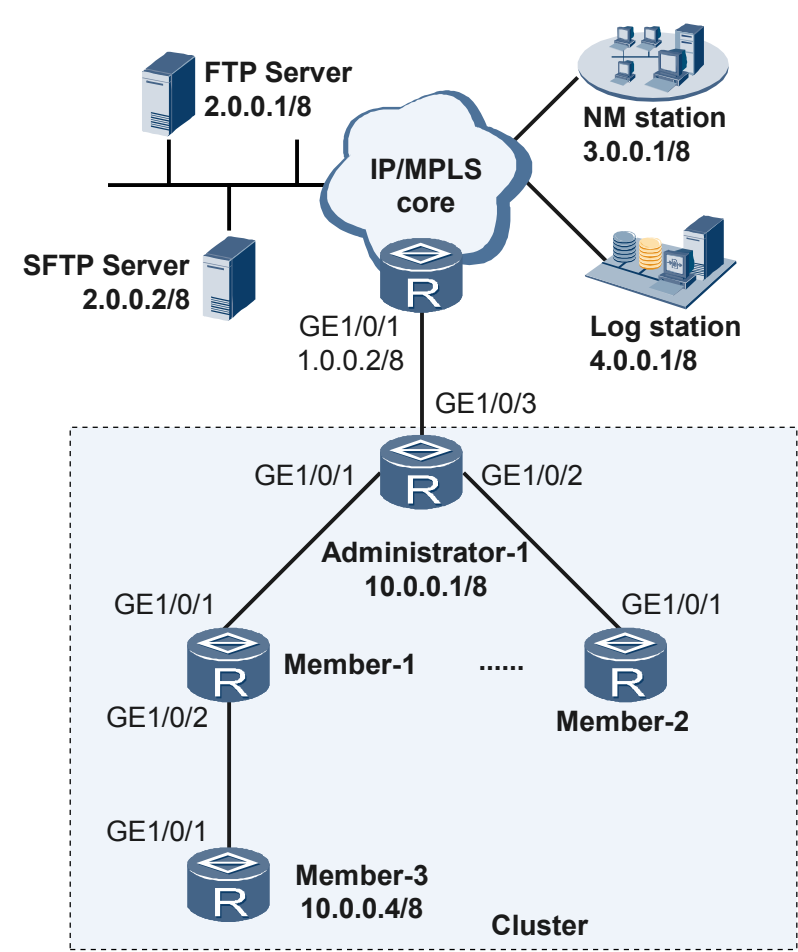
需要将所有成员交换机的配置文件同步到 FTP 服务器上，此时可以配置 HGMP 集群同步配置文件功能。

组网需求

如图 4-11，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要将所有成员交换机的配置文件同步到 FTP 服务器上，此时可以配置 HGMP 集群同步配置文件功能。

图 4-11 配置 HGMP 集群同步配置文件功能的典型组网图



设备	MAC 地址	设备	MAC 地址
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

配置思路

采用如下的思路配置 HGMP 集群同步配置文件的基本功能：

1. 根据“配置 HGMP 集群基本功能示例”中的配置步骤创建集群。
2. 配置 HGMP 集群内外设备 FTP 互通示例（NAT 方式）。

说明

- 配置 HGMP 集群内外设备 FTP 互通，可以采用 NAT 方式也可以采用非 NAT 方式。本例中采用 NAT 方式进行举例说明。
 - 如果不需要通过访问集群外部的 FTP 服务器来完成 HGMP 集群同步配置文件功能，那么此步骤可省略。
3. 在命令交换机上执行同步配置命令

数据准备

为完成此配置例，需准备如下的数据：

- 集群管理 VLAN 的 VLAN 编号是 10。
- VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
- 集群的地址池是 10.0.0.0/8。
- Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
```

```
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
Neighbor 1: Aging Time: 2(s)
MAC Address : 0002-0002-0002
Port Name : GigabitEthernet1/0/1
```

```

Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-1
Port Duplex : FULL
Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
Neighbor 1: Aging Time: 5(s)
MAC Address : 0003-0003-0003
Port Name : GigabitEthernet1/0/1
Software Version: NE20E-X6 Version V600R003C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : NE20E-X6

```

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```

[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 1。

```

[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit

```

配置成员交换机 2。

```

[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit

```

配置成员交换机 3。

```

[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit

```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```

[Administrator-1] display ntdp

```



```
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004  2          NE20E-X6
0003-0003-0003  1          NE20E-X6
0002-0002-0002  1          NE20E-X6
```

步骤 6 添加成员交换机

 说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name          Hops  MAC Address  DeviceType
Member-1      1     0002-0002-0002 NE20E-X6
Member-2      1     0003-0003-0003 NE20E-X6
Member-3      2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.
```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type      MAC Address      Status Device Name
-----
0    NE20E-X6          0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    NE20E-X6          0002-0002-0002  Up     HUAWEI_1.Member-1
2    NE20E-X6          0003-0003-0003  Up     HUAWEI_2.Member-2
3    NE20E-X6          0004-0004-0004  Up     HUAWEI_3.Member-3
```

步骤 7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port, The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
  Input: 0 packets, 0 bytes,
        0 unicast, 0 broadcast, 0 multicasts
  Output: 0 packets, 0 bytes,
        0 unicast, 0 broadcast, 0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name: "HUAWEI"
Role: Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled
```

```

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.

```

步骤 10 使能命令交换机的 FTP NAT 功能。

```

[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable

```

步骤 11 同步配置文件

在命令交换机上执行同步配置命令，成员交换机通过 NAT 方式同步配置文件到 FTP 服务器（2.0.0.1）上。

```

[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plugin-play ip 2.0.0.1 username hgmp password hgmp
[HUAWEI_0.Administrator-1-cluster] increment-config synchronization

```

步骤 12 检查配置结果

完成上述配置后，在命令交换机上执行 **display increment-synchronization-result** 命令，查看成员交换机的配置文件同步到 FTP 服务器的结果。可以看到结果是“success”。

```

[HUAWEI_0.Administrator-1] display increment-synchronization-result
The result of member switches' synchronization:

```

SN	Device	MacAddress	IpAddress	result
1	NE20E-X6	0002-0002-0002	10.0.0.2	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
3	NE20E-X6	0004-0004-0004	10.0.0.4	success

在 FTP 服务器上可以看到以成员交换机 MAC 地址命名的配置文件，配置 HGMP 集群同步配置文件成功。

----结束

配置文件

● Administrator-1 的配置文件

```

#
sysname Administrator-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
ip address 1.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch

```

```

port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
cluster-ftp-nat enable
ftp-server 2.0.0.1
sftp-server 2.0.0.2
logging-host 4.0.0.1
snmp-host 3.0.0.1
#
ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return

```

● Member-1 的配置文件

```

#
sysname Member-1
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return

```

● Member-2 的配置文件

```

#
sysname Member-2
#
FTP server enable
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5

```

```

ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return

```

- Member-3 的配置文件

```

#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return

```

4.5.10 配置 HGMP 集群安全特性示例

需要在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 和 NTDP 功能，以提高整个集群的安全性，此时可以配置 HGMP 集群安全特性。

组网需求

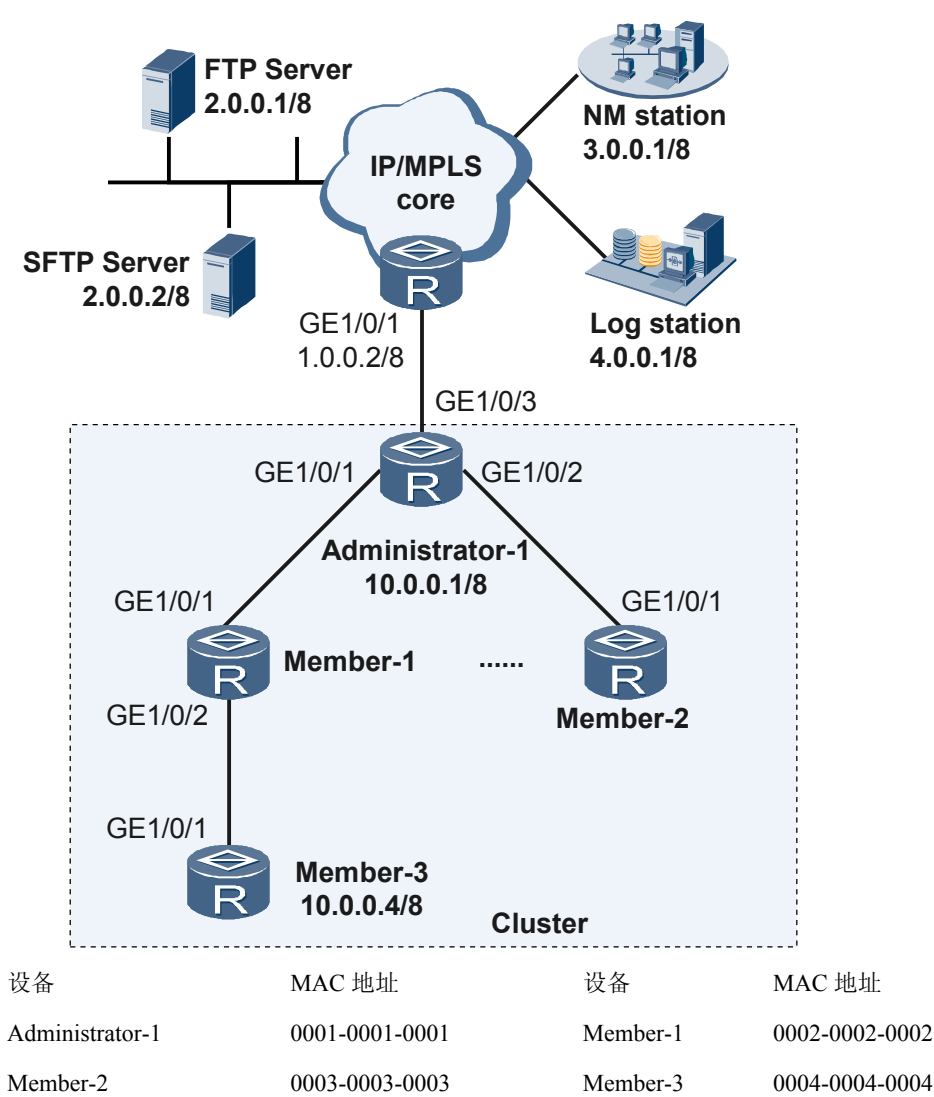
如图 4-12，所有的二层设备处于同一个集群，且 Administrator-1 是本集群的命令交换机，其他的二层设备都是成员交换机，Member-2 的成员编号是 2，Member-3 的成员编号是 3。

现在需要在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 和 NTDP 功能，以提高整个集群的安全性，此时可以配置 HGMP 集群安全特性。

说明

关闭成员交换机不相关端口的 NDP 或 NTDP 协议后，新的候选交换机接入成员交换机的不相关接口，新的候选交换机不能加入该集群。除非重新使能该成员交换机的不相关端口的 NDP 或 NTDP 协议。

图 4-12 配置 HGMP 集群安全特性的典型组网图



配置思路

- 采用如下的思路配置 HGMP 集群安全特性的基本功能：
1. 根据“[配置 HGMP 集群基本功能示例](#)”中的配置步骤创建集群。
 2. 在命令交换机上运行关闭成员交换机不相关端口的 NDP 和 NTDP 协议的命令。

数据准备

- 为完成此配置例，需准备如下的数据：
- 集群管理 VLAN 的 VLAN 编号是 10。
 - VLANIF 10 接口的 IP 地址是 1.0.0.1/8，且与 FTP 服务器之间有可达的路由。
 - 集群的地址池是 10.0.0.0/8。
 - Administrator 的集群 IP 地址是 10.0.0.1/8。

操作步骤

步骤 1 配置管理 VLAN

在设备上创建 VLAN 10，并把命令交换机和成员交换机的接口加入此 VLAN 中。

配置命令交换机。

```
<HUAWEI> system-view
[HUAWEI] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] undo shutdown
[Administrator-1-GigabitEthernet1/0/1] portswitch
[Administrator-1-GigabitEthernet1/0/1] port default vlan 10
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] undo shutdown
[Administrator-1-GigabitEthernet1/0/2] portswitch
[Administrator-1-GigabitEthernet1/0/2] port default vlan 10
[Administrator-1-GigabitEthernet1/0/2] quit
[Administrator-1] interface gigabitethernet 1/0/3
[Administrator-1-GigabitEthernet1/0/3] undo shutdown
[Administrator-1-GigabitEthernet1/0/3] portswitch
[Administrator-1-GigabitEthernet1/0/3] port default vlan 10
[Administrator-1-GigabitEthernet1/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

配置成员交换机 1。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] undo shutdown
[Member-1-GigabitEthernet1/0/1] portswitch
[Member-1-GigabitEthernet1/0/1] port default vlan 10
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] undo shutdown
[Member-1-GigabitEthernet1/0/2] portswitch
[Member-1-GigabitEthernet1/0/2] port default vlan 10
[Member-1-GigabitEthernet1/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

配置成员交换机 2。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] undo shutdown
[Member-2-GigabitEthernet1/0/1] portswitch
[Member-2-GigabitEthernet1/0/1] port default vlan 10
[Member-2-GigabitEthernet1/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

配置成员交换机 3。

```
<HUAWEI> system-view
[HUAWEI] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
```



```
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] undo shutdown
[Member-3-GigabitEthernet1/0/1] portswitch
[Member-3-GigabitEthernet1/0/1] port default vlan 10
[Member-3-GigabitEthernet1/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

步骤 2 配置 NDP

在设备上使能系统 NDP 和接口的 NDP 功能。

配置命令交换机。

```
[Administrator-1] ndp enable
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ndp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ndp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ndp enable
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ndp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ndp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ndp enable
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ndp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ndp enable
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ndp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看 NDP 的信息，可以看到接口的 NDP 状态为 Enable。Device Name 为邻居节点的主机名。Port Name 为邻居节点的与本接口相连的接口名称。

```
[Administrator-1] display ndp interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/1
  Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
  Neighbor 1: Aging Time: 2(s)
    MAC Address : 0002-0002-0002
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
    Device Name : Member-1
    Port Duplex : FULL
    Product Ver : NE20E-X6
Interface: GigabitEthernet1/0/2
  Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
  Neighbor 1: Aging Time: 5(s)
    MAC Address : 0003-0003-0003
    Port Name   : GigabitEthernet1/0/1
    Software Version: NE20E-X6 Version V600R003C00
    Device Name : Member-2
    Port Duplex : FULL
```

Product Ver : NE20E-X6

步骤 3 配置 NTDP

在设备上使能系统 NTDP 和接口的 NTDP 功能、并配置 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。



说明

NTDP 的拓扑收集范围的大小，由 PAF 文件决定。

配置命令交换机。

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface gigabitethernet 1/0/1
[Administrator-1-GigabitEthernet1/0/1] ntdp enable
[Administrator-1-GigabitEthernet1/0/1] quit
[Administrator-1] interface gigabitethernet 1/0/2
[Administrator-1-GigabitEthernet1/0/2] ntdp enable
[Administrator-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 1。

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface gigabitethernet 1/0/1
[Member-1-GigabitEthernet1/0/1] ntdp enable
[Member-1-GigabitEthernet1/0/1] quit
[Member-1] interface gigabitethernet 1/0/2
[Member-1-GigabitEthernet1/0/2] ntdp enable
[Member-1-GigabitEthernet1/0/2] quit
```

配置成员交换机 2。

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface gigabitethernet 1/0/1
[Member-2-GigabitEthernet1/0/1] ntdp enable
[Member-2-GigabitEthernet1/0/1] quit
```

配置成员交换机 3。

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface gigabitethernet 1/0/1
[Member-3-GigabitEthernet1/0/1] ntdp enable
[Member-3-GigabitEthernet1/0/1] quit
```

完成上述配置后，在命令交换机上查看全局 NTDP 配置信息，可以看到 NTDP 的定时拓扑收集时间是 10 分钟、NTDP 的拓扑收集范围是 3 跳。

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0ms
```

步骤 4 使能集群功能和配置管理 VLAN

配置命令交换机。

```
[Administrator-1] cluster enable
```

```
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

配置成员交换机 1。

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

配置成员交换机 2。

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

配置成员交换机 3。

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

在命令交换机上手动启动收集拓扑信息后，查看通过 NTDP 收集到的设备信息，可以看到相关设备的 MAC 和型号。

```
<Administrator-1> ntdp explore
<Administrator-1> display ntdp device-list
The device-list of NTDP:
```

MAC	HOP	IP	PLATFORM
0004-0004-0004	2		NE20E-X6
0003-0003-0003	1		NE20E-X6
0002-0002-0002	1		NE20E-X6
0001-0001-0001	0		NE20E-X6

步骤 5 创建集群

 说明

本配置步骤只能在命令交换机上执行。

在命令交换机上配置集群使用的 IP 地址范围是 10.0.0.0/8，其中，为命令交换机分配的 IP 地址是 10.0.0.1/8。

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

在命令交换机上创建名称为“HUAWEI”的集群。

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

完成上述配置后，在命令交换机上查看设备所属集群的信息。可以看到，设备名称已经改变，Cluster name 是 HUAWEI。Management VLAN ID 为 10。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
```

```

Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.

```

在命令交换机上查看候选交换机的信息，可以看到所有的候选交换机以及型号。

```

[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC          HOP  IP          PLATFORM
0004-0004-0004 2          NE20E-X6
0003-0003-0003 1          NE20E-X6
0002-0002-0002 1          NE20E-X6

```

步骤6 添加成员交换机

说明

- 本配置步骤只能在命令交换机上执行。
- 本配置举例采用自动添加成员交换机的方式。如果需要手动添加成员交换机，请参见“[添加成员交换机](#)”。

将所有候选交换机加入集群。

```

[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                Hops  MAC Address    DeviceType
Member-1            1     0002-0002-0002 NE20E-X6
Member-2            1     0003-0003-0003 NE20E-X6
Member-3            2     0004-0004-0004 NE20E-X6
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully.

```

完成上述配置后，在命令交换机上查看集群内命令交换机和成员交换机的信息。可以看到所有的成员交换机都已加入。并且 Status 为 Up。

```

[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-----
SN   Device Type          MAC Address      Status Device Name
-----
0    NE20E-X6              0001-0001-0001  Admin HUAWEI_0.Administrator-1
1    NE20E-X6              0002-0002-0002  Up    HUAWEI_1.Member-1
2    NE20E-X6              0003-0003-0003  Up    HUAWEI_2.Member-2
3    NE20E-X6              0004-0004-0004  Up    HUAWEI_3.Member-3

```

步骤7 配置 VLANIF 10 接口的 IP 地址

为了保证集群内成员交换机与集群外设备的正常通信，需要给命令交换机的 VLANIF 10 接口指定 IP 地址。

配置 VLANIF 10 接口的 IP 地址。

```

[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit

```

完成上述配置后，在命令交换机上查看接口状态，可以看到接口的状态为 UP。

```

[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP

```

```
Line protocol current state : UP
Last line protocol up time : 2010-06-28 21:25:52
Description:HUAWEI, HUAWEI Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 ClusterIP Sending Frames' Format is PKTFMT_ETHNT_
2, Hardware address is 0001-0001-0001
Physical is VLANIF
Current system time: 2010-07-01 14:37:11-08:00
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Last 0 seconds input rate 0 bits/sec, 0 packets/sec
  Last 0 seconds output rate 0 bits/sec, 0 packets/sec
  Input: 0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts
  Output:0 packets,0 bytes,
        0 unicast,0 broadcast,0 multicasts.
```

步骤 8 配置命令交换机的静态路由

配置静态路由的目的是保证集群设备与各服务器和主机之间有可达路由，也可以使用动态路由。

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

步骤 9 配置集群的公用服务器和主机

配置 FTP 服务器。

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

配置 SFTP 服务器。

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

配置 SNMP 的网管主机。

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

配置日志主机。

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

完成上述配置后，在命令交换机上查看本设备所属集群的信息，可以看到集群公用日志主机、SNMP 主机，FTP 服务器、SFTP 服务器等信息都已配置成功。

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id      : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join       : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

步骤 10 禁止 NDP 功能和 NTDP 功能

在所有的成员交换机不需要运行 NDP 和 NTDP 协议的接口上，禁止 NDP 功能和 NTDP 功能。

```
# 禁止不相关接口的NDP功能
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ndp
# 禁止不相关接口的NTDP功能
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ntdp
```

步骤 11 检查配置结果

完成上述配置后，在命令交换机上执行 **display member-interface-state** 命令，查看成员交换机不相关接口的 NDP 或 NTDP 的状态。可以看到结果是 “Success”。

```
[HUAWEI_0.Administrator-1] display member-interface-state ndp
The result of member switches executed disable member interface command:
```

SN	Device	MacAddress	IpAddress	result
3	NE20E-X6	0004-0004-0004	10.0.0.4	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
1	NE20E-X6	0002-0002-0002	10.0.0.2	success

```
[HUAWEI_0.Administrator-1] display member-interface-state ntdp
The result of member switches executed disable member interface command:
```

SN	Device	MacAddress	IpAddress	result
3	NE20E-X6	0004-0004-0004	10.0.0.4	success
2	NE20E-X6	0003-0003-0003	10.0.0.3	success
1	NE20E-X6	0002-0002-0002	10.0.0.2	success

----结束

配置文件

- Administrator-1 的配置文件

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
```

```
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

● Member-1 的配置文件

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 interface GigabitEthernet1/0/2
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
 cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

● Member-2 的配置文件

```
#
 sysname Member-2
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
 interface Vlanif10
#
 interface GigabitEthernet1/0/1
 undo shutdown
 portswitch
 port default vlan 10
 ntdp enable
 ndp enable
#
cluster
```

```
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Member-3 的配置文件

```
#
sysname Member-3
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 3
ntdp timer 10
ndp enable
#
interface Vlanif10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 10
ntdp enable
ndp enable
#
cluster
mngvlanid 10
administrator-address 0001-0001-0001 name HUAWEI
#
return
```


5 NTP 配置

关于本章

通过配置 NTP，可以保持网络中各设备的时钟运行一致。

5.1 NTP 简介

本节对 NTP 做了简单的介绍。

5.2 配置 NTP 基本功能

在 NTP 基本配置里，用户可以了解到如何配置 NTP 的基本功能，包括 NTP 的工作模式。

5.3 配置 NTP 安全机制

本节介绍如何配置 NTP 安全模式，从而在对安全要求比较高的网络中，实现可靠的时钟同步。

5.4 维护 NTP

本节介绍在出现 NTP 运行故障时，如何运行 `debugging` 命令对 NTP 进行调试。

5.5 NTP 配置举例

本节举例说明如何配置介绍 NTP。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

5.1 NTP 简介

本节对 NTP 做了简单的介绍。

5.1.1 NTP 概述

本节描述了 NTP 的基本原理和与运行模式。

5.1.2 NE20E-X6 支持的 NTP 特性

本节介绍 NE20E-X6 支持的 NTP 运行模式。

5.1.1 NTP 概述

本节描述了 NTP 的基本原理和与运行模式。

NTP（Network Time Protocol）的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用。

对于运行 NTP 的本地系统，既可以接收来自其他时钟源的同步，也可以作为时钟源去同步别的时钟，并且可以通过交换 NTP 报文互相同步。

NTP 报文封装在 UDP 报文中传输，使用端口号 123。

NTP 的应用

NTP 主要应用于需要网络中所有主机或路由器时钟保持一致的场景，比如：

- 网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
- 计费系统：要求所有设备的时钟保持一致。
- 完成某些功能：例如，定时重启网络中的所有路由器时，要求所有路由器的时钟保持一致。
- 多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟。
- 备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步。
- 用户登录时间：某些应用程序需要知道用户登录系统的时间以及文件修改的时间。

对于网络中的众多设备，如果依靠管理员手工输入命令来修改系统时钟，不仅工作量巨大，也不能保证时钟的精确性。通过配置 NTP，可以很快将网络中设备的时钟同步，同时保证很高的精度。

NTP 的优势：

- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。
- 支持访问控制和 MD5 验证。
- 支持采用单播、组播或广播方式发送协议报文。

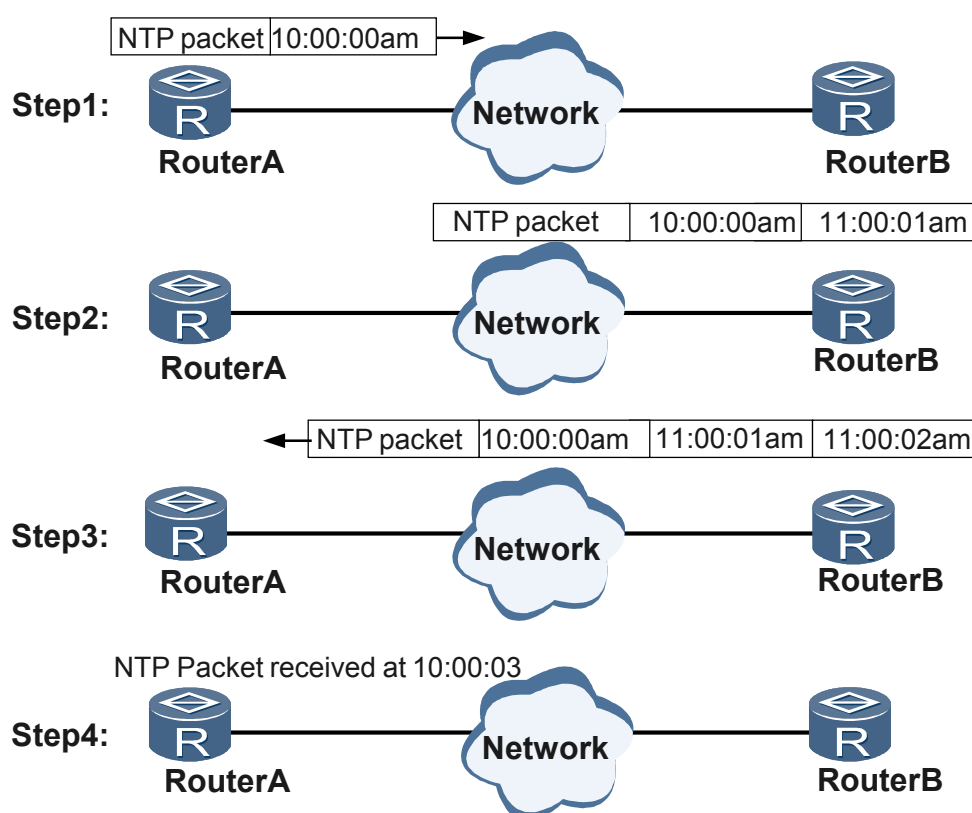
NTP 工作原理

NTP 基本工作原理如图 5-1 所示。Router A 和 Router B 通过广域网相连，它们都有自己独立的系统时钟，通过 NTP 实现系统时钟自动同步。

作如下假设：

- 在 Router A 和 Router B 的系统时钟同步之前，Router A 的时钟设定为 10:00:00am，Router B 的时钟设定为 11:00:00am。
- Router B 充当 NTP 时间服务器。Router A 的时钟与 Router B 的时钟同步。
- 数据包在 Router A 和 Router B 之间单向传输需要 1 秒。
- Router A 和 Router B 处理 NTP 数据包的时间都是 1 秒。

图 5-1 NTP 基本原理图



系统时钟同步的工作过程如下：

1. Router A 发送一个 NTP 消息包给 Router B，该消息包带有它离开 Router A 时的时间戳 10:00:00am (T1)。
2. 此 NTP 消息包到达 Router B 时，Router B 加上到达时间戳 11:00:01am (T2)。
3. 此 NTP 消息包离开 Router B 时，Router B 再加上离开时间戳 11:00:02am (T3)。
4. Router A 接收到该响应消息包时，加上新的时间戳 10:00:03am (T4)。

至此，Router A 拥有足够信息来计算以下两个重要参数：

- NTP 消息来回一个周期的时延：Delay= (T4-T1) - (T3-T2)。

- Router A 相对 Router B 的时间差: $\text{Offset} = ((T2 - T1) + (T3 - T4)) / 2$ 。

Router A 根据时间差和时延来设定自己的时钟，实现与 Router B 的时钟同步。

以上是 NTP 工作原理的简略描述，在 RFC1305 中，NTP 使用复杂的算法来确保时钟同步的精确性。

服务器和客户端的概念是相对而言的，提供时间标准的设备称为时间服务器，接收时间服务的设备称为客户端。

5.1.2 NE20E-X6 支持的 NTP 特性

本节介绍 NE20E-X6 支持的 NTP 运行模式。

NE20E-X6 支持如下几种 NTP 工作模式：

- [单播服务器/客户端模式](#)
- [对等体模式](#)
- [广播模式](#)
- [组播模式](#)
- [多播模式](#)

单播服务器/客户端模式

这种模式只需要在客户端配置，服务器端除了配置 NTP 主时钟外，不需要进行其他专门配置。

注意只能是客户端同步到服务器，服务器不会同步到客户端。

配置完成后：

1. 客户端向服务器发送同步请求报文，报文中的 Mode 字段设置为 3（客户模式）。
2. 服务器端收到请求报文后，自动工作在服务器模式，并发送应答报文，报文中的 Mode 字段设置为 4（服务器模式）。
3. 客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器端。

对等体模式

在对等体模式中，NTP 只需要在主动对等体（Symmetric active）端进行配置。

对等体模式下，主动对等体和被动对等体可以互相同步，等级低（层数大）的对等体向等级高（层数小）的对等体同步。

配置完成后：

- 主动对等体向被动对等体发送同步请求报文，报文中的 Mode 字段设置为 1（主动对等体）。
- 被动对等体收到请求报文后，自动工作在被动对等体模式，并发送应答报文，报文中的 Mode 字段设置为 2（被动对等体）。

广播模式

在广播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向广播地址 255.255.255.255 发送时钟同步报文。
- 客户端侦听来自服务器的广播消息包。
- 客户端接收到第一个广播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。
- 客户端进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。

组播模式

在组播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向组播目的地址 224.0.1.1 发送时钟同步报文。
- 客户端侦听来自服务器的组播消息包。
- 当客户端接收到第一个组播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。
- 客户端进入组播客户端模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。

多播模式

在多播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 多播客户端周期性地向指定组播地址的多播服务器发送时钟同步报文。缺省的组播目的地址为 224.0.1.1。
- 多播服务器侦听来自于多播客户端的多播报文并回应单播报文。
- 在收到第一个单播回应报文后，为估计网络时延，多播客户端与多播服务器进行暂时的关联，从而交换单播报文。
- 服务器进入多播服务器模式，继续侦听入方向的多播报文。

5.2 配置 NTP 基本功能

在 NTP 基本配置里，用户可以了解到如何配置 NTP 的基本功能，包括 NTP 的工作模式。

5.2.1 建立配置任务

在配置 NTP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

5.2.2 配置 NTP 主时钟

服务器端主时钟的层数一定要小于客户端时钟的层数，否则客户端无法跟服务器端的时钟进行同步。

5.2.3 配置更新客户端时钟的时间间隔

当服务器时钟改变时，客户端时钟应该使用设定的时间间隔进行同步。

5.2.4 配置单播服务器/客户端模式

服务器/客户端服务方式下，客户端选择与服务器的主时钟进行同步。

5.2.5 配置对等体模式

介绍了如何配置 NTP 对等体模式。两个对等体上的时钟可以互相同步，一方既可以主动发送请求消息到对方请求时钟同步，又可以响应对方主动发送来的请求消息去同步对方。

5.2.6 配置广播模式

介绍了如何在局域网中配置 NTP 广播模式，实现局域网中的时钟同步。

5.2.7 配置组播模式

介绍如何配置 NTP 组播模式对域内的设备进行时钟同步。

5.2.8 禁止指定接口接收 NTP 报文

当局域网中的某台主机不需要同步指定服务器的时钟时，可以禁止该主机的指定接口接收 NTP 报文。

5.2.9 检查配置结果

在配置 NTP 基本功能成功后，可以查看到 NTP 的基本功能的配置情况。

5.2.1 建立配置任务

在配置 NTP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 有 4 种工作模式：

- 服务器/客户端模式
- 对等体模式
- 广播模式
- 组播模式

在实际使用中，应根据网络部署情况选择适当的工作模式，以满足不同情况下的网络时钟同步需求。

对于单播服务器/客户端模式和对等体模式，还可以指定本地发送的所有 NTP 消息都使用同一接口的 IP 地址作为源 IP。

前置任务

在配置 NTP 基本功能之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网路层地址和路由协议，保证 NTP 报文可达

数据准备

在配置 NTP 基本功能之前，需要准备以下数据：

序号	数据
1	NTP 主时钟、主时钟的层数
2	收发 NTP 报文的接口

序号	数据
3	NTP 的版本
4	根据选用的工作模式，准备以下数据： ● 服务器/客户端模式：服务器的 IP 地址、服务器所属的 VPN 实例 ● 对等体模式：被动对等体的 IP 地址、被动对等体所属的 VPN 实例 ● 广播模式：发送和接收 NTP 广播包的接口、客户端允许建立的最大动态会话数目 ● 组播模式：NTP 组播消息包使用的组播组地址、组播消息包的生存周期 TTL、发送和接收 NTP 组播包的接口、客户端允许建立的最大动态会话数目
5	禁止接收 NTP 报文的接口

5.2.2 配置 NTP 主时钟

服务器端主时钟的层数一定要小于客户端时钟的层数，否则客户端无法跟服务器端的时钟进行同步。

背景信息

如果使用路由器提供 NTP 主时钟，请在作为 NTP 服务器的路由器上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service refclock-master [ip-address] [stratum]**配置 NTP 主时钟。

ip-address 是本地参考时钟的 IP 地址 127.127.t.u。t 的取值范围是 0 ~ 37。目前只能取 1，表示本地参考时钟；u 表示 NTP 进程号，取值范围是 0 ~ 3。

当不指定 IP 地址时，默认使用本地时钟 127.127.1.0 为 NTP 主时钟，层数为 8。

----结束

5.2.3 配置更新客户端时钟的时间间隔

当服务器时钟改变时，客户端时钟应该使用设定的时间间隔进行同步。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service sync-interval interval**，配置客户端更新时间间隔。

interval 是更新客户端时钟的时间间隔，取值范围是 180 ~ 600 秒。

----结束

5.2.4 配置单播服务器/客户端模式

服务器/客户端服务方式下，客户端选择与服务器的主时钟进行同步。

背景信息

通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

如果在服务器端指定了发送 NTP 报文的源地址，该地址必须与在客户端配置的服务端 IP 地址相同。否则，客户端无法处理服务器端发送的 NTP 报文，进而时钟同步失败。

操作步骤

- 配置 NTP 客户端。

请在作为客户端的路由器上,执行以下配置：

1. 执行命令 **system-view**，进入系统视图。
2. （可选）执行命令：

```
ntp-service source-interface interface-type interface-number [ vpn-instance vpn-instance-name ]
```

配置用来接收 NTP 报文的本地源接口。

3. 执行命令：

```
- ntp-service unicast-server ip-address [ version number ] [ authentication-keyid key-id | autokey ] [ source-interface interface-type interface-number | preference | vpn-instance vpn-instance-name | maxpoll max-number | minpoll min-number | burst | iburst | preempt ] *
```

配置指定 IPv4 地址的 NTP 服务器。

配置 NTP 服务器的 IP 地址。

步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口（**source-interface**），优先选择步骤 3 指定的源接口。

参数 *ip-address* 和 *ipv6-address* 指定了 NTP 服务器的 IP 地址。该地址只能是一个主机 IP 地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。



说明

指定单播 NTP 服务器后，本地路由器自动充当客户端的角色。服务器上只能配置一个主时钟。

- （可选）配置 NTP 服务器上发送 NTP 报文的源接口

请在作为客户端的路由器上,执行以下配置：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令：

```
ntp-service source-interface interface-type interface-number [ vpn-instance vpn-instance-name ]
```

配置用来发送 NTP 报文的本地源接口。

通常需要在客户端指定 NTP 服务器的源接口。之后，客户端与服务器端才能使用该接口交换 NTP 报文。

如果在服务器端指定了发送 NTP 报文的源接口，该接口必须与在客户端配置的服务端 IP 地址相同。否则，客户端无法处理服务器端发送的 NTP 报文，进而时钟同步失败。

----结束

5.2.5 配置对等体模式

介绍了如何配置 NTP 对等体模式。两个对等体上的时钟可以互相同步，一方既可以主动发送请求消息到对方请求时钟同步，又可以响应对方主动发送来的请求消息去同步对方。

操作步骤

- 配置 NTP 主动对等体

1. 执行命令 **system-view**，进入系统视图。
2. （可选）执行命令：

```
ntp-service source-interface interface-type interface-number [ vpn-instance vpn-instance-name ]
```

配置用来发送 NTP 报文的本地源接口。

3. 执行命令：

```
- ntp-service unicast-peer ip-address [ version number | [ authentication-keyid key-id | autokey ] | source-interface interface-type interface-number | preference | vpn-instance vpn-instance-name | maxpoll max-number | minpoll min-number | preempt ] *
```

配置指定 IPv4 地址的 NTP 对等体。

步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口(source-interface)，优先使用步骤 3 中指定的源接口。

参数 *ip-address* 和 *ipv6-address* 指定了 NTP 对等体的 IP 地址。该地址只能是一个主机 IP 地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。



说明

指定 NTP 对等体后，本地路由器进入对称主动模式。对称被动端不需要配置。

- （可选）配置 NTP 被动对等体的源接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令：

```
ntp-service source-interface interface-type interface-number [ vpn-instance vpn-instance-name ]
```

配置用来发送 NTP 报文的本地源接口。

通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

如果在主动对等体端指定了发送 NTP 报文的源接口，该接口必须与在被动对等体端配置的源接口相同。否则，主动对等体无法处理被动对等体发送的 NTP 报文，进而时钟同步失败。

----结束

5.2.6 配置广播模式

介绍了如何在局域网中配置 NTP 广播模式，实现局域网中的时钟同步。

操作步骤

- 配置一个 NTP 广播服务器

请在作为 NTP 广播服务器的路由器上,执行以下配置:

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，指定发送 NTP 广播包的接口。
3. 执行命令:
ntp-service broadcast-server [**version number** | [**authentication-keyid key-id** | **autokey**]] *

配置本地路由器作为 NTP 广播服务器。

配置完成后，本地路由器周期性地向广播地址 255.255.255.255 发送时钟同步报文。



说明

广播模式只能在同一局域网中使用。

- 配置一个 NTP 广播客户端

请在作为 NTP 广播客户端的路由器上,执行以下配置:

1. 执行命令 **system-view**，进入系统视图。
2. (可选) 执行命令 **ntp-service max-dynamic-sessions number**，配置本地允许建立的动态会话数目。
3. 执行命令 **interface interface-type interface-number**，指定接收 NTP 广播包的接口。
4. 执行命令 **ntp-service broadcast-client**，将本地路由器配置为 NTP 广播客户端。

步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

配置完成后，本地路由器接收来自 NTP 服务器的广播 NTP 报文，并同步本地时钟。

执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

5.2.7 配置组播模式

介绍如何配置 NTP 组播模式对域内的设备进行时钟同步。

操作步骤

- 配置一个 NTP 组播服务器

请在作为 NTP 服务器的路由器上,执行以下配置:

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 组播包的接口。
3. 执行命令：

```
- ntp-service multicast-server [ ip-address ] [ [ authentication-keyid key-id |  
autokey ] | ttl ttl-number | version number ] *
```

配置本地路由器作为一个 IPv4 网络上的 NTP 组播服务器。

- 配置本地路由器作为一个 IPv6 网络上的 NTP 组播服务器。

配置完成后，本地路由器周期性地向组播地址 224.0.1.1 发送时钟同步报文。

- 配置一个 NTP 组播客户端

请在作为客户端的路由器上,执行以下配置：

1. 执行命令 **system-view**，进入系统视图。
2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。
3. 执行命令 **interface** *interface-type interface-number*，指定接收 NTP 组播包的接口。
4. 执行命令：

配置本地路由器作为一个 NTP 组播客户端。

步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

配置完成后，本地路由器侦听来自 NTP 服务器的组播 NTP 报文，并同步本地时钟。

执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

5.2.8 禁止指定接口接收 NTP 报文

当局域网中的某台主机不需要同步指定服务器的时钟时，可以禁止该主机的指定接口接收 NTP 报文。

背景信息

在需要禁止某个接口接收 NTP 报文的路由器上，请进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令：

```
ntp-service in-interface disable [ ipv4 | ipv6 ]
```

禁止路由器上的接口接收 NTP 报文。

----结束

5.2.9 检查配置结果

在配置 NTP 基本功能成功后，可以查看到 NTP 的基本功能的配置情况。

前提条件

已经完成配置 NTP 基本功能的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions [verbose]** 查看 NTP 会话的状态。
- 执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<HUAWEI> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 10.00 ms
reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions [verbose]** 查看 NTP 会话的状态。

```
<HUAWEI> display ntp-service sessions
          source          reference          stra reach poll now offset delay disper
*****
[12345]127.127.1.0      LOCAL(0)              7    1    64    2    -    0.0    15.6
note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured, 6 vpn-instance
```

执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

```
<HUAWEI> display ntp-service trace
server 127.0.0.1, stratum 5, offset 0.024099, synch distance 0.06337
server 171.1.1.2, stratum 4, offset 0.028786, synch distance 0.04575
server 201.1.1.2, stratum 3, offset 0.035199, synch distance 0.03075
server 200.1.7.1, stratum 2, offset 0.039855, synch distance 0.01096
refid 127.127.1.0
```

5.3 配置 NTP 安全机制

本节介绍如何配置 NTP 安全模式，从而在对安全要求比较高的网络中，实现可靠的时钟同步。

5.3.1 建立配置任务

在配置 NTP 安全机制前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

5.3.2 配置 NTP 访问控制权限

在接收到一个访问请求报文后，NTP 服务器按照降序（peer, server, synchronization to query）对报文的访问限制进行匹配，以第一个匹配的访问权限为准。

5.3.3 使能 NTP 验证

客户端与服务器端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。

5.3.4 在单播服务器/客户端模式下配置 NTP 验证

通过在 NTP 客户端配置与指定 NTP 服务器同步时使用的密钥 ID，可以在 NTP 服务器/客户端模式下应用 NTP 验证。

5.3.5 在对等体模式下配置 NTP 验证

通过在本端配置与对等体端同步时使用的密钥 ID，可以在对等体模式下应用 NTP 验证。

5.3.6 在广播模式下配置 NTP 验证

通过在本本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在广播模式下应用 NTP 验证。

5.3.7 在组播模式下配置 NTP 验证

通过在本本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在组播模式下应用 NTP 验证。

5.3.8 在多播模式下配置 NTP 验证

5.3.9 检查配置结果

在成功配置 NTP 安全机制后，可以查看到 NTP 安全机制的配置情况。

5.3.10 配置 KOD

本节介绍如何配置 KOD 特性以及该特性在不同工作模式下的运行情况。

5.3.11 在服务器端配置 KOD

5.3.12 客户端-服务器模式下在客户端配置 KOD

5.3.13 多播模式下在客户端配置 KOD

5.3.14 在对等体模式下为客户端配置 KOD

5.3.15 检查配置结果

5.3.1 建立配置任务

在配置 NTP 安全机制前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 提供访问权限和 NTP 验证两种安全机制。

- 访问权限

通过设置访问权限保护本地 NTP 服务是 NE20E-X6 提供的一种比较简单的安全措施。

NE20E-X6 提供 4 个等级的访问限制。当一个 NTP 访问请求报文到达本地时，按照最小访问限制到最大访问限制对报文进行依次匹配，以第 1 个匹配的为准，匹配顺序如下：

- **peer**: 表示最小访问限制。远端设备可以给本地设备发送时间请求和控制查询，本地时钟也可以同步到远端服务器。
- **server**: 远端设备可以对本地设备进行时间请求和控制查询，但本地时钟不会同步到远端服务器。
- **synchronization**: 只允许远端设备对本地设备提出时间请求。
- **query**: 表示最大访问限制。只允许远端设备对本地设备进行控制查询。

- NTP 验证

在安全性要求较高的网络中，可以启用 NTP 验证功能。

配置 NTP 验证功能分为两部分：配置客户端、配置服务器端。

在配置 NTP 验证功能时，应注意以下原则：

- 客户端和服务器端均需要配置 NTP 验证功能。否则，NTP 验证功能不生效。
- 如果使能了 NTP 验证功能，应同时配置一个可信的密钥。
- 在服务器端和客户端上配置的密钥必须相同。
- 在 NTP 对等体模式下，主动对等体相当于客户端，被动对等体相当于服务器端。

前置任务

在配置 NTP 安全机制之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网络层地址和路由协议，保证客户端和路由器端路由可达
- 如果配置访问权限，需要配置用于进行访问控制的 ACL

数据准备

在配置 NTP 安全机制之前，需要准备以下数据：

序号	数据
1	ACL 规则
2	NTP 验证使用的密钥 ID 和密钥
3	NTP 主时钟、主时钟的层数
4	收发 NTP 报文的接口
5	NTP 的版本
6	根据选用的工作模式，准备以下数据： ● 服务器/客户端模式：服务器的 IP 地址、服务器所属的 VPN 实例 ● 对等体模式：被动对等体的 IP 地址、被动对等体所属的 VPN 实例 ● 广播模式：发送和接收 NTP 广播包的接口、客户端允许建立的最大动态会话数目 ● 组播模式：NTP 组播消息包使用的组播组地址、组播消息包的生存周期 TTL

5.3.2 配置 NTP 访问控制权限

在接收到一个访问请求报文后，NTP 服务器按照降序（peer, server, synchronization to query）对报文的访问限制进行匹配，以第一个匹配的访问权限为准。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 执行命令：

```
ntp-service access { peer | query | server | synchronization | synchronization | limited } { acl-  
number | ipv6 acl6-number } *
```

在本地路由器上配置 NTP 服务的访问控制权限。

用户需要根据实际需求决定在哪台设备上配置 `ntp-service access` 命令。

具体描述见表 5-1。

表 5-1 NTP 访问控制权限配置

NTP 工作模式	限制的 NTP 请求类型	进行配置的设备
单播 NTP 服务器/客户端模式	限制客户端同步到服务器端	客户端
单播 NTP 服务器/客户端模式	限制服务器端处理客户端发送的时钟同步请求	服务器端
NTP 对等体模式	限制客户端和服务器端进行时钟同步	主动对等体端
NTP 对等体模式	限制被动对等体端处理主动对等体发送的时钟请求	被动对等体端
NTP 组播模式	限制客户端同步到服务器端	NTP 组播客户端
NTP 广播模式	限制客户端同步到服务器端	NTP 广播客户端
NTP 多播客户端模式	限制客户端同步到服务器端	NTP 多播客户端
NTP 多播服务器模式	限制服务器端处理客户端发送的时钟同步请求	NTP 多播服务器

---结束

5.3.3 使能 NTP 验证

客户端与服务器端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。

背景信息



- NTP 客户端和服务端都需要进行配置。
- 客户端与服务端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。
- 必须先使能 NTP 验证功能，否则不会进行验证。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service authentication enable** 使能 NTP 验证功能。

步骤 3 执行命令 **ntp-service authentication-keyid key-id authentication-mode md5 password**，配置 NTP 验证密钥。

步骤 4 执行命令 **ntp-service reliable authentication-keyid key-id**，声明密钥可信。

----结束

5.3.4 在单播服务器/客户端模式下配置 NTP 验证

通过在 NTP 客户端配置与指定 NTP 服务器同步时使用的密钥 ID，可以在 NTP 服务器/客户端模式下应用 NTP 验证。

背景信息

请在作为 NTP 单播客户端的路由器上,执行以下配置:

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

- **ntp-service unicast-server ip-address [version number] [authentication-keyid key-id | autokey] | source-interface interface-type interface-number | preference | vpn-instance vpn-instance-name | maxpoll max-number | minpoll min-number | burst | iburst | preempt] ***

配置指定 IPv4 地址的 NTP 服务器。

- **ntp-service unicast-server ipv6 ipv6-address [[authentication-keyid key-id | autokey] | source-interface interface-type interface-number | preference | vpn-instance vpn-instance-name | maxpoll max-number | minpoll min-number | burst | iburst | preempt] ***

配置指定 IPv6 地址的 NTP 服务器。

----结束

5.3.5 在对等体模式下配置 NTP 验证

通过在本端配置与对等体端同步时使用的密钥 ID，可以在对等体模式下应用 NTP 验证。

背景信息

请在作为主动对等体端的路由器上,执行以下配置:

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令：

- **ntp-service unicast-peer** *ip-address* [**version** *number*] [**authentication-keyid** *key-id* | **autokey**] [**source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt**] *

配置指定 IPv4 地址的 NTP 对等体。

- **ntp-service unicast-peer** **ipv6** *ipv6-address* [[**authentication-keyid** *key-id* | **autokey**] | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt**] *

配置指定 IPv6 地址的 NTP 服务器。

----结束

5.3.6 在广播模式下配置 NTP 验证

通过在本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在广播模式下应用 NTP 验证。

背景信息

请在作为 NTP 广播服务器的路由器上，执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 广播包的接口。

步骤 3 执行命令 **ntp-service broadcast-server** [**version** *number*] [**authentication-keyid** *key-id* | **autokey**]] *配置本地路由器作为 NTP 广播服务器时使用的密钥 ID。

对于广播客户端的配置，参见“[配置广播模式](#)”。

----结束

5.3.7 在组播模式下配置 NTP 验证

通过在本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在组播模式下应用 NTP 验证。

背景信息

请在作为 NTP 组播服务器的路由器上，执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 组播包的接口。

步骤 3 执行命令：

- **ntp-service multicast-server** [*ip-address*] [[**authentication-keyid** *key-id* | **autokey**] | **ttl** *t11-number* | **version** *number*] *

在 IPv4 网络上配置 NTP 组播服务器使用的验证密钥 ID。

- **ntp-service multicast-server** [**ipv6** [*ipv6-address*]] [[**authentication-keyid** *key-id* | **autokey**] | **t11** *t11-number*] *

在 IPv6 网络上配置 NTP 组播服务器使用的验证密钥 ID。

对于组播客户端的配置，参见“[配置组播模式](#)”。

----结束

5.3.8 在多播模式下配置 NTP 验证

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type* *interface-number*，进入接口视图。

步骤 3 执行命令 **ntp-service manycast-client** [*ip-address* | **ipv6** [*ipv6-address*]] [[**authentication-keyid** *key-id* | **autokey**] | **t11** *t11-number*] *，配置 NTP 多播客户端使用的验证密钥 ID。

----结束

5.3.9 检查配置结果

在成功配置 NTP 安全机制后，可以查看到 NTP 安全机制的配置情况。

前提条件

已经完成 NTP 安全机制的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<HUAWEI> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 10.00 ms
reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

```
<HUAWEI> display ntp-service sessions
          source          reference          stra reach poll  now offset delay disper
*****
[12345] 127.127.1.0      LOCAL(0)              7    1    64    2    -    0.0    15.6
note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured, 6 vpn-instance
```

5.3.10 配置 KOD

本节介绍如何配置 KOD 特性以及该特性在不同工作模式下的运行情况。

应用环境

NTP 有以下工作模式：

- 服务器/客户端模式
- 对等体模式
- 多播模式

KOD 不可以应用在广播和组播模式下。

前置任务

在配置 NTP KOD 特性之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网络层地址和路由协议，保证客户端和路由器端路由可达

5.3.11 在服务器端配置 KOD

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ntp-service kod-enable**，使能 KOD。
- 步骤 3** 执行命令 **ntp-service access { peer | query | server | synchronization | limited } { acl-number | ipv6 acl6-number } ***，设置访问控制权限。
- 步骤 4** 执行命令 **ntp-service discard { min-interval min-interval-val | avg-interval avg-interval-val } ***，配置接收 NTP 报文的最小和平均时间间隔。
- 步骤 5** 执行命令 **ntp-service refclock-master [ip-address] [stratum]**，将本地时钟配置为 NTP 主时钟，为其他设备提供同步时间。

----结束

5.3.12 客户端-服务器模式下在客户端配置 KOD

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 根据要求执行如下命令，配置用来进行服务器和客户端时钟同步的验证密钥 ID：
- **ntp-service unicast-server ip-address [version number] [authentication-keyid key-id | autokey] [source-interface interface-type interface-number | preference | vpn-instance vpn-instance-name | maxpoll max-number | minpoll min-number | burst | iburst | preempt] ***

配置指定 IPv4 地址的 NTP 服务器。

- **ntp-service unicast-server** *ipv6 ipv6-address* [[*authentication-keyid key-id* | *autokey*] | *source-interface interface-type interface-number* | *preference* | *vpn-instance vpn-instance-name* | *maxpoll max-number* | *minpoll min-number* | *burst* | *iburst* | *preempt*] *

配置指定 IPv6 地址的 NTP 服务器。

----结束

5.3.13 多播模式下在客户端配置 KOD

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入接口视图。

步骤 3 执行命令 **ntp-service manycast-client** [*ip-address* | **ipv6** [*ipv6-address*]] [[*authentication-keyid key-id* | *autokey*] | *ttl ttl-number*] *，配置 NTP 多播客户端使用的验证密钥 ID。

----结束

5.3.14 在对等体模式下为客户端配置 KOD

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据要求执行如下命令，配置用来同步 NTP 对等体上时钟的验证密钥 ID：

- **ntp-service unicast-peer** *ip-address* [*version number* | [*authentication-keyid key-id* | *autokey*] | *source-interface interface-type interface-number* | *preference* | *vpn-instance vpn-instance-name* | *maxpoll max-number* | *minpoll min-number* | *preempt*] *

配置指定 IPv4 地址的 NTP 对等体。

- **ntp-service unicast-peer** **ipv6** *ipv6-address* [[*authentication-keyid key-id* | *autokey*] | *source-interface interface-type interface-number* | *preference* | *vpn-instance vpn-instance-name* | *maxpoll max-number* | *minpoll min-number* | *preempt*] *

配置指定 IPv6 地址的 NTP 服务器。

----结束

5.3.15 检查配置结果

前提条件

NTP KOD 的相关配置已经完成。

操作步骤

- 执行命令 **display current-configuration** 查看路由器上目前对 KOD 特性有效的配置参数。

----结束

5.4 维护 NTP

本节介绍在出现 NTP 运行故障时，如何运行 **debugging** 命令对 NTP 进行调试。

背景信息



注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

在出现 NTP 运行故障时，请在用户视图下执行中的 **debugging** 命令对 NTP 进行调试，查看调试信息，定位故障并分析故障原因。

打开调试开关的操作步骤请参考《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》中“维护与调试”的内容。

有关 **debugging** 命令的解释请参考《HUAWEI NetEngine20E-X6 高端业务路由器 命令手册》。

操作步骤

步骤 1 执行命令 **debugging ntp-service { access | adjustment | all | authentication | event | filter | packet | parameter | refclock | selection | synchronization | validity }** 打开 NTP 的调试开关。

----结束

5.5 NTP 配置举例

本节举例说明如何配置介绍 NTP。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

5.5.1 配置带验证的单播 NTP 服务器/客户端模式示例

本部分举例说明如何在单播服务器/客户端模式下配置 NTP 验证。客户端必须先使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。客户端和服务端都需要进行完整的配置，才能验证通过。

5.5.2 配置 NTP 对等体模式的示例

在对等体模式下，对等体双方可以相互同步对方的时钟。

5.5.3 配置带验证的 NTP 广播模式示例

在局域网中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

5.5.4 配置 NTP 组播模式示例

在组播域中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

5.5.5 配置 NTP 多播模式示例

5.5.6 使用私有方案在客户端/服务器模式下配置 NTP 自动密钥的示例

[5.5.7 使用可信方案在对等体模式下配置 NTP 自动密钥的示例](#)

[5.5.8 使用 IFF 方案在广播模式下配置 NTP 自动密钥的示例](#)

[5.5.9 使用 GQ 方案在组播模式下配置自动密钥的示例](#)

[5.5.10 使用 MV 方案在多播模式下配置 NTP 自动密钥的示例](#)

[5.5.11 在单播服务器/客户端模式下配置 NTP 验证的示例](#)

[5.5.12 在 NTP 对等体模式下配置 KOD 的示例](#)

[5.5.13 在 NTP 多播模式下配置 KOD 的示例](#)

5.5.1 配置带验证的单播 NTP 服务器/客户端模式示例

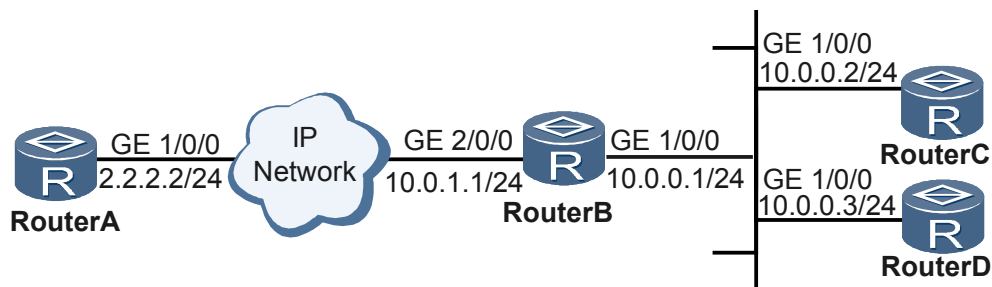
本部分举例说明如何在单播服务器/客户端模式下配置 NTP 验证。客户端必须先使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。客户端和服务端都需要进行完整的配置，才能验证通过。

组网需求

如图 5-2 所示：

- RouterA 作为 NTP 单播服务器，其本地时钟作为 NTP 主时钟，层数为 2。
- RouterB 作为 NTP 单播客户端，同步远端服务器 RouterA 的时钟。
- RouterC 和 RouterD 作为 NTP 客户端，把 RouterB 作为自己的 NTP 服务器。
- 使能 NTP 验证。

图 5-2 单播 NTP 服务器/客户端模式组网图



配置思路

配置思路如下：

1. 配置 RouterA 作为服务器，提供主时钟。
2. 配置 RouterB 作为 NTP 客户端，同步 RouterA 的时钟。
3. 配置 RouterC、RouterD 作为 NTP 客户端，同步 RouterB 的时钟。
4. 在所有的 Router 上使能 NTP 验证。



说明

- 在单播服务器/客户端模式下配置 NTP 验证时时，必须首先在客户端使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。
- 客户端和服务端都需要进行完整的配置，才能验证通过。

数据准备

为完成此配置例，需准备如下的数据：

- 参考时钟的 IP 地址
- NTP 主时钟的等级
- 验证密钥及其编号
- 密码

操作步骤

步骤 1 根据图 5-2，配置 IP 地址，配置 RouterA,RouterB,RouterC 和 RouterD 路由可达。具体配置过程略。

步骤 2 在 RouterA 上配置 NTP 主时钟并启动 NTP 验证功能。

在 RouterA 上指定使用自己的本地时钟作为参考时钟，层数为 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2

# 使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterA] ntp-service reliable authentication-keyid 42
```

注意服务器端与客户端必须配置相同的验证密钥。

步骤 3 在 RouterB 上配置 NTP 主时钟并启动 NTP 验证功能。

在 RouterB 上使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterB] ntp-service reliable authentication-keyid 42
```

指定 RouterA 作为 RouterB 的 NTP 服务器，并使用已配置的验证密钥。

```
[RouterB] ntp-service unicast-server 2.2.2.2 authentication-keyid 42
```

步骤 4 在 Router C 上指定 RouterB 作为 RouterC 的 NTP 服务器。

```
<RouterC> system-view
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 42
[RouterC] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 5 在 RouterD 上指定 RouterB 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterD] ntp-service reliable authentication-keyid 42
[RouterD] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 6 验证配置结果。

完成上述配置后，RouterB 可以同步 RouterA 的时钟。

查看 RouterB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 RouterA 低 1 级。

```
[RouterB] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 2.2.2.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

完成上述配置后，RouterC 可以同步 RouterB 的时钟。

查看 RouterC 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 RouterB 低 1 级。

```
[RouterC] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 RouterB 低 1 级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 Router A 的 NTP 状态。

```
[RouterA] display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 26.50 ms
peer dispersion: 10.00 ms
```


reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %%ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service refclock-master 2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.0.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
network 10.0.0.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %%ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 2.2.2.2 authentication-keyid 42
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.0.2 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %%ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
```

```
undo shutdown
ip address 10.0.0.3 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

5.5.2 配置 NTP 对等体模式的示例

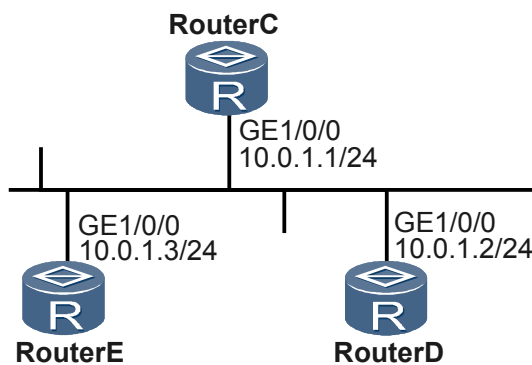
在对等体模式下，对等体双方可以相互同步对方的时钟。

组网需求

如图图 5-3 所示。在同一个局域网中有 3 台设备。

- RouterC 的本地时钟设为 NTP 主时钟，层数为 2。
- RouterD 将 RouterC 设为自己的 NTP 服务器。即，RouterD 作为客户端。
- RouterE 将 RouterD 设为自己的被动对等体。即，RouterE 作为主动对等体。

图 5-3 配置 NTP 对等体模式的组网图



配置思路

配置思路如下：

1. 配置 RouterC 的本地时钟作为 NTP 主时钟，RouterD 向 RouterC 请求时钟同步。
2. 配置 RouterE 和 RouterD 为对等体，RouterE 向 RouterD 发起时钟同步请求。
3. 最终实现 RouterC、RouterD、RouterE 的时钟同步。

数据准备

为完成此配置例，需准备如下的数据：

- RouterC 的 IP 地址
- RouterD 的 IP 地址
- NTP 主时钟的层数

操作步骤

步骤 1 配置 RouterC、RouterD、RouterE 的 IP 地址。

按照图 5-3 给每个接口配置 IP 地址。配置完成后，3 台 Router 之间可以互相 ping 通。
具体配置过程略。

步骤 2 配置 NTP 服务器/客户端模式

#将 RouterC 的本地时钟设为 NTP 主时钟，层数为 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

在 RouterD 上指定 RouterC 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service unicast-server 10.0.1.1
```

完成上述配置后，Router D 可以同步 Router C 的时钟。

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比 Router C 低 1 级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.0.1.1
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 62.50 ms
root dispersion: 0.20 ms
peer dispersion: 7.81 ms
reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
```

步骤 3 配置 NTP 单播对等体模式

在 RouterE 上指定 RouterD 作为自己的被动对等体。

```
<RouterE> system-view
[RouterE] ntp-service unicast-peer 10.0.1.2
```

由于 RouterE 没有配置主时钟，并且其时钟层数低于 RouterD，所以 RouterE 向 RouterD 同步。

步骤 4 验证配置结果。

同步后观测 RouterE 的状态。RouterE 的时钟状态为“synchronized”，即，已经完成同步。RouterE 的时钟层数为 4，比被动对等体 RouterD 低 1 级。

```
[RouterE] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.1.2
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 124.98 ms
root dispersion: 0.15 ms
peer dispersion: 10.96 ms
reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
```

----结束

配置文件

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.1 255.255.255.0
#
ntp-service refclock-master 2
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.2 255.255.255.0
#
ntp-service unicast-server 10.0.1.1
#
return
```

- Router E 的配置文件

```
#
 sysname RouterE
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.3 255.255.255.0
#
ntp-service unicast-peer 10.0.1.2
#
return
```

5.5.3 配置带验证的 NTP 广播模式示例

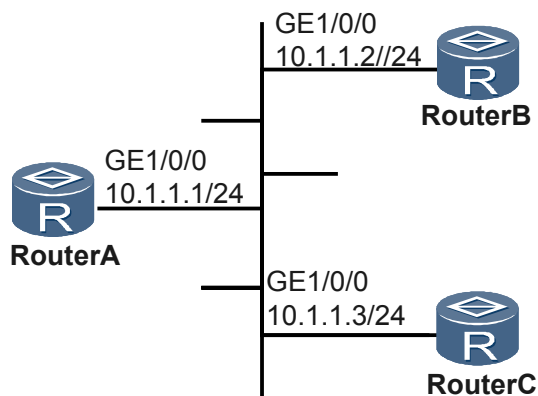
在局域网中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

组网需求

如图 5-4 所示:

- RouterA、RouterB 与 RouterC 处于同一网段内。
- RouterA 为 NTP 广播服务器，通过 GE1/0/0 接口发送广播报文。RouterA 的本地时钟作为 NTP 主时钟，层级为 3。
- RouterB 和 RouterC 分别从各自的接口 GE1/0/0 监听广播消息。

图 5-4 配置 NTP 广播模式的组网图



配置思路

配置思路如下：

1. 配置 RouterA 为 NTP 广播服务器。
2. 配置 RouterB 与 RouterC 为 NTP 广播客户端。
3. 在 RouterA、RouterB 和 RouterC 上配置 NTP 验证。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 以及 RouterC 的 IP 地址
- NTP 主时钟的层数
- 验证密钥及其编号

操作步骤

步骤 1 配置每台 Router 的 IP 地址。

按照图 5-4 配置 IP 地址,此处不再赘述。

步骤 2 配置 NTP 广播服务器，并启用验证。

配置 RouterA 的本地时钟为 NTP 主时钟，层级为 3。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 3
```

使能 NTP 验证。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterA] ntp-service reliable authentication-keyid 16
```

配置 RouterA 为 NTP 广播服务器，从接口 GE1/0/0 发送 NTP 广播消息包，并指定使用密钥 ID 16 加密。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service broadcast-server authentication-keyid 16
```

```
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 3 配置 RouterB。

使能 NTP 验证。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterB] ntp-service reliable authentication-keyid 16
```

配置 RouterB 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterB interface gigabitethernet 1/0/0]
[RouterB-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 4 配置 RouterC。

使能 NTP 验证。

```
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 16
```

配置 RouterC 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterC-GigabitEthernet1/0/0] quit
```

步骤 5 验证配置结果。

完成以上配置后，RouterB 和 RouterC 能够同步 RouterA 的时钟，

查看 RouterB 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterB 的时钟等级为 4，比 RouterA 的时钟低一等级。

```
[RouterB] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.42 ms
peer dispersion: 0.00 ms
reference time: 12:17:21.773 UTC Mar 7 2006(C7B7F851.C5EAF25B)
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
ntp-service broadcast-server authentication-keyid 16
#
ntp-service authentication enable
ntp-service authentication-keyid 16 authentication-mode md5 %ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
```

```
ntp-service refclock-master 3
#
return
```

- RouterB 的配置文件

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
ntp-service broadcast-client
#
ntp-service authentication enable
ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
#
Return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.3 255.255.255.0
ntp-service broadcast-client
#
ntp-service authentication enable
ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
#
return
```

5.5.4 配置 NTP 组播模式示例

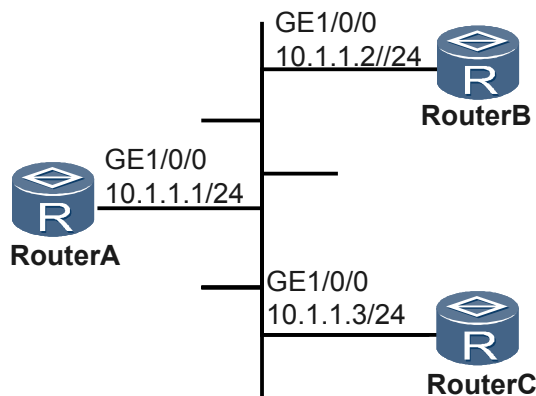
在组播域中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

组网需求

如图图 5-5 所示：

- RouterA、RouterB 与 RouterC 处于同一网段。
- RouterA 为 NTP 组播服务器，通过 GE1/0/0 接口发送组播报文。RouterA 的本地时钟作为 NTP 主时钟，层数为 2。
- RouterB 和 RouterC 分别从各自的接口 GE1/0/0 监听组播报文。

图 5-5 配置 NTP 组播模式的组网图



配置思路

配置思路如下：

1. 配置 RouterA 为 NTP 组播服务器。
2. 配置 RouterB 与 RouterC 作为 NTP 组播客户端。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 以及 RouterC 的 IP 地址
- NTP 主时钟的层数

操作步骤

步骤 1 配置每台 Router 的 IP 地址。

按图 5-5 配置 IP 地址。具体过程略。

步骤 2 配置 NTP 组播服务器。

配置 RouterA 的本地时钟为 NTP 主时钟，层数是 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2
```

配置 RouterA 作为 NTP 组播服务器，从 GE1/0/0 接口发送 NTP 组播报文。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-server
```

步骤 3 配置 RouterB。

配置 RouterB 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 4 配置 RouterC。

配置 RouterC 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 5 验证配置结果。

完成以上配置后，RouterB、RouterC 能够同步 RouterA 的时钟。

查看 RouterB 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterB 的时钟等级为 3，比 RouterA 的时钟低一等级。

```
[RouterB] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
```



```
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.66 ms
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005 (C61734FD.800303C0)
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 ntp-service refclock-master 2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 ntp-service multicast-server
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 ntp-service multicast-client
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.3 255.255.255.0
 ntp-service multicast-client
#
return
```

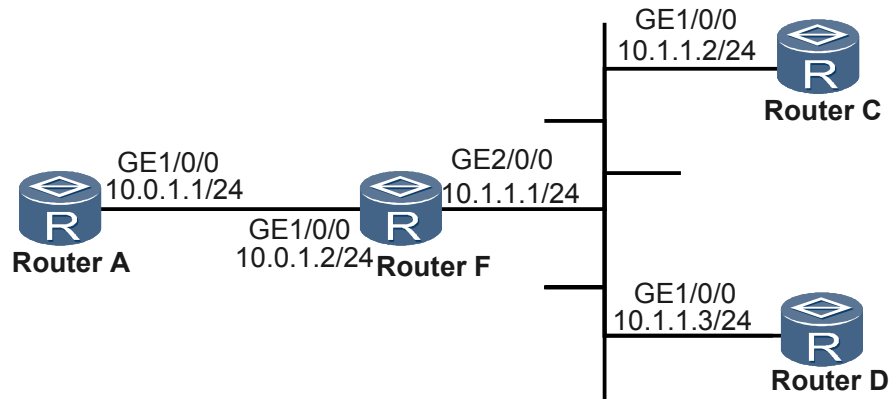
5.5.5 配置 NTP 多播模式示例

组网需求

如图图 5-6 所示:

- RouterC 与 RouterD 处于同一网段。RouterA 处于另一网段。RouterF 与两个网段相连。
- RouterC 为一个 NTP 多播服务器，通过 GE1/0/0 接口发送多播报文。RouterC 的本地时钟为 NTP 主时钟，等级为 2。
- RouterD 和 RouterA 为多播客户端，通过各自的 GE1/0/0 接口发送报文。

图 5-6 NTP 多播模式的组网图



配置注意事项

时钟同步前，在 console 接口视图下执行 **ping** 命令确认多播客户端与多播服务器之间路由可达。

配置思路

配置思路如下：

1. 将 RouterC 配置为 NTP 多播服务器。
2. 将 RouterA 与 RouterD 配置为 NTP 多播客户端。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterC、RouterD 以及 RouterF 的 IP 地址
- NTP 主时钟的等级

操作步骤

步骤 1 配置每台路由器的 IP 地址。

按图 5-6 配置 IP 地址。具体过程略。

步骤 2 配置 NTP 多播服务器。

配置 RouterC 的本地时钟为 NTP 主时钟，等级是 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

配置 RouterC 为 NTP 多播服务器。NTP 多播服务器在收到多播客户报文后，发送 NTP 多播报文。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-server
```

步骤 3 配置 RouterD。

配置 RouterD 为 NTP 多播客户端。RouterD 通过 GE1/0/0 接口向多播服务器发送 NTP 多播报文。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 4 配置 RouterA。

配置 RouterA 为 NTP 多播客户端。RouterA 通过 GE1/0/0 接口向多播服务器发送 NTP 多播报文。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 5 验证配置结果。

配置完成后，RouterA 和 RouterD 能跟 RouterC 进行时钟同步。

查看 RouterD 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterD 的时钟等级为 3，比 RouterC 的时钟低一等级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.66 ms
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005(C61734FD.800303C0)
autokey crypto flags: 0x80021
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.1 255.255.255.0
 ntp-service multicast-client
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 ntp-service multicast-server
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.3 255.255.255.0
ntp-service manycast-client
#
return
```

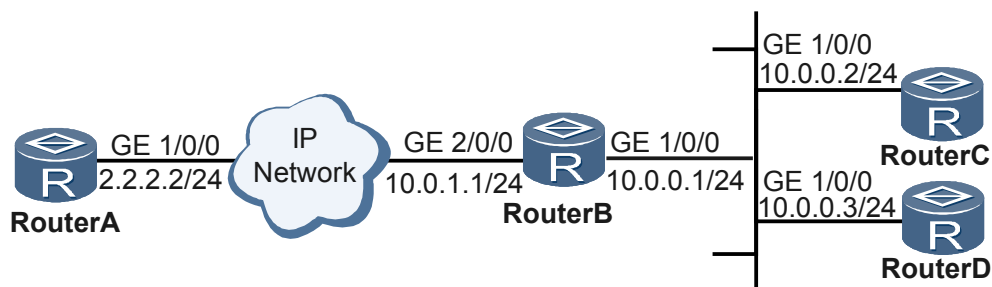
5.5.6 使用私有方案在客户端/服务器模式下配置 NTP 自动密钥的示例

Networking Requirements

如图 5-7 所示:

- RouterA 作为 NTP 单播服务器，其本地时钟作为 NTP 主时钟，等级为 2。
- RouterB 作为 NTP 单播客户端，与 RouterA 的时钟进行同步。
- RouterC 和 RouterD 作为 NTP 客户端，把 RouterB 作为自己的 NTP 服务器。
- 使能 NTP 验证。

图 5-7 使用私有方案在服务器/客户端模式下配置 NTP 自动密钥的组网图



配置注意事项

- 在客户端和服务器端配置自动密钥之前，确保密钥与证书文件已经存在。
- 在私有方案中，所有路由器上的密钥和证书文件都必须相同。
- 客户端和服务器端配置的验证密钥都必须是可信的，另外需要在客户端使能验证功能。

配置思路

配置思路如下：

1. 使能自动密钥，配置 RouterA 作为 NTP 服务器，提供主时钟。
2. 使能自动密钥，配置 RouterB 作为 NTP 客户端，同步 RouterA 的时钟。
3. 使能自动密钥，配置 RouterC 和 RouterD 同步 RouterB 的时钟。

说明

在配置服务器之前必须在所有路由器上使能 NTP 验证自动密钥。

数据准备

为完成此配置例，需准备如下的数据：

- 参考时钟的 IP 地址
- NTP 主时钟的等级。
- 验证自动密钥文件和证书
- 读取文件的密码

操作步骤

步骤 1 根据图 5-7，配置 IP 地址，配置 RouterA、RouterB、RouterC 和 RouterD 路由可达。具体配置过程略。

步骤 2 在 RouterA 上配置 NTP 主时钟并启动 NTP 验证功能。

指定 RouterA 的本地时钟作为 NTP 主时钟，等级为 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2
```

使能 NTP 验证，配置自动密钥。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication auto-key hostname private password Hello
```

注意服务器端与客户端必须配置相同的验证密钥。

NTP 读取证书文件 ntpkey_host_private, ntpkey_cert_private 以及(optional) ntpkey_sign_private。

步骤 3 在 RouterB 上配置 NTP 主时钟并启动 NTP 验证功能。

在 RouterB 上使能 NTP 验证功能并配置自动密钥。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication auto-key hostname private password Hello
```

指定 RouterA 作为 RouterB 的 NTP 服务器，并使用已配置的验证密钥。

```
[RouterB] ntp-service unicast-server 2.2.2.2 autokey
```

步骤 4 在 RouterC 上指定 RouterB 作为 RouterC 的 NTP 服务器。

```
<RouterC> system-view
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication auto-key hostname private password Hello
[RouterC] ntp-service unicast-server 10.0.0.1 autokey
```

步骤 5 在 RouterD 上指定 RouterB 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication auto-key hostname private password Hello
[RouterC] ntp-service unicast-server 10.0.0.1 autokey
```

步骤 6 验证配置结果。

完成上述配置后，RouterB 可以同步 RouterA 的时钟。

查看 RouterB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 3，比 RouterA 低 1 级。A。

```
[RouterB] display ntp-service status
```

```
clock status: synchronized
clock stratum: 3
reference clock ID: 2.2.2.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 218
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
autokey crypto flags: 0x80011
```

完成上述配置后，RouterC 可以同步 RouterB 的时钟。

查看 RouterC 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 4，比 RouterB 低 1 级。

```
[RouterC] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 218
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
autokey crypto flags: 0x80011
```

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 4，比 RouterB 低 1 级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 218
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
autokey crypto flags: 0x80011
```

查看 RouterA 的 NTP 状态。

```
[RouterA] display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 218
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 26.50 ms
peer dispersion: 10.00 ms
reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)
autokey crypto flags: 0x80011
```

----结束

配置文件

● RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication auto-key hostname private password Hello
ntp-service refclock-master 2
#
return
```

● RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.0.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
ntp-service authenticationenable
ntp-service authentication auto-key hostname private password Hello
ntp-service unicast-server 2.2.2.2 autokey
#
return
```

● RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.0.2 255.255.255.0
#
ntp-service authenticationenable
ntp-service authentication auto-key hostname private password Hello
ntp-service unicast-server 10.0.0.1 autokey
#
return
```

● RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.0.3 255.255.255.0
#
ntp-service authenticationenable
ntp-service authentication auto-key hostname private password Hello
ntp-service unicast-server 10.0.0.1 autokey
#
```

return

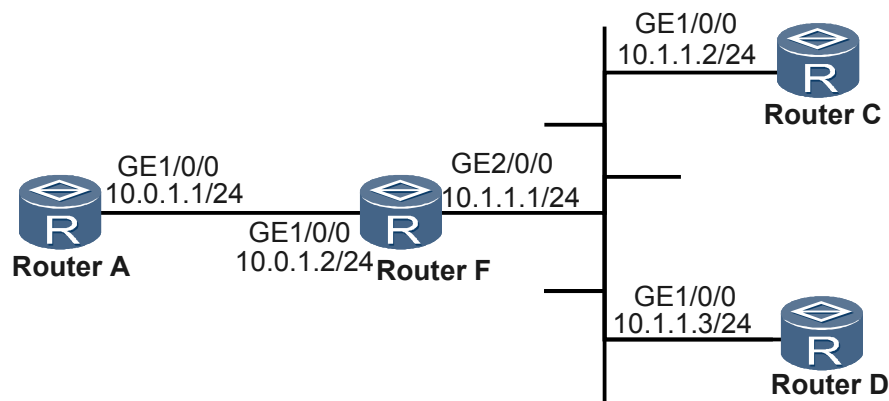
5.5.7 使用可信方案在对等体模式下配置 NTP 自动密钥的示例

组网需求

如图图 5-8 所示。在同一个局域网中有 3 台 Router。

- 将 RouterC 的本地时钟设为 NTP 主时钟，等级为 2。
- RouterD 将 RouterC 设为自己的 NTP 服务器。即，RouterD 作为客户端。
- RouterF 将 RouterD 设为自己的被动对等体。即，RouterF 作为主动对等体。

图 5-8 使用可信方案在对等体模式下配置 NTP 自动密钥的组网图



配置注意事项

在配置对等体模式前，确认对等体对于主机来说是可达的。

配置思路

配置思路如下：

1. 配置 RouterC 的本地时钟作为 NTP 主时钟，RouterD 同步 RouterC 的时钟。
2. 配置自动密钥，设置 RouterF 和 RouterD 为对等体，RouterF 向 RouterD 发起时钟同步请求。
3. 最终实现 RouterC、RouterD、RouterF 这 3 台路由器的时钟同步。

数据准备

为完成此配置例，需准备如下的数据：

- RouterC 的 IP 地址
- RouterD 的 IP 地址
- NTP 主时钟的等级
- 所有路由器的密钥和证书文件

- 读取文件的密码

操作步骤

步骤 1 配置 RouterC、RouterD、RouterF 的 IP 地址。

按照图 5-8 给每个接口配置 IP 地址。配置完成后，3 台 Router 之间可以互相 ping 通。
具体配置过程略。

步骤 2 配置 NTP 服务器/客户端模式

#将 RouterC 的本地时钟设为自己的参考时钟，等级为 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

使能 NTP 验证功能，配置自动密钥，确保证书文件 ntpkey_cert_routerc 是可信的。

```
<RouterC> system-view
<RouterC> ntp-service authentication enable
<RouterC> ntp-service authentication auto-key password Hello
```

NTP 读取证书文件 ntpkey_host_routerc, ntpkey_cert_routerc 以及(optional) ntpkey_sign_routerc。

在 RouterD 上指定 RouterC 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication auto-key password Hello
[RouterD] ntp-service unicast-server 10.1.1.2 autokey
```

NTP 读取以下文件：ntpkey_host_routerd; ntpkey_cert_routerd 以及(optional) ntpkey_sign_routerd。

完成上述配置后，Router D 可以同步 Router C 的时钟。

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 3，比 Router C 低 1 级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 27
clock offset: 0.0000 ms
root delay: 62.50 ms
root dispersion: 0.20 ms
peer dispersion: 7.81 ms
reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
autokey crypto flags: 0x80001
```

步骤 3 配置 NTP 单播对等体模式

在 RouterE 上指定 RouterD 作为自己的被动对等体。

```
<RouterF> system-view
[RouterF] ntp-service authentication enable
[RouterF] ntp-service authentication auto-key password Hello
[RouterF] ntp-service unicast-peer 10.1.1.3
```

NTP 读取以下文件 tpkey_host_routere; ntpkey_cert_routere, (optional) ntpkey_sign_routere。

由于 RouterE 没有配置主时钟，并且其时钟的等级低于 RouterD，所以 RouterF 同步 RouterD 的时钟。

步骤 4 验证配置结果。

同步后查看 RouterE 的状态。RouterE 的时钟状态为“synchronized”，即，已经完成同步。RouterE 的时钟等级为 4，比被动对等体 RouterD 低 1 级。

```
[RouterE] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.1.1.3
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 124.98 ms
root dispersion: 0.15 ms
peer dispersion: 10.96 ms
reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
autokey crypto flags: 0x80001
```

----结束

配置文件

● RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello
ntp-service refclock-master 2
#
return
```

● RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.3 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello
ntp-service unicast-server 10.1.1.2 autokey
#
return
```

● RouterF 的配置文件

```
#
 sysname RouterE
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.2 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello
ntp-service unicast-peer 10.1.1.3 autokey
#
```

return

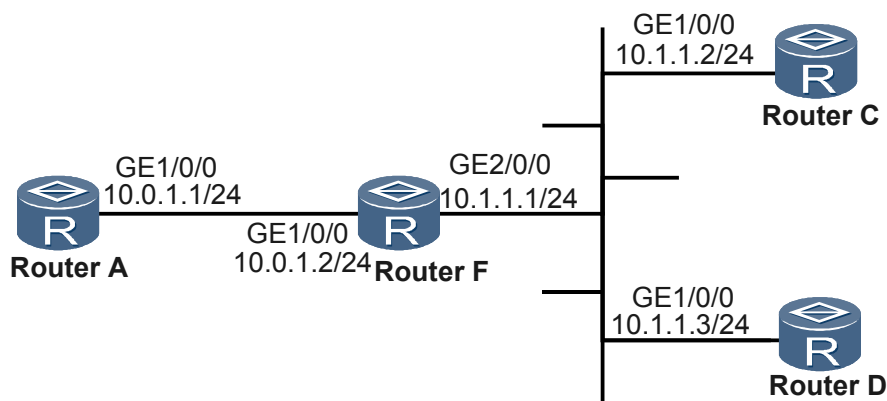
5.5.8 使用 IFF 方案在广播模式下配置 NTP 自动密钥的示例

组网需求

如图图 5-9 所示:

- RouterC 与 RouterD 处于同一网段。RouterA 处于另一网段。RouterF 与两个网段相连。
- RouterC 为一个 NTP 广播服务器，通过 GE 1/0/0 接口发送广播报文。RouterC 的本地时钟作为 NTP 主时钟，等级为 3。
- RouterD 和 RouterA 分别从各自的接口 GE1/0/0 监听广播消息。
- 使能 NTP 验证。

图 5-9 NTP 广播模式的组网图



配置注意事项

在客户端和服务端配置密钥之前，确认已经配置了自动密钥。

配置思路

配置思路如下：

1. 配置 RouterC 为 NTP 广播服务器。
2. 配置 RouterA 与 RouterD 为 NTP 广播客户端。
3. 在 RouterA、RouterC、和 RouterD 上配置 NTP 自动密钥。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterC、RouterD 以及 RouterF 的 IP 地址
- NTP 主时钟的等级

- 验证密钥和证书文件
- IFF 文件
- 打开文件的密码

操作步骤

步骤 1 配置每台 Router 的 IP 地址。

按图图 5-9 配置 IP 地址。具体过程略。

步骤 2 配置 NTP 广播服务器，并启用验证。

配置 RouterC 的本地时钟为 NTP 主时钟，等级为 3。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 3
```

使能 NTP 验证功能，配置自动密钥，并确认证书文件 ntpkey_cert_routerc 是可信的。

```
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey_host_routerc;ntpkey_cert_routerc, (optional)ntpkey_sign_routerc 以及 ntpkey_iffkey_routerc。

配置 RouterC 为 NTP 广播服务器，从接口 GE1/0/0 发送 NTP 广播消息包，并指定使用密钥 ID 16 加密。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service broadcast-server autokey
[RouterC-GigabitEthernet1/0/0] quit
```

步骤 3 配置 RouterD。

使能 NTP 验证。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey_host_routerd; ntpkey_cert_routerd, (optional) ntpkey_sign_routerd, 以及 ntpkey_iffkey_routerc。

配置 RouterD 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterD-GigabitEthernet1/0/0] quit
```

确认路由器上有 ntpkey_iffpar_routerc 文件。

完成上述配置后，Router D 可以同步 Router C 的时钟。

步骤 4 配置 RouterA。

使能 NTP 验证。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 tpkey_host_routera; ntpkey_cert_routera, (optional) ntpkey_sign_routera, 以及 ntpkey_iffkey_routerc。

配置 RouterA 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterA-GigabitEthernet1/0/0]quit
```

确认路由器上有 ntpkey_iffpar_routerc 文件。

步骤 5 验证配置结果。

完成以上配置后，RouterD 能够同步 RouterC 的时钟，而 RouterA 不能同步 RouterC 的时钟。这是因为 RouterA 和 RouterC 不在同一个网段，RouterA 收不到 RouterC 发出的广播报文；而 RouterD 和 RouterC 在同一个网段，因此 RouterD 能够收到 RouterC 发出的广播报文。

查看 RouterD 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterD 的时钟等级为 4，比 RouterC 的时钟低一等级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.42 ms
peer dispersion: 0.00 ms
reference time: 12:17:21.773 UTC Mar 7 2006(C7B7F851.C5EAF25B)
autokey crypto flags: 0x80021
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
ospf 1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.1.1 255.255.255.0
ntp-service broadcast-client
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```

● RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
ntp-service broadcast-server autokey
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
ntp-service refclock-master 3
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.3 255.255.255.0
ntp-service broadcast-client
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
Return
```

- RouterF 的配置文件

```
#
sysname RouterF
#
ospf 1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
return
```

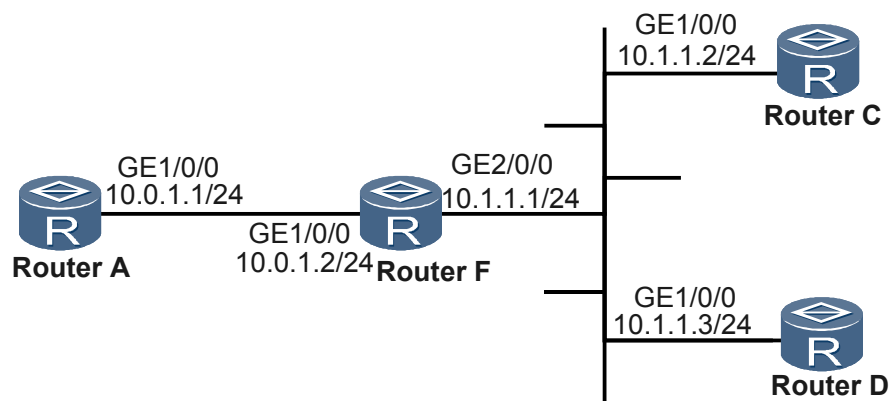
5.5.9 使用 GQ 方案在组播模式下配置自动密钥的示例

组网需求

如图图 5-10 所示:

- RouterC 与 RouterD 处于同一网段。RouterA 处于另一网段。RouterF 与两个网段相连。
- RouterC 为一个 NTP 组播服务器，通过 GE 1/0/0 接口发送组播报文。RouterC 的本地时钟作为 NTP 主时钟，级别为 2。
- RouterD 和 RouterA 分别从各自的接口 GE1/0/0 监听组播报文。

图 5-10 使用 GQ 方案在组播模式下配置 NTP 自动密钥的组网图



配置注意事项

确认客户端与服务器的组播组地址相同。

配置思路

配置思路如下：

1. 配置 RouterC 为 NTP 组播服务器。
2. 配置 RouterA 与 RouterD 作为 NTP 组播客户端。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterC、RouterD 以及 RouterF 的 IP 地址
- NTP 主时钟的等级
- 验证密钥和证书文件
- GQ 文件
- 打开文件的密码

操作步骤

步骤 1 配置每台路由器的 IP 地址。

按图图 5-10 配置 IP 地址。具体过程略。

步骤 2 配置 NTP 组播服务器。

配置 RouterC 的本地时钟为 NTP 主时钟，等级是 2。

```
<RouterC> system-view  
[RouterC] ntp-service refclock-master 2
```

使能 NTP 验证功能，配置自动密钥，并确认证书文件 ntpkey_cert_routerc 是可信的。

```
[RouterC] ntp-service authentication enable  
[RouterC] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey_host_routerc;ntpkey_cert_routerc, (optional)ntpkey_sign_routerc, 以及 ntpkey_gqkey_routerc。

配置 RouterC 作为 NTP 组播服务器，从 GE 1/0/0 接口发送 NTP 组播报文。

```
[RouterC] interface gigabitethernet 1/0/0  
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-server autokey
```

步骤 3 配置 RouterD。

使能 NTP 验证。

```
<RouterD> system-view  
[RouterD] ntp-service authentication enable  
[RouterD] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey_host_routerd; ntpkey_cert_routerd, (optional) ntpkey_sign_routerd, 以及 ntpkey_gqkey_routerc。

配置 RouterD 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ntp-service multicast-client
```

确认路由器上有 ntpkey_iffpar_routerc 文件。

步骤 4 配置 RouterA。

使能 NTP 验证。

```
<RouterA> system-view
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 tpkey_host_routera; ntpkey_cert_routera, (optional)ntpkey_sign_routera, 以及 ntpkey_gqkey_routerc。

配置 RouterA 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-client
```

确认路由器上有 ntpkey_iffpar_routerc 文件。

步骤 5 验证配置结果。

完成以上配置后，RouterD 能够同步 RouterC 的时钟，而 RouterA 不能同步 RouterC 的时钟。这是因为 RouterA 和 RouterC 不在同一个网段，RouterA 收不到 RouterC 发出的广播报文；而 RouterD 和 RouterC 在同一个网段，因此 RouterD 能够收到 RouterC 发出的广播报文。 sent from RouterC.

查看 RouterD 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized", 意味着时钟同步完成。RouterD 的时钟等级为 3，比 RouterC 的时钟低一等级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.66 ms
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005(C61734FD.800303C0)
autokey crypto flags: 0x80041
```

----结束

配置文件

● RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.1 255.255.255.0
 ntp-service multicast-client
#
 ntp-service authentication enable
 ntp-service authentication auto-key password Hello groupname RouterC
#
```


- ```
return
```
- RouterC 的配置文件
 

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
ntp-service multicast-server autokey
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```
  - RouterD 的配置文件
 

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.3 255.255.255.0
ntp-service multicast-client
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```

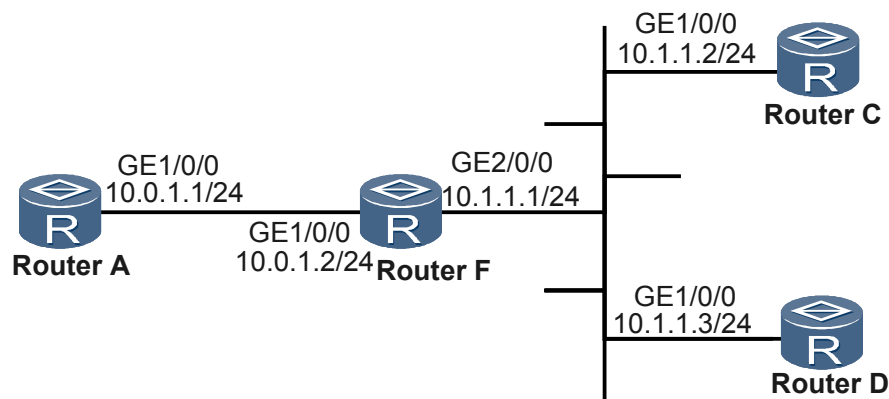
## 5.5.10 使用 MV 方案在多播模式下配置 NTP 自动密钥的示例

### 组网需求

如图图 5-11 所示:

- RouterC 与 RouterD 处于同一网段。RouterA 处于另一网段。RouterF 与两个网段相连。
- RouterC 为一个 NTP 多播服务器，通过 GE 1/0/0 接口发送多播报文。RouterC 的本地时钟为 NTP 主时钟，等级为 2。
- RouterD 和 RouterA 为多播客户端，通过各自的 GE 1/0/0 接口发送报文。

图 5-11 使用 MV 方案在多播模式下配置 NTP 自动密钥的组网图



## 配置注意事项

时钟同步前，在 console 接口视图下执行 **ping** 命令确认多播客户端与多播服务器之间路由可达。

## 配置思路

配置思路如下：

1. 将 RouterC 配置为 NTP 多播服务器。
2. 将 RouterA 与 RouterD 配置为 NTP 多播客户端。

## 数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterC、RouterD 以及 RouterF 的 IP 地址
- NTP 主时钟的等级
- 验证密钥和证书文件
- MV 文件
- 打开文件的密码

## 操作步骤

**步骤 1** 配置每台路由器的 IP 地址。

按图 [图 5-11](#) 配置 IP 地址。具体过程略。

**步骤 2** 配置 NTP 多播服务器。

# 配置 RouterC 的本地时钟为 NTP 主时钟，等级是 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

# 使能 NTP 验证功能，配置自动密钥，并确认证书文件 ntpkey\_cert\_routerc 是可信的。

```
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey\_host\_routerc;ntpkey\_cert\_routerc, (optional)ntpkey\_sign\_routerc, 以及 ntpkey\_mvkey\_routerc。

# 配置 RouterC 为 NTP 多播服务器。NTP 多播服务器在收到多播客户报文后，发送 NTP 多播报文。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-server
```

**步骤 3** 配置 RouterD。

# 使能 NTP 验证。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 ntpkey\_host\_routerd; ntpkey\_cert\_routerd, (optional) ntpkey\_sign\_routerd, 以及 ntpkey\_mvkey\_routerc。

# 配置 RouterD 为 NTP 多播客户端。RouterD 通过 GE 1/0/0 接口向多播服务器发送 NTP 多播报文。

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ntp-service multicast-client autokey
```

确认路由器上有 ntpkey\_iffpar\_routerc 文件。

#### 步骤 4 配置 RouterA。

# 使能 NTP 验证。

```
<RouterA> system-view
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication auto-key password Hello groupname RouterC
```

NTP 读取以下文件 tpkey\_host\_routera; ntpkey\_cert\_routera, (optional)ntpkey\_sign\_routera, 以及 ntpkey\_mvkey\_routerc。

# 配置 RouterA 做为 NTP 多播客户端，通过 GE 1/0/0 接口向多播服务器发送 NTP 多播报文。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-client autokey
```

确认路由器上有 ntpkey\_mvpar\_routerc 文件。

#### 步骤 5 验证配置结果。

配置完成后，RouterA 和 RouterD 能跟 RouterC 进行时钟同步。

查看 RouterD 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterD 的时钟等级为 3，比 RouterC 的时钟低一等级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 0.66 ms
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005 (C61734FD.800303C0)
autokey crypto flags: 0x80081
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.1.1 255.255.255.0
ntp-service multicast-client autokey
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
ntp-service manycast-server
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.3 255.255.255.0
ntp-service manycast-client autokey
#
ntp-service authentication enable
ntp-service authentication auto-key password Hello groupname RouterC
#
return
```

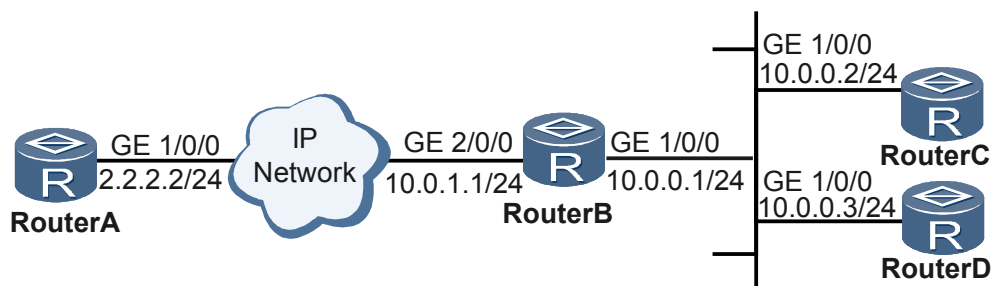
### 5.5.11 在单播服务器/客户端模式下配置 NTP 验证的示例

#### 组网需求

如图图 5-12 所示:

- RouterA 作为 NTP 单播服务器，其本地时钟作为 NTP 主时钟，等级为 2。
- RouterB 作为 NTP 单播客户端，与 RouterA 的时钟进行同步。
- RouterC 和 RouterD 作为 NTP 客户端，把 RouterB 作为自己的 NTP 服务器。
- 使能 NTP 验证。

图 5-12 单播 NTP 服务器/客户端模式组网图



#### 配置注意事项

- 在客户端和服务端配置密钥之前，确认已经配置了密钥。

- 客户端和服务端配置的验证密钥都必须是可信的，另外需要在客户端使能验证功能。

## 配置思路

配置思路如下：

1. 配置 RouterA 作为服务器，提供主时钟。
2. 配置 RouterB 作为 NTP 客户端，同步 RouterA 的时钟。
3. 配置 RouterC、RouterD 作为 NTP 客户端，同步 RouterB 的时钟。
4. 在所有的 Router 上使能 NTP 验证。

### 说明

- 在单播服务器/客户端模式下配置 NTP 验证时时，必须首先在客户端使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。
- 客户端和服务端都需要进行完整的配置，才能验证通过。

## 数据准备

为完成此配置例，需准备如下的数据：

- 参考时钟的 IP 地址
- NTP 主时钟的等级
- 验证密钥及其编号
- 密码

## 操作步骤

**步骤 1** 根据图 [图 5-12](#)，配置 IP 地址，配置 RouterA、RouterB、RouterC 和 RouterD 路由可达。具体配置过程略。

**步骤 2** 在 RouterA 上配置 NTP 主时钟并启动 NTP 验证功能。

# 指定 RouterA 的本地时钟作为 NTP 主时钟，等级为 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2
```

# 使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterA] ntp-service reliable authentication-keyid 42
```

注意服务器端与客户端必须配置相同的验证密钥。

# 配置 ACL 规则。

```
[RouterA] acl 2000
[RouterA] rule 2000 permit source 10.0.0.1 0
```

# 限制访问。

```
[RouterA] ntp-service access limited 2000
```

# 配置接收 NTP 报文的最小以及平均时间间隔。

```
[RouterA] ntp-service discard min-interval 4 avg-interval 4
```

# 使能 KOD。

```
[RouterA] ntp-service kod-enable
```

**步骤 3** 在 RouterB 上配置 NTP 主时钟并启动 NTP 验证功能。

# 在 RouterB 上使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterB] ntp-service reliable authentication-keyid 42
```

# 指定 RouterA 作为 RouterB 的 NTP 服务器，并使用已配置的验证密钥。

```
[RouterB] ntp-service unicast-server 2.2.2.2 authentication-keyid 42
```

**步骤 4** 在 RouterC 上指定 RouterB 作为 RouterC 的 NTP 服务器。

```
<RouterC> system-view
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 42
[RouterC] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

**步骤 5** 在 RouterD 上指定 RouterB 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 42
[RouterD] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

**步骤 6** 验证配置结果。

完成上述配置后，RouterB 可以同步 RouterA 的时钟。

查看 RouterB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 3，比服务器 RouterA 低 1 级。

```
[RouterB] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 2.2.2.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006 (C7B15BCC.D5604189)
autokey crypto flags: 0x80021
```

完成上述配置后，RouterC 可以同步 RouterB 的时钟。

查看 RouterC 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 4，比服务器 RouterB 低 1 级。

```
[RouterC] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2-18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
```

```
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
autokey crypto flags: 0x80021
```

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 4，比 RouterB 低 1 级。B。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.0.0.1
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 3.8128 ms
root delay: 31.26 ms
root dispersion: 74.20 ms
peer dispersion: 34.30 ms
reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
autokey crypto flags: 0x80021
```

查看 RouterA 的 NTP 状态。

```
[RouterA] display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 26.50 ms
peer dispersion: 10.00 ms
reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)
autokey crypto flags: 0x80021
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %ENC;8HX\#Q=~Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service refclock-master 2
acl 2000
rule 2000 permit source 10.0.0.1 0
ntp-service access limited 2000
ntp-service discard min-interval 4 avg-interval 4
ntp-service kod-enable
#
return
```

### ● RouterB 的配置文件

```
#
sysname RouterB
#
```

```

interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.0.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
network 10.0.0.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 2.2.2.2 authentication-keyid 42
#
return

```

- RouterC 的配置文件

```

#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.0.2 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return

```

- RouterD 的配置文件

```

#
sysname RouterD
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.0.3 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return

```

## 5.5.12 在 NTP 对等体模式下配置 KOD 的示例

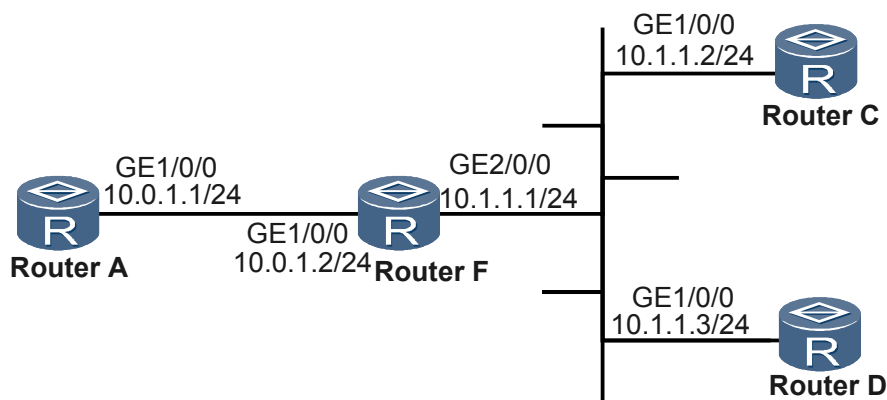
### 组网需求

如图 5-13 所示。在同一个局域网中有 3 台 Router。

- 将 RouterC 的本地时钟设为 NTP 主时钟，等级为 2。
- RouterD 将 RouterC 设为自己的 NTP 服务器。即，RouterD 作为客户端。
- RouterF 将 RouterD 设为自己的被动对等体。即，RouterF 作为主动对等体。



图 5-13 配置 NTP 对等体模式的组网图



## 配置注意事项

在配置对等体模式前，确认对等体对于主机来说是可达的。

## 配置思路

配置思路如下：

1. 配置 RouterC 的本地时钟作为 NTP 主时钟，RouterD 向 RouterC 请求时钟同步。
2. 配置 RouterF 和 RouterD 为对等体，RouterF 向 RouterD 发起时钟同步请求。
3. 最终实现 RouterC、RouterD、RouterF 这 3 台路由器的时钟同步。

## 数据准备

为完成此配置例，需准备如下的数据：

- RouterC 的 IP 地址
- RouterD 的 IP 地址
- NTP 主时钟的等级

## 操作步骤

### 步骤 1 配置 RouterC、RouterD、RouterF 的 IP 地址。

按照图 5-13 给每个接口配置 IP 地址。配置完成后，3 台路由器之间可以互相 ping 通。  
具体配置过程略。

### 步骤 2 配置 NTP 服务器/客户端模式

#将 RouterC 的本地时钟设为自己的参考时钟，等级为 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

# 在 Router 配置 ACL 规则限制访问。

```
<RouterD> system-view
```

```
[RouterD] acl 2000
[RouterD] rule 2000 permit source 128.1.1.4 0
[RouterD] ntp-service access limited 2000

配置接收 NTP 报文的最小以及平均时间间隔。

[RouterD] ntp-service discard min-interval 4 avg-interval 4

使能 KOD。

[RouterD] ntp-service kod-enable

在 RouterD 上指定 RouterC 作为 RouterD 的 NTP 服务器。

[RouterD] ntp-service unicast-server 10.1.1.2
```

完成上述配置后，Router D 可以同步 Router C 的时钟。

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的等级为 3，比 Router C 低 1 级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 62.50 ms
root dispersion: 0.20 ms
peer dispersion: 7.81 ms
reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
autokey crypto flags: 0x80021
```

### 步骤 3 配置 NTP 单播对等体模式

# 在 RouterF 上指定 RouterD 作为自己的被动对等体。

```
<RouterF> system-view
[RouterF] ntp-service unicast-peer 10.1.1.3
```

由于 RouterF 没有配置主时钟，并且其时钟层数低于 RouterD，所以 RouterF 向 RouterD 同步。

### 步骤 4 验证配置结果。

同步后查看 RouterF 的状态。RouterF 的时钟状态为“synchronized”，即，已经完成同步。RouterF 的时钟等级为 4，比被动对等体 RouterD 低 1 级。

```
[RouterF] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.1.1.3
nominal frequency: 64.0029 Hz
actual frequency: 64.0029 Hz
clock precision: 2^7
clock offset: 0.0000 ms
root delay: 124.98 ms
root dispersion: 0.15 ms
peer dispersion: 10.96 ms
reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
autokey crypto flags: 0x80021
```

----结束

## 配置文件

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
ntp-service refclock-master 2
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.3 255.255.255.0
#
acl 2000
 rule 2000 permit source 128.1.1.4 0
ntp-service access limited 2000
ntp-service discard min-interval 4 avg-interval 4
ntp-service kod-enable
 ntp-service unicast-server 10.1.1.2
#
return
```

- RouterF 的配置文件

```
#
 sysname RouterF
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.0.1.2 255.255.255.0
#
 ntp-service unicast-peer 10.1.1.3
#
return
```

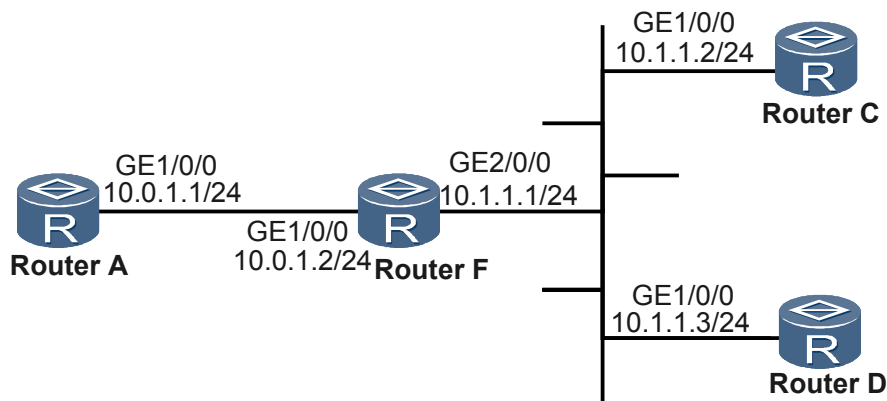
## 5.5.13 在 NTP 多播模式下配置 KOD 的示例

### 组网需求

如图图 5-14 所示:

- RouterC 与 RouterD 处于同一网段。RouterA 处于另一网段。RouterF 与两个网段相连。
- RouterC 为一个 NTP 多播服务器，通过 GE 1/0/0 接口发送多播报文。RouterC 的本地时钟为 NTP 主时钟，等级为 2。
- RouterD 和 RouterA 为多播客户端，通过各自的 GE 1/0/0 接口发送报文。

图 5-14 配置 NTP 多播模式的组网图



## 配置注意事项

时钟同步前，在 console 接口视图下执行 **ping** 命令确认多播客户端与多播服务器之间路由可达。

## 配置思路

配置思路如下：

1. 将 RouterC 配置为 NTP 多播服务器。
2. 将 RouterA 与 RouterD 配置为 NTP 多播客户端。

## 数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterC、RouterD 以及 RouterF 的 IP 地址
- NTP 主时钟的等级

## 操作步骤

**步骤 1** 配置每台路由器的 IP 地址。

按图 5-14 配置 IP 地址。具体过程略。

**步骤 2** 配置 NTP 多播服务器。

# 配置 RouterC 的本地时钟为 NTP 主时钟，等级是 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

# 配置 ACL 规则。

```
[RouterC] acl 2000
[RouterC] rule 2000 permit source 128.1.1.4 0
```

# 限制访问。

```
[RouterC] ntp-service access limited 2000
```

# 配置接收 NTP 报文的最小以及平均时间间隔。

```
[RouterC] ntp-service discard min-interval 4 avg-interval 4
```

# 使能 KOD。

```
[RouterC] ntp-service kod-enable
```

# 配置 RouterC 为 NTP 多播服务器。NTP 多播服务器在收到多播客户报文后，发送 NTP 多播报文。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-server
```

### 步骤 3 配置 RouterD。

# 配置 RouterD 做为 NTP 多播客户端，通过 GE 1/0/0 接口向多播服务器发送 NTP 多播报文。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ntp-service multicast-client
```

### 步骤 4 配置 RouterA。

# 配置 RouterA 为 NTP 多播客户端，通过 GE 1/0/0 接口向多播服务器发送 NTP 多播报文。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-client
```

### 步骤 5 验证配置结果。

配置完成后，RouterA 和 RouterD 能跟 RouterC 进行时钟同步。

查看 RouterD 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterD 的时钟等级为 3，比 RouterC 的时钟低一等级。

```
[RouterD] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.66 ms
root delay: 24.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Apr 25 2005 (C61734FD.800303C0)
autokey crypto flags: 0x80021
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.0.1.1 255.255.255.0
ntp-service multicast-client
#
```

```
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 ntp-service manycast-server
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.3 255.255.255.0
 ntp-service manycast-client
#
return
```

# 6 NQA 配置

## 关于本章

通过配置 NQA，可以有效的检测网络运行的状态，使运营商能够实时采集到各种网络运行指标。

### 6.1 NQA 简介

通过 NQA 简介用户可以了解到 NQA 的基本概念及其所实现的功能。

### 6.2 配置 ICMP 测试

介绍使用 ICMP 测试检测 IP 网络的连通性。

### 6.3 配置 DHCP 测试

介绍使用 NQA 测试与 DHCP 服务器建立连接及获得地址的速度。

### 6.4 配置 FTP 下载测试

介绍使用 NQA 测试 FTP 下载的主要性能指标。

### 6.5 配置 FTP 上载测试

介绍使用 NQA 测试 FTP 上载的主要性能指标。

### 6.6 配置 HTTP 测试

介绍使用 NQA 测试 HTTP 服务各阶段的响应速度。

### 6.7 配置 DNS 测试

介绍使用 NQA 测试 DNS 解析速度。

### 6.8 配置 Traceroute 测试

介绍使用 NQA 进行 Traceroute 测试，查看网络中每一跳的连通情况。

### 6.9 配置 SNMP 查询测试

介绍使用 NQA 测试主机与 SNMP Agent 之间的通信状况。

### 6.10 配置 TCP 测试

介绍使用 NQA 测试 TCP 端口的响应速度。

### 6.11 配置 UDP 测试

介绍使用 NQA 测试 UDP 端口的响应速度。

### 6.12 配置 Jitter 测试

介绍使用 NQA 测试网络的抖动情况。客户端和服务端都必须为华为设备才能进行 Jitter 测试。

#### 6.13 配置基于接口板发包的 Jitter 测试

使用基于接口板发送的 Jitter 测试可以得到更加精确的网络抖动情况的数据。

#### 6.14 配置 LSP Ping 测试

介绍使用 NQA 检测 LSP 隧道的运行情况。

#### 6.15 配置 LSP Jitter 测试

介绍使用 NQA 测试 LSP 隧道中报文传输时的抖动情况。

#### 6.16 配置 LSP Traceroute 测试

介绍使用 LSP Traceroute 测试测试隧道各个 LSR 的连通性。

#### 6.17 配置 ICMP Jitter 测试

介绍使用 ICMP Jitter 测试测试 IP 网络的抖动情况。

#### 6.18 配置基于接口板发包的 ICMP Jitter 测试

介绍使用基于接口板发送的 ICMP Jitter 测试测试 IP 网络的抖动情况。使用基于接口板发送的 ICMP Jitter 测试可以得到更加准确的了解到网络的抖动情况。

#### 6.19 配置 Path Jitter 测试

介绍使用 Path Jitter 测试测试报文传输路径上的各个设备的通信情况。

#### 6.20 配置 Path MTU 测试

介绍使用 Path MTU 测试测试报文传输路径上的路径 MTU 值。

#### 6.21 配置 NQA 测试例实现 MPing 保留组地址

介绍使用 NQA 进行 MPing 保留组地址测试，检测出接口所在网段上存在哪些保留组成员。

#### 6.22 配置 NQA 测试例实现 MPing 普通组地址

介绍使用 NQA 进行 MPing 普通地址测试，查看检查协议运行状态是否正常，确认组播分发树是否正确建立；检查网络中存在的组成员，计算从 MPing 发起者到组成员的 TTL、响应时间等参数。

#### 6.23 通过 NQA 检测从组播源到查询者的 RPF 路径

介绍使用 NQA 进行从组播源到查询者的 RPF 路径测试。

#### 6.24 通过 NQA 检测从组播源到查询者的组播路径

介绍使用 NQA 进行从组播源到查询者的组播路径测试。

#### 6.25 通过 NQA 检测从组播源到目的主机的 RPF 路径

介绍使用 NQA 进行从组播源到目的主机的 RPF 路径测试。

#### 6.26 通过 NQA 检测从组播源到目的主机的组播路径

介绍使用 NQA 进行从组播源到目的主机的组播路径测试。

#### 6.27 配置单跳 PW 的 PWE3 Ping 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Ping 测试，了解 PW 的连通情况。

#### 6.28 配置多跳 PW 的 PWE3 Ping 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Ping 测试，了解 PW 的连通情况。

#### 6.29 配置单跳 PW 的 PWE3 Trace 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Trace 测试，了解 PW 上各个设备的连通性。

#### 6.30 配置多跳 PW 的 PWE3 Trace 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Trace 测试，了解 PW 上各个设备的连通性。



### 6.31 配置多跳跨域 Kompella VLL 的 VC Trace 测试

介绍使用 NQA 进行多跳跨域 Kompella VLL 的 VC Trace 测试。

### 6.32 配置 NQA 测试组

当需要对多个目的地进行 ICMP、Jitter、TCP、UDP、SNMP、LSPPing、LSPJitter、ICMPJitter、PWE3Ping 等类型的测试时，可以采用 NQA 测试组的方式，将相同类型的测试例加入同一个测试组，进行统一管理。

### 6.33 配置 NQA 测试例的通用参数

介绍一些 NQA 测试常用的测试参数，并说明各个参数都可以应用到哪些测试例中。

### 6.34 配置 NQA 双向传输延迟阈值

介绍配置 NQA 双向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

### 6.35 配置 NQA 单向传输延迟阈值

介绍配置 NQA 单向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

### 6.36 配置 NQA 测试的 Trap 开关

通过配置 NQA 测试的 Trap 开关可以实现 NQA 测试成功或者失败产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

### 6.37 配置测试结果发送到 FTP 服务器

网管需要了解到设备的测试结果，如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

### 6.38 配置上下限 NQA 阈值告警

在 NQA 的测试结果超出阈值时，向网管发送告警信息，通知设备出现的变化情况。

### 6.39 配置 VPLS 组播 Ping 检测 VPLS 网络测试

介绍使用 NQA 进行 Martini 方式的 VPLS 网络测试，了解网络的连通情况。

### 6.40 配置 VPLS 组播 Ping 检测 Kompella VPLS 网络测试

介绍使用 NQA 进行 Kompella 方式的 VPLS 网络测试，了解网络的连通情况。

### 6.41 配置 MAC Trace 测试

MAC Trace 测试支持对 VLAN 和 VPLS 网络的检测。

### 6.42 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性

使用 NQA GMAC Ping 和 GMAC Trace 功能测试 VLAN 连通性，除了可以检测网络连通性和定位故障外，还可以获得时延等信息。

### 6.43 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性

使用 NQA GMAC Ping 和 GMAC Trace 功能测试 VPLS 连通性，除了可以检测网络连通性和定位故障外，还可以获得时延等信息。

### 6.44 配置 VPLS PW Ping 和 PW Trace 测试

### 6.45 配置 VPLS 组播 Trace 检测 VPLS 网络测试

### 6.46 配置 VPLS MAC Ping 测试

### 6.47 配置 VPLS MAC Trace 测试

### 6.48 配置 NQA 报文改写检查功能

NQA 报文改写检查功能用于检查报文内容是否被改写。

### 6.49 维护 NQA

在测试中需要对测试进行维护时，可以通过重新启动测试例，清空测试结果信息实现对测试例的维护。

#### 6.50 NQA 配置举例

介绍 NQA 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

## 6.1 NQA 简介

通过 NQA 简介用户可以了解到 NQA 的基本概念及其所实现的功能。

### 6.1.1 NQA 概述

通过 NQA 概述，用户可以了解到 NQA 的引入及其实现的功能。

### 6.1.2 NQA 与 Ping 的比较

通过 NQA 与 Ping 的比较，用户可以了解到 NQA 与 Ping 在测试方式方面的区别。

### 6.1.3 NQA 客户端和服务端

本节介绍到 NQA 客户端、服务器和 NQA 测试例之间的关系。

### 6.1.4 NE20E-X6 支持的 NQA 特性

介绍了 NE20E-X6 支持的 NQA 测试例类型及调度方式。

## 6.1.1 NQA 概述

通过 NQA 概述，用户可以了解到 NQA 的引入及其实现的功能。

随着运营商增值业务的开展，用户和运营商对 QoS 的相关要求越来越高，特别是在传统的 IP 网络承载语音和视频业务后，运营商与客户之间签订 SLA（Service Level Agreement）成为普遍现象。

为了让用户看到承诺的带宽是否达到需求，运营商需要设备侧提供相关的时延、抖动、丢包率等相关的统计参数，以及时了解网络的性能状况。

NE20E-X6 提供 NQA（Network Quality Analysis）功能满足上述需求。

NQA 可以测量网络上运行的各种协议的性能，使运营商能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、文件传输速率、FTP 连接时延、DNS 解析时延、DNS 解析错误率等。通过对这些指标进行控制，运营商可以为用户提供不同等级的网络服务，收取不同的费用。

同时，NQA 也是网络故障诊断和定位的有效工具。

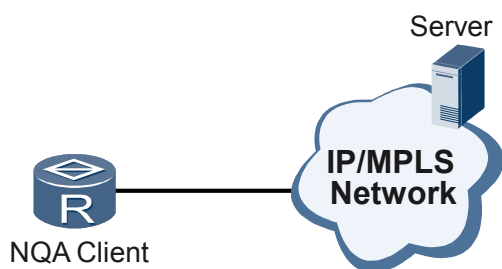
## 6.1.2 NQA 与 Ping 的比较

通过 NQA 与 Ping 的比较，用户可以了解到 NQA 与 Ping 在测试方式方面的区别。

NQA 是对 Ping 功能的扩展和增强。

Ping 使用 ICMP（Internet Control Message Protocol）测试数据包测试本端和指定目的端之间的往返时间，NQA 不但可以完成这项功能，还可以探测 TCP、UDP、DHCP、FTP、HTTP、SNMP 服务是否打开，以及测试各种服务的响应时间。如图 6-1 所示。

图 6-1 NQA 测试示意图



与 Ping 不同，NQA 不在控制台终端实时显示每个包的往返时间或是否超时，而是在测试结束后通过 **display nqa results** 命令来查看 NQA 的测试结果。

用户也可以通过网管来设置 NQA 各项操作的参数，并启动测试。

### 6.1.3 NQA 客户端和服务端

本节介绍到 NQA 客户端、服务器和 NQA 测试例之间的关系。

#### NQA 测试例和 NQA 客户端

NQA 可以对多个项目进行测试，每个项目都需要创建一个测试例，且每个测试例只能是某一种类型的 NQA 测试。

NQA 测试例在客户端创建。每个测试例都有一个管理员名称和一个操作标签，管理员名称和操作标签可以唯一确定一个测试例。

在测试例视图下，需要配置相关的测试参数。其中，有些参数只适用于某种类型的测试例，另外一些则适用于所有类型的测试例。

#### NQA 服务器

在大多数的测试项中，只需要配置 NQA Client 端。但在进行 TCP、UDP 和 Jitter 类型测试时，必须配置 NQA 服务器。

NQA 服务器负责处理 NQA 客户端发来的测试包，如图 6-2 所示，NQA 服务器通过监听功能对客户端发起的测试进行响应。

图 6-2 NQA 客户端和服务器的关系



可以在一个 NQA 服务器上创建多个 TCP 或 UDP 监听服务，每个监听服务对应一组指定的目的地址和端口号，目的地址和端口号可以重复。

#### NQA 测试执行

只有在 NQA 服务器上配置了相应的监听地址和端口号后，客户端发起的请求才能得到服务器的响应。并且，服务器监听服务中指定的 IP 地址、端口号要和客户端配置的参数一致。

创建测试例并配置好相关测试项参数之后，必须通过命令 **start** 启动 NQA 测试，并使用 **display nqa results** 命令查看测试结果。

### 6.1.4 NE20E-X6 支持的 NQA 特性

介绍了 NE20E-X6 支持的 NQA 测试例类型及调度方式。

## NQA 提供的特性

- 与网管的配合：
  - 网管可以完全管理 NQA 的所有功能
  - 支持 NQA MIB 用户接口
  - 支持 Disman-traceroute-MIB 用户接口
  - 支持 Disman-NSLookUp-MIB 用户接口
  - 支持 Disman-ping-MIB 用户接口
- 支持多种类型的测试：
  - ICMP 测试
  - DHCP 测试
  - FTP 测试
  - HTTP 测试
  - DNS 测试
  - Traceroute 测试
  - SNMP 测试
  - TCP 测试
  - UDP 测试
  - ICMP Jitter 测试
  - UDP Jitter 测试
  - LSP Ping 测试
  - LSP Jitter 测试
  - LSP Traceroute 测试
  - Mtrace 测试
  - Mping 测试
  - PWE3 Ping 测试
  - PWE3 Trace 测试
  - MAC Ping 测试
  - MAC Trace 测试
  - MACTunnel Ping 测试
  - VPLS MAC Ping 测试
  - VPLS MAC Trace 测试
  - Path Jitter 测试
  - Path MTU 测试
  - 基于接口板发包的 Jitter 测试
  - 基于接口板发包的 ICMP Jitter 测试
  - VPLS 组播 Ping 测试
  - VPLS 组播 Trace 测试
  - VPLS PW Ping 测试
  - VPLS PW Trace 测试

- GMAC Trace 测试
- GMAC Trace 测试
- Jitter 类型的测试例支持最大连续发送报文数目 3000，可模拟语音业务流量。
- 支持配置 2000 个测试例。
- 支持毫秒级和微秒级统计。
- 支持热备份：  
实现主控板和备板上 NQA 测试例的配置信息同步，发生主备倒换后时，NQA 测试例能正常测试，避免了主备倒换时主控板和备板上的数据不一致。
- 支持测试例的任务调度：  
实现对测试例的调度，降低设备的并发负担。  
对单个测试例，支持多种启动时间、结束时间的设置：
  - 支持立即启动、延迟启动、定时启动
  - 支持报文发送完后自动结束、立即结束、延迟结束、定时结束、生命周期结束多个任务同时启动时，设备主动合理分布启动时间和测试间隔。
- 对于 ICMP、Jitter、TCP、UDP、SNMP、LSP Ping、LSP Jitter、ICMP Jitter、PWE3 Ping、VPLS PW Ping 类型的测试，支持通过测试组管理多个测试例。
- 支持自动延时功能。可以最大限度的利用系统的资源，在规定的时间内完成测试例。
- 支持单向延迟统计和双向延迟统计，并且可以通过设定阈值，对测试结果中超过阈值的报文进行统计。
- 支持单向丢包统计。
- 支持动态减少测试例。
- 支持通过 FTP 将测试结果发送到 FTP 服务器。
- 支持灵活告警机制。即，根据被测对象的 OID，为被测对象设置上限和下限阈值，监控被测对象的性能。当测试结果超过阈值时，根据当前事件触发告警。

## 6.2 配置 ICMP 测试

介绍使用 ICMP 测试检测 IP 网络的连通性。

### 6.2.1 建立配置任务

在配置 ICMP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.2.2 配置 ICMP 测试参数

在 ICMP 测试时，需要配置的相关参数。

### 6.2.3 检查配置结果

在配置 ICMP 测试成功后，可以查看到测试的结果数据。

## 6.2.1 建立配置任务

在配置 ICMP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

ICMP 测试提供类似于普通 **ping** 命令的功能，但输出信息更为丰富。

## 前置任务

在配置 ICMP 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

## 数据准备

在配置 ICMP 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                   |
|----|--------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                 |
| 2  | 目的地址                                                                                 |
| 3  | (可选) VPN 实例名、发送测试报文的源接口、源 IP 地址、Echo Request 报文大小、TTL、ToS、填充字符、测试报文发送间隔、NQA 测试的失败百分比 |
| 4  | 启动方式和结束方式                                                                            |

## 6.2.2 配置 ICMP 测试参数

在 ICMP 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下述配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type icmp**，配置测试例类型为 ICMP。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5** (可选) 根据需要，配置 ICMP 测试其他参数。
- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
  - 执行命令 **source-interface interface-type interface-number**，配置发送测试报文的源接口。
  - 执行命令 **source-address ipv4 ip-address**，配置源地址。该参数相当于 **ping** 命令中的“-a”选项。
  - 执行命令 **datasize size**，配置 Echo Request 报文的大小，不包括 IP 头。该参数相当于 **ping** 命令中的“-s”选项。

- 执行命令 **ttl number**，配置 TTL 值。该参数相当于 **ping** 命令中的“-h”选项。
- 执行命令 **tos value**，配置服务类型，即 IP 报文头中 ToS 字段的值。该参数相当于 **ping** 命令中的“-tos”选项。
- 执行命令 **datafill fillstring**，配置填充字符。该参数相当于 **ping** 命令中的“-p”选项。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。该参数相当于 **ping** 命令中的“-m”选项。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

#### 步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.2.3 检查配置结果

在配置 ICMP 测试成功后，可以查看到测试的结果数据。

### 前提条件

已经完成 ICMP 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

### 任务示例

执行 **display nqa results** 命令，如果测试已经成功结束，可以看到以下信息。

- testFlag is inactive
- The test is finished
- Completion:success

对于 ICMP 类型的测试，还可以看到接收到响应报文的最小时间、最大时间、RTT（往返时延）。

```
<HUAWEI> display nqa results
```



```
NQA entry(admin, test) :testflag is inactive ,testtype is icmp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:10.112.58.3
Min/Max/Average Completion Time: 2/5/3
Sum/Square-Sum Completion Time: 9/33
Last Good Probe Time: 2010-06-21 15:33:09.2
Lost packet ratio: 0 %
```

## 6.3 配置 DHCP 测试

介绍使用 NQA 测试与 DHCP 服务器建立连接及获得地址的速度。

### 6.3.1 建立配置任务

在配置 DHCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.3.2 配置 DHCP 测试参数

在配置 DHCP 测试时，需要配置的相关参数

### 6.3.3 检查配置结果

在 DHCP 测试成功后，可以查看到 DHCP 测试的结果数据。

## 6.3.1 建立配置任务

在配置 DHCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

通过 NQA DHCP 测试，可以得到以下信息：

- 客户端与 DHCP 服务器之间建立连接的时间。
- 客户端获得地址的时间。

### 前置任务

在配置 DHCP 测试之前，需完成以下任务：

- 配置 DHCP 服务器或 DHCP Relay
- 配置 NQA 客户端与 DHCP 服务器或 DHCP Relay 间路由可达

### 数据准备

在配置 DHCP 测试之前，需要准备以下数据：

| 序号 | 数据                   |
|----|----------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名 |
| 2  | 与 DHCP 服务器相连的出接口     |

| 序号 | 数据                     |
|----|------------------------|
| 3  | (可选)：超时时间、NQA 测试的失败百分比 |
| 4  | 启动方式和结束方式              |

## 6.3.2 配置 DHCP 测试参数

在配置 DHCP 测试时，需要配置的相关参数

### 背景信息

 说明

NE20E-X6 支持将路由器配置为 DHCP 服务器，相关配置步骤请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 用户接入》的“DHCPv4 配置”。

在 NQA 客户端上进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type dhcp**，配置测试例类型为 DHCP。

**步骤 4** 执行命令 **source-interface interface-type interface-number**，指定发送 DHCP 请求报文的源接口。

该接口可以是与 DHCP 服务器相连的以太网口、Eth-Trunk 接口、Virtual-Ethernet 接口、Vlanif 接口。

**步骤 5** (可选) 根据需要，配置 DHCP 测试其他参数。

- 执行命令 **timeout time**，配置 NQA 测试例的操作超时时间。

 说明

对于 DHCP 测试，发送完探测报文后，等待响应的时间可能达到 10 秒。缺省情况下，超时时间是 15 秒，如需要设置为其他的值，建议设置的值在 10 秒以上。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。

- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } ]**，延迟指定时间后启动测试例。

----结束

### 6.3.3 检查配置结果

在 DHCP 测试成功后，可以查看到 DHCP 测试的结果数据。

#### 前提条件

已经完成 DHCP 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

#### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

#### 任务示例

执行 **display nqa results** 命令，如果测试已经成功结束，可以看到以下信息：

- testFlag is inactive
- The test is finished
- Completion:success

对于 DHCP 类型的测试，还可以在扩展结果中看到以下信息：

- 与服务器断开连接的次数；
- 断开连接操作的超时次数；
- 服务器忙的次数；
- 连接失败的次数
- 操作顺序错误次数；
- 丢弃操作次数；
- 操作统计错误次数；

```
<HUAWEI> display nqa results
NQA entry(admin, dhcp) :testFlag is inactive ,testtype is dhcp
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.1.1.3
 Min/Max/Average Completion Time: 1030/1030/1030
 Sum/Square-Sum Completion Time: 1030/1060900
 Last Good Probe Time: 2007-6-29 16:00:2.2
 Lost packet ratio: 0 %
```

## 6.4 配置 FTP 下载测试

介绍使用 NQA 测试 FTP 下载的主要性能指标。

### 6.4.1 建立配置任务

在配置 FTP 下载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.4.2 配置 FTP 下载测试参数

在配置 FTP 下载测试时，需要配置的相关参数。

### 6.4.3 检查配置结果

在 FTP 下载成功后，可以查看到 FTP 下载测试的结果数据。

### 6.4.1 建立配置任务

在配置 FTP 下载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

#### 应用环境

在 NQA 的 FTP 下载测试中，本地作为 FTP 客户端，从 FTP 服务器下载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

#### 前置任务

在配置 FTP 下载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA FTP 客户端与 FTP 服务器之间路由可达

#### 数据准备

在配置 FTP 下载测试之前，需要准备以下数据：

| 序号 | 数据                                               |
|----|--------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                             |
| 2  | FTP 服务器的 IP 地址                                   |
| 3  | (可选) FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号 |
| 4  | FTP 用户名和密码                                       |
| 5  | 要下载的文件名                                          |
| 6  | 启动方式和结束方式                                        |

## 6.4.2 配置 FTP 下载测试参数

在配置 FTP 下载测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type ftp**，配置测试例类型为 FTP。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5**（可选）根据需要，配置 FTP 测试其他参数

- 执行命令 **source-address ipv4 ip-address**，配置测试例的源地址。
- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-port port-number**，配置源端口。
- 执行命令 **destination-port port-number**，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 6** 执行命令 **ftp-operation get**，配置操作类型为 Get。

缺省情况下，FTP 操作类型为 Get 操作。

**步骤 7** 执行命令 **ftp-username name**，配置 FTP 用户名。

**步骤 8** 执行命令 **ftp-password password**，配置 FTP 密码。

**步骤 9** 执行命令 **ftp-filename file-name**，配置 FTP 操作文件名。

 说明

在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

**步骤 10** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.4.3 检查配置结果

在 FTP 下载成功后，可以查看到 FTP 下载测试的结果数据。

### 前提条件

已经完成 FTP 下载测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

### 任务示例

对于 FTP 下载测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<HUAWEI> display nqa results
NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
1 . Test 1 result The test is finished
 SendProbe:1
 Completion :success
 MessageBodyOctetsSum: 448
 Operation timeout number: 0
 Drop operation number:0
 CtrlConnTime Min/Max/Average: 438/438/438
 DataConnTime Min/Max/Average: 218/218/218
 SumTime Min/Max/Average: 656/656/656
 Average RTT:380
 Lost packet ratio: 0 %
 ResponseProbe:1
 RTD OverThresholds number: 0
 Stats errors number: 0
 System busy operation number:0
 Disconnect operation number: 0
```

## 6.5 配置 FTP 上载测试

介绍使用 NQA 测试 FTP 上载的主要性能指标。

### 6.5.1 建立配置任务

在配置 FTP 上载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.5.2 配置 FTP 上载测试参数

在配置 FTP 上载测试参数时，需要配置的相关参数。

### 6.5.3 检查配置结果

在 FTP 上载测试成功后，可以查看到 FTP 上载测试的结果数据。

## 6.5.1 建立配置任务

在配置 FTP 上载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

在 NQA 的 FTP 上载测试中，本地作为 FTP 客户端，向 FTP 服务器上载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

进行上载测试时，可以指定要上载的文件，也可以指定要上载的字节数，NQA 客户端自动构造测试文件上载。

### 前置任务

在配置 FTP 上载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA 客户端与 FTP 服务器之间路由可达

### 数据准备

在配置 FTP 上载测试之前，需要准备以下数据：

| 序号 | 数据                                               |
|----|--------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                             |
| 2  | FTP 服务器的 IP 地址                                   |
| 3  | FTP 用户名和密码                                       |
| 4  | (可选) FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号 |
| 5  | 要上载的文件名或文件大小                                     |
| 6  | 启动方式和结束方式                                        |

## 6.5.2 配置 FTP 上载测试参数

在配置 FTP 上载测试参数时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。



**步骤 2** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type** *ftp*，配置测试例类型为 FTP。

**步骤 4** 执行命令 **destination-address** *ipv4 ip-address*，配置目的地址。

**步骤 5** （可选）根据需要，配置 FTP 测试其他参数

- 执行命令 **source-address** *ipv4 ip-address*，配置测试例的源地址。
- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 6** 执行命令 **ftp-operation** *put*，配置操作类型为 Put。

缺省情况下,FTP 的操作类型是 GET。

**步骤 7** 执行命令 **ftp-username** *name*，配置 FTP 用户名。

**步骤 8** 执行命令 **ftp-password** *password*，配置 FTP 密码。

**步骤 9** 指定要上载的文件，有两种方式可以选择。

- 如果要上载指定名称的文件，使用命令 **ftp-filename** *file-name*。

 说明

- 可以不指定文件路径，系统会在当前路径下查找该文件。如果指定的文件名不存在，则按照指定文件名来构造一个文件，上载文件的大小为 1M。
- 文件名不能包含字符：“~、\*、/、\、'、"、，”，文件路径可以包含这些字符。
- 文件名中可以包含扩展名，但不能只有扩展名。如.txt。
- 如果要上载指定大小的文件，使用命令 **ftp-filesize** *size*。客户端将自动构建一个名为“nqa-ftp-test.txt”的文件上载。

 说明

在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

**步骤 10** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，延迟指定时间后启动测试例。

----结束

## 6.5.3 检查配置结果

在 FTP 上载测试成功后，可以查看到 FTP 上载测试的结果数据。



## 前提条件

已经完成 FTP 上载测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 执行 **display nqa results** 命令查看测试结果。

----结束

## 任务示例

对于 FTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<HUAWEI> display nqa results
NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
1 . Test 1 result The test is finished
 SendProbe:1
 Completion :success
 MessageBodyOctetsSum: 448
 Operation timeout number: 0
 Drop operation number:0
 CtrlConnTime Min/Max/Average: 438/438/438
 DataConnTime Min/Max/Average: 218/218/218
 SumTime Min/Max/Average: 656/656/656
 Average RTT:380
 Lost packet ratio: 0 %
 ResponseProbe:1
 RTD OverThresholds number: 0
 Stats errors number: 0
 System busy operation number:0
 Disconnect operation number: 0
```

## 6.6 配置 HTTP 测试

介绍使用 NQA 测试 HTTP 服务各阶段的响应速度。

### 6.6.1 建立配置任务

在配置 HTTP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.6.2 配置 HTTP 测试参数

在配置 HTTP 测试时，需要配置的相关参数。

### 6.6.3 检查配置结果

在 HTTP 测试成功后，可以查看到 HTTP 测试的结果数据。

## 6.6.1 建立配置任务

在配置 HTTP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

NQA 的 HTTP 测试提供三个阶段的响应速度：

- DNS 解析时间：客户端发送 DNS 报文给名字解析器，将 HTTP 服务器名字解析为 IP 地址，DNS 解析报文返回的时间。
- TCP 建立连接时间：客户端与 HTTP 服务器通过 TCP “三次握手” 建立连接所用的时间。
- 交易时间：客户端发送 Get 或 Post 报文给 HTTP 服务器，响应报文到达 HTTP 服务器的时间。

## 前置任务

在配置 HTTP 测试之前，需完成以下任务：

- 配置 HTTP 服务器
- 配置 NQA 客户端与 HTTP 服务器之间路由可达

## 数据准备

在配置 HTTP 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                      |
| 2  | HTTP 服务器名                                                                                                 |
| 3  | <ul style="list-style-type: none"><li>● （可选）源端口号</li><li>● （可选）目的端口号</li><li>● （可选）NQA 测试的失败百分比</li></ul> |
| 4  | HTTP 操作类型                                                                                                 |
| 5  | HTTP 测试所访问的页面和版本信息                                                                                        |
| 6  | 启动方式和结束方式                                                                                                 |

### 6.6.2 配置 HTTP 测试参数

在配置 HTTP 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 HTTP 客户端。

## 操作步骤

**步骤 1** 执行命令 `system-view`，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type http**，配置测试例类型为 HTTP。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5**（可选）根据需要，配置 HTTP 测试其他参数

- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **source-port port-number**，配置源端口。
- 执行命令 **destination-port port-number**，配置目的端口。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 6** 执行命令 **http-operation { get | post }**，配置 HTTP 操作类型。

缺省情况下，HTTP 操作类型为 Get 操作。

**步骤 7** 执行命令 **http-url deststring [ verstring ]**，配置 HTTP 测试所访问的页面以及 HTTP 版本信息。

 说明

执行命令 **http-url deststring [ verstring ]**，直接输入网页名即可。如果输入的内容中包含“http: //”、域名信息，则会导致测试例失败。

在不配置 HTTP 版本信息的情况下，缺省情况下支持 HTTP1.0。通过配置可以支持 HTTP1.1。

**步骤 8** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

----结束

## 6.6.3 检查配置结果

在 HTTP 测试成功后，可以查看到 HTTP 测试的结果数据。

### 前提条件

已经完成 HTTP 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 执行 **display nqa results** [ test-instance admin-name test-name ]命令查看测试结果。

----结束

## 任务示例

对于 HTTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段的响应速度。

- DNS 查询时间：DNSRTT
- TCP 连接建立时间：TCPConnectRTT
- 服务器返回数据时间：TransactionRTT、RTT

```
<HUAWEI> display nqa results
NQA entry (admin, http) :testflag is inactive ,testtype is http
1. Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:succcess RTD OverThresholdsnumber: 0
 MessageBodyOctetsSum: 411 TargetAddress: 100.2.1.200
 DNSQueryError number: 0 HTTPError number: 0
 TcpConnError number : 0 System busy operation number:0
 DNSRTT Sum/Min/Max:0/0/0 TCPConnectRTT Sum/Min/Max: 6/1/4
 TransactionRTT Sum/Min/Max: 3/1/1
 RTT Sum/Min/Max/Avg: 7/1/5/2
 DNSServerTimeout:0 TCPConnectTimeout:0 TransactionTimeout: 0
 Lost packet ratio:0%
```

## 6.7 配置 DNS 测试

介绍使用 NQA 测试 DNS 解析速度。

### 6.7.1 建立配置任务

在配置 DNS 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.7.2 配置 DNS 测试参数

在配置 DNS 测试时，需要配置的相关参数。

### 6.7.3 检查配置结果

在 DNS 测试成功后，可以查看到 DNS 测试的结果数据。

## 6.7.1 建立配置任务

在配置 DNS 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

DNS 测试用于检测将给定的 DNS 名称解析成 IP 地址的速度。

## 前置任务

在配置 DNS 测试之前，需完成以下任务：

- 配置 DNS 服务器

- 配置 NQA 客户端与 DNS 服务器之间路由可达

## 数据准备

在配置 DNS 测试之前，需要准备以下数据：

| 序号 | 数据                   |
|----|----------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名 |
| 2  | DNS 服务器的 IP 地址       |
| 3  | 要解析的目的主机名            |
| 4  | 启动方式和结束方式            |

## 6.7.2 配置 DNS 测试参数

在配置 DNS 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 DNS 客户端。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **dns resolve**，使能基于 DNS 的动态域名解析功能。  
缺省情况下，动态域名解析功能被禁止。
- 步骤 3** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 4** 执行命令 **test-type dns**，配置测试例类型为 DNS。
- 步骤 5** 执行命令 **dns-server ipv4 ip-address**，配置 DNS 服务器地址的 IPv4 地址。
- 步骤 6** 执行命令 **destination-address url urlstring**，配置目的主机名。
- 步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.7.3 检查配置结果

在 DNS 测试成功后，可以查看到 DNS 测试的结果数据。

### 前提条件

已经完成 DNS 测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

### 任务示例

对于 DNS 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is dns
1. Test 1 result The test is finished
 Send operation times: 1 Receive response times: 1
 Completion:succcess RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.82.55.191
 Min/Max/Average Completion Time: 4/4/4
 Sum/Square-Sum Completion Time: 4/16
 Last Good Probe Time: 2010-06-21 15:40:12.6
 Lost packet ratio: 0 %
```

## 6.8 配置 Traceroute 测试

介绍使用 NQA 进行 Traceroute 测试，查看网络中每一跳的连通情况。

### 6.8.1 建立配置任务

在配置 Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.8.2 配置 Traceroute 测试参数

在配置 Traceroute 测试时，需要配置的相关参数。

### 6.8.3 检查配置结果

在 Traceroute 测试成功后，可以查看到 Traceroute 测试的结果数据。

## 6.8.1 建立配置任务

在配置 Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

NQA 的 Traceroute 测试提供类似于普通 Traceroute 命令的功能，但输出信息更为丰富。

## 前置任务

在配置 Traceroute 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

## 数据准备

在配置 Traceroute 测试之前，需要准备以下数据：

| 序号 | 数据                                                |
|----|---------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                              |
| 2  | 目的地址                                              |
| 3  | （可选）：VPN 实例名、允许的最大跳失败数、报文的初始 TTL 和最大 TTL、源地址、目的端口 |
| 4  | 启动方式和结束方式                                         |

## 6.8.2 配置 Traceroute 测试参数

在配置 Traceroute 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type trace**，配置测试例类型为 Traceroute。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置 Traceroute 测试的目的地址。
- 步骤 5** （可选）根据需要，配置 Traceroute 测试其他参数。
  - 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
  - 执行命令 **tracert-hopfailtimes times**，配置 NQA 测试 Traceroute 测试例的跳失败数。
  - 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。
  - 执行命令 **tos value**，配置测试包的服务类型 TOS。
  - 执行命令 **source-address ipv4 ip-address**，配置源地址。
  - 执行命令 **destination-port port-number**，配置目的端口。

- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

#### 步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.8.3 检查配置结果

在 Traceroute 测试成功后，可以查看到 Traceroute 测试的结果数据。

### 前提条件

已经完成 Traceroute 测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

### 任务示例

对于 Traceroute 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到每一跳的统计信息。

```
<HUAWEI> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is trace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2010-06-21 15:41:01.7
1 . Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 1/2/1
 Sum/Square-Sum Completion Time: 4/6
 RTD OverThresholds number: 0
 Last Good Probe Time: 2010-06-21 15:41:01.7
 Destination ip address:10.112.58.3
 Lost packet ratio: 0 %
```



## 6.9 配置 SNMP 查询测试

介绍使用 NQA 测试主机与 SNMP Agent 之间的通信状况。

### 6.9.1 建立配置任务

在配置 SNMP 查询测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.9.2 配置 SNMP 测试参数

在配置 SNMP 测试时，需要配置的相关参数。

### 6.9.3 检查配置结果

在 SNMP 查询测试成功后，可以查看到 SNMP 查询测试的结果数据。

### 6.9.1 建立配置任务

在配置 SNMP 查询测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

#### 应用环境

通过 SNMP 查询测试，可以了解主机与 SNMP Agent 之间通信的统计信息。

#### 前置任务

在配置 SNMP 测试之前，需完成以下任务：

- 配置 SNMP Agent
- 配置 NQA 客户端与 SNMP Agent 之间路由可达

#### 数据准备

在配置 SNMP 查询测试之前，需要准备以下数据：

| 序号 | 数据                                  |
|----|-------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                |
| 2  | SNMP Agent 的 IP 地址                  |
| 3  | （可选）源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比 |
| 4  | 启动方式和结束方式                           |

### 6.9.2 配置 SNMP 测试参数

在配置 SNMP 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type snmp**，配置测试例类型为 SNMP。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址，即 SNMP Agent 的地址。

 说明

目的地址所指定的机器上必须启动网管功能，否则将收不到回应包。

**步骤 5**（可选）根据需要，配置 SNMP 测试其他参数。

- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **source-port port-number**，配置源端口。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.9.3 检查配置结果

在 SNMP 查询测试成功后，可以查看到 SNMP 查询测试的结果数据。

## 前提条件

已经完成 SNMP 查询测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 执行 **display nqa results** [ *test-instance admin-name test-name* ] 命令查看测试结果。

----结束

## 任务示例

对于 SNMP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.2.1.2
 Min/Max/Average Completion Time: 63/172/109
 Sum/Square-Sum Completion Time: 329/42389
 Last Good Probe Time: 2006-8-5 15:33:49.1
 Lost packet ratio: 0 %
```

## 6.10 配置 TCP 测试

介绍使用 NQA 测试 TCP 端口的响应速度。

### 6.10.1 建立配置任务

在配置 TCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.10.2 配置 TCP 服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

### 6.10.3 配置 TCP 客户端

在 TCP 客户端配置测试例时，需要配置的相关参数。

### 6.10.4 检查配置结果

在 TCP 测试成功后，可以查看到 TCP 测试的结果数据。

## 6.10.1 建立配置任务

在配置 TCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

NQA 支持对 TCP 连接指定端口的响应速度测试。

## 前置任务

在配置 TCP 测试之前，需配置 NQA 客户端与 TCP 服务器之间路由可达。

## 数据准备

在配置 TCP 测试之前，需要准备以下数据：

| 序号 | 数据                                         |
|----|--------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                       |
| 2  | TCP 服务器端监听的 IP 地址和端口号                      |
| 3  | (可选) 目的端口号、源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比 |
| 4  | 启动方式和结束方式                                  |

### 6.10.2 配置 TCP 服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

#### 背景信息

请在 NQA 服务器端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-server tcpconnect** [ **vpn-instance** *vpn-instance-name* ] *ip-address port-number*，配置 TCP 监听服务。

 说明

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

### 6.10.3 配置 TCP 客户端

在 TCP 客户端配置测试例时，需要配置的相关参数。

#### 背景信息

请在 NQA 客户端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type** **tcp**，配置测试例类型为 TCP。

**步骤 4** 执行命令 **destination-address** **ipv4** *ip-address*，配置目的地址。

**步骤 5** 执行命令 **destination-port** *port-number*，配置目的端口。

**步骤 6**（可选）根据需要，配置 TCP 测试其他参数。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，延迟指定时间后启动测试例。

测试类型 TCP Public 和 TCP Private 的不同之处在于：

- TCP Public 测试固定向目的地址的 7 号 TCP 端口发起连接建立请求，客户端不需要配置目的端口，但要在服务器端监听 7 号 TCP 端口。
- TCP Private 测试需要指定目的端口，并且服务器端要对应监听。

----结束

## 6.10.4 检查配置结果

在 TCP 测试成功后，可以查看到 TCP 测试的结果数据。

### 前提条件

已经完成 TCP 测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 在 NQA 客户端执行 **display nqa results** [ **test-instance** *admin-name test-name* ] 命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

## 任务示例

对于 TCP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry(admin, tcp) :testflag is inactive ,testtype is tcp
1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:0 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.2.1.2
 Min/Max/Average Completion Time: 31/62/51
 Sum/Square-Sum Completion Time: 155/8649
 Last Good Probe Time: 2006-8-5 15:55:15.3
 Lost packet ratio: 0 %
```

执行 **display nqa-server** 命令，查看 NQA 测试的服务器端状态。

```
<HUAWEI> display nqa-server
NQA Server Max: 5000 NQA Server Num: 1
NQA Concurrent TCP Server : 1 NQA Concurrent UDP Server: 0
NQA Concurrent ICMP Server : 0

nqa-server tcpconnect 10.112.58.3 2000 ACTIVE
```

## 6.11 配置 UDP 测试

介绍使用 NQA 测试 UDP 端口的响应速度。

### 6.11.1 建立配置任务

在配置 UDP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.11.2 配置 UDP 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

### 6.11.3 配置 UDP 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

### 6.11.4 检查配置结果

在 UDP 测试成功后，可以查看到 UDP 测试的结果数据。

## 6.11.1 建立配置任务

在配置 UDP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

NQA 支持对 UDP 连接指定端口的响应速度测试。

## 前置任务

在配置 UDP 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

## 数据准备

在配置 UDP 测试之前，需要准备以下数据：

| 序号 | 数据                                   |
|----|--------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                 |
| 2  | UDP 服务器端监听的 IP 地址和端口号                |
| 3  | UDP 客户端发送探测报文的目的地址和目的端口号             |
| 4  | （可选）：源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比 |
| 5  | 启动方式和结束方式                            |

### 6.11.2 配置 UDP 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

#### 背景信息

请在 NQA 服务器端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-server udpecho** [ **vpn-instance vpn-instance-name** ] *ip-address port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

**步骤 3** （可选）执行命令 **cpu-defend policy policy-number**，进入防攻击策略视图。

**步骤 4** （可选）执行命令 **undo udp-packet-defend enable**，去使能 UDP 报文攻击防范功能。

为了防止 pepsi 和 fraggle 等攻击方案利用设备的诊断端口 7，13，19 发起 udp 攻击，缺省情况下，NE20E-X6 的 UDP 报文攻击防范功是使能的，即接口板会丢弃目的端口号是 7、13、19 的报文。

所以，为了保证 udp 测试顺利进行，在配置目的端口号时请注意：

- 如果 NQA server 端使能了 udp 报文的攻击防范功能，则客户端不能配置目的端口号为 7，13 和 19。
- 如果非要用这几个目的端口，则在发起 udp 测试之前，务必确认 NQA server 端的 udp 报文攻击防范功能为关闭状态。

----结束

### 6.11.3 配置 UDP 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。



## 背景信息

请在 NQA 客户器端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type udp**，配置测试例类型为 UDP。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5** 执行命令 **destination-port port-number**，配置目的端口。

为了防止 pepsi 和 fraggle 等攻击方案利用设备的诊断端口 7、13、19 发起 udp 攻击，缺省情况下，NE20E-X6 的 UDP 报文攻击防范功能是使能的，即接口板会丢弃目的端口号是 7、13、19 的报文。

所以，为了保证 udp 测试顺利进行，在配置目的端口号时请注意：

- 如果 NQA server 端使能了 udp 报文的攻击防范功能，则客户端不能配置目的端口号为 7、13 和 19。
- 如果非要用这几个目的端口，则在发起 udp 测试之前，务必确认 NQA server 端的 udp 报文攻击防范功能为关闭状态。

**步骤 6** （可选）根据需要，配置 UDP 测试其他参数。

- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **source-port port-number**，配置源端口。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.11.4 检查配置结果

在 UDP 测试成功后，可以查看到 UDP 测试的结果数据。



## 前提条件

已经完成 UDP 测试功能的所有配置。

### 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

- 在 NQA 客户端执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

## 任务示例

对于 UDP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry(admin, udp) :testflag is inactive ,testtype is udp
1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.2.1.2
 Min/Max/Average Completion Time: 32/109/67
 Sum/Square-Sum Completion Time: 203/16749
 Last Good Probe Time: 2006-8-5 16:9:21.6
 Lost packet ratio: 0 %
```

执行 **display nqa-server** 命令，查看 NQA 测试的服务器端状态。

```
<HUAWEI> display nqa-server
NQA Server Max: 5000 NQA Server Num: 1
NQA Concurrent TCP Server : 0 NQA Concurrent UDP Server: 1
NQA Concurrent ICMP Server : 0

nqa-server udpecho 10.112.58.3 3000 ACTIVE Hardware-based
```

## 6.12 配置 Jitter 测试

介绍使用 NQA 测试网络的抖动情况。客户端和服务端都必须是华为设备才能进行 Jitter 测试。

### 6.12.1 建立配置任务

在配置 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.12.2 配置 Jitter 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

### 6.12.3 配置 Jitter 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

### 6.12.4 检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

## 6.12.1 建立配置任务

在配置 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

Jitter 测试的过程如下：

1. 源端以一定的时间间隔向目的端发送数据包。
2. 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。
3. 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

#### 说明

在客户端和服务端配置 NTP，可以有效提高测试的精度。

### 前置任务

在配置 Jitter 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

### 数据准备

在配置 Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                      |
| 2  | UDP 服务器端监听的 IP 地址和端口号                                                                                     |
| 3  | UDP 客户端发送探测报文的目的地址和目的端口号                                                                                  |
| 4  | （可选）：VPN 实例名、UDP 客户端发送探测报文的源地址、UDP 客户端发送探测报文的源端口号、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号 |
| 5  | 启动方式和结束方式                                                                                                 |

## 6.12.2 配置 Jitter 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

### 背景信息

请在 NQA 服务器端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-server udpecho** [ **vpn-instance** *vpn-instance-name* ] *ip-address* *port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

**步骤 3** （可选）执行命令 **cpu-defend policy** *policy-number*，进入防攻击策略视图。

**步骤 4** （可选）执行命令 **undo udp-packet-defend enable**，去使能 UDP 报文攻击防范功能。

为了防止 pepsy 和 fraggle 等攻击方案利用设备的诊断端口 7，13，19 发起 udp 攻击，缺省情况下，NE20E-X6 的 UDP 报文攻击防范功是使能的，即接口板会丢弃目的端口号是 7、13、19 的报文。

所以，为了保证 udp jitter 测试顺利进行，在配置目的端口号时请注意：

- 如果 NQA server 端使能了 udp 报文的攻击防范功能，则客户端不能配置目的端口号为 7，13 和 19。
- 如果非要用这几个目的端口，则在发起 udp 测试之前，务必确认 NQA server 端的 udp 报文攻击防范功能为关闭状态。

----结束

## 6.12.3 配置 Jitter 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

### 背景信息

 说明

系统支持统计 Jitter 测试最大单向延时。

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** （可选）执行命令 **nqa-jitter tag-version** *version-number*，配置 Jitter 报文的版本号。

在配置 Jitter 报文的版本号为 2 并配置单向丢包统计后，在测试结果中可以看到，从源端到目的端、从目的端到源端和未知方向的丢包情况。为网络管理员定位网络故障、检测恶意对网络的攻击提供依据。

**步骤 3** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 4** 执行命令 **test-type jitter**，配置测试例类型为 Jitter。

**步骤 5** 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

**步骤 6** 执行命令 **destination-port** *port-number*，配置目的端口。

为了防止 pps 和 fraggle 等攻击方案利用设备的诊断端口 7, 13, 19 发起 udp 攻击，缺省情况下，NE20E-X6 的 UDP 报文攻击防范功能是使能的，即接口板会丢弃目的端口号是 7、13、19 的报文。

所以，为了保证 udp jitter 测试顺利进行，在配置目的端口号时请注意：

- 如果 NQA server 端使能了 udp 报文的攻击防范功能，则客户端不能配置目的端口号为 7, 13 和 19。
- 如果非要用这几个目的端口，则在发起 udp 测试之前，务必确认 NQA server 端的 udp 报文攻击防范功能为关闭状态。

**步骤 7** （可选）根据需要，配置 Jitter 测试其他参数。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **probe-count** *number*，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum** *number*，配置每次测试所发送的测试包个数。

Jitter 测试是对 UDP 报文传输的延时变化进行统计分析。为了提高统计结果的准确性，每一次测试系统都会发送多个测试包。每次测试发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。

#### 说明

Jitter 测试的次数取决于 **probe-count** 命令的配置，而每次测试所发送的测试包的个数由 **jitter-packetnum** 命令确定。实际配置时，**probe-count** 命令设置的测试次数与 **jitter-packetnum** 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval** { *milliseconds interval* | *seconds interval* }，配置发送测试包的时间间隔。

Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。
- 执行命令 **jitter-codec** { *g711a* | *g711u* | *g729a* }，配置 NQA Jitter 测试例的模拟语音测试的编码类型。

此命令只在 Jitter 测试例用于语音测试时配置。

- 执行命令 **adv-factor** *factor-value*，配置模拟语音测试计算的补偿因子。  
此命令只在 Jitter 测试例用于语音测试时配置。

**步骤 8** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 立即启动测试例。
- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

## 6.12.4 检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

### 前提条件

已经完成 Jitter 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 在 NQA 客户端执行 **display nqa results** [ **test-instance** admin-name test-name ] 命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

### 任务示例

对于 Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
1. Test 2 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion:success RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/1/1/60 RTT Square Sum:60
 NumOfRTT:60 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:1 Min Positive DS:1
 Max Positive SD:1 Max Positive DS:1
 Positive SD Number:15 Positive DS Number:1
 Positive SD Sum:15 Positive DS Sum:1
 Positive SD Square Sum:15 Positive DS Square Sum:1
 Min Negative SD:1 Min Negative DS:1
 Max Negative SD:1 Max Negative DS:1
 Negative SD Number:15 Negative DS Number:1
 Negative SD Sum:15 Negative DS Sum:1
 Negative SD Square Sum:15 Negative DS Square Sum:1
 Min Delay SD:0 Min Delay DS:0
 Avg Delay SD:0 Avg Delay DS:0
 Max Delay SD:0 Max Delay DS:0
 Delay SD Square Sum:27 Delay DS Square Sum:1
```

```

Packet Loss SD:0
Packet Loss Unknown:0
Average of Jitter SD:1
jitter out value:0.0312500
NumberOfOWD:60
OWD SD Sum:27
ICPIF value: 0
TimeStamp unit: ms
Packet Rewrite Ratio: 0%
Packet Disorder Ratio: 0%
Fragment-disorder Ratio: 0%
Packet Loss DS:0
Average of Jitter:1
Average of Jitter DS:1
jitter in value:0.0020833
Packet Loss Ratio: 0%
OWD DS Sum:1
MOS-CQ value: 0
Packet Rewrite Number: 0
Packet Disorder Number: 0
Fragment-disorder Number: 0
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
1. Test 1 result The test is finished
SendProbe:60
Completion:success
OWD OverThresholds SD number:0
Min/Max/Avg/Sum RTT:1/1/1/60
NumOfRTT:60
Operation sequence errors number:0
System busy operation number:0
Min Positive SD:1
Max Positive SD:1
Positive SD Number:3
Positive SD Sum:3
Positive SD Square Sum:3
Min Negative SD:1
Max Negative SD:1
Negative SD Number:3
Negative SD Sum:3
Negative SD Square Sum:3
Min Delay SD:0
Avg Delay SD:0
Max Delay SD:0
Delay SD Square Sum:0
Packet Loss SD:0
Packet Loss Unknown:0
Average of Jitter SD:1
jitter out value:0.0062500
NumberOfOWD:60
OWD SD Sum:0
ICPIF value: 0
ResponseProbe:60
RTD OverThresholds number:0
OWD OverThresholds DS number:0
RTT Square Sum:60
Drop operation number:0
RTT Stats errors number:0
Operation timeout number:0
Min Positive DS:1
Max Positive DS:1
Positive DS Number:1
Positive DS Sum:1
Positive DS Square Sum:1
Min Negative DS:1
Max Negative DS:1
Negative DS Number:1
Negative DS Sum:1
Negative DS Square Sum:1
Min Delay DS:0
Avg Delay DS:0
Max Delay DS:0
Delay DS Square Sum:0
Packet Loss DS:0
Average of Jitter:1
Average of Jitter DS:1
jitter in value:0.0020833
Packet Loss Ratio: 0%
OWD DS Sum:0
MOS-CQ value: 0

```

## 6.13 配置基于接口板发包的 Jitter 测试

使用基于接口板发送的 Jitter 测试可以得到更加精确的网络抖动情况的数据。

### 6.13.1 建立配置任务

在配置基于接口板发包的 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.13.2 配置 Jitter 测试服务器端

对于基于接口板发送的 Jitter 测试，服务器端必须配置。

### 6.13.3 配置 Jitter 测试客户端

在客户端配置基于接口板发包的 Jitter 测试时，需要配置的相关参数。

### 6.13.4 检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

## 6.13.1 建立配置任务

在配置基于接口板发包的 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

使能接口板发包功能后，可以进一步提供测试结果数据的准确性。

## 前置任务

在配置 Jitter 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

## 数据准备

在配置 Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                      |
| 2  | UDP 服务器端监听的 IP 地址和端口号                                                                                     |
| 3  | UDP 客户端发送探测报文的目的地址和目的端口号                                                                                  |
| 4  | （可选）：VPN 实例名、UDP 客户端发送探测报文的源地址、UDP 客户端发送探测报文的源端口号、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号 |
| 5  | 启动方式和结束方式                                                                                                 |

### 6.13.2 配置 Jitter 测试服务器端

对于基于接口板发送的 Jitter 测试，服务器端必须配置。

## 背景信息

请在 NQA 服务器端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-server udpecho [ vpn-instance vpn-instance-name ] ip-address port-number**，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束



### 6.13.3 配置 Jitter 测试客户端

在客户端配置基于接口板发包的 Jitter 测试时，需要配置的相关参数。

#### 背景信息



说明

系统支持统计 Jitter 测试最大单向延时。

请在 NQA 客户端进行下列配置。

#### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type jitter**，配置测试例类型为 Jitter。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5** 执行命令 **destination-port port-number**，配置目的端口。
- 步骤 6** 执行命令 **hardware-based enable**，使能接口板发包功能。
- 步骤 7**（可选）根据需要，配置 Jitter 测试其他参数。
  - 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
  - 执行命令 **source-address ipv4 ip-address**，配置源地址。
  - 执行命令 **source-port port-number**，配置源端口。
  - 执行命令 **probe-count number**，配置每次发送的测试探针个数。
  - 执行命令 **jitter-packetnum number**，配置每次测试所发送的测试包个数。

Jitter 测试是对 UDP 报文传输的延时变化进行统计分析。为了提高统计结果的准确性，每一次测试系统都会发送多个测试包。每次测试发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。



Jitter 测试的次数取决于 probe-count 命令的配置，而每次测试所发送的测试包的个数由 jitter-packetnum 命令确定。实际配置时，probe-count 命令设置的测试次数与 jitter-packetnum 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval { milliseconds interval | seconds interval }**，配置发送测试包的时间间隔。

Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。
- 在系统视图下，执行命令 **nqa-jitter tag-version version-number**，配置 Jitter 报文的版本号。



配置单向丢包统计后，在测试结果中可以看到，从源端到目的端、从目的端到源端和未知方向的丢包情况。为网络管理员定位网络故障、检测恶意对网络的攻击提供依据。

- 执行命令 **timeout time** 配置测试例的操作超时时间。

#### 步骤 8 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.13.4 检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

### 前提条件

已经完成基于接口板发包的 Jitter 测试的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果，并且只能显示最近 5 次的测试结果。

### 操作步骤

- 步骤 1** 使用命令 **display nqa results [ test-instance admin-name test-name ]**，在 NQA 客户端查看测试结果。

----结束

### 任务示例

对于 Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
1 . Test 2 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion:succcess RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/1/1/60 RTT Square Sum:60
 NumOfRTT:60 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:1 Min Positive DS:1
 Max Positive SD:1 Max Positive DS:1
 Positive SD Number:15 Positive DS Number:1
 Positive SD Sum:15 Positive DS Sum:1
```

|                             |                             |
|-----------------------------|-----------------------------|
| Positive SD Square Sum:15   | Positive DS Square Sum:1    |
| Min Negative SD:1           | Min Negative DS:1           |
| Max Negative SD:1           | Max Negative DS:1           |
| Negative SD Number:15       | Negative DS Number:1        |
| Negative SD Sum:15          | Negative DS Sum:1           |
| Negative SD Square Sum:15   | Negative DS Square Sum:1    |
| Min Delay SD:0              | Min Delay DS:0              |
| Avg Delay SD:0              | Avg Delay DS:0              |
| Max Delay SD:0              | Max Delay DS:0              |
| Delay SD Square Sum:27      | Delay DS Square Sum:1       |
| Packet Loss SD:0            | Packet Loss DS:0            |
| Packet Loss Unknown:0       | Average of Jitter:1         |
| Average of Jitter SD:1      | Average of Jitter DS:1      |
| jitter out value:0.0312500  | jitter in value:0.0020833   |
| NumberOfOWD:60              | Packet Loss Ratio: 0%       |
| OWD SD Sum:27               | OWD DS Sum:1                |
| ICPIF value: 0              | MOS-CQ value: 0             |
| TimeStamp unit: ms          | Packet Rewrite Number: 0    |
| Packet Rewrite Ratio: 0%    | Packet Disorder Number: 0   |
| Packet Disorder Ratio: 0%   | Fragment-disorder Number: 0 |
| Fragment-disorder Ratio: 0% |                             |

## 6.14 配置 LSP Ping 测试

介绍使用 NQA 检测 LSP 隧道的运行情况。

### 6.14.1 建立配置任务

在配置 LSP Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.14.2 配置对 LSP 隧道的 LSP Ping 测试参数

在对 LSP 隧道执行 LSP Ping 测试前，应配置 LSP 隧道的 LSP Ping 测试参数

### 6.14.3 配置对 TE 隧道的 LSP Ping 测试参数

在对 TE 隧道执行 LSP Ping 测试前，应配置 TE 隧道的 LSP Ping 测试参数

### 6.14.4 配置对 CR-LSP 热备份隧道的 LSP Ping 测试参数

在对 CR-LSP 热备份隧道执行 LSP Ping 测试前，应配置 CR-LSP 热备份隧道的 LSP Ping 测试参数

### 6.14.5 检查配置结果

在 LSP Ping 测试成功后，可以查看到 LSP Ping 测试的结果数据。

## 6.14.1 建立配置任务

在配置 LSP Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

NQA 提供 LSP Ping 测试类型，可以对两种类型的 LSP 进行可达性检测，并收集 SLA 相关统计信息。

- 对 LSP 隧道的 LSP Ping 测试
- 对 MPLS TE Tunnel 的 LSP Ping 测试
- 对 MPLS CR-LSP 热备份隧道的 LSP Ping 测试

正确配置了测试例参数并启动测试后：

- NQA 构造 UDP 的 MPLS Echo Request 报文，在 IP 头填入 127/8 的地址作为 IP 的目的地址，按指定 LSP 进行 MPLS 域内转发。
- 接收端 Egress 监听 3503 端口发送的响应报文。
- 发送端通过接收到的响应报文，统计出测试结果。

## 前置任务

在配置 LSP Ping 测试之前，需完成以下任务：

- 建立 LSP 隧道
- 或 MPLS TE Tunnel
- 或 CR-LSP 热备份隧道

## 数据准备

在配置 LSP Ping 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                                    |
|----|-----------------------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                                  |
| 2  | <ul style="list-style-type: none"><li>● LSP 隧道：LSP Ping 测试的目的地址和掩码</li><li>● MPLS TE Tunnel：TE Tunnel 的接口编号</li></ul> |
| 3  | （可选）：Echo 报文响应模式、报文大小、TTL、LSP EXP、填充字符、测试间隔、测试失败的百分比                                                                  |
| 4  | 启动方式和结束方式                                                                                                             |

### 6.14.2 配置对 LSP 隧道的 LSP Ping 测试参数

在对 LSP 隧道执行 LSP Ping 测试前，应配置 LSP 隧道的 LSP Ping 测试参数

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type lsping**，配置测试例类型为 LSP Ping。
- 步骤 4** 执行命令 **lsp-type ipv4**，配置测试类型为 LSP 隧道的 LSP Ping 测试。
- 步骤 5** 执行命令 **destination-address ipv4 ip-address { lsp-masklen masklen | lsp-loopback loopback-address }**，配置 LSP Ping 测试的目的地址。

**步骤 6** (可选) 根据需要, 配置 LSP Ping 测试其他参数。

- 执行命令 **lsp-replymode** { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }, 配置 Echo 报文的响应模式

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功, 测试结果的显示信息都会显示测试失败。只是在测试成功时, 测试结果的显示信息中会显示超时测试报文的数量; 在测试失败时, 测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**, 配置源地址。
- 执行命令 **datasize size**, 配置测试报文的大小。

 说明

配置 **datasize** 大小加上报文头后的值不能超过接口的 MTU 值, 否则会导致测试失败。

- 执行命令 **ttl number**, 配置报文的最大 TTL 值。
- 执行命令 **lsp-exp exp**, 配置 LSP EXP 值。
- 执行命令 **datafill fillstring**, 配置报文的填充字段。
- 执行命令 **interval seconds interval**, 配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**, 配置 NQA 测试的失败百分比。

**步骤 7** 执行命令 **start**, 启动 NQA 测试。

命令 **start** 有多种形式, 根据实际需要选择其中一种启动方式:

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds second** | *hh:mm:ss* } | **lifetime** { **seconds second** | *hh:mm:ss* } } ], 立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds second** | *hh:mm:ss* } | **lifetime** { **seconds second** | *hh:mm:ss* } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds second** | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds second** | *hh:mm:ss* } | **lifetime** { **seconds second** | *hh:mm:ss* } } ], 延迟指定时间后启动测试例。

----结束

### 6.14.3 配置对 TE 隧道的 LSP Ping 测试参数

在对 TE 隧道执行 LSP Ping 测试前, 应配置 TE 隧道的 LSP Ping 测试参数

#### 背景信息

请在 NQA 客户端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**, 进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**, 建立 NQA 测试例, 并进入测试例视图。

**步骤 3** 执行命令 **test-type lsping**, 配置测试例类型为 LSP Ping。

**步骤 4** 执行命令 **lsp-type te**, 配置测试类型为 TE 隧道的 LSP Ping 测试。

**步骤 5** 执行命令 **lsp-tunnel tunnel tunnel-number**，配置 LSP Ping 测试的 TE Tunnel 接口。

**步骤 6**（可选）根据需要，配置 LSP Ping 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式

 说明

**lsp-replymode no-replay** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **datasize size**，配置测试报文的大小。

 说明

配置 **datasize** 大小加上报文头后的值不能超过接口的 MTU 值，否则会导致测试失败。

- 执行命令 **ttl number**，配置报文的最大 TTL 值。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **datafill fillstring**，配置报文的填充字段。
- 执行命令 **interval { milliseconds interval | seconds interval }**，配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

----结束

## 6.14.4 配置对 CR-LSP 热备份隧道的 LSP Ping 测试参数

在对 CR-LSP 热备份隧道执行 LSP Ping 测试前，应配置 CR-LSP 热备份隧道的 LSP Ping 测试参数

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type lsping**，配置测试例类型为 LSP Ping。

**步骤 4** 执行命令 **lsp-type te**，配置测试类型为 TE 隧道的 LSP Ping 测试。

**步骤 5** 执行命令 **lsp-tetunnel tunnel tunnel-number hot-standby**，配置 LSP Ping 测试的 TE Tunnel 接口，并指明探测备份隧道。

**步骤 6** (可选) 根据需要，配置 LSP Ping 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **datasize size**，配置测试报文的大小。

 说明

配置 **datasize** 大小加上报文头后的值不能超过接口的 MTU 值，否则会导致测试失败。

- 执行命令 **ttl number**，配置报文的最大 TTL 值。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **datafill fillstring**，配置报文的填充字段。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.14.5 检查配置结果

在 LSP Ping 测试成功后，可以查看到 LSP Ping 测试的结果数据。

### 前提条件

已经完成 LSP Ping 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 在 NQA 客户端执行 **display nqa results** [ **test-instance** *admin-name test-name* ]命令查看测试结果。

----结束

## 任务示例

对于 LSP Ping 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 接收每个报文的状态
  - 每个报文收到后的时间
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和（低 32 位和高 32 位）
  - 目的地址类型、目的地址
  - 报文最小往返时间、最大往返时间
  - 已收到回应的报文数目、已发送的报文数
  - 至今收到最后一个报文的时间

执行命令 **display nqa results**，看到显示结果如下：

```
<HUAWEI> display nqa results test-instance admin lsping
NQA entry(admin, test) :testflag is inactive ,testtype is lsping
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:100.1.1.200
 Min/Max/Average Completion Time: 4/5/4
 Sum/Square-Sum Completion Time: 13/57
 Last Good Probe Time: 2007-11-19 19:46:28.8
 Lost packet ratio: 0 %
```

## 6.15 配置 LSP Jitter 测试

介绍使用 NQA 测试 LSP 隧道中报文传输时的抖动情况。

### 6.15.1 建立配置任务

在配置 LSP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。



### 6.15.2 配置对 LDP 隧道的 LSP 抖动测试

在配置 LSP Jitter 测试时，对于 LDP 的 LSP 隧道抖动检测时，需要配置的相关参数。

### 6.15.3 配置对 MPLS TE 隧道的抖动测试

在配置 LSP Jitter 测试时，对于 TE 的 LSP 隧道抖动检测时，需要配置的相关参数。

### 6.15.4 检查配置结果

在 LSP Jitter 测试成功后，可以查看到 LSP Jitter 测试的结果数据。

## 6.15.1 建立配置任务

在配置 LSP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

NQA 提供 LSP Jitter 对静态 LSP、LDP LSP 和 TE Tunnel 进行可达性检测，并根据从隧道源端接收到的信息计算出数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间，从而清晰的反映出 MPLS 网络状况。



说明

LSP Jitter 测试不支持负载分担。

### 前置任务

在配置 LSP Jitter 测试之前，需正确建立 LSP 隧道或 MPLS TE Tunnel。

### 数据准备

在配置 LSP Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                                  |
|----|---------------------------------------------------------------------------------------------------------------------|
| 1  | 测试例的管理者标识、测试例名称标识                                                                                                   |
| 2  | <ul style="list-style-type: none"><li>● LSP 隧道：LSP Jitter 测试的目的地址和掩码</li><li>● MPLS TE 隧道：TE Tunnel 的接口编号</li></ul> |
| 3  | （可选）：Echo 报文响应模式、报文大小、TTL、LSP EXP、填充字符、报文超时时间、探针数目、测试间隔                                                             |
| 4  | 启动方式和结束方式                                                                                                           |

## 6.15.2 配置对 LDP 隧道的 LSP 抖动测试

在配置 LSP Jitter 测试时，对于 LDP 的 LSP 隧道抖动检测时，需要配置的相关参数。

### 背景信息

在 LSP 的 Ingress 端进行下列配置。



## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例。

**步骤 3** 执行命令 **test-type lspjitter**，配置测试例类型为 LSP Jitter。

**步骤 4** 执行命令 **lsp-type ipv4**，配置测试类型为普通 LSP 的抖动测试。

**步骤 5** 执行命令 **destination-address ipv4 ip-address { lsp-masklen masklen | lsp-loopback loopback-address }\***，配置 LSP Ping 测试的目的地址。

**步骤 6** (可选) 根据需要，配置 LSP Ping 测试其他参数：

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **datasize size**，配置测试报文的大小。
- 执行命令 **ttl number**，配置报文的最大 TTL 值。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **datafill fillstring**，配置报文的填充字段。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。

 说明

测试报文的发送间隔最小为 1 秒，最到为 60 秒。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 7** 启动测试例。根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

### 6.15.3 配置对 MPLS TE 隧道的抖动测试

在配置 LSP Jitter 测试时，对于 TE 的 LSP 隧道抖动检测时，需要配置的相关参数。

## 背景信息

在 TE 隧道的 Ingress 端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例。

**步骤 3** 执行命令 **test-type lspjitter**，配置测试例类型为 LSP Jitter。

**步骤 4** 执行命令 **lsp-type te**，配置测试类型为 MPLS TE 的抖动测试。

**步骤 5** 执行命令 **lsp-tetunnel tunnel tunnel-number**，配置 LSP Ping 测试的 MPLS TE 隧道接口。

**步骤 6** (可选) 根据需要，配置 LSP Ping 测试其他参数：

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式



**lsp-replymode no-replay** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **datasize size**，配置测试报文的大小。
- 执行命令 **ttl number**，配置报文的最大 TTL 值。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **datafill fillstring**，配置报文的填充字段。
- 执行命令 **interval { milliseconds interval | seconds interval }**，配置测试报文的发送间隔。



测试报文的发送间隔最小为 1 秒，最大为 60 秒。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 7** 启动测试例。根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

----结束

## 6.15.4 检查配置结果

在 LSP Jitter 测试成功后，可以查看到 LSP Jitter 测试的结果数据。

## 前提条件

已经完成 LSP Jitter 测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 在 NQA 客户端执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

## 任务示例

对于 LSP Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和（低 32 位和高 32 位）
  - 报文最小往返时间、最大往返时间
  - 目的地址类型、目的地址
  - 已收到回应的报文数目、已发送的报文数
  - 至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (admin, lspjitter) :testflag is inactive ,testtype is lspjitter
1. Test 1 result The test is finished
SendProbe:60 ResponseProbe:60
Completion:succcess RTD OverThresholds number:0
Min/Max/Avg/Sum RTT:1/24/3/156 RTT Square Sum:928
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:1 Max Positive SD:22
Positive SD Number:12 Positive SD Sum:33
Positive SD Square Sum:495 Min Negative SD:1
Max Negative SD:22 Negative SD Number:12
Negative SD Sum:34 Negative SD Square Sum:498
Packet Loss Unknown:0 Average of Jitter SD:2
jitter out value:0.8977973 Packet Loss Ratio: 0%
```

## 6.16 配置 LSP Traceroute 测试

介绍使用 LSP Traceroute 测试测试隧道各个 LSR 的连通性。

### 6.16.1 建立配置任务

在配置 LSP Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

#### 6.16.2 配置对 LSP 隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 LDP 的 LSP 隧道各个 LSR 检测时，需要配置的相关参数。

#### 6.16.3 配置对 TE 隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 TE 的 LSP 隧道各个 LSR 检测时，需要配置的相关参数。

#### 6.16.4 配置对 CR-LSP 热备份隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 CR-LSP 热备份隧道各个 LSR 检测时，需要配置的相关参数。

#### 6.16.5 检查配置结果

在 LSP Traceroute 测试成功后，可以查看到 LSP Traceroute 测试的结果数据。

## 6.16.1 建立配置任务

在配置 LSP Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

NQA 提供 LSP Traceroute 测试类型，可以检测两种类型的 LSP 隧道节点失效，并收集 SLA 相关统计信息。

- 对 LSP 隧道的 LSP Traceroute 测试
- 对 MPLS TE Tunnel 的 LSP Traceroute 测试
- 对 MPLS CR-LSP 热备份隧道的 LSP Traceroute 测试

正确配置了测试例参数并启动测试后：

- NQA 构造 UDP 的 MPLS Echo Request 报文，在 IP 头填入 127/8 的地址作为 IP 的目的地址，查找相应的 LSP。  
Echo Request 报文应该包含有 Downstream Mapping TLV（用来携带 LSP 在当前节点的下游信息，主要包括下一跳地址、出标签等）。  
对于 TE Tunnel，可以指定从 Tunnel 接口发送，从而找到相应的 CR-LSP。
- 第一次发送的 Traceroute Echo Request 报文 TTL 为 1，按指定的 LSP 进行 MPLS 域内转发，TTL 超时返回 MPLS Echo Reply 消息。
- 发送端继续以 TTL 递增方式发送 Echo Request 报文，直到整条 LSP 上的所有 LSR 都应答后，TraceRoute 过程完成。
- 发送端通过接收到的响应报文，统计出测试结果。

### 前置任务

在配置 LSP Traceroute 测试之前，需完成以下任务：

- 建立 LSP 隧道
- 或 MPLS TE Tunnel

- 或 CR-LSP 热备份隧道

## 数据准备

在配置 LSP Traceroute 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                                          |
|----|-----------------------------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                                        |
| 2  | <ul style="list-style-type: none"><li>● LSP 隧道：LSP Traceroute 测试的目的地址和掩码</li><li>● MPLS TE Tunnel：TE Tunnel 的接口编号</li></ul> |
| 3  | （可选）：Echo 报文响应模式、LSP EXP、允许的最大跳失败数、TTL                                                                                      |
| 4  | 启动方式和结束方式                                                                                                                   |

### 6.16.2 配置对 LSP 隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 LDP 的 LSP 隧道各个 LSR 检测时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type lsptrace**，配置测试例类型为 LSP Traceroute。

**步骤 4** 执行命令 **lsp-type ipv4**，配置测试类型为普通隧道的 LSP Traceroute 测试。

**步骤 5** 执行命令 **destination-address ipv4 ip-address { lsp-masklen masklen | lsp-loopback loopback-address }**，配置 LSP Traceroute 测试的目的地址。

**步骤 6** （可选）根据需要，配置 LSP Traceroute 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **tracert-hopfailtimes times**，配置 LSP Traceroute 测试的跳失败数。

- 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

### 6.16.3 配置对 TE 隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 TE 的 LSP 隧道各个 LSR 检测时，需要配置的相关参数。

#### 背景信息

请在 NQA 客户端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type lsptrace**，配置测试例类型为 LSP Traceroute。

**步骤 4** 执行命令 **lsp-type te**，配置测试类型为 TE 隧道的 LSP Traceroute 测试。

**步骤 5** 执行命令 **lsp-tetunnel tunnel tunnel-number**，配置 LSP Traceroute 测试的 TE Tunnel 接口。

**步骤 6**（可选）根据需要，配置 LSP Traceroute 测试其他参数。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **tracert-hopfailtimes times**，配置 LSP Traceroute 测试的跳失败数。
- 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。



**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，延迟指定时间后启动测试例。

----结束

## 6.16.4 配置对 CR-LSP 热备份隧道的 LSP Traceroute 测试参数

在配置 LSP Traceroute 测试时，对于 CR-LSP 热备份隧道各个 LSR 检测时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type lsptrace**，配置测试例类型为 LSP Traceroute。

**步骤 4** 执行命令 **lsp-type te**，配置测试类型为 TE 隧道的 LSP Traceroute 测试。

**步骤 5** 执行命令 **lsp-tetunnel tunnel tunnel-number hot-standby**，配置 LSP Traceroute 测试的 TE Tunnel 接口，并指明探测备份隧道。

**步骤 6** （可选）根据需要，配置 LSP Traceroute 测试其他参数。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **lsp-replymode** { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }，配置 Echo 报文的响应模式

 说明

**lsp-replymode no-reply** 进行单向测试。无论测试是否成功，测试结果的显示信息都会显示测试失败。只是在测试成功时，测试结果的显示信息中会显示超时测试报文的数量；在测试失败时，测试结果的显示信息中会显示测试报文丢弃的数量。

- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **tracert-hopfailtimes times**，配置 LSP Traceroute 测试的跳失败数。
- 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 延迟指定时间后启动测试例。

----结束

## 6.16.5 检查配置结果

在 LSP Traceroute 测试成功后，可以查看到 LSP Traceroute 测试的结果数据。

### 前提条件

已经完成 LSP Traceroute 测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 步骤 1** 在 NQA 客户端执行 **display nqa results** [ **test-instance** *admin-name test-name* ] 命令查看测试结果。

----结束

### 任务示例

对于 LSP Traceroute 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 序列号出错次数
  - 无路由连接次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和
  - 报文最小往返时间、最大往返时间
  - 目的地址



- 已收到回应的报文数目、已发送的报文数
- 至今收到最后一个报文的时间

```
<HUAWEI> display nqa results test-instance admin lsptrace
NQA entry(admin, lsptrace) :testflag is inactive ,testtype is lsptrace
 1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-4-24 11:22:21.2
 1 . Hop 1 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 50/60/56
 Sum/Square-Sum Completion Time: 170/9700
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-24 11:22:20.8
 Destination ip address:30.1.1.2
 Lost packet ratio: 0 %
 2 . Hop 2 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 80/110/93
 Sum/Square-Sum Completion Time: 280/26600
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-24 11:22:21.2
 Destination ip address:3.3.3.3
 Lost packet ratio: 0 %
```

## 6.17 配置 ICMP Jitter 测试

介绍使用 ICMP Jitter 测试测试 IP 网络的抖动情况。

### 6.17.1 建立配置任务

在配置 ICMP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.17.2 配置 ICMP Jitter 测试参数

在配置 ICMP Jitter 测试时，需要配置的相关参数。

### 6.17.3 检查配置结果

在 ICMP Jitter 测试成功后，可以查看到 ICMP Jitter 测试的结果数据。

## 6.17.1 建立配置任务

在配置 ICMP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

Jitter 测试的过程如下：

- 源端以一定的时间间隔向目的端发送数据包。
- 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。
- 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

在服务器端是非华为设备时，可以通过配置 ICMP Jitter 测试例，测试网络的抖动情况。

## 前置任务

在配置 ICMP Jitter 测试之前，需配置 NQA 客户端与服务器之间路由可达。

## 数据准备

在配置 Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                    |
|----|---------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                  |
| 2  | 目的 IP 地址                                                                              |
| 3  | （可选）：VPN 实例名、客户端发送探测报文的源地址、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、超时时间、NQA 测试的失败百分比、TTL 值、Tos 值 |
| 4  | 启动方式和结束方式                                                                             |

### 6.17.2 配置 ICMP Jitter 测试参数

在配置 ICMP Jitter 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type icmpjitter**，配置测试例类型为 Jitter。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5** （可选）根据需要，配置 Jitter 测试其他参数。
  - 执行命令 **icmp-jitter-mode { icmp-echo | icmp-timestamp }**
  - 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
  - 执行命令 **source-address ipv4 ip-address**，配置源地址。
  - 执行命令 **probe-count number**，配置每次发送的测试探针个数。
  - 执行命令 **jitter-packetnum number**，配置每次测试所发送的测试包个数。



Jitter 测试的次数取决于 `probe-count` 命令的配置，而每次测试所发送的测试包的个数由 `jitter-packetnum` 命令确定。实际配置时，`probe-count` 命令设置的测试次数与 `jitter-packetnum` 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval milliseconds interval**，配置发送测试包的时间间隔。

Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

#### 步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

----结束

### 6.17.3 检查配置结果

在 ICMP Jitter 测试成功后，可以查看到 ICMP Jitter 测试的结果数据。

#### 前提条件

已经完成 ICMP Jitter 测试的所有配置。



NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。

#### 操作步骤

- 使用命令 **display nqa results [ test-instance admin-name test-name ]**，在 NQA 客户端查看测试结果。

----结束

#### 任务示例

对于 ICMP Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin icmpjitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1 . Test 1 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion :success RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/144/12/709 RTT Square Sum:61007
 NumOfRTT:60 Drop operation number:0
```

|                                    |                             |
|------------------------------------|-----------------------------|
| Operation sequence errors number:0 | RTT Stats errors number:0   |
| System busy operation number:0     | Operation timeout number:0  |
| Min Positive SD:1                  | Min Positive DS:1           |
| Max Positive SD:138                | Max Positive DS:3           |
| Positive SD Number:7               | Positive DS Number:19       |
| Positive SD Sum:152                | Positive DS Sum:21          |
| Positive SD Square Sum :19116      | Positive DS Square Sum :27  |
| Min Negative SD:1                  | Min Negative DS:1           |
| Max Negative SD:21                 | Max Negative DS:4           |
| Negative SD Number:14              | Negative DS Number:19       |
| Negative SD Sum:152                | Negative DS Sum:22          |
| Negative SD Square Sum :2796       | Negative DS Square Sum :34  |
| Min Delay SD:1                     | Min Delay DS:0              |
| Max Delay SD:72                    | Max Delay DS:71             |
| Delay SD Square Sum:15111          | Delay DS Square Sum:14728   |
| Packet Loss SD:0                   | Packet Loss DS:0            |
| Packet Loss Unknown:0              | Average of Jitter:5         |
| Average of Jitter SD:14            | Average of Jitter DS:1      |
| jitter out value:4.7604818         | jitter in value:0.5399519   |
| NumberOfOWD:60                     | Packet Loss Ratio: 0%       |
| OWD SD Sum:339                     | OWD DS Sum:310              |
| ICPIF value: 0                     | MOS-CQ value: 0             |
| TimeStamp unit: ms                 | Packet Rewrite Number: 0    |
| Packet Rewrite Ratio: 0%           | Packet Disorder Number: 0   |
| Packet Disorder Ratio: 0%          | Fragment-disorder Number: 0 |
| Fragment-disorder Ratio: 0%        |                             |

## 6.18 配置基于接口板发包的 ICMP Jitter 测试

介绍使用基于接口板发送的 ICMP Jitter 测试测试 IP 网络的抖动情况。使用基于接口板发送的 ICMP Jitter 测试可以得到更加准确的了解到网络的抖动情况。

### 6.18.1 建立配置任务

在配置基于接口板发包的 ICMP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.18.2 配置 ICMP Jitter 测试服务器端

对于基于接口板发送的 Jitter 测试，服务器端必须配置。

### 6.18.3 配置 ICMP Jitter 测试客户端

在客户端配置基于接口板发包的 ICMP Jitter 测试时，需要配置的相关参数。

### 6.18.4 检查配置结果

在基于接口板发包的 ICMP Jitter 测试成功后，可以查看到 ICMP Jitter 测试的结果数据。

## 6.18.1 建立配置任务

在配置基于接口板发包的 ICMP Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

Jitter（抖动时间）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

Jitter 测试的过程如下：

- 源端以一定的时间间隔向目的端发送数据包。
- 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。

- 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

在服务器端是非华为设备时，可以通过配置基于接口板发包的 ICMP Jitter 测试例，测试网络的抖动情况，可以得到更加准确的测试结果。

## 前置任务

在配置基于接口板发包的 ICMP Jitter 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

## 数据准备

在配置 Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                          |
|----|---------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                        |
| 2  | ICMP 服务器端的 IP 地址                                                                            |
| 3  | 目的 IP 地址                                                                                    |
| 4  | （可选）：VPN 实例名、ICMP 客户端发送探测报文的源地址、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、TTL 值、测试报文的 ToS 值 |
| 5  | 启动方式和结束方式                                                                                   |

### 6.18.2 配置 ICMP Jitter 测试服务器端

对于基于接口板发送的 Jitter 测试，服务器端必须配置。

## 背景信息

请在 NQA 服务器端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-server icmp-server [ vpn-instance vpn-instance-name ] ip-address**，ICMP Jitter 测试的服务器。

----结束

### 6.18.3 配置 ICMP Jitter 测试客户端

在客户端配置基于接口板发包的 ICMP Jitter 测试时，需要配置的相关参数。

#### 背景信息



说明

请在 NQA 客户端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type icmpjitter**，配置测试例类型为 ICMPJitter。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5** 执行命令 **hardware-based enable**，使能接口板发包功能。

**步骤 6**（可选）根据需要，配置 Jitter 测试其他参数。

- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **probe-count number**，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum number**，配置每次测试所发送的测试包个数。

ICMPJitter 测试是对 ICMP 报文传输的延时变化进行统计分析。为了提高统计结果的准确性，每一次测试系统都会发送多个测试包。每次测试发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。



Jitter 测试的次数取决于 probe-count 命令的配置，而每次测试所发送的测试包的个数由 jitter-packetnum 命令确定。实际配置时，probe-count 命令设置的测试次数与 jitter-packetnum 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval { milliseconds interval | seconds interval }**，配置发送测试包的时间间隔。

Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 执行命令 **timeout time**，配置超时时间。
- 执行命令 **ttl number** 用来配置 NQA 测试例报文中的 TTL 值。
- 执行命令 **tos value** 用来配置测试包的服务类型 ToS。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。



- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

## 6.18.4 检查配置结果

在基于接口板发包的 ICMP Jitter 测试成功后, 可以查看到 ICMP Jitter 测试的结果数据。

### 前提条件

已经完成基于接口板发包的 ICMP Jitter 测试的所有配置。



说明

NQA 测试不会在终端自动显示测试结果, 必须使用 **display nqa results** 命令查看测试结果。

### 操作步骤

- 步骤 1** 使用命令 **display nqa results** [ **test-instance** admin-name test-name ], 在 NQA 客户端查看测试结果。

----结束

### 任务示例

对于 Jitter 类型的测试, 如果测试成功, 执行 **display nqa results** 命令, 可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin icmpjitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1 . Test 1 result The test is finished
SendProbe:60 ResponseProbe:60
Completion :success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:0/1/1/14 RTT Square Sum:14
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:0 Min Positive DS:1
Max Positive SD:0 Max Positive DS:1
Positive SD Number:0 Positive DS Number:1
Positive SD Sum:0 Positive DS Sum:1
Positive SD Square Sum :0 Positive DS Square Sum :1
Min Negative SD:1 Min Negative DS:0
Max Negative SD:1 Max Negative DS:0
Negative SD Number:2 Negative DS Number:0
Negative SD Sum:2 Negative DS Sum:0
Negative SD Square Sum :2 Negative DS Square Sum :0
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:1
Average of Jitter SD:1 Average of Jitter DS:1
jitter out value:0.0295593 jitter in value:0.0117767
NumberOfOWD:60 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
```

ICPIF value: 0  
TimeStamp unit: ms  
Packet Rewrite Ratio: 0%  
Packet Disorder Ratio: 0%  
Fragment-disorder Ratio: 0%

MOS-CQ value: 0  
Packet Rewrite Number: 0  
Packet Disorder Number: 0  
Fragment-disorder Number: 0

## 6.19 配置 Path Jitter 测试

介绍使用 Path Jitter 测试测试报文传输路径上的各个设备的通信情况。

### 6.19.1 建立配置任务

在配置 Path Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.19.2 配置 PathJitter 测试参数

在配置 Path Jitter 测试时，需要配置的相关参数。

### 6.19.3 检查配置结果

在 Path Jitter 测试测试成功后，可以查看到 Path Jitter 测试的结果数据。

## 6.19.1 建立配置任务

在配置 Path Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

网络中是由多台设备组成的，不同设备间的通信，可能需要穿过多个设备才能实现。为了便于更好的监控网络，通过执行 path Jitter 测试可以了解到整个网络中各个部分的通信状况。

### 前置任务

在配置 path Jitter 测试之前，需配置 NQA 客户端与 ICMP 服务器之间路由可达。

### 数据准备

在配置 path Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                      |
| 2  | UDP 客户端发送探测报文的地址                                                                                          |
| 3  | （可选）：VPN 实例名、UDP 客户端发送探测报文的源地址、UDP 客户端发送探测报文的源端口号、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号 |
| 4  | 启动方式和结束方式                                                                                                 |



## 6.19.2 配置 PathJitter 测试参数

在配置 Path Jitter 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type pathjitter**，配置测试例类型为 Path Jitter。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5**（可选）根据需要，配置 Jitter 测试的其他参数。

- 执行命令 **icmp-jitter-mode { icmp-echo | icmp-timestamp }**
- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **probe-count number**，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum number**，配置每次测试所发送的测试包个数。

#### 说明

Jitter 测试的次数取决于 probe-count 命令的配置，而每次测试所发送的测试包的个数由 jitter-packetnum 命令确定。实际配置时，probe-count 命令设置的测试次数与 jitter-packetnum 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval seconds interval**，配置发送测试包的时间间隔。

Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.19.3 检查配置结果

在 Path Jitter 测试成功后，可以查看到 Path Jitter 测试的结果数据。

### 前提条件

完成 path Jitter 测试的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。

### 操作步骤

- 步骤 1** 使用命令 **display nqa results [ test-instance admin-name test-name ]**，在 NQA 客户端查看测试结果。

----结束

### 任务示例

对于 ICMP Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin pathjitter
NQA entry(admin, pathjitter) :testflag is inactive ,testtype is pathjitter
Current Status:CLOSE
1 . Test 1 result The test is finished
Trace Completion Status:success
1 . Hop 1
Destination ip address:13.1.1.2
Jitter Completion Status:success Jitter Finish Status:finished
SendProbe:60 ResponseProbe:60
Min/Max/Avg/Sum RTT:1/4/2/115 RTT Square Sum:235
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:1 Min Positive DS:1
Max Positive SD:3 Max Positive DS:2
Positive SD Number:18 Positive DS Number:13
Positive SD Sum:20 Positive DS Sum:14
Positive SD Square Sum :26 Positive DS Square Sum :16
Min Negative SD:1 Min Negative DS:1
Max Negative SD:3 Max Negative DS:2
Negative SD Number:18 Negative DS Number:13
Negative SD Sum:21 Negative DS Sum:14
Negative SD Square Sum :29 Negative DS Square Sum :16
Max Delay SD:2 Max Delay DS:1
Average of Jitter:1 NumberOfOWD:60
Average of Jitter SD:1 Average of Jitter DS:1
jitter out value:0.4414088 jitter in value:0.3527651
OWD SD Sum:52 OWD DS Sum:3
2 . Hop 2
Destination ip address:110.1.1.1
Jitter Completion Status:failed Jitter Finish Status:finished
SendProbe:60 ResponseProbe:0
Min/Max/Avg/Sum RTT:0/0/0/0 RTT Square Sum:0
NumOfRTT:0 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:60
Min Positive SD:0 Min Positive DS:0
Max Positive SD:0 Max Positive DS:0
Positive SD Number:0 Positive DS Number:0
Positive SD Sum:0 Positive DS Sum:0
Positive SD Square Sum :0 Positive DS Square Sum :0
```

|                            |                           |
|----------------------------|---------------------------|
| Min Negative SD:0          | Min Negative DS:0         |
| Max Negative SD:0          | Max Negative DS:0         |
| Negative SD Number:0       | Negative DS Number:0      |
| Negative SD Sum:0          | Negative DS Sum:0         |
| Negative SD Square Sum :0  | Negative DS Square Sum :0 |
| Max Delay SD:0             | Max Delay DS:0            |
| Average of Jitter:0        | NumberOfOWD:0             |
| Average of Jitter SD:0     | Average of Jitter DS:0    |
| jitter out value:0.0000000 | jitter in value:0.0000000 |
| OWD SD Sum:0               | OWD DS Sum:0              |

## 6.20 配置 Path MTU 测试

介绍使用 Path MTU 测试测试报文传输路径上的路径 MTU 值。

### 6.20.1 建立配置任务

在配置 Path MTU 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.20.2 配置 Path MTU 测试参数

在置 Path MTU 测试时，需要配置的相关参数。

### 6.20.3 检查配置结果

在 Path MTU 测试测试成功后，可以查看到 Path MTU 测试的结果数据。

## 6.20.1 建立配置任务

在配置 Path MTU 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

网络中主机间的通信，可能需要穿越多个网络，不同的网络的 MTU 值可能是不同的，通过 Path MTU 测试可以了解到网络中路径的 MTU 值，在发送端控制报文的长度，可以减少因报文超过 MTU 值被丢弃所导致的发送错误的产生。

### 前置任务

在配置 Path MTU 测试之前，需配置 NQA 客户端与 ICMP 服务器之间路由可达。

### 数据准备

在配置 Jitter 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                                 |
|----|----------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                               |
| 2  | ICMP 服务器端监听的 IP 地址                                                                                 |
| 3  | ICMP 客户端发送探测报文的地址                                                                                  |
| 4  | （可选）：VPN 实例名、客户端发送探测报文的源地址、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号、路径的最大 MTU 值、步长值 |

| 序号 | 数据        |
|----|-----------|
| 5  | 启动方式和结束方式 |

## 6.20.2 配置 Path MTU 测试参数

在置 Path MTU 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type pathmtu**，配置测试例类型为 Path MTU。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5**（可选）根据需要，配置 Path MTU 测试的其他参数。

- 执行命令 **discovery-pmtu-max pmtu-max**，配置路径 MTU 测试范围的最大值。
- 执行命令 **step step**，配置路径 MTU 测试中的报文长度的递增步长值。
- 执行命令 **vpn-instance vpn-instance-name**，配置所测试的 VPN 实例。
- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **probe-count number**，配置每次发送的测试探针个数。
- 执行命令 **interval seconds interval**，配置发送测试包的时间间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.20.3 检查配置结果

在 Path MTU 测试成功后，可以查看到 Path MTU 测试的结果数据。

### 前提条件

已经完成 Path MTU 测试的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。

### 操作步骤

- 步骤 1** 使用命令 **display nqa results [ test-instance admin-name test-name ]**，在 NQA 客户端查看测试结果。

----结束

### 任务示例

对于 Path MTU 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance admin pathmtu
NQA entry(admin, pathmtu) :testflag is inactive ,testtype is pathmtu
1. Test 0 result The test is finished
 Completions: success Busies: 0
 Destination-address: 100.1.1.201 Discovery field min: 48 byte
 Discovery field max: 1600 byte Drops: 0
 MTU: 1148 Response probe: 13
 Send probe: 16 Optimum first step: 0 byte
 Second step: 100 byte Timeouts: 3
```

## 6.21 配置 NQA 测试例实现 MPing 保留组地址

介绍使用 NQA 进行 MPing 保留组地址测试，检测出接口所在网段上存在哪些保留组成员。

### 6.21.1 建立配置任务

在配置 NQA 测试例实现 MPing 保留组地址前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.21.2 创建 NQA MPing 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 6.21.3 配置 NQA MPing 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 6.21.4 （可选）调整 NQA MPing 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 6.21.5 启动 NQA MPing 测试例

启动 NQA 测试例进行测试。

### 6.21.6 检查配置结果

在 NQA 测试例实现 MPing 保留组地址测试后，可以查看到 MPing 保留组地址测试的结果数据。

## 6.21.1 建立配置任务

在配置 NQA 测试例实现 MPing 保留组地址前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

配置 MPing 目的组地址为保留组地址，可以检测出接口所在网段上存在哪些保留组成员。

保留组播组标识了符合特定条件的一组网络设备（即保留组成员）。当保留组成员接收到目的地址为保留组地址的 ICMP-Echo-Request 报文时，回复 ICMP-Echo-Reply 报文。常用的保留组地址有：

- 224.0.0.1：子网上的所有系统
- 224.0.0.2：子网上的所有路由器
- 224.0.0.5：OSPF IGP 路由器
- 224.0.0.13：PIM 路由器



说明

主机或路由器能否回应 ICMP-Echo-Reply 报文，与其上安装的操作系统及版本有关。

### 前置任务

无

### 数据准备

在配置 NQA MPing 测试例之前，需要准备以下数据。

| 序号 | 数据                                                                                                                                   |
|----|--------------------------------------------------------------------------------------------------------------------------------------|
| 1  | MPing 目的组地址                                                                                                                          |
| 2  | NQA 测试例名称                                                                                                                            |
| 3  | 发送 ICMP-Echo-Request 报文的出接口                                                                                                          |
| 4  | （可选）ICMP-Echo-Request 报文的大小、ICMP-Echo-Request 报文的填充字符、ICMP-Echo-Request 报文的发送个数、ICMP-Echo-Request 报文的发送间隔、等待 ICMP-Echo-Reply 报文的超时时间 |

## 6.21.2 创建 NQA MPing 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，创建 NQA 测试例，进入测试例视图。
- 步骤 3** 执行命令 **test-type mping**，规定该测试例的测试类型为 MPing。
- 步骤 4** 执行命令 **quit**，退出测试例视图。

----结束

### 6.21.3 配置 NQA MPing 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入测试例视图。
- 步骤 3** 执行命令 **destination-address ipv4 ip-address**，配置 MPing 目的组地址（即 ICMP-Echo-Request 报文的目的地址）为保留组地址。
- 步骤 4** 执行命令 **source-interface interface-type interface-number**，指定发送 ICMP-Echo-Request 报文的出接口。
- 步骤 5** 执行命令 **quit**，退出测试例视图。

----结束

### 6.21.4 （可选）调整 NQA MPing 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。本节各项配置均可选。

 说明

- 下列过程的步骤均为可选。
- MPing 属于 ICMP，继承 NQA ICMP 测试例调整功能。本节列举几种常用的调整命令。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入测试例视图。
- 步骤 3** 执行命令 **datasize size**，配 ICMP-Echo-Request 报文的大小。

- 步骤 4** 执行命令 **tos value**，配置 ICMP-Echo-Request 报文的服务优先级。
- 步骤 5** 执行命令 **datafill fillstring**，配置 ICMP-Echo-Request 报文的填充字符。
- 步骤 6** 执行命令 **probe-count number**，配置 ICMP-Echo-Request 报文的发送个数。
- 步骤 7** 执行命令 **interval seconds interval**，配置 ICMP-Echo-Request 报文的发送间隔，必须大于 **timeout** 命令设置的超时时间。
- 步骤 8** 执行命令 **timeout time**，配置等待 ICMP-Echo-Reply 报文的超时时间。
- 步骤 9** 执行命令 **quit**，退出测试组视图。

----结束

## 6.21.5 启动 NQA MPing 测试例

启动 NQA 测试例进行测试。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。



说明

MPing 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **start now**，启动 NQA 测试例。
- 步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

## 6.21.6 检查配置结果

在 NQA 测试例实现 MPing 保留组地址测试后，可以查看到 MPing 保留组地址测试的结果数据。

### 前提条件

已经完成 NQA 测试例实现 MPing 保留组地址测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 在 NQA 客户端执行 **display nqa-agent [ admin-name test-name ] [ verbose ]** 命令查看 NQA 客户端配置的测试例状态信息。



- 在 NQA 客户端执行 **display nqa results** [ *admin-name test-name* ] 命令查看 NQA 测试例运行结果。

----结束

## 任务示例

执行命令 **display nqa-agent**，可以看到全部或者单个配置的 nqa 测试例内容，也可以查看详细信息。

```
<HUAWEI> display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance admin mping
test-type mping
destination-address ipv4 224.0.0.5
source-interface GigabitEthernet0/0/0
nqa status : normal
```

对于 MPing 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry (admin, mping) :testflag is inactive ,testtype is mping
1. Test 1 result The test is finished
 Completion:success Timeouts number: 0
 Drops number: 0 TargetAddress: 224.0.0.1
 ProbeResponses number: 3 SentProbes number: 3
 Buses: 0
 1. Receiver 1
 CompletionTime Min/Max/Sum: 2/3/8
 Sum2CompletionTime: 22
 LastGoodProbe time: 2009-1-12 13:11:10.4
 RecevierAddress: 6.0.206.6
```

## 6.22 配置 NQA 测试例实现 MPing 普通组地址

介绍使用 NQA 进行 MPing 普通地址测试，查看检查协议运行状态是否正常，确认组播分发树是否正确建立；检查网络中存在的组成员，计算从 MPing 发起者到组成员的 TTL、响应时间等参数。

### 6.22.1 建立配置任务

在配置 NQA 测试例实现 MPing 普通组地址前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.22.2 创建 NQA MPing 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 6.22.3 配置 NQA MPing 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 6.22.4 （可选）调整 NQA MPing 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 6.22.5 启动 NQA MPing 测试例

启动 NQA 测试例进行测试。

### 6.22.6 检查配置结果

在 NQA 测试例实现 MPing 普通组地址测试后，可以查看到 MPing 普通组地址测试的结果数据。

## 6.22.1 建立配置任务

在配置 NQA 测试例实现 MPing 普通组地址前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

配置 MPing 目的组地址为普通组地址，则可以实现以下功能：

- 构造组播流量，触发一系列的协议过程。通过查看路由器上的组播路由信息，检查协议运行状态是否正常，确认组播分发树是否正确建立。
- （此用途要求主机支持 MPing 特性）通过对目的主机反馈的 ICMP-Echo-Reply 报文进行统计处理，检查网络中存在的组成员，计算从 MPing 发起者到组成员的 TTL、响应时间等。按照一定时间间隔连续执行多次 MPing，计算网络时延和路由抖动。

### 前置任务

如果使用普通组地址进行 MPing，网络中需要配置完备的组播功能。

### 数据准备

在执行 MPing 测试例之前，需要准备以下数据。

| 序号 | 数据                                                                                                                                   |
|----|--------------------------------------------------------------------------------------------------------------------------------------|
| 1  | MPing 目的组地址                                                                                                                          |
| 2  | NQA 测试例名称                                                                                                                            |
| 3  | 发送 ICMP-Echo-Request 报文的出接口                                                                                                          |
| 4  | （可选）ICMP-Echo-Request 报文的大小、ICMP-Echo-Request 报文的填充字符、ICMP-Echo-Request 报文的发送个数、ICMP-Echo-Request 报文的发送间隔和等待 ICMP-Echo-Reply 报文的超时时间 |

## 6.22.2 创建 NQA MPing 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 `system-view`，进入系统视图。
- 步骤 2** 执行命令 `nqa test-instance admin-name test-name`，创建 NQA 测试例，进入测试例视图。
- 步骤 3** 执行命令 `test-type mping`，规定该测试例的测试类型为 MPing。

**步骤 4** 执行命令 **quit**，退出测试例视图。

----结束

### 6.22.3 配置 NQA MPing 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

#### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入测试例视图。

**步骤 3** 执行命令 **destination-address ipv4 ip-address**，配置 MPing 目的组地址（即 ICMP-Echo-Request 报文的目的地址）为普通组地址。

**步骤 4** 执行命令 **source-interface interface-type interface-number**，指定发送 ICMP-Echo-Request 报文的出接口。

**步骤 5** 执行命令 **quit**，退出测试例视图。

----结束

### 6.22.4 （可选）调整 NQA MPing 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

#### 背景信息

在作为 NQA Client 的路由器上进行如下配置。本节各项配置均可选。

 说明

- 下列过程的步骤均为可选。
- MPing 属于 ICMP，继承 NQA ICMP 测试例调整功能。本节列举几种常用的调整命令。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入测试例视图。

**步骤 3** 执行命令 **datasize size**，配 ICMP-Echo-Request 报文的大小。

**步骤 4** 执行命令 **ttl number**，配置 ICMP-Echo-Request 报文的 TTL 值。

**步骤 5** 执行命令 **tos value**，配置 ICMP-Echo-Request 报文的服务优先级。

**步骤 6** 执行命令 **datafill fillstring**，配置 ICMP-Echo-Request 报文的填充字符。

**步骤 7** 执行命令 **probe-count number**，配置 ICMP-Echo-Request 报文的发送个数。

**步骤 8** 执行命令 **interval seconds interval**，配置 ICMP-Echo-Request 报文的发送间隔，必须大于 **timeout** 命令设置的超时时间。

**步骤 9** 执行命令 **timeout time**，配置等待 ICMP-Echo-Reply 报文的超时时间。

**步骤 10** 执行命令 **quit**，退出测试组视图。

----结束

## 6.22.5 启动 NQA MPing 测试例

启动 NQA 测试例进行测试。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

 说明

MPing 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 执行命令 **start now**，启动 NQA 测试例。

**步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

## 6.22.6 检查配置结果

在 NQA 测试例实现 MPing 普通组地址测试后，可以查看到 MPing 普通组地址测试的结果数据。

### 前提条件

已经完成 NQA 测试例实现 MPing 普通组地址测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 在 NQA 客户端执行 **display nqa-agent [ admin-name test-name ] [ verbose ]** 命令查看 NQA 客户端配置的测试例状态信息。
- 在 NQA 客户端执行 **display nqa results [ admin-name test-name ]** 命令查看 NQA 测试例运行结果。

----结束

## 任务示例

执行命令 **display nqa-agent**，可以看到全部或者单个配置的 nqa 测试例内容，也可以查看详细信息。

```
<HUAWEI> display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained: 999

nqa test-instance admin mping
test-type mping
destination-address ipv4 224.0.0.5
source-interface GigabitEthernet0/0/0
nqa status : normal
```

执行命令 **display nqa results**，如果测试成功，可以看到如下信息。

```
<HUAWEI> display nqa results
NQA entry (admin, mping) :testflag is inactive ,testtype is mping
1 . Test 1 result The test is finished
Completion:success Timeouts number: 0
Drops number: 0 TargetAddress: 224.1.2.1
ProbeResponses number: 3 SentProbes number: 3
Busies: 0
1 . Receiver 1
CompletionTime Min/Max/Sum: 2/3/8
Sum2CompletionTime: 22
LastGoodProbe time: 2009-1-12 13:11:10.4
RecevierAddress: 6.0.206.6
```

## 6.23 通过 NQA 检测从组播源到查询者的 RPF 路径

介绍使用 NQA 进行从组播源到查询者的 RPF 路径测试。

### 6.23.1 建立配置任务

在通过 NQA 检测从组播源到查询者的 RPF 路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.23.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 6.23.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 6.23.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 6.23.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

### 6.23.6 检查配置结果

在 NQA 测试例实现从组播源到查询者的 RPF 路径测试后，可以查看到从组播源到查询者的 RPF 路径的结果数据。

## 6.23.1 建立配置任务

在通过 NQA 检测从组播源到查询者的 RPF 路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

通过运行 NQA MTrace 测试例，可以检测从组播源到查询者的 RPF 路径。

进行此项检测时，不要求网络中存在真实的组播数据流，可以用来探测组播报文可能的传输路线。

在组播故障处理和日常维护中使用此项检测，有助于定位故障结点、减少配置错误。

## 前置任务

在执行 MTrace 之前，需要在网络中配置完备的组播功能。

## 数据准备

在配置 MTrace 之前，需要准备以下数据。

| 序号 | 数据                                                                             |
|----|--------------------------------------------------------------------------------|
| 1  | 组播源地址                                                                          |
| 2  | NQA 测试例名称                                                                      |
| 3  | (可选) VPN 实例的名称                                                                 |
| 4  | (可选) IGMP-Tracert-Request 报文的 TTL 值                                            |
| 5  | (可选) hop-by-hop 追踪模式下的最大跳数                                                     |
| 6  | (可选) IGMP-Tracert-Response 报文 (即封装 IGMP-Tracert-Response 消息的 IP 报文) 的目的地址和 TTL |
| 7  | (可选) 等待 IGMP-Tracert-Response 消息的超时时间                                          |
| 8  | (可选) 超时情况下查询者发起 MTrace 的最大次数                                                   |

### 6.23.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，创建测试例，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **test-type mtrace**，配置测试类型为 MTrace。
- 步骤 4** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

### 6.23.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

## 背景信息

按照测试目的，在创建了 NQA MTrace 测试例的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **mtrace-source-address ipv4 ip-address**，指定组播源地址。
- 步骤 4**（可选）执行命令 **vpn-instance vpn-instance-name**，配置 VPN 实例的名称。
- 步骤 5** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

### 6.23.4（可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

## 背景信息

在已配置了 MTrace 测试例基本功能的路由器上进行如下配置。

 说明

本节各项配置均可选。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **ttl number**，配置 IGMP-Tracert-Request 报文的 TTL 值，即 max-hop 追踪模式下的最大跳数。
- 步骤 4** 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，设置 hop-by-hop 追踪模式下的最大跳数。*first-ttl* 值必须为 1。
- 步骤 5** 执行命令 **mtrace-response-address ipv4 ip-address [ ttl value ]**，配置 IGMP-Tracert-Response 报文（即封装 IGMP-Tracert-Response 消息的 IP 报文）的目的地址和 TTL。
- 步骤 6** 执行命令 **timeout time**，配置等待 IGMP-Tracert-Response 消息的超时时间。
- 步骤 7** 执行命令 **probe-count number**，配置超时情况下查询者发起 MTrace 的最大次数。当查询者等待 IGMP-Tracert-Response 消息超时，会再次发起 MTrace。
- 步骤 8** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

### 6.23.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。



## 背景信息

在作为 NQA Client 的路由器上进行如下配置。

 说明

MTrace 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **start now**，启动 NQA 测试例。
- 步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

### 6.23.6 检查配置结果

在 NQA 测试例实现从组播源到查询者的 RPF 路径测试后，可以查看到从组播源到查询者的 RPF 路径的结果数据。

## 前提条件

已经完成 NQA 检测从组播源到查询者 RPF 路径测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

- 在 NQA 客户端执行 **display nqa-agent [ admin-name test-name ] [ verbose ]** 命令查看 NQA 客户端配置的测试例状态信息。
- 在 NQA 客户端执行 **display nqa results [ admin-name test-name ]** 命令查看 NQA 测试例运行结果。
- 在 NQA 客户端执行 **display nqa history** 命令查看 NQA 测试例历史信息。
- 在 NQA 客户端执行 **display mtrace statistics** 命令查看 MTrace 报文统计信息。

----结束

## 任务示例

执行命令 **display nqa-agent**，可以看到 NQA 测试例的内容。例如：

```
<HUAWEI> display nqa-agent admin aa verbose
```

## 6.24 通过 NQA 检测从组播源到查询者的组播路径

介绍使用 NQA 进行从组播源到查询者的组播路径测试。

### 6.24.1 建立配置任务



在通过 NQA 检测从组播源到查询者的组播路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

#### 6.24.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

#### 6.24.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

#### 6.24.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

#### 6.24.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

#### 6.24.6 检查配置结果

在 NQA 测试例实现从组播源到查询者的组播路径后，可以查看到从组播源到查询者的组播路径的结果数据。

## 6.24.1 建立配置任务

在通过 NQA 检测从组播源到查询者的组播路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

通过运行 NQA MTrace 测试例，可以检测从组播源到查询者的组播路径。

进行此项检测时，要求网络存在真实的组播数据流，且查询者位于组播分发树上。此项检测可以用来追踪报文实际转发路径。

此项检测主要有以下几种用途。

- 在组播故障处理和日常维护中执行此项检测，有助于定位故障结点、减少配置错误。
- 循环执行追踪，在追踪过程中收集流量信息，可以统计组播流速率。
- 网管通过分析 MTrace 输出的异常节点信息，产生告警信息或故障节点信息。

### 前置任务

在执行 MTrace 之前，需要在网络中配置完备的组播功能。

### 数据准备

在配置 MTrace 之前，需要准备以下数据。

| 序号 | 数据            |
|----|---------------|
| 1  | 测试例名称         |
| 2  | 组播源地址         |
| 3  | 组播组地址         |
| 4  | （可选）VPN 实例的名称 |

## 6.24.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，创建测试例，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **test-type mtrace**，配置测试类型为 MTrace。
- 步骤 4** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.24.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 背景信息

在创建了 NQA MTrace 测试例的路由器上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **mtrace-source-address ipv4 ip-address**，指定组播源地址。
- 步骤 4** 执行命令 **mtrace-group-address ipv4 ip-address**，指定组播组地址。必须是普通组地址。
- 步骤 5**（可选）执行命令 **vpn-instance vpn-instance-name**，配置 VPN 实例的名称。
- 步骤 6** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.24.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 背景信息

在已配置了 MTrace 测试例基本功能的路由器上进行如下配置。

 说明

本节各项配置均可选。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **ttl number**，配置 IGMP-Tracert-Request 报文的 TTL 值，即 max-hop 追踪模式的最大跳数。
- 步骤 4** 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置 hop-by-hop 追踪模式下的最大追踪跳数。*first-ttl* 值必须为 1。
- 步骤 5** 执行命令 **mtrace-response-address ipv4 ip-address [ ttl value ]**，配置 IGMP-Tracert-Response 报文（即封装 IGMP-Tracert-Response 消息的 IP 报文）的目的地址和 TTL。
- 步骤 6** 执行命令 **timeout time**，配置等待 IGMP-Tracert-Response 消息的超时时间。
- 步骤 7** 执行命令 **probe-count number**，配置超时情况下查询者发起 MTrace 的最大次数。当查询者等待 IGMP-Tracert-Response 消息超时，会再次发起 MTrace。
- 步骤 8** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

### 6.24.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。



说明

MTrace 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **start now**，启动 NQA 测试例。
- 步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

### 6.24.6 检查配置结果

在 NQA 测试例实现从组播源到查询者的组播路径后，可以查看到从组播源到查询者的组播路径的结果数据。

## 前提条件

已经完成 NQA 检测从组播源到查询者组播路径测试功能的所有配置。



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

- 在 NQA 客户端执行 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ] 命令查看 NQA 客户端配置的测试例状态信息。
- 在 NQA 客户端执行 **display nqa results** [ *admin-name test-name* ] 命令查看 NQA 测试例运行结果。
- 在 NQA 客户端执行 **display nqa history** 命令查看 NQA 测试例历史信息。
- 在 NQA 客户端执行 **display mtrace statistics** 命令查看 MTrace 报文统计信息。

----结束

## 任务示例

执行命令 **display nqa-agent**，可以看到 nqa 测试例配置内容。例如：

```
<HUAWEI> display nqa-agent admin aa verbose
```

## 6.25 通过 NQA 检测从组播源到目的主机的 RPF 路径

介绍使用 NQA 进行从组播源到目的主机的 RPF 路径测试。

### 6.25.1 建立配置任务

在通过 NQA 检测从组播源到目的主机的 RPF 路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.25.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 6.25.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 6.25.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 6.25.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

### 6.25.6 设置查询者过滤策略

此配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳上生效。

### 6.25.7 检查配置结果

在 NQA 检测从组播源到目的主机的 RPF 路径后，可以查看到从组播源到目的主机的 RPF 路径的结果数据。

## 6.25.1 建立配置任务

在通过 NQA 检测从组播源到目的主机的 RPF 路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

通过运行 NQA MTrace 测试例，可以检测从组播源到目的主机的 RPF 路径。

进行此项检测时，不要求网络中存在真实的组播数据流，可以用来探测组播报文可能的传输路线。

在组播故障处理和日常维护中使用此项检测，有助于定位故障结点、减少配置错误。

## 前置任务

在执行 MTrace 之前，需要在网络中配置完备的组播功能。

## 数据准备

在配置 MTrace 之前，需要准备以下数据。

| 序号 | 数据             |
|----|----------------|
| 1  | 测试例名称          |
| 2  | 组播源地址          |
| 3  | 目的主机地址         |
| 4  | (可选) VPN 实例的名称 |

## 6.25.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，创建测试例，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **test-type mtrace**，配置测试类型为 MTrace。
- 步骤 4** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.25.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 背景信息

按照测试目的，在创建了 NQA MTrace 测试例的路由器上进行如下配置。



说明

查询者必须满足以下条件之一：

- 与目的主机直接相连
- 能够单播 ping 通目的主机或者最后一跳路由器

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **mtrace-source-address ipv4 ip-address**，配置组播源地址。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的主机地址。
- 步骤 5** （可选）执行命令 **vpn-instance vpn-instance-name**，配置 VPN 实例的名称。
- 步骤 6** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.25.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

## 背景信息

在已配置了 MTrace 测试例基本功能的路由器上进行如下配置。



说明

本节各项配置均可选。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **ttl number**，配置 IGMP-Tracert-Request 报文的 TTL 值，即 max-hop 追踪模式下的最大跳数。
- 步骤 4** 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置 hop-by-hop 追踪模式下的最大跳数。*first-ttl* 值必须为 1。
- 步骤 5** 执行命令 **mtrace-response-address ipv4 ip-address [ ttl value ]**，配置 IGMP-Tracert-Response 报文（即封装 IGMP-Tracert-Response 消息的 IP 报文）的目的地址和 TTL。
- 步骤 6** 执行命令 **mtrace-query-type last-hop**，限定 MTrace 从指定的最后一跳路由器向源发起追踪。

当存在多台路由器与指定主机相连时，从不同的路由器发起的 RPF 路径可能不同，指定最后一跳路由器可以唯一确定一条 RPF 路径。

执行该命令时，必须指定最后一跳路由器地址。

- 步骤 7** 执行命令 **mtrace-last-hop-address ipv4 ip-address**，指定最后一跳路由器地址。

如果组播网络中存在其他厂商的设备，则必须指定最后一跳路由器地址。

**步骤 8** 执行命令 **source-address ipv4 ip-address**，配置 IGMP-Tracert-Query 报文源地址。必须是本地接口地址。

如果组播网络中存在其他厂商的设备，则必须配置 IGMP-Tracert-Query 报文源地址。

**步骤 9** 执行命令 **timeout time**，配置等待 IGMP-Tracert-Response 消息的超时时间。

**步骤 10** 执行命令 **probe-count number**，配置超时情况下查询者发起 MTrace 的最大次数。当查询者等待 IGMP-Tracert-Response 消息超时，会再次发起 MTrace。

**步骤 11** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.25.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

### 背景信息

在作为 NQA Client 的路由器上进行如下配置。

 说明

MTrace 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 执行命令 **start now**，启动 NQA 测试例。

**步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

## 6.25.6 设置查询者过滤策略

此配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳上生效。

### 背景信息

在连接用户主机的路由器上进行如下配置。

 说明

此项配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳路由器上生效。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **mtrace query-policy [ basic-acl-number ]**，配置查询者过滤策略。ACL 限定了可信任的查询者的地址范围，最后一跳路由器依据该 ACL 拒绝非法查询者发出的 IGMP-Tracert-Query 消息。



 说明

- 该命令只在最后一跳路由器上生效，且查询者不是最后一跳路由器。
- 该命令只对使用单播 IP 报文封装的 IGMP-Tracert-Query 消息进行过滤。
- 该命令不适用于从查询者本地发起的追踪。

----结束

## 6.25.7 检查配置结果

在 NQA 检测从组播源到目的主机的 RPF 路径后，可以查看到从组播源到目的主机的 RPF 路径的结果数据。

### 前提条件

已经完成 NQA 检测从组播源到目的主机 RPF 路径测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下，只能显示最近 5 次的测试结果。

### 操作步骤

- 在 NQA 客户端执行 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ] 命令查看 NQA 客户端配置的测试例状态信息。
- 在 NQA 客户端执行 **display nqa results** [ *admin-name test-name* ] 命令查看 NQA 测试例运行结果。
- 在 NQA 客户端执行 **display nqa history** 命令查看 NQA 测试例历史信息。
- 在 NQA 客户端执行 **display mtrace statistics** 命令查看 MTrace 报文统计信息。

----结束

### 任务示例

执行命令 **display nqa-agent**，可以看到 nqa 测试例配置内容。例如：

```
<HUAWEI> display nqa-agent admin aa verbose
```

## 6.26 通过 NQA 检测从组播源到目的主机的组播路径

介绍使用 NQA 进行从组播源到目的主机的组播路径测试。

### 6.26.1 建立配置任务

在通过 NQA 检测从组播源到目的主机的组播路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.26.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

### 6.26.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

### 6.26.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 6.26.5 启动 NQA MTrace 测试例



启动 NQA 测试例进行测试。

#### 6.26.6 设置查询者过滤策略

此配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳上生效。

#### 6.26.7 检查配置结果

在 NQA 检测从组播源到目的主机的组播路径后，可以查看到从组播源到目的主机的组播路径的结果数据。

## 6.26.1 建立配置任务

在通过 NQA 检测从组播源到目的主机的组播路径前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

通过运行 NQA MTrace 测试例，可以检测从组播源到目的主机的组播路径。

进行此项检测时，要求网络存在真实的组播数据流，且目的主机正在接收此数据。此项检测可以用来追踪报文实际转发路径。

此项检测主要有以下几种用途。

- 在组播故障处理和日常维护中执行此项检测，有助于定位故障结点、减少配置错误。
- 循环执行追踪，在追踪过程中收集流量信息，可以统计组播流速率。
- 网管通过分析 MTrace 输出的异常节点信息，产生告警信息或故障节点信息。

### 前置任务

在执行 MTrace 之前，需要在网络中配置完备的组播功能。

### 数据准备

在配置 MTrace 之前，需要准备以下数据。

| 序号 | 数据             |
|----|----------------|
| 1  | 测试例名称          |
| 2  | 组播源地址          |
| 3  | 组播组地址          |
| 4  | 目的主机地址         |
| 5  | (可选) VPN 实例的名称 |

## 6.26.2 创建 NQA MTrace 测试例

在进行 NQA 测试前，需要首先创建 NQA 测试例。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，创建测试例，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **test-type mtrace**，配置测试类型为 MTrace。
- 步骤 4** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

### 6.26.3 配置 NQA MTrace 测试例基本功能

配置 NQA 测试启动必须要配置的相关参数。

## 背景信息

按照测试目的，在创建了 NQA MTrace 测试例的路由器上进行如下配置。

 说明

查询者必须满足以下条件之一：

- 与目的主机直接相连
- 能够单播 ping 通目的主机或者最后一跳路由器
- 在从组播源到目的主机的组播路径上，例如第一跳路由器

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。
- 步骤 3** 执行命令 **mtrace-source-address ipv4 ip-address**，指定组播源地址。
- 步骤 4** 执行命令 **mtrace-group-address ipv4 ip-address**，指定组播组地址。必须是普通组地址。
- 步骤 5** 执行命令 **destination-address ipv4 ip-address**，配置目的主机地址。
- 步骤 6**（可选）执行命令 **vpn-instance vpn-instance-name**，配置 VPN 实例的名称。
- 步骤 7** 执行命令 **mtrace-query-type { all-router | destination | last-hop | multicast-tree }**，指定 MTrace 的发起方式。根据网络实际情况，指定正确的发起方式，有助于准确快速的执行追踪。如果不执行该命令则系统使用 **multicast-tree** 发起方式。

四种可选方式应用场景如下：

- **all-router** 适用于：当前路由器与目的主机直接相连。
- **destination** 适用于：当前路由器到目的主机单播报文可达。
- **last-hop** 适用于：已知最后一跳路由器地址，且当前路由器到最后一跳路由器单播报文可达。当指定为 **last-hop** 时，必须指定最后一跳路由器地址。
- **multicast-tree** 适用于：当前路由器在从组播源到目的主机的组播路径上。



### 注意

如果配置对指定的组播 VPN 网络进行组播 Trace，则不支持 **mtrace-query-type all-router** 选项配置。

**步骤 8** （可选）执行命令 **mtrace-last-hop-address ipv4 ip-address**，指定最后一跳路由器地址。

**步骤 9** （可选）执行命令 **source-address ipv4 ip-address**，配置 IGMP-Tracert-Query 报文源地址，必须是本地接口地址。当使用 multicast-tree 方式时，不支持此项配置。

**步骤 10** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.26.4 （可选）调整 NQA MTrace 测试例性能

配置 NQA 测试启动可选的配置，可以根据网络的运行情况，来选取相关的参数。

### 背景信息

在已配置了 MTrace 测试例基本功能的路由器上进行如下配置。



说明

本节各项配置均可选。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 执行命令 **ttl number**，配置 IGMP-Tracert-Request 报文的 TTL 值，即 max-hop 追踪模式下的最大跳数。

**步骤 4** 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置 hop-by-hop 追踪模式下的最大跳数。*first-ttl* 值必须为 1。

**步骤 5** 执行命令 **mtrace-last-hop-address ipv4 ip-address**，指定最后一跳路由器地址。

**步骤 6** 执行命令 **source-address ipv4 ip-address**，配置 IGMP-Tracert-Query 报文源地址，必须是本地接口地址。当使用 multicast-tree 方式时，不支持此项配置。

**步骤 7** 执行命令 **mtrace-response-address ipv4 ip-address [ ttl value ]**，配置 IGMP-Tracert-Response 报文（即封装 IGMP-Tracert-Response 消息的 IP 报文）的目的地址和 TTL。

**步骤 8** 执行命令 **timeout time**，配置等待 IGMP-Tracert-Response 消息的超时时间。

**步骤 9** 执行命令 **probe-count number**，配置超时情况下查询者发起 MTrace 的最大次数。当查询者等待 IGMP-Tracert-Response 消息超时，会再次发起 MTrace。

**步骤 10** 执行命令 **quit**，退出 NQA 测试例视图。

----结束

## 6.26.5 启动 NQA MTrace 测试例

启动 NQA 测试例进行测试。

## 背景信息

在作为 NQA Client 的路由器上进行如下配置。



说明

MTrace 的启动方式与其它 NQA 测试例相同，本节以一种方式为例。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 执行命令 **start now**，启动 NQA 测试例。

**步骤 4** 执行命令 **quit**，退出测试组视图。

----结束

## 6.26.6 设置查询者过滤策略

此配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳上生效。

## 背景信息

在连接用户主机的路由器上进行如下配置。



说明

此项配置只在接收到单播方式的 IGMP-Tracert-Query 报文的最后一跳路由器上生效。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **mtrace query-policy [ basic-acl-number ]**，配置查询者过滤策略。ACL 限定了可信任的查询者的地址范围，最后一跳路由器依据该 ACL 拒绝非法查询者发出的 IGMP-Tracert-Query 消息。



说明

- 该命令只在最后一跳路由器上生效，且查询者不是最后一跳路由器。
- 该命令只对使用单播 IP 报文封装的 IGMP-Tracert-Query 消息进行过滤。
- 该命令不适用于从查询者本地发起的追踪。

----结束

## 6.26.7 检查配置结果

在 NQA 检测从组播源到目的主机的组播路径后，可以查看到从组播源到目的主机的组播路径的结果数据。

## 前提条件

已经完成 NQA 检测从组播源到目的主机组播路径测试功能的所有配置。

## 背景信息



说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

- 在 NQA 客户端执行 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ] 命令查看 NQA 客户端配置的测试例状态信息。
- 在 NQA 客户端执行 **display nqa results** [ *admin-name test-name* ] 命令查看 NQA 测试例运行结果。
- 在 NQA 客户端执行 **display nqa history** 命令查看 NQA 测试例历史信息。
- 在 NQA 客户端执行 **display mtrace statistics** 命令查看 MTrace 报文统计信息。

----结束

## 任务示例

执行命令 **display nqa-agent**，可以看到 nqa 测试例配置内容。例如：

```
<HUAWEI> display nqa-agent admin aa verbose
```

## 6.27 配置单跳 PW 的 PWE3 Ping 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Ping 测试，了解 PW 的连通情况。

### 6.27.1 建立配置任务

在配置单跳 PW 的 PWE3 Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.27.2 配置单跳 PW 的 PWE3 Ping 测试参数

在配置单跳 PW 的 PWE3 Ping 测试时，需要配置的相关参数。

### 6.27.3 检查配置结果

在 NQA 检测单跳 PW 的 PWE3 Ping 测试后，可以查看到单跳 PW 的 PWE3 Ping 测试的结果数据。

## 6.27.1 建立配置任务

在配置单跳 PW 的 PWE3 Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

当需要通过 NQA 对单跳 PW（使用 LDP 方式作为信令）进行 Ping 测试，此时可以配置单跳 PW 的 PWE3 Ping 测试。

## 前置任务

在配置单跳 PW 的 PWE3 Ping 测试之前，需正确配置单跳动态 PW。

## 数据准备

在配置单跳 PW 的 PWE3 Ping 测试之前，需要准备以下数据：

| 序号 | 数据                                                 |
|----|----------------------------------------------------|
| 1  | PW 的 ID                                            |
| 2  | PW 的类型                                             |
| 3  | 连接 CE 的接口的类型和编号                                    |
| 4  | L2VC 的目的地址和 VC ID                                  |
| 5  | （可选）：Echo 报文响应模式、LSP EXP、允许的最大跳失败数、探针数目、TTL、报文超时时间 |
| 6  | 启动方式和结束方式                                          |

### 6.27.2 配置单跳 PW 的 PWE3 Ping 测试参数

在配置单跳 PW 的 PWE3 Ping 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type pwe3ping**，配置测试例类型为 PWE3 Ping。
- 步骤 4** （可选）执行命令 **vc-type ldp**，配置 PW 隧道建立方式。
- 步骤 5** （可选）执行命令 **local-pw-type { local-pw-type | ip-interworking }**，配置本端的 PW 类型。默认类型是 Ethernet。
- 步骤 6** （可选）执行命令 **label-type { control-word | label-alert | normal }**，配置 PW 标签类型。
- 步骤 7** 执行命令 **local-pw-id local-pw-id**，配置本端 PW ID。
- 步骤 8** （可选）根据需要，配置 PWE3 Ping 测试其他参数。
  - 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。
  - 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 步骤 9** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 延迟指定时间后启动测试例。

----结束

## 6.27.3 检查配置结果

在 NQA 检测单跳 PW 的 PWE3 Ping 测试后, 可以查看到单跳 PW 的 PWE3 Ping 测试的结果数据。

### 前提条件

已经完成单跳 PW 的 PWE3 Ping 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果, 必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 步骤 1** 在 NQA 客户端执行 **display nqa results** [ **test-instance** *admin-name test-name* ] 命令查看测试结果。

----结束

### 任务示例

对于单跳 PW 的 PWE3 Ping 类型的测试, 如果测试成功, 执行 **display nqa results** 命令, 可以看到以下信息。

- 错误统计:
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计:
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计:
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方
  - 报文最小往返时间、最大往返时间
  - 目的地址



已收到回应的报文数目、已发送的报文数

至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (admin, pwe3ping) :testflag is inactive ,testtype is pwe3ping
 1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:3.14.2.14
 Min/Max/Average Completion Time: 6/6/6
 Sum/Square-Sum Completion Time: 18/108
 Last Good Probe Time: 2009-2-27 9:0:42.3
 Lost packet ratio: 0 %
```

## 6.28 配置多跳 PW 的 PWE3 Ping 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Ping 测试，了解 PW 的连通情况。

### 6.28.1 建立配置任务

在配置多跳 PW 的 PWE3 Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.28.2 配置多跳 PW 的 PWE3 Ping 测试参数

在配置多跳 PW 的 PWE3 Ping 测试时，需要配置的相关参数。

### 6.28.3 检查配置结果

在 NQA 检测多跳 PW 的 PWE3 Ping 测试后，可以查看到多跳 PW 的 PWE3 Ping 测试的结果数据。

## 6.28.1 建立配置任务

在配置多跳 PW 的 PWE3 Ping 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

当需要通过 NQA 对多跳 PW（使用 LDP 方式作为信令）进行 Ping 测试，此时可以配置多跳 PW 的 PWE3 Ping 测试。

### 前置任务

在配置多跳 PW 的 PWE3 Ping 测试之前，需正确配置多跳动态 PW 或者配置多跳静态 PW。

### 数据准备

在配置多跳 PW 的 PWE3 Ping 测试之前，需要准备以下数据：

| 序号 | 数据         |
|----|------------|
| 1  | 本地 PW 的 ID |



| 序号 | 数据                                                       |
|----|----------------------------------------------------------|
| 2  | 对端 PW 的 ID 或 IP 地址                                       |
| 3  | PW 的类型                                                   |
| 4  | 测试可选参数（包括 Echo 报文响应模式、LSP EXP、允许的最大跳失败数、探针数目、TTL、报文超时时间） |
| 5  | 接入 CE 的接口类型和编号                                           |
| 6  | 启动方式和结束方式                                                |

## 6.28.2 配置多跳 PW 的 PWE3 Ping 测试参数

在配置多跳 PW 的 PWE3 Ping 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type pwe3ping**，配置测试例类型为 PWE3 Ping。

**步骤 4**（可选）执行命令 **vc-type ldp**，配置 PW 隧道建立方式。

**步骤 5**（可选）执行命令 **local-pw-type { local-pw-type | ip-interworking }**，配置本端的 PW 类型。默认类型是 Ethernet。

**步骤 6**（可选）执行命令 **label-type { control-word | label-alert }**，配置 PW 标签类型。

 说明

- 当 label-type 为 control-word 时，执行命令 **remote-pw-id remote-pw-id**，配置对端 PW ID。
- 当 label-type 为 label-alert 时，执行命令 **destination-address ipv4 ip-address { lsp-masklen mask-length | lsp-loopback loopback-address }**，配置 PWE3 Ping 测试的目的地址。

**步骤 7** 执行命令 **local-pw-id local-pw-id**，配置本端 PW ID。

**步骤 8**（可选）根据需要，配置 PWE3 Ping 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。

**步骤 9** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 立即启动测试例。
- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

### 6.28.3 检查配置结果

在 NQA 检测多跳 PW 的 PWE3 Ping 测试后, 可以查看到多跳 PW 的 PWE3 Ping 测试的结果数据。

#### 前提条件

已经完成多跳 PW 的 PWE3 Ping 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果, 必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

#### 操作步骤

**步骤 1** 在 NQA 客户端执行 **display nqa results** 命令查看测试例的任务调度情况。

----结束

#### 任务示例

对于多跳 PW 的 PWE3 Ping 类型的测试, 如果测试成功, 执行 **display nqa results** 命令, 可以看到以下信息。

- 错误统计:
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计:
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计:
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方
  - 报文最小往返时间、最大往返时间
  - 目的地址
  - 已收到回应的报文数目、已发送的报文数

至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (admin, pwe3ping) :testflag is inactive ,testtype is pwe3ping
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:8.1.1.2
 Min/Max/Average Completion Time: 4/6/5
 Sum/Square-Sum Completion Time: 16/88
 Last Good Probe Time: 2009-2-28 11:2:46.8
 Lost packet ratio: 0 %
```

## 6.29 配置单跳 PW 的 PWE3 Trace 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Trace 测试，了解 PW 上各个设备的连通性。

### 6.29.1 建立配置任务

在配置单跳 PW 的 PWE3 Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.29.2 配置单跳 PW 的 PWE3 Trace 测试参数

在配置单跳 PW 的 PWE3 Trace 测试时，需要配置的相关参数。

### 6.29.3 检查配置结果

在 NQA 检测单跳 PW 的 PWE3 Trace 测试后，可以查看到单跳 PW 的 PWE3 Trace 测试的结果数据。

## 6.29.1 建立配置任务

在配置单跳 PW 的 PWE3 Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

当需要通过 NQA 对单跳 PW（使用 LDP 方式作为信令）进行 Trace 测试，此时可以配置单跳 PW 的 PWE3 Trace 测试。

### 前置任务

在配置单跳 PW 的 PWE3 Trace 测试之前，需正确配置单跳动态 PW。

### 数据准备

在配置单跳 PW 的 PWE3 Trace 测试之前，需要准备以下数据：

| 序号 | 数据      |
|----|---------|
| 1  | PW 的 ID |
| 2  | PW 的类型  |

| 序号 | 数据                                                       |
|----|----------------------------------------------------------|
| 3  | 连接 CE 的接口的类型和编号                                          |
| 4  | L2VC 的目的地址和 VC ID                                        |
| 5  | 测试可选参数（包括 Echo 报文响应模式、LSP EXP、允许的最大跳失败数、探针数目、TTL、报文超时时间） |
| 6  | 启动方式和结束方式                                                |

## 6.29.2 配置单跳 PW 的 PWE3 Trace 测试参数

在配置单跳 PW 的 PWE3 Trace 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
  - 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
  - 步骤 3** 执行命令 **test-type pwe3trace**，配置测试例类型为 PWE3 Trace。
  - 步骤 4**（可选）执行命令 **vc-type ldp**，配置 PW 隧道建立方式。
  - 步骤 5**（可选）执行命令 **local-pw-type {local-pw-type | ip-interworking}**，配置本端的 PW 类型。默认类型是 Ethernet。
  - 步骤 6**（可选）执行命令 **label-type { control-word | label-alert | normal }**，配置 PW 标签类型。
  - 步骤 7** 执行命令 **local-pw-id local-pw-id**，配置本端 PW ID。
  - 步骤 8**（可选）根据需要，配置 PWE3 Trace 测试其他参数。
    - 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。
    - 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
    - 执行命令 **tracert-hopfailtimes times**，配置 PWE3 Trace 测试的跳失败数。
    - 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。
  - 步骤 9** 执行命令 **start**，启动 NQA 测试。
- 命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：
- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。

- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

### 6.29.3 检查配置结果

在 NQA 检测单跳 PW 的 PWE3 Trace 测试后, 可以查看到单跳 PW 的 PWE3 Trace 测试的结果数据。

#### 前提条件

已经完成单跳 PW 的 PWE3 Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果, 必须使用 **display nqa results** 命令查看测试结果, 并且只能显示最近 5 次的测试结果。

#### 操作步骤

- 步骤 1** 执行 **display nqa results** [ **test-instance** admin-name test-name ] 命令, 在 NQA 客户端查看测试结果。

----结束

#### 任务示例

对于单跳 PW 的 PWE3 Trace 类型的测试, 如果测试成功, 执行 **display nqa results** 命令, 可以看到以下信息。

- 错误统计:
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计:
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计:
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方
  - 报文最小往返时间、最大往返时间
  - 目的地址
  - 已收到回应的报文数目、已发送的报文数

至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (test, pwe3trace) :testflag is inactive ,testtype is pwe3trace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-2-28 0:42:37.5
1 . Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 8/10/9
 Sum/Square-Sum Completion Time: 28/264
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-2-28 0:42:37.5
 Destination ip address:3.14.2.14
 Lost packet ratio: 0 %
```

## 6.30 配置多跳 PW 的 PWE3 Trace 测试

介绍使用 NQA 进行单跳 PW 的 PWE3 Trace 测试，了解 PW 上各个设备的连通性。

### 6.30.1 建立配置任务

在配置多跳 PW 的 PWE3 Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.30.2 配置多跳 PW 的 PWE3 Trace 测试参数

在配置多跳 PW 的 PWE3 Trace 测试时，需要配置的相关参数。

### 6.30.3 检查配置结果

在 NQA 检测多跳 PW 的 PWE3 Trace 测试后，可以查看到多跳 PW 的 PWE3 Trace 测试的结果数据。

## 6.30.1 建立配置任务

在配置多跳 PW 的 PWE3 Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

当需要通过 NQA 对多跳 PW（使用 LDP 方式作为信令）进行 Trace 测试，此时可以配置多跳 PW 的 PWE3 Trace 测试。

### 前置任务

在配置多跳 PW 的 PWE3 Trace 测试之前，需正确配置多跳动态 PW 或者配置多跳静态 PW。

### 数据准备

在配置多跳 PW 的 PWE3 Trace 测试之前，需要准备以下数据：

| 序号 | 数据         |
|----|------------|
| 1  | 本地 PW 的 ID |

| 序号 | 数据                                                       |
|----|----------------------------------------------------------|
| 2  | 对端 PW 的 ID 或 IP 地址                                       |
| 3  | PW 的类型                                                   |
| 4  | 测试可选参数（包括 Echo 报文响应模式、LSP EXP、允许的最大跳失败数、探针数目、TTL、报文超时时间） |
| 5  | 接入 CE 的接口类型和编号                                           |
| 6  | 启动方式和结束方式                                                |

## 6.30.2 配置多跳 PW 的 PWE3 Trace 测试参数

在配置多跳 PW 的 PWE3 Trace 测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type pwe3trace**，配置测试例类型为 PWE3 Trace。

**步骤 4**（可选）执行命令 **vc-type ldp**，配置 PW 隧道建立方式。

**步骤 5**（可选）执行命令 **local-pw-type { local-pw-type | ip-interworking }**，配置本端的 PW 类型。默认类型是 Ethernet。

**步骤 6**（可选）执行命令 **label-type { control-word | label-alert | normal }**，配置 PW 标签类型。

 说明

- 当 label-type 为 control-word 时，执行命令 **remote-pw-id remote-pw-id**，配置对端 PW ID。
- 当 label-type 为 label-alert 时，执行命令 **destination-address ipv4 ip-address { lsp-masklen mask-length | lsp-loopback loopback-address }\***，配置 PWE3 Trace 测试的目的地址。
- 当 label-type 为 normal 时，执行命令 **destination-address ipv4 ip-address { lsp-masklen mask-length | lsp-loopback loopback-address }\***，配置 PWE3 Trace 测试的目的地址。

**步骤 7** 执行命令 **local-pw-id local-pw-id**，配置本端 PW ID。

**步骤 8**（可选）根据需要，配置 PWE3 Trace 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **tracert-hopfailtimes times**，配置 PWE3 Trace 测试的跳失败数。



- 执行命令 **tracert-lifetime first-ttl first-ttl max-ttl max-ttl**，配置报文的初始 TTL 和最大 TTL。

**步骤 9** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

----结束

### 6.30.3 检查配置结果

在 NQA 检测多跳 PW 的 PWE3 Trace 测试后，可以查看到多跳 PW 的 PWE3 Trace 测试的结果数据。

#### 前提条件

已经完成多跳 PW 的 PWE3 Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果，并且只能显示最近 5 次的测试结果。

#### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令，在 NQA 客户端查看测试结果。

----结束

#### 任务示例

对于多跳 PW 的 PWE3 Trace 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计：



- 成功执行测试次数
- 测试的响应时间总和
- RTT 平方
- 报文最小往返时间、最大往返时间
- 目的地址
- 已收到回应的报文数目、已发送的报文数
- 至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (admin, pwe3trace) :testflag is inactive ,testtype is pwe3trace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-2-28 10:58:35.5
1 . Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 4/10/7
 Sum/Square-Sum Completion Time: 23/197
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-2-28 10:58:35.4
 Destination ip address:3.14.99.3
 Lost packet ratio: 0 %
2 . Hop 2
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 7/9/8
 Sum/Square-Sum Completion Time: 24/194
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-2-28 10:58:35.5
 Destination ip address:12.14.21.12
 Lost packet ratio: 0 %
```

## 6.31 配置多跳跨域 Kompella VLL 的 VC Trace 测试

介绍使用 NQA 进行多跳跨域 Kompella VLL 的 VC Trace 测试。

### 6.31.1 建立配置任务

在配置多跳跨域 Kompella VLL 的 VC Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.31.2 配置多跳跨域 Kompella VLL 的 VC Trace 测试参数

在配置多跳跨域 Kompella VLL 的 VC Trace 测试时，需要配置的相关参数。

### 6.31.3 检查配置结果

在 NQA 检测多跳跨域 Kompella VLL 的 VC Trace 测试后，可以查看到多跳跨域 Kompella VLL 的 VC Trace 测试的结果数据。

## 6.31.1 建立配置任务

在配置多跳跨域 Kompella VLL 的 VC Trace 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

当需要通过 NQA 对多跳跨域 Kompella VLL 的 VC 进行 Trace 测试，此时可以配置多跳跨域 Kompella VLL 的 VC Trace 测试。

## 前置任务

在配置多跳跨域 Kompella VLL 的 VC Trace 测试之前，需正确配置 Kompella 方式的 VLL。

## 数据准备

在配置多跳跨域 Kompella VLL 的 VC Trace 测试之前，需要准备以下数据：

| 序号 | 数据                                                       |
|----|----------------------------------------------------------|
| 1  | VPN 实例的名称、RD                                             |
| 2  | VPN Target 属性                                            |
| 3  | CE 接入接口的 IP 地址                                           |
| 4  | PE 的 AS 号                                                |
| 5  | ASBR 之间接口的 IP 地址                                         |
| 6  | 确定 ASBR PE 上使用的路由策略                                      |
| 7  | 测试可选参数（包括 Echo 报文响应模式、LSP EXP、允许的最大跳失败数、探针数目、TTL、报文超时时间） |
| 8  | 启动方式和结束方式                                                |

### 6.31.2 配置多跳跨域 Kompella VLL 的 VC Trace 测试参数

在配置多跳跨域 Kompella VLL 的 VC Trace 测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type pwe3trace**，配置测试例类型为 PWE3 Trace。
- 步骤 4** 执行命令 **vc-type bgp**，配置 VC 的建立方式。
- 步骤 5** 执行命令 **local-pw-id local-pw-id**，配置本端 CE-ID。
- 步骤 6** 执行命令 **remote-pw-id remote-pw-id**，配置对端 CE-ID。
- 步骤 7** 执行命令 **vpn-instance vpn-instance-name**，配置 VPN 实例。
- 步骤 8**（可选）根据需要，配置 PWE3 Trace 测试其他参数。

- 执行命令 **lsp-replymode** { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }, 配置 Echo 报文的响应模式。
- 执行命令 **lsp-exp** exp, 配置 LSP EXP 值。
- 执行命令 **tracert-hopfailtimes** times, 配置 PWE3 Trace 测试的跳失败数。
- 执行命令 **tracert-lifetime** first-ttl first-ttl max-ttl max-ttl, 配置报文的初始 TTL 和最大 TTL。

**步骤 9** 执行命令 **start**, 启动 NQA 测试。

命令 **start** 有多种形式, 根据实际需要选择其中一种启动方式:

- 执行命令 **start now** [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } } | lifetime { seconds second | hh:mm:ss } } ], 立即启动测试例。
- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

### 6.31.3 检查配置结果

在 NQA 检测多跳跨域 Kompella VLL 的 VC Trace 测试后, 可以查看到多跳跨域 Kompella VLL 的 VC Trace 测试的结果数据。

#### 前提条件

已经完成多跳跨域 Kompella VLL 的 VC Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果, 必须使用 **display nqa results** 命令查看测试结果, 并且只能显示最近 5 次的测试结果。

#### 操作步骤

**步骤 1** 执行 **display nqa results** [ test-instance admin-name test-name ] 命令, 在 NQA 客户端查看测试结果。

----结束

#### 任务示例

对于多跳跨域 Kompella VLL 的 VC Trace 测试, 如果测试成功, 执行 **display nqa results** 命令, 可以看到以下信息。

- 错误统计:
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计:

- 发送每个报文的时间戳
- 每个报文收到后的时间
- 接收每个报文的状态
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和
  - 报文最小往返时间、最大往返时间
  - 目的地址
  - 已收到回应的报文数目、已发送的报文数
  - 至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (test, pwe3trace) :testflag is inactive ,testtype is pwe3trace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2009-3-2 9:26:57.0
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 4/12/8
Sum/Square-Sum Completion Time: 25/241
RTD OverThresholds number: 0
Last Good Probe Time: 2009-3-2 9:26:56.9
Destination ip address:20.1.1.2
Lost packet ratio: 0 %
2 . Hop 2
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 10/37/20
Sum/Square-Sum Completion Time: 60/1638
RTD OverThresholds number: 0
Last Good Probe Time: 2009-3-2 9:26:57.0
Destination ip address:30.1.1.2
Lost packet ratio: 0 %
```

## 6.32 配置 NQA 测试组

当需要对多个目的地进行 ICMP、Jitter、TCP、UDP、SNMP、LSPPing、LSPJitter、ICMPJitter、PWE3Ping 等类型的测试时，可以采用 NQA 测试组的方式，将相同类型的测试例加入同一个测试组，进行统一管理。

### 6.32.1 建立配置任务

在配置 NQA 测试组前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.32.2 创建 NQA 测试组

在配置 NQA 测试组时，需要配置的相关参数。

### 6.32.3 检查配置结果

在测试组测试成功后，可以查看到测试组测试的结果数据。

## 6.32.1 建立配置任务

在配置 NQA 测试组前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

当需要对多个目的地进行 ICMP、Jitter、TCP、UDP、SNMP、LSPPing、LSPJitter、ICMPJitter、PWE3Ping 类型的测试时，可以采用 NQA 测试组的方式，将相同类型的测试例加入同一个测试组，进行统一管理。

#### 说明

vpn-instance 有些特殊,如果加入组之前组员就设置了 vpn, 那么加入组之后就按组成员的 vpn 发包。如果加入组之后组成员才设置 vpn, 那么按组长设置的 vpn 发包。

### 前置任务

在配置 NQA 测试组之前，需配置 NQA 客户端与被测设备之间路由可达。

### 数据准备

在配置 NQA 测试组之前，需要准备以下数据：

| 序号 | 数据                   |
|----|----------------------|
| 1  | NQA 测试组的管理者、测试例的测试例名 |
| 2  | 成员测试例的管理者标识、测试例名称标识  |
| 3  | （可选）测试组的组测试周期        |
| 4  | 启动方式和结束方式            |

## 6.32.2 创建 NQA 测试组

在配置 NQA 测试组时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type { icmp | jitter | tcp | udp | snmp | lsping | lspjitter | icmpjitter | pwe3ping }**，配置测试例的测试类型。
- 步骤 4** 执行命令 **switch-to group**，将当前测试例升级为测试组。

**步骤 5** 执行命令 **quit**，退回到系统视图。

**步骤 6** 执行命令 **nqa test-instance admin-name test-name**，进入已存在的 NQA 测试例的视图。

**步骤 7** 执行命令 **join group nqa admin-name test-name**，将当前 NQA 测试例加入已创建的测试组。

**步骤 8** 执行命令 **quit**，退回到系统视图。

**步骤 9** 执行命令 **nqa test-instance admin-name test-name**，进入刚才创建的测试组视图。

**步骤 10** (可选) 执行 **group-testperiod period** 命令，配置测试组的组测试周期。

缺省情况下，NQA 测试组的测试周期是 60 秒。

在指定的组测试周期内，如测试组成员过多，可能导致组测试无法正常启动。请根据测试组成员个数，选择合适的组测试周期。

**步骤 11** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.32.3 检查配置结果

在测试组测试成功后，可以查看到测试组测试的结果数据。

### 前提条件

已经完成 NQA 测试组功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果，并且只能显示最近 5 次的测试结果。

### 操作步骤

- 执行 **display nqa results [ test-instance admin-name test-name ]**命令，在 NQA 客户端查看测试结果。
- 执行 **display nqa-agent [ admin-name test-name ] [ verbose ]**命令，在 NQA 客户端查看测试状态。

----结束

### 任务示例

执行命令 **display nqa results** 不能查看 NQA 测试组的测试结果，只能查看成员测试例的测试结果。

正确创建了测试组后，执行命令 **display nqa-agent**，在输出信息中的“nqa status”字段可以看到测试组及成员测试例的归属关系。

```
<HUAWEI> display nqa-agent
NQA Tests Max:200064 128 256 NQA Tests Number: 3
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance group icmp
test-type icmp
switch-to group
nqa status : group leader, group members number : 2
nqa test-instance admin test1
test-type icmp
destination-address ipv4 10.1.1.2
join group nqa group icmp
nqa status : group member, belong to group : group icmp
nqa test-instance admin test2
test-type icmp
destination-address ipv4 10.2.1.2
join group nqa group icmp
nqa status : group member, belong to group : group icmp
```

## 6.33 配置 NQA 测试例的通用参数

介绍一些 NQA 测试常用的测试参数，并说明各个参数都可以应用到哪些测试例中。

### 6.33.1 建立配置任务

在配置 NQA 测试例的通用参数前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.33.2 配置测试例的通用参数

指明各个测试在具体测试例中的应用。

### 6.33.3 检查配置结果

在配置 NQA 测试例的通用参数成功后，可以查看到测试组测试的结果数据。

## 6.33.1 建立配置任务

在配置 NQA 测试例的通用参数前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 应用环境

除了不同测试类型的具体配置参数外，NQA 还提供测试例的通用配置项。

对于本节介绍的通用配置，通常情况下，使用缺省值即可。

### 前置任务

在配置 NQA 通用参数之前，需正确创建 NQA 测试例。

## 6.33.2 配置测试例的通用参数

指明各个测试在具体测试例中的应用。

### 背景信息

请在 NQA 客户端进行下列配置。



## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入已建立的 NQA 测试例的测试例视图。

**步骤 3** 根据需要，配置测试例通用参数。

- 执行命令 **agetime hh:mm:ss**，配置 NQA 测试例的老化时间。

- 执行命令 **alarm entry-number { lost-packet-ratio | jitter-average | jitter-ds-average | jitter-sd-average | packet-loss-ds | packet-loss-sd | rtt-average } { absolute | delta } { falling-threshold threshold-value1 event-entry1 | rising-threshold threshold-value2 event-entry2 } \* [ description ]**，配置 NQA 测试例的告警。



不能对 PathMTU、Mping、Mtrace 测试例配置此参数。

- 执行命令 **datafill fillstring**，配置 NQA 测试例的填充字符。



不能对 SNMP、TCP、FTP、PathMTU、HTTP、DNS、DHCP、LSPTrace、PWE3 Trace 和 MTrace 测试配置此参数。对 ICMPJitter、PathJitter 测试例，当 icmp-jitter-type 为 icmp-echo 时支持此配置。

- 执行命令 **datasize size**，配置 NQA 测试例的报文大小。



不能对 SNMP、TCP、FTP、ICMPJitter、PathJitter、PathMTU、HTTP、DNS、LSPTrace、DHCP、PWE3 Trace 和 MTrace 测试配置此参数。

- 执行命令 **description string**，配置测试例描述。

- 执行命令 **destination-address ipv4 ip-address**，配置 NQA 测试例的目的 IP 地址。



不能对 DNS 和 DHCP 测试配置此参数。如果 lable-type 是 normal 和 lable-alart，PWE3 Ping 和 PEW3Trace 测试例支持此参数。

- 执行命令 **destination-address url urlstring**，配置 NQA 测试例的目的 url 地址。



只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的目的 url 地址。

- 执行命令 **destination-port port-number**，配置 NQA 测试例的目的端口号。



只能对 UDP、Jitter、TCP、Trace、FTP 和 HTTP 类型的测试例，配置 NQA 测试例的目的端口号。

- 执行命令 **dns-server ipv4 ip-address**，配置 NQA 测试中 DNS 测试例的 DNS 服务器地址。



只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的 DNS 服务器地址。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。



不能对 Trace、FTP、DNS、LSPTrace、PathMTU、PWE3 Trace、MPing 和 MTrace 测试配置此参数。

- 执行命令 **frequency interval**，配置 NQA 测试例的测试周期。

- 执行命令 **ftp-filename file-name**，配置 NQA 测试 FTP 测试例的文件名和文件路径。





说明

只能对 FTP 类型的测试例，配置 NQA 测试 FTP 测试例的文件名和文件路径。

- 执行命令 **ftp-filesize** *size*，配置 NQA 测试中 FTP 测试例测试的文件大小。



说明

只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例测试的文件大小。

- 执行命令 **ftp-operation** { **get** | **put** }，配置 NQA 测试中 FTP 测试例的操作类型。



说明

只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的操作类型。

- 执行命令 **ftp-password** *password*，配置 NQA 测试中 FTP 测试例的用户密码。



说明

只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的用户密码。

- 执行命令 **ftp-username** *name*，配置 NQA 测试的 FTP 测试例使用的用户名。



说明

只能对 FTP 类型的测试例，配置 NQA 测试的 FTP 测试例使用的用户名。

- 执行命令 **http-operation** { **get** | **post** }，配置 NQA 测试 HTTP 测试例的测试类型。



说明

只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的测试类型。

- 执行命令 **http-url** *deststring* [ *verstring* ]，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。



说明

只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。

- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置 NQA 测试例的报文间隔。



说明

只能对 ICMP、UDP、SNMP、Jitter、ICMPJitter、PathJitter、LSPJitter、TCP、LSPPing、PWE3 Ping 和 MPing 类型的测试例，配置 NQA 测试例的报文间隔。

- 执行命令 **jitter-packetnum** *number*，配置 NQA 测试例的测试报文个数。



说明

可以为除 PathJitter 外的所有 jitter 类型测试，配置 NQA 测试例的测试报文个数。

- 执行命令 **local-pw-id** *local-pw-id*，配置本端的 PW ID 或者 VC ID。



说明

PWE3 Ping 和 PWE3 Trace 类型的测试例可以配置此参数。

- 执行命令 **local-pw-type** *local-pw-type*，配置本端的 PW 类型。



说明

PWE3 Ping 和 PWE3 Trace 类型的测试例可以配置此参数。对 PWE3 Trace 而言，如果隧道类型为 BGP 时，取值为 ethernet，且不可配置。

- 执行命令 **lsp-exp** *exp*，配置 NQA 测试的 LSP EXP 值。



说明

LSPPing、LSPTTrace、LSPJitter、PWE3 Ping 和 PWE3 Trace 类型的测试例可以配置此参数。

- 执行命令 **lsp-replymode** { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }，配置 NQA 测试的 LSP 报文返回方式。



说明

LSPPing、LSPTTrace、LSPJitter、PWE3 Ping 和 PWE3 Trace 类型的测试例可以配置此参数。

- 执行命令 **lsp-tetunnel** *Tunnel*，配置 NQA 测试的可指定出接口。



LSPPing、LSPTrace 和 LSPJitter 类型的测试例可以配置此参数。

- 执行命令 **mtrace-source-address** **ipv4** *ip-address*，配置 NQA mtrace 测试例的组播源地址。



MTrace 类型的测试例可以配置此参数。

- 执行命令 **mtrace-last-hop-address** **ipv4** *ip-address*，配置 nqa 测试例的最后一跳地址。



MTrace 类型的测试例可以配置此参数。

- 执行命令 **mtrace-group-address** **ipv4** *ip-address*，配置 NQA mtrace 追踪的组播组地址。



MTrace 类型的测试例可以配置此参数。

- 执行命令 **mtrace-response-address** **ipv4** *ip-address* [**ttd** *value*]，配置 NQA mtrace 的回应地址，即 IGMP-Tracert-Response 报文的目的地址。



MTrace 类型的测试例可以配置此参数。

- 执行命令 **mtrace-query-type** { **all-router** | **last-hop** | **destination** | **multicast-tree** }，配置 MTrace 的发起方式，即 IGMP-Tracert-Query 报文的发送方式。



MTrace 类型的测试例可以配置此参数。

- 执行命令 **probe-count** *number*，配置一次测试的探针数。



不能对 FTP 和 DNS 测试配置此参数。

- 执行命令 **probe-failtimes** *times*，用来配置 NQA 测试例的报文失败数，即，发送 Trap 的阈值。



不能对 PathJitter、PathMTU、MPing 和 MTrace 测试配置此参数。

- 执行命令 **records history** *number*，配置 NQA 测试的最大历史记录数目。



不能对 PathMTU、MPing 和 MTrace 测试配置此参数。

- 执行命令 **records result** *number*，配置 NQA 测试的最大测试结果记录数目。

- 执行命令 **remote-pw-id** *remote-pw-id*，配置远端的 PW ID 或者 VC ID。



只能对 PWE3 Ping 和 PWE3 Trace 测试配置此参数。

- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。



不能对 DNS、DHCP、ICMPJitter、PathJitter、PathMTU、LSPPing、LSPTrace、LSPJitter、PWE3 Ping、PWE3 Trace、MPing 和 MTrace 测试配置此参数。

- 执行命令 **set-df**，不允许对报文分片。



只能对 Trace 类型的测试例，配置不允许对报文分片。

- 执行命令 **send-trap** { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** } \* }，配置 Trap 消息的发送条件。



不能对 PathMTU、PathJitter、MPing 和 MTrace 测试配置此参数。

- 执行命令 **source-address ipv4** *ip-address*, 配置 NQA 测试例的源 IP 地址。



不能对 DNS、DHCP、PWE3 Ping、PEW3Trace 和 MPing 测试配置此参数。

- 执行命令 **source-interface** *interface-type interface-number*, 配置 NQA 测试例的源接口。



只能对 ICMP、DHCP、MPing 和 PathMTU 类型的测试例, 配置 NQA 测试例的源接口。

- 执行命令 **source-port** *port-number*, 配置本次测试的源端口号。



只能对 UDP、SNMP、TCP、ICMPJitter、PathJitter、PathMTU、LSPJitter、FTP 和 HTTP 测试配置此参数。

- 执行命令 **test-failtimes** *times*, 配置当 NQA 测试连续测试失败达到一定的次数以后, 需要向网管发送 Trap 信息。



不能对 PathJitter、PathMTU、MPing 和 MTrace 测试配置此参数。

- 执行命令 **timeout** *time*, 配置测试超时时间。
- 执行命令 **ttl** *number*, 配置 NQA 测试例报文中的 TTL 值。



不能对 DNS、PathMTU、DHCP 和 PWE3 Ping 测试配置此参数。

- 执行命令 **tos** *value*, 配置测试包的服务类型 TOS。



不能对 DNS、DHCP、LSPPing、LSPTrace、LSPJitter、PathMTU、PWE3 Ping、PWE3 Trace 和 MTrace 测试配置此参数。

- 执行命令 **tracert-hopfailtimes** *times*, 配置 NQA 测试 Trace route 测试例的跳失败数。



只能对 Trace、LSPTrace、PathJitter 和 PWE3 Trace 测试例配置此参数。

- 执行命令 **tracert-livetime** *first-ttl first-ttl max-ttl max-ttl*, 配置 NQA 测试 Trace 测试例的生存时间。



只能对 Trace、LSPTrace、PWE3 Trace、PathJitter 和 MTrace 测试例配置生存时间。

- 执行命令 **vpn-instance** *vpn-instance-name*, 配置 NQA 测试例的 VPN 实例名。



不能对 DHCP、DNS、LSPPing、LSPTrace、LSPJitter、PWE3 Ping、MPing 和 MTrace 测试配置此参数。PWE3 Trace 测试只有当 vc-type 为 BGP 时支持配置此参数。

- 执行命令 **vc-type** { *ldp* | *bgp* }, 配置建立 L2VPN VC 的协议类型。



只能对 PWE3 Ping、PWE3 Trace 测试配置此参数。PWE3 Ping 只支持 LDP。

----结束

### 6.33.3 检查配置结果

在配置 NQA 测试例的通用参数成功后，可以查看到测试组测试的结果数据。

#### 前提条件

已经完成 NQA 测试例通用参数功能的所有配置。

#### 操作步骤

- 步骤 1** 执行 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ] 查看 NQA 测试例配置的通用参数。

----结束

#### 任务示例

```
<HUAWEI> display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 2
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance a a
 test-type pwe3trace
 local-pw-id 1
 vc-type bgp
 nqa status : normal
nqa test-instance a b
 test-type icmpjitter
 destination-address ipv4 100.1.1.201
 source-address ipv4 100.1.1.200
 hardware-based enable
 ttl 100
 tos 100
 timeout 20
 nqa status : normal
```

## 6.34 配置 NQA 双向传输延迟阈值

介绍配置 NQA 双向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

### 6.34.1 建立配置任务

在配置 NQA 双向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.34.2 配置双向传输延迟阈值

配置双向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

### 6.34.3 检查配置结果

在配置 NQA 双向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

### 6.34.1 建立配置任务

在配置 NQA 双向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

配置测试例的双向传输阈值后，在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

## 前置任务

在配置 NQA 阈值之前，需完成以下任务：

- 设备运行正常
- 正确创建 NQA 测试例并配置相关参数

## 数据准备

在配置阈值功能之前，需要准备以下数据。

| 序号 | 数据                   |
|----|----------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名 |
| 2  | 测试例的双向传输延迟阈值         |

### 6.34.2 配置双向传输延迟阈值

配置双向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

## 背景信息

在运行 NQA 测试例的路由器上进行如下配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 视图。
- 步骤 3** 执行命令 **test-type { dhcp | dns | ftp | http | icmp | jitter | lspjitter | lsping | lsptrace | snmp | tcp | trace | udp | pathmtu | pwe3trace | pwe3ping | macping | mactrace | mactnlping | icmpjitter | pathjitter | mping | mtrace | vplsping | vplstrace | vplsm ping | vplsmtrace | vplspwping | vplspwtrace | gmactrace | gmactrace }**，配置测试例类型。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5** （可选）执行命令 **destination-port port-number**，配置目的端口。
- 步骤 6** 执行命令 **threshold rtd rtd-value**，配置双向传输延迟阈值。
- 步骤 7** 执行命令 **send-trap rtd**，打开阈值 Trap 开关。

----结束

### 6.34.3 检查配置结果

在配置 NQA 双向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

## 前提条件

已经完成 NQA 双向传输延迟阈值测试功能的所有配置。

## 操作步骤

**步骤 1** 执行 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ] 命令查看 NQA 测试例阈值配置。

----结束

## 任务示例

执行命令 **display nqa-agent verbose**，可以查看 NQA 阈值的配置信息。例如：

```
<HUAWEI> display nqa-agent verbose
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance admin jitter
test-type jitter
destination-address ipv4 100.1.1.201
destination-port 80
threshold rtd 2000
send-trap rtd
nqa status : normal
```

## 6.35 配置 NQA 单向传输延迟阈值

介绍配置 NQA 单向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

### 6.35.1 建立配置任务

在配置 NQA 单向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.35.2 配置单向传输延迟阈值

配置单向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

### 6.35.3 检查配置结果

在配置 NQA 单向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

## 6.35.1 建立配置任务

在配置 NQA 单向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

在进行 Jitter 测试时（除 PathJitter 和 LSPJitter 外），网络设定单向传输延迟阈值，通过对测试结果中超过阈值的测试报文统计值进行分析，使网络管理人员能够有效的监控网络的运行情况。

## 前置任务

在配置 NQA 阈值之前，需完成以下任务：

- 设备运行正常
- 正确创建 NQA 测试例并配置相关参数

## 数据准备

在配置 NQA 阈值之前，需要准备以下数据。

| 序号 | 数据                   |
|----|----------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名 |
| 2  | 测试例的阈值               |

## 6.35.2 配置单向传输延迟阈值

配置单向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

### 背景信息

在运行 NQA 测试例的路由器上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 视图。
- 步骤 3** 执行命令 **test-type { jitter | icmpjitter }**，配置测试例类型。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5**（可选）执行命令 **destination-port port-number**，配置目的端口。
- 步骤 6** 执行命令 **threshold owd-sd owd-sd-value**，配置从源到目的的传输延迟阈值。
- 步骤 7** 执行命令 **threshold owd-ds owd-ds-value**，配置从目的到源的传输延迟阈值。

----结束

## 6.35.3 检查配置结果

在配置 NQA 单向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

### 前提条件

已经完成 NQA 单向传输延迟阈值测试功能的所有配置。

### 操作步骤

- 执行 **display nqa-agent test-instance verbose** 命令查看 NQA 测试例阈值配置。

----结束



## 任务示例

执行命令 **display nqa-agent test-instance verbose**，可以查看 NQA 阈值的配置信息。例如：

```
<HUAWEI> display nqa-agent verbose
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance admin jitter
test-type jitter
destination-address ipv4 100.1.1.201
destination-port 80
send-trap probefailure
send-trap testfailure
send-trap testcomplete
send-trap rtd
send-trap owd-sd
send-trap owd-ds
threshold owd-sd 2000
threshold owd-ds 2000
nqa status : normal
```

## 6.36 配置 NQA 测试的 Trap 开关

通过配置 NQA 测试的 Trap 开关可以实现 NQA 测试成功或者失败产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

### 6.36.1 建立配置任务

在配置 NQA 测试的 Trap 开关前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.36.2 配置发送测试失败发送 Trap

在 NQA 测试报文失败失败后，发送 Trap。

### 6.36.3 配置探测失败发送 Trap

在 NQA 测试失败后，发送 Trap。

### 6.36.4 配置探测完成发送 Trap

在 NQA 测试完成后，发送 Trap。

### 6.36.5 配置超过阈值发送 Trap

在 NQA 测试结果超过阈值后，发送 Trap。

### 6.36.6 检查配置结果

在配置 NQA 测试的 Trap 开关成功后，可以在 Trapbuffer 中看到告警信息。

## 6.36.1 建立配置任务

在配置 NQA 测试的 Trap 开关前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

NQA 测试成功或者失败都会产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

NQA 支持 DISMAN-PING-MIB 中定义的 3 类 TRAP。



- 发送 NQA 探测失败 Trap:  
检查某个探针是否收到相应的响应报文。  
如果连续没有收到响应报文的次数达到指定数目，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。
- 发送 NQA 测试失败 Trap:  
检查某个测试是否失败。  
如果测试例连续测试的失败次数达到指定数目，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。
- 发送 NQA 测试成功 Trap:  
当对某个目的地址的测试成功后，发送 Trap 通知网管。  
如果收到相应的响应报文，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。

NQA 支持超过单向延迟阈值或超过双向延迟阈值向网管发送 Trap。

- 对于所有的测试例如果双向传输延迟超过设置的阈值时，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。
- 对于 Jitter 类型的测试例（不包括 LSPJitter 和 PathJitter）如果从源到目的或从目的到源，任意一个方向的传输延迟超过设置的阈值，且 Trap 使能标志为真，则根据配置的网管地址向网管发送 Trap 信息。

Trap 报文包含目的 IP 地址信息、操作状态信息、结果地址信息、最小和最大 RTT、时间总和、已发送探测数、接收到的相应报文数、RTT 平方和，以及最后一次探测成功的时间。

## 前置任务

在配置 NQA 测试的 Trap 开关之前，需完成以下任务：

- NQA 客户端与网管站之间路由可达
- 正确创建 NQA 测试例并配置相关参数

## 数据准备

在配置 NQA 测试的 Trap 开关之前，需要准备以下数据：

| 序号 | 数据                                                                                                      |
|----|---------------------------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                                    |
| 2  | 触发 Trap 发送的 NQA 事件类型                                                                                    |
| 3  | <ul style="list-style-type: none"><li>● 触发 Trap 发送的测试失败次数（可选）</li><li>● 触发 Trap 发送的探测失败次数（可选）</li></ul> |

### 6.36.2 配置发送测试失败发送 Trap

在 NQA 测试报文失败失败后，发送 Trap。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type { jitter | icmpjitter }**，配置测试例类型。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5**（可选）执行命令 **destination-port port-number**，配置目的端口。
- 步骤 6** 执行命令 **send-trap testfailure**，发送 Trap 开关。  
缺省情况下，不发送 Trap 消息。
- 步骤 7** 执行命令 **test-failtimes times**，配置发送 Trap 的测试失败次数。  
缺省情况下，测试失败一次就会发送一条 Trap 信息。
- 结束

### 6.36.3 配置探测失败发送 Trap

在 NQA 测试失败后，发送 Trap。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type { jitter | icmpjitter }**，配置测试例类型。
- 步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。
- 步骤 5**（可选）执行命令 **destination-port port-number**，配置目的端口。
- 步骤 6** 执行命令 **send-trap probefailure**，发送 Trap 开关。  
缺省情况下，不发送 Trap 消息。
- 步骤 7** 执行命令 **probe-failtimes times**，配置发送 Trap 的探测失败次数。  
缺省情况下，探测失败一次就会发送一条 Trap 信息。
- 结束

### 6.36.4 配置探测完成发送 Trap

在 NQA 测试完成后，发送 Trap。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type** { *jitter* | *icmpjitter* }，配置测试例类型。

**步骤 4** 执行命令 **destination-address** *ipv4 ip-address*，配置目的地址。

**步骤 5**（可选）执行命令 **destination-port** *port-number*，配置目的端口。

**步骤 6** 执行命令 **send-trap testcomplete**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

## 6.36.5 配置超过阈值发送 Trap

在 NQA 测试结果超过阈值后，发送 Trap。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type** { *jitter* | *icmpjitter* }，配置测试例类型。

**步骤 4** 执行命令 **destination-address** *ipv4 ip-address*，配置目的地址。

**步骤 5**（可选）执行命令 **destination-port** *port-number*，配置目的端口。

**步骤 6** 执行命令 **send-trap** { *owd-ds* | *owd-sd* }\*，打开超过阈值发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

## 6.36.6 检查配置结果

在配置 NQA 测试的 Trap 开关成功后，可以在 Trapbuffer 中看到告警信息。

### 前提条件

已经完成 NQA 测试 Trap 开关测试功能的所有配置。

### 操作步骤

**步骤 1** 执行命令 **display trapbuffer** [ *size value* ] 查看 NQA 测试例发送的 Trap。

----结束

## 任务示例

执行命令 **display trapbuffer [ size value ]**，查看产生的告警信息。

例如：

```
<HUAWEI> display trapbuffer size 2
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 11
#May 6 2009 12:54:17 CBB6-PE3 SINDEX/4/INDEXMAP:OID 1.3.6.1.4.1.2011.5.25.110.2.0.1
ShortIFIndexMapTable changed.
#May 6 2009 11:02:37 CBB6-PE3 SRM_BASE/4/ENTITYREGSUCCESS: OID 1.3.6.1.4.1.2011.5.25.129.2.1.18
Physical entity register succeeded.
(EntityPhysicalIndex=17367040, BaseTrapSeverity=2, BaseTrapProbableCause=70144,
BaseTrapEventType=5, EntPhysicalContainedIn=1677721
6, EntPhysicalName="SRU slot 9", RelativeResource="", ReasonDescription="MPU9")
```

## 6.37 配置测试结果发送到 FTP 服务器

网管需要了解到设备的测试结果，如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

### 6.37.1 建立配置任务

在配置测试结果发送到 FTP 服务器前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.37.2 配置连接 FTP 服务器需要的参数

指定接收测试结果的 FTP 服务器地址和登录 FTP 服务器需要的用户名、密码。

### 6.37.3 使能通过 FTP 保存 NQA 测试结果功能

只有使能了 FTP 保存 NQA 测试结果功能后，才能向 FTP 服务器发送测试结果。

### 6.37.4 （可选）配置通过 FTP 保存测试结果的条数

配置保存在 FTP 服务器文件中的测试结果条目数。

### 6.37.5 （可选）配置通过 FTP 保存的测试结果的时间

系统每次能够发送两个测试结果到服务器端，如果 FTP 服务器端不支持文件续写的功能，每次发送的测试结果都将在 FTP 服务器端创建一个新的文件。

### 6.37.6 （可选）配置 FTP 传送成功向网管端发送 Trap

通过 FTP 保存测试结果成功后，向网管发送 Trap 通知网管测试文件已经保存成功。

### 6.37.7 启动测试例

启动测试例，测试结果会定时记录到文件中。

### 6.37.8 检查配置结果

在配置测试结果发送到 FTP 服务器成功后，可以查看到保存 NQA 测试结果的配置信息。

## 6.37.1 建立配置任务

在配置测试结果发送到 FTP 服务器前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

系统默认可以保存最近测试的 5 条测试结果，新产生的测试结果会覆盖最早的测试结果。如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果，把达到最大条数的测试结果发送统计结果到 FTP 服务器或定时发送统计结果到 FTP 服务器，可以有效避免测试结果丢失，便于网络管理者分析不同时间的测试结果，来综合考虑对网络的管理。

## 前置任务

在配置测试结果发送到 FTP 服务器之前，需要完成以下任务：

- 配置 FTP 服务器
- 配置 NQA 客户端与网管端路由可达。
- 配置测试例

## 数据准备

在配置测试结果发送到 FTP 服务器之前，需要准备以下数据：

| 序号 | 数据                  |
|----|---------------------|
| 1  | FTP 服务器地址           |
| 2  | 登录 FTP 服务器所需的用户名及密码 |
| 3  | 通过 FTP 保存测试结果的条数    |
| 4  | 通过 FTP 保存测试结果的时间    |

### 6.37.2 配置连接 FTP 服务器需要的参数

指定接收测试结果的 FTP 服务器地址和登录 FTP 服务器需要的用户名、密码。

## 背景信息

在 NQA 客户端上进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa-ftp-record ip-address ip-address** 或 **nqa-ftp-record vpn-instance vpn-instance**，配置 FTP 服务器地址。
- 步骤 3** 执行命令 **nqa-ftp-record username username**，配置 FTP 的用户名。
- 步骤 4** 执行命令 **nqa-ftp-record password password**，配置 FTP 的密码。
- 步骤 5** 执行命令 **nqa-ftp-record filename filename**，配置保存的文件名。

----结束

### 6.37.3 使能通过 FTP 保存 NQA 测试结果功能

只有使能了 FTP 保存 NQA 测试结果功能后，才能向 FTP 服务器发送测试结果。

#### 背景信息

在 NQA 客户端上进行下列配置。

#### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa-ftp-record enable**，使能 FTP 保存测试结果。
- 结束

### 6.37.4 （可选）配置通过 FTP 保存测试结果的条数

配置保存在 FTP 服务器文件中的测试结果条目数。

#### 背景信息

在 NQA 客户端上进行下列配置。

#### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa-ftp-record item-num item-number**，配置保存 FTP 测试结果到文件的条数。
- 结束

### 6.37.5 （可选）配置通过 FTP 保存的测试结果的时间

系统每次能够发送两个测试结果到服务器端，如果 FTP 服务器端不支持文件续写的功能，每次发送的测试结果都将在 FTP 服务器端创建一个新的文件。

#### 背景信息

在 NQA 客户端上进行下列配置。

#### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa-ftp-record time time**，配置保存 FTP 测试结果到文件的时间。
- 结束

### 6.37.6 （可选）配置 FTP 传送成功向网管端发送 Trap

通过 FTP 保存测试结果成功后，向网管发送 Trap 通知网管测试文件已经保存成功。

## 背景信息

在 NQA 客户端上进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa-ftp-record trap-enable**，配置 FTP 传送成功向网管端发送 Trap。

第一次发送成功后，不会触发告警，从第二次开始，每次发送成功都会触发告警。

----结束

## 6.37.7 启动测试例

启动测试例，测试结果会定时记录到文件中。

## 背景信息

在 NQA 客户端上进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 视图。

**步骤 3** 执行命令 **test-type** { dhcp | dns | ftp | http | icmp | jitter | lspjitter | lsping | lsptrace | snmp | tcp | trace | udp | pathmtu | pwe3trace | pwe3ping | macping | mactrace | mactnlping | icmpjitter | pathjitter | mping | mtrace | vplsping | vplstrace | vplsmpping | vplsmtrace | vplspwping | vplspwtrace | gmacping | gmactrace }，配置测试例类型。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**，配置目的地址。

**步骤 5**（可选）执行命令 **destination-port port-number**，配置目的端口。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { seconds second | hh:mm:ss } | **lifetime** { seconds second | hh:mm:ss } } ]，立即启动测试例。
- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { seconds second | hh:mm:ss } | **lifetime** { seconds second | hh:mm:ss } } ]，在指定时刻启动测试例。
- 执行命令 **start delay** { seconds second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { seconds second | hh:mm:ss } | **lifetime** { seconds second | hh:mm:ss } } ]，延迟指定时间后启动测试例。

----结束

## 6.37.8 检查配置结果

在配置测试结果发送到 FTP 服务器成功后，可以查看到保存 NQA 测试结果的配置信息。

## 前提条件

完成测试结果发送到 FTP 服务器的所有配置。

## 操作步骤

**步骤 1** 使用命令 **display nqa-ftp-record configuration**，查看保存 NQA 测试结果的配置信息。

----结束

## 任务示例

执行命令 **display nqa-ftp-record configuration**，可以查看到保存 NQA 测试结果的配置信息。

```
<HUAWEI> display nqa-ftp-record configuration
-----NQA FTP SAVE RECORD CONFIGURATION-----
FUNCTION: ENABLE TRAP: DISABLE
IP-ADDRESS:11.1.1.8
VPN-INSTANCE:
USERNAME:wang
PASSWORD:123
FILENAME:icmp
ITEM-NUM:10010
TIME:2
LAST FINISHED FILENAME:icmp20080605-150350.txt
```

## 6.38 配置上下限 NQA 阈值告警

在 NQA 的测试结果超出阈值时，向网管发送告警信息，通知设备出现的变化情况。

### 6.38.1 建立配置任务

在配置上下限 NQA 阈值告警前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.38.2 配置阈值告警相关事件

配置超过阈值时，系统需要采取的动作，可以记录日志、产生告警或者即可以记录日志也可以产生告警。

### 6.38.3 配置阈值告警

配置测试结果在超过阈值时产生触发相应的事件。

### 6.38.4 启动测试例

启动测试例，在出现超过阈值时，采取和事件对应的动作。

### 6.38.5 检查配置结果

在配置上下限 NQA 阈值告警成功后，可以查看到上下限 NQA 阈值告警的配置情况。

## 6.38.1 建立配置任务

在配置上下限 NQA 阈值告警前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

用户可以通过配置告警阈值的方式来对网络进行监控。在配置监控条件后，当测试的结果中的监控项超出了用户的设定的上限或下限阈值时，设备通过告警方式通知网管站，告知网络出现的情况，便于用户对网络实时的运行情况进行监控。



## 前置任务

在配置 NQA 阈值告警功能前，需要完成以下任务：

- 配置测试例

## 数据准备

在配置 NQA 告警阈值之前，需要准备以下数据：

| 序号 | 数据       |
|----|----------|
| 1  | 阈值相关的事件号 |
| 2  | 阈值告警号    |
| 3  | 上限阈值     |
| 4  | 下限阈值     |

### 6.38.2 配置阈值告警相关事件

配置超过阈值时，系统需要采取的动作，可以记录日志、产生告警或者即可以记录日志也可以产生告警。

#### 背景信息

在 NQA 客户端上进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa event event-entry { linkage admin-name test-name | log | trap | log-trap | none } [description ]**，配置事件号及相关联的事件。

----结束

### 6.38.3 配置阈值告警

配置测试结果在超过阈值时产生触发相应的事件。

#### 背景信息

在 NQA 客户端上进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入测试例视图。

**步骤 3** 执行命令 **test-type { dhcp | dns | ftp | http | icmp | jitter | lspjitter | lsping | lsptrace | snmp | tcp | trace | udp | pathmtu | pwe3trace | pwe3ping | macping | mactrace |**

**mactnlping | icmpjitter | pathjitter | mping | mtrace | vplsping | vplstrace | vplsm ping | vplsmtrace | vplspwping | vplspwtrace | gmacping | gmactrace** }, 配置测试例类型。

**步骤 4** 执行命令 **destination-address ipv4 ip-address**, 配置目的地址。

**步骤 5** (可选) 执行命令 **destination-port port-number**, 配置目的端口。

**步骤 6** 执行命令 **alarm entry-number { lost-packet-ratio | jitter-average | jitter-ds-average | jitter-sd-average | packet-loss-ds | packet-loss-sd | rtt-average } { absolute | delta } { falling-threshold threshold-value1 event-entry1 | rising-threshold threshold-value2 event-entry2 } \*** [ description description ], 配置告警号及阈值。

 说明

目前只支持绝对统计, 不支持相对统计。

----结束

## 6.38.4 启动测试例

启动测试例, 在出现超过阈值时, 采取和事件对应的动作。

### 操作步骤

**步骤 1** 执行命令 **system-view**, 进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**, 进入 NQA 视图。

**步骤 3** 执行命令 **start**, 启动 NQA 测试。

命令 **start** 有多种形式, 根据实际需要选择其中一种启动方式:

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**, 立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**, 在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**, 延迟指定时间后启动测试例。

----结束

## 6.38.5 检查配置结果

在配置上下限 NQA 阈值告警成功后, 可以查看到上下限 NQA 阈值告警的配置情况。

### 前提条件

完成上下限 NQA 阈值告警的所有配置。

### 操作步骤

- 使用命令 **display nqa event**, 查看配置的最大事件数量和已经配置的事件数量。
- 在 NQA 视图下, 使用命令 **display nqa alarm**, 查看配置的最大告警数量和已经配置的告警数。

- 使用命令 **display nqa-agent** [ *admin-name test-name* ] [ **verbose** ]，查看 NQA 客户端配置的测试例状态信息。。

----结束

## 任务示例

执行命令 **display nqa event**，可以查看到可配置的最大事件数量和已经配置的事件数量。

```
<HUAWEI> display nqa-event
NQA event information:
```

```

NQA Event Max: 5 NQA Event Number: 1

```

执行命令 **display nqa alarm**，可以查看到可配置的最大告警数量和已经配置的告警数。

```
[HUAWEI-nqa-admin-icmp] display nqa alarm
NQA alarm information:
```

```

NQA Alarm Max: 5 NQA Alarm Number: 2

```

执行命令 **display nqa-agent**，可以查看到 NQA 客户端配置的测试例状态信息。

```
<HUAWEI> display nqa agent
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000
nqa test-instance admin icmp
test-type icmp
destination-address ipv4 11.1.1.32
frequency 5
alarm 10 rtt-average 2 rising-threshold 200 10 falling-threshold 0 10
alarm 20 lost-packet-ratio 2 rising-threshold 10 10 falling-threshold 1 10
nqa status : normal
```

## 6.39 配置 VPLS 组播 Ping 检测 VPLS 网络测试

介绍使用 NQA 进行 Martini 方式的 VPLS 网络测试，了解网络的连通情况。

### 6.39.1 建立配置任务

在配置 Martini 方式的 VPLS 网络测试前了解它的应用环境、配置此特性的前置任务和  
数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.39.2 配置 VPLS 组播 Trace 检测组播转发

在配置 Martini 方式的 VPLS 网络测试时，需要配置的相关参数。

### 6.39.3 检查配置结果

在 Martini 方式的 VPLS 网络测试后，可以查看网络的连通情况数据。

## 6.39.1 建立配置任务

在配置 Martini 方式的 VPLS 网络测试前了解它的应用环境、配置此特性的前置任务和  
数据准备，可以帮助用户快速、准确地完成配置任务。

## 应用环境

VPLS 组播 Trace 可用于检查 VPLS 网络 PE 的 IGMP Snooping 功能是否正常及故障点所  
处位置。

## 前置任务

在配置 VPLS 组播 Ping 检测 Martini VPLS 网络测试之前，需完成以下任务：

- 配置 Martini VPLS 网络。
- 使能 VSI 域内设备的 IGMP Snooping。

## 数据准备

在配置 VPLS 组播 Ping 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                     |
|----|----------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                   |
| 2  | VSI 实例的名称                                                                              |
| 3  | (可选)：组播源地址、填充字符、发送回显请求报文的载荷长度、等待回显请求报文响应的超时时间、发送下一个回显请求报文的等待时间、回复模式、发送回显请求报文的优先级、失败百分比 |
| 4  | 组播 IP 地址                                                                               |
| 5  | 启动方式和结束方式                                                                              |

## 6.39.2 配置 VPLS 组播 Trace 检测组播转发

在配置 Martini 方式的 VPLS 网络测试时，需要配置的相关参数。

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type vplsmtrace**，配置测试例类型为 VPLS mTrace。

缺省情况下，NQA 的测试类型为 ICMP。

**步骤 4** 执行命令 **vsi vsiname**，配置测试例对应的 VSI 的名称。

**步骤 5** 执行命令 **destination-address ipv4 ip-address**，配置 VPLS mPing 测试的目的地址。

**步骤 6** (可选) 根据需要，配置 VPLS mPing 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。



lsp-replymode no-replay 进行单向测试，无论测试是否成功在测试结果的显示信息中都会显示测试失败。只是在测试成功时在测试结果的显示信息中，会显示测试报文超时的数量；在测试失败时在测试结果的显示信息中，会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。
- 执行命令 **datasize size**，配置测试报文的大小。



配置 **datasize** 大小加上报文头后的值不能超过接口 MTU 值，否则会导致测试失败。

- 执行命令 **ttl number**，配置 TTL 值。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值
- 执行命令 **datafill fillstring**，配置填充字符。
- 执行命令 **interval seconds interval**，配置测试报文的发送间隔。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

#### 步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.39.3 检查配置结果

在 Martini 方式的 VPLS 网络测试后，可以查看网络的连通情况数据。

### 前提条件

已经完成 VPLS 组播 Trace 测试功能的所有配置。



NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

**步骤 1** 执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

### 任务示例

对于 VPLS 组播 Trace 测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry (admin, vplsmping) :testflag is inactive ,testtype is vplsmping
```

```
1 . Test 1 result The test is finished
Completions: success Timeouts number: 0
Drops number: 0 TargetAddress: 225.1.1.1
ProbeResponses number: 6 SentProbes number: 3
Busies: 0 SequenceError number: 0
Lost packet ratio: 0%
1 . Receiver 1
CompletionTime Min/Max/Sum/Avg: 15/26/59/19
Sum2CompletionTime: 1225
LastGoodProbe time: 2009-4-23 11:48:9.4
RecevierAddress: 2.2.2.2
Fib hit: Hit
```

## 6.40 配置 VPLS 组播 Ping 检测 Kompella VPLS 网络测试

介绍使用 NQA 进行 Kompella 方式的 VPLS 网络测试，了解网络的连通情况。

### 6.40.1 建立配置任务

在配置 Kompella 方式的 VPLS 网络测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

### 6.40.2 配置 VPLS 组播 Ping 检测组播转发

在配置 Kompella 方式的 VPLS 网络测试时，需要配置的相关参数。

### 6.40.3 检查配置结果

在 Kompella 方式的 VPLS 网络测试后，可以查看网络的连通情况数据。

### 6.40.1 建立配置任务

在配置 Kompella 方式的 VPLS 网络测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

#### 应用环境

NQA 的 VPLS 组播 Ping 检测 Kompella VPLS 网络，可以实现收集 Kompella VPLS 网络中同一个 VSI 内的 PE 列表。

#### 前置任务

在配置 VPLS 组播 Ping 检测 Kompella VPLS 组网测试之前，需完成以下任务：

- 配置 Kompella VPLS 网络。

#### 数据准备

在配置 VPLS mPing 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                     |
|----|----------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                   |
| 2  | VSI 实例的名称                                                                              |
| 3  | （可选）：组播源地址、填充字符、发送回显请求报文的载荷长度、等待回显请求报文响应的超时时间、发送下一个回显请求报文的等待时间、回复模式、发送回显请求报文的优先级、失败百分比 |

| 序号 | 数据        |
|----|-----------|
| 4  | 组播 IP 地址  |
| 5  | 启动方式和结束方式 |

## 6.40.2 配置 VPLS 组播 Ping 检测组播转发

在配置 Kompella 方式的 VPLS 网络测试时，需要配置的相关参数。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type vplsm ping**，配置测试例类型为 VPLS mPing。

缺省情况下，NQA 的测试类型为 ICMP。

**步骤 4** 执行命令 **vsi vsi-name**，配置测试例对应的 VSI 的名称。

**步骤 5** 执行命令 **destination-address ipv4 ip-address**，配置 VPLS mPing 测试的目的地址。

**步骤 6**（可选）根据需要，配置 VPLS mPing 测试其他参数。

- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。

 说明

lsp-replymode no-reply 进行单向测试，无论测试是否成功在测试结果的显示信息中都会显示测试失败。只是在测试成功时在测试结果的显示信息中，会显示测试报文超时的数量；在测试失败时在测试结果的显示信息中，会显示测试报文丢弃的数量。

- 执行命令 **source-address ipv4 ip-address**，配置源地址。

- 执行命令 **datasize size**，配置测试报文的大小。

 说明

配置 datasize 大小加上报文头后的值不能超过接口 MTU 值，否则会导致测试失败。

- 执行命令 **tll number**，配置 TTL 值。

- 执行命令 **lsp-exp exp**，配置 LSP EXP 值

- 执行命令 **datafill fillstring**，配置填充字符。

- 执行命令 **interval { milliseconds interval | seconds interval }**，配置测试报文的发送间隔。

- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：



- 执行命令 **start now** [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 立即启动测试例。
- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

### 6.40.3 检查配置结果

在 Kompella 方式的 VPLS 网络测试后，可以查看网络的连通情况数据。

#### 前提条件

已经完成 VPLS 组播 Ping 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

#### 操作步骤

**步骤 1** 执行 **display nqa results** [ **test-instance** admin-name test-name ] 命令查看测试结果。

----结束

#### 任务示例

对于 VPLS 组播 Ping 下载测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和
  - 报文最小往返时间、最大往返时间
  - 目的地址
  - 已收到回应的报文数目、已发送的报文数

<HUAWEI> **display nqa results**

NQA entry (admin, vplsm ping) : testflag is inactive , testtype is vplsm ping



```
1 . Test 1 result The test is finished
 Completions: success Timeouts number: 0
 Drops number: 0 TargetAddress: 224.0.0.5
 ProbeResponses number: 6 SentProbes number: 3
 Busies: 0 SequenceError number: 0
 Lost packet ratio: 0%
1 . Receiver 1
 CompletionTime Min/Max/Sum/Avg: 15/26/59/19
 Sum2CompletionTime: 1225
 LastGoodProbe time: 2009-4-23 11:48:9.4
 RecevierAddress: 2.2.2.2
 Fib hit: Hit
```

## 6.41 配置 MAC Trace 测试

MAC Trace 测试支持对 VLAN 和 VPLS 网络的检测。

### 6.41.1 建立配置任务

NQA MAC Trace 测试用于检测两个 MEP（Maintenance association End Point，维护终结点）之间的网络连通性。

### 6.41.2 配置 MAC Trace 测试参数

在配置 MAC Trace 测试时，需要配置的相关参数。

### 6.41.3 检查配置结果

在 MAC Trace 测试成功后，可以查看到 MAC Trace 测试的结果数据。

### 6.41.1 建立配置任务

NQA MAC Trace 测试用于检测两个 MEP（Maintenance association End Point，维护终结点）之间的网络连通性。

## 应用环境

NQA 的 MAC Trace 测试提供类似于普通 Traceroute 命令的功能，支持对 VLAN 网络和 VPLS 网络的连通性检测，但输出信息更为丰富。对 VLAN 网络检测时，VLAN 网络中各设备需要使能以太网 CFM 的基本功能；对 VPLS 网络检测时，PE 上需要部署基于 VPLS 的以太网 CFM。

## 前置任务

在配置 MAC Trace 测试之前：

- 对于 VLAN 网络：需要正确配置 VLAN 并使能以太网 CFM 基本功能
- 对于 VPLS 网络：需正确配置 VPLS 网络，确保 VSI 状态 Up 并在 PE 上使能以太网 CFM 基本功能

## 数据准备

在配置 MAC Trace 测试之前，需要准备以下数据：

| 序号 | 数据                              |
|----|---------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名            |
| 2  | MD 名称、MA 名称、本端 MEP ID、目的 MAC 地址 |

| 序号 | 数据        |
|----|-----------|
| 3  | 启动方式和结束方式 |

## 6.41.2 配置 MAC Trace 测试参数

在配置 MAC Trace 测试时，需要配置的相关参数。

### 背景信息

请在需要发起 NQA MAC Trace 测试的 NQA 客户端进行下列配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type mactrace**，配置测试例类型为 mactrace。
- 步骤 4** 执行命令 **destination-address mac mac-address**，配置 mactrace 测试的目的 MAC 地址。
- 步骤 5** 执行命令 **md md-name ma ma-name**，指定发出 NQA 测试报文的 MD 和 MA。
- 步骤 6** 执行命令 **mep mep-id mep-id**，配置本端 MEP ID。
- 步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

----结束

## 6.41.3 检查配置结果

在 MAC Trace 测试成功后，可以查看到 MAC Trace 测试的结果数据。

### 前提条件

已经完成 MAC Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 执行 **display nqa results** [ *test-instance admin-name test-name* ] 命令查看测试结果。

----结束

## 任务示例

对于 mactrace 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到每一跳的统计信息。

```
<HUAWEI> display nqa results
NQA entry (mac, trace) :testflag is inactive ,testtype is mactrace
1. Test 1 result The test is finished
 Completion:success Attempts number:1
 Drop operation number:0 Operation timeout number:0
 System busy operation number:0
 Last good path Time:2000-01-05 02:35:35.0
```

## 6.42 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性

使用 NQA GMAC Ping 和 GMAC Trace 功能测试 VLAN 连通性，除了可以检测网络连通性和定位故障外，还可以获得时延等信息。

### 6.42.1 建立配置任务

GMAC（通用 MAC）Ping 和 GMAC Trace 测试可以检测 VLAN 网络中任意两台设备之间的连通状况、丢包时延等信息。

### 6.42.2 配置 GMAC Ping 测试参数

配置 GMAC Ping 测试 VLAN 前，需要正确配置 VLAN。

### 6.42.3 配置 GMAC Trace 测试参数

配置 GMAC Trace 测试 VLAN 前，需要正确配置 VLAN。

### 6.42.4 检查配置结果

## 6.42.1 建立配置任务

GMAC（通用 MAC）Ping 和 GMAC Trace 测试可以检测 VLAN 网络中任意两台设备之间的连通状况、丢包时延等信息。

## 应用环境

在未配置 MD、MA、MEP 的 VLAN 网络中，GMAC Ping 和 GMAC Trace 可以检测任意两台设备之间的连通状况、丢包时延等信息。GMAC Ping 和 GMAC Trace 通过在发起端指定目的 MAC 的请求报文，并解析应答报文的方式检测链路的连通性和定位故障。与 MAC Ping 和 Trace 相比，GMAC Ping 和 GMAC Trace 无需配置 MD、MA、MEP 参数。

## 前置任务

在配置 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性之前，需正确配置 VLAN 网络，并且：

- 对 GMAC Ping：发起端和接收端全局使能 GMAC Ping

- 对 GMAC Trace：发起端和接收端全局使能 GMAC Trace

## 数据准备

在配置 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性之前，需要准备以下数据：

| 序号 | 数据               |
|----|------------------|
| 1  | VLAN ID          |
| 2  | 目的 MAC 地址        |
| 3  | NQA 测试的启动方式和结束方式 |

## 6.42.2 配置 GMAC Ping 测试参数

配置 GMAC Ping 测试 VLAN 前，需要正确配置 VLAN。

## 背景信息

请在需要发起 NQA GMAC Ping 测试的 NQA 客户端进行下列配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type gmacping**，配置测试例类型为 GMAC Ping。

**步骤 4** 执行命令 **destination-address mac mac-address**，配置目的 MAC 地址。该 MAC 地址可以是桥 MAC 地址或接口 MAC 地址。

**步骤 5** 执行命令 **vlan vlan-id**，配置需要检测的 VLAN 的 VLAN ID。

 说明

更多可选参数，可以在配置了 NQA 测试例类型后，进入测试例视图，执行命令 **display nqa-parameter** 进行查看。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

### 6.42.3 配置 GMAC Trace 测试参数

配置 GMAC Trace 测试 VLAN 前，需要正确配置 VLAN。

#### 背景信息

请在需要发起 NQA GMAC Trace 测试的 NQA 客户端进行下列配置。

#### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type gmactrace**，配置测试例类型为 GMAC Trace。

**步骤 4** 执行命令 **destination-address mac mac-address**，配置目的 MAC 地址。该 MAC 地址可以是桥 MAC 地址或接口 MAC 地址。

**步骤 5** 执行命令 **vlan vlan-id**，配置需要检测的 VLAN 的 VLAN ID。

 说明

更多可选参数，可以在配置了 NQA 测试例类型后，进入测试例视图，执行命令 **display nqa-parameter** 进行查看。

**步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

### 6.42.4 检查配置结果

#### 前提条件

已经完成 GMAC Ping 和 GMAC Trace 测试 VLAN 连通性功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 在 NQA 客户端执行 **display nqa results** [ *test-instance admin-name test-name* ]命令查看测试结果。

----结束

## 任务示例

对于 GMAC Ping VLAN 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance gmacping
NQA entry(gmac,ping) :testflag is inactive ,testtype is gmacping
1. Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:succcess RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
 NumOfRTT:3 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:10 Min Positive DS:40
 Max Positive SD:10 Max Positive DS:40
 Positive SD Number:1 Positive DS Number:1
 Positive SD Sum:10 Positive DS Sum:40
 Positive SD Square Sum:100 Positive DS Square Sum:1600
 Min Negative SD:20 Min Negative DS:30
 Max Negative SD:20 Max Negative DS:30
 Negative SD Number:1 Negative DS Number:1
 Negative SD Sum:20 Negative DS Sum:30
 Negative SD Square Sum:400 Negative DS Square Sum:900
 Min Delay SD:0 Min Delay DS:0
 Max Delay SD:0 Max Delay DS:0
 Delay SD Square Sum:0 Delay DS Square Sum:0
 Packet Loss SD:0 Packet Loss DS:0
 Packet Loss Unknown:0 Average of Jitter:25
 Average of Jitter SD:15 Average of Jitter DS:35
 jitter out value:0.6119792 jitter in value:1.4062500
 NumberOfFOWD:0 Packet Loss Ratio: 0%
 OWD SD Sum:0 OWD DS Sum:0
 ICPIF value: 0 MOS-CQ value: 0
 TimeStamp unit: ms Packet Rewrite Number: 0
 Packet Rewrite Ratio: 0% Packet Disorder Number: 0
 Packet Disorder Ratio: 0% Fragment-disorder Number: 0
 Fragment-disorder Ratio: 0%
```

对于 GMAC Trace VLAN 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance gmactrace
NQA entry(gmac,trace) :testflag is inactive ,testtype is gmactrace
1. Test 1 result The test is finished
 Completion:succcess Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2010-07-23 14:23:20.4
1. Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 70/140/93
 Sum/Square-Sum Completion Time: 280/29400
 RTD OverThresholds number: 0
 Last Good Probe Time: 2010-07-23 14:23:20.4
 Destination ip address:3.3.3.3
 Lost packet ratio: 0 %
```

## 6.43 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性

使用 NQA GMAC Ping 和 GMAC Trace 功能测试 VPLS 连通性，除了可以检测网络连通性和定位故障外，还可以获得时延等信息。

### 6.43.1 建立配置任务

GMAC Ping 和 GMAC Trace 用于检测 VPLS 网络连通性，支持从 PE 和 CE 设备上发起和接收检测。

### 6.43.2 配置 GMAC Ping 测试参数

配置 GMAC Ping 测试例前，需要确保 VSI Up。

### 6.43.3 配置 GMAC Trace 测试参数

配置 GMAC Trace 测试例前，需要确保 VSI Up。

### 6.43.4 检查配置结果

## 6.43.1 建立配置任务

GMAC Ping 和 GMAC Trace 用于检测 VPLS 网络连通性，支持从 PE 和 CE 设备上发起和接收检测。

### 应用环境

NQA GMAC Ping 和 GMAC Trace 测试检测 VPLS 网络的连通性、丢包时延等信息，支持 PE 和 PE 之间、PE 和 CE 之间以及 CE 和 CE 之间的检测。与 MAC Ping 和 Trace 相比，GMAC Ping 和 GMAC Trace 无需配置 MD、MA、MEP 参数。

### 前置任务

在配置配置 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性之前，需正确配置 VPLS 网络，确保 VSI 状态 Up，并且：

- 对 GMAC Ping：发起端和接收端全局使能 GMAC Ping
- 对 GMAC Trace：发起端和接收端全局使能 GMAC Trace

### 数据准备

在配置 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性之前，需要准备以下数据：

| 序号 | 数据               |
|----|------------------|
| 1  | VSI 名称           |
| 2  | 目的 MAC 地址        |
| 3  | NQA 测试的启动方式和结束方式 |

## 6.43.2 配置 GMAC Ping 测试参数

配置 GMAC Ping 测试例前，需要确保 VSI Up。



## 背景信息

请在需要发起 NQA GMAC Ping 测试的 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type gmacping**，配置测试例类型为 GMAC Ping。
- 步骤 4** 执行命令 **destination-address mac mac-address**，配置目的 MAC 地址。MAC 地址可以是桥 MAC 地址或接口 MAC 地址。
- 步骤 5** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。
- 步骤 6** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

### 6.43.3 配置 GMAC Trace 测试参数

配置 GMAC Trace 测试例前，需要确保 VSI Up。

## 背景信息

请在需要发起 NQA GMAC Trace 测试的 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type gmactrace**，配置测试例类型为 GMAC Trace。
- 步骤 4** 执行命令 **destination-address mac mac-address**，配置目的 MAC 地址。MAC 地址可以是桥 MAC 地址或接口 MAC 地址。
- 步骤 5** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。



#### 步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

### 6.43.4 检查配置结果

#### 前提条件

已经完成 GMAC Ping 和 GMAC Trace 测试 VPLS 连通性功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

#### 操作步骤

- 步骤 1** 在 NQA 客户端执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

#### 任务示例

对于 VPLS GMAC Ping 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance gmacping
NQA entry(gmac,ping) :testflag is inactive ,testtype is gmacping
1. Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:success RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
 NumOfRTT:3 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:10 Min Positive DS:40
 Max Positive SD:10 Max Positive DS:40
 Positive SD Number:1 Positive DS Number:1
 Positive SD Sum:10 Positive DS Sum:40
 Positive SD Square Sum:100 Positive DS Square Sum:1600
 Min Negative SD:20 Min Negative DS:30
 Max Negative SD:20 Max Negative DS:30
 Negative SD Number:1 Negative DS Number:1
 Negative SD Sum:20 Negative DS Sum:30
 Negative SD Square Sum:400 Negative DS Square Sum:900
```

|                             |                             |
|-----------------------------|-----------------------------|
| Min Delay SD:0              | Min Delay DS:0              |
| Max Delay SD:0              | Max Delay DS:0              |
| Delay SD Square Sum:0       | Delay DS Square Sum:0       |
| Packet Loss SD:0            | Packet Loss DS:0            |
| Packet Loss Unknown:0       | Average of Jitter:25        |
| Average of Jitter SD:15     | Average of Jitter DS:35     |
| jitter out value:0.6119792  | jitter in value:1.4062500   |
| NumberOfOWD:0               | Packet Loss Ratio: 0%       |
| OWD SD Sum:0                | OWD DS Sum:0                |
| ICPIF value: 0              | MOS-CQ value: 0             |
| TimeStamp unit: ms          | Packet Rewrite Number: 0    |
| Packet Rewrite Ratio: 0%    | Packet Disorder Number: 0   |
| Packet Disorder Ratio: 0%   | Fragment-disorder Number: 0 |
| Fragment-disorder Ratio: 0% |                             |

对于 VPLS GMAC Trace 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance gmactrace
NQA entry(gmac,trace) :testflag is inactive ,testtype is gmactrace
1 . Test 1 result The test is finished
Completion:succcess Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %
```

## 6.44 配置 VPLS PW Ping 和 PW Trace 测试

### 6.44.1 建立配置任务

VPLS PW Ping 和 PW Trace 用于检测 VPLS PW 的连通性和定位 PW 故障。

### 6.44.2 配置 VPLS PW Ping 测试参数

配置 VPLS PW Ping 测试例前，需要确保 VSI Up。

### 6.44.3 配置 VPLS PW Trace 测试参数

配置 VPLS PW Trace 测试例前，需要确保 VSI Up。

### 6.44.4 检查配置结果

## 6.44.1 建立配置任务

VPLS PW Ping 和 PW Trace 用于检测 VPLS PW 的连通性和定位 PW 故障。

## 应用环境

VPLS 作为搭建电信城域网的技术主体，已经在全球很多地方获得了规模性应用。但在对业务的可管理性方面，现有的 VPLS 对业务进行监控的能力仍较差，迫切需要完善 VPLS 的 OAM 机制。

PW 的连通性关系到用户间流量转发是否正常，PW 的转发性能关系到网络能否符合签订的 SLA（Service Level Agreements）。NQA VPLS PW Ping 和 Trace 测试可以对指定的 PW 进行检测，提供时延、抖动等数据供用户参考，以使用户分析网络的健康状况。

前置任务

在配置 VPLS PW Ping 和 VPLS Trace 测试之前，需正确配置 VPLS 网络，确保 VSI 状态 Up。

数据准备

在配置 VPLS PW Ping 和 PW Trace 测试之前，需要准备以下数据：

| 序号 | 数据                                          |
|----|---------------------------------------------|
| 1  | VSI 名称及其类型（LDP 或 BGP）                       |
| 2  | 目的地址（LDP 方式）、本端 site-id 和远端 site-id（BGP 方式） |
| 3  | （可选）本地 PW、测试周期、发包个数、发包间隔、报文大小、填充内容、测试失败百分比  |
| 4  | NQA 测试的启动方式和结束方式                            |

6.44.2 配置 VPLS PW Ping 测试参数

配置 VPLS PW Ping 测试例前，需要确保 VSI Up。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type vplspwping**，配置测试例类型为 VPLS PW Ping。
- 步骤 4** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。
- 步骤 5** 根据建立 VC 的信令方式，选择如下步骤：
- 当 vc-type 为 LDP 时，执行命令 **destination-address ipv4 ip-address**，配置目的地址
  - 当 vc-type 为 BGP 时，
    1. 执行命令 **vc-type { ldp | bgp }**，配置 L2VPN 的协议类型为 BGP
    2. 执行命令 **local-pw-id local-pw-id**，配置本端的 Site ID
    3. 执行命令 **remote-pw-id remote-pw-id**，配置远端的 Site ID
- 步骤 6** （可选）根据需要，配置 VPLS PW Ping 测试其他参数。

- 执行命令 **probe-count** *number*，配置每次发送的测试探针个数。
- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置发送测试包的时间间隔。  
测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，测试结果的统计值误差会比较大。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 当 vc-type 为 LDP 时，执行命令 **local-pw-id** *local-pw-id*，配置本端的 PW ID。
- 执行命令 **lsp-replymode** { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }，配置 Echo 报文的响应模式。  
**no-reply** 表示不响应。**udp** 表示以 UDP 报文响应。**udp-via-vpls** 表示通过 IPv4 的 VPLS 的 UDP 报文响应。**udp-router-alert** 表示通过携带 Router Alert 的 UDP 报文响应。**level-control-channel** 表示通过应用程序级别的控制通道回复。
- 执行命令 **lsp-exp** *exp*，配置 LSP EXP 值。
- 执行命令 **remote-address** **ipv4** *remote-ip-address* 配置在 VLL 多跳接入时的远端地址。

#### 说明

更多可选参数，可以在配置了 NQA 测试例类型后，进入测试例视图，执行命令 **display nqa-parameter** 进行查看。

### 步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ]，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

## 6.44.3 配置 VPLS PW Trace 测试参数

配置 VPLS PW Trace 测试例前，需要确保 VSI Up。

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

**步骤 3** 执行命令 **test-type vplspwtrace**，配置测试例类型为 VPLS PW Trace。

**步骤 4** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。

**步骤 5** 根据建立 VC 的信令方式，选择如下步骤：

- 当 vc-type 为 LDP 时，执行命令 **destination-address ipv4 ip-address**，配置目的地址
- 当 vc-type 为 BGP 时，
  1. 执行命令 **vc-type { ldp | bgp }**，配置 L2VPN 的协议类型为 BGP
  2. 执行命令 **local-pw-id local-pw-id**，配置本端的 Site ID
  3. 执行命令 **remote-pw-id remote-pw-id** 配置远端的 Site ID

**步骤 6** （可选）根据需要，配置 VPLS PW Trace 测试其他参数。

- 执行命令 **probe-count number**，配置每次发送的测试探针个数。
- 执行命令 **interval { milliseconds interval | seconds interval }**，配置发送测试包的时间间隔。  
测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，测试结果的统计值误差会比较大。
- 执行命令 **fail-percent percent**，配置 NQA 测试的失败百分比。
- 当 vc-type 为 LDP 时，执行命令 **local-pw-id local-pw-id**，配置本端的 PW ID。
- 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 Echo 报文的响应模式。  
**no-reply** 表示不响应。**udp** 表示以 UDP 报文响应。**udp-via-vpls** 表示通过 IPv4 的 VPLS 的 UDP 报文响应。**udp-router-alert** 表示通过携带 Router Alert 的 UDP 报文响应。**level-control-channel** 表示通过应用程序级别的控制通道回复。
- 执行命令 **lsp-exp exp**，配置 LSP EXP 值。
- 执行命令 **remote-address ipv4 remote-ip-address** 配置在 VLL 多跳接入时的远端地址。

#### 说明

更多可选参数，可以在配置了 NQA 测试例类型后，进入测试例视图，执行命令 **display nqa-parameter** 进行查看。

**步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

## 6.44.4 检查配置结果

## 前提条件

已经完成 VPLS PW Ping 和 PW Trace 测试功能的所有配置。

### 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

**步骤 1** 在 NQA 客户端执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

## 任务示例

对于 VPLS PW Ping 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance vplspwping
NQA entry(vplspw,ping) :testflag is inactive ,testtype is vplspwping
1 . Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:success RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
 NumOfRTT:3 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:10 Min Positive DS:40
 Max Positive SD:10 Max Positive DS:40
 Positive SD Number:1 Positive DS Number:1
 Positive SD Sum:10 Positive DS Sum:40
 Positive SD Square Sum:100 Positive DS Square Sum:1600
 Min Negative SD:20 Min Negative DS:30
 Max Negative SD:20 Max Negative DS:30
 Negative SD Number:1 Negative DS Number:1
 Negative SD Sum:20 Negative DS Sum:30
 Negative SD Square Sum:400 Negative DS Square Sum:900
 Min Delay SD:0 Min Delay DS:0
 Max Delay SD:0 Max Delay DS:0
 Delay SD Square Sum:0 Delay DS Square Sum:0
 Packet Loss SD:0 Packet Loss DS:0
 Packet Loss Unknown:0 Average of Jitter:25
 Average of Jitter SD:15 Average of Jitter DS:35
 jitter out value:0.6119792 jitter in value:1.4062500
 NumberOfOWD:0 Packet Loss Ratio: 0%
 OWD SD Sum:0 OWD DS Sum:0
 ICPIF value: 0 MOS-CQ value: 0
 TimeStamp unit: ms Packet Rewrite Number: 0
 Packet Rewrite Ratio: 0% Packet Disorder Number: 0
 Packet Disorder Ratio: 0% Fragment-disorder Number: 0
 Fragment-disorder Ratio: 0%
```

对于 VPLS PW Trace 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results test-instance vplspwtrace
NQA entry(t, t) :testflag is inactive ,testtype is vplspwtrace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
```

```
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %
```

## 6.45 配置 VPLS 组播 Trace 检测 VPLS 网络测试

### 6.45.1 建立配置任务

#### 6.45.2 配置 VPLS 组播 Trace 检测组播转发

#### 6.45.3 检查配置结果

### 6.45.1 建立配置任务

#### 应用环境

VPLS 组播 Trace 可用于检查 VPLS 网络 PE 的 IGMP Snooping 功能是否正常及故障点所处位置。支持如下网络检测：

- Kompella 方式的 VPLS。
- Martini 方式的 VPLS

#### 前置任务

在配置 VPLS 组播 Trace 检测 VPLS 网络测试之前，需完成以下任务：

- 配置 VPLS 网络。
- 使能 VSI 域内设备的 IGMP Snooping。

#### 数据准备

在配置 VPLS 组播 Trace 测试之前，需要准备以下数据：

| 序号 | 数据                                                                                     |
|----|----------------------------------------------------------------------------------------|
| 1  | NQA 测试例的管理者、测试例的测试例名                                                                   |
| 2  | VSI 实例的名称                                                                              |
| 3  | （可选）：组播源地址、填充字符、发送回显请求报文的载荷长度、等待回显请求报文响应的超时时间、发送下一个回显请求报文的等待时间、回复模式、发送回显请求报文的优先级、失败百分比 |
| 4  | 组播 IP 地址、对端 IP 地址                                                                      |
| 5  | 启动方式和结束方式                                                                              |



## 6.45.2 配置 VPLS 组播 Trace 检测组播转发

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type vplsmtrace**，配置测试例类型为 VPLS Mtrace。
- 步骤 4** 执行命令 **vsi vsi-name**，配置测试例对应的 VSI 的名称。
- 步骤 5** 执行命令 **destination-address ipv4 ip-address**，配置 VPLS Mtrace 测试的目的地址。
- 步骤 6** 执行命令 **remote-address ipv4 remote-ip-address** 命令，配置 VPLS Mtrace 测试例的对端 IP 地址。
- 步骤 7** （可选）根据需要，配置 VPLS Mtrace 测试其他参数。
- 执行命令 **agetime hh:mm:ss**，配置 NQA 测试例的老化时间。
  - 执行命令 **description string**（NQA 视图），配置测试例描述。
  - 执行命令 **frequency interval**，配置 NQA 测试例的测试周期。
  - 执行命令 **timeout time**，配置测试超时时间。
  - 执行命令 **source-address ipv4 ip-address**，配置 NQA 测试例的源 IP 地址。
  - 执行命令 **tracert-hopfailtimes times**，配置 NQA 测试 Trace route 测试例的跳失败数。
  - 执行命令 **tracert-livetime first-ttl first-ttl max-ttl max-ttl**，配置 NQA 测试 Trace 测试例的生存时间。
  - 执行命令 **send-trap { all | [ owd-ds | owd-sd | probefailure | rtd | testcomplete | testfailure ] \* }**，配置 Trap 消息的发送条件。
  - 执行命令 **probe-failtimes times**，用来配置 NQA 测试例的报文失败数，即，发送 Trap 的阈值。
  - 执行命令 **test-failtimes times**，配置当 NQA 测试连续测试失败达到一定的次数以后，需要向网管发送 Trap 信息。
  - 执行命令 **lsp-exp exp**，配置 NQA 测试的 LSP EXP 值。
  - 执行命令 **lsp-replymode { no-reply | udp | udp-via-vpls | udp-router-alert | level-control-channel }**，配置 NQA 测试的 LSP 报文返回方式。

#### 说明

lsp-replymode no-replay 进行单向测试，无论测试是否成功在测试结果的显示信息中都会显示测试失败。只是在测试成功时在测试结果的显示信息中，会显示测试报文超时的数量；在测试失败时在测试结果的显示信息中，会显示测试报文丢弃的数量。

- 步骤 8** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]**，立即启动测试例。



- 执行命令 **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ], 延迟指定时间后启动测试例。

----结束

## 6.45.3 检查配置结果

### 前提条件

已经完成 VPLS 组播 Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

**步骤 1** 执行 **display nqa results** [ **test-instance** admin-name test-name ]命令查看测试结果。

----结束

### 任务示例

对于 VPLS 组播 Trace 测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<HUAWEI> display nqa results
NQA entry(admin, test) :testflag is inactive ,testtype is vplsmtrace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2009-12-03 09:42:46.7
1 . Hop 1
Send operation times: 1 Receive response times: 1
Min/Max/Average Completion Time: 0/0/0
Sum/Square-Sum Completion Time: 0/0
RTD OverThresholds number: 0
Last Good Probe Time: 2009-12-03 09:42:43.9
Destination ip address:7.7.7.9
Lost packet ratio: 0 %
2 . Hop 2
Send operation times: 1 Receive response times: 1
Min/Max/Average Completion Time: 0/0/0
Sum/Square-Sum Completion Time: 0/0
RTD OverThresholds number: 0
Last Good Probe Time: 2009-12-03 09:42:46.7
Destination ip address:6.6.6.6
Lost packet ratio: 0 %
```

## 6.46 配置 VPLS MAC Ping 测试

[6.46.1 建立配置任务](#)[6.46.2 配置 VPLS MAC Ping 测试参数](#)[6.46.3 检查配置结果](#)

## 6.46.1 建立配置任务

### 应用环境

完成 VPLS 网络配置后，可以通过 NQA 对 VPLS 网络进行 MAC Ping 测试，检测 VPLS 网络中二层转发链路的连通性。

### 前置任务

在配置 VPLS MAC Ping 测试之前，需正确配置 VPLS 网络，确保 VSI 状态 Up。

### 数据准备

在配置 VPLS MAC Ping 测试之前，需要准备以下数据：

| 序号 | 数据               |
|----|------------------|
| 1  | VSI Name、MAC 地址  |
| 2  | （可选）VLAN ID      |
| 3  | NQA 测试的启动方式和结束方式 |

## 6.46.2 配置 VPLS MAC Ping 测试参数

### 背景信息

请在 NQA 客户端进行下列配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type vplsping**，配置测试例类型为 VPLS MAC Ping。
- 步骤 4** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。
- 步骤 5** 执行命令 **destination-address mac mac-address**，配置与 VSI 关联的 MAC 地址。
- 步骤 6** （可选）执行命令 **vlan vlan-id**，配置 VLAN ID。
- 步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 立即启动测试例。
- 执行命令 **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ], 延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

## 6.46.3 检查配置结果

### 前提条件

已经完成 VPLS MAC Ping 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

### 操作步骤

- 步骤 1** 在 NQA 客户端执行 **display nqa results** [ **test-instance** *admin-name test-name* ] 命令查看测试结果。

----结束

### 任务示例

对于 VPLS MAC Ping 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 测试的响应时间总和
  - RTT 平方和（低 32 位和高 32 位）
  - 报文最小往返时间、最大往返时间
  - 目的地址类型、目的地址

已收到回应的报文数目、已发送的报文数  
至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (1, 1) :testflag is inactive ,testtype is vplsping
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:168.1.1.1
Min/Max/Average Completion Time: 21/30/24
Sum/Square-Sum Completion Time: 74/1870
Last Good Probe Time: 2009-4-21 9:49:50.1
Lost packet ratio: 0 %
```

6.47 配置 VPLS MAC Trace 测试

- 6.47.1 建立配置任务
- 6.47.2 配置 VPLS MAC Trace 测试参数
- 6.47.3 检查配置结果

6.47.1 建立配置任务

应用环境

完成 VPLS 网络配置后，可以通过 NQA 对 VPLS 网络进行 MAC Trace 测试，检测 VPLS 网络中二层转发链路的连通性。

前置任务

在配置 VPLS MAC Trace 测试之前，需正确配置 VPLS 网络，确保 VSI 状态 Up。

数据准备

在配置 VPLS MAC Trace 测试之前，需要准备以下数据：

| 序号 | 数据               |
|----|------------------|
| 1  | VSI ID、MAC 地址    |
| 2  | （可选）VLAN ID      |
| 3  | NQA 测试的启动方式和结束方式 |

6.47.2 配置 VPLS MAC Trace 测试参数

## 背景信息

请在 NQA 客户端进行下列配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **nqa test-instance admin-name test-name**，建立 NQA 测试例，并进入测试例视图。
- 步骤 3** 执行命令 **test-type vplstrace**，配置测试例类型为 VPLS vsi mac trace。
- 步骤 4** 执行命令 **vsi vsi-name**，配置需要测试的 VSI 的名称。
- 步骤 5** 执行命令 **destination-address mac mac-address**，配置与 VSI 关联的 MAC 地址。
- 步骤 6**（可选）执行命令 **vlan vlan-id**，配置 VLAN ID。
- 步骤 7** 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，立即启动测试例。
- 执行命令 **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，在指定时刻启动测试例。
- 执行命令 **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }**，延迟指定时间后启动测试例。

以上 **start** 命令各选项及参数意义请参见《命令参考》。

----结束

## 6.47.3 检查配置结果

### 前提条件

已经完成 VPLS MAC Trace 测试功能的所有配置。

 说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

## 操作步骤

- 步骤 1** 在 NQA 客户端执行 **display nqa results [ test-instance admin-name test-name ]** 命令查看测试结果。

----结束

## 任务示例

对于 VPLS MAC Trace 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

- 错误统计：
  - 无路由连接次数
  - 序列号出错次数
  - 测试例中的报文 Timeout 次数
- 每个测试报文的历史统计：
  - 发送每个报文的时间戳
  - 每个报文收到后的时间
  - 接收每个报文的状态
  - 目的地址
- 每个测试例的结果统计：
  - 成功执行测试次数
  - 已收到回应的报文数目、已发送的报文数
  - 至今收到最后一个报文的时间

```
<HUAWEI> display nqa results
NQA entry (test, vplstrace?) :testflag is inactive ,testtype is vplstrace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-4-21 9:51:4.1
1 . Hop 1
 Send operation times: 1 Receive response times: 1
 Min/Max/Average Completion Time: 0/0/0
 Sum/Square-Sum Completion Time: 0/0
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-21 9:51:1.5
 Destination ip address:
 Lost packet ratio: 0 %,
2 . Hop 2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average Completion Time: 0/0/0
 Sum/Square-Sum Completion Time: 0/0
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-21 9:51:4.1
 Destination ip address:
 Lost packet ratio: 0 %
```

## 6.48 配置 NQA 报文改写检查功能

NQA 报文改写检查功能用于检查报文内容是否被改写。

### 应用环境

IP 报文从源端到目的地传输过程中，由于设备硬件故障，可能导致报文内容改写。从而影响业务使用。以前，报文内容被改写时，通常很难定位，要通过实验室测试设备抓取报文、分析报文等手段，才能确定是否发生报文内容改写问题。

NQA 的报文改写检查功能提供了便捷的检测手段。该功能通过在源端发送的检测报文中填充指定比特数据，然后对收到的回应报文进行分析，从而判断从源端到目的端是否出现报文改写。通过对网段进行逐段测试，可以定位出现报文改写的设备。

## 前置任务

在配置 NQA 报文改写检查基本功能之前，需完成以下任务之一：

- [配置 Jitter 测试](#)
- [配置 ICMP Jitter 测试](#)

## 操作步骤

**步骤 1** 执行命令 [system-view](#)，进入系统视图。

**步骤 2** 执行命令 [nqa test-instance admin-name test-name](#)，进入 NQA 测试例视图。

**步骤 3** （可选）执行命令 [icmp-jitter-mode icmp-echo](#)，将 ICMP Jitter 测试模式配置为 [icmp-echo](#) 模式。

若配置 ICMP Jitter 测试，则需要执行该步骤；若配置 Jitter 测试，则无需执行该步骤。

**步骤 4** 执行命令 [packet-rewrite-check { alternant-binary | same-binary }](#)，使能报文填充检测功能。

[alternant-binary](#) 指定使用 0101 和 1010 交替填充检测报文。[same-binary](#) 指定使用全 0 和全 1 交替填充检测报文。

----结束

## 6.49 维护 NQA

在测试中需要对测试进行维护时，可以通过重新启动测试例，清空测试结果信息实现对测试例的维护。

### 6.49.1 重新启动测试例

在测试不成功时，可以在下一个时间段重新启动测试来尝试。

### 6.49.2 清除统计信息

当前的测试统计信息已经保存到 FTP 服务器，可以把相关的测试结果清除。

### 6.49.3 调试 NQA

在测试中遇到问题时，可以针对测试例进行调试。

## 6.49.1 重新启动测试例

在测试不成功时，可以在下一个时间段重新启动测试来尝试。

## 前提条件

在确认需要重新启动测试例的情况下，请在 NQA 视图下执行以下命令。

## 背景信息



### 注意

重新启动测试例，将终止正在运行的测试例。

---

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 执行命令 **restart** 重新启动一条 NQA 测试例。

----结束

## 6.49.2 清除统计信息

当前的测试统计信息已经保存到 FTP 服务器，可以把相关的测试结果清除。

## 前提条件

在确认需要清除统计信息时，请在 NQA 视图下执行以下的命令。

## 背景信息



### 注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

---

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **nqa test-instance admin-name test-name**，进入 NQA 测试例视图。

**步骤 3** 使用 **clear-records** 命令清除 NQA 测试例的所有历史统计和结果统计。

----结束

## 6.49.3 调试 NQA

在测试中遇到问题时，可以针对测试例进行调试。

## 前提条件

在出现运行故障时，请在用户视图下执行下面的 **debugging** 命令对 NQA 进行调试，查看调试信息，并定位故障的原因。输出调试信息的操作步骤请参考《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 系统管理》中的“信息中心配置”。



## 背景信息



### 注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

---

## 操作步骤

**步骤 1** 使用 **debugging nqa all** 命令打开 NQA 的调试开关。

----结束

## 6.50 NQA 配置举例

介绍 NQA 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

### 6.50.1 配置 ICMP 测试示例

通过配置 ICMP 测试可以检测到 IP 网络的连通性。

### 6.50.2 配置 DHCP 测试示例

通过配置 DHCP 测试可以检测到客户端和 DHCP 服务器的连接是否可以建立并可以检测到获取地址的速度。

### 6.50.3 配置 FTP 下载速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端从 FTP 服务器下载文件时的性能。

### 6.50.4 配置 FTP 上传速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端上传文件到 FTP 服务器时的性能。

### 6.50.5 配置 HTTP 测试示例

通过 HTTP 测试可以检测到客户端和 HTTP 服务器交互时的各个阶段的性能。

### 6.50.6 配置 DNS 测试示例

通过 DNS 测试可以检测到客户端和 DNS 服务器交付时的性能参数。

### 6.50.7 配置 Traceroute 测试示例

通过配置 Traceroute 测试可以检测到报文传输过程中客户端和报文传输路径中的设备的连通性。

### 6.50.8 配置 SNMP Query 测试示例

通过配置 SNMP Query 测试可以检测到客户端和网管之间通过 SNMP 通信时的性能。

### 6.50.9 配置 TCP 测试示例

通过配置 TCP 测试可以检测到客户端和服务端之间 TCP 的连通性。

### 6.50.10 配置 UDP 测试示例

通过配置 UDP 测试可以检测到客户端和服务端之间 UDP 的连通性。

### 6.50.11 配置 Jitter 测试示例

通过配置 Jitter 测试可以检测到网络中抖动情况。

#### 6.50.12 配置基于接口板发包的 Jitter 测试例

通过配置基于接口板发包的 Jitter 测试可以更加精确的检测到网络中的抖动情况。

#### 6.50.13 配置普通隧道 LSP Ping 测试示例

通过普通隧道 LSP Ping 测试可以检测 LSP 隧道的各个 LSR 之间的连通性。

#### 6.50.14 配置普通隧道 LSP Jitter 测试示例

通过普通隧道 LSP Jitter 测试可以检测报文在 LSP 隧道中传输时的抖动情况。

#### 6.50.15 配置 TE 隧道 LSP Jitter 测试示例

通过普通隧道 LSP Jitter 测试可以检测报文在 TE 隧道中传输时的抖动情况。

#### 6.50.16 配置 ICMP Jitter 测试示例

通过 ICMP Jitter 测试可以检测到网络中的抖动情况。ICMP Jitter 测试不需要配置服务器端，测试的对端设备可以是非华为设备。

#### 6.50.17 配置基于接口板发包的 ICMP Jitter 测试例

通过基于接口板发送的 ICMP Jitter 测试可以检测到更加准确的网络抖动情况。

#### 6.50.18 配置 Path Jitter 测试示例

通过 Path Jitter 测试可以检测到报文在传输路径中的抖动情况。

#### 6.50.19 配置 Path MTU 测试示例

通过 Path MTU 测试可以检测到报文在传输路径中的 MTU。

#### 6.50.20 配置 TE 隧道 LSP Traceroute 测试示例

通过 TE 隧道 LSP Traceroute 测试可以检测到 TE 隧道中的各个 LSR 的连通性。

#### 6.50.21 配置检测网段中的保留组成员示例

通过检测网段中的保留组成员可以检测出接口所在网段上存在哪些保留组成员。

#### 6.50.22 配置检测网络承载组播业务的性能示例

检测网络承载组播业务的性能，可以查看检查协议运行状态是否正常，确认组播分发树是否正确建立；检查网络中存在的组成员，计算从 MPing 发起者到组成员的 TTL、响应时间等参数。

#### 6.50.23 配置检测从组播源到当前路由器的 RPF 路径的测试例示例

通过检测从组播源到当前路由器的 RPF 路径的测试例，可以查看到从组播源到查询者的 RPF 路径。

#### 6.50.24 配置检测从组播源到当前路由器的组播路径的测试例示例

通过检测从组播源到当前路由器的组播路径的测试例，判断出组播数据如何从源到达当前路由器。

#### 6.50.25 配置检测从组播源到目的主机的 RPF 路径的测试例示例

通过检测从组播源到目的主机的 RPF 路径的测试例，检测从组播源到目的主机的 RPF 路径。

#### 6.50.26 配置检测从组播源到目的主机的组播路径的测试例示例

通过检测从组播源到目的主机的组播路径的测试例，检测从组播源到目的主机的组播路径。

#### 6.50.27 配置单跳 PW 的 PWE3 Ping 测试示例

通过单跳 PW 的 PWE3 Ping 测试，检测出 PE 之间 PW 的连通性。

#### 6.50.28 配置多跳 PW 的 PWE3 Ping 测试示例

通过多跳 PW 的 PWE3 Ping 测试，检测出 PE 之间 PW 的连通性。

#### 6.50.29 配置单跳 PW 的 PWE3 Trace 测试示例

通过单跳 PW 的 PWE3 Traceg 测试，检测出 PE 之间 PW 的连通性。

#### 6.50.30 配置多跳 PW 的 PWE3 Trace 测试示例

通过多跳 PW 的 PWE3 Traceg 测试，检测出 PE 之间 PW 的连通性。

#### 6.50.31 配置多跳跨域 Kompella L2VPN 的 VC Trace 测试示例

通过多跳跨域 Kompella L2VPN 的 VC Trace 测试使用多跳跨域 Kompella L2VPN 的 VC Trace 测试 PE1 与 PE2 之间的 PW 连通性状态。

#### 6.50.32 配置 NQA 测试组示例

通过 NQA 测试组，可以将相同类型的测试例加入同一个测试组，进行统一管理。

#### 6.50.33 配置向网管端发送 NQA 阈值告警示例

通过向网管端发送 NQA 阈值告警，网络管理人员可以清晰的了解到设备端发生的情况。

#### 6.50.34 配置测试结果发送到 FTP 服务器示例

通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

#### 6.50.35 配置 NQA 上下限阈值告警示例

在 NQA 的测试结果超出阈值时，可以发送告警或者生成日志或者既发送告警也生成日志。

#### 6.50.36 配置 Martini VPLS 的 VPLS 组播 Ping 测试示例

通过 VPLSMPING 测试例检测 Martini 方式 VPLS 网络的连通情况。

#### 6.50.37 配置 Kompella VPLS 的 VPLS 组播 Ping 测试示例

通过 VPLSMPING 测试例检测 Kompella 方式 VPLS 网络的连通情况。

#### 6.50.38 配置 Martini VPLS 的 VPLS 组播 Trace 测试示例

#### 6.50.39 配置 VPLS MAC Ping 测试示例

#### 6.50.40 配置 VPLS MAC Trace 测试示例

#### 6.50.41 配置 VPLS PW Ping 和 PW Trace 测试示例

#### 6.50.42 配置 MAC Trace 测试 VLAN 示例

#### 6.50.43 配置 MAC Trace 测试 VPLS 示例

#### 6.50.44 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 示例

#### 6.50.45 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 示例

#### 6.50.47 配置对指定的组播 VPN 网络进行从组播源到目的主机的 RPF 路径检测

通过 NQA 对指定的组播 VPN 网络进行测试，了解从组播源到目的主机的 RPF 路径连通情况。

#### 6.50.48 配置 NQA 上下限阈值告警、联动测试例事件示例

通过 NQA 测试例联动，实现对网络故障的动态监控。

#### 6.50.49 配置 CR-LSP 热备份隧道 LSP Traceroute 测试示例

通过 NQA 对 CR-LSP 热备份隧道进行测试，探测 LSP 的故障节点。

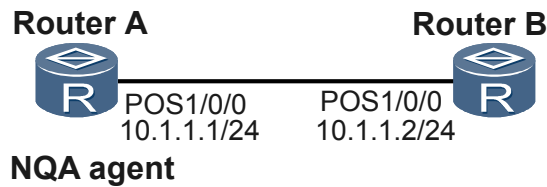
## 6.50.1 配置 ICMP 测试示例

通过配置 ICMP 测试可以检测到 IP 网络的连通性。

## 组网需求

如图 6-3 所示，RouterA 作为 NQA 客户端，测试 RouterB 是否可达。

图 6-3 ICMP 测试组网图



## 配置思路

1. 使用 NQA ICMP 测试功能，测试报文在本端（RouterA）和指定的目的端（RouterB）之间是否可达。
2. 使用 NQA ICMP 测试功能，测试报文在本端（RouterA）和指定的目的端（RouterB）之间的往返时间。

## 数据准备

为完成此配置例，需准备如下的数据：

- RouterB 的主机地址

## 操作步骤

### 步骤 1 配置 IP 地址（略）

### 步骤 2 使能 NQA 客户端，配置 ICMP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin icmp
[RouterA-nqa-admin-icmp] test-type icmp
[RouterA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

### 步骤 3 立即启动测试

```
[RouterA-nqa-admin-icmp] start now
```

### 步骤 4 验证测试结果

```
[RouterA-nqa-admin-icmp] display nqa results test-instance admin icmp
NQA entry(admin, icmp) :testFlag is inactive ,testtype is icmp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:10.1.1.2
Min/Max/Average Completion Time: 31/46/36
Sum/Square-Sum Completion Time: 108/4038
Last Good Probe Time: 2006-8-2 10:7:11.4
Lost packet ratio: 0 %
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
return
```

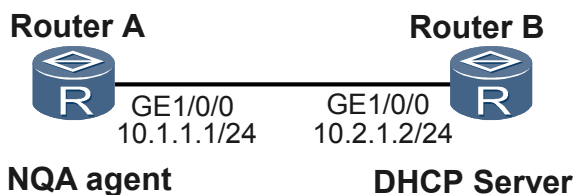
## 6.50.2 配置 DHCP 测试示例

通过配置 DHCP 测试可以检测到客户端和 DHCP 服务器的连接是否可以建立并可以检测到获取地址的速度。

## 组网需求

如图 6-4 所示，RouterB 作为 DHCP 服务器，使用 NQA DHCP 功能测试从 DHCP 服务器分配到 IP 地址的时间。

图 6-4 DHCP 测试组网图



## 配置思路

采用如下思路进行 DHCP 测试的配置：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 DHCP 测试例，查看是否能够从 DHCP Server 建立连接并分配到 IP 地址。

## 数据准备

为完成此配置例，需准备如下的数据：

- DHCP Server 的主机地址
- 源接口
- 超时时间

## 操作步骤

### 步骤 1 配置 IP 地址（略）

### 步骤 2 使能 NQA 客户端，配置 DHCP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin dhcp
[RouterA-nqa-admin-dhcp] test-type dhcp
[RouterA-nqa-admin-dhcp] source-interface gigabitethernet 1/0/0
[RouterA-nqa-admin-dhcp] timeout 20
```

### 步骤 3 启动测试操作

```
[RouterA-nqa-admin-dhcp] start now
```

### 步骤 4 验证测试结果

```
[RouterA-nqa-admin-dhcp] display nqa results test-instance admin dhcp
NQA entry (admin, dhcp) :testflag is inactive ,testtype is dhcp
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.2.1.2
 Min/Max/Average Completion Time: 1018/1019/1018
 Sum/Square-Sum Completion Time: 3055/3111009
 Last Good Probe Time: 2009-3-11 9:26:38.5
 Lost packet ratio: 0 %
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin dhcp
 test-type dhcp
 timeout 20
 source-interface GigabitEthernet1/0/0
#
return
```

### ● RouterB 的配置文件

```
#
sysname RouterB
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
```

```
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
return
```

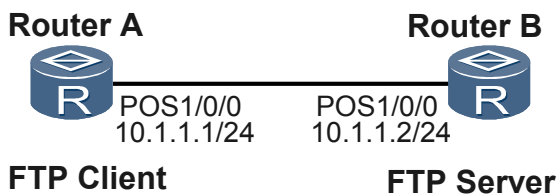
### 6.50.3 配置 FTP 下载速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端从 FTP 服务器下载文件时的性能。

#### 组网需求

如图 6-5 所示，RouterB 作为 FTP Server，登录 FTP 服务器的用户名为 user1，密码为 hello，要下载的文件名为 test.txt。

图 6-5 FTP 测试组网图



#### 配置思路

为完成此配置例，需准备如下的数据：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及从 FTP 服务器得到一个文件的时间。

#### 数据准备

为完成 FTP 下载速度测试，需准备如下数据：

- FTP 服务器的 IP 地址
- 进行测试的源 IP 地址
- FTP 用户名和密码
- FTP 测试操作文件

#### 操作步骤

**步骤 1** 配置 RouterA 和 RouterB 的 IP 地址（略）

**步骤 2** 配置 RouterB 作为 FTP 服务器

```
<RouterB> system-view
[RouterB] ftp server enable
[RouterB] aaa
[RouterB-aaa] local-user user1 password cipher hello
[RouterB-aaa] local-user user1 service-type ftp
[RouterB-aaa] local-user user1 ftp-directory flash:/
```

```
[RouterB-aaa] quit
```

### 步骤 3 在 RouterA 上配置 FTP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin ftp
[RouterA-nqa-admin-ftp] test-type ftp
[RouterA-nqa-admin-ftp] destination-address ipv4 10.1.1.2
[RouterA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[RouterA-nqa-admin-ftp] ftp-operation get
[RouterA-nqa-admin-ftp] ftp-username user1
[RouterA-nqa-admin-ftp] ftp-password hello
[RouterA-nqa-admin-ftp] ftp-filename test.txt
```

### 步骤 4 启动测试操作

```
[RouterA-nqa-admin-ftp] start now
```

### 步骤 5 验证测试结果

```
[RouterA-nqa-admin-ftp] display nqa results test-instance admin ftp
NQA entry(admin, ftp) :testFlag is inactive ,testtype is ftp
 1 . Test 1 result The test is finished
 SendProbe:1 ResponseProb:1
 Completion :success RTD OverThresholds number: 0
 MessageBodyOctetsSum: 448 Stats errors number: 0
 Operation timeout number: 0 System busy operation number:0
 Drop operation number:0 Disconnect operation number:0
 CtrlConnTime Min/Max/Average: 438/438/438
 DataConnTime Min/Max/Average: 218/218/218
 SumTime Min/Max/Average: 656/656/656
 Average RTT:656
 Lost packet ratio:0 %
```

----结束

## 配置文件

#### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin ftp
 test-type ftp
 destination-address ipv4 10.1.1.2
 source-address ipv4 10.1.1.1
 ftp-operation get
 ftp-filename test.txt
 ftp-username user1
 ftp-password hello
#
return
```

#### ● RouterB 的配置文件

```
#
sysname RouterB
#
FTP server enable
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
aaa
```



```
local-user user1 password cipher 3MQ*TZ,03KCQ=~Q`MAF4<1!!
local-user user1 service-type ftp
local-user user1 ftp-directory flash:/
#
return
```

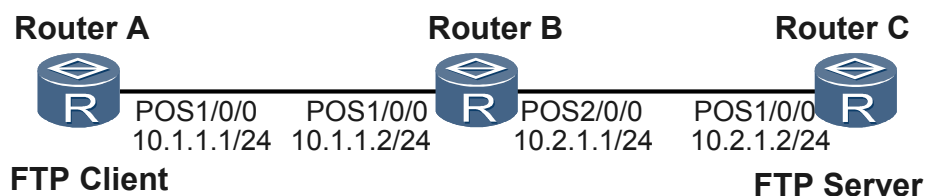
## 6.50.4 配置 FTP 上传速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端上传文件到 FTP 服务器时的性能。

### 组网需求

如图 6-6 所示，测试向 FTP Server，即 RouterC 上载文件的速度。

图 6-6 FTP 测试组网图



### 配置思路

采用如下思路进行 FTP 上传速度的测试：

1. RouterA 作为 NQA 客户端和 FTP Client。在 RouterA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及向 FTP 服务器上载一个文件的时间。
2. 登录 FTP 服务器的用户名为 user1，密码为 hello，构造大小为 10k 的文件上载。

### 数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器的 IP 地址
- 进行测试的 FTP 客户端源 IP 地址
- FTP 用户名和密码
- FTP 上载的文件大小

### 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置 RouterC 作为 FTP 服务器

```
<RouterC> system-view
[RouterC] ftp-server enable
[RouterC] aaa
[RouterC-aaa] local-user user1 password cipher hello
[RouterC-aaa] local-user user1 service-type ftp
[RouterC-aaa] local-user user1 ftp-directory flash:
```

```
[RouterC-aaa] quit
```

**步骤 3** 在 RouterA 上配置 FTP 类型的 NQA 测试例，构造一个大小为 10k 字节的文件上载

```
<RouterA> system-view
[RouterA] nqa test-instance admin ftp
[RouterA-nqa-admin-ftp] test-type ftp
[RouterA-nqa-admin-ftp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[RouterA-nqa-admin-ftp] ftp-operation put
[RouterA-nqa-admin-ftp] ftp-username user1
[RouterA-nqa-admin-ftp] ftp-password hello
[RouterA-nqa-admin-ftp] ftp-filesize 10
```

**步骤 4** 启动测试操作

```
[RouterA-nqa-admin-ftp] start now
```

**步骤 5** 验证测试结果

# 在 RouterA 上查看 NQA 测试结果。

```
[RouterA-nqa-admin-ftp] display nqa results test-instance admin ftp
NQA entry(admin, ftp) :testFlag is inactive ,testtype is ftp
1. Test 1 result The test is finished
 SendProbe:1 ResponseProb:1
 Completion :success RTD OverThresholds number: 0
 MessageBodyOctetsSum: 10240 Stats errors number: 0
 Operation timeout number: 0 System busy operation number:0
 Drop operation number:0 Disconnect operation number: 0
 CtrlConnTime Min/Max/Average: 657/657/657
 DataConnTime Min/Max/Average: 500/500/500
 SumTime Min/Max/Average: 1157/1157/1157
 Average RTT:656
 Lost packet ratio:0 %
```

# 在 RouterC 上可以看到增加了一个名为“nqa-ftp-test.txt”的文件。（以下只显示部分文件）

```
<RouterC> dir
Directory of flash:/
 0 -rw- 331 Jul 06 2007 18:34:34 private-data.txt
 1 -rw- 10240 Jul 06 2007 18:37:06 nqa-ftp-test.txt
2540 KB total (1536 KB free)
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin ftp
 test-type ftp
 destination-address ipv4 10.2.1.2
 source-address ipv4 10.1.1.1
 ftp-operation put
 ftp-filesize 10
 ftp-username user1
 ftp-password hello
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
```

```
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
FTP server enable
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
aaa
 local-user user1 password cipher 3MQ*TZ,03KCQ=`Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

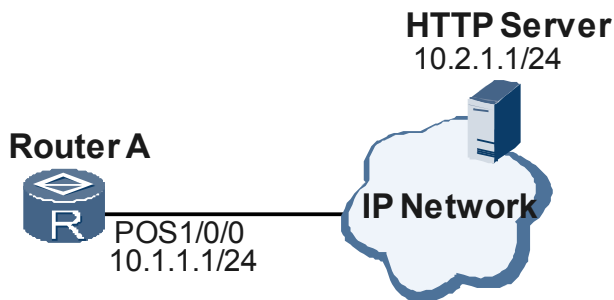
## 6.50.5 配置 HTTP 测试示例

通过 HTTP 测试可以检测到客户端和 HTTP 服务器交互时的各个阶段的性能。

### 组网需求

如图 6-7 所示。RouterA 通过广域网和 HTTP Server 相连。

图 6-7 HTTP 测试组网图



## 配置思路

采用如下思路进行 HTTP 响应速度的测试：

1. RouterA 做为 NQA 客户端。
2. 在 RouterA 上配置并启动 HTTP 测试例，使用 NQA HTTP 功能测试是否可以和指定的 HTTP 服务器建立连接，以及它们之间传输一个文件的时间。

## 数据准备

为完成此配置例，需准备如下的数据：

- HTTP Server 的主机地址
- HTTP 测试操作类型

## 操作步骤

### 步骤 1 配置 IP 地址（略）

### 步骤 2 使能 NQA 客户端，配置 HTTP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin http
[RouterA-nqa-admin-http] test-type http
[RouterA-nqa-admin-http] destination-address ipv4 10.2.1.1
[RouterA-nqa-admin-http] http-operation get
[RouterA-nqa-admin-http] http-url www.huawei.com
```

### 步骤 3 启动测试操作

```
[RouterA-nqa-admin-http] start now
```

### 步骤 4 验证测试结果

```
[RouterA-nqa-admin-http] display nqa results test-instance admin http
NQA entry(admin, http) :testFlag is inactive ,testtype is http
Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:succcess RTD OverThresholdsnumber: 0
 MessageBodyOctetsSum: 411 TargetAddress: 10.2.1.1
 DNSQueryError number: 0 HTTPError number: 0
 TcpConnError number : 0 System busy operation number:0
 DNSRTT Sum/Min/Max:0/0/0 TCPConnectRTT Sum/Min/Max: 4/1/2
 TransactionRTT Sum/Min/Max: 3/1/1
 RTT Sum/Min/Max/Avg: 7/2/3/2
 DNSServerTimeout:0 TCPConnectTimeout:0 TransactionTimeout: 0
 Lost packet ratio:0%
```

----结束

## 配置文件

### RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin http
 test-type http
```

```
destination-address ipv4 10.2.1.1
http-operation get
http-url www.huawei.com
#
return
```

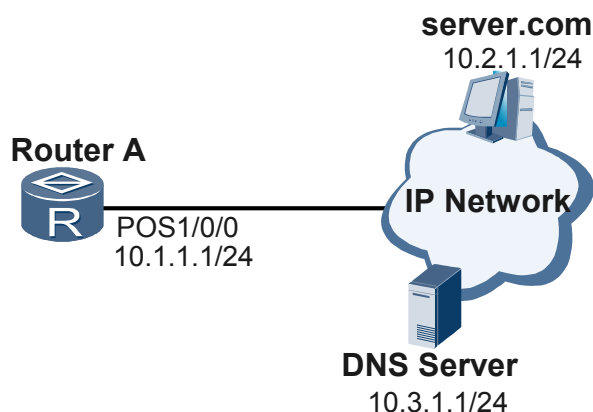
## 6.50.6 配置 DNS 测试示例

通过 DNS 测试可以检测到客户端和 DNS 服务器交付时的性能参数。

### 组网需求

如图 6-8 所示，路由器 RouterA 作为 DNS Client 端，通过域名（server.com）访问 IP 地址为 10.2.1.1/24 的主机。

图 6-8 DNS 测试组网图



### 配置思路

采用如下思路进行 DNS 解析速度的测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 DNS 测试例，测试是否可以和指定的 DNS 服务器建立连接，以及 DNS 地址解析的响应速度。

### 数据准备

为完成此配置例，需准备如下的数据：

- DNS Server 的 IP 地址
- 要访问的主机名

### 操作步骤

**步骤 1** 配置 RouterA、DNS Server 及所要访问的主机之间网络层可达（略）

**步骤 2** 配置 DNS 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] dns resolve
```

```
[RouterA] dns server 10.3.1.1
[RouterA] nqa test-instance admin dns
[RouterA-nqa-admin-dns] test-type dns
[RouterA-nqa-admin-dns] dns-server ipv4 10.3.1.1
[RouterA-nqa-admin-dns] destination-address url server.com
```

**步骤 3 启动测试操作**

```
[RouterA-nqa-admin-dns] start now
```

**步骤 4 验证测试结果**

```
[RouterA-nqa-admin-dns] display nqa results test-instance admin dns
NQA entry(admin, dns) :testFlag is inactive ,testtype is dns
1. Test 1 result The test is finished
Send operation times: 1 Receive response times: 1
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address: 10.3.1.1
Min/Max/Average Completion Time: 1/1/1
Sum/Square-Sum Completion Time: 1/1
Last Good Probe Time: 2007-7-3 10:52:5.7
Lost packet ratio: 0 %
```

----结束

**配置文件**

RouterA 的配置文件

```
#
 sysname RouterA
#
 dns resolve
 dns server 10.3.1.1
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin dns
 test-type dns
 destination-address url server.com
 dns-server ipv4 10.3.1.1
#
 ip route-static 10.3.1.0 255.255.255.0 10.1.1.2
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

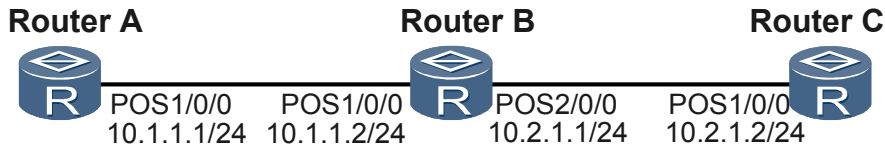
**6.50.7 配置 Traceroute 测试示例**

通过配置 Traceroute 测试可以检测到报文传输过程中客户端和报文传输路径中的设备的连通性。

**组网需求**

如图 6-9 所示，在 RouterA 上对 RouterC 接口 POS1/0/0 的 IP 地址进行 Traceroute 测试。

图 6-9 Traceroute 测试组网图



## 配置思路

采用如下思路进行 Traceroute 测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 Traceroute 测试例，测试到 RouterC 的每一跳统计信息。

## 数据准备

为完成此配置例，需准备如下的数据：

- Traceroute 测试的目的地址。

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置在 RouterA 上 Traceroute 类型的 NQA 测试例，目的地址为 10.2.1.2

```
<RouterA> system-view
[RouterA] nqa test-instance admin trace
[RouterA-nqa-admin-trace] test-type trace
[RouterA-nqa-admin-trace] destination-address ipv4 10.2.1.2
```

**步骤 3** 启动测试操作

```
[RouterA-nqa-admin-trace] start now
```

**步骤 4** 验证测试结果

# 在 RouterA 上查看 NQA 测试结果。

```
[RouterA-nqa-admin-trace] display nqa results test-instance admin trace
NQA entry(admin, trace) :testflag is inactive ,testtype is trace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2009-3-28 10:52:39.9
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1/1/1
Sum/Square-Sum Completion Time: 3/3
RTD OverThresholds number: 0
Last Good Probe Time: 2009-3-28 10:52:39.9
Destination ip address:10.1.1.2
Lost packet ratio: 0 %
2 . Hop 2
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1/1/1
Sum/Square-Sum Completion Time: 3/3
```

```
RTD OverThresholds number: 0
Last Good Probe Time: 2009-3-28 10:52:39.9
Destination ip address:10.2.1.2
Lost packet ratio: 0 %
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin trace
test-type trace
destination-address ipv4 10.2.1.2
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

## 6.50.8 配置 SNMP Query 测试示例

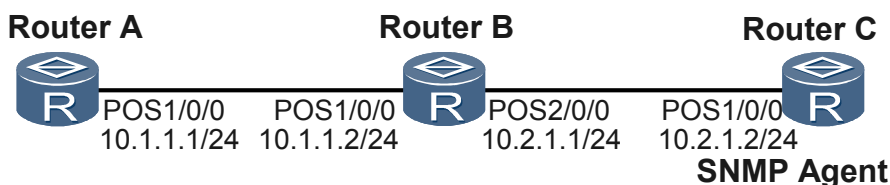
通过配置 SNMP Query 测试可以检测到客户端和网管之间通过 SNMP 通信时的性能。

### 组网需求

如图 6-10 所示。RouterC 使能 SNMP Agent，使用 NQA SNMP Query 功能测试从 RouterA 发出一个 SNMP 协议查询报文到收到响应报文所用的时间。



图 6-10 SNMP Query 测试组网图



## 配置思路

采用如下思路进行 SNMP Query 测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上创建并启动 SNMP Query 类型的测试例。
3. 在 RouterC 上使能 SNMP Agent。

## 数据准备

为完成此配置例，需准备如下的数据：

- SNMP Agent 的主机地址

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 在 RouterC 上启动 SNMP Agent 功能

```
<RouterC> system-view
[RouterC] snmp-agent
```

**步骤 3** 在 RouterA 上创建 SNMP 类型的测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin snmp
[RouterA-nqa-admin-snmp] test-type snmp
[RouterA-nqa-admin-snmp] destination-address ipv4 10.2.1.2
```

**步骤 4** 启动测试操作

```
[RouterA-nqa-admin-snmp] start now
```

**步骤 5** 验证测试结果

```
[RouterA-nqa-admin-snmp] display nqa results test-instance admin snmp
NQA entry(admin, snmp) :testFlag is inactive ,testtype is snmp
1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:0 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.2.1.2
 Min/Max/Average Completion Time: 63/172/109
 Sum/Square-Sum Completion Time: 329/42389
 Last Good Probe Time: 2006-8-5 15:33:49.1
 Lost packet ratio: 0 %
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin snmp
test-type snmp
destination-address ipv4 10.2.1.2
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100006294
snmp-agent sys-info version v3
#
return
```

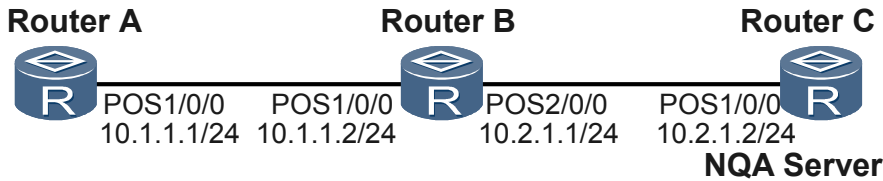
## 6.50.9 配置 TCP 测试示例

通过配置 TCP 测试可以检测到客户端和服务端之间 TCP 的连通性。

### 组网需求

如图 6-11 所示。使用 NQA TCP Private 功能测试 RouterA 到 RouterC 之间建立 TCP 连接的时间。

图 6-11 TCP 测试组网图



## 配置思路

采用如下思路进行 TCP 测试的配置：

1. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 TCP 类型的 NQA 测试例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 服务器主机地址
- 服务器端 TCP 服务的监听端口号

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 在 RouterC 上配置 NQA 服务器

# 配置 NQA 服务器 TCP 连接监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server tcpconnect 10.2.1.2 9000
```

**步骤 3** 配置 RouterA

# 使能 NQA 客户端，配置 TCP Private 类型的测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin tcp
[RouterA-nqa-admin-tcp] test-type tcp
[RouterA-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-tcp] destination-port 9000
```

**步骤 4** 启动测试

```
[RouterA-nqa-admin-tcp] start now
```

**步骤 5** 验证测试结果

```
[RouterA-nqa-admin-tcp] display nqa results test-instance admin tcp
NQA entry(admin, tcp) :testFlag is inactive ,testtype is tcp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:10.2.1.2
```

```
Min/Max/Average Completion Time: 46/63/52
Sum/Square-Sum Completion Time: 156/8294
Last Good Probe Time: 2006-8-5 15:53:17.8
Lost packet ratio: 0 %
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
nqa-server tcpconnect 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

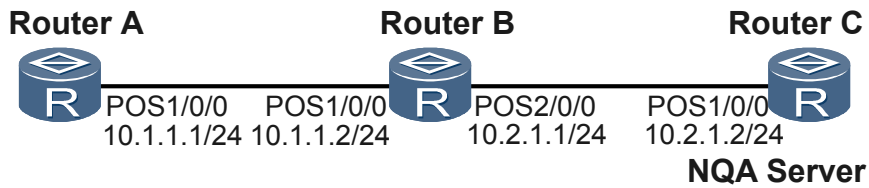
## 6.50.10 配置 UDP 测试示例

通过配置 UDP 测试可以检测到客户端和服务端之间 UDP 的连通性。

## 组网需求

如图 6-12 所示。使用 NQA UDP Public 功能测试 RouterA 与 RouterC 之间 UDP 协议报文的往返时间。

图 6-12 UDP 测试组网图



## 配置思路

采用如下思路进行 UDP 测试的配置：

1. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 UDP Public 类型的 NQA 测试例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 服务器端主机地址
- 服务器端 UDP 服务的监听端口号

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 在 RouterC 上配置 NQA 服务器

# 配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 10.2.1.2 6000
```

**步骤 3** 配置 RouterA

# 使能 NQA 客户端，配置 UDP Public 类型的测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin udp
[RouterA-nqa-admin-udp] test-type udp
[RouterA-nqa-admin-udp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-udp] destination-port 6000
```

**步骤 4** 启动测试

```
[RouterA-nqa-admin-udp] start now
```

**步骤 5** 验证测试结果

```
[RouterA-nqa-admin-udp] display nqa results test-instance admin udp
NQA entry(admin, udp) :testFlag is inactive ,testtype is udp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
```

```
Destination ip address:10.2.1.2
Min/Max/Average Completion Time: 32/109/67
Sum/Square-Sum Completion Time: 203/16749
Last Good Probe Time: 2006-8-5 16:9:21.6
Lost packet ratio: 0 %
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-port 6000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
 nqa-server udpecho 10.2.1.2 6000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

## 6.50.11 配置 Jitter 测试示例

通过配置 Jitter 测试可以检测到网络中抖动情况。

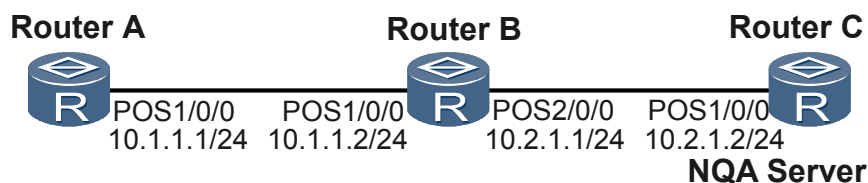
## 组网需求

如图 6-13 所示。使用 NQA Jitter 功能测试 RouterA 与 RouterC 之间传送报文的抖动时间。RouterA、RouterC 通过同步 RouterB 的时钟来保持时间的同步，从而提升测试精度。

 说明

关于时钟同步介绍请参见《HUAWEI NetEngine20E-X6 高端业务路由器 特性描述 系统管理》的“NTP”。

图 6-13 Jitter 测试组网图



## 配置思路

采用如下思路进行 Jitter 测试的配置：

1. RouterA 配置为 NTP 客户端，RouterB 为 NTP 服务器端。
2. RouterC 配置为 NTP 客户端，RouterB 为 NTP 服务器端。
3. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
4. 在 NQA 服务器上配置监听服务类型和监听端口号。
5. 在 NQA 客户端配置 Jitter 类型的 NQA 测试例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址
- 服务器端 UDP 服务的监听端口号

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置 RouterA 指定 RouterB 作为 NTP 服务器。

```
<RouterA> system-view
[RouterA] ntp-service unicast-server 10.1.1.2
```

**步骤 3** 配置 RouterC 指定 RouterB 作为 NTP 服务器。

```
<RouterC> system-view
[RouterC] ntp-service unicast-server 10.2.1.1
```

**步骤 4** 在 RouterC 上配置 NQA 服务器

# 配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
```

```
[RouterC] nqa-server udpecho 10.2.1.2 9000
```

## 步骤 5 配置 RouterA

# 使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-jitter] destination-port 9000
```

## 步骤 6 启动测试操作

```
[RouterA-nqa-admin-jitter] start now
```

## 步骤 7 验证测试结果

```
[RouterA-nqa-admin-jitter] display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
1. Test 1 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion:success RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/4/1/63 RTT Square Sum:75
 NumOfRTT:60 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:1 Min Positive DS:1
 Max Positive SD:1 Max Positive DS:3
 Positive SD Number:15 Positive DS Number:14
 Positive SD Sum:15 Positive DS Sum:16
 Positive SD Square Sum:15 Positive DS Square Sum:22
 Min Negative SD:1 Min Negative DS:1
 Max Negative SD:1 Max Negative DS:4
 Negative SD Number:16 Negative DS Number:12
 Negative SD Sum:16 Negative DS Sum:15
 Negative SD Square Sum:16 Negative DS Square Sum:27
 Min Delay SD:0 Min Delay DS:0
 Max Delay SD:2 Max Delay DS:1
 Delay SD Square Sum:4 Delay DS Square Sum:1
 Packet Loss SD:0 Packet Loss DS:0
 Packet Loss Unknown:0 Average of Jitter:1
 Average of Jitter SD:1 Average of Jitter DS:1
 jitter out value:0.0322917 jitter in value:0.0322917
 NumberOfOWD:60 Packet Loss Ratio: 0%
 OWD SD Sum:2 OWD DS Sum:1
 ICPIF value: 0 MOS-CQ value: 0
 TimeStamp unit: ms Packet Rewrite Number: 0
 Packet Rewrite Ratio: 0% Packet Disorder Number: 0
 Packet Disorder Ratio: 0% Fragment-disorder Number: 0
 Fragment-disorder Ratio: 0%
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin jitter
test-type jitter
destination-address ipv4 10.2.1.2
```



```
destination-port 9000
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
ntp-service unicast-server 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
#
nqa-server udpecho 10.2.1.2 9000
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
ntp-service unicast-server 10.2.1.1
#
return
```

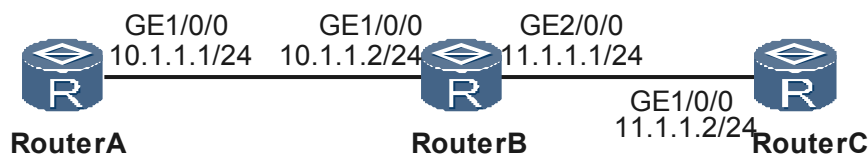
## 6.50.12 配置基于接口板发包的 Jitter 测试例

通过配置基于接口板发包的 Jitter 测试可以更加精确的检测到网络中的抖动情况。

### 组网需求

如图 6-14 所示。使用 NQA Jitter 功能测试 RouterA 与 RouterC 之间传送报文的抖动时间。通过使能接口发包功能，可以提升测试精度。

图 6-14 Jitter 测试组网图



### 配置思路

采用如下思路进行 Jitter 测试的配置：

1. RouterA 作为 NQA 客户端，RouterC 作为 NQA 服务器端。
2. 在 NQA 服务器上配置监听服务类型和监听端口号。
3. 在 NQA 客户端配置 Jitter 类型的 NQA 测试例。
4. 在 NQA 客户端配置接口板发包。

## 数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址
- 服务器端 UDP 服务的监听端口号

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 在 RouterC 上配置 NQA 服务器

# 配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 11.1.1.2 9000
```

**步骤 3** 配置 RouterA

# 使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 11.1.1.2
[RouterA-nqa-admin-jitter] destination-port 9000
```

**步骤 4** 使能接口板发包功能

```
[RouterA-nqa-admin-jitter] hardware-based enable
```

**步骤 5** 启动测试操作

```
[RouterA-nqa-admin-jitter] start now
```

**步骤 6** 验证测试结果

```
[RouterA-nqa-admin-jitter] display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testFlag is inactive ,testtype is jitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1. Test 1 result The test is finished
SendProbe:60 ResponseProbe:60
Completion :success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:0/1/1/14 RTT Square Sum:14
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:0 Min Positive DS:1
Max Positive SD:0 Max Positive DS:1
Positive SD Number:0 Positive DS Number:1
Positive SD Sum:0 Positive DS Sum:1
Positive SD Square Sum :0 Positive DS Square Sum :1
Min Negative SD:1 Min Negative DS:0
Max Negative SD:1 Max Negative DS:0
Negative SD Number:2 Negative DS Number:0
Negative SD Sum:2 Negative DS Sum:0
Negative SD Square Sum :2 Negative DS Square Sum :0
Min Delay SD:0 Min Delay DS:0
```

|                             |                             |
|-----------------------------|-----------------------------|
| Max Delay SD:0              | Max Delay DS:0              |
| Delay SD Square Sum:0       | Delay DS Square Sum:0       |
| Packet Loss SD:0            | Packet Loss DS:0            |
| Packet Loss Unknown:0       | Average of Jitter:1         |
| Average of Jitter SD:1      | Average of Jitter DS:1      |
| jitter out value:0.0295593  | jitter in value:0.0117767   |
| NumberOfOWD:60              | Packet Loss Ratio: 0%       |
| OWD SD Sum:0                | OWD DS Sum:0                |
| ICPIF value: 0              | MOS-CQ value: 0             |
| TimeStamp unit: ms          | Packet Rewrite Number: 0    |
| Packet Rewrite Ratio: 0%    | Packet Disorder Number: 0   |
| Packet Disorder Ratio: 0%   | Fragment-disorder Number: 0 |
| Fragment-disorder Ratio: 0% |                             |

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 11.1.1.2
 destination-port 9000
 hardware-based enable
#
 ip route-static 11.1.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.1.2 255.255.255.0
#
nqa-server udpecho 11.1.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 11.1.1.1
#
return
```

## 6.50.13 配置普通隧道 LSP Ping 测试示例

通过普通隧道 LSP Ping 测试可以检测 LSP 隧道的各个 LSR 之间的连通性。

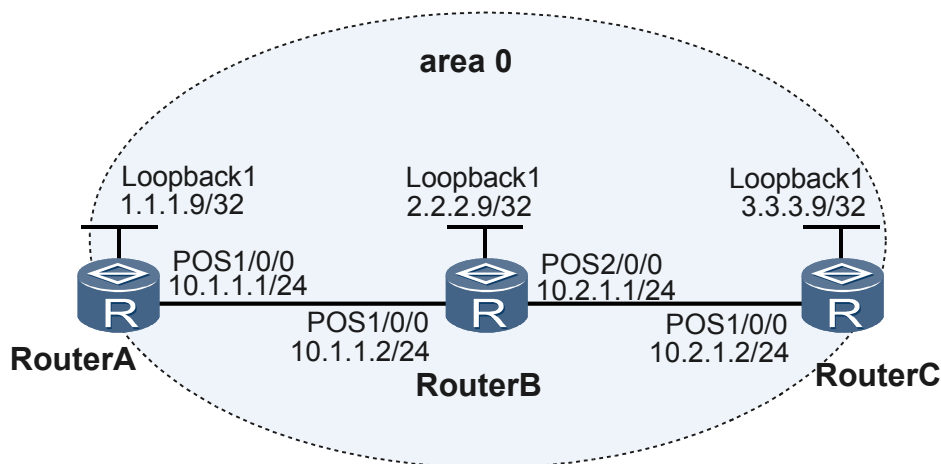
## 组网需求

如图 6-15 所示。

- RouterA、RouterB、RouterC 都运行 OSPF 协议，并学习到彼此 Loopback 接口的 32 位主机路由。
- RouterA、RouterB、RouterC 上都启用 MPLS 和 MPLS LDP。
- RouterA、RouterB、RouterC 之间的 POS 接口都启用 MPLS 和 MPLS LDP，正确触发 LDP LSP 的建立。

使用 NQA LSP Ping 功能测试 RouterA 与 RouterC 之间的 LSP 连通性状态。

图 6-15 LSP Ping 测试组网图



## 配置思路

采用如下思路进行 LSPPing 测试的配置：

1. RouterA 做为 NQA 客户端。
2. RouterC 做为 NQA 服务器端。
3. 在 RouterA 上建立 LSPPing 测试用例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址及掩码

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置 RouterA

# 使能 NQA 客户端，配置普通隧道的 LSP Ping 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin lsping
```

```
[RouterA-nqa-admin-lspping] test-type lspping
[RouterA-nqa-admin-lspping] lsp-type ipv4
[RouterA-nqa-admin-lspping] destination-address ipv4 3.3.3.9 lsp-masklen 32
```

### 步骤3 启动测试操作

```
[RouterA-nqa-admin-lspping] start now
```

### 步骤4 验证测试结果

```
[RouterA-nqa-admin-lspping] display nqa results test-instance admin lspping
NQA entry(admin, lspping) :testFlag is inactive ,testtype is lspping
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:3.3.3.9
Min/Max/Average Completion Time: 1/1/1
Sum/Square-Sum Completion Time: 3/3
Last Good Probe Time: 2007-1-30 15:32:56.1
Lost packet ratio:0%
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
nqa test-instance admin lspping
test-type lspping
destination-address ipv4 3.3.3.9 lsp-masklen 32
#
return
```

### ● RouterB 的配置文件

```
#
sysname RouterB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
```

```
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
undo shutdown
link-protocol ppp
ip address 10.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.255
#
Return
```

## 6.50.14 配置普通隧道 LSP Jitter 测试示例

通过普通隧道 LSP Jitter 测试可以检测报文在 LSP 隧道中传输时的抖动情况。

### 组网需求

如图 6-15 示。

- RouterA、RouterB、RouterC 都运行 OSPF 协议，并学习到彼此 Loopback 接口的 32 位主机路由。
- RouterA、RouterB、RouterC 上都启用 MPLS 和 MPLS LDP。
- RouterA、RouterB、RouterC 之间的 POS 接口都启用 MPLS 和 MPLS LDP，正确触发 LDP LSP 的建立。

要求使用 NQA LSP Ping 功能测试 RouterA 与 RouterC 之间的 LSP 连通性状态。

## 配置思路

采用如下思路进行 Lspjitter 测试的配置:

1. RouterA 做为 NQA 客户端。
2. RouterC 做为 NQA 服务器端。
3. 在 RouterA 上建立 LSPJitter 测试用例。

## 数据准备

为完成此配置例, 需准备如下数据:

- 服务器端的主机地址及掩码

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达 (略)

**步骤 2** 配置 RouterA、RouterB 和 RouterC 之间 LDP (略)

配置 LDP 的步骤请参考 HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-MPLS》

**步骤 3** 配置 RouterA 为 NQA 客户端

# 使能 NQA 客户端, 配置 LDP LSP 的 Ping 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin lspjitter
[RouterA-nqa-admin-lspjitter] test-type lspjitter
[RouterA-nqa-admin-lspjitter] lsp-type ipv4
[RouterA-nqa-admin-lspjitter] destination-address ipv4 3.3.3.9 lsp-masklen 32 lsp-loopback 127.0.0.1
```

**步骤 4** 启动测试操作

```
[RouterA-nqa-admin-lspjitter] start now
```

**步骤 5** 验证测试结果

```
[RouterA-nqa-admin-lspjitter] display nqa results test-instance admin lspjitter
 SendProbe:60 ResponseProbe:60
 Completion :success RTD OverThresholds number:0
 Min/Max/Avg/Sum RTT:1/1/1/60 RTT Square Sum:60
 NumOfRTT:60 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:0 Max Positive SD:0
 Positive SD Number:0 Positive SD Sum:0
 Positive SD Square Sum :0 Min Negative SD:0
 Max Negative SD:1 Negative SD Number:1
 Negative SD Sum:1 Negative SD Square Sum :1
 Packet Loss Unknown:0 Average of Jitter SD:1
 jitter out value:0.0162967 Lost packet ratio:0%
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
mpls lsr-id 1.1.1.9
mpls
```

```
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
nqa test-instance admin lspjitter
test-type lspjitter
destination-address ipv4 3.3.3.9 lsp-masklen 32 lsp-loopback 127.0.0.1
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
undo shutdown
link-protocol ppp
ip address 10.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
```



```
ip address 10.2.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.255
#
Return
```

## 6.50.15 配置 TE 隧道 LSP Jitter 测试示例

通过普通隧道 LSP Jitter 测试可以检测报文在 TE 隧道中传输时的抖动情况。

### 组网需求

如图 6-15 所示。

- Router A、Router B、Router C 都运行 OSPF 协议，并学习到彼此 Loopback 接口的 32 位主机路由。
- Router A、Router B、Router C 上都启用 MPLS、MPLS TE 和 MPLS RSVP-TE。
- Router A、Router B、Router C 之间的 POS 接口都启用 MPLS、MPLS TE 和 MPLS RSVP-TE，建立一条从 Router A 到 Router C 的 TE 隧道。

使用 NQA LSP Jitter 功能测试 TE 隧道。

### 配置思路

采用如下思路进行 LSP Jitter 测试的配置：

1. RouterA 做为 NQA 客户端，在 RouterA 上建立 LSP Jitter 测试用例。
2. RouterC 做为 NQA 服务器端。

### 数据准备

为完成此配置例，需准备如下数据：

- MPLS TE 隧道接口

### 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置 RouterA、RouterB 和 RouterC 的 MPLS RSVP-TE（略）

**步骤 3** 配置 RouterA 上建立到 RouterC 的 TE 隧道（略）

配置 MPLS RSVP-TE 的步骤请参考 HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-MPLS》

**步骤 4** 配置 RouterA 的 NQA 测试例

# 使能 NQA 客户端，配置 TE 隧道的 LSP Jitter 测试例。

```
<RouterA> system-view
```

```
[RouterA] nqa test-instance admin lspjitter
[RouterA-nqa-admin-lspjitter] test-type lspjitter
[RouterA-nqa-admin-lspjitter] lsp-type te
[RouterA-nqa-admin-lspjitter] lsp-tetunnel tunnel 1/0/0
```

**步骤 5 启动测试操作**

```
[RouterA-nqa-admin-lspjitter] start now
```

**步骤 6 验证测试结果**

```
[RouterA-nqa-admin-lspjitter] display nqa results test-instance admin lspjitter
SendProbe:60 ResponseProbe:60
Completion :success RTD OverThresholds number:0
Min/Max/Avg/Sum RTT:1/1/1/60 RTT Square Sum:60
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:0 Max Positive SD:0
Positive SD Number:0 Positive SD Sum:0
Positive SD Square Sum :0 Min Negative SD:0
Max Negative SD:1 Negative SD Number:1
Negative SD Sum:1 Negative SD Square Sum :1
Packet Loss Unknown:0 Average of Jitter SD:1
jitter out value:0.0162967
```

----结束

**配置文件**

## ● RouterA 的配置文件

```
#
sysname RouterA
#
mpls lsr-id 1.1.1.9
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 5000
mpls rsvp-te
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.9
mpls te tunnel-id 100
mpls te bandwidth ct0 3000
mpls te commit
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
mpls-te enable
#
nqa test-instance admin lspjitter
```

```
test-type lspjitter
lsp-type te
lsp-tetunnel Tunnel1/0/0
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
mpls lsr-id 2.2.2.9
mpls
mpls te
mpls rsvp-te
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 5000
mpls rsvp-te
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth bc0 5000
mpls rsvp-te
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
mpls-te enable
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
mpls lsr-id 3.3.3.9
mpls
mpls te
mpls rsvp-te
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 5000
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
```

```
opaque-capability enable
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.255
mpls-te enable
#
return
```

## 6.50.16 配置 ICMP Jitter 测试示例

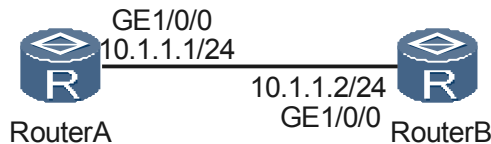
通过 ICMP Jitter 测试可以检测到网络中的抖动情况。ICMP Jitter 测试不需要配置服务器端，测试的对端设备可以是非华为设备。

### 组网需求

如图 6-16 所示。

RouterA 作为 NQA 客户端，测试与 RouterB 之间网络的抖动情况。

图 6-16 ICMP Jitter 测试组网图



### 配置思路

采用如下思路进行 ICMP Jitter 测试的配置：

1. RouterA 做为 NQA 客户端，在 RouterA 上建立 ICMP Jitter 测试用例。
2. RouterB 做为 NQA 服务器端。

### 数据准备

为完成此配置例，需准备如下数据：

- RouterB 的 IP 地址

### 操作步骤

**步骤 1** 配置 RouterA 和 RouterB 之间可达（略）

**步骤 2** 配置 RouterA 的 NQA 测试例

# 使能 NQA 客户端，配置 ICMP Jitter 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin icmpjitter
[RouterA-nqa-admin-icmpjitter] test-type icmpjitter
[RouterA-nqa-admin-icmpjitter] destination-address ipv4 10.1.1.2
```

**步骤 3** 启动测试操作

```
[RouterA-nqa-admin-icmpjitter] start now
```

#### 步骤4 验证测试结果

```
[RouterA-nqa-admin-icmpjitter] display nqa results test-instance admin icmpjitter
NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1. Test 1 result The test is finished
SendProbe:60 ResponseProbe:60
Completion :success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:1/3/1/65 RTT Square Sum:77
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:1 Min Positive DS:1
Max Positive SD:3 Max Positive DS:1
Positive SD Number:18 Positive DS Number:15
Positive SD Sum:22 Positive DS Sum:15
Positive SD Square Sum :32 Positive DS Square Sum :15
Min Negative SD:1 Min Negative DS:1
Max Negative SD:2 Max Negative DS:1
Negative SD Number:21 Negative DS Number:14
Negative SD Sum:22 Negative DS Sum:14
Negative SD Square Sum :24 Negative DS Square Sum :14
Min Delay SD:0 Min Delay DS:0
Max Delay SD:1 Max Delay DS:1
Delay SD Square Sum:4 Delay DS Square Sum:1
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:1
Average of Jitter SD:1 Average of Jitter DS:1
jitter out value:0.5599658 jitter in value:0.3574005
NumberOfOWD:60 Packet Loss Ratio: 0%
OWD SD Sum:4 OWD DS Sum:1
ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin icmpjitter
test-type icmpjitter
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
return
```

## 6.50.17 配置基于接口板发包的 ICMP Jitter 测试例

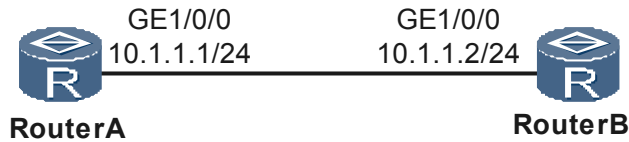
通过基于接口板发送的 ICMP Jitter 测试可以检测到更加准确的网络抖动情况。

## 组网需求

如图 6-17 所示。

RouterA 作为 NQA 客户端，测试与 RouterB 之间网络的抖动情况。使能接口板发包功能，可以提高测试的精度。

图 6-17 基于接口板发包的 ICMP Jitter 测试组网图



## 配置思路

采用如下思路进行 ICMP Jitter 测试的配置：

1. RouterA 做为 NQA 客户端，在 Router A 上建立 ICMP Jitter 测试用例。
2. RouterB 做为 NQA 服务器端。
3. 在 RouterA 上使能接口板发包的功能。

## 数据准备

为完成此配置例，需准备如下数据：

- RouterA、RouterB 的 IP 地址

## 操作步骤

**步骤 1** 配置 RouterA 和 RouterB 之间可达（略）

**步骤 2** 配置 RouterB 作为 ICMP 服务器。

```
配置 ICMP 服务器地址。
<RouterB> system-view
[RouterB] nqa-server icmp-server 10.1.1.2
```

**步骤 3** 配置 RouterA 的 NQA 测试例

```
使能 NQA 客户端，配置 ICMP Jitter 测试例。
<RouterA> system-view
[RouterA] nqa test-instance admin icmpjitter
[RouterA-nqa-admin-icmpjitter] test-type icmpjitter
[RouterA-nqa-admin-icmpjitter] destination-address ipv4 10.1.1.2
```

**步骤 4** 使能接口板发包功能

```
[RouterA-nqa-admin-icmpjitter] hardware-based enable
```

**步骤 5** 启动测试操作

```
[RouterA-nqa-admin-icmpjitter] start now
```

**步骤 6** 验证测试结果

```
<HUAWEI> display nqa results test-instance admin icmpjitter
```

```

NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1. Test 1 result The test is finished
SendProbe:60 ResponseProbe:60
Completion :success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:0/1/1/14 RTT Square Sum:14
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:0 Min Positive DS:1
Max Positive SD:0 Max Positive DS:1
Positive SD Number:0 Positive DS Number:1
Positive SD Sum:0 Positive DS Sum:1
Positive SD Square Sum :0 Positive DS Square Sum :1
Min Negative SD:1 Min Negative DS:0
Max Negative SD:1 Max Negative DS:0
Negative SD Number:2 Negative DS Number:0
Negative SD Sum:2 Negative DS Sum:0
Negative SD Square Sum :2 Negative DS Square Sum :0
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:1
Average of Jitter SD:1 Average of Jitter DS:1
jitter out value:0.0295593 jitter in value:0.0117767
NumberOfOWD:60 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%

```

----结束

## 配置文件

- RouterA 的配置文件

```

#
sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin icmpjitter
 test-type icmpjitter
 destination-address ipv4 10.1.1.2
 hardwar-based enable
#
return

```

- RouterB 的配置文件

```

#
sysname RouterB
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
nqa-server icmp-server 100.1.1.200
#
return

```

## 6.50.18 配置 Path Jitter 测试示例

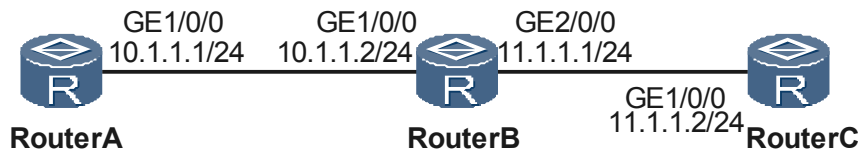
通过 Path Jitter 测试可以检测到报文在传输路径中的抖动情况。

### 组网需求

如图 6-18 所示。

RouterA 作为 NQA 客户端，测试与 RouterC 之间网络的抖动情况。

图 6-18 ICMP Jitter 测试组网图



### 配置思路

采用如下思路进行 Path Jitter 测试的配置：

1. RouterA 做为 NQA 客户端，在 Router A 上建立 Path Jitter 测试用例。
2. RouterC 做为 NQA 服务器端。

### 数据准备

为完成此配置例，需准备如下数据：

- RouterA、RouterB 和 RouterC 的 IP 地址

### 操作步骤

**步骤 1** 配置 RouterA 和 RouterC 之间可达（略）

**步骤 2** 配置 RouterA 的 NQA 测试例

# 使能 NQA 客户端，配置 Path Jitter 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin pathjitter
[RouterA-nqa-admin-pathjitter] test-type pathjitter
[RouterA-nqa-admin-pathjitter] destination-address ipv4 11.1.1.2
[RouterA-nqa-admin-pathjitter] icmp-jitter-mode icmp-echo
```

**步骤 3** 启动测试操作

```
[RouterA-nqa-admin-pathjitter] start now
```

**步骤 4** 验证测试结果

```
[RouterA-nqa-admin-pathjitter] display nqa results test-instance admin pathjitter
NQA entry(admin, pathjitter) ::testflag is inactive ,testtype is pathjitter
Current Status:CLOSE
1. Test 1 result The test is finished
Trace Completion Status:succcess
1. Hop 1
```



```

Destination ip address:10.1.1.2
Jitter Completion Status:succcess Jitter Finish Status:finished
SendProbe:60 ResponseProbe:60
Min/Max/Avg/Sum RTT:1/5/1/73 RTT Square Sum:111
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:1 Min Positive DS:2
Max Positive SD:1 Max Positive DS:2
Positive SD Number:10 Positive DS Number:1
Positive SD Sum:10 Positive DS Sum:2
Positive SD Square Sum :10 Positive DS Square Sum :4
Min Negative SD:0 Min Negative DS:0
Max Negative SD:0 Max Negative DS:0
Negative SD Number:0 Negative DS Number:0
Negative SD Sum:0 Negative DS Sum:0
Negative SD Square Sum :0 Negative DS Square Sum :0
Max Delay SD:2 Max Delay DS:3
Average of Jitter:1 NumberOfOWD:60
Average of Jitter SD:1 Average of Jitter DS:2
jitter out value:0.0861913 jitter in value:0.0189286
OWD SD Sum:11 OWD DS Sum:62
2 . Hop 2
Destination ip address:11.1.1.2
Jitter Completion Status:succcess Jitter Finish Status:finished
SendProbe:60 ResponseProbe:60
Min/Max/Avg/Sum RTT:2/14/3/170 RTT Square Sum:634
NumOfRTT:60 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:1 Min Positive DS:1
Max Positive SD:6 Max Positive DS:6
Positive SD Number:4 Positive DS Number:18
Positive SD Sum:9 Positive DS Sum:24
Positive SD Square Sum :39 Positive DS Square Sum :56
Min Negative SD:0 Min Negative DS:0
Max Negative SD:0 Max Negative DS:0
Negative SD Number:0 Negative DS Number:0
Negative SD Sum:0 Negative DS Sum:0
Negative SD Square Sum :0 Negative DS Square Sum :0
Max Delay SD:7 Max Delay DS:7
Average of Jitter:1 NumberOfOWD:60
Average of Jitter SD:2 Average of Jitter DS:1
jitter out value:0.0946116 jitter in value:0.2699488
OWD SD Sum:70 OWD DS Sum:100

```

----结束

## 配置文件

### ● RouterA 的配置文件

```

#
sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
ospf 2
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
nqa test-instance admin pathjitter
 test-type pathjitter
 destination-address ipv4 11.1.1.2
 icmp-jitter-mode icmp-echo
#
return

```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
#
ospf 11
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 11.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 11.1.1.0 0.0.0.255
#
return
```

## 6.50.19 配置 Path MTU 测试示例

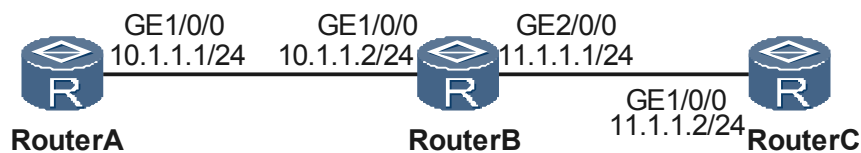
通过 Path MTU 测试可以检测到报文在传输路径中的 MTU。

### 组网需求

如图 6-19 所示。

RouterA 作为 NQA 客户端，测试与 RouterC 之间路径 MTU。

图 6-19 Path MTU 测试组网图



### 配置思路

采用如下思路进行 Path MTU 测试的配置：

1. RouterA 做为 NQA 客户端，在 Router A 上建立 Path MTU 测试用例。

2. RouterC 做为 NQA 服务器端。

## 数据准备

为完成此配置例，需准备如下数据：

- RouterA、RouterB 和 RouterC 的 IP 地址

## 操作步骤

**步骤 1** 配置 RouterA 和 RouterC 之间可达（略）

**步骤 2** 配置 RouterA 的 NQA 测试例

# 使能 NQA 客户端，配置 Path MTU 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin pathmtu
[RouterA-nqa-admin-pathmtu] test-type pathmtu
[RouterA-nqa-admin-pathmtu] destination-address ipv4 11.1.1.2
```

**步骤 3** 启动测试操作

```
[RouterA-nqa-admin-pathmtu] start now
```

**步骤 4** 验证测试结果

```
[RouterA-nqa-admin-pathmtu] display nqa results test-instance admin pathmtu
NQA entry(admin, pathmtu) ::testflag is inactive ,testtype is pathmtu
 1. Test 0 result The test is finished
 Completions: success Busies: 0
 Destination-address: 11.1.1.2 Discovery field min: 48 byte
 Discovery field max: 1500 byte Drops: 0
 MTU: 1492 Response probe: 41
 Send probe: 47 Optimum first step: 38 byte
 Second step: 10 byte Timeouts: 6
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
ospf 2
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
nqa test-instance admin pathmtu
 test-type pathmtu
 destination-address ipv4 11.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 undo shutdown
```

```
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
#
ospf 11
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 11.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 11.1.1.0 0.0.0.255
#
return
```

## 6.50.20 配置 TE 隧道 LSP Traceroute 测试示例

通过 TE 隧道 LSP Traceroute 测试可以检测到 TE 隧道中的各个 LSR 的连通性。

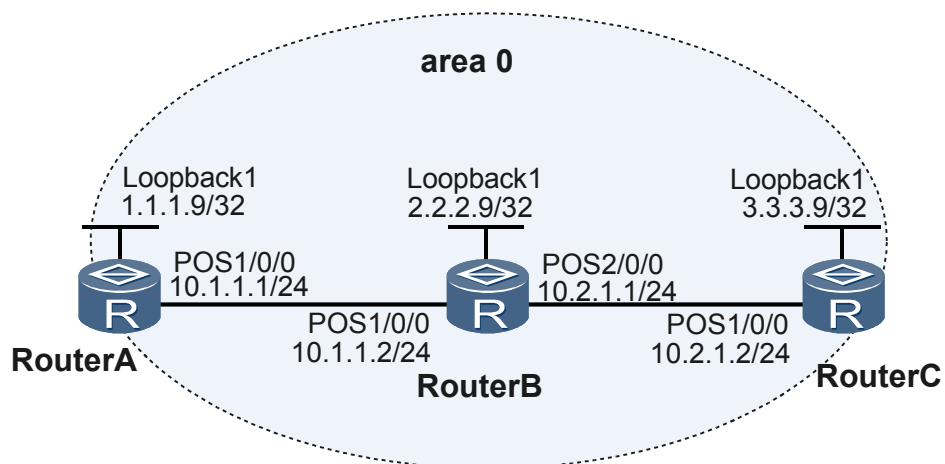
### 组网需求

如图 6-20 所示。

- RouterA、RouterB、RouterC 都运行 OSPF 协议，并学习到彼此 Loopback 接口的 32 位主机路由。
- RouterA、RouterB、RouterC 上都启用 MPLS、MPLS TE 和 MPLS RSVP-TE。
- RouterA、RouterB、RouterC 之间的 POS 接口都启用 MPLS、MPLS TE 和 MPLS RSVP-TE，建立一条从 RouterA 到 RouterC 的 TE 隧道。

使用 NQA LSP Traceroute 功能测试 TE 隧道。

图 6-20 LSP Traceroute 测试组网图



## 配置思路

采用如下思路进行 LSP Traceroute 测试的配置：

1. RouterA 做为 NQA 客户端，在 RouterA 上建立 LSP Traceroute 测试用例。
2. RouterC 做为 NQA 服务器端。

## 数据准备

为完成此配置例，需准备如下的数据：

- lsp-tetunnel tunnel 接口编号

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置 RouterA、RouterB 和 RouterC 的 MPLS RSVP-TE（略）

**步骤 3** 配置 RouterA 上建立到 RouterC 的 TE 隧道（略）

配置 MPLS RSVP-TE 的步骤请参考 HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-MPLS》

**步骤 4** 配置 RouterA 的 NQA 测试例

# 使能 NQA 客户端，配置 TE 隧道的 LSP Traceroute 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin lsptracert
[RouterA-nqa-admin-lsptracert] test-type lsptracert
[RouterA-nqa-admin-lsptracert] lsp-type te
[RouterA-nqa-admin-lsptracert] lsp-tetunnel tunnel 1/0/0
```

**步骤 5** 启动测试操作

```
[RouterA-nqa-admin-lspjitter] start now
```

**步骤 6** 验证测试结果

```
[RouterA-nqa-admin-lspjitter] display nqa results test-instance admin lspjitter
NQA entry(admin, lsptrace) :testFlag is inactive ,testtype is lsptrace
1 . Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2006-8-24 11:22:21.2
1 . Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 1050/1090/1053
 Sum/Square-Sum Completion Time: 3160/3331000
 RTD OverThresholds number: 0
 Last Good Probe Time: 2006-8-24 11:22:17.2
 Destination ip address:10.1.1.2
2 . Hop 2
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 1050/1490/1323
 Sum/Square-Sum Completion Time: 3970/5367500
 RTD OverThresholds number: 0
 Last Good Probe Time: 2006-8-24 11:22:21.2
```

Destination ip address:3.3.3.9

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
 sysname RouterA
#
 mpls lsr-id 1.1.1.9
 mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth 5000
 mpls rsvp-te
#
 interface LoopBack1
 undo shutdown
 ip address 1.1.1.9 255.255.255.255
#
 interface Tunnel1/0/0
 undo shutdown
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.9
 mpls te tunnel-id 100
 mpls te bandwidth ct0 3000
 mpls te commit
#
 ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 1.1.1.9 0.0.0.0
 mpls-te enable
#
 nqa test-instance admin lspjitter
 test-type lspjitter
 lsp-type te
 lsp-tetunnel Tunnel1/0/0
#
return
```

### ● RouterB 的配置文件

```
#
 sysname RouterB
#
 mpls lsr-id 2.2.2.9
 mpls
 mpls te
 mpls rsvp-te
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
```

```
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth 5000
mpls rsvp-te
#
interface Pos2/0/0
 link-protocol ppp
undo shutdown
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth 5000
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 2.2.2.9 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.2.1.0 0.0.0.255
 mpls-te enable
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
mpls lsr-id 3.3.3.9
mpls
 mpls te
 mpls rsvp-te
#
interface Pos1/0/0
 link-protocol ppp
undo shutdown
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth 5000
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 10.2.1.0 0.0.0.255
 mpls-te enable
#
Return
```

## 6.50.21 配置检测网段中的保留组成员示例

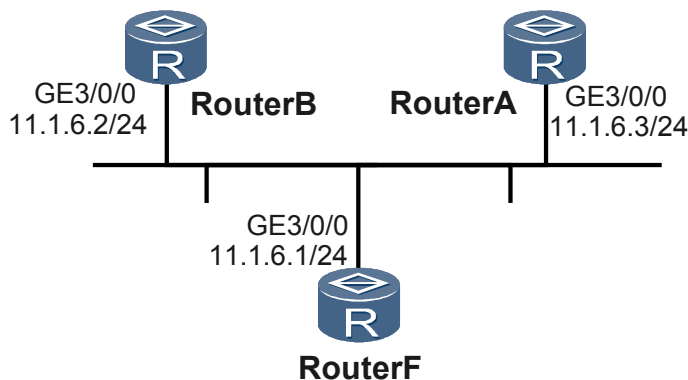
通过检测网段中的保留组成员可以检测出接口所在网段上存在哪些保留组成员。

### 组网需求

如图 6-21 所示，Router A、Router B 和 Router F 连接在同一个共享网段上。Router A 连接该网段的接口上运行 OSPF。需求：检测该网段上还存在哪些 OSPF IGP 路由器。

解决方案：保留组播组 224.0.0.5 代表网段上所有 OSPF IGP 路由器。执行 mping 功能，可以检测指定网段上是否存在保留组地址所代表的网络设备。

图 6-21 mping 保留组地址组网图



## 配置思路

本例中采用的配置思路如下：

1. 将 Router A 作为 NQA Client，配置 NQA mping 测试例：组地址为 224.0.0.5，出接口为 GE3/0/0。
2. 查看配置效果。
3. 启动测试例，验证检测结果。如果 Router A 接收到 RouterB 和 Router F 的回应报文，表明 Router B 和 Router F 上的相应接口也运行了 OSPF。

## 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mping
- 保留组地址：224.0.0.5

## 操作步骤

### 步骤 1 在 Router A 上配置 NQA mping 测试例

```
<HUAWEI> sysname Router A
[RouterA] nqa test-instance admin mping
[RouterA-nqa-admin-mping] test-type mping
[RouterA-nqa-admin-mping] destination-address ipv4 224.0.0.5
[RouterA-nqa-admin-mping] source-interface gigabitethernet 3/0/0
```

### 步骤 2 验证配置结果。

```
[RouterA-nqa-admin-mping] display nqa-agent verbose

NQA Tests Max:2000 NQA Tests Number: 4
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance admin mping,
test-type mping,
destination-address ipv4 224.0.0.5,
```



```
source-interface GigabitEthernet3/0/0,
nqa status : normal
```

### 步骤 3 启动测试例

```
[RouterA-nqa-admin-mping] start now
```

### 步骤 4 验证检测结果

检测结果显示，该网段上还存在着两个 224.0.0.5 的组成员：11.1.6.2（Router B）和 11.1.6.1（Router F）。这表明 RTB 和 RTF 上的相应接口也运行了 OSPF。

```
[RouterA-nqa-admin-mping] display nqa results test-instance admin mping
NQA entry (admin, mping) :testflag is inactive ,testtype is mping
1 . Test 1 result The test is finished
Completion:success Timeouts number: 0
Drops number: 0 TargetAddress: 224.0.0.5
ProbeResponses number: 3 SentProbes number: 3
Busies: 0
1 . Receiver 1
CompletionTime Min/Max/Sum: 10/80/100
Sum2CompletionTime: 6600
LastGoodProbe time: 2007-1-20 11:6:40.2
RecevierAddress: 11.1.6.2
2 . Receiver 2
CompletionTime Min/Max/Sum: 10/80/130
Sum2CompletionTime: 8100
LastGoodProbe time: 2007-1-20 11:6:40.2
RecevierAddress: 11.1.6.1
```

----结束

## 配置文件

Router A 的配置文件如下：

```

sysname RouterA

interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.3 255.255.255.0

ospf 1
area 0.0.0.0
network 11.1.6.0 0.0.0.255

nqa admin mping
test-type mping
destination-address ipv4 224.0.0.5
source-interface GigabitEthernet3/0/0

return
```

Router B 的配置文件如下：

```

sysname RouterB

interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.2 255.255.255.0

ospf 1
area 0.0.0.0
network 11.1.6.0 0.0.0.255

return
```

Router F 的配置文件如下：

```
#
 sysname RouterF
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.6.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 11.1.6.0 0.0.0.255
#
return
```

## 6.50.22 配置检测网络承载组播业务的性能示例

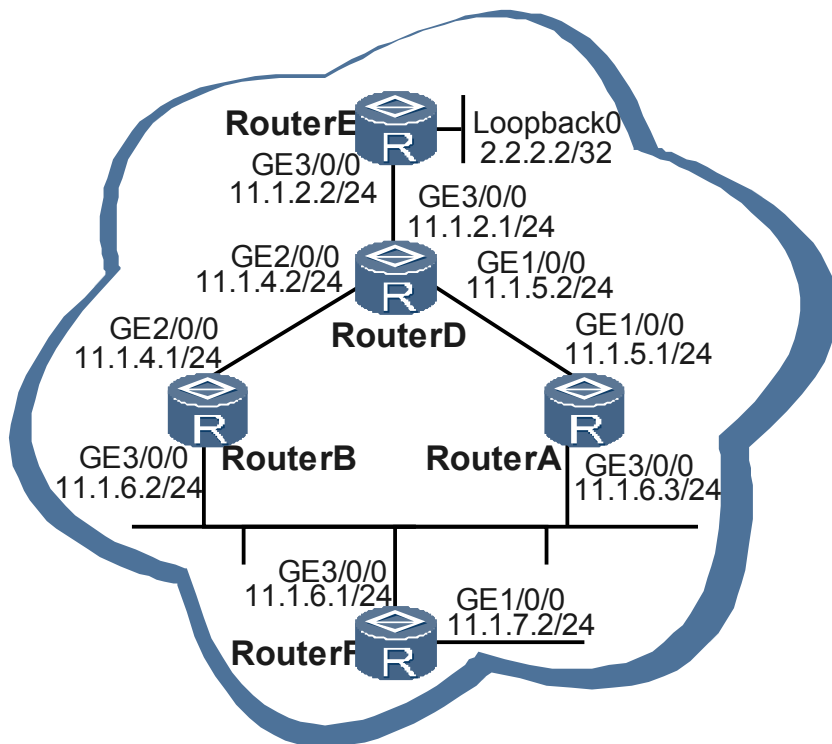
检测网络承载组播业务的性能，可以查看检查协议运行状态是否正常，确认组播分发树是否正确建立；检查网络中存在的组成员，计算从 MPing 发起者到组成员的 TTL、响应时间等参数。

### 组网需求

如图 6-22 所示，各路由器之间运行 OSPF，单播路由正常。网络中新部署了 PIM-DM 组播功能。需求：检测各路由器能否正常处理组播数据。

解决方案：使用 mping（普通组地址），构造一定流量的组播数据，触发组播分发树的建立。同时检查各个路由器上是否存在正确的组播路由表项。使用 NQA MPing 测试例实现 MPing 功能。

图 6-22 MPing 普通组地址组网图



## 配置思路

本例中采用的配置思路如下。

1. 在 RouterF 的接口 GE1/0/0 静态加入组播组 225.0.0.1。
2. 将 RouterE 作为 NQA Client，配置 MPing 测试例：组地址为 225.0.0.1。
3. 查看配置结果。
4. 启动测试例，验证检测结果。
5. 检查各个路由器上的组播路由表项是否正确建立，验证组播转发树是否正确建立。

## 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mping
- 普通组地址：225.0.0.1

## 操作步骤

### 步骤 1 在 RouterF 的接口 GE1/0/0 静态加入组播组 225.0.0.1

```
<RouterF> system-view
[RouterF] interface gigabitethernet 1/0/0
[RouterF-GigabitEthernet1/0/0] igmp enable
[RouterF-GigabitEthernet1/0/0] igmp static-group 225.0.0.1
```

### 步骤 2 在 RouterE 上配置 NQA mping 测试例

```
<RouterE> system-view
[RouterE] nqa test-instance admin mping
[RouterE-nqa-admin-mping] test-type mping
[RouterE-nqa-admin-mping] destination-address ipv4 225.0.0.1
```

### 步骤 3 查看配置结果

```
[RouterE-nqa-admin-mping] display nqa-agent verbose
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance admin mping
test-type mping
destination-address ipv4 225.0.0.1
nqa status : normal
```

### 步骤 4 启动测试例

```
[RouterE-nqa-admin-mping] start now
```

### 步骤 5 验证测试结果

# 查看存在的保留组成员。根据收到探针查看到存在的保留组成员。

```
[RouterE-nqa-admin-mping] display nqa results test-instance admin mping
NQA entry(admin, mping) :testflag is active ,testtype is mping
 1. Test 1 result The test is running
 Completion:finish Timeouts number: 3
 Drops number: 0 TargetAddress: 225.0.0.1
 ProbeResponses number: 0 SentProbes number: 3
 Busies: 0
```

### 步骤 6 验证路由器上的路由表项

# RouterE 的组播转发表项，可以看到在 RouterE 建立了(11.1.0.2, 225.0.0.1)表项，组播数据从 loopback 口发出。

```
<RouterE> display pim routing-table
Vpn-instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
(11.1.0.2, 225.0.0.1)
 Protocol: pim-dm, Flag: LOC
 UpTime: 00:05:41
 Upstream interface: looback0
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet3/0/0
 Protocol: pim-dm, UpTime: 00:04:27, Expires: never
```

# RouterD 的组播转发表项，可以看到在 RouterD 收到组播数据报文后建立了(11.1.0.2, 225.0.0.1)表项，上游接口是 GigabitEthernet3/0/0。

```
<RouterD> display pim routing-table
Vpn-instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
(11.1.0.2, 225.0.0.1)
 Protocol: pim-dm, Flag:
 UpTime: 00:06:23
 Upstream interface: GigabitEthernet3/0/0
 Upstream neighbor: 11.1.2.2
 RPF prime neighbor: 11.1.2.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet2/0/0
 Protocol: pim-dm, UpTime: 00:05:09, Expires: never
```

# RouterA 的组播转发表项，可以看到在 RouterA 收到组播数据报文后建立了(11.1.0.2, 225.0.0.1)表项，上游接口是 GigabitEthernet3/0/0。

```
<RouterA> display pim routing-table
Vpn-instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
(11.1.0.2, 225.0.0.1)
 Protocol: pim-dm, Flag: ACT
 UpTime: 00:01:23
 Upstream interface: GigabitEthernet3/0/0
 Upstream neighbor: 11.1.6.2
 RPF prime neighbor: 11.1.6.2
 Downstream interface(s) information: None
```

# RouterB 的组播转发表项，可以看到在 RouterB 收到组播数据报文后建立了(11.1.0.2, 225.0.0.1)表项，上游接口是 GigabitEthernet2/0/0。

```
<RouterB> display pim routing-table
Vpn-instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
(11.1.0.2, 225.0.0.1)
 Protocol: pim-dm, Flag: ACT
 UpTime: 00:02:44
 Upstream interface: GigabitEthernet2/0/0
 Upstream neighbor: 11.1.4.2
 RPF prime neighbor: 11.1.4.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet3/0/0
 Protocol: pim-dm, UpTime: 00:01:30, Expires: never
```

# RouterF 的组播转发表项，可以看到在 RouterF 收到组播数据报文后建立了(11.1.0.2, 225.0.0.1)表项，上游接口是 GigabitEthernet3/0/0。

```
<RouterF> display pim routing-table
Vpn-instance: public net
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.0.0.1)
```

```

Protocol: pim-dm, Flag: WC
UpTime: 00:06:36
Upstream interface: NULL
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
 1: GigabitEthernet1/0/0
 Protocol: igmp, UpTime: 00:06:36, Expires: never
(11.1.0.2, 225.0.0.1)
Protocol: pim-dm, Flag: ACT
UpTime: 00:03:40
Upstream interface: GigabitEthernet3/0/0
 Upstream neighbor: 11.1.6.2
 RPF prime neighbor: 11.1.6.2
Downstream interface(s) information:
Total number of downstreams: 1
 1: GigabitEthernet1/0/0
 Protocol: pim-dm, UpTime: 00:03:40, Expires: -

```

----结束

## 配置文件

- RouterA 的配置文件

```

#
 sysname RouterA
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.1 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.6.3 255.255.255.0
 pim dm
#
 pim
#
 ospf 1
 area 0.0.0.0
 network 11.1.5.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
return

```

- RouterB 的配置文件

```

#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.4.2 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.6.2 255.255.255.0
 pim dm
#
 pim
#
 ospf 1

```

```
area 0.0.0.0
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.2 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.4.2 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.2.1 255.255.255.0
 pim dm
#
pim
#
ospf 1
 area 0.0.0.0
 network 11.1.2.0 0.0.0.255
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
return
```

- RouterE 的配置文件

```
#
sysname RouterE
#
multicast routing-enable
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.2.2 255.255.255.0
 pim dm
#
interface LoopBack0
 undo shutdown
 ip address 2.2.2.2 255.255.255.255
 pim dm
#
ospf 1
 area 0.0.0.0
 network 11.1.2.2 0.0.0.255
 network 2.2.2.2 0.0.0.0
#
nqa admin mping
 test-type mping
 destination-address ipv4 225.0.0.1
#
return
```

- RouterF 的配置文件

```
#
#
sysname RouterF
#
```

```
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.7.2 255.255.255.0
pim dm
igmp static-group 225.0.0.1
igmp enable
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.2 255.255.255.0
pim dm
#
pim
#
ospf 1
area 0.0.0.0
network 11.1.6.0 0.0.0.255
network 11.1.7.0 0.0.0.255
#
return
```

### 6.50.23 配置检测从组播源到当前路由器的 RPF 路径的测试例示例

通过检测从组播源到当前路由器的 RPF 路径的测试例，可以查看到从组播源到查询者的 RPF 路径。

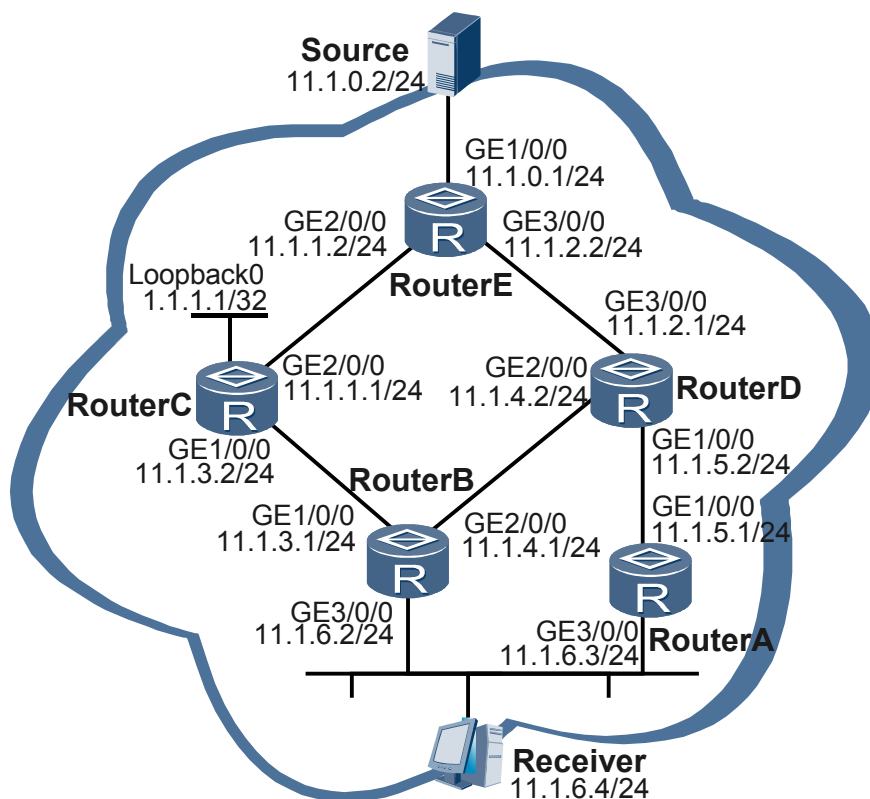
#### 组网需求

如图 6-23 所示，在 PIM-SM 组播网络中，Receiver 加入组播组 225.1.1.1，正常接收 Source 发送的组播数据。需求：判断沿 RPF 路径，如何从 Source 到达 RouterB。

解决方案：在 RouterB 上执行 MTrace，检测从组播源到当前路由器的 RPF 路径。

使用 NQA MTrace 测试例实现 MTrace 功能。

图 6-23 MTrace 组网图



## 配置思路

本例中采用的配置思路如下。

1. 将 RouterB 作为 NQA Client，配置 MTrace 测试例。
2. 启动测试例，验证检测结果。

## 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mtrace
- 组播源地址 11.1.0.2/24

## 操作步骤

**步骤 1** 在 RouterB 上配置 NQA MTrace 测试例。

```
<RouterB> system-view
[RouterB] nqa test-instance admin mtrace
[RouterB-nqa-admin-mtrace] test-type mtrace
[RouterB-nqa-admin-mtrace] mtrace-source-address ipv4 11.1.0.2
```

**步骤 2** 在 RouterC 上查看组播路由。可以看到 RouterC 在收到组播数据后建立了(11.1.0.2, 225.1.1.1)表项，且上游接口是 GigabitEthernet2/0/0，下游接口是 GigabitEthernet1/0/0。



```
[RouterC]display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entries; 1 (S, G) entries
(*, 225.1.1.1)
 RP: 1.1.1.1 (local)
 Protocol: pim-sm, Flag: WC
 UpTime: 00:28:52
 Upstream interface: Register
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet1/0/0
 Protocol: pim-sm, UpTime: 00:28:52, Expires: 00:02:38
(11.1.0.2, 225.1.1.1)
 RP: 1.1.1.1 (local)
 Protocol: pim-sm, Flag: SPT 2MSDP ACT
 UpTime: 00:12:33
 Upstream interface: GigabitEthernet2/0/0
 Upstream neighbor: 11.1.1.2
 RPF prime neighbor: 11.1.1.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet1/0/0
 Protocol: pim-sm, UpTime: 00:12:33, Expires: -
```

### 步骤3 启动测试例。

```
[RouterB-nqa-admin-mtrace] start now
```

### 步骤4 验证测试结果。可以看到从组播源到 RouterB 的 RPF 路径是 RouterE-RouterD-RouterB。

```
[RouterB-nqa-admin-mtrace] display nqa results test-instance admin mtrace
NQA entry(admin, mtrace) : testFlag is inactive ,testtype is mtrace
1 . Test 4 result The test is finished
 Completions: success Query Mode: max-hop
 Current Hop:3 Current Probe:1
 SendProbe:1 ResponseProb:1
 Timeout Count:0 Busy Count:0
 Drop Count:0 Max Path Ttl:4
 Responder:11.1.2.2 Response Rtt: 57
 mtrace start time: 2007-2-7 17:26:17.3
 Last Good Probe Time: 2007-2-7 17:26:17.4
 Last Good Path Time: 2007-2-7 17:26:17.4
1 . Hop 1
 Outgoing Interface Address: 0.0.0.0
 Incoming Interface Address: 11.1.4.1
 Prehop RouterAddress: 11.1.4.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:4
 SG Packet Count:0xffffffff Hop Time Delay(ms): 0xffffffff
 Input Packet Count:9218 Output Packet Count: 0xffffffff
 Input Rate(pps):0 Output Rate(pps):0
 Input Loss Rate: 15.58% SG Loss Rate: 0xffffffff
2 . Hop 2
 Outgoing Interface Address: 11.1.4.2
 Incoming Interface Address: 11.1.2.1
 Prehop RouterAddress: 11.1.2.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:3
 SG Packet Count:0xffffffff Hop Time Delay(ms):393
 Input Packet Count:9639 Output Packet Count:9222
 Input Rate(pps):0 Output Rate(pps):0
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
3 . Hop 3
 Outgoing Interface Address: 11.1.2.2
 Incoming Interface Address: 11.1.0.1
 Prehop RouterAddress: 0.0.0.0
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:2
 SG Packet Count:0xffffffff Hop Time Delay(ms): 0xffffffff
```

|                             |                           |
|-----------------------------|---------------------------|
| Input Packet Count:105321   | Output Packet Count:16320 |
| Input Rate(pps):7           | Output Rate(pps):0        |
| Input Loss Rate: 0xffffffff | SG Loss Rate: 0xffffffff  |

----结束

## 配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.6.3 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.4.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.6.2 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
nqa admin mtrace
 test-type mtrace
 mtrace-source-address ipv4 11.1.0.2
#
```

Return

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.1.1 255.255.255.0
 pim sm
#
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 igmp enable
 pim sm
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 11.1.1.0 0.0.0.255
 network 11.1.3.0 0.0.0.255
#
Return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.4.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.2.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

- RouterE 的配置文件

```
#
```

```
sysname RouterE
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.0.1 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.2.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

## 6.50.24 配置检测从组播源到当前路由器的组播路径的测试例示例

通过检测从组播源到当前路由器的组播路径的测试例，判断出组播数据如何从源到达当前路由器。

### 组网需求

如图 6-23 所示，在 PIM-SM 组播网络中，Receiver 加入组播组 225.1.1.1，正常接收 Source 发送的组播数据。已知 RTB 上能够接收组播数据。需求：判断组播数据如何从 Source 到达 RTB。

解决方案：在 Router B 上使用 NQA MTrace 测试例实现 MTrace 功能，检测从组播源到当前路由器的组播路径。

### 配置思路

本例中采用的配置思路如下。

1. 将 Router B 作为 NQA Client，配置 MTrace 测试例。
2. 启动测试例，验证检测结果。

### 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mtrace
- 组播源地址 11.1.0.2
- 组播组地址 225.1.1.1

## 操作步骤

**步骤 1** 在 Router B 上配置 NQA MTrace 测试例。

```
<RouterB> system-view
[RouterB] nqa test-instance admin mtrace
[RouterB-nqa-admin-mtrace] test-type mtrace
[RouterB-nqa-admin-mtrace] mtrace-source-address ipv4 11.1.0.2
[RouterB-nqa-admin-mtrace] mtrace-group-address ipv4 225.1.1.1
```

**步骤 2** 启动测试例。

```
[RouterB-nqa-admin-mtrace] start now
```

**步骤 3** 验证测试结果。可以看到从组播源到 Router B 的 RPF 路径是 Router E-Router D-Router B。

```
[RouterB-nqa-admin-mtrace] display nqa results test-instance admin mtrace
NQA entry(admin, mtrace) :testFlag is inactive ,testtype is mtrace
1. Test 1 result The test is finished
 Completions: success Query Mode: max-hop
 Current Hop:3 Current Probe:1
 SendProbe:1 ResponseProb:1
 Timeout Count:0 Busy Count:0
 Drop Count:0 Max Path Ttl:4
 Responder:11.1.2.2 Response Rtt: 64
 mtrace start time: 2007-2-7 17:9:11.1
 Last Good Probe Time: 2007-2-7 17:9:11.1
 Last Good Path Time: 2007-2-7 17:9:11.1
1. Hop 1
 Outgoing Interface Address: 0.0.0.0
 Incoming Interface Address: 11.1.4.1
 Prehop RouterAddress: 11.1.4.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:4
 SG Packet Count:62 Hop Time Delay(ms):1
 Input Packet Count:8845 Output Packet Count: 0xffffffff
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
2. Hop 2
 Outgoing Interface Address: 11.1.4.2
 Incoming Interface Address: 11.1.2.1
 Prehop Router Address: 11.1.2.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:3
 SG Packet Count:65 Hop Time Delay(ms): 0xffffffff
 Input Packet Count:9264 Output Packet Count:8792
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
3. Hop 3
 Outgoing Interface Address: 11.1.2.2
 Incoming Interface Address: 11.1.0.1
 Prehop Router Address: 0.0.0.0
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:2
 SG Packet Count:0 Hop Time Delay(ms): 0xffffffff
 Input Packet Count:98002 Output Packet Count:15987
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
```

----结束

## 配置文件

- Router A 的配置文件

```
#
sysname RouterA
#
multicast routing-enable
```

```
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.5.1 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.3 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
return
```

- Router B 的配置文件

```
#
sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.3.1 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.4.1 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
nqa admin mtrace
test-type mtrace
mtrace-source-address ipv4 11.1.0.2
mtrace-group-address ipv4 225.1.1.1
#
return
```

- Router C 的配置文件

```
#
sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.3.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
```

```
pim sm
#
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 igmp enable
 pim sm
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 11.1.1.0 0.0.0.255
 network 11.1.3.0 0.0.0.255
#
Return
```

#### ● Router D 的配置文件

```
#
 sysname RouterD
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.4.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.2.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

#### ● Router E 的配置文件

```
#
 sysname RouterE
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.0.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 11.1.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.2.2 255.255.255.0
```

```
igmp enable
pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.4.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

## 6.50.25 配置检测从组播源到目的主机的 RPF 路径的测试例示例

通过检测从组播源到目的主机的 RPF 路径的测试例，检测从组播源到目的主机的 RPF 路径。

### 组网需求

如图 6-23 所示，在 PIM-SM 组播网络中，Receiver 加入组播组 225.1.1.1，正常接收 Source 发送的组播数据。已知 RouterB 是最后一跳路由器。需求：判断沿 RPF 路径，如何从 Source 到达 Receiver。

解决方案：在 RouterC 上执行使用 NQA MTrace 测试例实现 MTrace 功能，检测从组播源到目的主机的 RPF 路径。

### 配置思路

本例中采用的配置思路如下。

1. 将 RouterC 作为 NQA Client，配置 MTrace 测试例。
2. 启动测试例，验证检测结果。

### 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mtrace
- 组播源地址 11.1.0.2/24
- 目的主机地址 11.1.6.4
- 最后一跳路由器地址 11.1.6.2

### 操作步骤

**步骤 1** 在 RouterC 上配置 NQA MTrace 测试例。

```
<RouterC> system-view
[RouterC] nqa test-instance admin mtrace
[RouterC-nqa-admin-mtrace] test-type mtrace
[RouterC-nqa-admin-mtrace] mtrace-source-address ipv4 11.1.0.2
[RouterC-nqa-admin-mtrace] destination-address ipv4 11.1.6.4
[RouterC-nqa-admin-mtrace] mtrace-query-type last-hop
[RouterC-nqa-admin-mtrace] mtrace-last-hop-address ipv4 11.1.6.2
```

**步骤 2** 启动测试例。

```
[RouterC-nqa-admin-mtrace] start now
```



**步骤 3** 验证测试结果。可以看到从组播源到 Router C 的 RPF 路径是 RouterE-RouterD-RouterB。

```
[RouterC-nqa-admin-mtrace] display nqa results test-instance admin mtrace
NQA entry(admin, mtrace) :testFlag is inactive ,testtype is mtrace
1 . Test 1 result The test is finished
 Completions: success Query Mode: max-hop
 Current Hop:3 Current Probe:1
 SendProbe:1 ResponseProb:1
 Timeout Count:0 Busy Count:0
 Drop Count:0 Max Path Ttl:4
 Responder:11.1.0.2 Response Rtt: 62
 mtrace start time: 2007-2-7 17:36:18.1
 Last Good Probe Time: 2007-2-7 17:36:18.1
 Last Good Path Time: 2007-2-7 17:36:18.1
1 . Hop 1
 Outgoing Interface Address: 11.1.6.2
 Incoming Interface Address: 11.1.4.1
 Prehop Router Address: 11.1.4.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:4
 SG Packet Count:0xffffffff Hop Time Delay(ms):65
 Input Packet Count:9424 Output Packet Count:9815
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
2 . Hop 2
 Outgoing Interface Address: 11.1.4.2
 Incoming Interface Address: 11.1.2.1
 Prehop RouterAddress: 11.1.2.2
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:3
 SG Packet Count:0xffffffff Hop Time Delay(ms):1
 Input Packet Count:9849 Output Packet Count:9429
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
3 . Hop 3
 Outgoing Interface Address: 11.1.2.2
 Incoming Interface Address: 11.1.0.1
 Prehop Router Address: 0.0.0.0
 Protocol : PIM Forward Code:NO_ERROR
 Forward Ttl:1 Current Path Ttl:2
 SG Packet Count:0xffffffff Hop Time Delay(ms): 0xffffffff
 Input Packet Count:109581 Output Packet Count:16529
 Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
 Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff
```

----结束

## 配置文件

- Router A 的配置文件

```
#
sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.5.1 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.3 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
```

```
network 11.1.6.0 0.0.0.255
#
pim
#
return
```

- Router B 的配置文件

```
#
sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.3.1 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
return
#
```

- RouterC 的配置文件

```
#
sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.3.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
pim sm
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
nqa admin mtrace
test-type mtrace
destination-address ipv4 11.1.6.4
mtrace-query-type last-hop
mtrace-last-hop-address ipv4 11.1.6.2
mtrace-source-address ipv4 11.1.0.2
#
return
```

```
#
● RouterD 的配置文件
#
sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.5.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.4.2 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.2.1 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
Return
● RouterE 的配置文件
#
sysname RouterE
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.0.1 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.2.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

## 6.50.26 配置检测从组播源到目的主机的组播路径的测试例示例

通过检测从组播源到目的主机的组播路径的测试例，检测从组播源到目的主机的组播路径。

### 组网需求

如图 6-23 所示，在 PIM-SM 组播网络中，Receiver 加入组播组 225.1.1.1，正常接收 Source 发送的组播数据。需求：判断组播数据如何从 Source 到达 Receiver。

解决方案：在 RouterC 上使用 NQA MTrace 测试实现 MTrace 功能，检测从组播源到目的主机的组播路径。

### 配置思路

本例中采用的配置思路如下。

1. 将 RouterC 作为 NQA Client，配置 MTrace 测试例。
2. 启动测试例，验证检测结果。

### 数据准备

本例中需要准备的数据如下。

- 测试例名称：admin mtrace
- 组播源地址 11.1.0.2
- 组播组地址 225.1.1.1
- 目的主机地址 11.1.6.4

### 操作步骤

**步骤 1** 在 RouterC 上配置 NQA MTrace 测试例。

```
<RouterC> system-view
[RouterC] nqa test-instance admin mtrace
[RouterC-nqa-admin-mtrace] test-type mtrace
[RouterC-nqa-admin-mtrace] mtrace-source-address ipv4 11.1.0.2
[RouterC-nqa-admin-mtrace] mtrace-group-address ipv4 225.1.1.1
[RouterC-nqa-admin-mtrace] destination-address ipv4 11.1.6.4
[RouterC-nqa-admin-mtrace] mtrace-query-type destination
```

**步骤 2** 启动测试例。

```
[RouterC-nqa-admin-mtrace] start now
```

**步骤 3** 验证测试结果。可以看到从组播源到 Router B 的 RPF 路径是 RouterE-RouterD-RouterB。

```
[RouterC-nqa-admin-mtrace] display nqa results test-instance admin mtrace
NQA entry(admin, mtrace) :testFlag is inactive ,testtype is mtrace
1 . Test 1 result The test is finished
Completions: success Query Mode: max-hop
Current Hop:3 Current Probe:1
SendProbe:1 ResponseProb:1
Timeout Count:0 Busy Count:0
Drop Count:0 Max Path Ttl:4
Responser:11.1.2.2 Response Rtt: 83
mtrace start time: 2007-2-7 17:26:53.2
Last Good Probe Time: 2007-2-7 17:26:53.3
Last Good Path Time: 2007-2-7 17:26:53.3
1 . Hop 1
Outgoing Interface Address: 11.1.6.2
```

```

Incoming Interface Address: 11.1.4.1
Prehop RouterAddress: 11.1.4.2
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:4
SG Packet Count:255 Hop Time Delay(ms): 0xffffffff
Input Packet Count:9207 Output Packet Count:9596
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

2 . Hop 2
Outgoing Interface Address: 11.1.4.2
Incoming Interface Address: 11.1.2.1
Prehop RouterAddress: 11.1.2.2
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:3
SG Packet Count:255 Hop Time Delay(ms):327
Input Packet Count:9627 Output Packet Count:9222
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

3 . Hop 3
Outgoing Interface Address: 11.1.2.2
Incoming Interface Address: 11.1.0.1
Prehop RouterAddress: 0.0.0.0
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:2
SG Packet Count:0 Hop Time Delay(ms): 0xffffffff
Input Packet Count:105129 Output Packet Count:16320
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

```

----结束

## 配置文件

- RouterA 的配置文件

```

#
 sysname RouterA
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 11.1.6.3 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 11.1.3.0 0.0.0.255
 network 11.1.6.0 0.0.0.255
#
pim
#
return

```

- RouterB 的配置文件

```

#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 11.1.3.1 255.255.255.0

```

```

pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.4.1 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.6.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
return
#

```

- RouterC 的配置文件

```

#
sysname RTC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.3.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
pim sm
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
nqa admin mtrace
test-type mtrace
destination-address ipv4 11.1.6.4
mtrace-query-type destination
mtrace-source-address ipv4 11.1.0.2
mtrace-group-address ipv4 225.1.1.1
#
Return

```

- RouterD 的配置文件

```

#
sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.5.2 255.255.255.0
pim sm

```

```
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.4.2 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.2.1 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

- RouterE 的配置文件

```
#
sysname RouterE
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.0.1 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
pim sm
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 11.1.2.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 11.1.3.0 0.0.0.255
network 11.1.4.0 0.0.0.255
network 11.1.6.0 0.0.0.255
#
pim
#
Return
```

## 6.50.27 配置单跳 PW 的 PWE3 Ping 测试示例

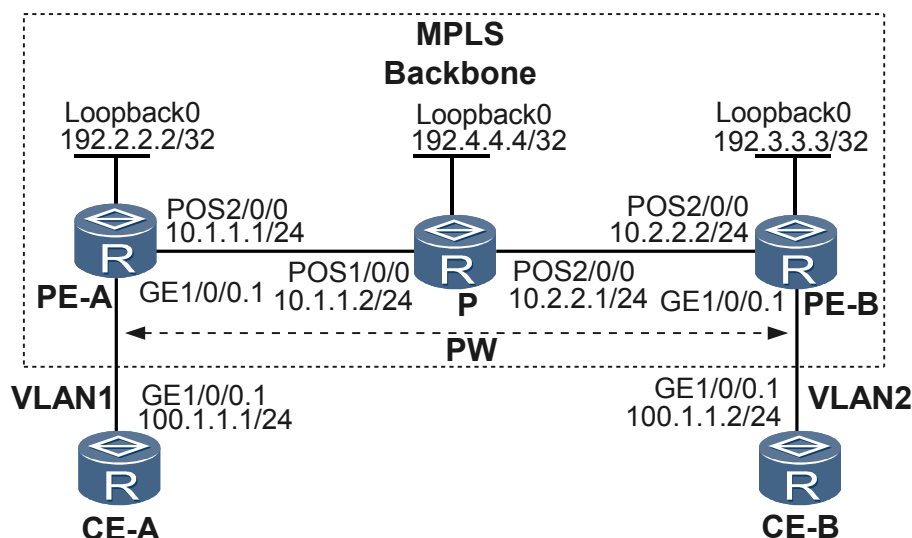
通过单跳 PW 的 PWE3 Ping 测试，检测出 PE 之间 PW 的连通性。

### 组网需求

如图 6-24 所示。CE-A、CE-B 分别通过 VLAN 方式接入 PE-A 和 PE-B。PE-A 和 PE-B 用 MPLS 骨干网连接。在 PE-A 和 PE-B 之间使用 LSP 隧道建立动态 PW。

使用单跳 PW 的 PWE3 Ping 功能测试 PE-A 与 PE-B 之间的 PW 连通性状态。

图 6-24 单跳 PW 的 PWE3 Ping 测试组网示例



## 配置思路

采用如下思路进行配置：

1. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
2. 在骨干网上配置 MPLS 基本能力，建立 LSP 隧道。且 PW 两端的 PE 之间要建立 MPLS LDP 远端对等体关系。
3. 在 PE 上创建 MPLS L2VC 连接。
4. 在 PE-A 上配置单跳 PW 的 PWE3 Ping 测试例。

## 数据准备

完成本例配置，需准备如下数据：

- PW 两端的 L2VC ID（必须一致）
- 各个 PE 及 P 上的 MPLS LSR-ID
- 设置 PE 远端对等体的 IP 地址

## 操作步骤

### 步骤 1 配置单跳动态 PW。

在 MPLS 骨干网上配置单跳动态 PW。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“PWE3 配置”。

### 步骤 2 配置单跳 PW 的 PWE3 Ping 测试例。

# 配置 PE-A。

```
<PE-A> system-view
[PE-A] nqa test-instance test pwe3ping
```



```
[PE-A-nqa-test-pwe3ping] test-type pwe3ping
[PE-A-nqa-test-pwe3ping] local-pw-id 100
[PE-A-nqa-test-pwe3ping] local-pw-type vlan
[PE-A-nqa-test-pwe3ping] label-type control-word
```

### 步骤 3 启动测试操作。

```
[PE-A-nqa-test-pwe3ping] start now
```

### 步骤 4 验证测试结果。

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE-A-nqa-test-pwe3ping] display nqa results
NQA entry(test, pwe3ping) :testFlag is inactive ,testtype is pwe3ping
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:succcess OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:10.2.2.2
Min/Max/Average Completion Time: 60/110/86
Sum/Square-Sum Completion Time: 260/23800
Last Good Probe Time: 2006-9-29 14:35:43.2
```

----结束

## 配置文件

### ● CE-A 的配置文件

```
#
sysname CE-A
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 1
ip address 100.1.1.1 255.255.255.0
#
return
```

### ● PE-A 的配置文件

```
#
sysname PE-A
#
mpls lsr-id 192.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 192.3.3.3
remote-ip 192.3.3.3
#
pw-template wwt
peer-address 192.3.3.3
control-word
vccv cc cw cv lsp-ping
interface GigabitEthernet 1/0/0.1
undo shutdown
mpls l2vc 192.3.3.3 pw-template wwt 100
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
```

```
mpls ldp
#
interface LoopBack0
ip address 192.2.2.2 0.0.0.0
#
nqa test-instance test pwe3ping
test-type pwe3ping
local-pw-id 100
local-pw-type vlan
label-type control-word
#
ospf 1
area 0.0.0.0
network 192.2.2.2 255.255.255.255
network 10.1.1.0 0.0.0.255
#
return
```

- P 的配置文件

```
#
sysname P
#
mpls lsr-id 192.4.4.4
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.4.4.4 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.2.0 0.0.0.255
#
return
```

- PE-B 的配置文件

```
#
sysname PE-B
#
mpls lsr-id 192.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 192.2.2.2
remote-ip 192.2.2.2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.2 255.255.255.0
```

```
mpls
mpls ldp
#
pw-template wwt
peer-address 192.2.2.2
control-word
vccv cc cw cv lsp-ping
interface GigabitEthernet 1/0/0.1
undo shutdown
mpls l2vc 192.2.2.2 pw-template wwt 100
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.3.3.3 0.0.0.0
network 10.2.2.0 0.0.0.255
#
return
```

- CE-B 的配置文件

```
#
sysname CE-B
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 2
ip address 100.1.1.2 255.255.255.0
#
return
```

## 6.50.28 配置多跳 PW 的 PWE3 Ping 测试示例

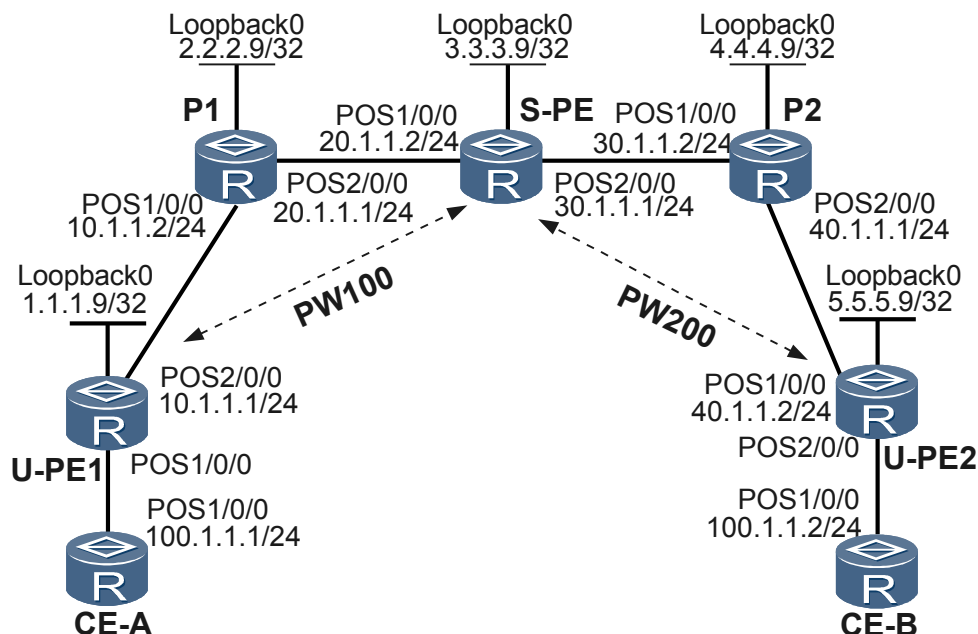
通过多跳 PW 的 PWE3 Ping 测试，检测出 PE 之间 PW 的连通性。

### 组网需求

如图 6-25 所示。CE-A、CE-B 分别通过 PPP 方式接入 U-PE1 和 U-PE2。U-PE1 和 U-PE2 通过 MPLS 骨干网连接。使用 LSP 隧道，并以 S-PE 作为交换节点，在 U-PE1 和 U-PE2 之间建立多跳动态 PW。

使用多跳 PW 的 PWE3 Ping 功能测试 U-PE1 与 U-PE2 之间的 PW 连通性状态。

图 6-25 多跳 PW 的 PWE3 Ping 测试组网示例



## 配置思路

采用如下思路进行配置：

1. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
2. 在骨干网上配置 MPLS 基本能力，建立 LSP 隧道。U-PE1 与 S-PE 之间、U-PE2 与 S-PE 之间需建立 MPLS LDP 远端对等体关系。
3. U-PE 之间创建 MPLS L2VC 连接。
4. 在交换节点 S-PE 上创建交换 PW。
5. 在 U-PE1 上配置多跳 PW 的 PWE3 Ping 测试例。

## 数据准备

完成本例配置，需准备如下数据：

- U-PE1 与 U-PE2 上的 L2VC ID（应设置成不同值）
- U-PE1、S-PE 及 U-PE2 的 MPLS LSR-ID
- 远端对等体的 Remote-IP
- 交换 PW 的封装类型
- U-PE 上的 PW 模板名及模板参数

## 操作步骤

### 步骤 1 配置多跳动态 PW。

在 MPLS 骨干网上配置多跳纯动态 PW。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“PWE3 配置”。

## 步骤 2 配置多跳 PW 的 PWE3 Ping 测试例。

# 配置 U-PE1。

```
<U-PE1> system-view
[U-PE1] nqa test-instance test pwe3ping
[U-PE1-nqa-test-pwe3ping] test-type pwe3ping
[U-PE1-nqa-test-pwe3ping] local-pw-id 100
[U-PE1-nqa-test-pwe3ping] local-pw-type ppp
[U-PE1-nqa-test-pwe3ping] label-type control-word
[U-PE1-nqa-test-pwe3ping] remote-pw-id 200
```

## 步骤 3 启动测试操作。

```
[U-PE1-nqa-test-pwe3ping] start now
```

## 步骤 4 验证测试结果。

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[U-PE1-nqa-test-pwe3ping] display nqa results
NQA entry(test, pwe3ping) :testFlag is inactive ,testtype is pwe3ping
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:40.1.1.2
 Min/Max/Average Completion Time: 60/110/86
 Sum/Square-Sum Completion Time: 260/23800
 Last Good Probe Time: 2006-9-29 14:38:48.2
 Lost packet ratio: 0 %
```

----结束

## 配置文件

### ● CE-A 的配置文件

```
#
 sysname CE-A
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 100.1.1.1 255.255.255.0
#
 return
```

### ● U-PE1 的配置文件

```
#
 sysname U-PE1
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls l2vpn
#
 mpls ldp
#
 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9
#
```

```

pw-template wwt
 peer-address 3.3.3.9
 control-word
 vccv cc cw cv lsp-ping
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 mpls l2vc 3.3.3.9 pw-template wwt 100
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
nqa test-instance test pwe3ping
 test-type pwe3ping
 local-pw-id 100
 local-pw-type ppp
 remote-pw-id 200
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 1.1.1.9 0.0.0.0
#
return

```

#### ● P1 的配置文件

```

#
 sysname P1
#
 mpls lsr-id 2.2.2.9
 mpls
#
 mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 undo shutdown
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 2.2.2.9 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 20.1.1.0 0.0.0.255
#
return

```

#### ● S-PE 的配置文件

```

#
 sysname S-PE

```

```
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
mpls switch-l2vc 5.5.5.9 200 between 1.1.1.9 100 encapsulation ppp
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
mpls ldp remote-peer 5.5.5.9
remote-ip 5.5.5.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
undo shutdown
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
#
return
```

## ● P2 的配置文件

```
#
sysname P2
#
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
undo shutdown
ip address 4.4.4.9 255.255.255.255
#
ospf 1
```

```

 area 0.0.0.0
 network 4.4.2.9 0.0.0.0
 network 30.1.1.0 0.0.0.255
 network 40.1.1.0 0.0.0.255
 #
● U-PE2 的配置文件
 #
 sysname U-PE2
 #
 mpls lsr-id 5.5.5.9
 mpls
 #
 mpls l2vpn
 #
 mpls ldp
 #
 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9
 #
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls ldp
 #
 pw-template wwt
 peer-address 3.3.3.9
 control-word
 vccv cc cw cv lsp-ping
 interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 mpls l2vc 3.3.3.9 pw-template wwt 100
 #
 interface LoopBack0
 ip address 5.5.5.9 255.255.255.255
 #
 ospf 1
 area 0.0.0.0
 network 5.5.5.9 0.0.0.0
 network 40.1.1.0 0.0.0.255
 #
 return
● CE-B 的配置文件
 #
 sysname CE-B
 #
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 #
 return

```

## 6.50.29 配置单跳 PW 的 PWE3 Trace 测试示例

通过单跳 PW 的 PWE3 Traceg 测试，检测出 PE 之间 PW 的连通性。

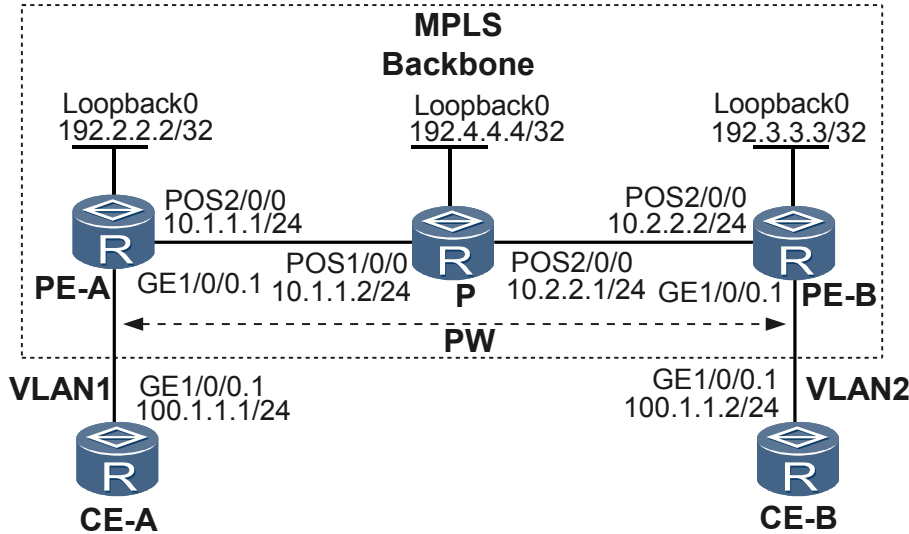
### 组网需求

如图 6-26 所示。CE-A、CE-B 分别通过 VLAN 方式接入 PE-A 和 PE-B。PE-A 和 PE-B 用 MPLS 骨干网连接。在 PE-A 和 PE-B 之间使用 LSP 隧道建立动态 PW。

使用单跳 PW 的 PWE3 Trace 功能测试 PE-A 与 PE-B 之间的 PW 连通性状态。



图 6-26 单跳 PW 的 PWE3 Trace 测试组网示例



配置思路

采用如下思路进行配置：

1. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
2. 在骨干网上配置 MPLS 基本能力，建立 LSP 隧道。且 PW 两端的 PE 之间要建立 MPLS LDP 远端对等体关系。
3. 在 PE 上创建 MPLS L2VC 连接。
4. 在 PE-A 上配置单跳 PW 的 PWE3 Trace 测试例。

数据准备

完成本例配置，需准备如下数据：

- PW 两端的 L2VC ID（必须一致）
- 各个 PE 及 P 上的 MPLS LSR-ID
- 设置 PE 远端对等体的 IP 地址

操作步骤

步骤 1 配置单跳动态 PW。

在 MPLS 骨干网上配置单跳动态 PW。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“PWE3 配置”。

步骤 2 配置单跳 PW 的 PWE3 Trace 测试例。

# 配置 PE-A。

```
<PE-A> system-view
[PE-A] nqa test-instance test pwe3trace
```

```
[PE-A -nqa-test-pwe3trace] test-type pwe3trace
[PE-A -nqa-test-pwe3trace] local-pw-type vlan
[PE-A -nqa-test-pwe3trace] local-pw-id 100
```

**步骤 3** 启动测试操作。

```
[PE-A -nqa-test-pwe3trace] start now
```

**步骤 4** 验证测试结果。

在 PE 上执行 **display nqa history** 命令，可以看到相应状态为成功。

```
[PE-A-nqa-test-pwe3trace] display nqa history
NQA entry(test, pwe3trace) history:
Index T/H/P Response Status Address Time
1 1/1/1 4 success 10.1.1.2 2006-9-30 9:33:3.301
2 1/1/2 5 success 10.1.1.2 2006-9-30 9:33:3.307
3 1/1/3 3 success 10.1.1.2 2006-9-30 9:33:3.311
4 1/2/1 6 success 3.3.3.9 2006-9-30 9:33:3.318
5 1/2/2 6 success 3.3.3.9 2006-9-30 9:33:3.324
6 1/2/3 6 success 3.3.3.9 2006-9-30 9:33:3.331
```

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE-A-nqa-test-pwe3trace] display nqa results
NQA entry(test, pwe3trace) :testFlag is inactive ,testtype is pwe3trace
1. Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2006-9-24 11:22:21.2
1. Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1090/1053
Sum/Square-Sum Completion Time: 3160/3331000
OverThresholds number: 0
Last Good Probe Time: 2006-9-24 11:22:17.2
Destination ip address:10.1.1.2
Lost packet ratio: 0 %
2. Hop 2
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1490/1323
Sum/Square-Sum Completion Time: 3970/5367500
OverThresholds number: 0
Last Good Probe Time: 2006-8-24 11:22:21.2
Destination ip address:10.2.2.2
Lost packet ratio: 0 %
```

----结束

**配置文件**

## ● CE-A 的配置文件

```
#
sysname CE-A
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 1
ip address 100.1.1.1 255.255.255.0
#
return
```

## ● PE-A 的配置文件

```
#
sysname PE-A
#
mpls lsr-id 192.2.2.2
```

```
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 192.3.3.3
remote-ip 192.3.3.3
#
pw-template wwt
peer-address 192.3.3.3
control-word
vccv cc cw cv lsp-ping
interface GigabitEthernet1/0/0.1
vlan-type dot1q 2
mpls l2vc 192.3.3.3 pw-template wwt 100
#
interface Pos2/0/0
undo shutdown
link-protocol ppp
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.2.2.2 0.0.0.0
#
nqa test-instance test pwe3trace
test-type pwe3trace
local-pw-type vlan
local-pw-id 100
#
ospf 1
area 0.0.0.0
network 192.2.2.2 0.0.0.0
network 10.1.1.0 0.0.0.255
#
return
```

## ● P 的配置文件

```
#
sysname P
#
mpls lsr-id 192.4.4.4
mpls
#
mpls ldp
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
undo shutdown
ip address 192.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.4.4.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

```
network 10.2.2.0 0.0.0.255
#
return
```

- PE-B 的配置文件

```
#
sysname PE-B
#
mpls lsr-id 192.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 192.2.2.2
remote-ip 192.2.2.2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.2 255.255.255.0
mpls
mpls ldp
#
pw-template wwt
peer-address 192.2.2.2
control-word
vccv cc cw cv lsp-ping
interface GigabitEthernet1/0/0.1
vlan-type dot1q 2
mpls l2vc 192.2.2.2 pw-template wwt 100
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.3.3.3 0.0.0.0
network 10.2.2.0 0.0.0.255
#
return
```

- CE-B 的配置文件

```
#
sysname CE-B
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 2
ip address 100.1.1.2 255.255.255.0
#
return
```

### 6.50.30 配置多跳 PW 的 PWE3 Trace 测试示例

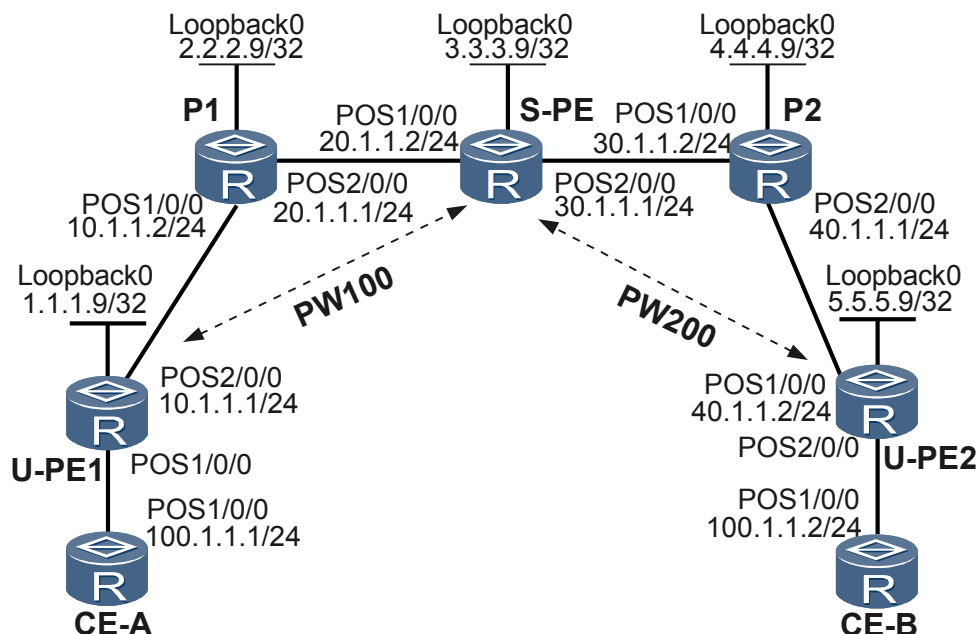
通过多跳 PW 的 PWE3 Traceg 测试，检测出 PE 之间 PW 的连通性。

#### 组网需求

如图 6-27 所示。CE-A、CE-B 分别通过 PPP 方式接入 U-PE1 和 U-PE2。U-PE1 和 U-PE2 通过 MPLS 骨干网连接。使用 LSP 隧道，并以 S-PE 作为交换节点，在 U-PE1 和 U-PE2 之间建立多跳动态 PW。

使用多跳 PW 的 PWE3 Trace 功能测试 U-PE1 与 U-PE2 之间的 PW 连通性状态。

图 6-27 多跳 PW 的 PWE3 Trace 测试组网示例



## 配置思路

采用如下思路进行配置：

1. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
2. 在骨干网上配置 MPLS 基本能力，建立 LSP 隧道。U-PE1 与 S-PE 之间、U-PE2 与 S-PE 之间需建立 MPLS LDP 远端对等体关系。
3. U-PE 之间创建 MPLS L2VC 连接。
4. 在交换节点 S-PE 上创建交换 PW。
5. 在 U-PE1 上配置多跳 PW 的 PWE3 Trace 测试例。

## 数据准备

完成本例配置，需准备如下数据：

- U-PE1 与 U-PE2 上的 L2VC ID（应设置成不同值）
- U-PE1、S-PE 及 U-PE2 的 MPLS LSR-ID
- 远端对等体的 Remote-IP
- 交换 PW 的封装类型
- U-PE 上的 PW 模板名及模板参数

## 操作步骤

### 步骤 1 配置多跳动态 PW。

在 MPLS 骨干网上配置多跳纯动态 PW。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“PWE3 配置”。

## 步骤 2 配置多跳 PW 的 PWE3 Trace 测试例。

# 配置 U-PE1。

```
<U-PE1> system-view
[U-PE1] nqa test-instance test pwe3trace
[U-PE1-nqa-test-pwe3trace] test-type pwe3trace
[U-PE1-nqa-test-pwe3trace] local-pw-id 100
[U-PE1-nqa-test-pwe3trace] local-pw-type ppp
[U-PE1-nqa-test-pwe3trace] label-type control-word
[U-PE1-nqa-test-pwe3trace] remote-pw-id 200
```

## 步骤 3 启动测试操作。

```
[U-PE1-nqa-test-pwe3trace] start now
```

## 步骤 4 验证测试结果。

在 PE 上执行 **display nqa history** 命令，可以看到相应状态为成功。

```
[U-PE1-nqa-test-pwe3trace] display nqa history
NQA entry(test, pwe3trace) history:
Index T/H/P Response Status Address Time
1 1/1/1 4 success 10.1.1.2 2006-9-30 9:33:3.301
2 1/1/2 5 success 10.1.1.2 2006-9-30 9:33:3.307
3 1/1/3 3 success 10.1.1.2 2006-9-30 9:33:3.311
4 1/2/1 6 success 20.1.1.2 2006-9-30 9:33:3.318
5 1/2/2 6 success 20.1.1.2 2006-9-30 9:33:3.324
6 1/2/3 6 success 20.1.1.2 2006-9-30 9:33:3.331
7 1/3/1 6 success 30.1.1.2 2006-9-30 9:33:3.318
8 1/3/2 6 success 30.1.1.2 2006-9-30 9:33:3.324
9 1/3/3 6 success 30.1.1.2 2006-9-30 9:33:3.331
10 1/4/1 6 success 5.5.5.9 2006-9-30 9:33:3.318
11 1/4/2 6 success 5.5.5.9 2006-9-30 9:33:3.324
12 1/4/3 6 success 5.5.5.9 2006-9-30 9:33:3.331
```

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[U-PE1-nqa-test-pwe3trace] display nqa results
NQA entry(test, pwe3trace) :testFlag is inactive ,testtype is pwe3trace
1 . Test 1 result The test is finished
Completion:succcess Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2006-9-24 11:22:21.2
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1090/1053
Sum/Square-Sum Completion Time: 3160/3331000
OverThresholds number: 0
Last Good Probe Time: 2006-9-24 11:22:17.2
Destination ip address:10.1.1.2
2 . Hop 2
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1490/1323
Sum/Square-Sum Completion Time: 3970/5367500
OverThresholds number: 0
Last Good Probe Time: 2006-8-24 11:22:21.2
Destination ip address:20.1.1.2
3 . Hop 3
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1490/1323
Sum/Square-Sum Completion Time: 3970/5367500
OverThresholds number: 0
Last Good Probe Time: 2006-8-24 11:22:21.2
```

```
Destination ip address:30.1.1.2
4 . Hop 4
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 1050/1490/1323
Sum/Square-Sum Completion Time: 3970/5367500
OverThresholds number: 0
Last Good Probe Time: 2006-8-24 11:22:21.2
Destination ip address:5.5.5.9
```

----结束

## 配置文件

- CE-A 的配置文件

```
#
sysname CE-A
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 100.1.1.1 255.255.255.0
#
return
```

- U-PE1 的配置文件

```
#
sysname U-PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
pw-template wwt
peer-address 3.3.3.9
control-word
vccv cc cw cv lsp-ping
interface Pos1/0/0
undo shutdown
link-protocol ppp
mpls l2vc 3.3.3.9 pw-template wwt 100
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.9 255.255.255.255
#
nqa test-instance test pwe3trace
test-type pwe3trace
local-pw-id 100
local-pw-type ppp
label-type control-word
remote-pw-id 200
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
```

```

return
```

- P1 的配置文件

```

sysname P1

mpls lsr-id 2.2.2.9
mpls

mpls ldp

interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp

interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.1 255.255.255.0
mpls
mpls ldp

interface LoopBack0
ip address 2.2.2.9 255.255.255.255

ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255

return
```

- S-PE 的配置文件

```

sysname S-PE

mpls lsr-id 3.3.3.9
mpls

mpls l2vpn

mpls switch-l2vc 5.5.5.9 200 between 1.1.1.9 100 encapsulation ppp

mpls ldp

mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9

mpls ldp remote-peer 5.5.5.9
remote-ip 5.5.5.9

interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.2 255.255.255.0
mpls
mpls ldp

interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.1 255.255.255.0
mpls
mpls ldp
#
```



```
interface LoopBack0
 undo shutdown
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 20.1.1.0 0.0.0.255
 network 30.1.1.0 0.0.0.255
#
return
```

## ● P2 的配置文件

```
#
 sysname P2
#
 mpls lsr-id 4.4.4.9
 mpls
#
 mpls ldp
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 30.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
 interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
 interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 4.4.2.9 0.0.0.0
 network 30.1.1.0 0.0.0.255
 network 40.1.1.0 0.0.0.255
#
```

## ● U-PE2 的配置文件

```
#
 sysname U-PE2
#
 mpls lsr-id 5.5.5.9
 mpls
#
 mpls l2vpn
#
 mpls ldp
#
 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
 pw-template wwt
 peer-address 3.3.3.9
 control-word
 vccv cc cw cv lsp-ping
```

```

interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 mpls l2vc 3.3.3.9 pw-template wwt 100
#
interface LoopBack0
 ip address 5.5.5.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 5.5.5.9 0.0.0.0
 network 40.1.1.0 0.0.0.255
#
return

```

- CE-B 的配置文件

```

#
sysname CE-B
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
#
return

```

### 6.50.31 配置多跳跨域 Kompella L2VPN 的 VC Trace 测试示例

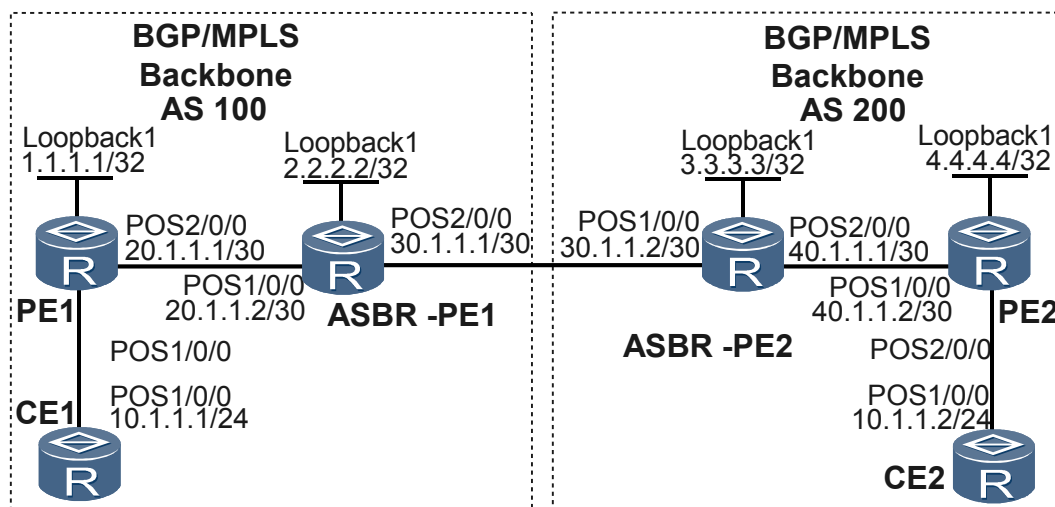
通过多跳跨域 Kompella L2VPN 的 VC Trace 测试使用多跳跨域 Kompella L2VPN 的 VC Trace 测试 PE1 与 PE2 之间的 PW 连通性状态。

#### 组网需求

如图 6-28 所示。MPLS 骨干网路由器使用 OSPF 作为 IGP 实现同一个 AS 内部的互通。并采用 Multi-Hop 跨域方式实现 Kompella L2VPN。

使用多跳跨域 Kompella L2VPN 的 VC Trace 测试 PE1 与 PE2 之间的 PW 连通性状态。

图 6-28 多跳跨域 Kompella L2VPN 的 VC Trace 测试组网示例



## 配置思路

采用如下思路进行配置：

1. 在骨干网上运行 IGP 协议，使同一个 AS 域内的各路由器能互通。
2. 在骨干网上使能 MPLS，在 PE 与 ASBR-PE 之间建立动态 LSP 隧道。
3. 同一 AS 的 PE 和 ASBR-PE 之间建立 IBGP，在各 ASBR-PE 之间配置 EBGP。
4. 在 ASBR-PE 上需配置路由策略，使能标签路由功能。
5. 在 PE1 和 PE2 之间建立 MP-EBGP 对等体关系。
6. 在 PE1 和 PE2 之间创建 Kompella 方式 L2VPN 连接。在 ASBR 上配置 L2VPN 实例。
7. 在 PE1 上配置多跳跨域 Kompella L2VPN 的 VC Trace 测试例。

## 数据准备

完成本例配置，需准备如下数据：

- 配置 OSPF 所需的数据
- PE 及 ASBR PE 上的 MPLS LSR-ID
- PE 上创建的 L2VPN 实例名、路由标识 RD 及收发路由属性 VPN-Target
- PE 上 CE 连接的名称、CE ID、CE-Range（默认值为 10）、Default-Offset（为 1 或 0，默认值为 0）
- ASBR-PE 上使用的路由策略

## 操作步骤

### 步骤 1 配置多跳跨域 Kompella L2VPN。

在 MPLS 骨干网上配置多跳跨域 Kompella L2VPN。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“MPLS L2VPN 配置”。

### 步骤 2 配置多跳跨域 Kompella L2VPN 的 VC Trace 测试例。

# 配置 PE1。

```
<U-PE1> system-view
[U-PE1] nqa test-instance test pwe3trace
[U-PE1-nqa-test-pwe3trace] test-type pwe3trace
[U-PE1-nqa-test-pwe3trace] vc-type bgp
[U-PE1-nqa-test-pwe3trace] local-pw-id 1
[U-PE1-nqa-test-pwe3trace] remote-pw-id 2
[U-PE1-nqa-test-pwe3trace] vpn-instance vpn1
```

### 步骤 3 启动测试操作。

```
[U-PE1-nqa-test-pwe3trace] start now
```

### 步骤 4 验证测试结果。

在 PE 上执行 **display nqa history** 命令，可以看到相应状态为成功。

```
[U-PE1-nqa-test-pwe3trace] display nqa history
NQA entry(test, pwe3trace) history:
Index T/H/P Response Status Address Time
1 1/1/1 4 success 10.1.1.2 2006-9-30 9:33:3.301
```

|    |       |           |          |                      |
|----|-------|-----------|----------|----------------------|
| 2  | 1/1/2 | 5 success | 10.1.1.2 | 2006-9-30 9:33:3.307 |
| 3  | 1/1/3 | 3 success | 10.1.1.2 | 2006-9-30 9:33:3.311 |
| 4  | 1/2/1 | 6 success | 20.1.1.2 | 2006-9-30 9:33:3.318 |
| 5  | 1/2/2 | 6 success | 20.1.1.2 | 2006-9-30 9:33:3.324 |
| 6  | 1/2/3 | 6 success | 20.1.1.2 | 2006-9-30 9:33:3.331 |
| 7  | 1/3/1 | 6 success | 30.1.1.2 | 2006-9-30 9:33:3.318 |
| 8  | 1/3/2 | 6 success | 30.1.1.2 | 2006-9-30 9:33:3.324 |
| 9  | 1/3/3 | 6 success | 30.1.1.2 | 2006-9-30 9:33:3.331 |
| 10 | 1/4/1 | 6 success | 5.5.5.9  | 2006-9-30 9:33:3.318 |
| 11 | 1/4/2 | 6 success | 5.5.5.9  | 2006-9-30 9:33:3.324 |
| 12 | 1/4/3 | 6 success | 5.5.5.9  | 2006-9-30 9:33:3.331 |

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[U-PE1-nqa-test-pwe3trace] display nqa results
NQA entry (test, pwe3trace) :testflag is inactive ,testtype is pwe3trace
1. Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-3-2 9:26:57.0
1. Hop 1
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 4/12/8
 Sum/Square-Sum Completion Time: 25/241
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-3-2 9:26:56.9
 Destination ip address:20.1.1.2
 Lost packet ratio: 0 %
2. Hop 2
 Send operation times: 3 Receive response times: 3
 Min/Max/Average Completion Time: 10/37/20
 Sum/Square-Sum Completion Time: 60/1638
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-3-2 9:26:57.0
 Destination ip address:30.1.1.2
 Lost packet ratio: 0 %
```

----结束

## 配置文件

- CE1 的配置文件

```
#
sysname CE2
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
return
```

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
mpls l2vpn
#
mpls ldp
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
```

```
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
bgp 100
peer 4.4.4.4 as-number 200
peer 4.4.4.4 ebgp-max-hop 255
peer 4.4.4.4 connect-interface LoopBack1
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 4.4.4.4 enable
peer 2.2.2.2 enable
peer 2.2.2.2 label-route-capability
#
l2vpn-family
policy vpn-target
peer 4.4.4.4 enable
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 20.1.1.0 0.0.0.255
#
nqa test-instance test pwe3trace
test-type pwe3trace
vc-type bgp
local-pw-id 1
remote-pw-id 2
vpn-instance vpn1
#
mpls l2vpn vpn1 encapsulation ppp
route-distinguisher 100:1
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
ce cel id 1 range 10 default-offset 0
connection ce-offset 2 interface Pos1/0/0
#
#
return
```

## ● ASBR-PE1 的配置文件

```
#
sysname ASBR1
#
stp region-configuration
region-name 00e0954d347d
active region-configuration
#
mpls lsr-id 2.2.2.2
mpls
mpls l2vpn
#
mpls ldp
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 20.1.1.2 255.255.255.252
mpls
mpls ldp
```

```

#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.1 255.255.255.252
mpls
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
bgp 100
peer 1.1.1.1 as-number 100
peer 1.1.1.1 connect-interface LoopBack1
peer 30.1.1.2 as-number 200
peer 30.1.1.2 connect-interface Pos2/0/0
#
ipv4-family unicast
undo synchronization
network 1.1.1.1 255.255.255.255
peer 1.1.1.1 enable
peer 1.1.1.1 route-policy policy1 export
peer 1.1.1.1 label-route-capability
peer 30.1.1.2 enable
peer 30.1.1.2 route-policy policy1 export
peer 30.1.1.2 label-route-capability
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 20.1.1.0 0.0.0.255
#
route-policy policy1 permit node 1
apply mpls-label
#
return

```

#### ● ASBR-PE2 的配置文件

```

#
sysname ASBR2
#
mpls lsr-id 3.3.3.3
mpls
mpls l2vpn
#
mpls ldp
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 30.1.1.2 255.255.255.252
mpls
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
bgp 200
peer 4.4.4.4 as-number 200
peer 4.4.4.4 connect-interface LoopBack1
peer 30.1.1.1 as-number 100
peer 30.1.1.1 connect-interface Pos1/0/0
#
ipv4-family unicast
undo synchronization

```

```

network 4.4.4.4 255.255.255.255
peer 4.4.4.4 enable
peer 4.4.4.4 route-policy policy1 export
peer 4.4.4.4 label-route-capability
peer 30.1.1.1 enable
peer 30.1.1.1 route-policy policy1 export
peer 30.1.1.1 label-route-capability
#
l2vpn-family
policy vpn-target
peer 4.4.4.4 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 40.1.1.0 0.0.0.255
#
route-policy policy1 permit node 1
apply mpls-label
#
return

```

## ● PE2 的配置文件

```

#
sysname PE2
#
mpls lsr-id 4.4.4.4
mpls
mpls l2vpn
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
#
interface LoopBack1
undo shutdown
ip address 4.4.4.4 255.255.255.255
#
bgp 200
peer 1.1.1.1 as-number 100
peer 1.1.1.1 ebgp-max-hop 255
peer 1.1.1.1 connect-interface LoopBack1
peer 3.3.3.3 as-number 200
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 1.1.1.1 enable
peer 3.3.3.3 enable
peer 3.3.3.3 label-route-capability
#
l2vpn-family
policy vpn-target
peer 1.1.1.1 enable
#
ospf 1
area 0.0.0.0
network 40.1.1.0 0.0.0.255
network 4.4.4.4 0.0.0.0
#
mpls l2vpn vpn1 encapsulation ppp

```

```

route-distinguisher 200:1
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
ce ce2 id 2 range 10 default-offset 0
connection ce-offset 1 interface Pos2/0/0
#
#
return

```

- CE2 的配置文件

```

#
sysname CE2
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
Return

```

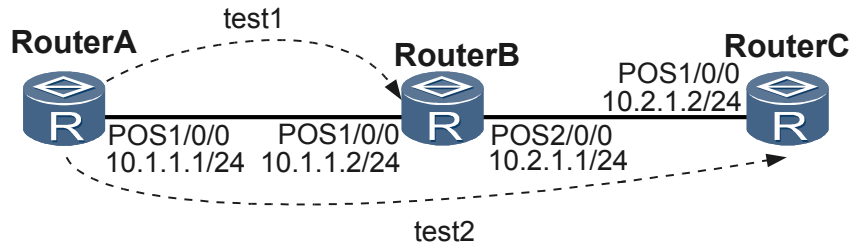
### 6.50.32 配置 NQA 测试组示例

通过 NQA 测试组，可以将相同类型的测试例加入同一个测试组，进行统一管理。

#### 组网需求

如图 6-29 所示,RouterA 作为 NQA 客户端，测试 RouterB 和 RouterC 是否可达。

图 6-29 NQA 测试组组网图



#### 配置思路

采用如下思路进行配置：

1. RouterA 作为 NQA 客户端。
2. 建立一个 NQA 测试组，其中包含两个测试例，分别测试报文在 RouterA 和 RouterB、RouterC 之间是否可达，以及报文的往返时间。

#### 数据准备

为完成此配置例，需准备如下的数据：

- RouterB、RouterC 的主机地址
- 测试组启动时间



## 操作步骤

**步骤 1** 配置 RouterA、RouterB、RouterC 之间路由可达（略）

**步骤 2** 在 RouterA 上创建 ICMP 类型的 NQA 测试组

```
<RouterA> system-view
[RouterA] nqa test-instance group icmp
[RouterA-nqa-group-icmp] test-type icmp
[RouterA-nqa-group-icmp] switch-to group
[RouterA-nqa-group-icmp] quit
```

**步骤 3** 在 RouterA 上分别建立到 RouterB 的测试例 admin test1 和到 RouterC 的测试例 admin test2

```
[RouterA] nqa test-instance admin test1
[RouterA-nqa-admin-test1] test-type icmp
[RouterA-nqa-admin-test1] join group nqa group icmp
[RouterA-nqa-admin-test1] destination-address ipv4 10.1.1.2
[RouterA-nqa-admin-test1] quit
[RouterA] nqa test-instance admin test2
[RouterA-nqa-admin-test2] test-type icmp
[RouterA-nqa-admin-test2] join group nqa group icmp
[RouterA-nqa-admin-test2] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-test2] quit
```

**步骤 4** 回到测试组，设置 10 秒后启动测试

```
[RouterA] nqa test-instance group icmp
[RouterA-nqa-group-icmp] start delay seconds 10
```

# 执行命令 **display nqa-agent**，可以看到客户端上的测试组和成员测试例状态。

```
[RouterA-nqa-group-icmp] display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 3
NQA Flow Max:1000 NQA Flow Remained:1000

nqa test-instance group icmp
test-type icmp
switch-to group
nqa status : group leader, group members number : 2
nqa test-instance admin test1
test-type icmp
destination-address ipv4 10.1.1.2
join group nqa group icmp
nqa status : group member, belong to group : group icmp
nqa test-instance admin test2
test-type icmp
destination-address ipv4 10.2.1.2
join group nqa group icmp
nqa status : group member, belong to group : group icmp
```

**步骤 5** 等待 20 秒左右，验证测试结果

```
<RouterA> display nqa results
NQA entry(admin, test1) :testflag is inactive ,testtype is icmp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:100.1.1.201
Min/Max/Average Completion Time: 2/2/2
Sum/Square-Sum Completion Time: 6/12
Last Good Probe Time: 2009-3-31 15:54:32.4
Lost packet ratio: 0 %

NQA entry(admin, test2) :testflag is inactive ,testtype is icmp
1. Test 1 result The test is finished
```

```

Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:100.1.1.201
Min/Max/Average Completion Time: 1/1/1
Sum/Square-Sum Completion Time: 3/3
Last Good Probe Time: 2009-3-31 15:54:40.4
Lost packet ratio: 0 %

```

----结束

## 配置文件

### ● RouterA 的配置文件

```

#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance group icmp
 switch-to group
 test-type icmp
nqa test-instance admin test1
 test-type icmp
 join group nqa group icmp
 destination-address ipv4 10.1.1.2
nqa test-instance admin test2
 test-type icmp
 join group nqa group icmp
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return

```

### ● RouterB 的配置文件

```

#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
return

```

### ● RouterC 的配置文件

```

#
 sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#

```

```
return
```

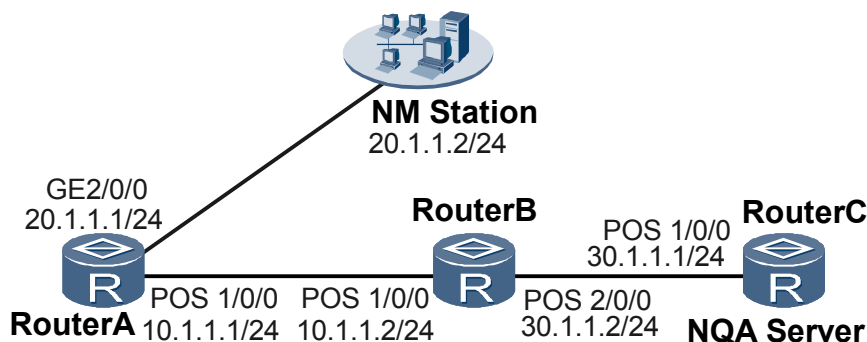
### 6.50.33 配置向网管端发送 NQA 阈值告警示例

通过向网管端发送 NQA 阈值告警，网络管理人员可以清晰的了解到设备端发生的情况。

#### 组网需求

如图 6-30 所示在配置 Jitter 测试例时，配置阈值并启动告警功能。启动 Jitter 测试例，在测试结束后，当从 RouterA 到 RouterC 或从 RouterC 到 RouterA 的测试报文中，有超过设定的单向传输告警阈值，或测试报文的往返时间超过设定的双向传输阈值时，RouterA 会向网管端发送一次 Trap 消息。通过 NM Station 接收到的 Trap 消息，网络管理人员可以清晰的看到产生告警的原因。

图 6-30 配置 NQA 阈值组网图



#### 说明

关于时钟同步介绍请参见《HUAWEI NetEngine20E-X6 高端业务路由器 特性描述 系统管理》的“NTP”。

#### 配置思路

采用如下思路进行阈值的配置：配置一个 Jitter 测试例

1. 配置 NQA 阈值功能
2. 开启 Trap 发送开关
3. 配置向网管端发送 Trap

#### 数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址及端口号
- 监听服务类型及监听端口号
- RTD 阈值和 OWD 阈值
- 网管端地址

## 操作步骤

**步骤 1** 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

**步骤 2** 配置一个 Jitter 测试例

# 在 RouterC 上配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 30.1.1.2 9000
```

# 在 RouterA 上使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 30.1.1.2
[RouterA-nqa-admin-jitter] destination-port 9000
```

**步骤 3** 配置 NQA 阈值功能

# 在 RouterA 上配置 RTD 阈值。

```
[RouterA-nqa-admin-jitter] threshold rtd 20
```

# 在 RouterA 上配置 OWD-DS 阈值。

```
[RouterA-nqa-admin-jitter] threshold owd-ds 100
```

# 在 RouterA 上配置 OWD-SD 阈值。

```
[RouterA-nqa-admin-jitter] threshold owd-sd 100
```

**步骤 4** 开启发送 Trap 的功能

```
[RouterA-nqa-test-jitter] send-trap owd-ds owd-sd rtd
[RouterA-nqa-test-jitter] quit
```

**步骤 5** 配置向网管发送 Trap 的功能

```
[RouterA] snmp-agent target-host trap address udp-domain 20.1.1.2 params securityname public v2c
```

**步骤 6** 启动测试操作

```
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] start now
[RouterA-nqa-admin-jitter] quit
[RouterA] quit
```

**步骤 7** 检查配置结果

# 显示各路由器的 NQA 测试结果信息。

```
<RouterA> display nqa result
NQA entry(test, jitter) :testflag is inactive ,testtype is jitter
1 . Test 1 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion:succcess RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/1/1/60 RTT Square Sum:60
 NumOfRTT:60 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:0 Min Positive DS:1
 Max Positive SD:0 Max Positive DS:1
 Positive SD Number:0 Positive DS Number:5
 Positive SD Sum:0 Positive DS Sum:5
 Positive SD Square Sum:0 Positive DS Square Sum:5
 Min Negative SD:0 Min Negative DS:1
 Max Negative SD:0 Max Negative DS:1
```

|                            |                           |
|----------------------------|---------------------------|
| Negative SD Number:0       | Negative DS Number:6      |
| Negative SD Sum:0          | Negative DS Sum:6         |
| Negative SD Square Sum:0   | Negative DS Square Sum:6  |
| Min Delay SD:0             | Min Delay DS:0            |
| Max Delay SD:0             | Max Delay DS:0            |
| Delay SD Square Sum:0      | Delay DS Square Sum:0     |
| Packet Loss SD:0           | Packet Loss DS:0          |
| Packet Loss Unknown:0      | Average of Jitter:1       |
| Average of Jitter SD:0     | Average of Jitter DS:1    |
| jitter out value:0.0000000 | jitter in value:0.0114583 |
| NumberOfOWD:60             | Packet Loss Ratio: 0%     |
| OWD SD Sum:0               | OWD DS Sum:0              |
| ICPIF value: 0             | MOS-CQ value: 0           |

# 在告警缓冲区检查是否产生 Trap 消息。

<RouterA> **display trapbuffer**

Trapping Buffer Configuration and contents:enabled  
allowed max buffer size : 1024

actual buffer size : 256  
channel number : 3 , channel name : trapbuffer  
dropped messages : 0  
overwritten messages : 2550  
current messages : 256  
#Jul 9 00:28:34 2009 HUAWEI NQA/4/RTDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.16 NQA entry RTD  
over threshold. (OwnerIndex=admin, TestName=jitter)  
#Jul 9 00:28:34 2009 HUAWEI NQA/4/SDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.17 NQA entry OWD-SD  
over threshold. (OwnerIndex=admin, TestName=jitter)  
#Jul 9 00:28:34 2009 HUAWEI NQA/4/DSTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.  
18 NQA entry OWD-DS over threshold. (OwnerIndex=admin, TestName=jitter)

# 在网管端查看是否可以正确接收到 Trap 消息。(略)

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 20.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
nqa test-instance test jitter
 test-type jitter
 destination-address ipv4 30.1.1.2
 destination-port 9000
 threshold rtd 20
 threshold owd-sd 100
 threshold owd-ds 100
 send-trap rtd
 send-trap owd-sd
 send-trap owd-ds
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100007B29
```

```
snmp-agent sys-info version v2c
snmp-agent target-host trap address udp-domain 20.1.1.2 params securityname
public v2c
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 30.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.1
 network 10.1.1.0 0.0.0.255
 network 30.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 30.1.1.2 255.255.255.0
#
 nqa-server udpecho 30.1.1.2 9000
#
ospf 1
 area 0.0.0.1
 network 30.1.1.0 0.0.0.255
#
return
```

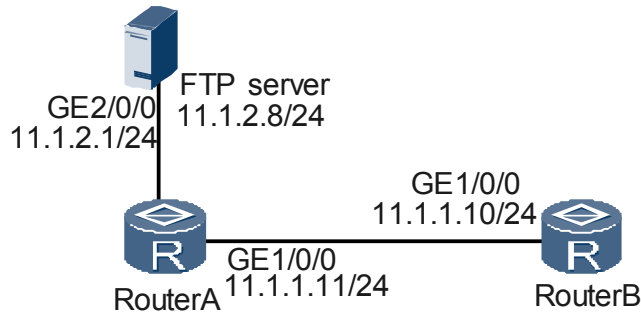
## 6.50.34 配置测试结果发送到 FTP 服务器示例

通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

### 组网需求

如图 6-31 所示，RouterA 作为客户端进行 ICMP 测试，测试的结果通过 FTP 发送到 FTP Server。

图 6-31 测试结果发送到 FTP 服务器组网图



## 配置思路

本例中采用的配置思路如下。

1. 配置连接 FTP 服务器需要的参数。
2. 使能通过 FTP 保存测试结果的功能。
3. 配置 FTP 保存测试结果的条数。
4. 配置 FTP 保存测试结果的时间。
5. 配置发送
6. 启动测试例。
7. 检查配置结果。

## 数据准备

本例中需要准备的数据如下。

- 登录 FTP 服务器所需的用户名和密码
- FTP 保存测试结果的条数
- 配置 FTP 保存测试结果的时间

## 操作步骤

### 步骤 1 配置连接 FTP 服务器需要的参数。

# 配置连接 FTP 服务器的地址。

```
<RouterA> system-view
[RouterA] nqa-ftp-record ip-address 11.1.2.8
```

# 配置连接 FTP 服务器所需的用户名。

```
[RouterA] nqa-ftp-record username ftp
[RouterA] nqa-ftp-record password ftp
```

# 配置测试结果保存的文件名。

```
[RouterA] nqa-ftp-record filename icmp
```

**步骤 2** 配置通过 FTP 保存测试结果到文件的条数。

```
[RouterA] nqa-ftp-record item-num 10010
```

**步骤 3** 配置通过 FTP 保存测试结果到文件的时间。

```
[RouterA] nqa-ftp-record time 2
```

**步骤 4** 配置 FTP 传送成功向网管端发送 Trap

```
[RouterA] nqa-ftp-record trap-enable
```

**步骤 5** 在 RouterA 使能通过 FTP 保存 NQA 测试结果功能。

```
<RouterA> system-view
[RouterA] nqa-ftp-record enable
```

**步骤 6** 启动测试例

```
[RouterA] nqa test-instance admin icmp
[RouterA-admin-icmp] start now
```

**步骤 7** 检查配置结果

# 显示各路由器的 NQA 测试结果信息。

```
<RouterA> display nqa-ftp-record configuration
-----NQA FTP SAVE RECORD CONFIGURATION-----
FUNCTION: ENABLE TRAP: ENABLE
IP-ADDRESS:11.1.1.8
VPN-INSTANCE:
USERNAME:ftp
PASSWORD:ftp
FILENAME:icmp
ITEM-NUM:10010
TIME:2
LAST FINISHED FILENAME:icmp20080605-150350.txt
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.11 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 11.1.2.1 255.255.255.0
#
interface NULL0
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
nqa-ftp-record enable
nqa-ftp-record trap-enable
nqa-ftp-record ip-address 11.1.1.8
nqa-ftp-record username ftp
nqa-ftp-record password ftp
nqa-ftp-record filename icmp
nqa-ftp-record item-num 10010
nqa-ftp-record time 2
```



```
nqa test-instance admin icmp
test-type icmp
destination-address ipv4 11.1.1.10
frequency 5
#
snmp-agent
snmp-agent local-engineid 000007DB7F000001000021D7
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 11.1.1.8 params securityname wan
snmp-agent trap enable feature-name nqa trap-name nqaftpsaverecordnotification
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
ip address 11.1.1.10 255.255.255.0
#
return
```

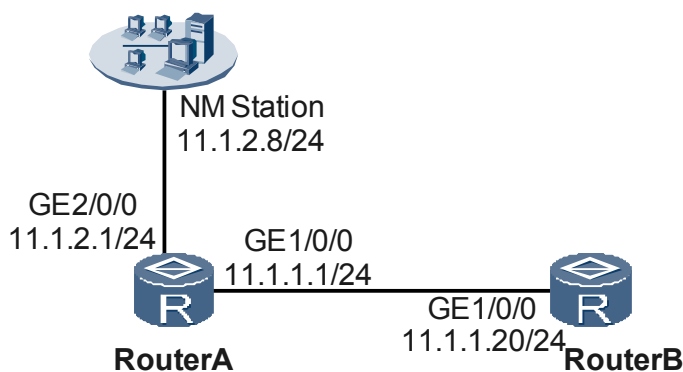
### 6.50.35 配置 NQA 上下限阈值告警示例

在 NQA 的测试结果超出阈值时，可以发送告警或者生成日志或者既发送告警也生成日志。

#### 组网需求

如图 6-32 所示，RouterA 作为客户端进行 ICMP Jitter 测试，对测试结果的丢包率进行监控，在测试结果中的丢包率超过阈值后向网管端发送 Trap。

图 6-32 配置 NQA 阈值告警组网图



#### 配置思路

本例中采用的配置思路如下。

1. 配置阈值告警相关事件。
2. 配置阈值告警。
3. 配置向网管发送告警消息。
4. 启动测试例。

## 数据准备

本例中需要准备的数据如下。

- 阈值相关事件号
- 阈值告警号
- 阈值上限和下限
- 网管端的地址

## 操作步骤

**步骤 1** 配置 RouterA 为 ICMP Jitter 测试的客户端。（略）

**步骤 2** 在 RouterA 配置告警相关事件。

```
<RouterA> system-view
[RouterA] nqa event 10 log-trap
```

**步骤 3** 配置阈值告警。

```
[RouterA] nqa test-instance admin icmpjitter
[RouterA-nqa-admin-icmpjitter] test-type icmpjitter
[RouterA-nqa-admin-icmpjitter] destination-address ipv4 11.1.1.20
[RouterA-nqa-admin-icmpjitter] frequency 5
[RouterA-nqa-admin-icmpjitter] alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-
threshold 10 10
[RouterA-nqa-admin-icmpjitter] quit
```

**步骤 4** 配置向网管发送告警。

# 配置 SNMP 基本功能。

```
[RouterA] snmp community read public
[RouterA] snmp community write private
[RouterA] snmp sys-info version v2c
```

# 配置通过 SNMP 向网管端发送 Trap。

```
[RouterA] snmp trap enable feature-name nqa trap-name nqafallingalarmnotification
[RouterA] snmp trap enable feature-name nqa trap-name nqarisinalarmnotification
[RouterA] snmp target-host trap address udp-domain 11.1.2.8 params securityname alarm v2c
```

**步骤 5** 验证配置结果。

```
<RouterA> display nqa-event
NQA event information:
```

```

NQA Event Max: 5 NQA Event Number: 1

```

```
[RouterA-nqa-admin-icmp] display nqa-alarm
NQA alarm information:
```

```

NQA Alarm Max: 5 NQA Alarm Number: 1

```

```
<RouterA> display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 1
NQA Flow Max:1000 NQA Flow Remained:1000
nqa test-instance admin icmpjitter
test-type icmpjitter
```

```
destination-address ipv4 11.1.1.20
frequency 5
alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-threshold 1
0 10
nqa status : normal
```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 11.1.2.1 255.255.255.0
#
interface NULL0
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
nqa-jitter tag-version 2
nqa event 10 log-trap
nqa test-instance admin icmpjitter
 test-type icmpjitter
 destination-address ipv4 11.1.1.20
 frequency 5
 alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-threshold 1
0 10
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100000B31
snmp-agent sys-info version v2c v3
snmp-agent target-host trap address udp-domain 11.1.2.8 params securityname alarm v2c
snmp-agent trap enable feature-name NQA trap-name nqaRisingAlarmNotification
snmp-agent trap enable feature-name NQA trap-name nqaFallingAlarmNotification
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
aps fast-interval 0
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.20 255.255.255.0
#
return
```

## 6.50.36 配置 Martini VPLS 的 VPLS 组播 Ping 测试示例

通过 VPLSMPING 测试例检测 Martini 方式 VPLS 网络的连通情况。

## 组网需求

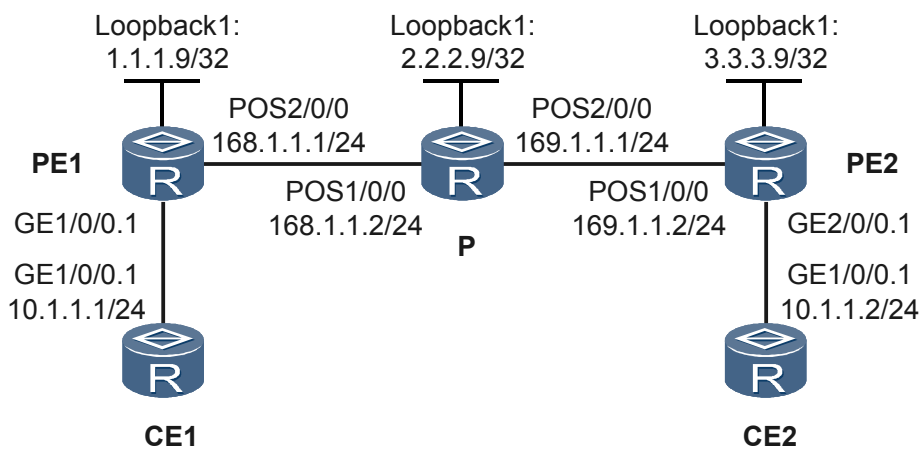
如图 6-33 所示。

两台路由器 PE1 和 PE2 作为 PE 使能 VPLS 功能。CE1 挂在 PE1 路由器上，CE2 挂在 PE2 上。CE1 和 CE2 属于一个 VPLS。采用 LDP 作为 VPLS 信令建立 PW，配置 VPLS，实现 CE1 与 CE2 的互通。PE 设备使能 IGMP Snooping。

NQA 的 VPLS 组播 Ping 功能可以实现对图 6-33 所示网络如下性能指标的检测：

- 对 VPLS 域内指定 VSI 的 PE 设备进行组播连通性检测。
- 对 VPLS 域内指定 VSI 的 egress 节点设备进行 IGMP Snooping 功能检测。

图 6-33 Martini 方式 VPLS 组网图



## 配置思路

采用如下的思路配置 Martini 方式 VPLS 的基本功能：

1. 配置 Martini VPLS。
2. 在 PE1，PE2 上使能 IGMP Snooping。
3. 在 PE1 上配置 NQA VPLS mPing 测试例，指定非保留组播为目的地址发起测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口
- Ping 的目的组播地址

## 操作步骤

### 步骤 1 配置 Martini VPLS

在 MPLS 骨干网上配置 Martini VPLS。具体配置过程请参见《配置指南 VPN》“VPLS 配置”。

#### 步骤 2 使能 IGMP Snooping

在 PE1, PE2 上使能 IGMP Snooping。具体配置过程请参见《配置指南 IP 组播》“二层组播配置”。

#### 步骤 3 配置 NQA VPLS mPing 测试例，指定非保留组播地址为目的地址。

#在 PE1 执行以下操作：

```
<PE1> system-view
[PE1] nqa test-instance test vplsm ping
[PE1-nqa-test-vplsm ping] test-type vplsm ping
[PE1-nqa-test-vplsm ping] destination-address ipv4 225.0.0.1
[PE1-nqa-test-vplsm ping] vsi a2
```

#### 步骤 4 启动测试操作。

```
[PE1-nqa-test-vplsm ping] start now
```

#### 步骤 5 验证测试结果

```
[PE1-nqa-test-vplsm ping] display nqa results test-instance test vplsm ping
NQA entry (admin, vplsm ping) :testflag is inactive ,testtype is vplsm ping
 1 . Test 1 result The test is finished
 Completions: success Timeouts number: 0
 Drops number: 0 TargetAddress: 225.0.0.1
 ProbeResponses number: 3 SentProbes number: 3
 Busies: 0 SequenceError number: 0
 Lost packet ratio: 0%
 1 . Receiver 1
 CompletionTime Min/Max/Sum/Avg: 30/190/260/87
 Sum2CompletionTime: 38600
 LastGoodProbe time: 2009-4-23 11:48:9.4
 ReceiverAddress: 168.1.1.1
 Fib hit: Hit
```

----结束

## 配置文件

#### ● CE1 的配置文件

```
#
sysname CE1
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.1.1 255.255.255.0
#
return
```

#### ● CE2 的配置文件

```
#
sysname CE2
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.2.1 255.255.255.0
#
return
```

## ● PE1 的配置文件

```
#
 sysname PE1
#
 igmp-snooping enable
#

mpls lsr-id 1.1.1.9
mpls
mpls l2vpn
#
vsi a2 static
 pwsignal ldp
 vsi-id 2
peer 3.3.3.9
 igmp-snooping enable
#
mpls ldp
#
mpls ldp remote-peer pe2
 remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
 vlan-type dot1q 10
 l2 binding vsi a2
#
interface Pos2/0/0
 link-protocol ppp
 ip address 168.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 168.1.1.0 0.0.0.255
#
nqa test-instance test vplsm ping
 test-type vplsm ping
 destination-address ipv4 225.0.0.1
 vsi a2
#
return
```

## ● P 的配置文件

```
#
 sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 ip address 168.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
```

```
ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 168.1.1.0 0.0.0.255
 network 169.1.1.0 0.0.0.255
 network 2.2.2.9 0.0.0.0
#
return
```

- PE2 的配置文件

```
#
sysname PE2
#
igmp-snooping enable
#
mpls lsr-id 3.3.3.9
mpls
mpls l2vpn
#
vsi a2 static
 pwsignal ldp
 vsi-id 2
peer 1.1.1.9
igmp-snooping enable
#
mpls ldp
#
mpls ldp remote-peer pe1
 remote-ip 1.1.1.9
#
interface Pos1/0/0
 link-protocol ppp
 ip address 169.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0.1
 vlan-type dot1q 10
 l2 binding vsi a2
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 169.1.1.0 0.0.0.255
#
return
```

### 6.50.37 配置 Kompella VPLS 的 VPLS 组播 Ping 测试示例

通过 VPLSMPING 测试例检测 Kompella 方式 VPLS 网络的连通情况。

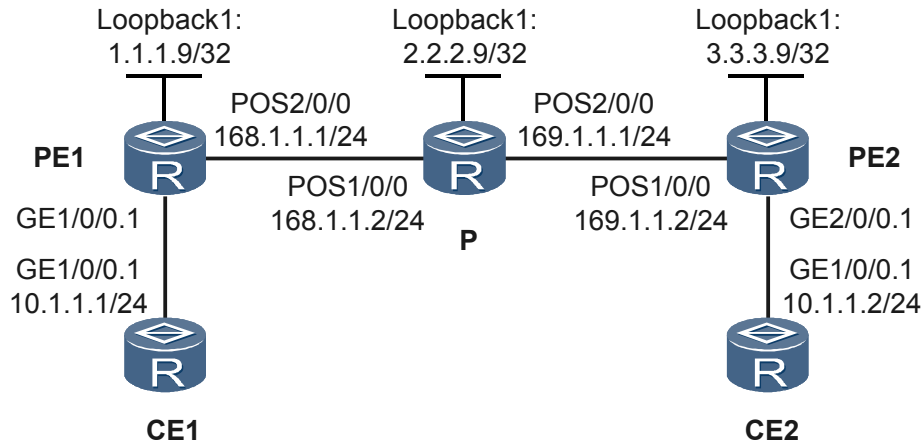
#### 组网需求

如图 6-34 所示。

两台路由器 PE1 和 PE2 作为 PE 启动 VPLS 功能。CE1 挂在 PE1 上，CE2 挂在 PE2 上。CE1 和 CE2 属于一个 VPLS。

采用 BGP 作为 VPLS 信令建立 PW，通过配置 VPN Target 实现 VPLS PE 的自动发现，实现 CE1 与 CE2 的互通。使用 NQA VPLS mPing 功能测试 PE1 与 PE2 之间的组播转发功能是否正常。

图 6-34 Kompella 方式 VPLS 组网图



## 配置思路

采用如下的思路配置 Kompella 方式 VPLS 的基本功能：

1. 配置 Kompella VPLS。
2. 在 PE1 上发起 NQA VPLS mPing，指定保留组播为目的地址发起测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- 对等体的 IP 地址
- PE1、PE2 上的 VSI 名称
- PE1、PE2 上的 BGP AS 号
- VSI 的信令模式为 BGP
- PE 上 VSI 的 RD 和 VPN-Target，VSI 所属的 Site ID
- 绑定 VSI 的接口和接口上封装的 VLAN ID 值
- Ping 的目的组播地址

## 操作步骤

### 步骤 1 配置 Kompella VPLS。

在 MPLS 骨干网上配置 Kompella VPLS。具体配置过程请参见《配置指南 VPN》“VPLS 配置”。

### 步骤 2 配置 NQA VPLS mPing 测试例，指定保留组播地址为目的地址。

# 在 PE1 执行以下操作：

```
<PE1> system-view
[PE1] nqa test-instance test vplsmping
[PE1-nqa-test-vplsmping] test-type vplsmping
[PE1-nqa-test-vplsmping] destination-address ipv4 224.0.0.1
[PE1-nqa-test-vplsmping] vsi a2
```



### 步骤 3 启动测试操作

```
[PE1-nqa-test-vplsmping] start now
```

### 步骤 4 验证测试结果

```
<PE1> display nqa results test-instance test vplsmping
NQA entry (admin, vplsmping) :testflag is inactive ,testtype is vplsmping
 1 . Test 1 result The test is finished
 Completions: success Timeouts number: 0
 Drops number: 0 TargetAddress: 224.0.0.1
 ProbeResponses number: 3 SentProbes number: 3
 Busies: 0 SequenceError number: 0
 Lost packet ratio: 0%
 1 . Receiver 1
 CompletionTime Min/Max/Sum/Avg: 30/190/260/87
 Sum2CompletionTime: 38600
 LastGoodProbe time: 2009-4-23 11:48:9.4
 RecevierAddress: 168.1.1.1
 Fib hit: NoHit
```

----结束

## 配置文件

- CE1 的配置文件

```
#
sysname CE1
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.1.1 255.255.255.0
#
return
```

- CE2 的配置文件

```
#
sysname CE2
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.2.1 255.255.255.0
#
return
```

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.9
mpls
mpls l2vpn
#
vsi bgp1 auto
pwsignal bgp
route-distinguisher 168.1.1.1:1
vpn-target 100:1 import-extcommunity
vpn-target 100:1 export-extcommunity
site 1 range 5 default-offset 0
#
mpls ldp
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
```

```

12 binding vsi bgp1
#
interface Pos2/0/0
 link-protocol ppp
 ip address 168.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack1
#
 vpls-family
 policy vpn-target
 peer 3.3.3.9 enable
#
ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 168.1.1.0 0.0.0.255
#
nqa test-instance test vplsmping
 test-type vplsmping
 destination-address ipv4 224.0.0.1
 vsi a2
#
return

```

#### ● P 的配置文件

```

#
 sysname P
#
 mpls lsr-id 2.2.2.9
 mpls
#
 mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 ip address 168.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 ip address 169.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 168.1.1.0 0.0.0.255
 network 169.1.1.0 0.0.0.255
 network 2.2.2.9 0.0.0.0
#
return

```

#### ● PE2 的配置文件

```

#
 sysname PE2
#
 mpls lsr-id 3.3.3.9
 mpls

```

```
mpls l2vpn
#
vsi bgp1 auto
pwsignal bgp
route-distinguisher 169.1.1.2:1
vpn-target 100:1 import-extcommunity
vpn-target 100:1 export-extcommunity
site 2 range 5 default-offset 0
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
vlan-type dot1q 10
l2 binding vsi bgp1
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
bgp 100
peer 1.1.1.9 as-number 100
peer 1.1.1.9 connect-interface LoopBack1
#
vpls-family
policy vpn-target
peer 1.1.1.9 enable
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 169.1.1.0 0.0.0.255
return
```

## 6.50.38 配置 Martini VPLS 的 VPLS 组播 Trace 测试示例

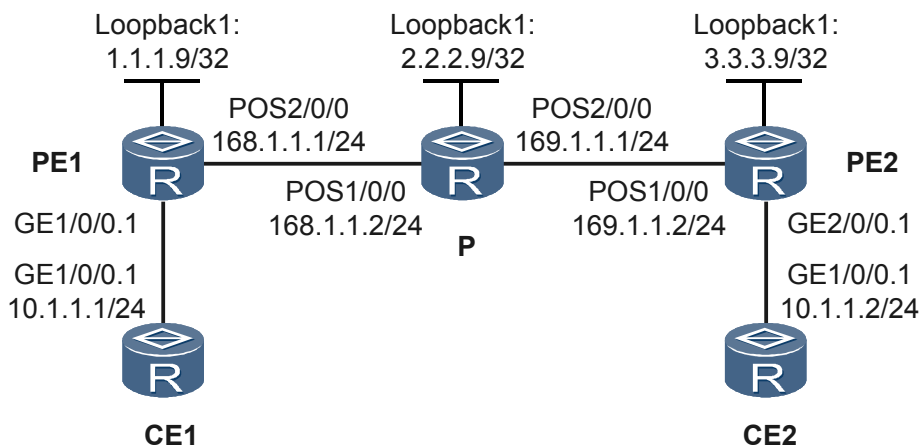
### 组网需求

如图 6-35 所示。

两台路由器 PE1 和 PE2 作为 PE 使能 VPLS 功能。CE1 挂在 PE1 路由器上，CE2 挂在 PE2 上。CE1 和 CE2 属于一个 VPLS。采用 LDP 作为 VPLS 信令建立 PW，配置 VPLS，实现 CE1 与 CE2 的互通。PE 设备使能 IGMP Snooping。

NQA 的 VPLS 组播 Trace 功能可以实现对图 6-35 所示网络验证 PE 设备的 IGMP Snooping 是否正常，对 PE 进行路径发现及故障定位。

图 6-35 Martini 方式 VPLS 组网图



## 配置思路

采用如下的思路配置 Martini 方式 VPLS 的基本功能：

1. 配置 Martini VPLS。
2. 在 PE1，PE2 上使能 IGMP Snooping。
3. 在 PE1 上配置 NQA VPLS mTrace 测试例，指定非保留组播为目的地址发起测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口
- Trace 的目的组播地址

## 操作步骤

### 步骤 1 配置 Martini VPLS

在 MPLS 骨干网上配置 Martini VPLS。具体配置过程请参见《配置指南 VPN》“VPLS 配置”。

### 步骤 2 使能 IGMP Snooping

在 PE1，PE2 上使能 IGMP Snooping。具体配置过程请参见《配置指南 IP 组播》“二层组播配置”。

### 步骤 3 配置 NQA VPLS mTrace 测试例，指定非保留组播地址为目的地址。

# 在 PE1 执行以下操作：

```
<PE1> system-view
[PE1] nqa test-instance test vplsmtrace
[PE1-nqa-test-vplsmtrace] test-type vplsmtrace
[PE1-nqa-test-vplsmtrace] destination-address ipv4 225.0.0.1
```

```
[PE1-nqa-test-vplsmtrace] vsi a2
[PE1-nqa-test-vplsmtrace] remote-address ipv4 3.3.3.9
```

#### 步骤4 启动测试操作

```
[PE1-nqa-test-vplsmtrace] start now
```

#### 步骤5 验证测试结果

```
[PE1-nqa-test-vplsmtrace] display nqa results test-instance test vplsmtrace
NQA entry(test, vplsmtrace) :testflag is inactive ,testtype is vplsmtrace
1. Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2009-12-03 09:42:46.7
1. Hop 1
Send operation times: 1 Receive response times: 1
Min/Max/Average Completion Time: 0/0/0
Sum/Square-Sum Completion Time: 0/0
RTD OverThresholds number: 0
Last Good Probe Time: 2009-12-03 09:42:43.9
Destination ip address:3.3.3.9
Lost packet ratio: 0 %
```

----结束

## 配置文件

### ● CE1 的配置文件

```
#
sysname CE1
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.1.1 255.255.255.0
#
return
```

### ● CE2 的配置文件

```
#
sysname CE2
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 100.1.2.1 255.255.255.0
#
return
```

### ● PE1 的配置文件

```
#
sysname PE1
#
igmp-snooping enable
#

mpls lsr-id 1.1.1.9
mpls
mpls l2vpn
#
vsi a2 static
```

```

pwsignal ldp
vsi-id 2
peer 3.3.3.9
igmp-snooping enable
#
mpls ldp
#
mpls ldp remote-peer pe2
remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
l2 binding vsi a2
#
interface Pos2/0/0
link-protocol ppp
ip address 168.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 168.1.1.0 0.0.0.255
#
nqa test-instance test vplsmtrace
test-type vplsmtrace
destination-address ipv4 225.0.0.1
vsi a2
remote-address ipv4 3.3.3.9
#
return

```

- P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
ip address 168.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 168.1.1.0 0.0.0.255
network 169.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return

```

- PE2 的配置文件

```
#
 sysname PE2
#
 igmp-snooping enable
#
 mpls lsr-id 3.3.3.9
 mpls
 mpls l2vpn
#
 vsi a2 static
 pwsignal ldp
 vsi-id 2
 peer 1.1.1.9
 igmp-snooping enable
#
 mpls ldp
#
 mpls ldp remote-peer pe1
 remote-ip 1.1.1.9
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 169.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
 interface GigabitEthernet2/0/0.1
 vlan-type dot1q 10
 l2 binding vsi a2
#
 interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
 ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 169.1.1.0 0.0.0.255
#
return
```

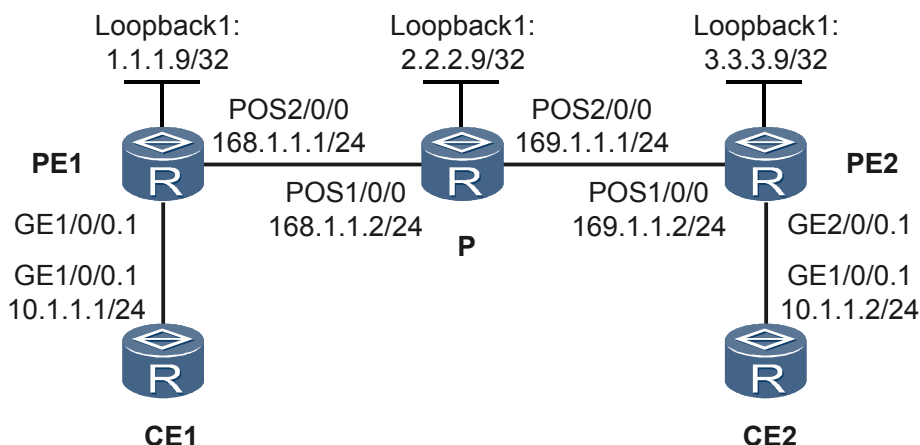
### 6.50.39 配置 VPLS MAC Ping 测试示例

#### 组网需求

如图 6-36，两台路由器 PE1 和 PE2 作为 PE 启动 VPLS 功能。CE1 挂在 PE1 设备上，CE2 挂在 PE2 上。CE1 和 CE2 属于一个 VPLS。采用 LDP 作为 VPLS 信令建立 PW，配置 VPLS，实现 CE1 与 CE2 的互通。

使用 VPLS MAC Ping 测试 VPLS 网络的连通性。

图 6-36 配置 VPLS MAC Ping 测试组网图



## 配置思路

采用如下的思路配置 VPLS MAC Ping 测试的基本功能：

1. 配置 Martini 方式 VPLS 网络。
2. 在 PE1 上配置 VPLS MAC Ping 测试例。
3. 启动 NQA 测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID。
- 对等体的 IP 地址及建立对等体时使用的隧道策略。
- 绑定 VSI 的接口。
- Ping 对端的 MAC 地址。

## 操作步骤

### 步骤 1 配置 Martini 方式 VPLS 网络。

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“VPLS 配置”。

### 步骤 2 配置 Martini 方式 VPLS 网络的 VPLS MAC Ping 测试例。

# 配置 PE1。

```
<PE1> system-view
[PE1] nqa test-instance test vplsping
[PE1-nqa-test-vplsping] test-type vplsping
[PE1-nqa-test-vplsping] vsi a2
[PE1-nqa-test-vplsping] destination-address mac 00e0-5952-6f01
```

### 步骤 3 启动测试操作。

```
[PE1-nqa-test-vplsping] start now
```



**步骤 4** 验证测试结果。

在 PE 上执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE1-nqa-test-vplsing] display nqa results
NQA entry (test, vplsing) :testflag is inactive ,testtype is vplsing
1. Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:170.1.1.1
 Min/Max/Average Completion Time: 21/30/24
 Sum/Square-Sum Completion Time: 74/1870
 Last Good Probe Time: 2009-4-21 9:49:50.1
 Lost packet ratio: 0 %
```

----结束

**配置文件**

## ● CE1 的配置文件

```
#
 sysname CE1
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.1 255.255.255.0
#
return
```

## ● CE2 的配置文件

```
#
 sysname CE2
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.2 255.255.255.0
#
return
```

## ● PE1 的配置文件

```
#
 sysname PE1
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls l2vpn
#
 vsi a2 static
 pwsignal ldp
 vsi-id 2
 peer 3.3.3.9
#
 mpls ldp
#
 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 12 binding vsi a2
```

```
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 168.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
nqa test-instance test vplsing
 test-type vplsing
 vsi a2
 mac 00e0-5952-6f01
#
ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 168.1.1.0 0.0.0.255
#
return
```

- P 的配置文件

```
#
 sysname P
#
 mpls lsr-id 2.2.2.9
 mpls
#
 mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 168.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 169.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 168.1.1.0 0.0.0.255
 network 169.1.1.0 0.0.0.255
 network 2.2.2.9 0.0.0.0
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 mpls lsr-id 3.3.3.9
 mpls
#
 mpls l2vpn
#
vsi a2 static
 pwsignal ldp
 vsi-id 2
 peer 1.1.1.9
```

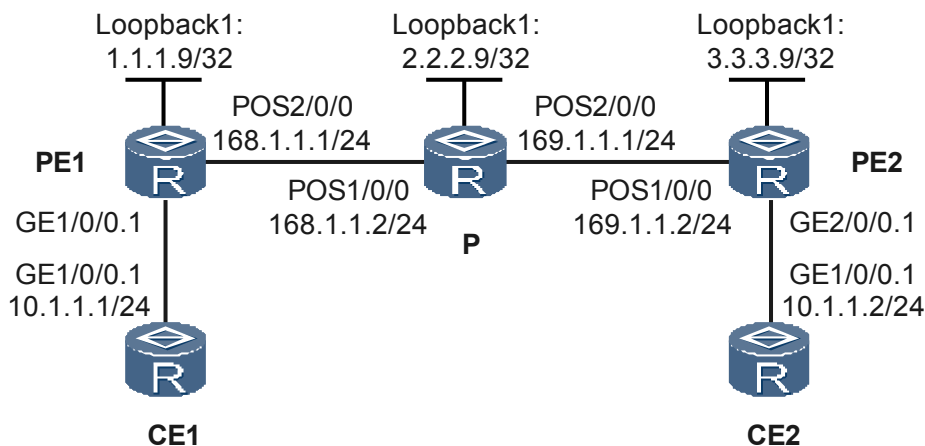
```
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
undo shutdown
vlan-type dot1q 10
12 binding vsi a2
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 169.1.1.0 0.0.0.255
#
return
```

## 6.50.40 配置 VPLS MAC Trace 测试示例

### 组网需求

如图 6-37 所示，使用 VPLS MAC Trace 测试 VPLS 网络的连通性，定位故障。

图 6-37 配置 VPLS MAC Trace 测试组网



### 配置思路

采用如下的思路配置配置 VPLS MAC Trace 测试的基本功能：

1. 配置 Martini 方式 VPLS 网络。

2. 在 PE1 上配置 VPLS MAC Trace 测试例。
3. 启动 NQA 测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口
- Trace 对端的 MAC 地址

## 操作步骤

### 步骤 1 配置 Martini 方式 VPLS 网络

具体配置过程请参见 HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“VPLS 配置”

### 步骤 2 配置 Martini 方式 VPLS 网络的 VPLS MAC Trace 测试例

# 配置 PE1

```
<PE1> system-view
[PE1] nqa test-instance test vplstrace
[PE1-nqa-test-vplstrace] test-type vplstrace
[PE1-nqa-test-vplstrace] vsi a2
[PE1-nqa-test-vplstrace] destination-address mac 00e0-5952-6f01
```

### 步骤 3 启动测试操作

```
[PE1-nqa-test-vplstrace] start now
```

### 步骤 4 验证测试结果

在 PE 上执 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE1-nqa-test-vplstrace] display nqa results
NQA entry (test, vplstrace) :testflag is inactive ,testtype is vplstrace
1. Test 1 result The test is finished
 Completion:success Attempts number:1
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Drop operation number:0
 Last good path Time:2009-4-21 9:51:4.1
1. Hop 1
 Send operation times: 1 Receive response times: 1
 Min/Max/Average Completion Time: 0/0/0
 Sum/Square-Sum Completion Time: 0/0
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-21 9:51:1.5
 Destination ip address:
 Lost packet ratio: 0 %,
2. Hop 2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average Completion Time: 0/0/0
 Sum/Square-Sum Completion Time: 0/0
 RTD OverThresholds number: 0
 Last Good Probe Time: 2009-4-21 9:51:4.1
 Destination ip address:
 Lost packet ratio: 0 %
```

----结束

## 配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.1 255.255.255.0
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.2 255.255.255.0
#
return
```

- PE1 的配置文件

```
#
 sysname PE1
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls l2vpn
#
vsi a2 static
 pwsignal ldp
 vsi-id 2
 peer 3.3.3.9
#
 mpls ldp
#
 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 l2 binding vsi a2
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 168.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 168.1.1.0 0.0.0.255
#
return
```

- P 的配置文件

```
#
 sysname P
#
```

```

mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 168.1.1.0 0.0.0.255
network 169.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return

```

#### ● PE2 的配置文件

```

#
sysname PE2
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 1.1.1.9
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi a2
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 169.1.1.0 0.0.0.255
#
return

```

## 6.50.41 配置 VPLS PW Ping 和 PW Trace 测试示例

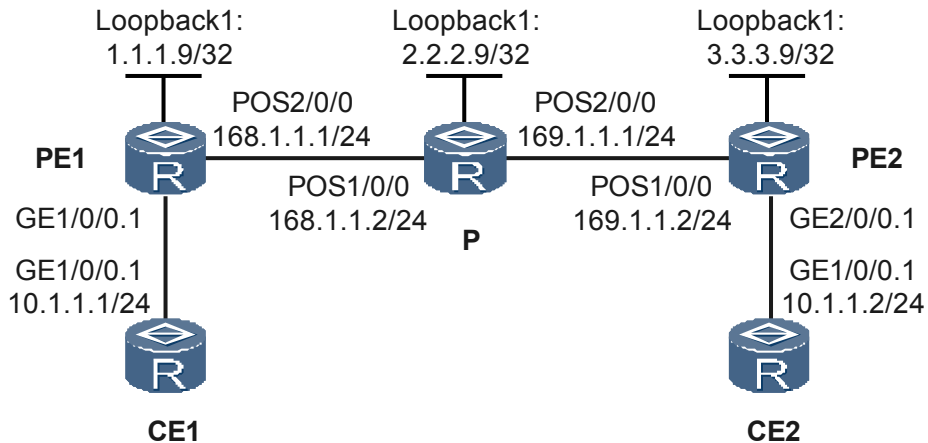
### 组网需求

PW 的连通性关系到用户间流量转发是否正常，PW 的转发性能关系到网络能否符合签订的 SLA。VPLS PW Ping 和 PW Trace 正是这样的工具，用于测量 PW 的连通性，收集 PW 的性能数据，进行路径发现和故障定位隔离等。

NQA 与普通命令行发起方式检测原理相同，NQA 的优点是增加了调度和结果收集的机制以及阈值告警等。Trace 用于故障定位和路径发现，可以与 Ping 结合起来，当 Ping 发现问题后，联动 Trace 测试例，记录当时出现故障的问题所在。

如图 6-38 所示，使用 VPLS PW Ping 和 PW Trace 测试 VPLS 网络的连通性，定位 PW 故障。

图 6-38 配置 VPLS PW Ping 和 PW Trace 测试组网



### 配置思路

采用如下的思路配置 VPLS PW Ping 和 PW Trace 测试的基本功能：

1. 配置 VPLS 网络，为 NQA 测试例启动配置业务环境。本例配置的是 Martini 方式 VPLS 网络。
2. 在 PE1 上配置 PW Ping 和 PW Trace 测试例。指定测试例的必选配置。
3. 启动 NQA 测试。

### 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口

## 操作步骤

### 步骤 1 配置 Martini 方式 VPLS 网络

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“VPLS 配置”

### 步骤 2 配置 VPLS PW Ping 和 PW Trace 测试例

#### 1. 配置 VPLS PW Ping 测试例并启动测试操作

# 配置 PE1

```
<PE1> system-view
[PE1] nqa test-instance test vplspwping
[PE1-nqa-test-vplspwping] test-type vplspwping
[PE1-nqa-test-vplspwping] vsi a2
[PE1-nqa-test-vplspwping] destination-address ipv4 3.3.3.9
```

# 启动测试操作

```
[PE1-nqa-test-vplstrace] start now
```

#### 2. 配置 VPLS PW Trace 测试例并启动测试操作

# 配置 PE1

```
<PE1> system-view
[PE1] nqa test-instance test vplspwtrace
[PE1-nqa-test-vplspwtrace] test-type vplspwtrace
[PE1-nqa-test-vplspwtrace] vsi a2
[PE1-nqa-test-vplspwtrace] destination-address ipv4 3.3.3.9
```

# 启动测试操作

```
[PE1-nqa-test-vplstrace] start now
```

### 步骤 3 验证测试结果

在 PE 上分别进入 PW Ping 和 PW Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE1-nqa-test-vplspwping] display nqa results
NQA entry(vplspw,ping) :testflag is inactive ,testtype is vplspwping
1 . Test 1 result The test is finished
SendProbe:3 ResponseProbe:3
Completion:success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
NumOfRTT:3 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:10 Min Positive DS:40
Max Positive SD:10 Max Positive DS:40
Positive SD Number:1 Positive DS Number:1
Positive SD Sum:10 Positive DS Sum:40
Positive SD Square Sum:100 Positive DS Square Sum:1600
Min Negative SD:20 Min Negative DS:30
Max Negative SD:20 Max Negative DS:30
Negative SD Number:1 Negative DS Number:1
Negative SD Sum:20 Negative DS Sum:30
Negative SD Square Sum:400 Negative DS Square Sum:900
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:25
Average of Jitter SD:15 Average of Jitter DS:35
```



```

jitter out value:0.6119792 jitter in value:1.4062500
NumberOfOWD:0 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%

[PE1-nqa-test-vplspwtrace] display nqa results
NQA entry(vplspw, tracert) :testflag is inactive ,testtype is vplspwtrace
1. Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1. Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %

```

----结束

## 配置文件

- CE1 的配置文件

```

#
sysname CE1
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
return

```

- CE2 的配置文件

```

#
sysname CE2
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
return

```

- PE1 的配置文件

```

#
sysname PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 3.3.3.9
#
mpls ldp
#

```

```

mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
12 binding vsi a2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
nqa test-instance test vplspwping
test-type vplspwping
vsi a2
destination-address ipv4 3.3.3.9
#
nqa test-instance test vplspwtrace
test-type vplspwtrace
vsi a2
destination-address ipv4 3.3.3.9
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 168.1.1.0 0.0.0.255
#
return

```

- P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 168.1.1.0 0.0.0.255
network 169.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return

```

- PE2 的配置文件

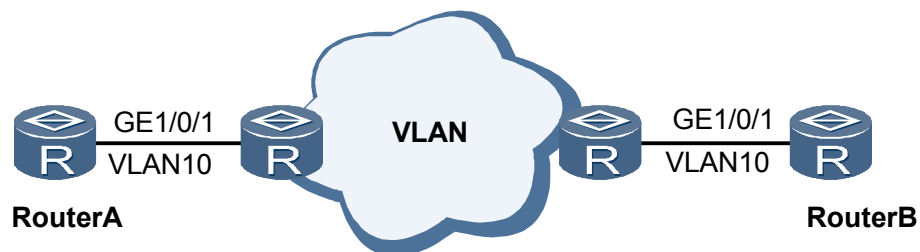
```
#
 sysname PE2
#
 mpls lsr-id 3.3.3.9
 mpls
#
 mpls l2vpn
#
 vsi a2 static
 pwsignal ldp
 vsi-id 2
 peer 1.1.1.9
#
 mpls ldp
#
 mpls ldp remote-peer 1.1.1.9
 remote-ip 1.1.1.9
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 169.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 vlan-type dot1q 10
 l2 binding vsi a2
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 169.1.1.0 0.0.0.255
#
return
```

## 6.50.42 配置 MAC Trace 测试 VLAN 示例

### 组网需求

如图 6-39 所示，所有设备在同一个 VLAN 网络中，各设备均使能了以太网 CFM 的基本功能。使用 VLAN MAC Trace 测试 VLAN 网络的连通性、定位故障。

图 6-39 配置 MAC Trace 测试 VLAN 组网



### 配置思路

采用如下的思路配置 MAC Trace 测试 VLAN 的基本功能：

1. 配置 VLAN 网络，为 NQA 测试例启动配置业务环境。
2. 配置以太网 CFM，将 CFM 与 VLAN 映射。
3. 在 RouterA 上配置 NQA MAC Trace 测试例。指定测试例的必选配置。
4. 启动 NQA 测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VLAN ID
- 对端 MAC 地址

## 操作步骤

**步骤 1** 配置 RouterA 和 RouterB 加入 VLAN 10。

# 配置 RouterA。

```
<HUAWEI> system-view
<HUAWEI> sysname RouterA
[RouterA] vlan 10
[RouterA-vlan10] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] portswitch
[RouterA-GigabitEthernet1/0/1] port default vlan 10
```

# 配置 RouterB 配置与 RouterA 类似，此处略。

**步骤 2** 配置 RouterA 和 RouterB 之间的以太网 CFM 功能，并将 MA 与 VLAN 10 映射

# 配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] cfm version standard
[RouterA] cfm enable
[RouterA] cfm md md1
[RouterA-md-md1] ma ma1
[RouterA-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/1 outward
[RouterA-md-md1-ma-ma1] remote-mep mep-id 2
[RouterA-md-md1-ma-ma1] map vlan 10
[RouterA-md-md1-ma-ma1] quit
[RouterA-md-md1] quit
```

# 配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] cfm version standard
[RouterB] cfm enable
[RouterB] cfm md md1
[RouterB-md-md1] ma ma1
[RouterB-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/1 outward
[RouterB-md-md1-ma-ma1] remote-mep mep-id 1
[RouterB-md-md1-ma-ma1] map vlan 10
[RouterB-md-md1-ma-ma1] quit
[RouterB-md-md1] quit
```

 说明

指定 MEP 所在的接口必须是二层接口，且一个接口上只能创建一个 MEP。

在 RouterA 上执行 **display cfm remote-mep** 查看以太网 CFM 状态，显示结果为 Up。

```
[RouterA] display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPS : 1 up, 0 down, 0 disable

MD Name : md1
Level : 0
MA Name : ma1
RMEP ID : 2
Vlan ID : --
VSI Name : --
MAC : --
CCM Receive : enabled
Trigger-If-Down : disabled
CFM Status : up
```

### 步骤3 配置 VLAN MAC Trace 测试例

# 配置 RouterA。

```
<RouterA> system-view
[RouterA] nqa test-instance test mactrace
[RouterA-nqa-test-mactrace] test-type mactrace
[RouterA-nqa-test-mactrace] destination-address mac 00e0-fca4-8ae7
[RouterA-nqa-test-mactrace] md md1 ma ma1
[RouterA-nqa-test-mactrace] mep mep-id 1
```

# 启动测试操作。

```
[RouterA-nqa-test-mactrace] start now
```

### 步骤4 验证测试结果

在 RouterA 上进入 MAC Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[RouterA-nqa-test-mactrace] display nqa results
NQA entry (mac, trace) :testflag is inactive ,testtype is mactrace
1. Test 1 result The test is finished
 Completion:success Attempts number:1
 Drop operation number:0 Operation timeout number:0
 System busy operation number:0
 Last good path Time:2000-01-05 02:35:35.0
```

----结束

## 配置文件

### ● RouterA 的配置文件

```
#
sysname RouterA
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
#

cfm md md1
ma ma1
mep mep-id 1 interface GigabitEthernet1/0/1 outward
remote-mep mep-id 2
map vlan 10
#
nqa test-instance test mactrace
```

```
test-type mactrace
destination-address mac 00e0-fca4-8ae7
md md1 ma mal
mep mep-id 1
#
return

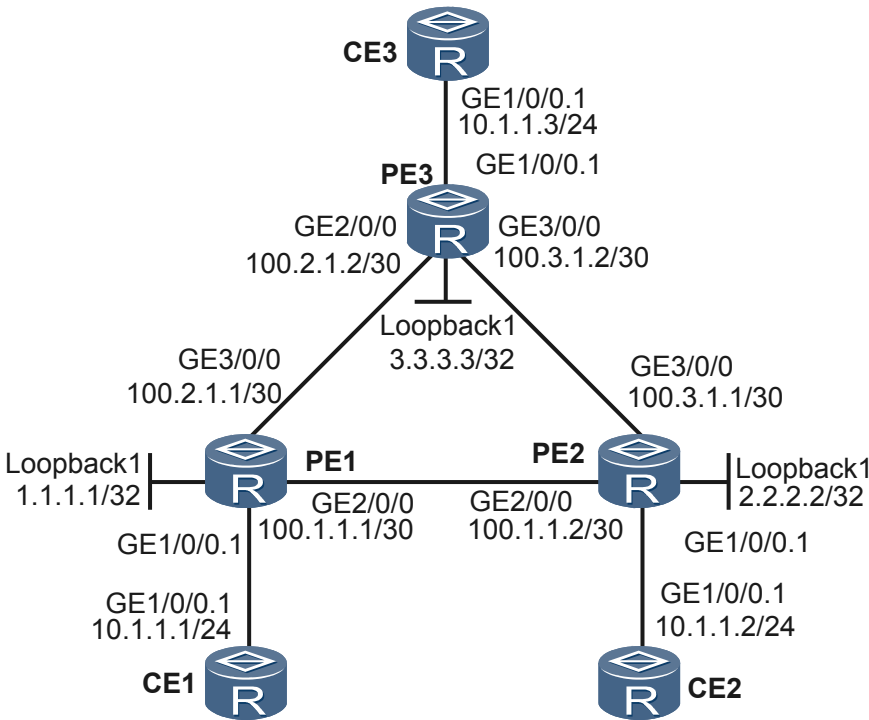
● RouterB 的配置文件
#
sysname RouterB
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
#
cfm md md1
ma mal
mep mep-id 1 interface GigabitEthernet1/0/1 outward
remote-mep mep-id 1
map vlan 10
#
return
```

6.50.43 配置 MAC Trace 测试 VPLS 示例

组网需求

如图 6-40 所示 VPLS 网络中，使用 NQA VPLS MAC Trace 测试 VPLS 网络的连通性并定位故障。三台 PE 配置 CFM 功能。在 PE1 上配置 NQA VPLS MAC Trace 测试例，设置目的 MAC 地址为 PE2 的接口 MAC 地址，从 PE1 发起测试，测试 PE1 和 PE2 之间的连通性。

图 6-40 配置 MAC Trace 测试 VPLS 组网



## 配置思路

采用如下的思路配置 MAC Trace 测试 VPLS 的基本功能：

1. 配置 Martini VPLS，为 NQA 测试例启动配置业务环境。
2. 在 PE 上配置基于 VPLS 的以太网 CFM。
3. 在 PE1 上配置 NQA VPLS MAC Trace 测试例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IP 地址
- 各个 PE 上的 MPLS LSR-ID
- PE1、PE2 和 PE3 上的 VSI 名称和 VSI-ID
- 绑定 VSI 的接口
- 以太网 CFM 中 MD 的名称和级别、MA 的名称和 MEP 的 ID、MEP 所在接口的名称、MEP 的类型
- 目的 MAC 地址

## 操作步骤

**步骤 1** 配置 Martini VPLS 在 MPLS 骨干网上配置 Martni VPLS。

请参见配置文件，具体配置过程请参见《配置指南 VPN》“VPLS 配置”。

**步骤 2** 在 PE 上配置以太网 CFM 功能

# 配置 PE1。

```
[PE1] cfm version standard
[PE1] cfm enable
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] ccm-interval 30
[PE1-md-md1-ma-ma1] map vsi ldpl
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/0.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] remote-mep mep-id 3
[PE1-md-md1-ma-ma1] quit
```

# 配置 PE2。

```
[PE2] cfm version standard
[PE2] cfm enable
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] ccm-interval 30
[PE2-md-md1-ma-ma1] map vsi ldpl
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/0.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] remote-mep mep-id 3
[PE2-md-md1-ma-ma1] quit
```

# 配置 PE3。

```
[PE3] cfm version standard
[PE3] cfm enable
```

```
[PE3] cfm md md1
[PE3-md-md1] ma mal
[PE3-md-md1-ma-mal] ccm-interval 30
[PE3-md-md1-ma-mal] map vsi ldpl
[PE3-md-md1-ma-mal] mep mep-id 3 interface gigabitethernet 1/0/0.1 inward
[PE3-md-md1-ma-mal] remote-mep mep-id 1
[PE3-md-md1-ma-mal] remote-mep mep-id 2
[PE3-md-md1-ma-mal] quit
```

### 步骤 3 配置 VPLS MAC Trace 测试例

# 配置 PE1。

```
<PE1> system-view
[PE1] nqa test-instance test mactrace
[PE1-nqa-test-mactrace] test-type mactrace
[PE1-nqa-test-mactrace] destination-address mac 00e0-fca4-8ae7
[PE1-nqa-test-mactrace] md md1 ma mal
[PE1-nqa-test-mactrace] mep mep-id 1
```

# 启动测试操作。

```
[PE1-nqa-test-mactrace] start now
```

### 步骤 4 验证测试结果

在 PE1 上进入 MAC Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果成功。

```
[PE1-nqa-test-mactrace] display nqa results
NQA entry (mac, trace) :testflag is inactive ,testtype is mactrace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Drop operation number:0 Operation timeout number:0
System busy operation number:0
Last good path Time:2000-01-05 02:35:35.0
```

----结束

## 配置文件

### ● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 2
peer 2.2.2.2
peer 3.3.3.3
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
12 binding vsi ldpl
```



```
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.2.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
cfm md mdl
ma mal
ccm-interval 30
map vsi ldp1
mep mep-id 1 interface gigabitEthernet 1/0/0.1 inward
remote-mep mep-id 2
remote-mep mep-id 3
#
nqa test-instance test mactrace
test-type mactrace
destination-address mac 00e0-fca4-8ae7
md mdl ma mal
mep mep-id 1
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.3
network 100.2.1.0 0.0.0.3
#
return
```

## ● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
mpls l2vpn
#
vsi ldp1 static
pwsignal ldp
vsi-id 2
peer 1.1.1.1
peer 3.3.3.3
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi ldp1
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.1.1.2 255.255.255.252
mpls
mpls ldp
```

```
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.3.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
cfm md mdl
ma mal
ccm-interval 30
map vsi ldpl
mep mep-id 2 interface gigabitEthernet 1/0/0.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
remote-mep mep-id 3
remote-mep ccm-receive mep-id 3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.3
network 100.3.1.0 0.0.0.3
#
return
```

#### ● PE3 的配置文件

```
#
sysname PE3
#
cfm version standard
cfm enable
#
mpls lsr-id 3.3.3.3
mpls
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 2
peer 1.1.1.1
peer 2.2.2.2
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi ldpl
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.2.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.3.1.2 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
```

```
#
cfm md mdl
 ma mal
 ccm-interval 30
 map vsi ldp1
 mep mep-id 3 interface gigabitethernet 1/0/0.1 inward
 mep ccm-send mep-id 3 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
#
ospf 1
 area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 100.2.1.0 0.0.0.3
 network 100.3.1.0 0.0.0.3
#
return
```

- CE1 的配置文件

```
#
sysname CE1
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.1 255.255.255.0
#
return
```

- CE2 的配置文件

```
#
sysname CE2
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.2 255.255.255.0
#
return
```

- CE3 的配置文件

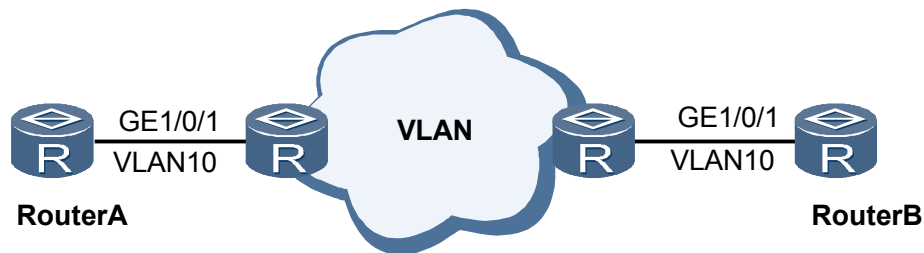
```
#
sysname CE3
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.3 255.255.255.0
#
return
```

## 6.50.44 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 示例

## 组网需求

如图 6-41 所示，所有设备在 VLAN 10 网络中。SwitchA 和 SwitchB 设备全局使能了 GMAC Ping 和 GMAC Trace 开关。在 SwitchA 上配置 NQA GMAC Ping 和 GMAC Trace 测试例，目的端为 RouterB。通过发起 NQA 测试例，检测 SwitchA 和 SwitchB 之间的连通性，并可以得到时延等信息。

图 6-41 配置 GMAC Ping 和 GMAC Trace 测试 VLAN 组网



## 配置思路

采用如下的思路配置 GMAC Ping 和 GMAC Trace 测试 VLAN 的基本功能：

1. 配置 VLAN 网络，为 NQA 测试例启动配置业务环境。
2. 在需要发起 GMAC Ping 和 GMAC Trace 的 NQA 客户端上配置 NQA 测试例。指定测试例的必选配置。
3. 启动 NQA 测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- Router
- VLAN ID
- 对端 MAC 地址

## 操作步骤

**步骤 1** 配置 RouterA 和 RouterB 加入 VLAN 10。

# 配置 RouterA。

```
<HUAWEI> system-view
<HUAWEI> sysname RouterA
[RouterA] vlan 10
[Router-vlan10] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] portswitch
[RouterA-GigabitEthernet1/0/1] port default vlan 10
```

# 配置 RouterB 配置与 RouterA 类似，此处略。

**步骤 2** 配置 CFM 协议的版本为标准版本，使能 GMAC Ping 和 GMAC Trace 开关

# 配置 RouterA。

```
[RouterA] cfm version standard
[RouterA] ping mac enable
[RouterA] trace mac enable
```

# 配置 RouterB 配置与 RouterA 类似，此处略。

### 步骤 3 配置 VLAN GMAC Ping 和 VLAN GMAC Trace 测试例

1. 配置 VLAN GMAC Ping 测试例并启动测试操作。

# 配置 RouterA。

```
<RouterA> system-view
[RouterA] nqa test-instance test gmacping
[RouterA-nqa-test-gmacping] test-type gmacping
[RouterA-nqa-test-gmacping] vlan 10
[RouterA-nqa-test-gmacping] destination-address mac 00e0-fca4-8ae7
```

# 启动测试操作。

```
[RouterA-nqa-test-gmacping] start now
```

2. 配置 VLAN GMAC Trace 测试例并启动测试操作

# 配置 RouterA。

```
<RouterA> system-view
[RouterA] nqa test-instance test gmactrace
[RouterA-nqa-test-gmactrace] test-type gmactrace
[RouterA-nqa-test-gmacping] vlan 10
[RouterA-nqa-test-gmacping] destination-address mac 00e0-fca4-8ae7
```

# 启动测试操作。

```
[RouterA-nqa-test-gmacping] start now
```

### 步骤 4 验证测试结果

在 RouterA 上分别进入 GMAC Ping 和 GMAC Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[RouterA-nqa-test-gmacping] display nqa results
NQA entry(gmac,ping) :testflag is inactive ,testtype is gmacping
1. Test 1 result The test is finished
SendProbe:3 ResponseProbe:3
Completion:succcess RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
NumOfRTT:3 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:10 Min Positive DS:40
Max Positive SD:10 Max Positive DS:40
Positive SD Number:1 Positive DS Number:1
Positive SD Sum:10 Positive DS Sum:40
Positive SD Square Sum:100 Positive DS Square Sum:1600
Min Negative SD:20 Min Negative DS:30
Max Negative SD:20 Max Negative DS:30
Negative SD Number:1 Negative DS Number:1
Negative SD Sum:20 Negative DS Sum:30
Negative SD Square Sum:400 Negative DS Square Sum:900
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:25
Average of Jitter SD:15 Average of Jitter DS:35
jitter out value:0.6119792 jitter in value:1.4062500
NumberOfOWD:0 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
```

```

ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%
[RouterA-nqa-test-gmactrace] display nqa results
NQA entry(gmac, tracert) :testflag is inactive ,testtype is gmactrace
1 . Test 1 result The test is finished
Completion:succcess Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %

```

----结束

## 配置文件

- RouterA 的配置文件

```

#
sysname RouterA
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
#
cfm version standard
ping mac enable
trace mac enable
#
nqa test-instance test gmacping
test-type gmacping
vlan 10
destination-address mac 00e0-fca4-8ae7
#
nqa test-instance test gmactrace
test-type gmactrace
vlan 10
destination-address mac 00e0-fca4-8ae7
#
return

```

- RouterB 的配置文件

```

#
sysname RouterB
#
interface GigabitEthernet1/0/1
undo shutdown
portswtich
port default vlan 10
#
cfm version standard
ping mac enable
trace mac enable
#
return

```

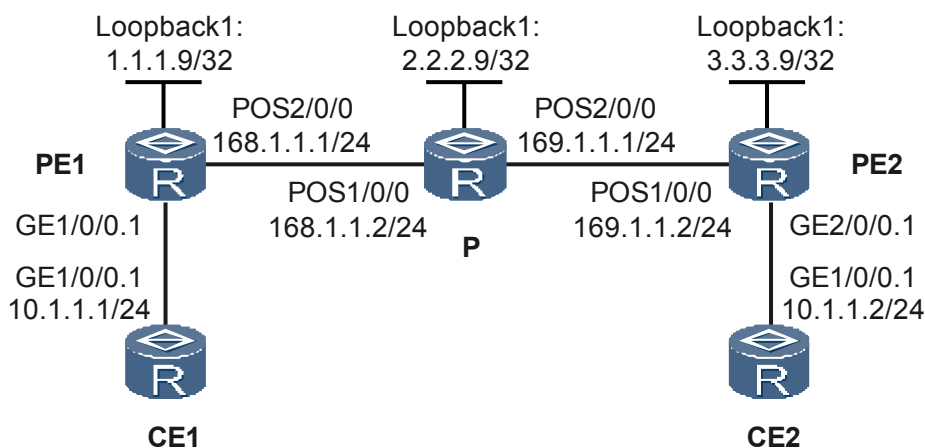
## 6.50.45 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 示例

### 组网需求

GMAC Ping 和 GMAC Trace 支持 PE 和 CE 上的检测，即支持 PE 和 PE 之间、CE 和 CE 之间以及 PE 和 CE 之间的检测。

如图 6-42 所示 VPLS 网络中，使用 NQA VPLS GMAC Ping 和 GMAC Trace 测试 VPLS 网络的连通性，定位故障。在 PE1 上配置 NQA GMAC Ping 和 GMAC Trace 测试例，正确配置 PE2 的桥 MAC 为目的 MAC 地址，并配置 VSI Name，发起测试。NQA 与普通命令行发起方式检测原理相同，NQA 的优点是增加了调度和结果收集的机制以及阈值告警等。

图 6-42 配置 GMAC Ping 和 GMAC Trace 测试 VPLS 组网



### 配置思路

采用如下的思路配置 GMAC Ping 和 GMAC Trace 测试 VPLS 的基本功能：

1. 配置 VPLS 网络，为 NQA 测试例启动配置业务环境。本例配置的是 Martini 方式 VPLS 网络。
2. 在 PE1 上配置 GMAC Ping 和 GMAC Trace 测试例。指定测试例的必选配置。
3. 启动 NQA 测试。

### 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口
- 对端 MAC 地址

## 操作步骤

### 步骤 1 配置 Martini 方式 VPLS 网络

配置步骤请参见配置文件。具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“VPLS 配置”。

### 步骤 2 配置 CFM 协议的版本为标准版本，使能 GMAC Ping 和 GMAC Trace 开关

# 配置 PE1。

```
[PE1] cfm version standard
[PE1] ping mac enable
[PE1] trace mac enable
```

# PE2 的配置与 PE1 类似，此处略。

### 步骤 3 配置 VPLS GMAC Ping 和 GMAC Trace 测试例

#### 1. 配置 VPLS GMAC Ping 测试例并启动测试操作。

# 配置 PE1。

```
<PE1> system-view
[PE1] nqa test-instance test gmacping
[PE1-nqa-test-gmacping] test-type gmacping
[PE1-nqa-test-gmacping] vsi a2
[PE1-nqa-test-gmacping] destination-address 00e0-fca4-8ae7
```

# 启动测试操作。

```
[PE1-nqa-test-gmacping] start now
```

#### 2. 配置 VPLS GMAC Trace 测试例并启动测试操作

# 配置 PE1。

```
<PE1> system-view
[PE1] nqa test-instance test gmactrace
[PE1-nqa-test-gmactrace] test-type gmactrace
[PE1-nqa-test-gmactrace] vsi a2
[PE1-nqa-test-gmactrace] destination-address 00e0-fca4-8ae7
```

# 启动测试操作。

```
[PE1-nqa-test-gmactrace] start now
```

### 步骤 4 验证测试结果

在 PE1 上分别进入 GMAC Ping 和 GMAC Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE1-nqa-test-gmacping] display nqa results
NQA entry(gmac,ping) :testflag is inactive ,testtype is gmacping
1 . Test 1 result The test is finished
 SendProbe:3 ResponseProbe:3
 Completion:succcess RTD OverThresholds number:0
 OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
 Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
 NumOfRTT:3 Drop operation number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 System busy operation number:0 Operation timeout number:0
 Min Positive SD:10 Min Positive DS:40
 Max Positive SD:10 Max Positive DS:40
 Positive SD Number:1 Positive DS Number:1
 Positive SD Sum:10 Positive DS Sum:40
 Positive SD Square Sum:100 Positive DS Square Sum:1600
 Min Negative SD:20 Min Negative DS:30
```



```

Max Negative SD:20 Max Negative DS:30
Negative SD Number:1 Negative DS Number:1
Negative SD Sum:20 Negative DS Sum:30
Negative SD Square Sum:400 Negative DS Square Sum:900
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:25
Average of Jitter SD:15 Average of Jitter DS:35
jitter out value:0.6119792 jitter in value:1.4062500
NumberOfOWD:0 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%
[PE1-nqa-test-gmactrace] display nqa results
NQA entry(gmac, tracert) :testflag is inactive ,testtype is gmactrace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %

```

----结束

## 配置文件

- CE1 的配置文件
 

```

#
sysname CE1
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
return

```
- CE2 的配置文件
 

```

#
sysname CE2
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
return

```
- PE1 的配置文件
 

```

#
sysname PE1
#
mpls lsr-id 1.1.1.9
mpls

```

```

#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 3.3.3.9
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi a2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
cfm version standard
ping mac enable
trace mac enable
#
nqa test-instance test gmacping
test-type gmacping
vsi a2
destination-address mac 00e0-fca4-8ae7
#
nqa test-instance test gmactrace
test-type gmactrace
vsi a2
destination-address mac 00e0-fca4-8ae7
nqa test-instance test gmactrace
test-type gmactrace
vsi a2
destination-address 00e0-fca4-8ae7
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 168.1.1.0 0.0.0.255
#
return

```

#### ● P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0

```

```

link-protocol ppp
undo shutdown
ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 168.1.1.0 0.0.0.255
network 169.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return

```

#### ● PE2 的配置文件

```

#
sysname PE2
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 1.1.1.9
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi a2
#
cfm version standard
ping mac enable
trace mac enable
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 169.1.1.0 0.0.0.255
#
return

```

## 6.50.46 配置 VPLS PW Ping 和 PW Trace 测试示例

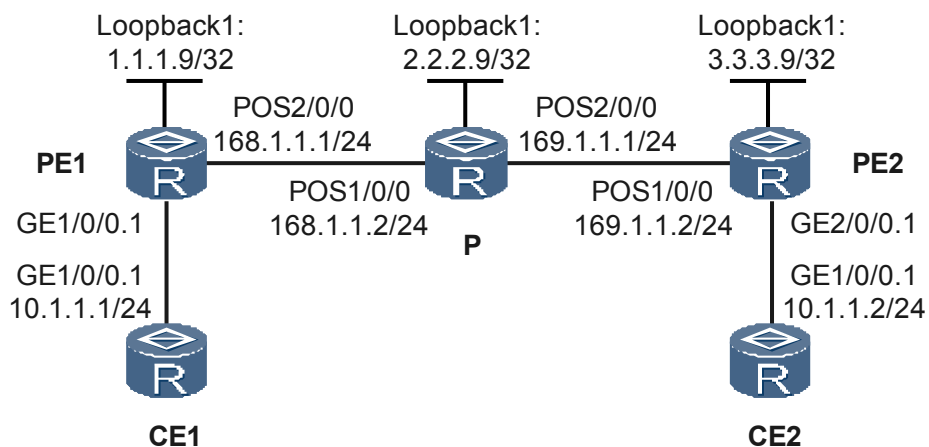
## 组网需求

PW 的连通性关系到用户间流量转发是否正常，PW 的转发性能关系到网络是否符合签订的 SLA。VPLS PW Ping 和 PW Trace 正是这样的工具，用于测量 PW 的连通性，收集 PW 的性能数据，进行路径发现和故障定位隔离等。

NQA 与普通命令行发起方式检测原理相同，NQA 的优点是增加了调度和结果收集的机制以及阈值告警等。Trace 用于故障定位和路径发现，可以与 Ping 结合起来，当 Ping 发现问题后，联动 Trace 测试例，记录当时出现故障的问题所在。

如图 6-43 所示，使用 VPLS PW Ping 和 PW Trace 测试 VPLS 网络的连通性，定位 PW 故障。

图 6-43 配置 VPLS PW Ping 和 PW Trace 测试组网



## 配置思路

采用如下的思路配置 VPLS PW Ping 和 PW Trace 测试的基本功能：

1. 配置 VPLS 网络，为 NQA 测试例启动配置业务环境。本例配置的是 Martini 方式 VPLS 网络。
2. 在 PE1 上配置 PW Ping 和 PW Trace 测试例。指定测试例的必选配置。
3. 启动 NQA 测试。

## 数据准备

为完成此配置例，需准备如下的数据：

- VSI 名称及 VSI ID
- 对等体的 IP 地址及建立对等体时使用的隧道策略
- 绑定 VSI 的接口

## 操作步骤

### 步骤 1 配置 Martini 方式 VPLS 网络

具体配置过程请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南 VPN》“VPLS 配置”

## 步骤 2 配置 VPLS PW Ping 和 PW Trace 测试例

### 1. 配置 VPLS PW Ping 测试例并启动测试操作

# 配置 PE1

```
<PE1> system-view
[PE1] nqa test-instance test vplspwping
[PE1-nqa-test-vplspwping] test-type vplspwping
[PE1-nqa-test-vplspwping] vsi a2
[PE1-nqa-test-vplspwping] destination-address ipv4 3.3.3.9
```

# 启动测试操作

```
[PE1-nqa-test-vplstrace] start now
```

### 2. 配置 VPLS PW Trace 测试例并启动测试操作

# 配置 PE1

```
<PE1> system-view
[PE1] nqa test-instance test vplspwtrace
[PE1-nqa-test-vplspwtrace] test-type vplspwtrace
[PE1-nqa-test-vplspwtrace] vsi a2
[PE1-nqa-test-vplspwtrace] destination-address ipv4 3.3.3.9
```

# 启动测试操作

```
[PE1-nqa-test-vplstrace] start now
```

## 步骤 3 验证测试结果

在 PE 上分别进入 PW Ping 和 PW Trace 测试例视图，执行 **display nqa results** 命令，可以看到测试结果为成功。

```
[PE1-nqa-test-vplspwping] display nqa results
NQA entry(vplspw,ping) :testflag is inactive ,testtype is vplspwping
1 . Test 1 result The test is finished
SendProbe:3 ResponseProbe:3
Completion:success RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:1/30/14/41 RTT Square Sum:1001
NumOfRTT:3 Drop operation number:0
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:10 Min Positive DS:40
Max Positive SD:10 Max Positive DS:40
Positive SD Number:1 Positive DS Number:1
Positive SD Sum:10 Positive DS Sum:40
Positive SD Square Sum:100 Positive DS Square Sum:1600
Min Negative SD:20 Min Negative DS:30
Max Negative SD:20 Max Negative DS:30
Negative SD Number:1 Negative DS Number:1
Negative SD Sum:20 Negative DS Sum:30
Negative SD Square Sum:400 Negative DS Square Sum:900
Min Delay SD:0 Min Delay DS:0
Max Delay SD:0 Max Delay DS:0
Delay SD Square Sum:0 Delay DS Square Sum:0
Packet Loss SD:0 Packet Loss DS:0
Packet Loss Unknown:0 Average of Jitter:25
Average of Jitter SD:15 Average of Jitter DS:35
jitter out value:0.6119792 jitter in value:1.4062500
NumberOfOWD:0 Packet Loss Ratio: 0%
OWD SD Sum:0 OWD DS Sum:0
ICPIF value: 0 MOS-CQ value: 0
TimeStamp unit: ms Packet Rewrite Number: 0
```

```

Packet Rewrite Ratio: 0% Packet Disorder Number: 0
Packet Disorder Ratio: 0% Fragment-disorder Number: 0
Fragment-disorder Ratio: 0%
[PE1-nqa-test-vplspwtrace] display nqa results
NQA entry(vplspw, tracert) :testflag is inactive ,testtype is vplspwtrace
1 . Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2010-07-23 14:23:20.4
1 . Hop 1
Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 70/140/93
Sum/Square-Sum Completion Time: 280/29400
RTD OverThresholds number: 0
Last Good Probe Time: 2010-07-23 14:23:20.4
Destination ip address:3.3.3.3
Lost packet ratio: 0 %

```

----结束

## 配置文件

- CE1 的配置文件

```

#
sysname CE1
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
return

```

- CE2 的配置文件

```

#
sysname CE2
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
return

```

- PE1 的配置文件

```

#
sysname PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 3.3.3.9
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
undo shutdown

```

```

 vlan-type dot1q 10
 12 binding vsi a2
 #
 interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 168.1.1.1 255.255.255.0
 mpls
 mpls ldp
 #
 interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
 #
 nqa test-instance test vplspwping
 test-type vplspwping
 vsi a2
 destination-address ipv4 3.3.3.9
 #
 nqa test-instance test vplspwtrace
 test-type vplspwtrace
 vsi a2
 destination-address ipv4 3.3.3.9
 #
 ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 168.1.1.0 0.0.0.255
 #
 return

```

#### ● P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 168.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 169.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 168.1.1.0 0.0.0.255
 network 169.1.1.0 0.0.0.255
 network 2.2.2.9 0.0.0.0
#
return

```

#### ● PE2 的配置文件

```

#
sysname PE2
#
mpls lsr-id 3.3.3.9
mpls

```

```
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 1.1.1.9
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi a2
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 169.1.1.0 0.0.0.255
#
return
```

## 6.50.47 配置对指定的组播 VPN 网络进行从组播源到目的主机的 RPF 路径检测

通过 NQA 对指定的组播 VPN 网络进行测试，了解从组播源到目的主机的 RPF 路径连通情况。

### 组网需求

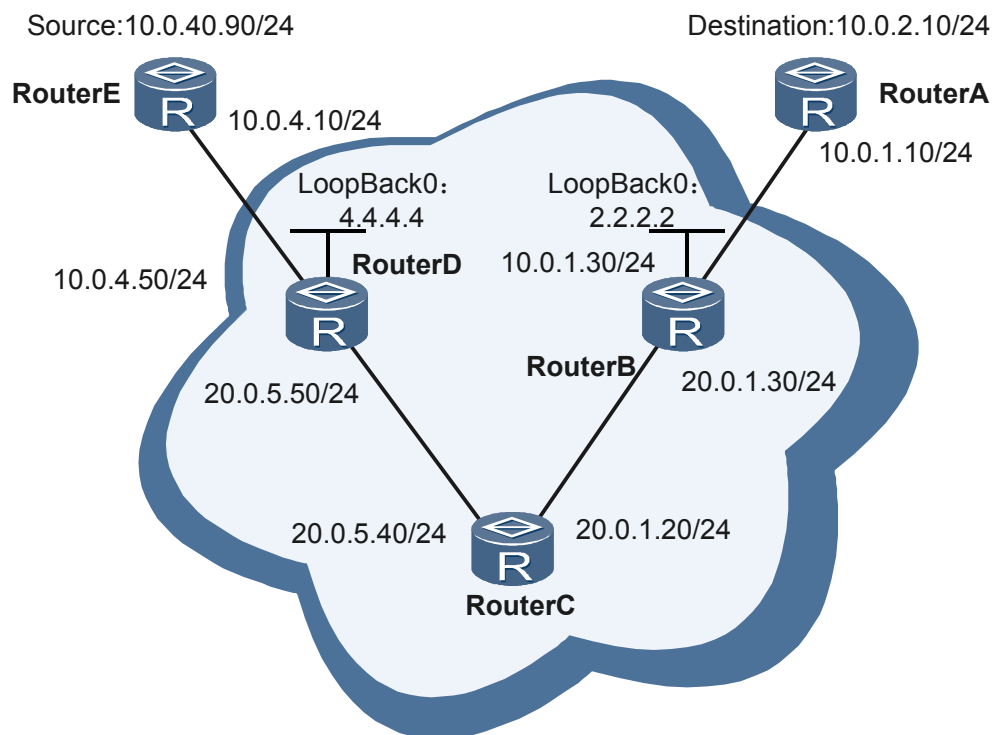
如图 6-44 所示的单自治域 MPLS/BGP VPN 网络中，使用 MD 方案部署组播业务。

Receiver 端加入组播组 225.1.1.1，接收 Source 端发送的组播数据。其中 RouterA 是最后一跳。

在 RouterB 上对指定的组播 VPN 网络进行组播 Trace 实现路径检测功能，可以检测从组播源到目的主机的 RPF 路径，并且可以得到路径节点信息，从而对故障节点的检测提供了手段。



图 6-44 配置单自治域 MD VPN 组网图



## 配置思路

采用如下思路进行组播 VPN 网络测试的配置：

1. 配置 BGP/MPLS IP VPN，确保 VPN 网络正常运行、单播路由畅通。
2. 全网启动组播功能和 PIM 功能，在 PE 和 P 之间建立公网实例组播、PE 和 CE 之间建立 VPN 实例组播。
3. 在各 PE 上为同一 VPN 实例配置相同的 Share-Group 地址、相同的 MTI 及相同的 Switch-MDT 切换地址池范围。
4. 在各 PE 上配置 MTI 地址为公网中的 IBGP Peer 接口地址，并在 MTI 上使能 PIM 协议。
5. 将 RouterB 作为 NQA Client，配置 MTrace 测试例。
6. 启动测试例，验证检测结果。

## 数据准备

为完成此配置例，需准备如下的数据：

- 测试例名称：admin mtrace
- 组播源 IP 地址：10.0.40.90/24
- 目的主机 IP 地址：10.0.2.10/24
- 最后一跳 IP 地址：10.0.1.10/24
- VPN 实例名：red

## 操作步骤

**步骤 1** 配置 BGP/MPLS IP VPN，确保 VPN 网络正常运行、单播路由畅通(略)

具体配置过程请参见《配置指南 VPN》“BGP/MPLS IP VPN 配置”。

**步骤 2** 全网启动组播功能和 PIM 功能，在 PE 和 P 之间建立公网实例组播、PE 和 CE 之间建立 VPN 实例组播(略)

具体配置过程请参见《配置指南 IP 组播》“IPv4 组播 VPN 配置”。

**步骤 3** 在各 PE 上为同一 VPN 实例配置相同的 Share-Group 地址、相同的 MTI 及相同的 Switch-MDT 切换地址池范围(略)

具体配置过程请参见《配置指南 IP 组播》“IPv4 组播 VPN 配置”。

**步骤 4** 在各 PE 上配置 MTI 地址为公网中的 IBGP Peer 接口地址，并在 MTI 上使能 PIM 协议(略)

具体配置过程请参见《配置指南 IP 组播》“IPv4 组播 VPN 配置”。

**步骤 5** 在 RouterB 上配置 NQA MTrace 测试例。

```
<RouterB> system-view
[RouterB] nqa test-instance admin mtrace
[RouterB-nqa-admin-mtrace] test-type mtrace
[RouterB-nqa-admin-mtrace] mtrace-source-address ipv4 10.0.40.90
[RouterB-nqa-admin-mtrace] destination-address ipv4 10.0.2.10
[RouterB-nqa-admin-mtrace] mtrace-query-type last-hop
[RouterB-nqa-admin-mtrace] vpn-instance red
[RouterB-nqa-admin-mtrace] mtrace-last-hop-address ipv4 10.0.1.10
```

**步骤 6** 启动测试操作

```
[RouterB-nqa-admin-mtrace] start now
```

**步骤 7** 验证测试结果

# 在 RouterB 执行命令 **display this** 查看测试例配置情况。

```
<RouterB> display this
#
nqa test-instance admin mtrace
test-type mtrace
destination-address ipv4 10.0.2.10
mtrace-last-hop-address ipv4 10.0.2.20
mtrace-source-address ipv4 10.0.40.90
mtrace-query-type last-hop
vpn-instance red
#
return
```

# 在 RouterB 执行命令 **display nqa results**，可以看到从组播源到目的主机的 RPF 路径是 RouterE->RouterD->RouterB->RouterA。

```
<RouterB> display nqa results test-instance admin mtrace
NQA entry(admin, mtrace) :testFlag is inactive ,testtype is mtrace
1. Test 1 result The test is finished
Completions: success Query Mode: max-hop
Current Hop:4 Current Probe:1
SendProbe:1 ResponseProb:1
Timeout Count:0 Busy Count:0
Drop Count:0 Max Path Ttl:5
Responser:10.0.4.10 Response Rtt: 50
mtrace start time: 2008-12-31 14:16:46.2
Last Good Probe Time: 2007-2-7 17:36:18.3
Last Good Path Time: 2007-2-7 17:36:18.3
```

```

1 . Hop 1
Outgoing Interface Address: 10.0.2.20
Incoming Interface Address: 10.0.1.10
Prehop Router Address: 10.0.1.30
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:5
SG Packet Count:0xffffffff Hop Time Delay(ms):1
Input Packet Count:0 Output Packet Count:0
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

2 . Hop 2
Outgoing Interface Address: 10.0.1.30
Incoming Interface Address: 0.0.0.0
Prehop Router Address: 0.0.0.0
Protocol : Unknown Forward Code:ADMIN_PROHIB
Forward Ttl:1 Current Path Ttl:4
SG Packet Count:0xffffffff Hop Time Delay(ms):1
Input Packet Count:0 Output Packet Count:0
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

3 . Hop 3
Outgoing Interface Address: 0.0.0.0
Incoming Interface Address: 10.0.4.50
Prehop Router Address: 10.0.4.10
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:3
SG Packet Count:0xffffffff Hop Time Delay(ms):1
Input Packet Count:0 Output Packet Count:313
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

4 . Hop 4
Outgoing Interface Address: 10.0.4.10
Incoming Interface Address: 10.0.40.80
Prehop Router Address: 0.0.0.0
Protocol : PIM Forward Code:NO_ERROR
Forward Ttl:1 Current Path Ttl:2
SG Packet Count:0xffffffff Hop Time Delay(ms):0xffffffff
Input Packet Count:0 Output Packet Count:0
Input Rate(pps): 0xffffffff Output Rate(pps): 0xffffffff
Input Loss Rate: 0xffffffff SG Loss Rate: 0xffffffff

```

----结束

## 配置文件

- RouterA 的配置文件

```

#
sysname RouterA
#
router id 1.1.1.1
#
multicast routing-enable
#
interface Ethernet0/0/0
undo shutdown
ip address 10.0.1.10 255.255.255.0
pim sm
igmp static-group 225.1.1.1
#
interface Ethernet0/0/2
undo shutdown
ip address 10.0.2.20 255.255.255.0
pim sm
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
pim sm
#

```

```
rip 2
 network 10.0.0.0
 import-route direct
#
igmp
#
nqa test-instance admin mtrace
 test-type mtrace
 mtrace-source-address ipv4 10.0.40.90
 mtrace-response-address ipv4 10.0.1.10
#
return
```

● RouterB 的配置文件

```
#
 sysname RouterB
#
 router id 2.2.2.2
#
 multicast routing-enable
#
 ip vpn-instance red

 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
 multicast routing-enable
 multicast-domain share-group 239.1.1.1 binding mtunnel 0
 multicast-domain switch-group-pool 225.2.2.0 255.255.255.240
#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls ldp
#
 interface Ethernet0/0/1
 undo shutdown
 ip binding vpn-instance red
 ip address 10.0.1.30 255.255.255.0
 pim sm
#
 interface Ethernet0/0/2
 undo shutdown
 ip address 20.0.1.30 255.255.255.0
 pim sm
 mpls
 mpls ldp
#
 interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
 interface MTunnel0
 ip binding vpn-instance red
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
 bgp 100
 group vpn-g internal
 peer vpn-g connect-interface LoopBack1
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 group vpn-g
#
 ipv4-family unicast
 undo synchronization
 peer vpn-g enable
 peer 4.4.4.4 enable
 peer 4.4.4.4 group vpn-g
#
 ipv4-family vpnv4
```

```

policy vpn-target
peer vpn-g enable
peer 4.4.4.4 enable
peer 4.4.4.4 group vpn-g
#
ipv4-family vpn-instance red
import-route direct
import-route rip 2
#
ospf 1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
network 20.0.1.0 0.0.0.255
network 10.0.3.0 0.0.0.255
network 2.2.2.2 0.0.0.0
#
rip 2 vpn-instance red
network 10.0.0.0
network 20.0.0.0
import-route direct
import-route bgp cost 3
#
igmp
#
nqa test-instance admin mtrace
test-type mtrace
destination-address ipv4 10.0.2.10
mtrace-last-hop-address ipv4 10.0.2.20
mtrace-source-address ipv4 10.0.40.90
mtrace-query-type last-hop
vpn-instance red
#
return

```

#### ● RouterC 的配置文件

```

#
sysname RouterC
#
router id 3.3.3.3
#
multicast routing-enable
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface Ethernet0/0/0
undo shutdown
ip address 20.0.1.20 255.255.255.0
pim sm
mpls
mpls ldp
#
interface Ethernet0/0/1
undo shutdown
ip address 20.0.5.40 255.255.255.0
pim sm
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 20.0.1.0 0.0.0.255
network 20.0.5.0 0.0.0.255
network 3.3.3.3 0.0.0.0

```

```
#
igmp
#
pim
 c-bsr LoopBack1
 c-rp LoopBack1
#
return
```

● RouterD 的配置文件

```
#
sysname RouterD
#
router id 4.4.4.4
#
multicast routing-enable
#
ip vpn-instance red
 ipv4-family
 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
 multicast routing-enable
 multicast-domain share-group 239.1.1.1 binding mtunnel 0
 multicast-domain switch-group-pool 225.2.2.0 255.255.255.240
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
#
interface Ethernet0/0/1
 undo shutdown
 ip address 20.0.5.50 255.255.255.0
 pim sm
 mpls
 mpls ldp
#
interface Ethernet0/0/2
 undo shutdown
 ip binding vpn-instance red
 ip address 10.0.4.50 255.255.255.0
 pim sm
 igmp enable
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 pim sm
#
interface MTunnel0
 ip binding vpn-instance red
 ip address 4.4.4.4 255.255.255.255
 pim sm
#
bgp 100
 group vpn-g internal
 peer vpn-g connect-interface LoopBack1
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 group vpn-g
#
 ipv4-family unicast
 undo synchronization
 peer vpn-g enable
 peer 2.2.2.2 enable
 peer 2.2.2.2 group vpn-g
#
 ipv4-family vpnv4
 policy vpn-target
 peer vpn-g enable
 peer 2.2.2.2 enable
```

```
peer 2.2.2.2 group vpn-g
#
ipv4-family vpn-instance red
import-route direct
import-route rip 2
#
ospf 1
area 0.0.0.0
network 20.0.5.0 0.0.0.255
network 10.0.4.0 0.0.0.255
network 4.4.4.4 0.0.0.0
#
rip 2 vpn-instance red
network 10.0.0.0
network 20.0.0.0
import-route direct
import-route bgp cost 3
#
igmp
#
return
```

- RouterE 的配置文件

```
#
sysname RouterE
#
router id 5.5.5.5
#
multicast routing-enable
#
interface Ethernet0/0/0
undo shutdown
ip address 10.0.40.80 255.255.255.0
pim sm
#
interface Ethernet0/0/1
undo shutdown
ip address 10.0.4.10 255.255.255.0
pim sm
#
interface LoopBack1
ip address 5.5.5.5 255.255.255.255
pim sm
#
rip 2
network 10.0.0.0
import-route direct
import-route bgp
#
igmp
#
pim
c-bsr LoopBack1
c-rp LoopBack1
#
return
```

## 6.50.48 配置 NQA 上下限阈值告警、联动测试例事件示例

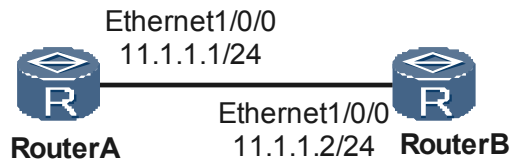
通过 NQA 测试例联动，实现对网络故障的动态监控。

### 组网需求

如图 6-45 所示。

使用 NQA Jitter 功能对 RouterA 与 RouterB 之间丢包率进行监控。如果测试结果中的丢包率超过阈值，则启动与事件关联的联动测试例，测试 RouterB 是否可达。

图 6-45 配置 NQA 阈值告警组网图



## 配置思路

采用如下思路进行联动测试例的配置：

1. RouterA 做为 NQA 客户端，RouterB 做为 NQA 服务器端。
2. 在 NQA 客户端配置 ICMP 类型联动测试例。
3. 在 NQA 客户端配置联动测试例事件。
4. 在 NQA 客户端配置 ICMP Jitter 类型主测试例。
5. 在 NQA 客户端配置阈值告警。
6. 在 NQA 客户端启动 ICMP Jitter 类型主测试例。

## 数据准备

为完成此配置例，需准备如下的数据：

- 联动测试例索引
- 阈值相关事件号
- 阈值告警号
- 阈值上限和下限

## 操作步骤

### 步骤 1 使能 NQA 客户端，配置 ICMP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin icmp
[RouterA-nqa-admin-icmp] test-type icmp
[RouterA-nqa-admin-icmp] destination-address ipv4 11.1.1.2
[RouterA-nqa-admin-icmp] quit
```

### 步骤 2 在 RouterA 配置联动测试例事件，将测试例 admin icmp 设置为联动测试例

```
[RouterA] nqa event 10 linkage admin icmp
```

### 步骤 3 在 RouterA 配置 ICMP 类型的 NQA 测试例

```
[RouterA] nqa test-instance admin icmpjitter
[RouterA-nqa-admin-icmpjitter] test-type icmpjitter
[RouterA-nqa-admin-icmpjitter] destination-address ipv4 11.1.1.2
```

# 配置阈值告警。

```
[RouterA-nqa-admin-icmpjitter] alarm 10 lost-packet-ratio absolute rising-threshold 80 10 falling-threshold 10 10
```

### 步骤 4 启动测试操作

```
[RouterA-nqa-admin-icmpjitter] start now
```

### 步骤 5 验证测试结果

# 查看与告警相关联的事件信息。



```
<RouterA> display nqa event
NQA Event Information:
```

| Event-Entry | Event-type | Description | Admin-Name | Operation-Tag |
|-------------|------------|-------------|------------|---------------|
| 10          | linkage    |             | admin      | icmp          |

# 查看所有测试例的当前告警信息。

```
<RouterA> display nqa alarm
NQA Alarm Information:
```

| Admin-Name | Operation-Tag | Alarm-Entry | AlarmType | Event-Entry |
|------------|---------------|-------------|-----------|-------------|
| admin      | icmpjitter    | 10          | Rising    | 10          |
| admin      | icmpjitter    | 10          | Falling   | 10          |

# 查看 NQA 测试的客户端状态。

```
<RouterA> display nqa-agent
NQA Tests Max:2000 NQA Tests Number: 2
NQA Flow Max:1000 NQA Flow Remained:1000
```

```
nqa test-instance admin icmp
test-type icmp
destination-address ipv4 11.1.1.2
nqa status : normal
nqa test-instance admin icmpjitter
test-type icmpjitter
destination-address ipv4 11.1.1.2
alarm 10 lost-packet-ratio absolute rising-threshold 80 10 falling-threshold 10 10
nqa status : normal
```

# 查看 NQA 测试的测试结果。

```
<RouterA> display nqa results
```

```
NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
1. Test 1 result The test is finished
Send operation times: 3 Receive response times: 0
Completion:failed RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:3
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:11.1.1.2
Min/Max/Average Completion Time: 0/0/0
Sum/Square-Sum Completion Time: 0/0
Last Good Probe Time: 0-0-0 0:0:0.0
Lost packet ratio: 100 %

NQA entry(admin, icmpjitter) :testflag is inactive ,testtype is icmpjitter
1. Test 1 result The test is finished
SendProbe:60 ResponseProbe:0
Completion:failed RTD OverThresholds number:0
OWD OverThresholds SD number:0 OWD OverThresholds DS number:0
Min/Max/Avg/Sum RTT:0/0/0/0 RTT Square Sum:0
NumOfRTT:0 Drop operation number:60
Operation sequence errors number:0 RTT Stats errors number:0
System busy operation number:0 Operation timeout number:0
Min Positive SD:0 Min Positive DS:0
Max Positive SD:0 Max Positive DS:0
Positive SD Number:0 Positive DS Number:0
Positive SD Sum:0 Positive DS Sum:0
Positive SD Square Sum:0 Positive DS Square Sum:0
Min Negative SD:0 Min Negative DS:0
Max Negative SD:0 Max Negative DS:0
Negative SD Number:0 Negative DS Number:0
Negative SD Sum:0 Negative DS Sum:0
Negative SD Square Sum:0 Negative DS Square Sum:0
```

|                            |                           |
|----------------------------|---------------------------|
| Min Delay SD:0             | Min Delay DS:0            |
| Max Delay SD:0             | Max Delay DS:0            |
| Delay SD Square Sum:0      | Delay DS Square Sum:0     |
| Packet Loss SD:0           | Packet Loss DS:0          |
| Packet Loss Unknown:0      | Average of Jitter:0       |
| Average of Jitter SD:0     | Average of Jitter DS:0    |
| jitter out value:0.0000000 | jitter in value:0.0000000 |
| NumberOfOWD:0              | Packet Loss Ratio: 100%   |
| OWD SD Sum:0               | OWD DS Sum:0              |
| ICPIF value: 0             | MOS-CQ value: 0           |

----结束

## 配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 interface Ethernet1/0/0
 ip address 11.1.1.1 255.255.255.0
#
 nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 11.1.1.2
 nqa test-instance admin icmpjitter
 test-type icmpjitter
 destination-address ipv4 11.1.1.2
 nqa event 10 linkage admin icmp
 nqa test-instance admin icmpjitter
 alarm 10 lost-packet-ratio absolute rising-threshold 80 10 falling-threshold 10 10
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 interface Ethernet1/0/0
 ip address 11.1.1.2 255.255.255.0
#
return
```

## 6.50.49 配置 CR-LSP 热备份隧道 LSP Traceroute 测试示例

通过 NQA 对 CR-LSP 热备份隧道进行测试，探测 LSP 的故障节点。

## 组网需求

如图 6-46 所示的 MPLS VPN 网络,从 RouterA 上建立一条 TE 隧道，目的地址为 RouterC，并配置 CR-LSP 热备份（hot-standby）隧道。

- RouterA、RouterB、RouterC、RouterD 都运行 OSPF 协议，并学习到彼此 Loopback 接口的 32 位主机路由。
- RouterA、RouterB、RouterC、RouterD 上都启用 MPLS、MPLS TE 和 MPLS RSVP-TE。
- RouterA、RouterB、RouterC、RouterD 之间的接口都启用 MPLS、MPLS TE 和 MPLS RSVP-TE，建立从 RouterA 到 RouterC 的 TE 隧道。

其中：

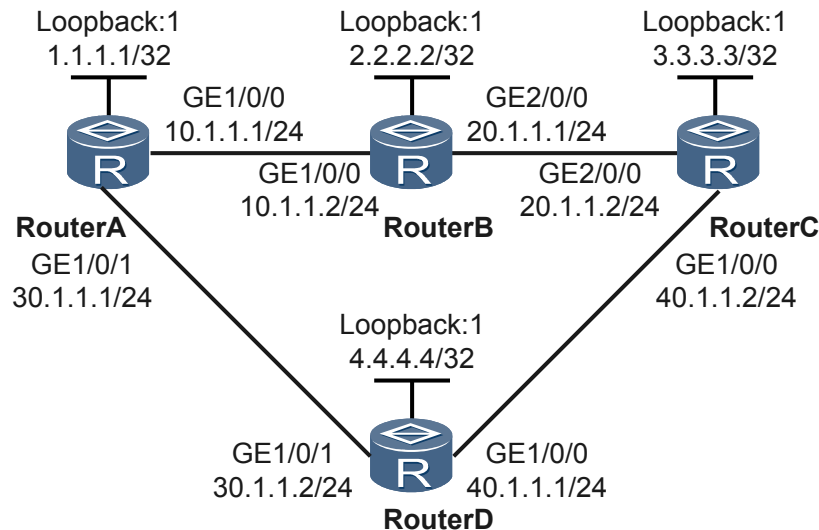
- 主 CR-LSP 的路径为 RouterA-->RouterB-->RouterC

- 备份 CR-LSP 的路径为 RouterA-->RouterD-->RouterC

当主 CR-LSP 故障时，流量切换到备份 CR-LSP。当主 CR-LSP 故障恢复，延时 15 秒后再进行流量回切。

但是当备份 CR-LSP 出现故障不能承载主链路切换过来的流量时，需要对这条备份链路进行检测。应用 NQA LSP Traceroute 可以实现对 CR-LSP 热备份（hot-standby）隧道进行连通性的检测。NQA 集成的备份链路的检测功能，可以对备份链路的连通性及性能状况进行实时的检测，便于链路故障的检测和定位。

图 6-46 LSP Traceroute 测试组网图



## 配置思路

采用如下思路进行 LSP Traceroute 测试的配置：

1. RouterA 做为 NQA 客户端，在 RouterA 上建立 LSP Traceroute 测试用例。
2. RouterC 做为 NQA 服务器端。

## 数据准备

为完成此配置例，需准备如下的数据：

- lsp-tunnel tunnel 接口编号

## 操作步骤

### 步骤 1 配置 RouterA、RouterB、RouterC 和 RouterD 之间路由可达

具体配置内容请参见本例的配置文件。

### 步骤 2 配置 RouterA、RouterB、RouterC 和 RouterD 的 MPLS RSVP-TE

具体配置内容请参见本例的配置文件。

### 步骤 3 配置 RouterA 上建立到 RouterC 的 TE 隧道

具体配置内容请参见本例的配置文件。

**步骤 4 配置 RouterA 的 NQA 测试例**

# 使能 NQA 客户端，配置 TE 隧道的 LSP Traceroute 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin lsptrace
[RouterA-nqa-admin-lsptrace] test-type lsptrace
[RouterA-nqa-admin-lsptrace] lsp-type te
[RouterA-nqa-admin-lsptrace] lsp-tetunnel tunnel 1/0/0 hot-standby
```

**步骤 5 启动测试操作**

```
[RouterA-nqa-admin-lsptrace] start now
```

**步骤 6 验证测试结果**

```
[RouterA-nqa-admin-lsptrace] display nqa results test-instance admin lsptrace
NQA entry(admin, lsptrace) :testFlag is inactive ,testtype is lsptrace
 1. Test 1 result The test is finished
Completion:success Attempts number:1
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Drop operation number:0
Last good path Time:2009-4-24 11:22:21.2
 1. Hop 1 Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 50/60/56
Sum/Square-Sum Completion Time: 170/9700
RTD OverThresholds number: 0
Last Good Probe Time: 2009-4-24 11:22:20.8
Destination ip address:30.1.1.2
Lost packet ratio: 0 %
 2. Hop 2 Send operation times: 3 Receive response times: 3
Min/Max/Average Completion Time: 80/110/93
Sum/Square-Sum Completion Time: 280/26600
RTD OverThresholds number: 0
Last Good Probe Time: 2009-4-24 11:22:21.2
Destination ip address:3.3.3.3
Lost packet ratio: 0 %
```

----结束

**配置文件**

## ● RouterA 的配置文件

```
#
sysname RouterA
#
mpls lsr-id 1.1.1.1
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
explicit-path backup
next hop 30.1.1.2
next hop 40.1.1.2
next hop 3.3.3.3
#
explicit-path main
next hop 10.1.1.2
next hop 20.1.1.2
next hop 3.3.3.3
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls te
```

```

mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 30.1.1.1 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te tunnel-id 100
mpls te record-route
mpls te path explicit-path main
mpls te path explicit-path backup secondary
mpls te backup hot-standby wtr 15
mpls te backup ordinary best-effort
mpls te commit
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
network 30.1.1.0 0.0.0.255
mpls-te enable
#
nqa test-instance admin lsptrace
test-type lsptrace
lsp-type te
lsp-tetunnel Tunnel1/0/0 hot-standby
#
return

```

## ● RouterB 的配置文件

```

#
sysname RouterB
#
mpls lsr-id 2.2.2.2
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 20.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ospf 1
opaque-capability enable
area 0.0.0.0

```

```
network 10.1.1.0 0.0.0.255
network 2.2.2.2 0.0.0.0
network 20.1.1.0 0.0.0.255
mpls-te enable
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
interface GigabitEthernet2/0/0
ip address 20.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface GigabitEthernet1/0/0
ip address 40.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 40.1.1.0 0.0.0.255
network 3.3.3.3 0.0.0.0
mpls-te enable
#
return
```

- RouterD 的配置文件

```
#
sysname RouterD
#
mpls lsr-id 4.4.4.4
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
interface GigabitEthernet1/0/1
ip address 30.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface GigabitEthernet1/0/0
ip address 40.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 50000
mpls rsvp-te
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
```

```
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 4.4.4.4 0.0.0.0
 network 30.1.1.0 0.0.0.255
 network 40.1.1.0 0.0.0.255
 mpls-te enable
#
return
```





# 7 NetStream 配置

## 关于本章

NetStream 是一种基于网络流信息的采集、统计与发布技术，可以对网络中的通信量和资源使用情况进行分类统计，帮助用户实现对各种业务的管理和计费。

### 7.1 NetStream 简介

Internet 的高速发展，为用户提供了更高的带宽资源，同时要求用户对自己的网络资源进行更细致的监控和管理，因此就需要一种技术来满足此需求。NetStream 技术就是这样一种基于网络流量信息的统计技术，它可以对网络中的通信流量和资源使用情况进行分类统计，基于各种业务和资源进行网络的监控和管理。

### 7.2 配置 IPv4 网络的流量统计

配置流量统计后对流经自己的网络流量进行采样和处理，并向 NDC 输出 NetStream 原始流信息，以便 NDC 进行更为灵活的后续处理。与聚合流统计相比，运行原始流统计功能对 NDE 设备性能的影响较小，但是由于原始流数据量远大于聚合流数据量，所以原始流会占用 NDE 更多的存储空间和网络带宽。

### 7.3 配置 MPLS 网络的流量统计

配置 MPLS 网络的流量统计对封装 IPv4 报文的 MPLS 流量进行外三层标签信息的采集。在 MPLS 网络上的流量进行原始流统计，可以帮助用户监控 MPLS 网络的使用情况。

### 7.4 配置聚合流的流量统计

NDE 设备完成原始流信息采集后，用户可以根据不同的统计需求，将原始流数据进行聚合，再输出到 NDC 进行分析。这样可以减少因统计功能产生的网络数据量，也可以避免不必要的信息干扰。

### 7.5 配置 NetStream 多地址输出

通过配置 NetStream 多址输出，可以使指定的流量输出到指定的服务器。

### 7.6 维护 NetStream

维护 NetStream 包括如何清除 NetStream 统计信息。

### 7.7 配置举例

请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

## 7.1 NetStream 简介

Internet 的高速发展，为用户提供了更高的带宽资源，同时要求用户对自己的网络资源进行更细致的监控和管理，因此就需要一种技术来满足此需求。NetStream 技术就是这样一种基于网络流量信息的统计技术，它可以对网络中的通信流量和资源使用情况进行分类统计，基于各种业务和资源进行网络的监控和管理。

### 7.1.1 NetStream 概述

NetStream 技术的实现涉及三个设备角色：负责采集数据的 NDE，存储数据的 NDC 和分析统计数据的 NDA。路由器作为 NDE 采集网络流量信息。

### 7.1.2 NE20E-X6 支持的 NetStream 特性

NetStream 可以对 IPv4，MPLS 和 VPN 报文进行采样和分析。

### 7.1.1 NetStream 概述

NetStream 技术的实现涉及三个设备角色：负责采集数据的 NDE，存储数据的 NDC 和分析统计数据的 NDA。路由器作为 NDE 采集网络流量信息。

Internet 的高速发展，为用户提供了更高的带宽资源，同时要求用户对自己的网络资源进行更细致的监控和管理，因此就需要一种技术来满足此需求。

NetStream 技术就是这样一种基于网络流量信息的统计技术，它可以对网络中的通信流量和资源使用情况进行分类统计，基于各种业务和资源进行网络的监控和管理。NetStream 主要有如下应用：

- 计费

NetStream 为基于资源（如线路、带宽和时段等）占用情况的计费提供了精细的数据，这些数据包括 IP 地址、包数、字节数、时间、ToS 和应用类型等。ISP 可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。

- 网络规划和分析

NetStream 可以为先进的网络管理工具提供关键信息，以便优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。

- 网络监控

NetStream 技术能够实现实时的网络监控功能。RMON、RMON-2 和基于信息流的分析技术可以用来形象化地表示单个路由器和全网范围内的流量模式，并提供预先故障检测、高效故障排除和快速问题解决功能。

- 应用监控和分析

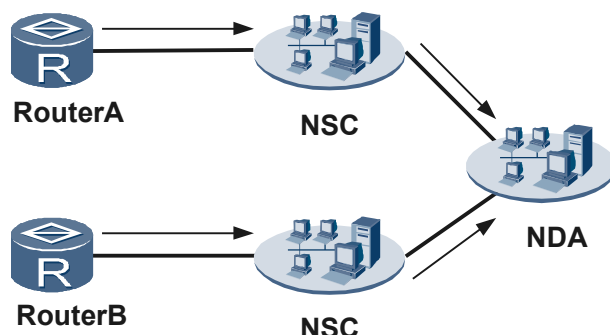
通过 NetStream 技术，可以获得详细的网络应用信息。例如，网络管理员可以查看 Web、FTP、Telnet 和其它著名的 TCP/IP 应用所占通信流量的百分比。Internet 内容和服务提供商可以根据这些信息来规划和分配网络和应用资源以满足用户需求。

- 异常流量检测

通过对 NetStream 流进行分析，可以实时检测网络中的异常流量，比如各种网络攻击，通过网管侧的告警，以及与设备的联动，可以对网络安全进行保障。

NetStream 主要包括三个设备 NDE（NetStream Data Exporter），NSC（NetStream Collector），NDA（NetStream Data Analyzer），三个设备之间的关系如下图所示。

图 7-1 NetStream 的设备角色



NDE 负责流量的采集和发送。NSC 设备负责收集和存储 NDE 发来的流量统计数据信息。NDA 对统计信息进行分析，分析的结果为网络计费，网络规划，网络监控，应用监控和分析等提供依据。

设备实现的是 NDE 功能，需要完成报文采集、流聚合和流输出功能。

## 7.1.2 NE20E-X6 支持的 NetStream 特性

NetStream 可以对 IPv4，MPLS 和 VPN 报文进行采样和分析。

### IPv4 网络流量的采样和统计

产品支持对 IPv4 网络流量报文的原始流量进行采样和统计。包括：单播和组播报文、uRPF/RPF 丢弃报文和分片报文。原始流统计提供除七元组外还有源 AS、目的 AS、VPNID、TCP-flag 统计和 BGP 下一跳统计。

### MPLS 网络流量的采样和统计

产品支持对 MPLS（Multi-Protocol Label Switching）网络中的报文进行采样和统计。包括对 MPLS 报文的三层标签采样和 MPLS 报文的 IP 报头采样。

### 采样方式

本产品支持四种采样方式：固定报文采样、随机报文采样、固定时间采样和随机时间采样。可以在系统视图、接口视图和 ACL 视图下配置采样方式和采样比。

- 随机报文间隔采样  
随机报文间隔采样表示两次采样间隔为配置的采样值 *random-packets*。即，对于使能 NetStream 的接口，按照采样比 M: 1，在采样间隔内通过的 N\*M 个报文中随机采样 N 个报文。
- 固定报文间隔采样  
固定报文间隔表示两次采样间隔为配置的采样值 *fix-packets*。即，对于使能 NetStream 的接口，根据采样间隔 N 内固定采样第 N 个通过的报文。
- 随机采样的时间间隔  
随机时间间隔采样表示每间隔 *random-time* 时间随机采样一个报文。
- 固定时间间隔采样

固定时间间隔采样表示每间隔 *fix-time* 时间采样一个报文。

## 原始流和聚合流版本

产品支持原始流和聚合流两种输出方式。原始流按 V5/V9 版本输出，聚合流按 V8/V9 版本输出。

## 统计信息的聚合

产品支持多种聚合输出方式：

- as
- as-tos
- bgp-nexthop-tos
- destination-prefix
- destination-prefix-tos
- index-tos
- mpls-label
- prefix
- prefix-tos
- protocol-port
- protocol-port-tos
- source-index-tos
- source-prefix
- source-prefix-tos
- vlan-id

## NetStream 业务处理方式

产品支持两种 NetStream 业务板的处理方式：分布式和集中式。

- 分布式  
单个接口板可以独立完成报文的采集、流聚合和流输出功能，支持完整的 NetStream 功能。
- 集中式  
单个接口板不支持 Netstream 流处理功能，接口板只对报文进行采样，并将采样报文发送到 Netstream 业务板集中进行流聚合和流输出的处理。

## 老化方式

产品支持 NetStream 流的老化方式有：活跃时间超时老化、非活跃时间超时老化、TCP 连接断开老化和计数溢出老化和强制老化。

- 非活跃时间老化  
非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。
- 活跃时间老化

活跃时间是指从第一个报文到达当前的时间间隔。当缓存区中的流超过此时间间隔后，等待新的流到来时，系统对缓存区的流进行老化。

- TCP 连接断开老化

对于 TCP 连接，当有标志位 FIN 或 RST 的报文发送时，标志位被置位时，表示一次会话结束。当一条已经存在的 TCP 协议流中采集到一条标志为 FIN 或 RST 的报文时，系统就会把相应的流进行老化。

- 计数溢出老化

流缓存区中的流需要记录流过的报文字节数，当字节数量超过定义的上限时，缓存区就会溢出。当路由器检测到流的字节统计计数超过限制时，系统就会自动对流进行老化。

- 强制老化

可以通过命令行直接老化缓存区的流。

## 7.2 配置 IPv4 网络的流量统计

配置流量统计后对流经自己的网络流量进行采样和处理，并向 NDC 输出 NetStream 原始流信息，以便 NDC 进行更为灵活的后续处理。与聚合流统计相比，运行原始流统计功能对 NDE 设备性能的影响较小，但是由于原始流数据量远大于聚合流数据量，所以原始流会占用 NDE 更多的存储空间和网络带宽。

### 7.2.1 建立配置任务

在配置 IPv4 网络的流量统计功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

### 7.2.2 （可选）调整设备的 AS 域和接口索引模式

为了使 NDA 可以正常接收和解析 NDE 设备输出的 NetStream 报文，NDE 和 NDA 设备的 AS 域模式和接口索引类型必须一致。

### 7.2.3 配置 NetStream 业务的处理方式

路由器接口采集到的流量将被送到业务处理板进行后续的统计处理。NetStream 业务处理方式分为分布式和集中式两种。请根据接口板的支持情况选择适当的业务处理方式。

### 7.2.4 使能接口的 NetStream 功能

请根据业务需要使能整机或某些接口的 NetStream 功能。

### 7.2.5 （可选）配置原始流 TCP-flag 的统计功能

可以通过配置原始流的 TCP-flag 统计功能，提取网络报文中的 TCP-flag 信息发送给网管。网管再根据各个 flag 值对应的数据流数量，判断网络是否遭到了 TCP 异常报文的攻击。

### 7.2.6 （可选）配置模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

### 7.2.7 配置 NetStream 报文的输出

要使原始流报文正确地输出到网管端，需配置原始流的老化时间，报文输出的格式，源地址和目的地址。

### 7.2.8 配置 NetStream 的采样方式和采样比

根据不同的报文间隔和时间间隔，路由器提供四种采样方式，采样间隔可配。采样间隔越小，采得的样品越多，NDA 得到的信息越接近现网实际情况，因此产生的业务流量也越大。请可根据需要选择合适的采样方式和采样比。

### 7.2.9 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

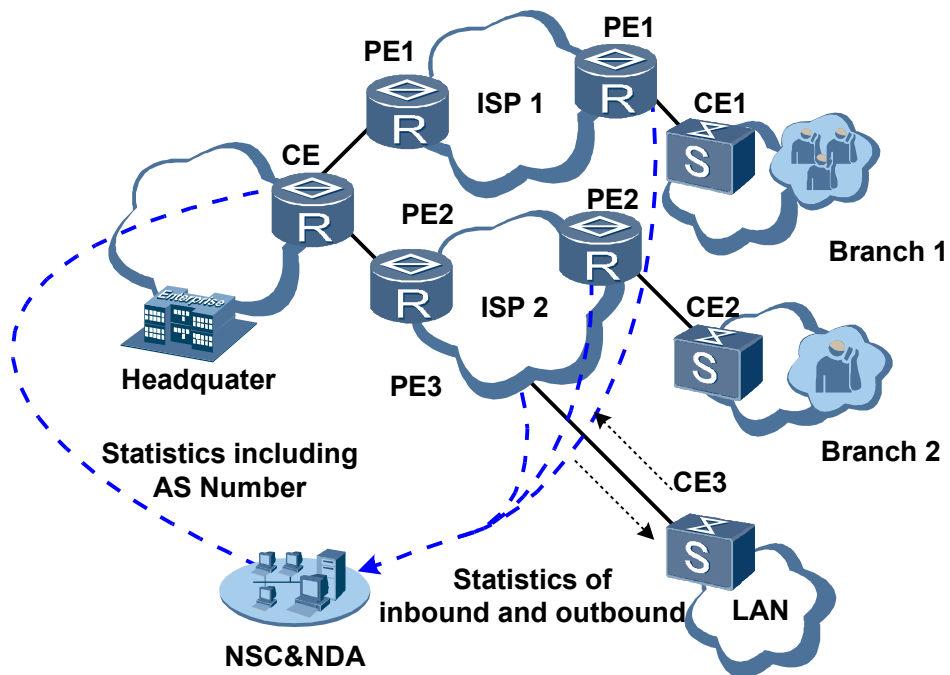
## 7.2.1 建立配置任务

在配置 IPv4 网络的流量统计功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

### 应用环境

如图 7-2 所示，运营商可以对路由器部署 NetStream 获得统计数据来分析网络业务模式。根据部署 NetStream 获得统计信息可以针对用户可以实行灵活的计费策略；也可以根据用户侧流量的统计信息详细分析，详细了解用户流量的情况，进行有效的网络管理。从而保障网络安全运营，实现对网络的监控。

图 7-2 IPv4 网络的流量统计示意图



### 前置任务

在配置 IPv4 网络的流量统计之前，需要完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up
- 配置静态路由或 IGP 协议，使各节点间的 IP 路由可达

### 数据准备

在配置 IPv4 网络的流量统计之前，需要准备以下数据。



| 序号 | 数据                        |
|----|---------------------------|
| 1  | 使能 NetStream 的接口名称及编号     |
| 2  | NetStream 报文输出的版本号        |
| 3  | NetStream 报文输出的 IP 地址及端口号 |

## 7.2.2 （可选）调整设备的 AS 域和接口索引模式

为了使 NDA 可以正常接收和解析 NDE 设备输出的 NetStream 报文，NDE 和 NDA 设备的 AS 域模式和接口索引类型必须一致。

### 背景信息

- **AS 域模式：**根据协议规定，IP 报文中的 AS 字段长度为 16bit，但是在某些地区的网络中，IP 报文的 AS 字段为 32bit。针对网络中 AS 域模式的不同，在配置 NetStream 功能时，为了使 NDE 设备能正常采集到 AS 域间的流量信息，需要对 NDE 设备的 AS 域模式进行切换。



#### 注意

在使用 32 位 AS 域模式的网络中，网管必须要能够识别 32 位 AS 域值，否则网管端就无法识别设备发送来的域间流量信息。

- **接口索引：**网管利用 NetStream 输出报文中携带的接口索引查找输出流量对应的具体接口信息。接口索引分为 16 位和 32 位两种，不同厂家的网管设备支持的接口索引可能不同。NDE 设备须根据网管设备的支持情况来选取 NetStream 输出报文中携带的接口索引类型。如，网管可以支持对 32 位接口索引的解析，则可以配置 NetStream 输出报文中携带的接口索引的类型为 32 位。

在配置接口索引类型或 AS 域模式从 16 位切换到 32 位时，必须同时满足以下条件：

- 原始流输出版本为 v9。
- 所有聚合流的输出版本为 v9。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream as-mode { 16 | 32 }**，配置路由器的 AS 域模式。

缺省情况下，路由器工作在 16 位 AS 域模式。

**步骤 3** 执行命令 **ip netstream export index-switch { 16 | 32 }**，配置路由器输出 NetStream 报文中携带的接口索引的长度类型。

缺省情况下，路由器输出 NetStream 报文携带的接口索引长度为 16 位。

----结束

## 7.2.3 配置 NetStream 业务的处理方式

路由器接口采集到的流量将被送到业务处理板进行后续的统计处理。NetStream 业务处理方式分为分布式和集中式两种。请根据接口板的支持情况选择适当的业务处理方式。

### 背景信息

本产品提供两种配置 NetStream 业务处理方式：

- 配置 NetStream 业务处理方式为分布式
- 配置 NetStream 业务处理方式为集中式

#### 说明

- 若接口板支持分布式处理方式时，可以选择 NetStream 业务处理方式为分布式。
- 若接口板不支持 Netstream 流处理功能，可以选择 NetStream 业务处理方式为集中式。这样接口板对报文进行采样后，将采样报文送到 NetStream 业务板集中进行流聚合和流输出的处理。

### 操作步骤

- 配置 NetStream 业务处理方式为分布式

请在配置 NetStream 业务的路由器上，进行以下的配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **slot slot-id**，进入需要进行 NetStream 采样的接口板的槽位视图。
3. 执行命令 **ip netstream sampler to slot self**，配置 NetStream 业务处理方式为分布式。

- 配置 NetStream 业务处理方式为集中式

请在配置 NetStream 业务的路由器上，进行以下的配置。

1. （可选）执行命令 **set board-type slot slot-id netstream**，设置 SPUC 单板业务模式为 NetStream 模式。

#### 说明

用户可以通过 **display device slot-id** 命令查看当前 SPUC 单板所处的业务模式是否为 NetStream。

2. 执行命令 **system-view**，进入系统视图。
3. 执行命令 **slot slot-id**，进入需要进行 NetStream 采样的接口板的槽位视图。
4. 根据实际情况选择：
  - 执行命令 **ip netstream sampler to slot slot-id1**，配置 NetStream 业务处理方式为集中式并指定处理采样流量的 NetStream 业务板。
  - 执行命令 **ip netstream sampler to slot slot-id2 backup**，配置 NetStream 业务处理方式为集中式并指定处理采样流量的 NetStream 备用业务板。

----结束

## 7.2.4 使能接口的 NetStream 功能

请根据业务需要使能整机或某些接口的 NetStream 功能。

### 背景信息

使能接口的 NetStream 功能后，默认将对以下报文进行 NetStream 统计：



- 单播报文
- 组播报文
- URPF/RPF 丢弃报文
- 分片报文



说明

对于绑定 VPN 实例的接口，对该 VPN 实例的所有报文进行 NetStream 统计。

请在需要进行流量统计的路由器上，进行以下的配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。

**步骤 3** 执行命令 **ip netstream { inbound | outbound }**，使能接口的 NetStream 功能。



说明

- 使能接口的 NetStream 功能的同时使能对报文的 BGP 下一跳进行统计。
- 版本 5 不支持 BGP 下一跳统计。

缺省情况下，不使能单播的 NetStream 入统计和出统计功能。

**步骤 4** （可选）执行命令 **ip netstream statistics enable**，使能接口采样报文的统计功能。



说明

设备最多支持 128 个接口的采样报文统计。

----结束

## 7.2.5 （可选）配置原始流 TCP-flag 的统计功能

可以通过配置原始流的 TCP-flag 统计功能，提取网络报文中的 TCP-flag 信息发送给网管。网管再根据各个 flag 值对应的数据流数量，判断网络是否遭到了 TCP 异常报文的攻击。

## 背景信息

请在需要进行流量统计的路由器上，进行以下的配置。

用户在检测 TCP flood 攻击时，可以通过配置原始流的 TCP-flag 的统计功能，提取 TCP-flag 信息，并进行分析。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream tcp-flag enable**，用来配置原始流支持 TCP-flag 信息的统计。

缺省情况下，不使能原始流支持 TCP-flag 的统计。

----结束

## 7.2.6 （可选）配置模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

### 背景信息



说明

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

为了 NSC 准确地接收并处理统计信息，需要向 NSC 发送统计信息的相关模板，通过配置模板刷新参数，使 NSC 与系统间的模板同步。

option 模板主要包含 NetStream 的配置信息，其中 **export-stats** 和 **sampler** 分别代表系统选项和接口选项。

在配置 option 模板刷新参数的同时使能输出系统选项统计或接口选项统计的功能。选择参数 **export-stats** 将使能系统选项统计功能，选择参数 **sampler** 将使能接口选项统计功能。

请在进行流量统计的路由器上，进行以下的配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream export template option { application-label | export-stats | refresh-rate packet-number | sampler | timeout-rate timeout-interval }**，配置 option 模板的刷新参数。

**步骤 3** 执行命令 **ip netstream export template timeout-rate timeout-interval**，配置原始流信息以版本 9 输出时对应的模板刷新参数。

----结束

## 7.2.7 配置 NetStream 报文的输出

要使原始流报文正确地输出到网管端，需配置原始流的老化时间，报文输出的格式，源地址和目的地址。

### 背景信息

NE20E-X6 支持的可配置的 NetStream 流老化方式有：活跃时间超时老化、非活跃时间超时老化和强制老化。

- 非活跃时间超时老化

非活跃时间 *inactive-interval* 是指从最后一个报文到达接口板缓存区的时间到当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

- 活跃时间超时老化

活跃时间 *active-interval* 是指从第一个报文到达接口板缓存区的时间到当前的时间间隔。当缓存区中的流超过此间隔时间后，等新的流到来时，系统对缓存区的流进行老化。

- 强制老化

可以通过命令行直接老化缓存区的流。

NetStream 原始流报文输出有 V5 和 V9 两种格式可供选择。V5 不支持模版，V9 可以选择模版。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2**（可选）请根据实际需要，选择原始流的老化输出方式：

- 执行命令 **ip netstream timeout active active-interval**，配置 NetStream 原始流的活跃老化时间。  
缺省情况下，NetStream 原始流的活跃老化时间为 30 分钟。
- 执行命令 **ip netstream timeout inactive inactive-interval**，配置 NetStream 原始流的非活跃老化时间。  
缺省情况下，NetStream 原始流的非活跃老化时间为 30 秒。
- 在系统视图下，执行 **reset ip netstream cache slot slot-id** 命令强制老化缓存区的原始流。



### 注意

执行 **reset ip netstream cache slot slot-id** 命令强制老化缓存区的原始流之前，必须先在接口视图下执行 **undo ip netstream { inbound | outbound }** 命令暂时去使能采样功能。否则，从执行 **reset ip netstream cache slot slot-id** 命令起 30 秒之内，系统采样得到的原始流信息就会直接被强制输出，无法进行聚合处理。

执行 **reset ip netstream cache slot slot-id** 命令 30 秒以后，才可以重新使能接口的采样功能。

---

**步骤 3**（可选）执行命令 **ip netstream export version { 5 | 9 } [ origin-as | peer-as ] [ bgp-nexthop ]**，配置输出报文的格式。

NetStream 原始流输出报文支持版本 5 和版本 9 两种报文格式。版本 9 和版本 5 不兼容。

版本 9 基于模板方式输出原始流，统计信息输出更为灵活，而且更容易扩展新定义的流元素以及生成新的记录。

版本 5 格式固定，系统开销小，大多数情况下可使用版本 5 作为 NetStream 原始流报文的输出版本。但在以下几种情况下，必须使用版本 9 作为 NetStream 原始流的输出版本。

- 输出报文需要携带 BGP 下一跳信息。
- 输出报文携带的接口索引需要由 16 位扩展到 32 位。

缺省情况下，原始流按照版本 5 格式输出。版本 5 格式输出不支持 bgp-nexthop。

**步骤 4** 执行命令 **ip netstream export source ip-address**，配置统计信息输出的源地址。

**步骤 5** 执行命令 **ip netstream export host ip-address port**，配置统计信息输出的目的地址和对端 NDC 的 UDP 端口号。最多可以配置两个目的地址，以支持两个 NDC 的备份。若路由器已经配置两个目的地址，更改 NetStream 报文输出的目的地址前，需要删除原来配置的目的地址。

----结束

## 7.2.8 配置 NetStream 的采样方式和采样比

根据不同的报文间隔和时间间隔，路由器提供四种采样方式，采样间隔可配。采样间隔越小，采得的样品越多，NDA 得到的信息越接近现网实际情况，因此产生的业务流量也越大。请可根据需要选择合适的采样方式和采样比。

### 背景信息

本产品提供两种配置 NetStream 业务处理方式：

- 配置 NetStream 普通采样
- 配置 NetStream ACL 采样

### 操作步骤

- 配置 NetStream 普通采样

请在需要进行流量统计的路由器上，进行以下的配置。

1. 执行命令 **system-view**，进入系统视图。
2. 请根据实际情况选择以下配置：
  - 配置系统视图下采样功能，请执行命令 **ip netstream sampler { fix-packets fix-packets | random-packets random-packet | fix-time fix-time | random-time random-time } { inbound | outbound }**。
  - 配置接口视图下采样功能，请按照以下步骤配置。
    - (1) 执行命令 **interface interface-type interface-number**，进入接口视图。
    - (2) 执行命令 **ip netstream sampler { fix-packets fix-packets | random-packets random-packet | fix-time fix-time | random-time random-time } { inbound | outbound }**，配置采样功能。



说明

E3/T3 和 MP-Group 接口不支持 **fix-packets fix-packets** 和 **random-packets random-packet** 参数。GRE Tunnel 接口仅支持 **fix-packets fix-packets** 参数。

- 配置 NetStreamACL 采样

请在需要进行流量统计的路由器上，进行以下的配置。

配置 NetStreamACL 采样过程中，基于类的 QoS 配置的操作步骤请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-QoS》。相关命令请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **traffic classifier classifier-name [ operator { and | or } ]**，定义类并进入类视图。

**operator** 缺省为 **and**，即类视图下各匹配规则之间的关系为逻辑与。
3. 执行命令 **if-match acl access-list-number**，定义 ACL 匹配规则。
4. 执行命令 **quit**，退出类视图。
5. 执行命令 **traffic behavior behavior -name**，定义动作并进入动作视图。
6. 执行命令 **ip netstream sampler { fix-packets fix-packets | random-packets random-packet | fix-time fix-time | random-time random-time }**，配置采样功能。
7. 执行命令 **quit**，退出动作视图。

8. 执行命令 **traffic policy** *policy-name*，定义策略并进入策略视图。
9. 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在策略中为类制定采用的动作。
10. 执行命令 **quit**，退出类视图。
11. 执行命令 **interface** *interface-type* *interface-number*，进入接口视图。
12. 执行命令 **traffic policy** *policy-name* { **inbound** | **outbound** }，应用策略。

----结束

## 7.2.9 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

### 操作步骤

- 使用 **display device** *slot-id* 命令查看 SPU 单板业务模式类型是否为 NetStream。
- 使用 **display ip netstream cache origin slot** *slot-id* 命令查看 NetStream 流缓存区的信息。
- 使用 **display ip netstream statistics slot** *slot-id* 命令查看 NetStream 报文的统计信息。
- 使用 **display ip netstream statistics interface** { *interface-type* | *interface-number* } 命令查看接口采样报文的统计信息。
- 使用命令查看系统视图和聚合视图下的 NetStream 配置信息。
- 使用命令查看所有视图下的 NetStream 配置信息。

----结束

### 任务示例

如果 SPU 单板业务模式为 NetStream 模式，执行命令 **display device 3**，可以看到路由器的 SPU 单板类型显示为 NetStream。

```
<HUAWEI> display device 3
SPU3's detail information:

Description: Service Processing Unit - Netstream
Board status: Normal
Register: Registered
Uptime: 2009/01/19 12:03:21
CPU Utilization(%): 5%
Mem Usage(%): 39%
Clock information:
State item State
Current syn-clock: 18
Current line-clock: 23
Syn-clock state: Locked VCX0_OK REF_OK
Syn-clock 17 state: Activated
Syn-clock 18 state: Activated
Line-clock 23 state: Inactivated
Line-clock 24 state: Inactivated
Statistic information:
Statistic item Statistic number
SERDES interface link lost: 0
Mpu switches: 0
Syn-clock switches: 0

```

如果 NetStream 配置成功，执行命令 **display ip netstream cache origin slot 3**，可以看到路由器的 NetStream 流缓存区的统计到的 IP 报文的各种统计信息。

```
<HUAWEI> display ip netstream cache origin slot 3
Show information of IP and MPLS cache of slot 3 is starting.
get show cache user data success.
```

| DstIf             |         | DstP | Msk | Pro          | Tos | Flags     | Packets |
|-------------------|---------|------|-----|--------------|-----|-----------|---------|
| SrcIf             |         | SrcP | Msk | NextHop      |     |           |         |
| DstIP             |         |      |     | DstAs        |     |           |         |
| SrcIP             |         |      |     | SrcAs        |     |           |         |
| BGP: BGP          | NextHop |      |     | TopLabelType |     | Direction |         |
| Label1            | Exp1    |      |     | Bottom1      |     |           |         |
| Label2            | Exp2    |      |     | Bottom2      |     |           |         |
| Label3            | Exp3    |      |     | Bottom3      |     |           |         |
| TopLabelIpAddress |         |      |     | VlanId       |     |           |         |
| -----             |         |      |     |              |     |           |         |
| Null              |         | 0    | 0   | 6            | 0   | 0         | 19054   |
| ET1               |         | 0    | 0   | 0            |     |           |         |
| 3::200:0:300:2    |         |      |     |              | 0   |           |         |
| 1::200:0:100:1    |         |      |     |              | 0   |           |         |
| 0.0.0.0           |         |      | 0   |              |     | in        |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0.0.0.0           |         |      | 0   |              |     |           |         |
| Null              |         | 0    | 0   | 6            | 0   | 2         | 23569   |
| ET1               |         | 3    | 0   | 0            |     |           |         |
| 3::200:0:300:2    |         |      |     |              | 0   |           |         |
| 1::200:0:100:1    |         |      |     |              | 0   |           |         |
| 0.0.0.0           |         |      | 0   |              |     | in        |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0                 | 0       |      | 0   |              |     |           |         |
| 0.0.0.0           |         |      | 0   |              |     |           |         |

如果 NetStream 配置成功，执行命令 **display ip netstream statistics interface { interface-type | interface-number }**，可以看到路由器的接口 GE3/0/0 采样报文的统计信息。

```
[HUAWEI] display ip netstream statistics interface GigabitEthernet3/0/0
Netstream statistic information of <GigabitEthernet3/0/0> :
Inbound :
IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
Outbound :
IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
```

## 7.3 配置 MPLS 网络的流量统计

配置 MPLS 网络的流量统计对封装 IPv4 报文的 MPLS 流量进行外三层标签信息的采集。在 MPLS 网络上的流量进行原始流统计，可以帮助用户监控 MPLS 网络的使用情况。

### 7.3.1 建立配置任务

在配置 MPLS 网络的流量统计功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

### 7.3.2 （可选）调整设备的 AS 域和接口索引模式

为了使 NDA 可以正常接收和解析 NDE 设备输出的 NetStream 报文，NDE 和 NDA 设备的 AS 域模式和接口索引类型必须一致。

### 7.3.3 配置 NetStream 采样的处理方式



路由器接口采集到的流量将被送到业务处理板进行后续的统计处理。NetStream 业务处理方式分为分布式和集中式两种。请根据接口板的支持情况选择适当的业务处理方式。

#### 7.3.4 使能接口的 NetStream 统计功能

请根据业务需要使能整机或某些接口的 NetStream 功能。

#### 7.3.5 配置 MPLS 报文的统计功能

对于 MPLS 报文可选择采集内层 IP 报文头信息或采集标签信息，用户可根据实际需要进行选配。默认情况下只采集内层 IP 报文头信息。

#### 7.3.6 （可选）配置模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

#### 7.3.7 配置 NetStream 报文的输出

要使原始流报文正确地输出到网管端，需配置原始流的老化时间，报文输出的格式，源地址和目的地址。

#### 7.3.8 配置 NetStream 的采样

根据不同的报文间隔和时间间隔，路由器提供四种采样方式，采样间隔可配。采样间隔越小，采得的样品越多，NDA 得到的信息越接近现网实际情况，因此产生的业务流量也越大。请可根据需要选择合适的采样方式和采样比。

#### 7.3.9 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

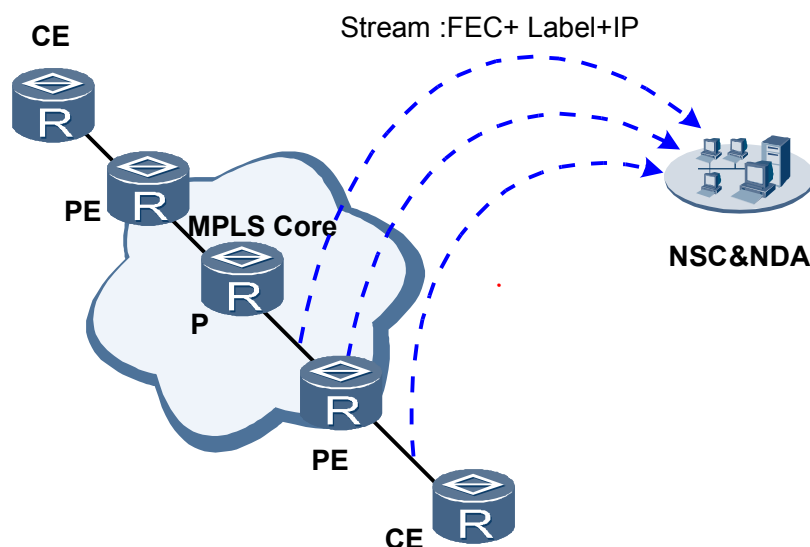
### 7.3.1 建立配置任务

在配置 MPLS 网络的流量统计功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

#### 应用环境

如图 7-3 所示，在 MPLS 骨干网中，运营商可以通过在 PE 用户侧接口上部署 NetStream 对 MPLS 网络进行计费；在 PE 网络侧以及 P 路由器上部署 NetStream，通过对 MPLS 流量进行统计，可以精确地分析 MPLS 业务的模式。

图 7-3 配置 MPLS 网络的流量统计组网图



## 前置任务

在配置 MPLS 网络的流量统计之前，需要完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up
- 配置静态路由或 IGP 协议，使各节点间的 IP 路由可达
- 配置 MPLS 基本能力

## 数据准备

在配置 MPLS 网络的流量统计之前，需要准备以下数据。

| 序号 | 数据                        |
|----|---------------------------|
| 1  | 使能 NetStream 的接口名称及编号     |
| 2  | NetStream 报文输出的版本号        |
| 3  | NetStream 报文输出的 IP 地址及端口号 |

### 7.3.2 （可选）调整设备的 AS 域和接口索引模式

为了使 NDA 可以正常接收和解析 NDE 设备输出的 NetStream 报文，NDE 和 NDA 设备的 AS 域模式和接口索引类型必须一致。

## 背景信息

- **AS 域模式：**根据协议规定，IP 报文中的 AS 字段长度为 16bit，但是在某些地区的网络中，IP 报文的 AS 字段为 32bit。针对网络中 AS 域模式的不同，在配置 NetStream 功能时，为了使 NDE 设备能正常采集到 AS 域间的流量信息，需要对 NDE 设备的 AS 域模式进行切换。



#### 注意

在使用 32 位 AS 域模式的网络中，网管必须要能够识别 32 位 AS 域值，否则网管端就无法识别设备发送来的域间流量信息。

- **接口索引：**网管利用 NetStream 输出报文中携带的接口索引查找输出流量对应的具体接口信息。接口索引分为 16 位和 32 位两种，不同厂家的网管设备支持的接口索引可能不同。NDE 设备须根据网管设备的支持情况来选取 NetStream 输出报文中携带的接口索引类型。如，网管可以支持对 32 位接口索引的解析，则可以配置 NetStream 输出报文中携带的接口索引的类型为 32 位。

在配置接口索引类型或 AS 域模式从 16 位切换到 32 位时，必须同时满足以下条件：

- 原始流输出版本为 v9。
- 所有聚合流的输出版本为 v9。



## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream as-mode { 16 | 32 }**，配置路由器的 AS 域模式。

缺省情况下，路由器工作在 16 位 AS 域模式。

**步骤 3** 执行命令 **ip netstream export index-switch { 16 | 32 }**，配置路由器输出 NetStream 报文中携带的接口索引的长度类型。

缺省情况下，路由器输出 NetStream 报文携带的接口索引长度为 16 位。

----结束

### 7.3.3 配置 NetStream 采样的处理方式

路由器接口采集到的流量将被送到业务处理板进行后续的统计处理。NetStream 业务处理方式分为分布式和集中式两种。请根据接口板的支持情况选择适当的业务处理方式。

#### 背景信息

具体配置过程请参见“[配置 NetStream 业务的处理方式](#)”。

### 7.3.4 使能接口的 NetStream 统计功能

请根据业务需要使能整机或某些接口的 NetStream 功能。

#### 背景信息

具体配置过程请参见“[使能接口的 NetStream 功能](#)”。

### 7.3.5 配置 MPLS 报文的统计功能

对于 MPLS 报文可选择采集内层 IP 报文头信息或采集标签信息，用户可根据实际需要进行选配。默认情况下只采集内层 IP 报文头信息。

#### 背景信息

请在需要进行流量统计的路由器上，进行以下的配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream mpls-aware { ip-only | label-and-ip | label-only }**，配置对 MPLS 报文的统计功能。

请根据用户对 MPLS 报文采样信息的需求选择采样方式。

- 如果用户对于 MPLS 报文不采集内层 IP 报文只采集标签，则选择 **label-only**。
- 如果用户对于 MPLS 报文既采集内层 IP 报文也采集标签，则选择 **label-and-ip**。

----结束

### 7.3.6 （可选）配置模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

#### 背景信息

为了 NSC 准确地接收并处理统计信息，路由器需要向 NSC 发送统计信息相关的模板，通过配置模板刷新参数，使 NSC 与路由器间的模板同步。

option 模板主要包含 NetStream 的配置信息，其中 **export-stats** 和 **sampler** 分别代表系统选项和接口选项，在配置 option 模板刷新参数的同时，将使能输出系统选项统计或接口选项统计的功能。

选择参数 **export-stats** 将使能系统选项统计功能，选择参数 **sampler** 将使能接口选项统计功能。



说明

只有配置 NetStream 输出报文的格式为版本 9，才能配置此步骤。

请在需要进行流量统计的路由器上，进行以下配置。

#### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream export template option { application-label | export-stats | refresh-rate packet-number | sampler | timeout-rate timeout-interval }**，配置 option 模板的刷新参数。
- 步骤 3** 执行命令 **ip netstream export template timeout-rate timeout-interval**，配置原始流信息以版本 9 输出时对应的模板刷新参数。

----结束

### 7.3.7 配置 NetStream 报文的输出

要使原始流报文正确地输出到网管端，需配置原始流的老化时间，报文输出的格式，源地址和目的地址。

#### 背景信息

具体配置过程请参见“[配置 NetStream 报文的输出](#)”。

### 7.3.8 配置 NetStream 的采样

根据不同的报文间隔和时间间隔，路由器提供四种采样方式，采样间隔可配。采样间隔越小，采得的样品越多，NDA 得到的信息越接近现网实际情况，因此产生的业务流量也越大。请可根据需要选择合适的采样方式和采样比。

#### 背景信息

具体配置过程请参见“[配置 NetStream 的采样](#)”。

### 7.3.9 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

#### 操作步骤

- 使用 **display device slot-id** 命令查看 SPU 单板业务模式类型是否为 NetStream。
- 使用 **display ip netstream cache origin slot slot-id** 命令查看 NetStream 流缓存区的信息。
- 使用 **display ip netstream statistics slot slot-id** 命令查看 NetStream 报文的统计信息。
- 使用 **display ip netstream statistics interface { interface-type | interface-number }** 命令查看接口采样报文的统计信息。
- 使用命令查看系统视图和聚合视图下的 NetStream 配置信息。
- 使用命令查看所有视图下的 NetStream 配置信息。

----结束

#### 任务示例

如果 SPU 单板业务模式为 NetStream 模式，执行命令 **display device 3**，可以看到路由器的 SPU 单板类型显示为 NetStream。

```
<HUAWEI> display device 3
SPU3's detail information:

Description: Service Processing Unit - Netstream
Board status: Normal
Register: Registered
Uptime: 2009/01/19 12:03:21
CPU Utilization(%): 5%
Mem Usage(%): 39%
Clock information:
State item State
Current syn-clock: 18
Current line-clock: 23
Syn-clock state: Locked VCX0_OK REF_OK
Syn-clock 17 state: Activated
Syn-clock 18 state: Activated
Line-clock 23 state: Inactivated
Line-clock 24 state: Inactivated
Statistic information:
Statistic item Statistic number
SERDES interface link lost: 0
Mpu switches: 0
Syn-clock switches: 0

```

如果 NetStream 配置成功，执行命令 **display ip netstream cache origin slot 3**，可以看到路由器的 NetStream 流缓存区的统计到的 MPLS 报文的各种统计信息。

```
<HUAWEI> display ip netstream cache origin slot 3
Show information of IP and MPLS cache of slot 3 is starting.
get show cache user data success.
```

|          |         |              |         |           |       |         |
|----------|---------|--------------|---------|-----------|-------|---------|
| DstIf    | DstP    | Msk          | Pro     | Tos       | Flags | Packets |
| SrcIf    | SrcP    | Msk          | NextHop |           |       |         |
| DstIP    | DstAs   |              |         |           |       |         |
| SrcIP    | SrcAs   |              |         |           |       |         |
| BGP: BGP | NextHop | TopLabelType |         | Direction |       |         |

| Label1            | Exp1   | Bottom1 |   |   |   |    |       |
|-------------------|--------|---------|---|---|---|----|-------|
| Label2            | Exp2   | Bottom2 |   |   |   |    |       |
| Label3            | Exp3   | Bottom3 |   |   |   |    |       |
| TopLabelIpAddress | VlanId |         |   |   |   |    |       |
| <hr/>             |        |         |   |   |   |    |       |
| Null              |        | 0       | 0 | 6 | 0 | 0  | 19054 |
| ET1               |        | 0       | 0 | 0 |   |    |       |
| 3::200:0:300:2    |        |         |   |   | 0 |    |       |
| 1::200:0:100:1    |        |         |   |   | 0 |    |       |
| 0.0.0.0           |        |         | 0 |   |   | in |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0.0.0.0           |        |         | 0 |   |   |    |       |
| <hr/>             |        |         |   |   |   |    |       |
| Null              |        | 0       | 0 | 6 | 0 | 2  | 23569 |
| ET1               |        | 3       | 0 | 0 |   |    |       |
| 3::200:0:300:2    |        |         |   |   | 0 |    |       |
| 1::200:0:100:1    |        |         |   |   | 0 |    |       |
| 0.0.0.0           |        |         | 0 |   |   | in |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0                 | 0      |         | 0 |   |   |    |       |
| 0.0.0.0           |        |         | 0 |   |   |    |       |

如果 NetStream 配置成功，执行命令 **display ip netstream statistics interface { interface-type | interface-number }**，可以看到路由器的接口 GE3/0/0 采样报文的统计信息。

```
[HUAWEI] display ip netstream statistics interface GigabitEthernet3/0/0
Netstream statistic information of <GigabitEthernet3/0/0> :
Inbound :
 IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
Outbound :
 IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
```

## 7.4 配置聚合流的流量统计

NDE 设备完成原始流信息采集后，用户可以根据不同的统计需求，将原始流数据进行聚合，再输出到 NDC 进行分析。这样可以减少因统计功能产生的网络数据量，也可以避免不必要的信息干扰。

### 7.4.1 建立配置任务

在配置 IPv4/MPLS/VPN 网络原始流的聚合输出功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

### 7.4.2 配置聚合功能

配置聚合模式即是指定原始流聚合的特征值类型。这些指定特征值相同的原始流数据会聚合成为一条聚合流输出到 NDC，满足用户的定向统计需求。

### 7.4.3 （可选）配置 NetStream 报文输出的格式

NetStream 聚合流报文支持以版本 8 和版本 9 两种格式输出。缺省情况下，聚合流按照版本 8 格式输出。

### 7.4.4 （可选）配置聚合流模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

### 7.4.5 （可选）配置老化时间

NetStream 流可以按照设定的老化时间定时输出。可配置的 NetStream 流老化时间有：活跃时间超时老化和非活跃时间超时老化。

### 7.4.6 配置 NetStream 报文的输出

要使聚合流报文正确地输出到网管端，需配置报文输出的源地址和目的地址。

#### 7.4.7 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

### 7.4.1 建立配置任务

在配置 IPv4/MPLS/VPN 网络原始流的聚合输出功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

#### 应用环境

对于运营商，对设备特别是高速接口部署 NetStream，如果按照 V5 版本输出且采样比较密集的情况下，路由器和服务器性能都会受到极大的影响。可以采用聚合流的方式，减少对系统资源的占用并可以根据聚合流聚合方式灵活的特点，输出满足用户需要的数据。

#### 前置任务

在配置聚合流的流量统计之前，需要完成以下任务：

- 保证接口的工作正常。
- 配置接口的链路层属性。
- 配置接口的 IP 地址。
- 使能路由器的 NetStream 流量统计功能。



说明

关于路由器的 NetStream 流量统计功能配置，请参见“[配置 IPv4 网络的流量统计](#)”和“[配置 MPLS 网络的流量统计](#)”。

#### 数据准备

在配置聚合流的流量统计之前，需要准备以下数据。

| 序号 | 数据                        |
|----|---------------------------|
| 1  | 使能 NetStream 的接口名称及编号     |
| 2  | NetStream 报文输出的版本号        |
| 3  | NetStream 报文输出的 IP 地址及端口号 |

### 7.4.2 配置聚合功能

配置聚合模式即是指定原始流聚合的特征值类型。这些指定特征值相同的原始流数据会聚合成为一条聚合流输出到 NDC，满足用户的定向统计需求。

#### 背景信息

请在需要进行流量统计的路由器上，进行以下的配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream aggregation { as | as-tos | bgp-nexthop-tos | destination-prefix | destination-prefix-tos | index-tos | mpls-label | prefix | prefix-tos | protocol-port | protocol-port-tos | source-index-tos | source-prefix | source-prefix-tos | vlan-id }**，进入聚合配置模式视图。
- 步骤 3** 执行命令 **enable**，使能聚合功能。
- 步骤 4** （可选）执行命令 **mask { source | destination } minimum mask-length**，配置聚合的掩码。



说明

聚合的掩码只可以在 destination-prefix、destination-prefix-tos、prefix、prefix-tos、source-prefix、source-prefix-tos 这 6 中聚合方式中配置。

----结束

### 7.4.3 （可选）配置 NetStream 报文输出的格式

NetStream 聚合流报文支持以版本 8 和版本 9 两种格式输出。缺省情况下，聚合流按照版本 8 格式输出。

## 背景信息

请在需要进行流量统计的路由器上，进行以下的配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream aggregation { as | as-tos | bgp-nexthop-tos | destination-prefix | destination-prefix-tos | index-tos | mpls-label | prefix | prefix-tos | protocol-port | protocol-port-tos | source-index-tos | source-prefix | source-prefix-tos | vlan-id }**，进入聚合配置模式视图。
- 步骤 3** 执行命令 **export version { 8 | 9 }**，配置聚合流输出的报文格式。

- **bgp-nexthop-tos**，**index-tos**，**mpls-label**，**source-index-tos** 和 **vlan-id** 聚合流仅支持版本 9 格式输出。
- 缺省情况下，其他聚合流按照版本 8 格式输出。

----结束

### 7.4.4 （可选）配置聚合流模板刷新参数

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

## 背景信息



说明

只有配置 NetStream 输出报文的格式为版本 9，才能进行此步骤配置。

请在需要进行流量统计的路由器上，进行以下的配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream aggregation { as | as-tos | bgp-nexthop-tos | destination-prefix | destination-prefix-tos | index-tos | mpls-label | prefix | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-index-tos | source-prefix-tos | vlan-id }**，进入聚合配置模式视图。
- 步骤 3** 执行命令 **template timeout-rate timeout-interval**，配置聚合流信息以版本 9 输出时对应的模板刷新参数。
- 结束

## 7.4.5 （可选）配置老化时间

NetStream 流可以按照设定的老化时间定时输出。可配置的 NetStream 流老化时间有：活跃时间超时老化和非活跃时间超时老化。

### 背景信息

在需要对流进行采用的路由器上进行以下的配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream aggregation timeout active active-interval**，配置 NetStream 聚合流的活跃老化时间。
- 步骤 3** 执行命令 **ip netstream aggregation timeout inactive inactive-interval**，配置 NetStream 聚合流的非活跃老化时间。
- 缺省情况下，NetStream 聚合流的活跃老化时间为 30 分钟，非活跃老化时间为 300 秒。
- 结束

## 7.4.6 配置 NetStream 报文的输出

要使聚合流报文正确地输出到网管端，需配置报文输出的源地址和目的地址。

### 背景信息

请在需要进行流量统计的路由器上，进行以下的配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **ip netstream aggregation { as | as-tos | bgp-nexthop-tos | destination-prefix | destination-prefix-tos | index-tos | mpls-label | prefix | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-prefix-tos | vlan-id }**，进入聚合视图。
- 步骤 3** 执行命令 **ip netstream export host ip-address port**，配置 NetStream 报文输出的目的地址及端口号。



**步骤 4** 执行命令 **ip netstream export source ip-address**，配置 NetStream 报文输出的源地址。

----结束

## 7.4.7 检查配置结果

在日常维护工作中，或已经完成 NetStream 统计功能的相关配置后，可以在任意视图下选择执行以下命令，了解当前设备上的 NetStream 功能运行状态。

### 操作步骤

- 使用 **display device slot-id** 命令查看 SPU 单板业务模式类型是否为 NetStream。
- 使用 **display ip netstream cache { as | as-tos | bgp-nexthop-tos | destination-prefix | destination-prefix-tos | index-tos | mpls-label | prefix | prefix-tos | protocol-port | protocol-port-tos | source-index-tos | source-prefix | source-prefix-tos | vlan-id } slot slot-id** 命令查看缓存区中各种聚合的信息。
- 使用 **display ip netstream statistics slot slot-id** 命令查看 NetStream 报文的统计信息。
- 使用命令查看系统视图和聚合视图下的 NetStream 配置信息。
- 使用命令查看所有视图下的 NetStream 配置信息。

----结束

### 任务示例

如果 SPU 单板业务模式为 NetStream 模式，执行命令 **display device 3**，可以看到路由器的 SPU 单板类型显示为 NetStream。

```
<HUAWEI> display device 3
SPU3's detail information:
```

```

Description: Service Processing Unit - Netstream
Board status: Normal
Register: Registered
Uptime: 2009/01/19 12:03:21
CPU Utilization(%): 5%
Mem Usage(%): 39%
Clock information:
State item State
Current syn-clock: 18
Current line-clock: 23
Syn-clock state: Locked VCXO_OK REF_OK
Syn-clock 17 state: Activated
Syn-clock 18 state: Activated
Line-clock 23 state: Inactivated
Line-clock 24 state: Inactivated
Statistic information:
Statistic item Statistic number
SERDES interface link lost: 0
Mpu switches: 0
Syn-clock switches: 0

```

如果 NetStream 目的地址和前缀聚合配置成功，执行命令 **display ip netstream cache destination-prefix slot 3**，可以看到路由器的 NetStream 流缓存区的统计到的 IP 或 MPLS 报文的目的地址 AS 域、掩码和前缀的详细信息。

```
<HUAWEI> display ip netstream cache destination-prefix slot 3
Show information of aggregation-prefix cache of slot 3 is starting.
get show cache user data success.
```



| DstIf<br>SrcIf | DstAs<br>SrcAs | DstMsk<br>SrcMsk | DstPre<br>SrcPre | Streams | Packets | Direction |
|----------------|----------------|------------------|------------------|---------|---------|-----------|
| GI3/0/9        | 0              | 32               | 192.168.111.2    |         |         |           |
| Local          | 0              | 32               | 192.168.111.1    | 1       | 8       | out       |

## 7.5 配置 NetStream 多地址输出

通过配置 NetStream 多址输出，可以使指定的流量输出到指定的服务器。

- 7.5.1 建立配置任务
- 在配置 NetStream 采集流量多地址输出前了解它的应用环境、配置此特性的前置任务和  
数据准备，可以帮助您快速、准确地完成配置任务。
- 7.5.2 使能接口的 NetStream 功能
- 7.5.3 配置 NetStream 的采样比
- 7.5.4 配置 NetStream 的采样模式
- 7.5.5 配置报文的输出格式
- 7.5.6 配置统计信息的多地址输出
- 7.5.7 检查配置结果

### 7.5.1 建立配置任务

在配置 NetStream 采集流量多地址输出前了解它的应用环境、配置此特性的前置任务和  
数据准备，可以帮助您快速、准确地完成配置任务。

#### 应用环境

路由器的不同接口上连接不同的网络。部署 NetStream 后，为了对网络更好的进行分类  
监控，需要把指定接口上采集到的流量统计信息输出到指定的服务器进行分析。

#### 前置任务

无

#### 数据准备

在配置 NetStream 采集流量多地址输出之前，需要执行如下的配置过程。

| 序号 | 数据            |
|----|---------------|
| 1  | 报文的输出格式       |
| 2  | 统计信息输出的地址和端口号 |

### 7.5.2 使能接口的 NetStream 功能

## 背景信息

在需要统计流量信息的路由器上进行以下的配置。

## 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。
- 步骤 3** 执行命令 **ip netstream { inbound | outbound }**，使能接口的 NetStream 统计功能。
- 步骤 4**（可选）执行命令 **ip netstream statistics enable**，使能接口采样报文的统计功能。



说明

设备最多支持 128 个接口的采样报文统计。

----结束

## 7.5.3 配置 NetStream 的采样比

### 背景信息

在需要统计流量信息的路由器上进行以下的配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。
- 步骤 3** 执行命令 **ip netstream sampler { fix-packet fix-packet-number | random-packet random-packet-number | fix-time fix-time-value | random-time random-time-value } { inbound | outbound }**，配置 NetStream 的入统计或者出统计采样比。

----结束

## 7.5.4 配置 NetStream 的采样模式

### 背景信息

在需要统计流量信息的路由器上进行以下的配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **slot slot-id**，进入槽位视图。
- 步骤 3** 执行命令 **ip netstream sampler to slot { self | slot-id }**，配置 NetStream 的采样模式。

----结束

## 7.5.5 配置报文的输出格式

## 背景信息

在需要统计接口流信息的路由器上进行以下的配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **ip netstream export version version**，配置原始流统计信息的输出版本格式。

----结束

## 7.5.6 配置统计信息的多地址输出

### 背景信息

在需要配置指定统计信息输出到指定服务器的路由器上，进行以下的配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 创建 NetStream 监控业务视图。

- 执行命令 **ip netstream monitor monitor-name**，对 IPv4 流创建 NetStream 监控业务视图。

**步骤 3** 执行命令 **ip netstream export host ip-address port**，配置流量统计输出的目的地址。

**步骤 4** 执行命令 **quit**，退回到系统视图。

**步骤 5** 执行命令 **interface interface-type interface-number**，进入接口视图。

**步骤 6** 在接口流量的入方向或者出方向上部署 NetStream 监控业务。

- 执行命令 **ip netstream monitor monitor-name { inbound | outbound }**，在接口流量的入方向或者出方向上对 IPv4 流部署 NetStream 监控业务。

----结束

## 7.5.7 检查配置结果

### 前提条件

已经完成 NetStream 统计信息多地址输出的所有配置。

### 操作步骤

- 显示主控板或者接口板上的监控业务信息。
  - 执行命令 **display ip netstream monitor { all | monitor-name } [ slot slot-id ]**，显示主控板或者接口板上的监控 IPv4 流业务信息。
- 使用 **display ip netstream statistics interface { interface-type | interface-number }** 命令查看接口采样报文的统计信息。

----结束

## 任务示例

执行命令 **display ip netstream monitor**，显示主控板上的监控业务信息。

```
[HUAWEI]display ip netstream monitor all
Monitor test
ID : 1
AppCount : 2
First address : 10.2.1.2
First port : 5000
Second address : 0.0.0.0
Second port : 0
Monitor test1
ID : 1
AppCount : 2
First address : 10.1.1.1
First port : 6000
Second address : 0.0.0.0
Second port : 0
```

如果 NetStream 配置成功，执行命令 **display ip netstream statistics interface { interface-type | interface-number }**，可以看到路由器的接口 GE3/0/0 采样报文的统计信息。

```
[HUAWEI] display ip netstream statistics interface GigabitEthernet3/0/0
Netstream statistic information of <GigabitEthernet3/0/0> :
Inbound :
IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
Outbound :
IPV4 :11 Bytes, IPV6 :12 Bytes, Total :23 Bytes
```

## 7.6 维护 NetStream

维护 NetStream 包括如何清除 NetStream 统计信息。

### 7.6.1 强制老化原始流

强制老化指定槽位单板上缓存区的原始流，输出原始流或聚合流。

### 7.6.1 强制老化原始流

强制老化指定槽位单板上缓存区的原始流，输出原始流或聚合流。

## 背景信息

执行此命令强制老化指定槽位上缓存区的原始流，输出原始流或聚合流。



注意

执行 **reset ip netstream cache slot slot-id** 命令强制老化缓存区的原始流之前，必须先接口视图下执行 **undo ip netstream** 命令暂时去使能采样功能。否则，从执行 **reset ip netstream cache slot slot-id** 命令起 30 秒之内，系统采样得到的原始流信息就会直接被强制输出，无法进行聚合处理。

执行 **reset ip netstream cache slot slot-id** 命令 30 秒以后，才可以重新使能接口的采样功能。

---

## 操作步骤

- 在系统视图下，执行 **reset ip netstream cache slot slot-id** 命令强制老化缓存区的原始流。

----结束

## 7.7 配置举例

请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

### 7.7.1 配置 IPv4 网络用户侧异常流量统计分析示例

在数据通信网络中，PE 设备经常会遇到用户侧的非法流量的攻击。在 PE 设备的用户侧接口上使能 NetStream 统计功能，实时采集网络流量的统计信息并发往网管端分析，可以帮助运营商实现对用户侧流量的监控和管理，达到抑制病毒流量传播的目的。

### 7.7.2 配置 IPv4 网络 VLANIF 流量统计示例

VLANIF 接口可以连通不同的 VLAN 间的流量。在 VLANIF 接口上使能 NetStream 功能，实现对 VLAN 间流量的监控。

### 7.7.3 配置 IPv4 网络 GRE 流量统计示例

在 GRE 隧道接口上使能 NetStream 功能，实现对 GRE 隧道流量的监控。

### 7.7.4 配置 MPLS 网络的流量统计示例

MPLS 流量是通过标签进行转发的。在 MPLS 网络中使能标签统计功能，可以获取 MPLS 报文的外三层标签信息。

### 7.7.5 配置聚合流的流量统计示例

如果两个运营商需要统计经过各自 AS 域流量，实现流量的分账，可以在边界路由器上使能 NetStream 功能，并对原始流信息进行 AS 聚合处理。网管可分析出不同 AS 域的流量分布情况，实现流量分账的目的。

### 7.7.6 配置统计信息输出主机备份示例

向两台网管同时输出 NetStream 统计信息，实现统计信息的备份和异地分析。

### 7.7.7 配置 VLAN 聚合流量统计示例

通过配置 VLAN 聚合流量统计，运营商的网管系统可以监控到接入运营商网络的不同用户的业务流量，为计费提供依据。

### 7.7.8 配置 NetStream 接口索引映射示例

通过配置 NetStream 接口索引输出为 32 位的接口索引，使网管直接根据输出的 32 位接口索引取得接口名称。

### 7.7.9 配置 NetStream 的多地址输出

配置 NetStream 多址后，不同接口的统计信息，可以根据不同的输出方向进行输出。

## 7.7.1 配置 IPv4 网络用户侧异常流量统计分析示例

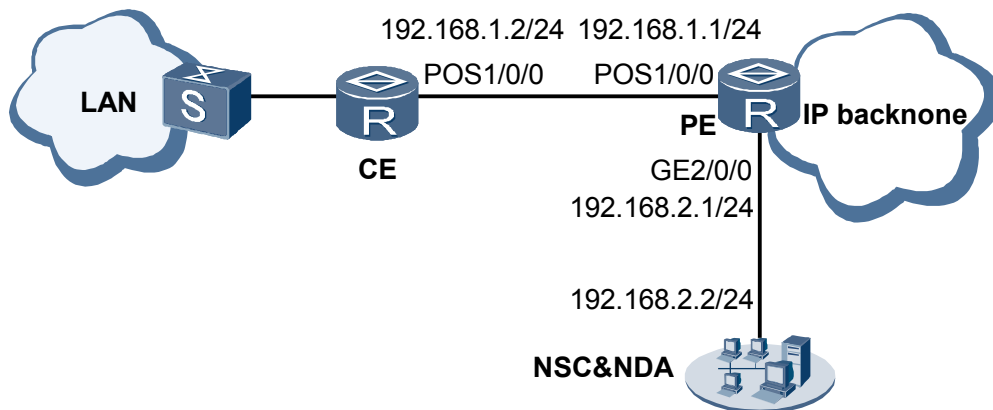
在数据通信网络中，PE 设备经常会遇到用户侧的非法流量的攻击。在 PE 设备的用户侧接口上使能 NetStream 统计功能，实时采集网络流量的统计信息并发往网管端分析，可以帮助运营商实现对用户侧流量的监控和管理，达到抑制病毒流量传播的目的。

## 组网需求

如图 7-4 所示，应用 NetStream 的分析方法，对网络中用户侧报文的源 IP、目的 IP、端口、协议等详细信息进行统计，可以快速进行蠕虫病毒中毒终端的检测、DoS/DDoS 攻

击源和目的检测、垃圾邮件源的检测、私设地下网站检测和用户行为分析等。用户还可以根据流量的特征快速定位病毒类型和感染病毒等异常流量的 IP 地址。并根据 NetStream 数据流的其它特征在其他网络设备上采取相应的限制、过滤措施，从而达到抑制病毒流量传播的目的。

图 7-4 配置 IPv4 网络用户侧异常流量统计分析组网图



## 配置思路

采用如下的思路配置 IPv4 网络用户侧流量统计：

1. 配置 PE 与 CE 之间网络互通。
2. 配置 PE 用户侧接口的 NetStream 入统计和出统计功能。

## 数据准备

为完成此配置例，需准备如下的数据：

- PE 用户侧接口。
- NetStream 报文输出的版本号。
- NetStream 信息输出的目的地址、目的端口、源地址。
- NetStream 业务板的槽位号，本举例中 NetStream 业务板位于 4 号槽位。

## 操作步骤

### 步骤 1 配置 PE 与 CE 之间网络互通

# 按照图 7-4 配置各接口 IP 地址和掩码，具体配置过程略。

### 步骤 2 配置 PE 用户侧接口 POS1/0/0 的 NetStream 统计功能

# 配置 SPUC 单板的 NetStream 业务处理方式为集中式。

```

<PE> set board-type slot 4 netstream
<PE> system-view
[PE] slot 1
[PE-slot-1] ip netstream sampler to slot 4
[PE-slot-1] return

```

# 配置 PE 接口 POS1/0/0 的 NetStream 入统计和出统计功能。

```
[PE] interface pos 1/0/0
[PE-Pos1/0/0] undo shutdown
[PE-Pos1/0/0] ip netstream inbound
[PE-Pos1/0/0] ip netstream outbound
[PE-Pos1/0/0] quit

配置原始流 TCP-flag 的统计功能。

[PE] ip netstream tcp-flag enable

配置版本 5 输出目的地址，目的端口和源地址。

[PE] ip netstream export host 192.168.2.2 9001
[PE] ip netstream export source 192.168.2.1

配置 NetStream 采样，采样方式为固定报文采样。

[PE] ip netstream sampler fix-packets 10000 inbound
[PE] ip netstream sampler fix-packets 10000 outbound
```

步骤 3 检查配置效果

```
配置成功后，在用户视图下执行命令 display ip netstream cache origin slot 4，可以看到 NetStream 流缓存区中的各种原始流的信息。

<PE> display ip netstream cache origin slot 4
Show information of IP and MPLS cache of slot 4 is starting.
get show cache user data success.
```

| DstIf             |      | DstP    | Msk | Pro          | Tos       | Flags | Packets |
|-------------------|------|---------|-----|--------------|-----------|-------|---------|
| SrcIf             |      | SrcP    | Msk | NextHop      |           |       |         |
| DstIP             |      |         |     | DstAs        |           |       |         |
| SrcIP             |      |         |     | SrcAs        |           |       |         |
| BGP:              | BGP  | NextHop |     | TopLabelType | Direction |       |         |
| Label1            | Exp1 |         |     | Bottom1      |           |       |         |
| Label2            | Exp2 |         |     | Bottom2      |           |       |         |
| Label3            | Exp3 |         |     | Bottom3      |           |       |         |
| TopLabelIpAddress |      |         |     | VlanId       |           |       |         |

|           |   |   |    |            |   |    |       |
|-----------|---|---|----|------------|---|----|-------|
| P01/0/0   |   | 0 | 24 | 6          | 0 | 0  | 19054 |
| P02/0/0   |   | 0 | 0  | 17.0.0.2   |   |    |       |
| 10.0.0.2  |   |   |    | 0          |   |    |       |
| 10.2.10.1 |   |   |    | 0          |   |    |       |
| 0.0.0.0   |   |   | 0  |            |   | in |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0.0.0.0   |   |   | 0  |            |   |    |       |
| P01/0/0   |   | 0 | 24 | 6          | 0 | 2  | 23569 |
| P02/0/0   |   | 3 | 0  | 17.0.0.2   |   |    |       |
| 25.10.0.2 |   |   |    | 0          |   |    |       |
| 10.2.10.1 |   |   |    | 0          |   |    |       |
| 0.0.0.0   |   |   | 0  |            |   | in |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0.0.0.0   |   |   | 0  |            |   |    |       |
| P01/0/0   |   | 0 | 24 | 6          | 0 | 2  | 23539 |
| P02/0/0   |   | 3 | 0  | 10.10.10.2 |   |    |       |
| 11.0.10.2 |   |   |    | 0          |   |    |       |
| 10.2.10.1 |   |   |    | 0          |   |    |       |
| 0.0.0.0   |   |   | 0  |            |   | in |       |
| 0         | 0 |   | 0  |            |   |    |       |
| 0         | 0 |   | 0  |            |   |    |       |

```
0 0 0
0.0.0.0 0 0
```

----结束

## 配置文件

- CE 的配置文件

```
#
sysname CE
#
interface Pos 1/0/0
ip address 192.168.1.2 255.255.255.0
#
return
```

- PE 的配置文件

```
#
sysname PE
#
ip netstream tcp-flag enable
#
interface gigabitethernet 2/0/0
ip address 192.168.2.1 255.255.255.0
#
interface Pos 1/0/0
ip address 192.168.1.1 255.255.255.0
ip netstream inbound
ip netstream outbound
#
slot 1
ip netstream sampler to slot 4
#
ip netstream sampler fix-packets 10000 inbound
ip netstream sampler fix-packets 10000 outbound
ip netstream export source 192.168.2.1
ip netstream export host 192.168.2.2 9001
#
return
```

## 7.7.2 配置 IPv4 网络 VLANIF 流量统计示例

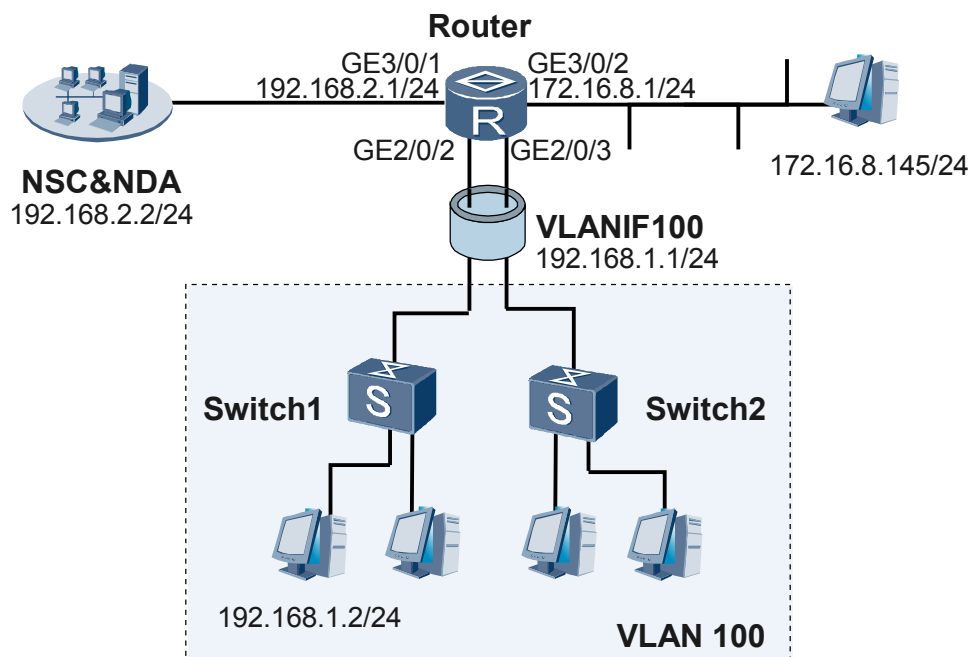
VLANIF 接口可以连通不同的 VLAN 间的流量。在 VLANIF 接口上使能 NetStream 功能，实现对 VLAN 间流量的监控。

## 组网需求

如图 7-5 所示，将路由器中 GE2/0/2 接口与 GE2/0/3 接口加入 VLANIF，并配置 VLANIF 的 NetStream 入统计功能。



图 7-5 配置 IPv4 网络 VLANIF 流量统计组网图



## 配置思路

配置 VLANIF 接口的 NetStream 统计功能的思路如下：

1. 配置 VLAN 及 VLANIF 的接口。
2. 配置各接口的 IP 地址。
3. 配置 NetStream 入统计功能。

## 数据准备

为完成此配置举例，需要准备如下数据：

- 配置接口的 IP 地址和子网掩码
- 输出目的主机地址和端口号
- NetStream 业务板的槽位号，本举例中 NetStream 业务板位于 4 号槽位。

## 操作步骤

**步骤 1** 在路由器上创建 VLAN 及 VLANIF 并配置各接口的地址

# 创建 ID 为 100 的 VLAN。

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
```

# 将接口 GE2/0/2 与 GE2/0/3 加入 VLAN 100。

```
[HUAWEI] interface gigabitethernet2/0/2
[HUAWEI-GigabitEthernet2/0/2] undo shutdown
[HUAWEI-GigabitEthernet2/0/2] portswitch
```

```
[HUAWEI-GigabitEthernet2/0/2] port default vlan 100
[HUAWEI-GigabitEthernet2/0/2] quit
[HUAWEI] interface gigabitethernet2/0/3
[HUAWEI-GigabitEthernet2/0/3] undo shutdown
[HUAWEI-GigabitEthernet2/0/3] portswitch
[HUAWEI-GigabitEthernet2/0/3] port default vlan 100
[HUAWEI-GigabitEthernet2/0/3] quit

创建 VLANIF 接口并配置 IP 地址。

[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 255.255.255.0
[HUAWEI-Vlanif100] quit

配置接口 GE3/0/1 与 GE3/0/2 的 IP 地址。

[HUAWEI] interface gigabitethernet3/0/1
[HUAWEI-GigabitEthernet3/0/1] ip address 192.168.2.1 255.255.255.0
[HUAWEI-GigabitEthernet3/0/1] undo shutdown
[HUAWEI-GigabitEthernet3/0/1] quit
[HUAWEI] interface gigabitethernet3/0/2
[HUAWEI-GigabitEthernet3/0/2] ip address 172.16.8.1 255.255.255.0
[HUAWEI-GigabitEthernet3/0/2] undo shutdown
[HUAWEI-GigabitEthernet3/0/2] quit
```

## 步骤 2 配置 VLANIF100 的 NetStream 统计功能

# 配置 SPUC 单板的 NetStream 业务处理方式为集中式。

```
<HUAWEI> set board-type slot 4 netstream
<HUAWEI> system-view
[HUAWEI] slot 2
[HUAWEI-slot-2] ip netstream sampler to slot 4
[HUAWEI-slot-2] return
```

# 配置 VLANIF100 的 NetStream 入统计功能。

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip netstream inbound
[HUAWEI-Vlanif100] quit
```

# 配置版本 5 输出格式的目的地址、目的端口和源地址。

```
[HUAWEI] ip netstream export host 192.168.2.2 9001
[HUAWEI] ip netstream export source 192.168.2.1
[HUAWEI] quit
```

# 配置 NetStream 采样。

```
[HUAWEI] ip netstream sampler fix-packets 10000 inbound
```

## 步骤 3 检查配置效果

# 配置成功后，在用户视图下 **display ip netstream cache origin slot 4**，NetStream 流缓存区的信息以及统计输出报文信息。

```
<HUAWEI> display ip netstream cache origin slot 4
Show information of IP and MPLS cache of slot 4 is starting.
get show cache user data success.
```

|          |         |      |     |              |     |           |         |
|----------|---------|------|-----|--------------|-----|-----------|---------|
| DstIf    |         | DstP | Msk | Pro          | Tos | Flags     | Packets |
| SrcIf    |         | SrcP | Msk |              |     | NextHop   |         |
| DstIP    |         |      |     |              |     | DstAs     |         |
| SrcIP    |         |      |     |              |     | SrcAs     |         |
| BGP: BGP | NextHop |      |     | TopLabelType |     | Direction |         |
| Label1   | Exp1    |      |     | Bottom1      |     |           |         |
| Label2   | Exp2    |      |     | Bottom2      |     |           |         |
| Label3   | Exp3    |      |     | Bottom3      |     |           |         |

| TopLabelIpAddress | VlanId |    |    |           |
|-------------------|--------|----|----|-----------|
| GI2/0/2           | 0      | 24 | 6  | 0 0 19054 |
| VL100             | 0      | 0  | 17 | 0.0.2     |
| 24.0.0.2          |        |    |    | 0         |
| 1.1.1.1           |        |    |    | 0         |
| 0.0.0.0           |        | 0  |    | in        |
| 0                 | 0      | 0  |    |           |
| 0                 | 0      | 0  |    |           |
| 0                 | 0      | 0  |    |           |
| 0.0.0.0           |        | 0  |    |           |

----结束

配置文件

HUAWEI 的配置文件。

```
#
 sysname HUAWEI
#
vlan batch 100
#
 ip netstream sampler fix-packets 10000 inbound
 ip netstream export source 192.168.2.1
 ip netstream export host 192.168.2.2 9001
#
interface Vlanif100
 ip address ip address 192.168.1.1 255.255.255.0
 ip netstream inbound
#
interface GigabitEthernet2/0/2
 undo shutdown
 portswitch
 port default vlan 100
#
interface GigabitEthernet2/0/3
 undo shutdown
 portswitch
 port default vlan 100
#
interface GigabitEthernet3/0/1
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet3/0/2
 undo shutdown
 ip address 192.16.8.1 255.255.255.0
#
 slot 2
 ip netstream sampler to slot 4
#
return
```

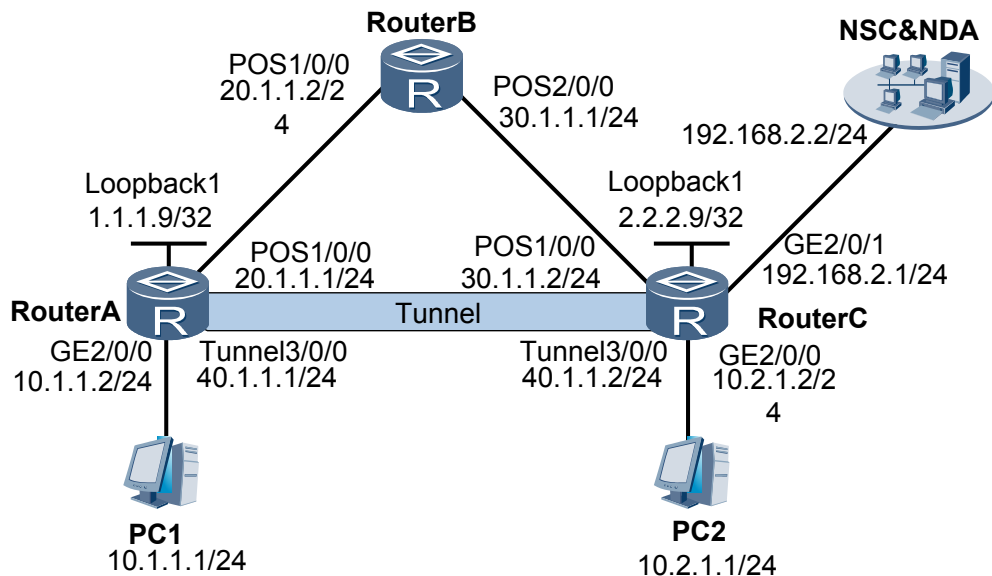
7.7.3 配置 IPv4 网络 GRE 流量统计示例

在 GRE 隧道接口上使能 NetStream 功能，实现对 GRE 隧道流量的监控。

组网需求

如图 7-6，在 IPv4 网络 GRE 隧道中，通过在 RouterC 节点部署 NetStream 入统计和出统计，对用户的流量进行监控。

图 7-6 配置 IPv4 网络 GRE 流量统计组网图



## 配置思路

采用如下的思路配置 IPv4 网络 GRE 流量统计：

1. 配置 GRE 静态路由的基本功能。
2. 配置骨干网设备 RouterC 的 NetStream 的入统计和出统计。

## 数据准备

为完成此配置例，需准备如下的数据：

- 运行 OSPF 所需数据
- 两端绑定 GRE 协议的 Loopback 接口
- GRE 隧道两端的源地址、目的地址、Tunnel 接口 IP 地址

## 操作步骤

### 步骤 1 配置各接口 IP 地址

按照图 7-6 配置各物理接口和 Loopback 接口的 IP 地址，并使用 **undo shutdown** 命令使各物理接口 Up，具体配置过程略。

### 步骤 2 配置 GRE 静态路由的基本功能

关于的 GRE 静态路由的基本功能的配置方法，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-VPN》中的“GRE 协议配置”。

### 步骤 3 配置 RouterC 接口 Tunnel3/0/0 的 NetStream 统计功能

# 配置 SPUC 单板的 NetStream 业务处理方式为集中式。

```
<RouterC> set board-type slot 4 netstream
<RouterC> system-view
```

```
[RouterC] slot 5
[RouterC-slot-5] ip netstream sampler to slot 4
[RouterC-slot-5] return

配置接口 Tunnel3/0/0 的 NetStream 入统计和出统计功能。

[RouterC] interface tunnel3/0/0
[RouterC-Tunnel3/0/0] ip netstream inbound
[RouterC-Tunnel3/0/0] ip netstream outbound
[RouterC-Tunnel3/0/0] quit

配置版本 5 输出目的地址，目的端口和源地址。

[RouterC] ip netstream export host 192.168.2.2 9001
[RouterC] ip netstream export source 192.168.2.1

配置 NetStream 采样，采样方式为固定报文采样。

[RouterC] ip netstream sampler fix-packets 10000 inbound
[RouterC] ip netstream sampler fix-packets 10000 outbound
```

步骤 4 检查配置效果

```
配置成功后，在用户视图下执行命令 display ip netstream cache origin slot 4，可以看到 NetStream 流缓存区的信息。

<RouterC> display ip netstream cache origin slot 4
Show information of IP-only cache of slot 4 is starting.
get show cache user data success.
```

| DstIf             |         | DstP | Msk | Pro          | Tos       | Flags | Packets |
|-------------------|---------|------|-----|--------------|-----------|-------|---------|
| SrcIf             |         | SrcP | Msk | NextHop      |           |       |         |
| DstIP             |         |      |     | DstAs        |           |       |         |
| SrcIP             |         |      |     | SrcAs        |           |       |         |
| BGP: BGP          | NextHop |      |     | TopLabelType | Direction |       |         |
| Label1            | Exp1    |      |     | Bottom1      |           |       |         |
| Label2            | Exp2    |      |     | Bottom2      |           |       |         |
| Label3            | Exp3    |      |     | Bottom3      |           |       |         |
| TopLabelIpAddress |         |      |     | VlanId       |           |       |         |

GI2/0/0

TL3/0/0

10.0.0.2

10.2.10.1

0.0.0.0

0

0

0

0.0.0.0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

TL3/0/0

GI2/0/0

10.2.10.1

10.0.0.2

0.0.0.0

0

0

0

0.0.0.0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

19054

17.0.0.2

0

0

in

19054

17.0.0.2

0

0

in

----结束

配置文件

- RouterA 的配置文件
- ```
#
```

```
sysname RouterA
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 20.1.1.1 255.255.255.0
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
target-board 5
binding tunnel gre
#
interface Tunnel3/0/0
undo shutdown
tunnel-protocol gre
ip address 40.1.1.1 255.255.255.0
source LoopBack1
destination 2.2.2.9
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
ip route-static 10.2.1.0 255.255.255.0 Tunnel3/0/0
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 20.1.1.2 255.255.255.0
#
interface Pos2/0/0
undo shutdown
link-protocol ppp
ip address 30.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.2.1.2 255.255.255.0
#
interface gigabitethernet 2/0/1
undo shutdown
ip address 192.168.2.1 255.255.255.0
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 30.1.1.2 255.255.255.0
#
```

```
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
target-board 5
binding tunnel gre
#
interface Tunnel3/0/0
undo shutdown
tunnel-protocol gre
ip address 40.1.1.2 255.255.255.0
source LoopBack1
destination 1.1.1.9
ip netstream inbound
#
ospf 1
area 0.0.0.0
network 30.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel3/0/0
#
slot 5
ip netstream sampler to slot 4
#
ip netstream sampler fix-packets 10000 inbound
ip netstream sampler fix-packets 10000 outbound
ip netstream export source 192.168.2.1
ip netstream export host 192.168.2.2 9001
#
return
```

7.7.4 配置 MPLS 网络的流量统计示例

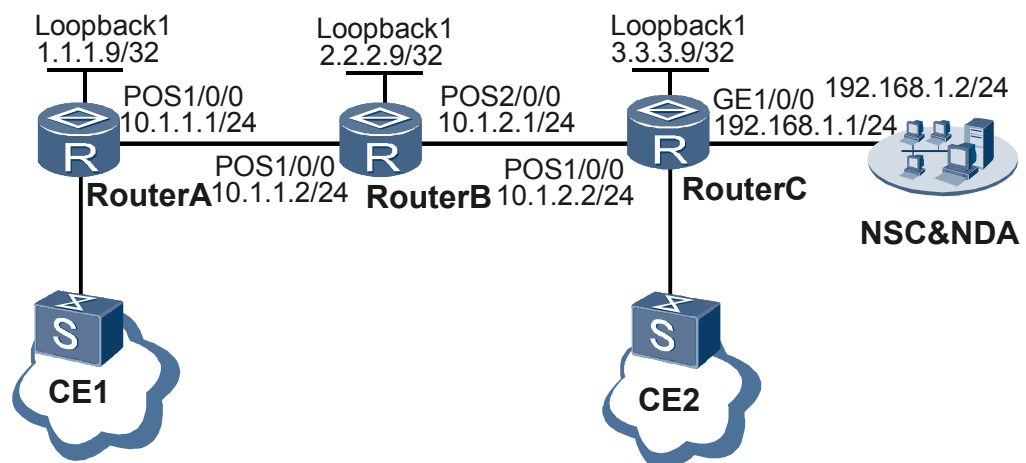
MPLS 流量是通过标签进行转发的。在 MPLS 网络中使能标签统计功能，可以获取 MPLS 报文的外三层标签信息。

组网需求

如图 7-7 所示，RouterA、RouterB 和 RouterC 均支持 MPLS，运行 OSPF 作为 MPLS 骨干网上的 IGP。

RouterA 和 RouterB、RouterB 和 RouterC 之间建立本地 LDP 会话；RouterA 和 RouterC 之间建立远端 LDP 会话。在 RouterA 部署 MPLS 流量的 NetStream 统计。

图 7-7 配置 MPLS 网络的流量统计组网图



配置思路

采用如下的思路配置 MPLS 网络的流量统计：

1. 配置各路由器之间的 LDP 会话。
2. 分别在建立远端会话的两端路由器上指定各自的远端对等体及其地址。
3. NetStream 信息输出的目的地址、目的端口、源地址。

数据准备

为完成此配置例，需准备如下的数据：

- 各路由器接口的 IP 地址如图 7-7，OSPF 进程号为 1，所在的区域为 Area0。
- RouterA 的远端对等体为 RouterC，其名称为 Routerc，IP 地址为 3.3.3.9。
- RouterC 的远端对等体为 RouterA，其名称为 Routera，IP 地址为 1.1.1.9。
- NetStream 业务板的槽位号，本举例中 Netstream 业务板位于 4 号槽位。

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 7-7 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置各路由器之间的 LDP 会话

配置 OSPF 协议发布各路由器接口所连网段和 LSR ID 的主机路由，使能路由器和接口的 MPLS 基本能力，使能 LDP。

关于的静态 MPLS TE 隧道的配置方法，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-MPLS》中的“MPLS 基本配置”。

步骤 3 使能 RouterB 接口 POS1/0/0 的 NetStream 统计功能

配置 SPUC 单板的 NetStream 采样处理方式。

```
<RouterB> set board-type slot 4 netstream
<RouterB> system-view
[RouterB] slot 1
[RouterB-slot-1] ip netstream sampler to slot 4
[RouterB-slot-1] return
```

配置 RouterB 接口 POS1/0/0 的 NetStream 入统计和出统计功能。

```
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] ip netstream inbound
[RouterB-Pos1/0/0] ip netstream outbound
[RouterB-Pos1/0/0] quit
```

配置对 MPLS 报文既采集内层 IP 报文也采集标签。

```
[RouterB] ip netstream mpls-aware label-and-ip
```

配置版本 5 输出目的地址，目的端口和源地址。

```
[RouterB] ip netstream export host 192.168.1.2 2100
[RouterB] ip netstream export source 10.1.2.1
```

配置 NetStream 采样，采样方式为固定报文采样。

```
[RouterB] ip netstream sampler fix-packets 10000 inbound
```



```
[RouterB] ip netstream sampler fix-packets 10000 outbound
```

步骤 4 检查配置效果

配置成功后，在用户视图下执行命令 **display ip netstream cache origin slot 4**，NetStream 流缓存区的信息以及统计输出报文信息。

```
<RouterB> display ip netstream cache origin slot 4
Show information of IP-only cache of slot 4 is starting.
get show cache user data success.
```

DstIf		DstP	Msk	Pro	Tos	Flags	Packets
SrcIf		SrcP	Msk	NextHop			
DstIP		DstAs					
SrcIP		SrcAs					
BGP: BGP NextHop		TopLabelType		Direction			
Label1	Exp1	Bottom1					
Label2	Exp2	Bottom2					
Label3	Exp3	Bottom3					
TopLabelIpAddress		VlanId					

P01/0/0		0	24	6	0	0	19054
P02/0/0		0	0	17.0.0.2			
10.0.0.2					0		
10.2.10.1					0		
0.0.0.0			0		in		
1024	3		1				
0	0		0				
0	0		0				
1.1.1.9			0				

----结束

配置文件

● RouterA 的配置文件

```
#
 sysname RouterA
#
 mpls lsr-id 1.1.1.9
 mpls
  lsp-trigger all
#
 mpls ldp
#
 mpls ldp remote-peer routerc
 remote-ip 3.3.3.9
#
 interface Pos1/0/0
  undo shutdown
  link-protocol ppp
  ip address 10.1.1.1 255.255.255.0
  mpls
  mpls ldp
#
 interface LoopBack1
  ip address 1.1.1.9 255.255.255.255
#
 ospf 1
  area 0.0.0.0
   network 10.1.1.0 0.0.0.255
   network 1.1.1.9 0.0.0.0
#
return
```

● RouterB 的配置文件

```

#
sysname RouterB
#
mpls lsr-id 2.2.2.9
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
  undo shutdown
  link-protocol ppp
  ip address 10.1.1.2 255.255.255.0
  mpls
  mpls ldp
  ip netstream inbound
  ip netstream outbound
#
interface Pos2/0/0
  undo shutdown
  link-protocol ppp
  ip address 20.1.1.1 255.255.255.0
  mpls
  mpls ldp
#
interface LoopBack1
  ip address 2.2.2.9 255.255.255.255
#
slot 1
  ip netstream sampler to slot 4
#
ip netstream sampler fix-packets 10000 inbound
ip netstream sampler fix-packets 10000 outbound
ip netstream export source 10.1.2.1
ip netstream export host 192.168.1.2 9001
#
ospf 1
  area 0.0.0.0
    network 10.1.1.0 0.0.0.255
    network 20.1.1.0 0.0.0.255
    network 2.2.2.9 0.0.0.0
#
return

```

● RouterC 的配置文件

```

#
sysname RouterC
#
ip netstream mpls-aware label-and-ip
#
mpls lsr-id 3.3.3.9
mpls
  lsp-trigger all
#
mpls ldp
#
mpls ldp remote-peer routera
remote-ip 1.1.1.9
#
interface Pos1/0/0
  undo shutdown
  link-protocol ppp
  ip address 20.1.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface LoopBack1
  ip address 3.3.3.9 255.255.255.255
#
ospf 1

```

```
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 3.3.3.9 0.0.0.0
#
return
```

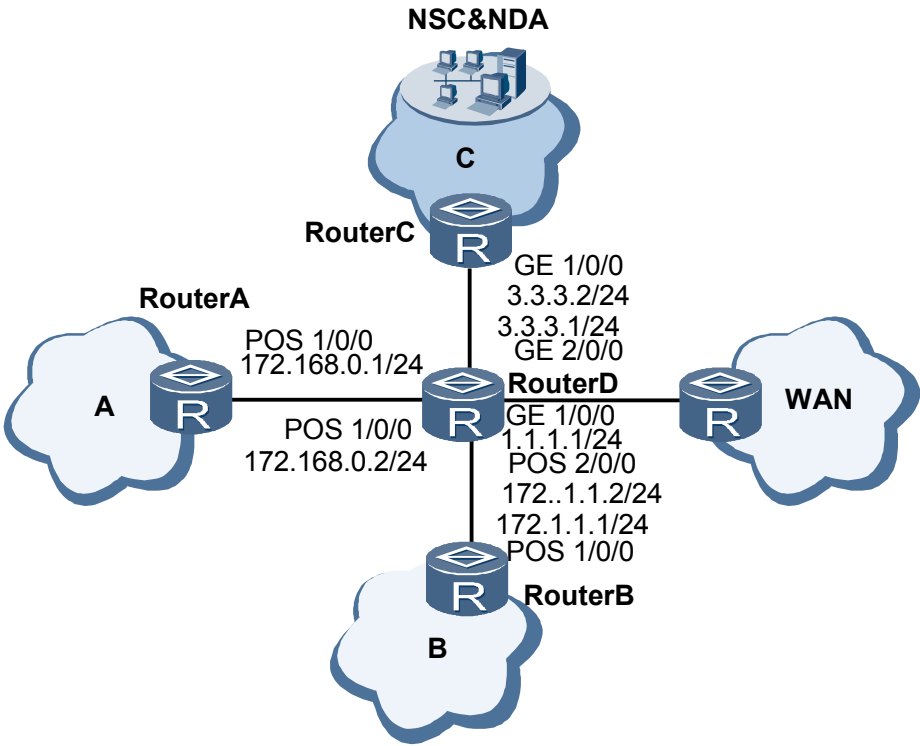
7.7.5 配置聚合流的流量统计示例

如果两个运营商需要统计经过各自 AS 域 的流量，实现流量的分账，可以在边界路由器上使能 NetStream 功能，并对原始流信息进行 AS 聚合处理。网管可分析出不同 AS 域的流量分布情况，实现流量分账的目的。

组网需求

如图 7-8 所示，网络 A 和网络 B 可以通过 RouterD 接入到 WAN（Wide Area Network）中，在 RouterD 中进行流量的采集，将采集聚合后发送到 NSC 中。

图 7-8 配置聚合流的流量统计组网图



配置思路

- 采用如下的思路完成配置聚合流的流量统计：
- 1. 配置局域网络中的出口路由器和 WAN 路由可达。
 - 2. 配置接入路由器和 NSC 路由可达。
 - 3. 配置接入路由器发送流量统计到指定的 NSC。

4. 配置接入路由器发送流量统计到 NSC 的入接口。
5. 配置流量的采样聚合功能，减少网管的数据流量。
6. 在接入路由器的入接口使能 NetStream 功能。

数据准备

为完成此配置例，需要准备如下数据：

- 接口的 IP 地址
- NSC 的地址
- 输出的版本信息
- NetStream 流量统计的采样比例
- NetStream 业务板的槽位号，本举例中 Netstream 业务板位于 4 号槽位。

操作步骤

步骤 1 配置各路由器的 IP 地址（略）

步骤 2 配置 RouterA、RouterB 和 WAN 路由可达

配置 RouterA 和 RouterD 路由可达

```
<RouterA> system-view
[RouterA] ip route-static 1.1.1.1 24 pos 1/0/0
```

配置 RouterB 和 RouterD 路由可达

```
<RouterB> system-view
[RouterB] ip route-static 1.1.1.1 24 pos 1/0/0
```

步骤 3 配置 RouterD 和 NSC 路由可达

配置 RouterD 和 RouterC 路由可达

```
<RouterD> system-view
[RouterD] ip route-static 2.2.2.1 24 3.3.3.2
```

步骤 4 在路由 RouterD 上使能 NetStream 功能

配置 SPUC 单板的 NetStream 采样处理方式为中心式。

```
<RouterD> set board-type slot 1 netstream
<RouterD> system-view
[RouterD] slot 1
[RouterD-slot-1] ip netstream sampler to slot 4
[RouterD-slot-1] return
```

使能 NetStream 出统计功能。

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ip netstream inbound
```

配置版本 9 聚合流的输出。

```
[RouterD] ip netstream aggregation prefix
[RouterD-aggregation-prefix] enable
[RouterD-aggregation-prefix] ip netstream export host 2.2.2.1 3000
[RouterD-aggregation-prefix] ip netstream export source 3.3.3.1
[RouterD-aggregation-prefix] export version 9
```

配置报文的采样功能。

```
[RouterD-GigabitEthernet1/0/0] ip netstream sampler fix-packets 1000 inbound
[RouterD-GigabitEthernet1/0/0] quit
```

步骤 5 验证配置结果

```
# 在路由器端查看是否有流的输出。

[RouterD] display ip netstream cache prefix slot 4
Show information of aggregation-prefix cache of slot 4 is starting.
get show cache user data success.
```

DstIf	DstAs	DstMsk	DstPre			
SrcIf	SrcAs	SrcMsk	SrcPre	Streams	Packets	Direction

GI1/0/0	0	24	24.0.0.0			
PO2/0/0	0	32	0	1	650	in

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
link-protocol ppp
ip address 172.168.0.1 255.255.0.0
#
ip route-static 1.1.1.1 255.255.0 POS1/0/0
#
return
```
- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
link-protocol ppp
ip address 172.1.1.1 255.255.0.0
#
ip route-static 1.1.1.1 255.255.0 POS1/0/0
#
return
```
- RouterC 的配置文件

```
#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
ip address 3.3.3.2 255.255.0.0
#
return
```
- RouterD 的配置文件

```
#
sysname RouterD
#
ip netstream aggregation prefix
enable
export version 9
ip netstream export source 3.3.3.1
ip netstream export host 2.2.2.1 3000
#
interface Pos1/0/0
```

```
link-protocol ppp
ip address 172.168.0.2 255.255.255.0
#
interface Pos1/0/1
link-protocol ppp
ip address 172.1.1.2 255.255.255.0
#
slot 2
ip netstream sampler to slot 4
#
interface GigabitEthernet2/0/0
ip address 1.1.1.1 255.255.255.0
ip netstream inbound
ip netstream sampler fix-packets 1000 inbound
#
interface GigabitEthernet2/0/1
ip address 3.3.3.1 255.255.255.0
#
return
```

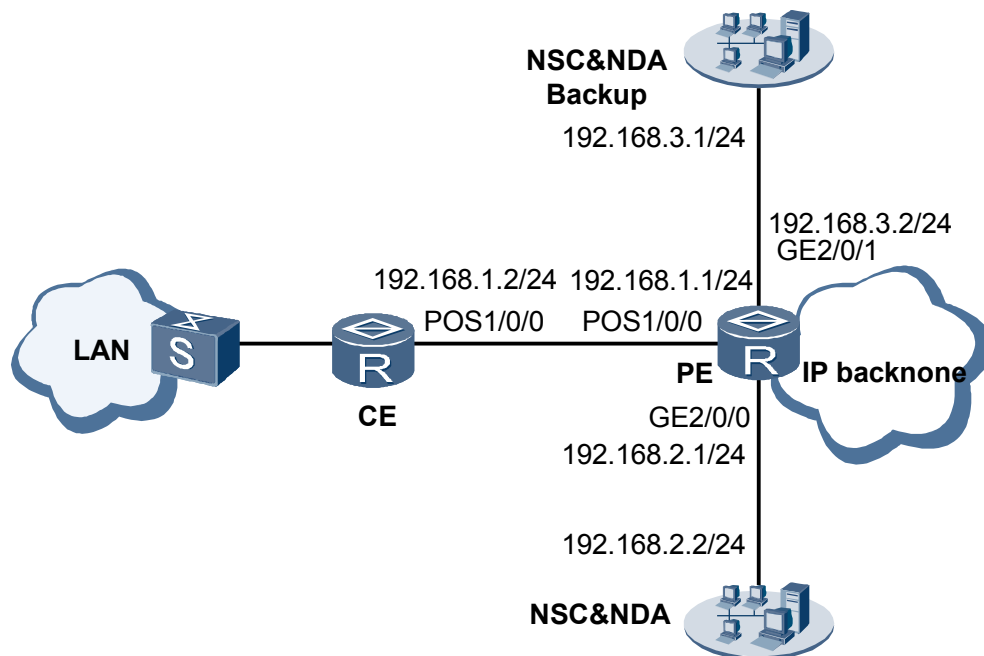
7.7.6 配置统计信息输出主机备份示例

向两台网管同时输出 NetStream 统计信息，实现统计信息的备份和异地分析。

组网需求

如图 7-9 所示，为了保证部署 NetStream 设备上的统计信息的完整性，将统计到的流量分担到两台服务器。实现两个 NSC 互为统计信息的备份。

图 7-9 配置统计信息输出双主机备份组网图



配置思路

采用如下的思路配置统计信息输出双主机备份：

1. 配置采样分析异常网络流量
2. 配置统计信息输出双主机备份

数据准备

为完成此配置例，需准备如下的数据：

- PE 路由器用户侧接口。
- NetStream 报文输出的版本号。
- NetStream 报文输出的目的地址、目的端口、源地址。
- NetStream 报文输出备份主机的目的地址、目的端口。
- NetStream 业务板的槽位号，本举例中 Netstream 业务板位于 4 号槽位。

操作步骤

步骤 1 配置 PE 与 CE 之间网络互通

具体配置过程请参见“[配置 IPv4 网络用户侧异常流量统计分析示例](#)”中的步骤 1。

步骤 2 配置 PE 用户侧接口 GE1/0/0 的 NetStream 统计功能

具体配置过程请参见“[配置 IPv4 网络用户侧异常流量统计分析示例](#)”中的步骤 2。

步骤 3 配置统计信息输出备份主机

配置版本 5 输出目的地址，目的端口。

```
[PE] ip netstream export host 192.168.3.1 9002
```

步骤 4 验证配置结果

在用户视图下，执行命令 **display ip netstream global**，可以看到 NetStream 统计输出报文的统计信息中有两个目的地址。

```
<PE> display ip netstream global
system
ip netstream sampler fix-packets 10000 inbound
ip netstream sampler fix-packets 10000 outbound
ip netstream export source 192.168.2.1
ip netstream export host 192.168.2.2 9001
ip netstream export host 192.168.3.1 9002
```

----结束

配置文件

● CE 的配置文件

```
#
sysname CE
#
interface Pos 1/0/0
link-protocol ppp
ip address 192.168.1.2 255.255.255.0
#
return
```

● PE 的配置文件

```
#
sysname PE
#
```

```
interface gigabitethernet 1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Pos 1/0/0
 ip address 192.168.1.1 255.255.255.0
 ip netstream inbound
 ip netstream outbound
#
slot 1
 ip netstream sampler to slot 4
#
ip netstream sampler fix-packets 10000 inbound
ip netstream sampler fix-packets 10000 outbound
ip netstream export source 192.168.2.1
ip netstream export host 192.168.2.2 9001
ip netstream export host 1192.168.3.1 9002
#
return
```

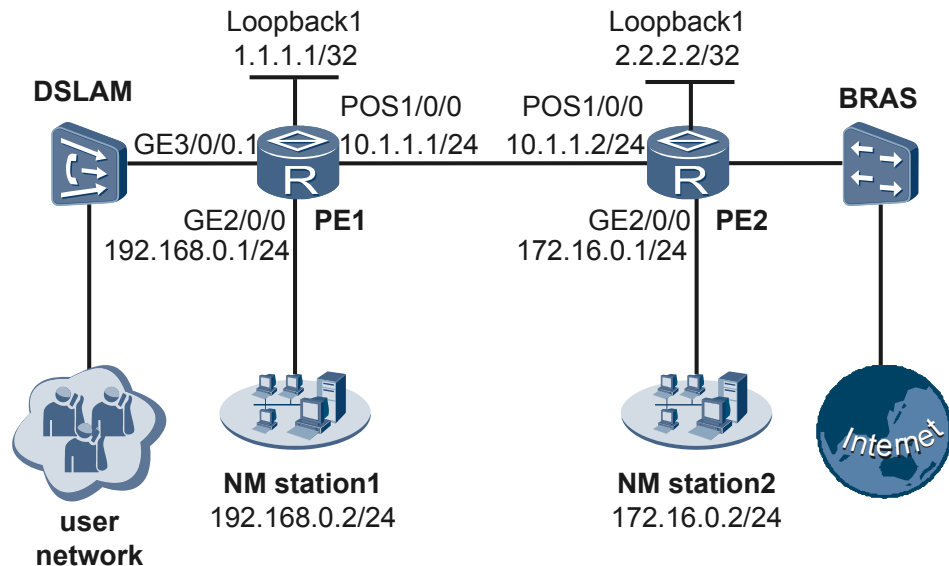
7.7.7 配置 VLAN 聚合流量统计示例

通过配置 VLAN 聚合流量统计，运营商的网管系统可以监控到接入运营商网络的不同用户的业务流量，为计费提供依据。

组网需求

如图 7-10 所示用户网络通过 DSLAM 设备接入到 Martini 方式的 VLL，VPN PE 端的子接口上部 NetStream VLAN 聚合的流量统计，运营商的网管系统可以监控到接入运营商网络的不同用户的业务流量，为计费提供依据。

图 7-10 配置 VLAN 聚合流量统计组网



配置思路

采用如下的思路配置 VLAN 聚合流量统计：

1. 配置 Martini 方式的 VLL

2. 使能接口的 NetStream 功能
3. 配置 NetStream 的采样比
4. 配置 NetStream 的采样模式
5. 配置 VLAN 聚合功能
6. 配置统计信息输出的源地址
7. 配置统计信息输出的目的地址和端口号

数据准备

完成该举例，需要准备如下数据：

- 采样比
- 统计信息输出的源地址
- 统计信息输出的目的地址和端口号

操作步骤

步骤 1 配置 Martini 方式的 VLL

关于 Martini 方式的 VLL 配置方法，请参见《HUAWEI NetEngine20E-X6 配置指南-VPN》中的“配置 Martini 方式 VLL”。

步骤 2 在 PE1 上配置 NetStream 功能

使能接口出入统计功能。

```
<PE1> system-view
[PE1] interface gigabitethernet 3/0/0.1
[PE1-GigabitEthernet3/0/0.1] ip netstream inbound
```

步骤 3 在 PE1 上配置 NetStream 的采样比

```
[PE1-GigabitEthernet3/0/0.1] ip netstream sampler fix-packets 100 inbound
[PE1-GigabitEthernet3/0/0.1] quit
```

步骤 4 在 PE1 上配置 NetStream 的采样模式

```
[PE1] slot 3
[PE1-slot-3] ip netstream sampler to slot self
[PE1-slot-3] quit
```

步骤 5 在 PE1 上配置 VLAN 聚合

```
[PE1] ip netstream aggregation vlan-id
[PE1-aggregation-vlanid] enable
```

步骤 6 在 PE1 上配置统计信息输出的源地址

```
[PE1-aggregation-vlanid] ip netstream export source 1.1.1.1
```

步骤 7 在 PE1 上配置统计信息输出的目的地址

```
[PE1-aggregation-vlanid] ip netstream export host 192.168.0.2 6000
[PE1-aggregation-vlanid] ip netstream export host 172.16.0.2 6000
[PE1-aggregation-vlanid] quit
```

步骤 8 验证配置效果

执行命令 **display netstream all** 查看所有视图下的 NetStream 配置信息。

```
[PE1] display netstream all
ip netstream aggregation vlan-id
enable
```

```

ip netstream export source 1.1.1.1
ip netstream export host 192.168.0.2 6000
ip netstream export host 172.16.0.2 6000
slot 3
GigabitEthernet3/0/0.1
ip netstream inbound
ip netstream sampler fix-packets 100 inbound
slot
slot 3:ip netstream sampler to slot self

```

执行命令 **display ip netstream cache vlan-id slot slot-id**, 查看 NetStream 流缓存区的信
息。

```

[PE1] display ip netstream cache vlan-id slot 3
Show information of aggregation-vlanid cache is starting.
get show cache user data success.
SrcIf          VlanId    Packets    Streams    Direction
-----

```

```

GI3/0/0.1      10        28443654   3276647    in

```

执行命令 **display ip netstream statistic slot slot-id**, 查看 NetStream 的统计信息。

```

[PE1] display ip netstream statistic slot 3
Netstream statistic information on slot 3:

```

length of packets	Number	Protocol	Number
1 ~ 64	: 0	IPV4	: 3052043
65 ~ 128	: 30000000	IPV6	: 0
129 ~ 256	: 1495697	MPLS	: 0
257 ~ 512	: 0	L2	: 28443654
513 ~ 1024	: 0	Total	: 31495697
1025 ~ 1500	: 0		
longer than 1500	: 0		

Aggregation	Current Streams Created Streams	Aged Streams Exported Packets	Exported Streams
origin	1 488	487 116	---
as	0	0	
as-tos	0	0	0
protport	0	0	0
protporttos	0	0	0
srcprefix	0	0	0
srcpretos	0	0	0
dstprefix	0	0	0
dstpretos	0	0	0
prefix	0	0	0
prefix-tos	0	0	0
mpls-label	0	0	0
vlan-id	0	0	0
all-aggre	3276649 23	210 0	0

```

Velocity Of Creating Streams (streams/second): 102

```

srcprefix = source-prefix, srcpretos = source-prefix-tos,
dstprefix = destination-prefix, dstpretos = destination-prefix-tos,
protoport = protocol-port, protoporttos = protocol-port-tos,
all-aggre = all aggregation streams,
"----" means that the current board is not supported.

----结束

配置文件

● PE1 的配置文件

```
#
 sysname PE1
#
 mpls lsr-id 1.1.1.1
 mpls
#
 mpls l2vpn
 mpls l2vpn default martini
#
 mpls ldp
#
 ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 1.1.1.1 0.0.0.0
#
 interface GigabitEthernet2/0/0
 undo shutdown
 ip address 192.168.0.1 255.255.255.0
#
 interface GigabitEthernet3/0/0
 undo shutdown
#
 interface GigabitEthernet3/0/0.1
 vlan-type dot1q 10
 mpls l2vc 2.2.2.2 10
 ip netstream inbound
 ip netstream sampler fix-packets 100 inbound
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
 interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
 ip netstream aggregation vlan-id
 enable
 ip netstream export source 1.1.1.1
 ip netstream export host 192.168.0.2 6000
 ip netstream export host 172.16.0.2 6000
#
 ip route-static 172.16.0.0 255.255.255.0 10.1.1.2
#
 slot 3
 ip netstream sampler to slot self
#
return
```

● PE2 的配置文件

```
#
#
 sysname PE2
#
```

```
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
mpls l2vpn default martini
#
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 172.16.0.1 255.255.255.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 10.1.1.0 0.0.0.255
#
return
```

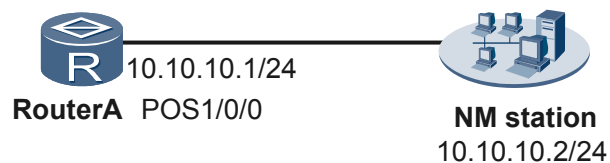
7.7.8 配置 NetStream 接口索引映射示例

通过配置 NetStream 接口索引输出为 32 位的接口索引，使网管直接根据输出的 32 位接口索引取得接口名称。

组网需求

如图 7-11 图所示，当用户部署 NetStream 业务时，采用 v9 格式输出采样报文时。通过配置 NetStream 接口索引输出为 32 位的接口索引，使网管直接根据输出的 32 位接口索引取得接口名称。

图 7-11 配置 NetStream 接口索引映射示例组网图



配置思路

采用如下的思路配置接口索引映射功能：

1. 配置路由器输出的 NetStream 报文目的地址为 10.10.10.2，并确保路由器与网管之间的链路可达。
2. 切换 NetStream 索引为 32 位。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 的管理 IP 地址为 10.10.10.1。
- NetStream 的索引值为 32 位。

操作步骤

步骤 1 配置原始流输出报文为版本 9。

```
<HUAWEI> system-view
[HUAWEI] ip netstream export version 9
```

步骤 2 配置聚合流输出报文为版本 9。

```
[HUAWEI] ip netstream aggregation as
[HUAWEI-aggregation-as] export version 9
[HUAWEI-aggregation-as] quit
[HUAWEI] ip netstream aggregation as-tos
[HUAWEI-aggregation-astos] export version 9
[HUAWEI-aggregation-astos] quit
[HUAWEI] ip netstream aggregation destination-prefix
[HUAWEI-aggregation-dstpre] export version 9
[HUAWEI-aggregation-dstpre] quit
[HUAWEI] destination-prefix-tos
[HUAWEI-aggregation-dstpretos] export version 9
[HUAWEI-aggregation-dstpretos] quit
[HUAWEI] ip netstream aggregation mpls-label
[HUAWEI-aggregation-mplslabel] export version 9
[HUAWEI-aggregation-mplslabel] quit
[HUAWEI] ip netstream aggregation prefix
[HUAWEI-aggregation-prefix] export version 9
[HUAWEI-aggregation-prefix] quit
[HUAWEI] ip netstream aggregation prefix-tos
[HUAWEI-aggregation-prefixtos] export version 9
[HUAWEI-aggregation-prefixtos] quit
[HUAWEI] ip netstream aggregation protocol-port
[HUAWEI-aggregation-protport] export version 9
[HUAWEI-aggregation-protport] quit
[HUAWEI] ip netstream aggregation protocol-port-tos
[HUAWEI-protporttos] export version 9
[HUAWEI-protporttos] quit
[HUAWEI] ip netstream aggregation source-prefix
[HUAWEI-aggregation-srcpre] export version 9
[HUAWEI-aggregation-srcpre] quit
[HUAWEI] ip netstream aggregation source-prefix-tos
[HUAWEI-aggregation-srcpretos] export version 9
[HUAWEI-aggregation-srcpretos] quit
```

步骤 3 配置输出报文的接口索引为 32 位

```
[HUAWEI] ip netstream export index-switch 32
```

步骤 4 验证配置结果

查看配置后的当前的 NetStream 索引。

```
<HUAWEI> display netstream global

ip netstream export version 9
ip netstream export index-switch 32
ip netstream mpls-aware label-and-ip
ip netstream aggregation as
enable
export version 9
ip netstream aggregation as-tos
export version 9
```

```
ip netstream aggregation destination-prefix
enable
export version 9
ip netstream aggregation destination-prefix-tos
enable
export version 9
ip netstream aggregation mpls-label
enable
ip netstream aggregation prefix
enable
export version 9
ip netstream aggregation prefix-tos
export version 9
ip netstream aggregation protocol-port
enable
export version 9
ip netstream aggregation protocol-port-tos
enable
export version 9
ip netstream aggregation source-prefix
enable
export version 9
ip netstream aggregation source-prefix-tos
enable
export version 9
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname HUAWEI

#
interface POS1/0/0
undo shutdown
ip address 10.10.10.1 255.255.255.0
#
ip netstream export version 9
#
ip netstream aggregation as
enable
export version 9
#
ip netstream aggregation as-tos
enable
export version 9
#
ip netstream aggregation destination-prefix
enable
export version 9
#
ip netstream aggregation destination-prefix-tos
enable
export version 9
#
ip netstream aggregation mpls-label
enable
#
ip netstream aggregation prefix
enable
export version 9
#
ip netstream aggregation prefix-tos
enable
export version 9
#
```

```
ip netstream aggregation protocol-port
enable
export version 9
#
ip netstream aggregation protocol-port-tos
enable
export version 9
#
ip netstream aggregation source-prefix
enable
export version 9
#
ip netstream aggregation source-prefix-tos
enable
export version 9
#
ip netstream export index-switch 32
#
return
```

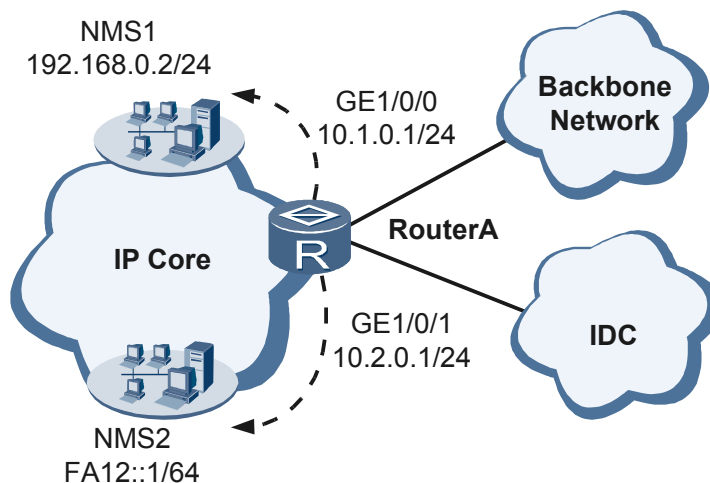
7.7.9 配置 NetStream 的多地址输出

配置 NetStream 多址后，不同接口的统计信息，可以根据不同的输出方向进行输出。

组网需求

如图 7-12 所示，路由器 RouterA 的 GE1/0/0 接口和 GE1/0/1 接口分别连接骨干网络和 IDC（Information Data Centre）。在 RouterA 的 GE1/0/0 接口和 GE1/0/1 的入方向分别部署 NetStream，从 GE1/0/0 采集到流量信息输出到 IPv4 网管 NMS1，从 GE1/0/1 采集到的流量信息输出到 IPv6 网管 NMS2。

图 7-12 配置 NetStream 的多地址输出组网



配置思路

采用如下的思路配置 NetStream 的多地址输出：

1. 使能接口的 NetStream 功能
2. 配置 NetStream 的采样比

3. 配置 NetStream 的采样模式
4. 配置 NetStream 的多地址输出

数据准备

完成该举例，需要准备如下数据：

- 采样比
- 统计信息输出的目的地址和端口号

操作步骤

步骤 1 在 RouterA 上配置 NetStream 功能

使能接口出入统计功能。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip netstream inbound
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip netstream inbound
```

步骤 2 在 RouterA 上配置 NetStream 的采样比

```
[RouterA-GigabitEthernet1/0/1] ip netstream sampler fix-packets 100 inbound
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip netstream sampler fix-packets 100 inbound
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 3 在 RouterA 上配置 NetStream 的采样模式

```
[RouterA] slot3
[RouterA-slot-3] ip netstream sampler to slot self
[RouterA-slot-3] quit
```

步骤 4 配置 NetStream 的多地址输出

```
[RouterA] ip netstream monitor monitor1
[RouterA-monitor-monitor1] ip netstream export host 192.168.0.2 6000
[RouterA-monitor-monitor1] quit
[RouterA] ip netstream monitor monitor2
[RouterA-monitor-monitor2] ip netstream export host ipv6 FA12::1 6000
[RouterA-monitor-monitor2] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip netstream monitor monitor1 inbound
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip netstream monitor monitor2 inbound
[RouterA-GigabitEthernet1/0/1] quit
```

步骤 5 验证配置效果

执行命令 **display ip netstream monitor all** 查看所有的监控业务信息。

```
[RouterA] display ip netstream monitor all
Monitor monitora
ID          : 1
AppCount    : 1
First address : 192.168.0.2
First port   : 6000
Second address : 0.0.0.0
Second port  : 0
Monitor monitorb
ID          : 2
AppCount    : 1
```


First address : FA12::1
First port : 6000
Second address : 0.0.0.0
Second port : 0

执行命令 **display ip netstream statistics**，查看 NetStream 的统计信息。

[RouterA] **display ip netstream statistics slot 3**
Netstream statistic information on slot 3:

length of packets		Number	Protocol	Number
1	~	64 : 0	IPV4	: 3052043
65	~	128 : 30000000	IPV6	: 0
129	~	256 : 1495697	MPLS	: 0
257	~	512 : 0	L2	: 28443654
513	~	1024 : 0	Total	: 31495697
1025	~	1500 : 0		
longer than 1500		: 0		

Aggregation	Current Streams Created Streams	Aged Streams Exported Packets	Exported Streams
origin	1 488	487 116	---
as	0	0	
	0	0	0
as-tos	0	0	
	0	0	0
protport	0	0	
	0	0	0
protporttos	0	0	
	0	0	0
srcprefix	0	0	
	0	0	0
srcpretos	0	0	
	0	0	0
dstprefix	0	0	
	0	0	0
dstpretos	0	0	
	0	0	0
prefix	0	0	
	0	0	0
prefix-tos	0	0	
	0	0	0
mpls-label	0	0	
	0	0	0
vlan-id	0	0	
	0	0	0
all-aggre	3276649	210	
	23	0	0

Velocity Of Creating Streams (streams/second): 102

srcprefix = source-prefix, srcpretos = source-prefix-tos,
dstprefix = destination-prefix, dstpretos = destination-prefix-tos,
protport = protocol-port, protporttos = protocol-port-tos,
all-aggre = all aggregation streams,
"---" means that the current board is not supported.

----结束

任务示例

RouterA 的配置文件

```
#  
sysname RouterA
```

```
#
ip netstream monitor monitor1
ip netstream export host 192.168.0.1 6000
#
ip netstream monitor monitor2
ip netstream export host ipv6 FA12::1 6000
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/0
ip netstream inbound
ip netstream sampler fix-packets 100 inbound
ip netstream monitor monitor1 inbound
#
interface GigabitEthernet1/0/1
ip netstream inbound
ip netstream sampler fix-packets 100 inbound
ip netstream monitor monitor2 inbound
#
ip route-static 192.168.0.0 255.255.255.0 10.1.0.2
#
slot 3
ip netstream sampler to slot self
#
return
```

8 Ping 和 Tracert

关于本章

通过 Ping 和 Tracert 可以检测网络的连通性。

8.1 ping 和 tracert 简介

通过 Ping 和 Tracert 用户可以了解到 Ping 和 Tracert 的基本原理和 NE20E-X6 系统对 Ping 和 Tracert 特性的支持情况。

8.2 配置 ping 和 tracert 检测网络

通过 ping 和 tracert 可以检测到网络的连通情况。

8.3 使用 Ping 和 Trace 检测 LDP LSP

通过 Ping 和 Trace 检测 LDP LSP 的连通性。

8.4 使用 Ping 和 Tracert 检测 TE Tunnel

通过 Ping 和 Trace 检测 TE Tunnel 中节点之间的连通性。

8.5 使用 Ping 和 Tracert 检测 VLL 网络

通过 Ping 和 Trace 检测 VLL 网络中 PE 节点之间的连通性。

8.6 使用 Ping 和 Tracert 检测 PWE3 网络

用户通过 ping 和 Tracert 检查 PWE3 网络中 PW 的连通性。

8.7 使用 Ping 和 Tracert 检测 VPLS 网络

用户通过 ping 和 Tracert 检查 VPLS 网络中的连通性。

8.8 使用 Ping 和 Tracert 检测 BGP/MPLS IP VPN 网络

使用 Ping 检测 BGP/MPLS IP VPN 网络的连通性。

8.9 使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络

使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络。

8.10 使用 Ping 和 Tracert 检测 TE Tunnel 叶子节点故障

在 P2MP TE Tunnel 网络中，用户通过 Ping 和 Tracert 实现 P2MP 所有叶子节点或单条叶子节点的检测。

8.11 使用 Ping 检测 MPLS 网络

在 MPLS 网络中可通过指定头节点强制走 IP 转发，可以实现 MPLS 网络故障和 IP 网络故障区分。

8.12 使用 Ping 检测 Trunk 链路

用户可以使用 Ping 命令检测 Trunk 成员链路。

8.13 使用 Ping 和 Trace 检测多跳 PW

用户可以使用 Ping 和 Trace 检测 MH-PW。

8.14 使用 Service Ping 检测 PWE3 网络

使用 Service Ping 检测 PWE3 网络，可以在本端得到远端的 PWE3 配置信息，确认本端和远端的配置是否一致。

8.15 使用 Service Ping 检测 VLL 接入 VPLS 网络

用户通过 Service Ping 检测 VLL 接入 VPLS 网络，可以在本端得到远端的 PW 配置信息，确认本端和远端的配置是否一致。

8.16 配置智能 ping 检测网络

通过智能 ping 可以方便地检测到网络的连通情况，省去繁琐的参数设置过程。

8.1 ping 和 tracert 简介

通过 Ping 和 Tracert 用户可以了解到 Ping 和 Tracert 的基本原理和 NE20E-X6 系统对 Ping 和 Tracert 特性的支持情况。

8.1.1 ping 和 tracert

当设备出现故障时，可以首先使用 Ping 与 Tracert 命令测试网络连接是否正常工作。

8.1.1 ping 和 tracert

当设备出现故障时，可以首先使用 Ping 与 Tracert 命令测试网络连接是否正常工作。

ping 命令主要用于检查网络连接及主机是否可达。

tracert 命令用于测试数据包从发送主机到目的地所经过的网关，它主要检查网络连接是否可达，以及分析网络什么地方发生了故障。

tracert 的执行过程如下：

1. 首先发送一个 TTL 为 1 的数据包。
2. 到达第一跳时 TTL 超时，第一跳路由器发回一个 ICMP 错误消息，指明此数据包不能被发送。
3. 发送主机将 TTL 加 1，重新发送此数据包。
4. 第二跳路由器返回 TTL 超时。

以上步骤循环进行，直到到达目的地。这样，发送主机就能够记录每一个 ICMP TTL 超时消息的源地址，得到 IP 数据包到达目的地所经历的路径。

8.2 配置 ping 和 tracert 检测网络

通过 ping 和 tracert 可以检测到网络的连通情况。

8.2.1 建立配置任务

在配置 ping 和 tracert 检测网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.2.2 使用 ping 检测网络连接是否正常

使用 Ping 检测网络中两个节点之间的连通性。

8.2.3 使用 tracert 检测网络发生故障的位置

使用 Tracert 检测网络中各个节点之间的连通性。

8.2.1 建立配置任务

在配置 ping 和 tracert 检测网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

客户端无法正常上网，需要使用 **ping** 和 **tracert** 检测网络连接是否正常。

前置任务

在配置 Ping 和 Tracert 测试之前，需完成以下任务：

- 客户端的网络连接线连接正确。
- 客户端正确配置了 IP 地址。

数据准备

在配置 ping 和 tracert 检测网络之前，需要准备以下数据。

序号	数据
1	客户端的 IP 地址。
2	网关的 IP 地址。

8.2.2 使用 ping 检测网络连接是否正常

使用 Ping 检测网络中两个节点之间的连通性。

背景信息

在客户端进行如下的配置。

操作步骤

步骤 1 执行命令 **ping** [ip] [-a source-ip-address | -c count | -d | -f | -h ttl-value | -i interface-type interface-number [source] } | -m time | -n | -name | -p pattern | -q | -r | -s packetsize | -t timeout | -tos tos-value | -v | -vpn-instance vpn-instance-name] * host，测试网络连接是否正常。

以上 **ping** 命令只列出了部分参数，各参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时后仍没有收到响应报文，则输出“Request time out”，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

 说明

如果 **ping** 的目的地址是广播地址，则回应报文中的源地址是广播地址。

```
<HUAWEI> ping 202.38.160.244
PING 202.20.36.25: 56 data bytes, press CTRL_C to break
  Reply from 202.20.36.25: bytes=56 Sequence=1 ttl=255 time=2 ms
  Reply from 202.20.36.25: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 202.20.36.25: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 202.20.36.25: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 202.20.36.25: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 202.20.36.25 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

----结束

8.2.3 使用 tracert 检测网络发生故障的位置

使用 Tracert 检测网络中各个节点之间的连通性。

背景信息

在客户端进行如下的配置。下列操作可在所有视图下进行。当使用 **tracert** 命令检查网络连接是否可达时，可以使用 **icmp time-exceed** 命令指定 ICMP Time Exceeded 报文的格式。

操作步骤

步骤 1 （可选）执行命令 **icmp time-exceed { extension { compliant | non-compliant } | classic }**，指定 ICMP Time Exceeded 报文的格式。

步骤 2 执行命令 **tracert [-a source-ip-address | -f first-ttl | -m max-ttl | -p port | -q nqueries | -v | -vpn-instance vpn-instance-name | -w timeout] * host**，测试故障发生的位置。

以上 **tracert** 命令只列出了部分参数，该命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

下面是应用 **tracert** 分析网络情况的例子。

```
<HUAWEI> tracert -m 10 35.1.1.48
traceroute to 35.1.1.48 (35.1.1.48), max hops: 10 ,packet length: 40
 1  128.3.112.1      19 ms      19 ms      0 ms
 2  128.32.216.1     39 ms      39 ms      19 ms
 3  128.32.136.23    39 ms      40 ms      39 ms
 4  128.32.168.22    39 ms      39 ms      39 ms
 5  128.32.197.4     40 ms      59 ms      59 ms
 6  131.119.2.5      59 ms      59 ms      59 ms
 7  129.140.70.13    99 ms      99 ms      80 ms
 8  129.140.71.6     139 ms     239 ms     319 ms
 9  129.140.81.7     220 ms     199 ms     199 ms
10  35.1.1.48        239 ms     239 ms     239 ms
```

从上面结果可以看出从源主机到目的地都经过了哪些网关。

----结束

8.3 使用 Ping 和 Trace 检测 LDP LSP

通过 Ping 和 Trace 检测 LDP LSP 的连通性。

8.3.1 建立配置任务

在配置使用 Ping 和 Trace 检测 LDP LSP 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.3.2 使用 Ping 检测 LDP LSP

使用 ping 检测 LSP 中的各个 LSR 之间的连通性。

8.3.3 使用 Tracert 检测 LDP LSP 连通性

使用 tracert 检测 LSP 中的各个 LSR 之间的连通性。

8.3.1 建立配置任务

在配置使用 Ping 和 Trace 检测 LDP LSP 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

根据用户指定的 FEC、掩码，在 Ingress 上使用 **ping lsp** 或 **tracert lsp** 命令，可以检测到目的 Egress 的 LDP LSP 的连通性。如果 Ingress 上配置了负载分担，需要指定下一跳地址来检测指定 LDP LSP 的连通性。

前置任务

在使用 Ping 和 Trace 检测 LDP LSP 前，需完成以下任务：

- 正确配置 LDP LSP

数据准备

在使用 Ping 和 Trace 检测 LDP LSP 之前，需要准备以下数据。

序号	数据
1	LDP LSP 的目的 IPv4 地址和掩码长度
2	（可选）发送 Echo 请求报文的源 IPv4 地址、发送 Echo 请求报文的数目、发送的 Echo 请求报文的 EXP 值、发送的 Echo 请求报文的 TTL 值、应答模式、发送的净荷报文长度、等待 Echo 应答的超时时间

8.3.2 使用 Ping 检测 LDP LSP

使用 ping 检测 LSP 中的各个 LSR 之间的连通性。

背景信息

在需要检测连通性的 LSP 沿途节点上执行如下操作。

操作步骤

步骤 1 执行命令 **ping lsp** [**-a** source-ip | **-c** count | **-exp** exp-value | **-h** ttl-value | **-m** interval | **-r** reply-mode | **-s** packet-size | **-t** time-out | **-v**] * **ip** destination-address mask-length [ip-address] [**nexthop** nexthop-address | **draft6**]，测试 LDP LSP 链路是否连通。

以上 **ping** 命令各选项及参数意义请参见 HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。

- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping lsp -v ip 3.3.3.3 32
LSP PING FEC: IPV4 PREFIX 3.3.3.3/32 : 100 data bytes, press CTRL_C to break
  Reply from 3.3.3.3: bytes=100 Sequence=1 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=2 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=3 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=4 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=5 time = 5 ms Return Code 3, Subcode 1
--- FEC: IPV4 PREFIX 3.3.3.3/32 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/5 ms
```

----结束

8.3.3 使用 Tracert 检测 LDP LSP 连通性

使用 tracert 检测 LSP 中的各个 LSR 之间的连通性。

背景信息

在需要检测连通性的 LSP 沿途节点上执行如下操作。

操作步骤

- 步骤 1** 执行命令 **tracert lsp** **[-a source-ip | -exp exp-value | -h ttl-value | -r reply-mode | -t time-out] * ip destination-address mask-length [ip-address] [nexthop nexthop-address] [draft6]**，定位 LDP LSP 故障发生的位置。

以上 **tracert lsp** 命令各选项及参数意义请参见 HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

```
<HUAWEI> tracert lsp ip 3.3.3.3 32 nexthop 66.1.1.2
TTL  Replier      Time    Type    Downstream
0                Ingress  66.1.1.2/[17 ]
1    66.1.1.2      230 ms  Transit 88.1.1.1/[3 ]
2    3.3.3.3       80 ms   Egress
```

从上述结果中可以看出，从源主机到指定目的 IP 地址经过的 LSP 节点以及到每一跳的响应时间。

----结束

8.4 使用 Ping 和 Tracert 检测 TE Tunnel

通过 Ping 和 Trace 检测 TE Tunnel 中节点之间的连通性。

8.4.1 建立配置任务

在使用 Ping 和 Trace 检测 TE Tunnel 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.4.2 使用 Ping 检测 TE Tunnel 连通性

通过 Ping 方式检测 TE Tunnel 链路的连通性。

8.4.3 使用 Trace 检测 TE Tunnel 连通性

通过 Tracert 方式检测 TE Tunnel 链路的连通性。

8.4.1 建立配置任务

在使用 Ping 和 Trace 检测 TE Tunnel 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

通过 Ping/Tracert 方式检测 TE Tunnel 链路的连通性。通过在 Ingress 上发起到 Egress 的 Ping/Tracert LSP 命令，检测 TE Tunnel 的连通性。如果 Tunnel 配置了 hot-standby LSP，可以通过命令行指定，检测该 hot-standby LSP 的连通性。

前置任务

在使用 Ping 和 Trace 检测 TE Tunnel 前，需完成以下任务：

- 正确配置 TE Tunnel

数据准备

在使用 Ping 和 Trace 检测 TE Tunnel 之前，需要准备以下数据。

序号	数据
1	TE Tunnel 的接口编号
2	(可选) 发送 echo 请求报文的源 IPv4 地址、发送 echo 请求报文的数目、发送的 echo 请求报文的 EXP 值、发送的 echo 请求报文的 TTL 值、应答模式、发送的净荷报文长度、等待 echo 应答的超时时间

8.4.2 使用 Ping 检测 TE Tunnel 连通性

通过 Ping 方式检测 TE Tunnel 链路的连通性。

背景信息

在需要检测连通性的 TE Tunnel 沿途节点上执行如下操作。

操作步骤

- 步骤 1** 执行命令 **ping lsp** `[ -a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v ] * te tunnel tunnel-number [ hot-standby ] [ draft6 ]`，检测 TE tunnel 沿途节点的连通性。

以上 **ping** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。

- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping lsp te tunnel 1/0/0
LSP PING FEC: RSVP IPV4 SESSION QUERY Tunnel1/0/0 : 100 data bytes, press CTRL_C to break
  Reply from 20.1.1.2: bytes=100 Sequence=0 time = 50 ms
  Reply from 40.1.1.2: bytes=100 Sequence=1 time = 28 ms
  Reply from 20.1.1.2: bytes=100 Sequence=2 time = 33 ms
  Reply from 40.1.1.2: bytes=100 Sequence=3 time = 52 ms
  Reply from 20.1.1.2: bytes=100 Sequence=4 time = 8 ms

--- FEC: RSVP IPV4 SESSION QUERY Tunnel1/0/0 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 8/34/52 ms
```

----结束

8.4.3 使用 Trace 检测 TE Tunnel 连通性

通过 Tracert 方式检测 TE Tunnel 链路的连通性。

背景信息

在需要检测连通性的 TE Tunnel 沿途节点上执行如下操作。

操作步骤

- 步骤 1** 执行命令 **tracert lsp** [**-a** source-ip | **-exp** exp-value | **-h** ttl-value | **-r** reply-mode | **-t** time-out] * **te tunnel** tunnel-number [[**hot-standby**]] [**draft6**] [**multipoint** [**leaf-destination** ip-address]]，查看数据包从 TE tunnel 入节点到出节点所经过的网关，定位故障发生的位置。

以上 **tracert** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

```
<HUAWEI> tracert lsp te tunnel 1/0/0
LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to break.
  TTL   Replier          Time    Type    Downstream
  0
  1     10.1.2.2          63 ms   Ingress 10.1.2.2/[13312 ]
  2     6.6.6.6           93 ms   Egress
```

从上述结果中可以看出，从源主机到指定目的 IP 地址经过的 LSP 节点以及到每一跳的响应时间。

----结束

8.5 使用 Ping 和 Tracert 检测 VLL 网络

通过 Ping 和 Trace 检测 VLL 网络中 PE 节点之间的连通性。

8.5.1 建立配置任务

在使用 Ping 和 Trace 检测 VLL 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.5.2 使用 Ping 检测 VLL 网络连通性

通过 Ping 检测 VLL 网络中 PE 节点之间的连通性。

8.5.3 使用 Tracert 检测 VLL 网络连通性

通过 Tracert 检测 VLL 网络中 PE 节点之间的连通性。

8.5.1 建立配置任务

在使用 Ping 和 Trace 检测 VLL 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在 Kompella VLL 组网中，用户可以通过 **ping** 命令检查 PW 的连通性。

同时，可以通过 **tracert** 命令获取网络中数据包从发送端到目的端所经过的 PE 和 P 设备的信息，从而检查二层转发链路的连通性并分析定位网络故障。

前置任务

在使用 Ping 和 Tracert 检测 VLL 网络前，需完成以下任务：

- 正确配置 VLL 网络

数据准备

在使用 Ping 和 Tracert 检测 VLL 网络之前，需要准备以下数据。

序号	数据
1	本端 PW 的类型和 PW ID。
2	（可选）远端 PW ID、发送 Echo 请求报文的数目、发送 Echo 请求报文的时间间隔、发送 Echo 请求报文的字节数、发送 Echo 请求报文超时的时间值

8.5.2 使用 Ping 检测 VLL 网络连通性

通过 Ping 检测 VLL 网络中 PE 节点之间的连通性。

背景信息

在需要检测连通性的 Kompella 方式 VLL 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据组网需求，执行如下命令检测 VLL 网络的连通性：

- 使用 label-alert 通道：**ping vc vpn-instance** *vpn-name* *local-ce-id* *remote-ce-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-v**] * **label-alert**
- 使用 control-word 通道：**ping vc vpn-instance** *vpn-name* *local-ce-id* *remote-ce-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-v**] * **control-word**

使用 **ping vc vpn-instance** 命令检测 VLL 网络之前，必须确保：

- 正确配置 Kompella 方式 VLL 网络

- 配置 PW 模板，并在 PW 模板视图中进行如下配置：
 - 使用控制字通道：使用 **control-word** 命令使能控制字功能。
 - 使用 MPLS Router Alert 通道：使用 **control-word** 命令使能控制字功能。

以上 **ping vc vpn-instance** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

命令执行结果输出包括：

- 对每一个 ping 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping vc ethernet 100 control-word remote 100
Reply: bytes=100 Sequence=1 time = 11 ms
Reply: bytes=100 Sequence=2 time = 4 ms
Reply: bytes=100 Sequence=3 time = 4 ms
Reply: bytes=100 Sequence=4 time = 4 ms
Reply: bytes=100 Sequence=5 time = 4 ms

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 4/5/11 ms
```

----结束

8.5.3 使用 Tracert 检测 VLL 网络连通性

通过 Tracert 检测 VLL 网络中 PE 节点之间的连通性。

背景信息

在需要定位故障的 Kompella 方式 VLL 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据组网环境，执行如下命令定位 VLL 网络故障：

- 使用 control-word 通道：**tracert vc - vpn-instance** *vpn-name local-ce-id remote-ce-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**full-lsp-path**] [**draft6**]
- 使用 label-alert 通道：**tracert vc - vpn-instance** *vpn-name local-ce-id remote-ce-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**full-lsp-path**] [**draft6**]
- 使用普通模式：**tracert vc** *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**remote** *remote-ip-address*] } [**full-lsp-path**] [**draft6**]

使用 **tracert vc - vpn-instance** 命令检测 VLL 网络之前，必须确保：

- 正确配置 Kompella 方式 VLL 网络
- 配置 PW 模板，使能 VCCV-PING 功能。在 PW 模板视图中进行如下配置：
 - 使用控制字通道：先使用 **control-word** 命令使能控制字功能。

- 使用 MPLS Router Alert 通道：使用 **control-word** 命令使能控制字功能。
- 普通模式：使用 **control-word** 命令使能控制字功能。

控制字通道和普通模式不能同时配置使用。

以上 **tracert vc - vpn-instance** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

```
<HUAWEI> tracert vc ppp 100 control-word remote 200 full-lsp-path
TTL   Replier           Time    Type      Downstream
0                               Ingress  20.1.1.2/[17409 3 ]
1    20.1.1.2          110 ms  Transit  30.1.1.2/[17408 3 11264 ]
2    30.1.1.2           50 ms  Transit  40.1.1.1/[3 ]
3    4.4.4.4            50 ms  Egress
```

从上述结果中可以看出，PW 路径上的每个节点以及到每一个节点的响应时间。

----结束

8.6 使用 Ping 和 Tracert 检测 PWE3 网络

用户通过 ping 和 Tracert 检查 PWE3 网络中 PW 的连通性。

8.6.1 建立配置任务

在使用 Ping 和 Trace 检测 PWE3 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.6.2 使用 Ping 检测 PWE3 网络连通性

用户通过 ping 命令检查 PWE3 网络中 PW 的连通性。

8.6.3 使用 Tracert 检测 PWE3 网络连通性

用户通过 tracert 命令获取网络中数据包从发送端到目的端所经过的 SPE 和 P 设备的信息，检查 PW 的连通性并定位网络故障节点。

8.6.1 建立配置任务

在使用 Ping 和 Trace 检测 PWE3 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

- PWE3 组网环境中，用户通过 **ping** 命令检查 PWE3 网络中 PW 的连通性。接收端 PE 收到 Echo 请求报文后，会提取 FEC 信息，发送到 L2VPN 层面，判断是否到达了 Egress 节点。如果是会返回 Echo 应答报文。
 - PW 必须配置 PW 模板才能使能 VCCV-PING。
 - 可以使用 control-word 或 label-alert 两种检测方式。
 - 如果用户指定通过应用平面的控制通道发送 Echo 应答报文，PW 通道必须使能 label-alert 能力。
 - 对于多跳 PW，如果通过 label-alert 方式检测，则在 SPE 节点也会将 Echo 请求报文上送到 L2VPN 层面。此时 L2VPN 判断不是 Egress 节点后，会继续转发。不会返回 Echo 应答报文。
- PWE3 组网环境中，用户通过 **tracert** 命令获取网络中数据包从发送端到目的端所经过的 SPE 和 P 设备的信息，检查 PW 的连通性并定位网络故障节点。
发送的 Echo 请求报文的 TTL 值依次递增 1。中间节点接收到 Echo 请求报文后，判断出 TTL 超时，将携带当前节点的下一跳信息返回 Echo 应答。Tracert 操作终止的

条件有两个：一是到达 Egress 节点。二是到达 TTL 上限值。与 Ping 不同的是，tracert 增加了 normal 检测方式。normal 方式和 control-word 方式不能同时配置使用。

前置任务

在使用 Ping 和 Tracert 检测 PWE3 网络前，需完成以下任务：

- 正确配置 PWE3 网络。

数据准备

在使用 Ping 和 Trace 检测 PWE3 网络之前，需要准备以下数据。

序号	数据
1	本地 PW 的类型和 PW ID。
2	(可选) 远端 PW ID、发送 echo request 报文的数目、发送下一个报文的等待时间、发送 echo request 报文的字节数、发送 echo request 报文超时的时间值、

8.6.2 使用 Ping 检测 PWE3 网络连通性

用户通过 ping 命令检查 PWE3 网络中 PW 的连通性。

背景信息

在 PWE3 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据需要，执行如下命令检测 PWE3 网络的连通性：

- 使用 control-word 通道：

```
ping vc pw-type pw-id [ -c echo-number | -m time-value | -s data-bytes | -t timeout-value | -v ] * control-word [ remote peer-pw-id ] [ draft6 ]
```

- 使用 label-alert 通道：

```
ping vc pw-type pw-id [ -c echo-number | -m time-value | -s data-bytes | -t timeout-value | -v ] * label-alert [ remote remote-ip-address ] [ draft6 ]
```

使用 ping vc 命令检测 PWE3 网络之前，必须确保：

- 正确配置 PWE3 网络
- 配置 PW 模板，使能 VCCV-PING。并在 PW 模板视图中进行如下配置：
 - 使用控制字通道：先使用 control-word 命令使能控制字功能。
 - 使用 MPLS Router Alert 通道：使用 control-word 命令使能控制字功能。

以上 ping vc 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

命令执行结果输出包括：

- 对每一个 ping 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping vc ethernet 100 control-word remote 100
Reply: bytes=100 Sequence=1 time = 11 ms
      Reply: bytes=100 Sequence=2 time = 4 ms
      Reply: bytes=100 Sequence=3 time = 4 ms
      Reply: bytes=100 Sequence=4 time = 4 ms
      Reply: bytes=100 Sequence=5 time = 4 ms

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics---
      5 packet(s) transmitted
      5 packet(s) received
      0.00% packet loss
      round-trip min/avg/max = 4/5/11 ms
```

----结束

8.6.3 使用 Tracert 检测 PWE3 网络连通性

用户通过 **tracert** 命令获取网络中数据包从发送端到目的端所经过的 SPE 和 P 设备的信息，检查 PW 的连通性并定位网络故障节点。

背景信息

在 PWE3 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据组网环境，执行如下命令定位 PWE3 网络故障：

- 使用 control-word 通道：
tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**remote** *remote-pw-id*] } [**full-lsp-path**] [**draft6**]
- 使用 label-alert 通道：
tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**remote** *remote-ip-address*] } [**full-lsp-path**] [**draft6**]
- 使用普通模式：
tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**remote** *remote-ip-address*] } [**full-lsp-path**] [**draft6**]

使用 **tracert vc** 命令检测 PWE3 网络之前，必须确保：

- 正确配置方式 PWE3 网络
- 配置 PW 模板，使能 VCCV-PING。并在 PW 模板视图进行如下配置：
 - 使用控制字通道：先使用 **control-word** 命令使能控制字功能。
 - 使用 MPLS Router Alert 通道：使用 **control-word** 命令使能控制字功能。
 - 普通模式：使用 **control-word** 命令使能控制字功能。

控制字通道和普通模式不能同时配置使用。

以上 **tracert vc** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。


```
<HUAWEI> tracert vc ppp 100 control-word remote 200 full-lsp-path
TTL   Replier           Time    Type      Downstream
0
1     20.1.1.2          110 ms  Transit   30.1.1.2/[17408 3 11264 ]
2     30.1.1.2          50 ms   Transit   40.1.1.1/[3 ]
3     4.4.4.4           50 ms   Egress
```

从上述结果中可以看出，PW 路径上的每个节点以及到每一个节点的响应时间。

----结束

8.7 使用 Ping 和 Tracert 检测 VPLS 网络

用户通过 ping 和 Tracert 检查 VPLS 网络中的连通性。

8.7.1 建立配置任务

在使用 Ping 和 Trace 检测 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.7.2 使用 Ping 检测 VPLS 网络连通性

Ping 支持跨域方式 VPLS。

8.7.3 使用 Tracert 检测 VPLS 网络连通性

Tracert 不支持跨域方式 VPLS。

8.7.1 建立配置任务

在使用 Ping 和 Trace 检测 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

可以使用 ping 和 tracert 命令检测 VPLS 网络的连通性。

使用这两条命令只支持检测单跳 PW。在 HVPLS 网络，ping 或 tracert 操作在第一跳终结。如果命令行指定了 PW ID，则检测指定 PW。如果没有指定 PW ID，则使用 VSI ID 进行检测。

Ping 支持跨域方式 VPLS，Tracert 不支持跨域方式 VPLS。

前置任务

在使用 Ping 和 Tracert 检测 VPLS 网络前，需完成以下任务：

- 正确配置 VPLS 网络

数据准备

在使用 Ping 和 Trace 检测 VPLS 网络之前，需要准备以下数据。

序号	数据
1	（可选）Martini 方式：VSI 名称、远端 PE 地址、本端 PW 的 ID
2	Kompella 方式：VSI 名称、本地 CE ID、远端 CE ID

序号	数据
3	(可选) 发送 Echo 请求报文的数目、发送 Echo 请求报文的间隔时间、发送 Echo 请求报文的字节数、发送 Echo 请求报文超时的时间值、对端回送 MPLS Echo 应答报文的模式、发送的 Echo 请求的 EXP 值

8.7.2 使用 Ping 检测 VPLS 网络连通性

Ping 支持跨域方式 VPLS。

背景信息

在 VPLS 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据组网方式，执行如下命令检测 VPLS 网络的连通性：

- Kompella 方式：**ping vpls** [-c echo-number | -m time-value | -s data-bytes | -t timeout-value | -r reply-mode | -exp exp-value | -v] * vsi vsi-name local-site-id remote-site-id
- Martini 方式：**ping vpls** [-c echo-number | -m time-value | -s data-bytes | -t timeout-value | -r reply-mode | -exp exp-value | -v] * vsi vsi-name peer peer-address [negotiate-vc-id vc-id]

以上 **ping** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping vpls -c 10 -m 10 -s 65 -t 100 -v vsi test 10 10
Reply: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
Reply: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
10 packet(s) transmitted
10 packet(s) received
0.00% packet loss
round-trip min/avg/max = 15/21/32 ms
```

----结束

8.7.3 使用 Tracert 检测 VPLS 网络连通性

Tracert 不支持跨域方式 VPLS。

背景信息

在 VPLS 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 根据组网方式，执行如下命令定位 VPLS 网络故障：

- Kompella 方式：**tracert vpls** [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **vsi** *vsi-name* *local-site-id* *remote-site-id* [**full-lsp-path**]
- Martini 方式：**tracert vpls** [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

以上 **tracert** 命令各选项及参数意义请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

```
<HUAWEI> tracert vpls vsi test 10 10 full-lsp-path
TTL   Replier           Time   Type      Downstream
0                               Ingress 20.1.1.2/[17409 3 ]
1    20.1.1.2         110 ms Transit 30.1.1.2/[17408 3 11264 ]
2    30.1.1.2         50 ms  Transit 40.1.1.1/[3 ]
3    4.4.4.4          50 ms  Egress
```

从上述结果中可以看出，PW 路径上的每个节点以及到每一个节点的响应时间。

----结束

8.8 使用 Ping 和 Tracert 检测 BGP/MPLS IP VPN 网络

使用 Ping 检测 BGP/MPLS IP VPN 网络的连通性。

8.8.1 建立配置任务

在使用 Ping 检测 BGP/MPLS IP VPN 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.8.2 使用 Ping 检测 BGP/MPLS IP VPN 网络的连通性

在 PE 上使用 **ping lsp** 命令 Ping 对端 PE，可以检测 MPLS IP VPN 网络 LSP 隧道的连通性。

8.8.1 建立配置任务

在使用 Ping 检测 BGP/MPLS IP VPN 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

正确配置 VPN 网络后，在 PE 上使用 **ping lsp** 命令 Ping 对端 PE，可以检测 MPLS IP VPN 网络 LSP 隧道的连通性。

其中的公网隧道可能是：

- 等价负载分担 LDP LSP 链路
- TE 隧道
- VPN FRR 的备用隧道

私网路由均为叠代公网隧道路由而出。

如果 Ping 的是 CE 地址并且 CE 和 PE 之间链路故障，可以 Ping 通，因为实质检测的是 PE 到 PE 的端到端链路。

前置任务

在使用 Ping 检测 BGP/MPLS IP VPN 网络前，需完成以下任务：

- 正确配置 BGP/MPLS IP VPN 网络

数据准备

在使用 Ping 检测 BGP/MPLS IP VPN 网络之前，需要准备以下数据。

序号	数据
1	VPN 实例名称、远端 PE IP 地址
2	（可选）发送 Echo 请求报文的源 IPv4 地址、发送 Echo 请求报文的数目、发送的 Echo 请求报文的 EXP 值、发送的 Echo 请求报文的 TTL 值、应答模式、发送的净荷报文长度、等待 Echo 应答的超时时间

8.8.2 使用 Ping 检测 BGP/MPLS IP VPN 网络的连通性

在 PE 上使用 ping lsp 命令 Ping 对端 PE，可以检测 MPLS IP VPN 网络 LSP 隧道的连通性。

背景信息

在 BGP/MPLS IP VPN 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 执行命令 **ping lsp** [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * vpn-instance vpn-name remote remote-address mask-length，检测 BGP/MPLS IP VPN 网络的连通性：

以上 **ping** 命令各选项及参数意义请参见《NE20E-X6 命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping lsp -v vpn-instance test remote 3.3.3.3 32
LSP PING FEC: IPV4 PREFIX 3.3.3.3/32 : 100 data bytes, press CTRL_C to break
Reply from 3.3.3.3: bytes=100 Sequence=1 time = 4 ms Return Code 3, Subcode 1
```

```
Reply from 3.3.3.3: bytes=100 Sequence=2 time = 4 ms Return Code 3, Subcode 1
Reply from 3.3.3.3: bytes=100 Sequence=3 time = 4 ms Return Code 3, Subcode 1
Reply from 3.3.3.3: bytes=100 Sequence=4 time = 4 ms Return Code 3, Subcode 1
Reply from 3.3.3.3: bytes=100 Sequence=5 time = 5 ms Return Code 3, Subcode 1
--- FEC: IPV4 PREFIX 3.3.3.3/32 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 4/4/5 ms
```

----结束

8.9 使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络

使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络。

8.9.1 建立配置任务

使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.9.2 使用 MAC Ping 检测 VPLS 网络连通性

使用 VPLS MAC Ping 检测 VPLS 网络。

8.9.3 使用 MAC Trace 检测 VPLS 网络连通性

使用 VPLS MAC Trace 检测 VPLS 网络。

8.9.1 建立配置任务

使用 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

完成 VPLS 网络配置后，可以通过 NQA 对 VPLS 网络进行 MAC VSI Ping 测试或 MAC VSI Trace 测试，检测 VPLS 网络中二层转发链路的连通性。

通过 VPLS MAC Ping 可以检测 VPLS 网络是否存在到目的 MAC 的可达 VPLS 路径，但是并不能确定报文转发所经过的真实路径。如果网络存在故障，可以使用 VPLS MAC Trace 功能来定位现故障的具体位置。

前置任务

- 正确配置 VPLS 网络。

数据准备

在配置 VPLS MAC Ping 和 VPLS MAC Trace 检测 VPLS 网络之前，需要准备以下数据。

序号	数据
1	VSI Name、MAC 地址
2	(可选) VLAN ID

序号	数据
3	(可选) 对于 VPLS MAC Ping: 发送请求报文次数、请求报文的等待时间、请求报文的报文大小、等待应答报文的超时时间、报文优先级、回复模式
4	(可选) 对于 VPLS MAC Trace: 请求报文的报文大小、等待应答报文的超时时间、报文优先级、初始 TTL、最大 TTL、回复模式

8.9.2 使用 MAC Ping 检测 VPLS 网络连通性

使用 VPLS MAC Ping 检测 VPLS 网络。

背景信息

在需要检测连通性的 VPLS 网络 PE 设备上执行如下操作。

操作步骤

步骤 1 执行命令 **ping vpls mac** *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id*] [**-c** *count* | **-m** *time-value* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *tll*]*, 测试 VPLS 网络连接是否正常。

以上 **ping** 命令各选项及参数意义请参见《命令参考》。

命令执行结果输出包括:

- 对每一个 **ping** 报文的响应情况, 如果超时到仍没有收到响应报文, 则输出 “Request time out”, 否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。
- 最后的统计信息,

```
<HUAWEI> ping vpls mac 00e0-5952-6f01 vsi v123
Ping mac 00e0-5952-6f01 vsi v123 : 100 data bytes , press CTRL_C to break
  Reply from 10.1.1.1 : bytes=100 sequence=1 time = 1ms
  Reply from 10.1.1.1 : bytes=100 sequence=2 time = 1ms
  Reply from 10.1.1.1 : bytes=100 sequence=3 time = 2ms
  Reply from 10.1.1.1 : bytes=100 sequence=4 time = 3ms
  Reply from 10.1.1.1 : bytes=100 sequence=5 time = 2ms
The IP address of the PE is 5.5.5.9 and the interface on the PE is GigabitEthernet5/0/0.100.
--- vsi : v123 00e0-5952-6f01 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/2/3 ms
```

----结束

8.9.3 使用 MAC Trace 检测 VPLS 网络连通性

使用 VPLS MAC Trace 检测 VPLS 网络。

背景信息

在需要检测连通性的 VPLS 网络 PE 设备上执行如下操作。

操作步骤

步骤 1 执行命令 **trace vpls mac** *mac-address vsi vsi-name [vlan vlan-id] [-t timeout | -f first-ttl | -m max-ttl | -exp exp | -r replymode] **，测试 VPLS 网络故障发生的位置。

以上 **trace** 命令各选项及参数意义请参见《命令参考》。

命令执行结果输出包括：

```
<HUAWEI> trace vpls mac 00e0-5952-6f01 vsi v123
```

从上述结果中可以看出，从源主机到指定 VSI 的 MAC 地址，经过了哪些网关，到每一跳的响应时间。

----结束

8.10 使用 Ping 和 Tracert 检测 TE Tunnel 叶子节点故障

在 P2MP TE Tunnel 网络中，用户通过 Ping 和 Tracert 实现 P2MP 所有叶子节点或单条叶子节点的检测。

8.10.1 建立配置任务

在使用 Ping 和 Trace 检测 P2MP 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.10.2 使用 Ping 检测 TE Tunnel 叶子节点故障

Ping 支持 P2MP 网络连通性检测。

8.10.3 使用 Tracert 检测 TE Tunnel 叶子节点故障

Tracert 支持 P2MP 网络故障节点检测。

8.10.1 建立配置任务

在使用 Ping 和 Trace 检测 P2MP 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

当前 IPTV 业务倍受运营商关注，即将成为运营商业务的主要增长点，基于 RSVP-TE 建立的 P2MP 隧道能够天然满足上述需求。当组播业务承载于 MPLS P2MP 业务之上时，网络会融合组播和 MPLS 的优势。同时，对于部署 IP/MPLS 的骨干网，能够统一组播业务和单播业务的转发平面，更有利于用户对网络的部署和升级。

在 P2MP TE Tunnel 存在的情况下：

- 在 Ingress 节点上发起到 Tunnel 隧道叶子 Egress 节点的 Ping/Tracert，实现 P2MP 所有叶子节点的检测。
- 通过指定叶子节点的 leaf-destination，实现 P2MP 单条叶子节点的检测。

前置任务

在使用 Ping 和 Tracert 检测 P2MP 网络前，需完成以下任务：

- 骨干网各设备配置 IP 地址和 IGP 路由，使各设备能够互通
- PE 上使能 MPLS 基本能力和 MPLS RSVP，建立 RSVP-LSP 隧道

- P2MP 隧道 Tunnel 已建立并且 UP

数据准备

在使用 Ping 和 Tracert 检测 P2MP 网络之前，需要准备以下数据。

序号	数据
1	P2MP 隧道 Tunnel 名称、叶子 LSP 的目的地址

8.10.2 使用 Ping 检测 TE Tunnel 叶子节点故障

Ping 支持 P2MP 网络连通性检测。

背景信息



说明

若 P2MP tunnel 隧道比较复杂，叶子节点比较多，Ping 整条隧道会引起同一时间隧道报文流量比较大，任务比较繁忙。

操作步骤

步骤 1 根据检测需求，执行如下命令检测 P2MP 网络的连通性：

- 对 P2MP 网络单个叶子节点进行检测：**ping lsp** [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * **te tunnel tunnel-number** [[**hot-standby** | **draft6**] | **multipoint leaf-destination ip-address**]
- 对 P2MP 网络所有叶子节点进行检测：**ping lsp** [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * **te tunnel tunnel-number** [[**hot-standby** | **draft6**] | **multipoint**]

以上 **ping** 命令各选项及参数意义请参见《NE20E-X6 命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出“request timeout”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping lsp -c 2 te Tunnel 1/0/0 multipoint
```

```
LSP PING FEC: RSVP IPV4 SESSION QUERY Tunnel1/0/0 : 100 data bytes, press CTRL_C to break
```

```
Reply from 20.1.1.1: bytes=100 Sequence=0 time = 50 ms
```

```
Reply from 20.1.1.2: bytes=100 Sequence=0 time = 28 ms
```

```
Reply from 20.1.1.3: request timeout
```

```
Reply from 20.1.1.1: bytes=100 Sequence=1 time = 50 ms
```

```
Reply from 20.1.1.2: bytes=100 Sequence=1 time = 28 ms
```

```
Reply from 20.1.1.3: request timeout
```

```
--- Egress: 20.1.1.1 ping statistics ---
```

```
2 packet(s) transmitted
```

```
2 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 8/34/52 ms
```

```
--- Egress: 20.1.1.2 ping statistics ---
```



```
2 packet(s) transmitted
2 packet(s) received
0.00% packet loss
round-trip min/avg/max = 8/34/52 ms

--- Egress: 20.1.1.3 ping statistics ---
2 packet(s) transmitted
0 packet(s) received
100.00% packet loss
round-trip min/avg/max = 0/0/0 ms
```

----结束

8.10.3 使用 Tracert 检测 TE Tunnel 叶子节点故障

Tracert 支持 P2MP 网络故障节点检测。

背景信息



说明

若 P2MP tunnel 隧道比较复杂，叶子节点比较多，Tracert 整条隧道会引起同一时间报文流量比较大，任务比较繁忙。

操作步骤

步骤 1 根据组网方式，执行如下命令定位 P2MP 网络故障：

- 对 P2MP 网络单个叶子节点进行检测：**tracert lsp** [**-a source-ip** | **-exp exp-value** | **-h ttl-value** | **-r reply-mode** | **-t time-out**] * **te tunnel tunnel-number** [[**hot-standby**] [**draft6**] [**multipoint leaf-destination ip-address**]]
- 对 P2MP 网络所有叶子节点进行检测：**tracert lsp** [**-a source-ip** | **-exp exp-value** | **-h ttl-value** | **-r reply-mode** | **-t time-out**] * **te tunnel tunnel-number** [[**hot-standby**] [**draft6**] [**multipoint**]]

以上 **tracert** 命令各选项及参数意义请参见《NE20E-X6 命令参考》。

```
<HUAWEI> tracert lsp te Tunnel1/0/0 multipoint
LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to break.
TTL   Replier      Time    Type    Downstream
0
1      2.1.1.1         63 ms   Transit  2.1.1.1/[11];2.2.1.1/[13]
1      2.2.1.1         23 ms   Transit  3.1.1.1/[22];3.1.2.1/[3]
2      3.1.1.1         43 ms   Transit  3.2.1.1/[12];3.2.2.1/[3]
2      3.1.2.1         43 ms   Egress
2      3.2.1.1         23 ms   Transit  4.2.1.1/[3];4.2.1.2/[3]
2      3.2.2.1         33 ms   Egress
3      4.1.1.1         43 ms   Egress
3      4.1.1.2         43 ms   Egress
3      4.2.1.1         13 ms   Egress
3      4.2.1.2         53 ms   Egress
```

从上述结果中可以看出，LSP 路径上的每个节点以及到每一个节点的响应时间。

----结束

8.11 使用 Ping 检测 MPLS 网络

在 MPLS 网络中可通过指定头节点强制走 IP 转发，可以实现 MPLS 网络故障和 IP 网络故障区分。

8.11.1 建立配置任务

在使用 Ping 检测 MPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.11.2 使用 Ping 检测 MPLS 网络 IP 转发是否正常

Ping 支持 MPLS 网络的 IP 转发检测。

8.11.1 建立配置任务

在使用 Ping 检测 MPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

传统的 Ping 命令用于检测 IP 网络，Ping LSP 命令用于检测 MPLS 网络。然而对于使能了 MPLS 的网络，无论 Ping 还是 Ping LSP 都是根据 TunnelID 进行转发，即使 MPLS 转发失败也不会采取 IP 转发。所以当 MPLS 链路出现问题时，用户无法准确判断出故障出现在 IP 网络还是 MPLS 网络。

针对上述场景，可以指定 **ip-forwarding** 选项强制 Ping 检测报文通过 IP 转发，定位故障是否属于 IP 网络。

前置任务

在使用 Ping 和 Tracert 检测 MPLS 网络前，需完成以下任务：

- 各设备配置 IP 地址和 IGP 路由

数据准备

在使用 Ping 和 Tracert 检测 MPLS 网络之前，需要准备以下数据。

序号	数据
1	目的地址 IP 地址

8.11.2 使用 Ping 检测 MPLS 网络 IP 转发是否正常

Ping 支持 MPLS 网络的 IP 转发检测。

操作步骤

步骤 1 对 MPLS 网络进行 IP 转发检测：**ping** [ip] [-a source-ip-address | -c count | -d | -f | -h ttl-value | -i interface-type interface-number [source] | -m time | -n | -name | -p pattern | -q | -r | -s packet-size | -system-time | -t timeout | -tos tos-value | -v | -vpn-instance vpn-instance-name] * host **ip-forwarding**

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。

- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping 10.1.1.2 ip-forwarding
PING 10.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=170 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
--- 18.18.18.18 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/66/170 ms
```

----结束

8.12 使用 Ping 检测 Trunk 链路

用户可以使用 Ping 命令检测 Trunk 成员链路。

8.12.1 建立配置任务

在使用 Ping 检测 Trunk 成员链路前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.12.2 使用 Ping 检测三层 Trunk 成员接口连通性

Ping 支持 Trunk 成员链路检测。

8.12.1 建立配置任务

在使用 Ping 检测 Trunk 成员链路前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

Trunk 链路的每一个成员端口都具有独立的传输路径，承载业务的相应时延、抖动、丢包率等可能不相同。当 Trunk 链路承载的业务质量大幅下降的时候，可以先执行 **trunk member-port-inspect** 命令使能成员接口检测功能，然后再通过 **ping** 命令测试成员端口的网络连接是否正常。

前置任务

在使用 Ping 检测 Trunk 成员链路前，需完成以下任务：

- 配置 IP 地址和 IGP 路由，使各设备能够互通

数据准备

在使用 Ping 检测 Trunk 成员链路之前，需要准备以下数据。

序号	数据
1	对端 IP 地址、本端出接口

8.12.2 使用 Ping 检测三层 Trunk 成员接口连通性

Ping 支持 Trunk 成员链路检测。

背景信息

必须在本端设备执行 **trunk member-port-inspect** 命令使能 Trunk 成员接口检测功能，才可以使用 Ping 命令进行成员链路检测。

说明

执行 **trunk member-port-inspect** 命令会对设备上所有三层 Trunk 接口生效，所以在检测结束后需要及时去使能，避免耗费系统资源。

操作步骤

步骤 1 对 MPLS 网络进行三层 Trunk 成员接口连通性检测：**ping [ip] [-a source-ip-address | -c count | -d | -f | -h ttl-value | -i interface-type interface-number [source] | -m time | -n | -name | -p pattern | -q | -r | -s packetsize | -system-time | -t timeout | -tos tos-value | -v | -vpn-instance vpn-instance-name] * host [ip-forwarding]**

说明

只能实现单跳检测。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping -i gigabitethernet 2/0/0 10.1.1.2
PING 10.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=170 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
--- 18.18.18 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/66/170 ms
```

----结束

8.13 使用 Ping 和 Trace 检测多跳 PW

用户可以使用 Ping 和 Trace 检测 MH-PW。

8.13.1 建立配置任务

在使用 Ping 和 Trace 检测 MH-PW 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.13.2 使用 Ping 检测 MH-PW 连通性

Ping 支持 MH-PW 连通性检测。

8.13.3 使用 Trace 检测 MH-PW 连通性

Tracert 支持 MH-PW 网络故障节点检测。

8.13.1 建立配置任务

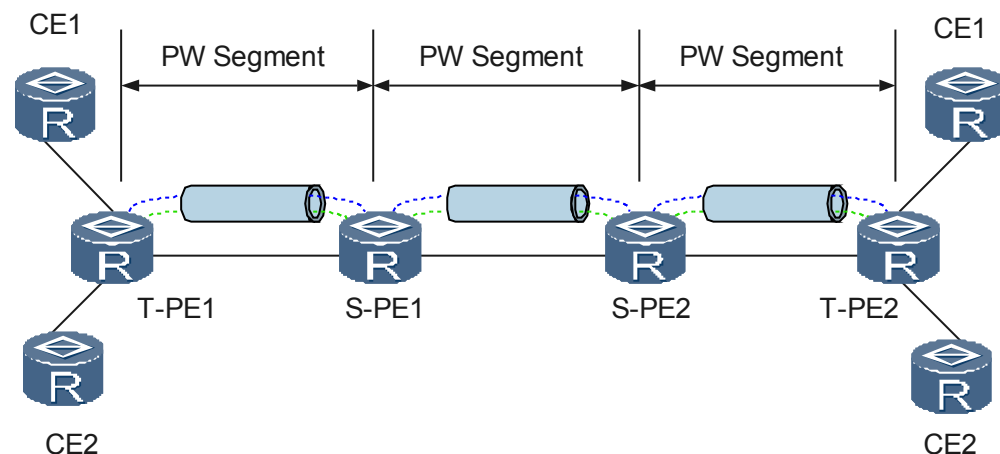
在使用 Ping 和 Trace 检测 MH-PW 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

采用 LDP 作信令的 PW 多跳的典型网络拓扑如图 8-1 所示，多跳 PW 主要适用于以下场景：

- 两台 PE 之间不在同一个 AS 域中，且不能在两台 PE 之间建立信令连接或者建立隧道。
- 两台 PE 上的信令不同，比如一端运行 LDP 一端运行 RSVP。
- 如果接入设备可以运行 MPLS，但又没有能力建立大量的 LDP 会话，这时可以把 UFPE（User Facing Provider Devices）作为 U-PE，把高性能的设备 S-PE 作为 LDP 会话的交换节点，类似信令反射器。

图 8-1 MS-PW 网络组网图



采用 MS-PW 技术，不同类型网络可以实现互联，实现对原有数据网络的改造及增强。但是，由于不同厂商设备或不同版本设备作为 S-PE 对 TTL 复制方式选取不同方案，导致使用传统的 Ping/Tracert 检测工具无法实现 MS-PW 连通性检测。

说明

MPLS TTL 的复制方式有以下两种：

- Uniform: 多跳 PW 经过每个 S-PE 节点时，将内层标签 TTL 值映射到外层公网标签 TTL 字段。此后报文在 MPLS 网络中按照标准的 TTL 处理方式处理。
- Pipe: 多跳 PW 经过每个 S-PE 节点时，外层公网标签 TTL 字段值为固定值。此后报文在 MPLS 网络中按照标准的 TTL 处理方式处理。

NE20E-X6 提供的 VCCV Ping/Tracert 可以实现多跳 PW 的连通性检测。用户在获取 SPE 设备的 TTL 复制方式后，在头节点发起按此复制方式的 Ping/Tracert 检测。

说明

建议全网中 TTL 的复制行为保持一致，否则测试可能失败。

对于图 8-1 所示的组网：

- CE1/CE2 Ethernet 方式接入 T-PE1/T-PE2。
- T-PE1 和 S-PE1 之间建立 PW，S-PE1 与 S-PE2 之间建立 PW，S-PE2 和 T-PE2 之间建立 PW，从而形成 MS-PW。
- MS-PW 使能。

Ping/Tracert 命令支持 Controlword, Normal 和 LabelAlert 三种检测方式，可以实现对图 8-1 所示网络进行检测：

TTL 复制方式	检测工具	检测场景	Control word	Normal	LabelAlert	命令样例
Uniform	Ping	TPE-SPE	Y 必须指定 TTL，TTL 取值为检测发起端和目的端之间经过的 SPE 节点数目 + TPE 节点数目 + P 节点数目	Y TTL 取值为检测发起端和目的端之间经过的 SPE 节点数目 + TPE 节点数目 + P 节点数目	Y	ping vc vlan 100 control-word remote 10.10.10.10 100 ttl 1
		TPE-TPE	Y 可以不指定 TTL	Y TTL 取值为检测发起端和目的端之间经过的 SPE 节点数目 + TPE 节点数目（检测发起端不算） + P 节点数目	Y	ping vc vlan 100 label-alert remote 12.12.12.12
	Tracert	TPE-SPE	Y	Y	Y	tracert vc ppp 100 control-word remote 200
		TPE-TPE	Y	Y	Y	

TTL 复制方式	检测工具	检测场景	Control word	Normal	LabelAlert	命令样例
Pipe	Ping	TPE-SPE	Y 可以不指定 TTL，如果指定 TTL，其取值为源端和目的端之间 SPE 节点数目 + 1	Y 可以不指定 TTL，如果指定 TTL，其取值为源端和目的端之间 SPE 节点数目 + 1	Y	ping vc vlan 100 normal remote 12.12.12.12 200 ttl 3
		TPE-TPE	Y 可以不指定 TTL，如果指定 TTL，其取值为源端和目的端之间 SPE 节点数目 + 1	Y 可以不指定 TTL，如果指定 TTL，其取值为源端和目的端之间 SPE 节点数目 + 1	Y	ping vc vlan 100 normal remote 12.12.12.12 200 ttl 3
	Tracert 此时不显示 P 节点信息	TPE-SPE	Y	Y	Y	tracert vc ppp 100 control-word remote 200
		TPE-TPE	Y	Y	Y	

Ping/Tracert 针对 MS-PW 组网，对同一域内多跳 PW 提供了一种检测手段，从而使多跳 PW 网络可维护性提升，保证了业务质量。

前置任务

在使用 Ping 和 Tracert 检测域间 MS-PW 网络前，需完成以下任务：

- 为各 AS 的 MPLS 骨干网分别配置 IGP，实现同一 AS 内骨干网的 IP 连通性
- 为各 AS 的 MPLS 骨干网分别配置 MPLS 基本能力
- 为各 AS 的 MPLS 骨干网分别配置 MPLS LDP，建立 LDP LSP

数据准备

在使用 Ping 和 Tracert 检测域间 MS-PW 网络前，需要准备以下数据。

序号	数据
1	目的 IP 地址
2	TTL 复制方式

8.13.2 使用 Ping 检测 MH-PW 连通性

Ping 支持 MH-PW 连通性检测。

背景信息

Ping 支持的两种 TTL 复制方式：

- **Pipe**

如果指定 Pipe 模式，探测报文经过 MPLS 域时，IP TTL 只在 Ingress 和 Egress 分别减 1，整个 MPLS 域被当作了一跳。

- **Uniform**

如果指定 Uniform 模式，探测报文在 MPLS 域中每经过一跳，IP TTL 减 1。

操作步骤

步骤 1 对 MH-PW 连通性检测：**ping vc pw-type pw-id [-c echo-number | -m time-value | -s data-bytes | -t timeout-value | -exp exp-value | -r reply-mode | -v] * { normal [no-control-word] } [remote remote-ip-address peer-pw-id] [ttl ttl-value] [pipe | uniform]**

命令执行结果输出包括：

- 对每一个 **ping vc** 报文的响应情况，如果超时到仍没有收到响应报文，则输出 “Request time out”，否则显示响应报文中数据字节数、报文序号、响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

```
<HUAWEI> ping vc 10.1.1.2 pipe
PING 10.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=170 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
--- 18.18.18 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/66/170 ms
```

----结束

8.13.3 使用 Trace 检测 MH-PW 连通性

Tracert 支持 MH-PW 网络故障节点检测。

背景信息

Tracert 支持的两种 TTL 复制方式：

- **Pipe**

如果指定 Pipe 模式，探测报文经过 MPLS 域时，IP TTL 只在 Ingress 和 Egress 分别减 1，整个 MPLS 域被当作了一跳。

- **Uniform**

如果指定 Uniform 模式，探测报文在 MPLS 域中每经过一跳，IP TTL 减 1。

操作步骤

步骤 1 MH-PW 网络故障节点检测：**tracert vc** *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [[**remote** *remote-pw-id*] **draft6**] | **remote** *remote-ip-address*] [**full-lsp-path**] [**pipe** | **uniform**]

以上 **tracert vc** 命令各选项及参数意义请参见《NE20E-X6 命令参考》。

```
<HUAWEI> tracert vc 4.2.1.2 uniform
LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to break.
TTL   Replier           Time    Type    Downstream
0
1      2.1.1.1             63 ms  Transit 3.1.1.1/[22];3.1.2.1/[3]
1      2.2.1.1             23 ms  Transit 3.2.1.1/[12];3.2.2.1/[3]
2      3.1.1.1             43 ms  Transit 4.1.1.1/[3];4.1.1.2/[3]
2      3.1.2.1             43 ms  Egress
2      3.2.1.1             23 ms  Transit 4.2.1.1/[3];4.2.1.2/[3]
2      3.2.2.1             33 ms  Egress
3      4.1.1.1             43 ms  Egress
3      4.1.1.2             43 ms  Egress
3      4.2.1.1             13 ms  Egress
3      4.2.1.2             53 ms  Egress
```

从上述结果中可以看出，LSP 路径上的每个节点以及到每一个节点的响应时间。

----结束

8.14 使用 Service Ping 检测 PWE3 网络

使用 Service Ping 检测 PWE3 网络，可以在本端得到远端的 PWE3 配置信息，确认本端和远端的配置是否一致。

8.14.1 建立配置任务

Service Ping 目前支持动态 PWE3 网络。

8.14.2 使用 Service Ping 检测 PWE3 网络

用户使用 Service Ping 检测 PWE3 网络，可以在本端获取远端的 PWE3 配置信息，检验本端和远端的配置一致性。

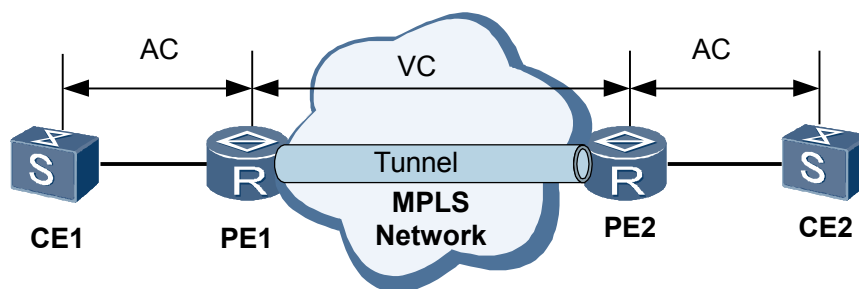
8.14.1 建立配置任务

Service Ping 目前支持动态 PWE3 网络。

应用环境

图 8-2 为 PWE3 典型组网图。

图 8-2 PWE3 典型组网图



Service Ping 工具主要用来检测网络上 PE 间配置是否一致，以保证业务连接的正常建立。

以往这些配置的一致性，需要网络维护人员人为的检查和比对，如果设备上 PWE3 业务比较多，则人为检查就会比较困难，并且容易出现错误。

前置任务

在使用 Service Ping 检测 PWE3 网络前，需完成以下任务：

- 正确配置 PWE3 网络。

数据准备

在使用 Service Ping 检测 PWE3 网络之前，需要准备以下数据。

序号	数据
1	CE 与 PE 之间的接口类型和编号

8.14.2 使用 Service Ping 检测 PWE3 网络

用户使用 Service Ping 检测 PWE3 网络，可以在本端获取远端的 PWE3 配置信息，检验本端和远端的配置一致性。

背景信息

在 PWE3 网络的 PE 设备上执行如下操作。

操作步骤

步骤 1 执行命令 **ping vpn-config peer-address peer-address interface { interface-type interface-number | interface-name } [secondary] [local] [remote]**，检测 PWE3 网络的连通性。

peer-address peer-address：指定对端 PE 的 IP 地址。

interface { interface-type interface-number | interface-name }：指定 AC 接口的类型和编号。

secondary：指定检测备用 PW。

local: 指定请求报文使用 LSP 封装。

remote: 指定回应报文使用 LSP 封装。

命令执行结果如下，详细字段说明请参考命令 [ping vpn-config](#) 说明。

```
<HUAWEI> ping vpn-config peer-address 200.0.0.5 interface GigabitEthernet1/0/8 secondary
VPN-CONFIG PING: Prese CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
```

	local	remote
VPN Type:	PWE3	PWE3
VSI Name:	N/A	N/A
VSI ID:	N/A	N/A
Admin State:	N/A	N/A
Oper State:	N/A	N/A
MTU:	1500	1500
CE Count:	1	1
Control Word:	Disable	Disable
Primary Or Secondary:	Secondary	N/A
Actual IP Addr:	200.0.0.6	200.0.0.5
Expected Peer IP:	200.0.0.5	200.0.0.6
SPE:	NO	NO
PW-ID:	10002	10002
VC-Type:	ethernet	ethernet
Egress Lable:	328707	328705
Ingress Lable:	328705	328707
LSP Tunnel Used:	NO	NO

----结束

8.15 使用 Service Ping 检测 VLL 接入 VPLS 网络

用户通过 Service Ping 检测 VLL 接入 VPLS 网络，可以在本端得到远端的 PW 配置信息，确认本端和远端的配置是否一致。

8.15.1 建立配置任务

在使用 Service Ping 检测 VLL 接入 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.15.2 使用 Service Ping 检测 VLL 接入 VPLS 网络连通性

用户使用 Service Ping 检测 VLL 接入 VPLS 网络 PW 的连通性。

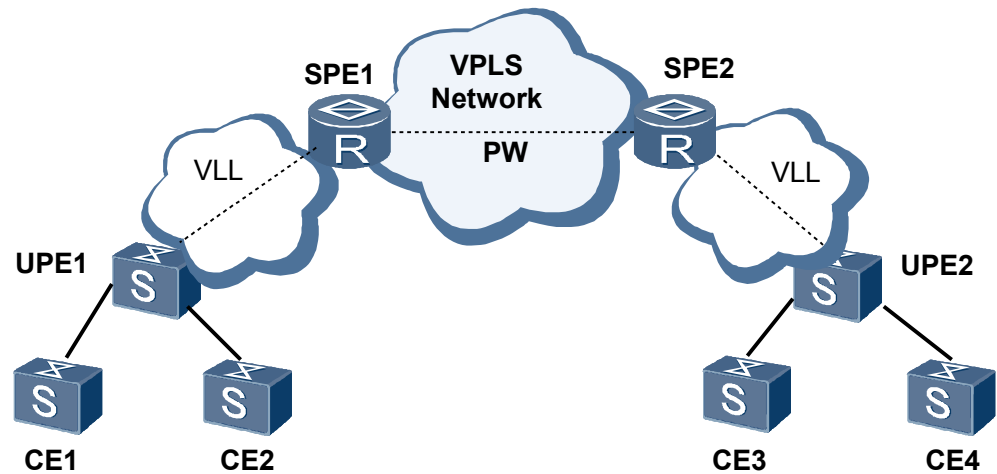
8.15.1 建立配置任务

在使用 Service Ping 检测 VLL 接入 VPLS 网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

图 8-3 为 VLL 接入 VPLS 网络典型组网图。

图 8-3 VLL 接入 VPLS 典型组网图



Service Ping 工具主要用来检测网络上 PE 间配置是否一致，以保证业务连接的正常建立。

以往这些配置的一致性，需要网络维护人员人为的检查和比对，如果设备上 VLL 接入 VPLS 业务比较多，则人为检查就会比较困难，并且容易出现错误。

前置任务

在使用 Service Ping 检测 VLL 接入 VPLS 网络前，需完成以下任务：

- 正确配置 VLL 接入 VPLS 网络。

数据准备

在使用 Service Ping 检测 VLL 接入 VPLS 网络之前，需要准备以下数据。

序号	数据
1	CE 与 PE 之间的接口类型和编号

8.15.2 使用 Service Ping 检测 VLL 接入 VPLS 网络连通性

用户使用 Service Ping 检测 VLL 接入 VPLS 网络 PW 的连通性。

背景信息

在 VLL 接入 VPLS 网络的 PE 设备上执行如下操作。

操作步骤

- 步骤 1** 执行命令 `ping vpn-config peer-address peer-address interface { interface-type interface-number | interface-name } [ secondary ] [ local ] [ remote ]`，检测 VLL 接入 VPLS 网络的连通性。

peer-address *peer-address*: 指定对端 PE 的 IP 地址。

interface { *interface-type interface-number* | *interface-name* }: 指定 AC 接口的类型和编号。

secondary: 指定检测备用 PW。

local: 指定请求报文使用 LSP 封装。

remote: 指定回应报文使用 LSP 封装。

命令执行结果如下，详细字段说明请参考命令 [ping vpn-config](#) 说明。

```
<HUAWEI> ping vpn-config peer-address 200.0.0.2 interface GigabitEthernet 3/0/7.1
VPN-CONFIG PING: Prese CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
```

	local	remote
VPN Type:	PWE3	Martini VPLS
VSI Name:	N/A	vppls1
VSI ID:	N/A	10089
Admin State:	N/A	Up
Oper State:	N/A	Up
MTU:	1500	1500
CE Count:	1	0
Control Word:	Disable	N/A
Primary Or Secondary:	Primary	N/A
Actual IP Addr:	200.0.0.5	200.0.0.2
Expected Peer IP:	200.0.0.2	200.0.0.5
SPE:	NO	YES
PW-ID:	10089	10089
VC-Type:	vlan	vlan
Egress Lable:	394240	328704
Ingress Lable:	328704	394240
LSP Tunnel Used:	NO	NO

----结束

8.16 配置智能 ping 检测网络

通过智能 ping 可以方便地检测到网络的连通情况，省去繁琐的参数设置过程。

8.16.1 建立配置任务

在配置智能 ping 检测网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

8.16.2 使用智能 ping 检测网络连接是否正常

使用智能 Ping 检测网络中两个节点之间的连通性。

8.16.1 建立配置任务

在配置智能 ping 检测网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

应用传统的 **ping** 命令检测 IP 网络是否正常时，需要对复杂的 ping 参数进行设置。为了方便用户使用，通过智能 ping 即可一键启动 ping 操作，使 ping 内部设置的相关参数自动进行排列组合，进而在一定程度上完成链路的故障发现。

前置任务

在配置智能 ping 测试之前，需完成以下任务：

- 配置 IP 地址。
- 配置路由协议，使各节点间的 IP 路由可达。

数据准备

在配置智能 ping 之前，需要准备以下数据。

序号	数据
1	目的 IP 地址。
2	（可选）源 IP 地址。
3	（可选）VPN 实例名。

8.16.2 使用智能 ping 检测网络连接是否正常

使用智能 Ping 检测网络中两个节点之间的连通性。

操作步骤

步骤 1 执行命令 **ping smart** [**-a source-ip-address** | **-vpn-instance vpn-instance-name** | **-c count**] *
host 测试网络连接是否正常。

命令执行结果输出包括：

- 执行 **ping smart** 命令后报文的响应情况。包括对五个组合参数（超时时间 Timeout、等待时间 Interval、报文填充字节 Payload、报文长度 Size 和 ToS 值）取值的全排列组合。如果超时到仍没有收到响应报文，则输出“Timeout”，否则显示每种组合测试的 3 个报文所对应的响应时间。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

<HUAWEI> **ping smart 10.1.1.2**

Timeout (ms)	Interval (ms)	Payload (byte)	Size (byte)	Tos	Reply1 (ms)	Reply2 (ms)	Reply (ms)
2000	20	0x00	64	0	5ms	3ms	1ms,
2000	500	0x00	64	1	1ms	1ms	1ms,
10000	20	0x00	64	2	1ms	12ms	1ms,
10000	500	0x00	64	3	1ms	2ms	1ms,
2000	20	0xFF	64	4	1ms	1ms	1ms,
2000	500	0xFF	64	5	1ms	88ms	1ms,
10000	20	0xFF	64	6	1ms	1ms	1ms,
10000	500	0xFF	64	7	27ms	1ms	28ms,

```

2000 20 0x5a 64 0 1ms 1ms 1ms,
2000 500 0x5a 64 1 1ms 1ms 1ms,
10000 20 0x5a 64 2 2ms 19ms 1ms,
10000 500 0x5a 64 3 1ms 1ms 2ms,
2000 20 0xa5 64 4 1ms 1ms 1ms,
2000 500 0xa5 64 5 2ms 1ms 1ms,
10000 20 0xa5 64 6 1ms 2ms 1ms,
10000 500 0xa5 64 7 3ms 6ms 3ms,
2000 20 0x00 256 0 2ms 1ms 1ms,
2000 500 0x00 256 1 1ms 1ms 1ms,
10000 20 0x00 256 2 2ms 3ms 1ms,
10000 500 0x00 256 3 2ms 1ms 2ms,
2000 20 0xFF 256 4 2ms 1ms 2ms,
2000 500 0xFF 256 5 2ms 1ms 1ms,
10000 20 0xFF 256 6 1ms 1ms 1ms,
10000 500 0xFF 256 7 1ms 1ms 1ms,
2000 20 0x5a 256 0 1ms 2ms 1ms,
2000 500 0x5a 256 1 1ms 1ms 3ms,
10000 20 0x5a 256 2 2ms 1ms 1ms,
10000 500 0x5a 256 3 1ms 1ms 1ms,
2000 20 0xa5 256 4 2ms 1ms 1ms,
2000 500 0xa5 256 5 2ms 2ms 1ms,
10000 20 0xa5 256 6 2ms 1ms 2ms,
10000 500 0xa5 256 7 2ms 3ms 2ms,
2000 20 0x00 1500 0 6ms 16ms 5ms,
2000 500 0x00 1500 1 6ms 6ms 6ms,
10000 20 0x00 1500 2 6ms 7ms 10ms,
10000 500 0x00 1500 3 6ms 10ms 6ms,
2000 20 0xFF 1500 4 5ms 6ms 6ms,
2000 500 0xFF 1500 5 6ms 6ms 6ms,
10000 20 0xFF 1500 6 5ms 5ms 5ms,
10000 500 0xFF 1500 7 16ms 5ms 6ms,
2000 20 0x5a 1500 0 6ms 6ms 6ms,
2000 500 0x5a 1500 1 6ms 8ms 6ms,
10000 20 0x5a 1500 2 6ms 9ms 5ms,
10000 500 0x5a 1500 3 37ms 5ms 9ms,
2000 20 0xa5 1500 4 31ms 5ms 6ms,
2000 500 0xa5 1500 5 7ms 7ms 7ms,
10000 20 0xa5 1500 6 6ms 6ms 13ms,
10000 500 0xa5 1500 7 8ms 9ms 8ms,
2000 20 0x00 4478 0 10ms 8ms 7ms,
2000 500 0x00 4478 1 9ms 8ms 9ms,
10000 20 0x00 4478 2 8ms 7ms 7ms,
10000 500 0x00 4478 3 9ms 8ms 9ms,
2000 20 0xFF 4478 4 8ms 33ms 8ms,
2000 500 0xFF 4478 5 9ms 9ms 8ms,
10000 20 0xFF 4478 6 7ms 13ms 9ms,
10000 500 0xFF 4478 7 8ms 8ms 8ms,
2000 20 0x5a 4478 0 8ms 9ms 7ms,
2000 500 0x5a 4478 1 8ms 8ms 8ms,
10000 20 0x5a 4478 2 8ms 43ms 8ms,
10000 500 0x5a 4478 3 8ms 10ms 8ms,
2000 20 0xa5 4478 4 7ms 8ms 18ms,
2000 500 0xa5 4478 5 8ms 8ms 8ms,
10000 20 0xa5 4478 6 9ms 8ms 11ms,
10000 500 0xa5 4478 7 8ms 11ms 7ms,,

---10.1.1.2 ping statistics ---
192 packet (s) transmitted,
192 packet (s) received,
0.00% packet loss,
round-trip min/avg/max = 1/6/88 ms

```

---结束

9 LLDP 配置

关于本章

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。NE20E-X6 通过运行该协议可以清晰地得知与之相连所有设备的二层信息。

9.1 LLDP 简介

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。

9.2 配置 LLDP 功能

配置 LLDP 功能如何配置 LLDP 功能，同时说明配置任务间的逻辑关系。

9.3 维护 LLDP

维护 LLDP 包括如何监控 LLDP 功能，以及如何清除关于 LLDP 统计数据。

9.4 配置举例

请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

9.1 LLDP 简介

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。

9.1.1 LLDP 概述

LLDP 协议用于发现网络当前第二层的连接情况。

9.1.2 NE20E-X6 支持的 LLDP 特性

NE20E-X6 支持的 LLDP 特性包括以下几个概念：MIB，NSAP Identifier，LLDP Agent，LLDP 管理地址和 LLDP 告警。

9.1.1 LLDP 概述

LLDP 协议用于发现网络当前第二层的连接情况。

背景

目前以太网技术在局域网、城域网都有非常广泛的应用。随着大规模组网的需求，对网络管理（以下简称为网管）能力的要求也越来越高。例如获取相连设备的拓扑状态、设备间的配置冲突等，这些问题都需要解决。

现阶段许多网管软件都使用“自动发现（Automated Discovery）”功能来跟踪拓扑的变化。但是绝大多数网管软件最多只能分析到第三层网络拓扑结构，将设备分组到各个 IP 子网。这些数据只是一些有关设备增加和移除的基本事件，无法确定设备通过哪些接口跟另外一个设备相连，即无法说明设备的位置以及网络操作方式。

LLDP 介绍

第二层发现（Layer 2 Discovery）准确定位了诸如哪些设备附带有那些接口，以及哪些设备与其他设备相互连接等信息，并显示出了客户端、交换机、路由器和应用服务器以及网络服务器之间的路径。这些详细的信息对查询网络失败的根源将很有帮助。

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。该协议规定设备的每个接口上都存储着本端状态信息，并且设备可以向其邻居节点发送本端状态信息，当需要时接口还可以向它们邻居节点发送状态更新的信息，邻居节点将接收到的信息存储在标准的 SNMP（Simple Network Management Protocol）MIB（Management Information Base）中。网管系统可从 MIB 处查询出当前第二层的连接情况。IEEE 802.1ab 标准中还规定网管系统利用 LLDP 所提供的信息去发现第二层的不合理的配置。

通过运行该协议网络系统可以清晰地得知与之相连所有设备的二层信息，既有利于网管规模迅速扩大，同时掌握更详细的网络拓扑信息、变化信息。LLDP 协议还有助于发现网络中实际存在的不合理的配置并上报给网管系统，及时消除错误配置。

9.1.2 NE20E-X6 支持的 LLDP 特性

NE20E-X6 支持的 LLDP 特性包括以下几个概念：MIB，NSAP Identifier，LLDP Agent，LLDP 管理地址和 LLDP 告警。

MIB

MIB: 管理信息数据库。MIB 数据库分为 LLDP Local System MIB 和 LLDP Remote System MIB。

LLDP Local System MIB: LLDP 本地系统管理信息数据库（以下简称 LLDP 本地 MIB），用来保存本设备信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。

LLDP Remote System MIB: LLDP 远端系统管理信息数据库（以下简称 LLDP 远端 MIB），用来保存相邻设备的信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。

NSAP Identifier

NSAP (Network Service Access Point) Identifier: 由设备 ID、接口 ID 组成的一个标识符，在 MIB 中起索引的作用。

LLDP Agent

LLDP Agent: LLDP 代理，用于管理接口的 LLDP 操作。

LLDP Agent 要完成下列任务：

- 维护 LLDP 本地 MIB 的信息。
- 在本端状态发生变化的情况下，提取 LLDP 本地 MIB 信息向邻居节点发送。在本端状态没有变化的情况下，按照一定的周期提取 LLDP 本地 MIB 信息向邻居节点发送。
- 识别并处理收到的 LLDP 报文。
- 维护 LLDP 远端 MIB 库。
- LLDP 本地 MIB 或 LLDP 远端 MIB 的状态发生变化的情况下，向网管发送 LLDP 告警。

LLDP 管理地址

LLDP 管理地址（以下简称管理地址）是供网管系统标识设备并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，更有利于清晰地了解到当前的拓扑状态，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 字段中传送给邻居节点。

LLDP 告警

LLDP 告警是 LLDP 本地 MIB 库和远端 MIB 库发生变化的情况下，设备向网管系统发送的更新拓扑的提示信息。触发告警的原因有：

- 全局 LLDP 使能的状态变化
- 本地管理地址改变
- 邻居信息发生变化

LLDP 告警功能对全局起作用，控制所有接口发送告警的能力。

9.2 配置 LLDP 功能

配置 LLDP 功能如何配置 LLDP 功能，同时说明配置任务间的逻辑关系。

9.2.1 建立配置任务

在配 LLDP 功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

9.2.2 （可选）使能 LLDP 告警

在路由器上使能 LLDP 告警功能后，当它的全局 LLDP 使能状态、管理 IP 地址或者邻居信息发生变化时，会向网管系统发送拓扑信息更新的告警。

9.2.3 使能全局 LLDP 功能

使能设备的 LLDP 功能后，路由器能向使能 LLDP 功能的邻居节点发送携带本端状态信息的 LLDP 报文，同时也能通过 LLDP 报文获取使能 LLDP 功能的邻居节点的状态信息。

9.2.4 （可选）去使能接口 LLDP 功能

在使能全局 LLDP 功能的情况下，缺省情况下所有接口都处于使能 LLDP 功能的状态。当部分接口需要使用 LLDP 功能，而另一部分接口需要禁用 LLDP 功能的情况下，在需要禁用 LLDP 功能的接口视图下执行 `undo lldp enable` 命令去使能 LLDP 功能。

9.2.5 （可选）配置 LLDP 管理地址

LLDP 管理地址是供网管系统标识设备并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，更有利于清晰地了解到当前的拓扑状态，便于网络管理。

9.2.6 （可选）配置 LLDP 属性

可配置的 LLDP 属性包括发送 LLDP 报文的时间周期，发送 LLDP 报文的延迟时间，本端信息在邻居节点中保持的时间倍数，接口 LLDP 功能重新使能的延迟时间和邻居信息变化告警的延迟时间。

9.2.7 检查配置结果

在配置 LLDP 功能成功后，可以查看到已经完成的 LLDP 功能的配置是否满足要求。

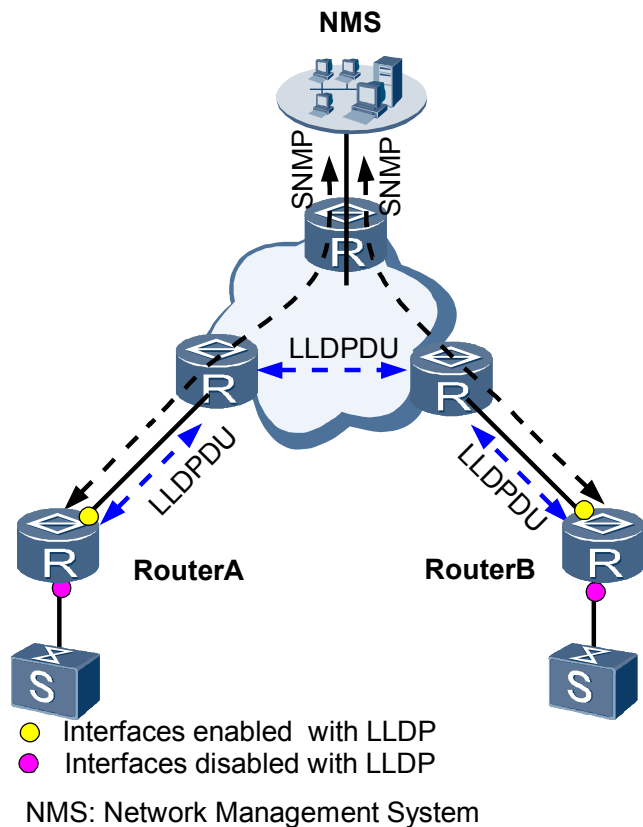
9.2.1 建立配置任务

在配 LLDP 功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

LLDP 功能用于获取邻居信息和拓扑发现。如图 9-1 所示，需要网管系统 NMS（Network Management System）收集 RouterA 和 RouterB 的拓扑信息的时候，需要在 RouterA 和 RouterB 上使能 LLDP 功能，使 RouterA 和 RouterB 互相发送状态信息以便网管系统获取拓扑信息。为了能够让网络设备查找，需要在 RouterA 和 RouterB 上配置 LLDP 管理地址。当 RouterA 和 RouterB 的全局 LLDP 使能状态、管理 IP 地址或者邻居信息发生变化的时候，会向网管系统发送拓扑信息更新的告警。这种情况下，需要在设备上使能 LLDP 告警功能。

图 9-1 LLDP 应用环境组网图



前置任务

在配置 LLDP 功能之前，需完成以下任务：

- 需要配置用于 LLDP 管理的 IP 地址
LLDP 报文中携带的 LLDP 管理地址是用来标识设备的，必须选用网管系统能够唯一标识设备并且方便管理的 IP 地址（如管理网口地址），该地址需要在配置 LLDP 管理地址之前配置。

数据准备

在配置 LLDP 功能之前，需要准备以下数据。

序号	数据
1	用作 LLDP 管理地址的 IP 地址
2	发送 LLDP 报文的时间周期
3	发送 LLDP 报文的延迟时间
4	本端信息在邻居节点中保持的时间倍数
5	接口 LLDP 模块从禁用状态到重新使能的延迟时间

序号	数据
6	发送邻居信息变化告警的延迟时间

9.2.2 （可选）使能 LLDP 告警

在路由器上使能 LLDP 告警功能后，当它的全局 LLDP 使能状态、管理 IP 地址或者邻居信息发生变化时，会向网管系统发送拓扑信息更新的告警。

背景信息

在设备上使能或去使能全局 LLDP 功能、更改 LLDP 管理地址或者邻居信息发生变化的时候需要向网管系统发送拓扑信息更新的告警的时候，需要在设备上使能 LLDP 告警功能。

请在 RouterA 和 RouterB 上进行如下配置。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 执行命令 `snmp-agent trap enable lldp`，使能 LLDP 告警功能。

----结束

9.2.3 使能全局 LLDP 功能

使能设备的 LLDP 功能后，路由器能向使能 LLDP 功能的邻居节点发送携带本端状态信息的 LLDP 报文，同时也能通过 LLDP 报文获取使能 LLDP 功能的邻居节点的状态信息。

背景信息

使能设备 LLDP 功能的情况下，路由器能够向使能 LLDP 功能的邻居节点发送携带本端状态信息的 LLDP 报文，同时也能通过 LLDP 报文获取使能 LLDP 功能的邻居节点的状态信息。网络管理系统可从路由器上获取当前设备的二层的连接状态信息并进行网络拓扑的分析。

请在 RouterA 和 RouterB 上进行如下配置。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 执行命令 `lldp enable`，使能全局 LLDP 功能。

----结束

9.2.4 （可选）去使能接口 LLDP 功能

在使能全局 LLDP 功能的情况下，缺省情况下所有接口都处于使能 LLDP 功能的状态。当部分接口需要使用 LLDP 功能，而另一部分接口需要禁用 LLDP 功能的情况下，在需要禁用 LLDP 功能的接口视图下执行 `undo lldp enable` 命令去使能 LLDP 功能。

背景信息



说明

以下的去使能接口 LLDP 功能的操作只能在使能全局 LLDP 功能的前提下才可执行。

在使能全局 LLDP 功能的情况下，所有接口缺省情况下都处于使能 LLDP 功能的状态。当部分接口需要使用 LLDP 功能，而另一部分接口需要禁用 LLDP 功能的情况下，在需要禁用 LLDP 功能的接口视图下执行 **undo lldp enable** 命令去使能 LLDP 功能。

请在 RouterA 和 RouterB 上与需要禁用 LLDP 功能的设备相连的接口上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface { ethernet | gigabitethernet } interface-number**，进入接口视图。

步骤 3 执行命令 **undo lldp enable**，去使能接口 LLDP 功能。

----结束

9.2.5 （可选）配置 LLDP 管理地址

LLDP 管理地址是供网管系统标识设备并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，更有利于清晰地了解到当前的拓扑状态，便于网络管理。

背景信息



说明

以下的配置 LLDP 管理地址的操作只能在使能全局 LLDP 功能的前提下才可执行。

LLDP 管理地址必须是一个合法的并且是存在于设备上的单播 IP 地址。

请在 RouterA 和 RouterB 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp management-address ip-address**，配置 LLDP 管理地址。

----结束

9.2.6 （可选）配置 LLDP 属性

可配置的 LLDP 属性包括发送 LLDP 报文的时间周期，发送 LLDP 报文的延迟时间，本端信息在邻居节点中保持的时间倍数，接口 LLDP 功能重新使能的延迟时间和邻居信息变化告警的延迟时间。

操作步骤

- （可选）配置发送 LLDP 报文的时间周期

根据具体的需求在 RouterA 和 RouterB 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **lldp message-transmission interval interval**，配置发送 LLDP 报文的时间周期。

缺省值是 30 秒。

LLDP 报文发送时间周期的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负担，造成资源的浪费。

LLDP 报文发送时间周期 *interval* 与延迟时间 *delay* 互相有制约关系，所以调整 *interval* 的取值时候需要注意与 *delay* 的取值的配合。

- 增加 *interval* 不受 *delay* 的制约，只要小于或等于 32768 就可以。
- 减小 *interval* 的时候，*interval* 的目标取值一定要大于或等于四倍的当前 *delay* 值。所以 *interval* 要取的目标值小于四倍的 *delay* 的时候，需要先将 *delay* 调整到小于或等于 *interval* 目标值的四分之一，然后再将 *interval* 减小到目标值。

● （可选）配置发送 LLDP 报文的延迟时间

根据具体的需求在 RouterA 和 RouterB 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **lldp message-transmission delay delay**，配置发送 LLDP 报文的延迟时间。

缺省值是 2 秒。

LLDP 报文发送延迟时间的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负载，造成资源的浪费。

LLDP 报文发送延迟时间 *delay* 与时间周期 *interval* 互相有制约关系，所以调整 *delay* 的取值时候需要注意与 *interval* 的取值的配合。

- 减小 *delay* 不受 *interval* 的制约，只要大于或等于 1 就可以。
- 增加 *delay* 的时候，*delay* 的目标取值一定要小于或等于四分之一的当前 *interval* 值。所以 *delay* 要取的目标值大于四分之一的当前 *interval* 值的时候，需要先将当前 *interval* 值调整到大于或等于 *delay* 目标值的四倍，然后再将 *delay* 增加到目标值。

● （可选）配置本端信息在邻居节点中保持的时间倍数

根据具体的需求在 RouterA 和 RouterB 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **lldp message-transmission hold-multiplier hold**，配置本端信息在邻居节点中保持时间的倍数。

缺省值是 4。

增加该值能够延长本端信息在邻居节点中保持的时间。

- （可选）配置接口 LLDP 功能重新使能的延迟时间

根据具体的需求在 RouterA 和 RouterB 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **lldp restart-delay delay**，配置接口 LLDP 功能重新使能的延迟时间。

缺省值是 2 秒。

通过配置该参数控制接口的 LLDP 协议状态频繁改变，减少由此导致的邻居节点的拓扑振荡。

- （可选）配置邻居信息变化告警的延迟时间

根据具体的需求在 RouterA 和 RouterB 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **lldp trap-interval interval**，配置邻居信息变化告警的延迟时间。

缺省值是 5 秒。

当邻居信息频繁发生变化的时候延长该延迟时间来减少设备频繁向网管系统发送信息，以达到抑制拓扑振荡目的。

----结束

9.2.7 检查配置结果

在配置 LLDP 功能成功后，可以查看到已经完成的 LLDP 功能的配置是否满足要求。

操作步骤

- 步骤 1** 使用 **display lldp local [interface interface-type interface-number]** 命令查看设备的本地 LLDP 状态。

----结束

任务示例

在配置成功之后，执行 **display lldp local** 命令查看设备的 LLDP 功能处于 enable 状态，去使能 LLDP 功能的接口 LLDP 功能处于 disable 状态、LLDP 管理地址为 10.10.10.1、LLDP 告警处于 enable 状态，发送 LLDP 报文的时间周期和延迟时间、本端信息在邻居节点中保持时间的倍数、LLDP 模块重新使能的延迟时间、邻居信息变化告警的延迟时间等 LLDP 属性的值配置正确。

```
<HUAWEI> display lldp local
System information:
ChassisIdSubtype: macAddress
ChassisId: 00e0-fcc8-1b31
SysName: HUAWEI
SysDesc: Huawei Versatile Routing Platform Software
```

```

VRP (R) software, Version 5.90 (NE20E V600R003C00)
Copyright (C) 2000-2009 Huawei Technologies Co., Ltd.
HUAWEI NE20E-X6
SysCapSupported: bridge
SysCapEnabled: bridge
LLDPUptime: 2007/6/20 15:41:49
System configuration:
LLDP enable status:          enable          (default is disable)
LldpMsgTxInterval:          50s             (default is 30s)
LldpMsgTxHoldMultiplier:    10              (default is 4)
LldpReinitDelay:            7s              (default is 2s)
LldpTxDelay:                 8s              (default is 2s)
LldpNotificationInterval:    9s             (default is 5s)
LldpNotificationEnable:      enable          (default is disable)
Management address:          IP: 10.10.10.1
Remote Table Statistics:
RemTablesLastChangeTime:     0 days, 0 hours, 0 minutes, 0 seconds
RemTableInserts:             0
RemTableDeletes:             0
RemTableDrops:               0
RemTablesAgeouts:            0
Neighbors Total:             0
Port information:
Interface GigabitEthernet1/0/0:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/0
PortDesc: GigabitEthernet1/0/0 Interface
LLDP Enable Status:          disable         (default is disable)
LLDP Running Status:         stop
Neighbors Total:             0

```

9.3 维护 LLDP

维护 LLDP 包括如何监控 LLDP 功能，以及如何清除关于 LLDP 统计数据。

9.3.1 清除 LLDP 统计信息

通过命令 `reset lldp statistic` 清除 LLDP 的统计信息。

9.3.2 监控 LLDP 运行状态

通过命令 `display lldp local`，`display lldp statistics` 和 `display lldp neighbor` 监控 LLDP 的运行情况。

9.3.1 清除 LLDP 统计信息

通过命令 `reset lldp statistic` 清除 LLDP 的统计信息。

操作步骤

步骤 1 在用户视图下执行 `reset lldp statistic [ interface interface-type interface-number ]` 命令清除关于 LLDP 报文的统计信息（包括收包数、发包数、错误包数、错误帧数等）。

----结束

9.3.2 监控 LLDP 运行状态

通过命令 `display lldp local`，`display lldp statistics` 和 `display lldp neighbor` 监控 LLDP 的运行情况。

操作步骤

- 在任意视图下执行 **display lldp local** [**interface interface-type interface-number**] 命令查看全局或指定接口的当前 LLDP 状态。
- 在任意视图下执行 **display lldp statistics** [**interface interface-type interface-number**] 命令查看设备接口收发报文统计信息。
- 在任意视图下执行 **display lldp neighbor** [**interface interface-type interface-number**] 命令查看设备接口的邻居信息。

----结束

9.4 配置举例

请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

9.4.1 配置 LLDP 功能示例

两台路由器都有到网管系统（NMS）的可达路由，且通过以太网接口相互直连。两台路由器同时使能 LLDP 功能后，可以通过 LLDP 协议获取彼此的状态信息。

9.4.2 配置有 Eth-Trunk 的网络的 LLDP 功能示例

两台通过 Eth-Trunk 接口相连的路由器，部分加入 Eth-Trunk 的接口能够收发 LLDP 报文，以获取彼此的状态信息。同时另外一部分加入 Eth-Trunk 的接口可禁止收发 LLDP 报文。

9.4.3 配置一个接口有多邻居的网络的 LLDP 功能示例

多台路由器之间可以通过可达链路互相发送 LLDP 报文，获取彼此的状态信息。同时网管系统能够通过 LLDP 管理地址查找与之相连的路由器以获取网络拓扑信息。

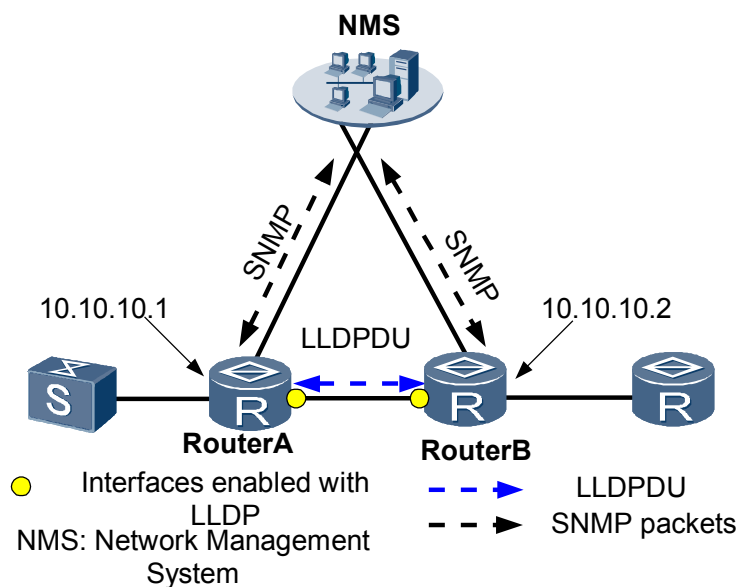
9.4.1 配置 LLDP 功能示例

两台路由器都有到网管系统（NMS）的可达路由，且通过以太网接口相互直连。两台路由器同时使能 LLDP 功能后，可以通过 LLDP 协议获取彼此的状态信息。

组网需求

如图 9-2 所示，RouterA 和 RouterB 的以太网接口相互直连，并且 RouterA 和 RouterB 都有到网管系统（NMS）的可达路由。要求 RouterA 和 RouterB 之间可以通过 LLDP 协议获取彼此的状态信息，同时网管系统能够通过 LLDP 管理地址查找 RouterA 和 RouterB 获取拓扑信息。当 LLDP 管理地址变化、去使能全局 LLDP 功能和邻居信息发生变化的时候，要求 RouterA 向网管系统发送 LLDP 告警。

图 9-2 配置 LLDP 功能组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 RouterA 和 RouterB 的 LLDP 告警。
2. 使能 RouterA 和 RouterB 的全局 LLDP 功能。
3. 配置 RouterA 和 RouterB 的管理 IP 地址方便网管系统进行管理。
4. 配置 RouterA 和 RouterB 的 LLDP 属性。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。
- 发送 LLDP 报文的周期为 60 秒、延迟时间为 9 秒，发送邻居信息变化的 LLDP 告警延迟时间为 10 秒。

操作步骤

步骤 1 使能 RouterA 和 RouterB 的 LLDP 告警

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] snmp-agent trap enable lldp
```

配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] snmp-agent trap enable lldp
```

步骤 2 使能 RouterA 和 RouterB 的全局 LLDP 功能

配置 RouterA。

```
[RouterA] lldp enable
```

配置 RouterB。

```
[RouterB] lldp enable
```

步骤 3 配置 RouterA 和 RouterB 的管理 IP 地址

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

步骤 4 配置 RouterA 和 RouterB 的 LLDP 属性

配置 RouterA。

```
[RouterA] lldp message-transmission interval 60
```

```
[RouterA] lldp message-transmission delay 9
```

```
[RouterA] lldp trap-interval 10
```

配置 RouterB。

请参见 RouterA 的配置。

步骤 5 验证配置结果

查看各设备的 LLDP 是否使能、LLDP 管理地址是否配置、LLDP 告警功能是否使能以及 LLDP 属性的值是否为所配置的值。

● 查看 RouterA。

```
<RouterA> display lldp local
```

System information:

ChassisIdSubtype: macAddress

ChassisId: 00e0-fcc8-1b31

SysName: RouterA

SysDesc: Huawei Versatile Routing Platform Software

VRP (R) software, Version 5.90 (NE20E V600R003C00)

Copyright (C) 2000-2009 Huawei Technologies Co., Ltd.

HUAWEI NE20E-X6

SysCapSupported: bridge

SysCapEnabled: bridge

LLDPUpTime: 2008/6/20 15:41:49

System configuration:

LLDP enable status: enable (default is disable)

LldpMsgTxInterval: 60s (default is 30s)

LldpMsgTxHoldMultiplier: 4 (default is 4)

LldpReinitDelay: 2s (default is 2s)

LldpTxDelay: 9s (default is 2s)

LldpNotificationInterval: 10s (default is 5s)

LldpNotificationEnable: enable (default is disable)

Management address: IP: 10.10.10.1

Remote Table Statistics:

RemTablesLastChangeTime: 0 days, 0 hours, 0 minutes, 0 seconds

RemTableInserts: 0

RemTableDeletes: 0

RemTableDrops: 0

RemTablesAgeouts: 0

Neighbors Total: 0

```
Port information:
Interface GigabitEthernet1/0/0:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/0
PortDesc: GigabitEthernet1/0/0 Interface
LLDP Enable Status:          enable          (default is disable)
LLDP Running Status:         running
Neighbors Total:             0
```

- 查看 RouterB。

请参见 RouterA 的查看过程。

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
lldp enable
#
snmp-agent trap enable lldp
#
lldp message-transmission interval 60
#
lldp message-transmission delay 9
#
lldp trap-interval 10
#
lldp management-address 10.10.10.1
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
lldp enable
#
snmp-agent trap enable lldp
#
lldp message-transmission interval 60
#
lldp message-transmission delay 9
#
lldp trap-interval 10
#
lldp management-address 10.10.10.2
#
return
```

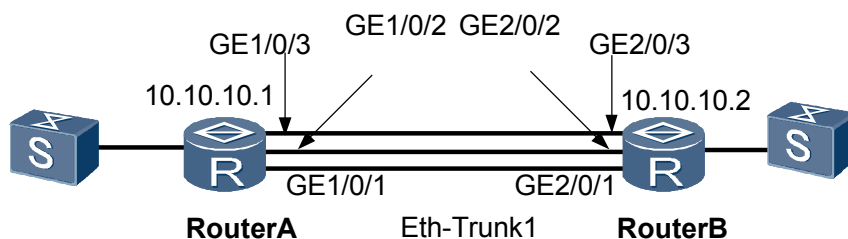
9.4.2 配置有 Eth-Trunk 的网络的 LLDP 功能示例

两台通过 Eth-Trunk 接口相连的路由器，部分加入 Eth-Trunk 的接口能够收发 LLDP 报文，以获取彼此的状态信息。同时另外一部分加入 Eth-Trunk 的接口可禁止收发 LLDP 报文。

组网需求

如图 9-3 所示，RouterA 和 RouterB 之间通过 Eth-Trunk 相连。要求 RouterA 和 RouterB 各有三个以太网接口加入 Eth-Trunk，同时要求 RouterA 和 RouterB 各有两个加入 Eth-Trunk 的接口能够收发 LLDP 报文，以获取彼此的状态信息。而 RouterA 和 RouterB 的另外一个加入 Eth-Trunk 的接口禁止收发 LLDP 报文。

图 9-3 配置有 Eth-Trunk 的网络的 LLDP 功能组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 RouterA 和 RouterB 的全局 LLDP 功能。
2. 配置 RouterA 和 RouterB 的管理 IP 地址以便在邻居设备中标识本端设备。
3. 将 RouterA 和 RouterB 的以太网物理接口加入到 Eth-Trunk 中。
4. 去使能 RouterA 和 RouterB 上加入到 Eth-Trunk 的不需要收发 LLDP 报文的成员接口的 LLDP 功能。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。
- RouterA 和 RouterB 相连的 Eth-Trunk 的编号，加入到该 Eth-Trunk 的成员接口的编号。

操作步骤

步骤 1 使能 RouterA 和 RouterB 的全局 LLDP 功能

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] lldp enable
```

配置 RouterB。

请参见 RouterA 的配置。

步骤 2 配置 RouterA 和 RouterB 的管理 IP 地址以便在邻居设备中标识本端设备

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

步骤 3 配置 RouterA 和 RouterB 的 Eth-Trunk

配置 RouterA。

```
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] quit
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] eth-trunk 1
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] eth-trunk 1
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] interface GigabitEthernet 1/0/3
[RouterA-GigabitEthernet1/0/3] eth-trunk 1
```

配置 RouterB。

请参见 RouterA 的配置。

步骤 4 去使能 RouterA 和 RouterB 上加入到 Eth-Trunk 的不收发 LLDP 报文的成员接口的 LLDP 功能

配置 RouterA。

```
[RouterA] interface gigabitEthernet1/0/3
[RouterA-GigabitEthernet1/0/3] undo lldp enable
```

配置 RouterB。

```
[RouterB] interface gigabitEthernet2/0/3
[RouterB-GigabitEthernet2/0/3] undo lldp enable
```

步骤 5 验证配置结果

查看各设备的 LLDP 是否使能、LLDP 管理地址是否配置、加入 Eth-Trunk1 的成员接口的 LLDP 使能状态是否为所配置的状态。

● 查看 RouterA 的配置。

```
<RouterA> display lldp local
System information:
ChassisIdSubtype: macAddress
ChassisId: 00e0-fcc8-1b31
SysName: RouterA
SysDesc: Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.90 (NE20E V600R003C00)
Copyright (C) 2000-2009 Huawei Technologies Co., Ltd.
HUAWEI NE20E-X6
SysCapSupported: bridge
SysCapEnabled: bridge
LLDPUpTime: 2007/6/21 14:46:58
System configuration:
LLDP enable status:          enable          (default is disable)
LldpMsgTxInterval:          30s              (default is 30s)
LldpMsgTxHoldMultiplier:    4                (default is 4)
LldpReinitDelay:             2s              (default is 2s)
LldpTxDelay:                 2s              (default is 2s)
LldpNotificationInterval:    5s              (default is 5s)
LldpNotificationEnable:      enable          (default is disable)
Management address:          IP: 10.10.10.1
Remote Table Statistics:
RemTablesLastChangeTime:     0 days, 0 hours, 0 minutes, 0 seconds
RemTableInserts:             0
RemTableDeletes:             0
RemTableDrops:               0
RemTablesAgeouts:            0
Neighbors Total:             0
Port information:
Interface GigabitEthernet1/0/1:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/1
PortDesc: GigabitEthernet1/0/1 Interface
LLDP Enable Status:          enable          (default is disable)
```



```
LLDP Running Status:          running
Neighbors Total:              0
Interface GigabitEthernet1/0/2:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/2
PortDesc: GigabitEthernet1/0/2 Interface
LLDP Enable Status:           enable          (default is disable)
LLDP Running Status:          running
Neighbors Total:              0
Interface GigabitEthernet1/0/3:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/3
PortDesc: GigabitEthernet1/0/3 Interface
LLDP Enable Status:           disable        (default is disable)
LLDP Running Status:          stop
Neighbors Total:              0
```

● 查看 RouterB 的配置。

请参见 RouterA 的查看过程。

查看各设备的成员接口是否已经加入到 Eth-Trunk1。

● 查看 RouterA 的配置。

```
<RouterA> display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 10         Hash arithmetic: According to MAC
System Priority: 32768         System ID: 00e0-fcc8-1b31

-----
ActorPortName      Status   PortType  PortPri  PortNo   PortKey   PortState
GigabitEthernet1/0/1 Selected 1GE       32768    1031     305       11111100
GigabitEthernet1/0/2 Unselect 1GE       32768    1028     305       11100000
GigabitEthernet1/0/3 Selected 1GE       32768    1032     305       11111100
Partner:

-----
ActorPortName      SysPri   SystemID   PortPri  PortNo   PortKey   PortState
GigabitEthernet1/0/1 100      0018-8201-4da7 32768    3079     305       11111100
GigabitEthernet1/0/2 100      0018-8201-4da7 32768    3076     305       11100000
GigabitEthernet1/0/3 100      0018-8201-4da7 100      3080     305       11111100
```

● 查看 RouterB 的配置。

请参见 RouterA 的查看过程。

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
lldp enable
#
interface Eth-Trunk1
#
interface GigabitEthernet1/0/1
eth-trunk 1
#
interface GigabitEthernet1/0/2
eth-trunk 1
#
interface GigabitEthernet1/0/3
eth-trunk 1
undo lldp enable
#
```

```
lldp management-address 10.10.10.1
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
lldp enable
#
interface Eth-Trunk1
#
interface GigabitEthernet2/0/1
eth-trunk 1
#
interface GigabitEthernet2/0/2
eth-trunk 1
#
interface GigabitEthernet2/0/3
eth-trunk 1
undo lldp enable
#
lldp management-address 10.10.10.2
#
return
```

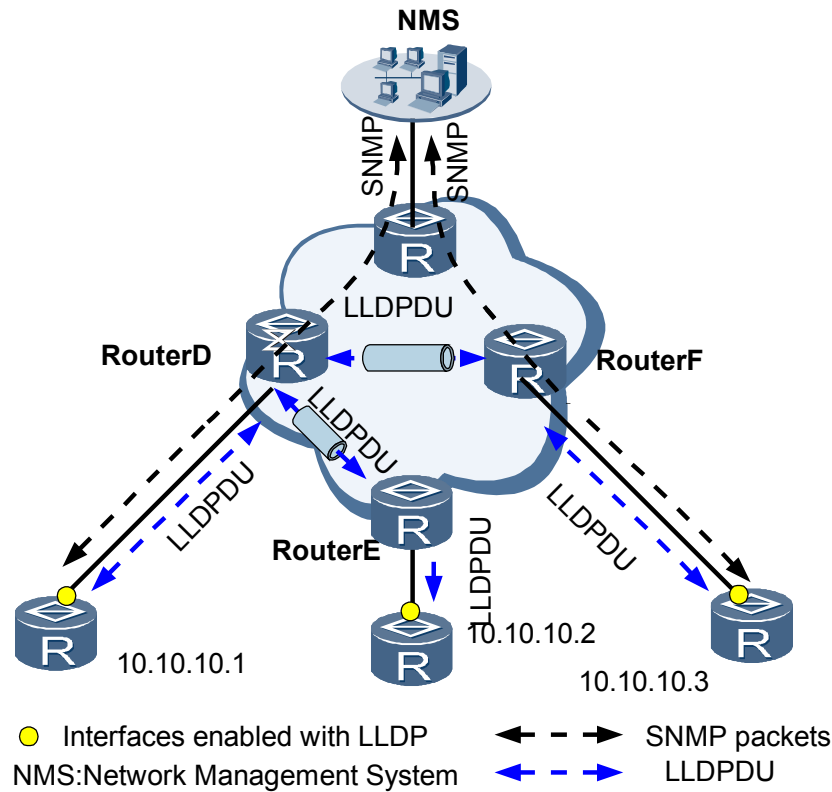
9.4.3 配置一个接口有多邻居的网络的 LLDP 功能示例

多台路由器之间可以通过可达链路互相发送 LLDP 报文，获取彼此的状态信息。同时网管系统能够通过 LLDP 管理地址查找与之相连的路由器以获取网络拓扑信息。

组网需求

如图 9-4 所示，RouterA 与 RouterB 和 RouterC 之间有可达链路，其中 RouterA 和 RouterC 与网管系统之间有可达路由。要求 RouterA 与 RouterB 和 RouterC 之间可以通过可达链路互相发送 LLDP 报文，获取彼此的状态信息。同时网管系统能够通过 LLDP 管理地址查找 RouterA 和 RouterC 获取拓扑信息。

图 9-4 配置一个接口有多邻居的网络的 LLDP 功能组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 配置 RouterA、RouterB 和 RouterC 的 LLDP 全局使能。
2. 配置 RouterA、RouterB 和 RouterC 的管理 IP 地址方便在邻居节点中标识本设备。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 和 RouterC 的管理 IP 地址。

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 的 LLDP 全局使能

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] lldp enable
```

配置 RouterB。

请参见 RouterA 的配置。

配置 RouterC。

请参见 RouterA 的配置。

步骤 2 配置 RouterA、RouterB 和 RouterC 的管理 IP 地址

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

配置 RouterC。

```
[RouterC] lldp management-address 10.10.10.3
```

步骤 3 验证配置结果

查看各设备的 LLDP 功能是否使能、LLDP 管理地址是否配置。

● 查看 RouterA 的配置。

```
<RouterA> display lldp local
System information:
ChassisIdSubtype: macAddress
ChassisId: 00e0-fcc8-1b31
SysName: RouterA
SysDesc: Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.90 (NE20E V600R003C00)
Copyright (C) 2000-2009 Huawei Technologies Co., Ltd.
HUAWEI NE20E-X6
SysCapSupported: bridge
SysCapEnabled: bridge
LLDPUpTime: 2008/6/20 15:41:49
System configuration:
LLDP enable status:          enable          (default is disable)
LldpMsgTxInterval:          30s              (default is 30s)
LldpMsgTxHoldMultiplier:    4               (default is 4)
LldpReinitDelay:            2s              (default is 2s)
LldpTxDelay:                2s              (default is 2s)
LldpNotificationInterval:    5s              (default is 5s)
LldpNotificationEnable:      disable         (default is disable)
Management address:          IP: 10.10.10.1
Remote Table Statistics:
RemTablesLastChangeTime:     0 days, 0 hours, 0 minutes, 0 seconds
RemTableInserts:             0
RemTableDeletes:             0
RemTableDrops:               0
RemTablesAgeouts:            0
Neighbors Total:             0
Port information:
Interface GigabitEthernet1/0/0:
PortId Subtype: interfaceName
PortId: GigabitEthernet1/0/0
PortDesc: GigabitEthernet1/0/0 Interface
LLDP Enable Status:          enable          (default is disable)
LLDP Running Status:         running
Neighbors Total:             0
```

● 查看 RouterB 的配置。

请参见 RouterA 的查看过程。

● 查看 RouterC 的配置。

请参见 RouterA 的查看过程。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 lldp enable
#
 lldp management-address 10.10.10.1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 lldp enable
#
 lldp management-address 10.10.10.2
#
return
```

RouterC 的配置文件

```
#
 sysname RouterC
#
 lldp enable
#
 lldp management-address 10.10.10.3
#
return
```


10 故障管理

关于本章

10.1 故障管理简介

10.2 配置告警管理

配置告警管理后，可以配置告警类型、告警延迟上报、基于网管主机的告警相关性抑制或基于接口的告警屏蔽。

10.3 配置事件管理

配置事件管理后，可以配置事件类型，事件延迟上报。

10.4 配置实体故障隔离

通过本节可以了解到配置实体故障隔离的应用环境、前置任务和操作步骤。用户可针对单板和灵活子卡配置实体故障隔离功能，立即给已经发生故障的单板或灵活子卡下电，使得故障第一时间得到处理。

10.5 维护

本节主要讲述维护故障管理的方法。

10.6 配置举例

配置故障管理的应用示例。配置示例中包括组网需求、配置注意事项和配置思路等。

10.1 故障管理简介

10.1.1 故障管理

10.1.1 故障管理

故障管理的目的是通过对系统中存在的、或潜在的故障采取检测、诊断、隔离、恢复、告警和预警等措施，消除或减轻故障对系统功能的影响，增强系统容错能力，以提高系统可靠性。

10.2 配置告警管理

配置告警管理后，可以配置告警类型、告警延迟上报、基于网管主机的告警相关性抑制或基于接口的告警屏蔽。

10.2.1 建立配置任务

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

10.2.2 配置告警级别

用户可以修改系统定义的告警类型和级别。

10.2.3 配置告警延迟上报

用户可以通过设置告警的延迟上报周期，来控制告警上报频率。

10.2.4 配置告警相关性抑制

设置告警相关性抑制后，系统将屏蔽衍生告警，只保留根源告警上报至网管。

10.2.5 检查配置结果

告警管理配置成功后，可以查看到告警的内容及注册信息。

10.2.1 建立配置任务

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

应用环境

用户可以使用故障管理，对系统进行配置告警管理，包括调整告警级别、实现告警延迟上报及告警相关性抑制等功能。

前置任务

在配置告警管理之前，需要完成以下任务：

- 路由器安装完毕并加电启动正常。

数据准备

在配置告警管理之前，需要准备以下数据。

序号	数据
1	告警名称
2	告警级别 ● 1: Critical ● 2: Major ● 3: Minor ● 4: Warning ● 5: Indeterminate ● 6: Cleared
3	告警延迟上报周期和恢复告警延迟上报周期
4	告警相关性抑制的网管主机 IP 地址、网管侧显示的安全名、VPN 实例名、接口名

10.2.2 配置告警级别

用户可以修改系统定义的告警类型和级别。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **alarm**，进入告警管理视图。

步骤 3 执行命令 **alarm-name alarm-name severity severity**，配置告警的级别。

如果用户只关注某几种告警，可以将这几种告警级别设置为最高级，并配置过滤条件，则系统将只向网管上报这几种告警。

----结束

10.2.3 配置告警延迟上报

用户可以通过设置告警的延迟上报周期，来控制告警上报频率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **alarm**，进入告警管理视图。

步骤 3 执行命令 **delay-suppression enable**，打开告警延迟上报开关。

缺省情况下，告警延迟上报开关打开，对延迟上报周期内的闪断告警和重复告警进行抑制。

步骤 4 执行命令 **suppression alarm-name alarm-name { cause-period cause-seconds | clear-period clear-seconds }**，设置告警延迟上报周期。

对某一告警设置了告警延迟上报周期后，在延迟上报周期内，

- 系统中如果没有该告警的匹配告警，则在延迟上报周期达到后上报该告警。到达前不上报指定的告警，周期到达后系统再上报该告警。
- 系统中如果有该告警的匹配告警，则该告警及其配对告警将从告警队列中丢弃，不进行上报。

使用参数 **cause-period** *cause-seconds*，可以设置告警的延迟上报周期。

使用参数 **clear-period** *clear-seconds*，可以设置恢复告警的延迟上报周期。

----结束

10.2.4 配置告警相关性抑制

设置告警相关性抑制后，系统将屏蔽衍生告警，只保留根源告警上报至网管。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **alarm**，进入告警管理视图。

步骤 3 执行命令 **correlation-analyze enable**，使能告警相关性分析功能。

缺省情况下，系统告警相关性抑制开关关闭。设置告警相关性抑制之前，请确保已经使能系统告警相关性分析功能。

步骤 4 执行以下命令，配置告警相关性抑制或屏蔽。

- 配置基于网管主机的告警相关性抑制。
 1. 执行命令 **quit**，返回系统视图。
 2. 执行命令 **alarm correlation-suppress enable [target-host ip-address securityname securityname [vpn-instance vpn-instance-name]]**，配置基于网管主机的告警相关性抑制。

缺省情况下，基于网管主机的告警相关性抑制开关处于打开状态，衍生告警不上报任何网管主机。关闭告警相关性抑制开关后，衍生告警将上报网管主机。

- 如果指定参数 **target-host**、**securityname securityname** 以及 **vpn-instance vpn-instance-name**，系统将不上报衍生告警至指定的网管主机。
- 如果不指定参数，系统将不上报衍生告警至所有网管主机。

- 配置基于接口的告警屏蔽。

执行命令 **mask interface interface-type interface-number**，配置基于接口的告警屏蔽。

缺省情况下，系统不对接口进行告警屏蔽。

配置了接口上的告警屏蔽后，该接口上产生的衍生告警将不上报网管。

----结束

10.2.5 检查配置结果

告警管理配置成功后，可以查看到告警的内容及注册信息。

前提条件

已完成告警管理的所有配置。

背景信息

- 使用 **display alarm active** 命令查看当前系统中的活动告警。
- 使用 **display alarm history** 命令查看系统中的历史告警。
- 使用 **display alarm information [name alarm-name]** 命令查看告警的注册信息。
- 使用 **display this** 命令查看告警延迟上报周期的信息。

任务示例

执行命令 **display alarm active**，可以看到当前的活动告警。例如：

```
<HUAWEI> display alarm active
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

1/RootCause/2010-7-8 17:38:46/-/0x502001/linkDown/Critical/Start/OID 1.3.6.1.6.3.1.1.5.3
Interface 5 turned into DOWN state.
```

执行命令 **display alarm history**，可以看到历史告警。例如：

```
<HUAWEI> display alarm history
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

3/Independent/2010-7-14 9:40:20/2010-7-14 9:40:23/0x502001/linkDown/Critical/End/0
ID 1.3.6.1.6.3.1.1.5.3 Interface 5 turned into DOWN state.
```

执行命令 **display alarm information [name alarm-name]**，可以看到告警的注册信息。例如：

```
<HUAWEI> display alarm information name linkup
*****
AlarmName: linkUp
AlarmType: Resume Alarm
AlarmLevel: Critical
Suppress Period: 10s
CauseAlarmName: linkDown
Match VB Name: ifIndex ifAdminStatus
*****
```

在告警管理视图下执行命令 **display this**，可以看到告警延迟上报周期的信息。例如：

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] display this
#
alarm
 suppression alarm-name hwElmiEvcStatusNotActiveFault0ccur cause-period 5
#
return
```

10.3 配置事件管理

配置事件管理后，可以配置事件类型，事件延迟上报。

10.3.1 建立配置任务

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

10.3.2 配置事件延迟上报

用户可以通过设置事件的延迟上报周期，来控制事件上报频率。

10.3.3 检查配置结果

事件管理配置成功后，可以查看到事件的内容及注册信息。

10.3.1 建立配置任务

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

应用环境

用户可以使用事件管理，对系统进行配置事件管理、调整事件级别、实现事件延迟上报等功能。

前置任务

在配置事件管理之前，需要完成以下任务：

- 路由器安装完毕并加电启动正常。

数据准备

在配置事件管理之前，需要准备以下数据。

序号	数据
1	事件名称
2	事件延迟上报周期

10.3.2 配置事件延迟上报

用户可以通过设置事件的延迟上报周期，来控制事件上报频率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **event**，进入事件管理视图。

步骤 3 执行命令 **delay-suppression enable**，打开事件延迟上报开关。

缺省情况下，事件延迟上报开关打开，对延迟上报周期内的事件进行抑制。

步骤 4 执行命令 **suppression event-name event-name period seconds**，设置事件延迟上报周期。

对某一事件设置了事件延迟上报周期后，在该周期内，系统中如果有同样的事件产生，则后产生的事件将被丢弃。延迟上报周期到达时，系统发送该事件。

----结束

10.3.3 检查配置结果

事件管理配置成功后，可以查看到事件的内容及注册信息。

前提条件

已完成事件管理的所有配置。

背景信息

- 使用 **display event** 命令查看事件的内容。
- 使用 **display event information [name event-name]** 命令查看事件的注册信息。
- 使用 **display this** 命令查看事件延迟上报周期的信息。

任务示例

执行命令 **display event**，可以看到当前系统中的事件。例如：

```
<HUAWEI> display event
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

1/Independent/2010-7-8 17:21:44/-/0x4055a000/hwCfgManEventlog/Warning/Start/OID
1.3.6.1.4.1.2011.6.10.2.1 Configure changed. (EventIndex=1, CommandSource=3, ConfigSource=4,
ConfigDestination=2)
```

执行命令 **display event information [name event-name]**，可以看到历史事件。例如：

```
<HUAWEI> display event information name hwcfgmaneventlog
*****
EventName: hwCfgManEventlog
EventType: Critical Event
EventLevel: Warning
Suppress Period: 3s
Match VB Name: hwCfgLogSrcCmd hwCfgLogSrcData hwCfgLogDesData
*****
```

在事件管理视图下执行命令 **display this**，可以看到事件延迟上报周期的信息。例如：

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event] display this
#
event
 suppression event-name hwelmivlannotcfg period 5
#
return
```

10.4 配置实体故障隔离

通过本节可以了解到配置实体故障隔离的应用环境、前置任务和操作步骤。用户可针对单板和灵活子卡配置实体故障隔离功能，立即给已经发生故障的单板或灵活子卡下电，使得故障第一时间得到处理。

应用环境

当单板和灵活子卡发生故障后，会使得对端设备连续丢包，影响用户业务的正常进行。用户可以配置实体故障隔离功能，对已经发生故障的单板或灵活子卡隔离下电。

前置任务

在配置实体故障隔离之前，需完成以下任务：

- 路由器上电，自检正常

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **entity-fault { board | card } isolate enable**，配置实体故障隔离功能。

缺省情况下，未使能单板或灵活子卡的故障隔离功能。

----结束

检查配置结果

执行 **display this** 命令查看单板或灵活子卡的故障隔离功能是否使能。

```
[HUAWEI] display this
#
  entity-fault board isolate enable
  entity-fault card isolate enable
#
return
```

显示信息加粗部分，表示单板和灵活子卡的故障隔离功能已经使能。

10.5 维护

本节主要讲述维护故障管理的方法。

10.5.1 清除告警信息

在确认需要清除告警信息后，请在告警管理视图下执行清除命令。

10.5.2 清除事件信息

在确认需要清除事件信息后，请在事件管理视图下执行清除命令。

10.5.1 清除告警信息

在确认需要清除告警信息后，请在告警管理视图下执行清除命令。

背景信息



注意

清除告警信息会导致网管无法以任何方式获取清空前的信息。务必仔细确认网管是否需要获取待清除的告警信息。

在日常维护工作中，可以在告警管理视图下选择执行以下命令，清除告警信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **alarm**，进入告警管理视图。

步骤 3 执行命令 **clear alarm active { all | sequence-number sequence-number }**，清除系统中的活动告警信息。

----结束

10.5.2 清除事件信息

在确认需要清除事件信息后，请在事件管理视图下执行清除命令。

背景信息



注意

清除事件信息会导致网管无法以任何方式获取清空前的信息。务必仔细确认网管是否需要获取待清除的事件信息。

在日常维护工作中，可以在事件管理视图下选择执行以下命令，清除事件信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **event**，进入事件管理视图。

步骤 3 执行命令 **clear event all**，清除系统中的事件信息。

----结束

10.6 配置举例

配置故障管理的应用示例。配置示例中包括组网需求、配置注意事项和配置思路等。

10.6.1 配置告警管理示例

配置告警管理的示例。在本示例中，通过配置告警的延迟上报和相关性抑制，屏蔽非关键告警。

10.6.1 配置告警管理示例

配置告警管理的示例。在本示例中，通过配置告警的延迟上报和相关性抑制，屏蔽非关键告警。

组网需求

用户登录到路由器进行告警管理。

配置注意事项

无

配置思路

采用如下思路配置告警管理的示例：

1. 配置告警参数。
2. 配置告警延迟上报。
3. 配置基于网管主机的告警相关性抑制。
4. 配置基于接口的告警屏蔽。

数据准备

为完成此配置例，需准备如下的数据：

- 告警的级别。
- 告警延迟上报周期。
- 网管主机 IP 地址、安全名及 VPN 实例名。
- 告警屏蔽的接口类型和接口编号。

操作步骤

步骤 1 配置 SNMPv3 用户和告警主机

具体配置 SNMPv3 用户和告警主机的步骤请参见“[SNMP 配置](#)”的相关内容。

步骤 2 设置 linkDown 的告警级别为 Major

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] alarm-name linkdown severity major
```

步骤 3 设置告警 linkDown 的延迟上报周期为 5 秒

```
[HUAWEI-alarm] delay-suppression enable
[HUAWEI-alarm] suppression alarm-name linkdown cause-period 5
```

步骤 4 设置 IP 地址是 192.168.3.1、网管侧用户名是 aa 的网管主机告警相关性抑制

```
[HUAWEI-alarm] correlation-analyze enable
[HUAWEI-alarm] quit
[HUAWEI] alarm correlation-suppress enable target-host 192.168.3.1 securityname aa
```


步骤 5 设置 GE1/0/1 接口上的告警屏蔽

```
[HUAWEI] alarm
[HUAWEI-alarm] filter interface gigabitethernet1/0/1
```

步骤 6 验证配置结果

配置完成之后，执行如下命令，查看告警信息。

```
<HUAWEI> display alarm information name linkdown
```

```
*****
AlarmName: linkDown
AlarmType: Alarm
AlarmLevel: Major
Suppress Period: 5s
CauseAlarmName: NA
Match VB Name: ifIndex ifAdminStatus
*****
```

可以看到 linkDown 的注册信息。

```
<HUAWEI> display alarm active
```

```
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

2/RootCause/2010-9-1 14:53:8/-/0x502001/linkDown/Critical/Start/OID 1.3.6.1.6.
3.1.1.5.3 Interface 5 turned into DOWN state.
3/nonRootCause/2010-9-1 14:53:8/-/0x701d2000/hwOspfV3IfStateChange/Major/Start
/OID 1.3.6.1.4.1.2011.5.25.147.0.8 The status of the non-virtual interface has c
hanged. (IfIndex=5, InstanceId=0, RouterId=185273099, IfState=1, ChgReason=8, If
Name=Ethernet0/0/1)/RootCauseSequence: (2)
4/nonRootCause/2010-9-1 14:53:8/-/0x701d2002/hwOspfV3NbrStateChange/Major/Sta
rt/OID 1.3.6.1.4.1.2011.5.25.147.0.2 The status of the non-virtual neighbor has c
hanged. (IfIndex=5, InstanceId=0, NbrRouterId=16843009, RouterId=185273099, NbrS
tate=1, ChgReason=12, IfName=Ethernet0/0/1)/RootCauseSequence: (3)
```

可以看到 linkDown 是根源告警，hwOspfV3IfStateChange 是衍生告警。

----结束

配置文件

```
#
sysname HUAWEI
#
snmp-agent
snmp-agent local-engineid 800007DB0300E000030003CA
snmp-agent sys-info version all
snmp-agent group v3 huawei
snmp-agent target-host trap address udp-domain 10.164.9.211 params securityname
user v3
snmp-agent usm-user v3 user huawei
snmp-agent trap enable feature-name CONFIGURATION trap-name linkDown
#
alarm
alarm-name linkDown severity major
suppression alarm-name linkDown cause-period 5
correlation-analyze enable
filter interface GigabitEthernet1/0/1
#
return
```


A 术语

列出了本手册中使用的术语，及对应的英文全称和中文解释。

C

clock offset	时钟偏移量指将本地时钟调节到与所选参考时钟一致所要调节的量。

D

多选	同时选定多个小方框。

F

服务代码	在使用 SM 方式的点播类业务中提供给用户点播的内容/应用提供商代码。

G

关键词	描述产品的特征，关键词之间用 分开添加产品信息时，产品的名称和作者会作为关键词出现在关键词一栏。

J

Jitter	报文的抖动时间。相邻报文到达相同目的地址，发送报文的时间差与接收报文的时间差的差值，是衡量网络性能的一个重要参数。

M

MD	Multicast Domains，也称为组播域，是组播 VPN 的实现方案。MD 方案仅需要 PE 支持多实例，对于 CE 和 P 是透明的。MD 表示各个 PE 上，能够互相发送和接收组播报文的所有 VPN 实例组成的集合。不同的 VPN 实例属于不同的 MD。一个 MD 为一个特定的 VPN 服务，在该 VPN 中传输的所有私网组播数据，都在此 MD 内传输。
N	
NetStream	NetStream 是网络流量统计工具。可以对网络中的通信量和资源使用情况进行分类和统计，实现对各种业务和不同的 QoS 进行管理和计费。
P	
Ping	Ping（Packet Internet Groper）命令主要用于检查网络连接及主机是否可达。源主机向目的主机发送 ICMP 请求报文，目的主机向源主机发送 ICMP 回应报文。
PWE3	在分组交换网络 PSN 中尽可能真实地模仿 ATM、帧中继、以太网、低速 TDM 电路和 SONET/SDH 等业务的基本行为和特征的一种二层业务承载技术。
Q	
企业代码	网络中公司地址和身份的标识、地址翻译、计费、结算等均以企业代码为依据。
R	
roundtrip delay	往返延迟规定了本地时钟在指定时间内将一条信息发送到参考时钟的能力。
T	
Tracert	tracert 命令用于测试数据包从发送主机到目的地所经过的网关，它主要检查网络连接是否可达，以及分析网络什么地方发生了故障。
Y	
业务代码	业务代码表示业务类别，由内容/应用服务提供商自己制定，由字母或数字组成（其中字母大小写均可），长度最大为 10 位。

B 缩略语

列出了本手册中使用的缩略语，及对应的英文全称和中文解释。

3

3DES	Triple Data Encryption Standard	三重数据加密标准

A

AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ADSL	Asymmetric Digital Subscriber Line	非/不对称数字用户线路
AH	Authentication Header	验证头
APPN	Advanced Peer-to-Peer Networking	高级点对点连网
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System; Access Server	自治系统；接入服务器
ASCII	American Standard Code for Information Interchange	美国信息交换标准码
ASPF	Application Specific Packet Filter	基于应用层状态的包过滤防火墙
ATM	Asynchronous Transfer Mode	异步传输模式
AUX	Auxiliary (port)	备份口

B

BGP	Border Gateway Protocol	边界网关协议
BRI	Basic Rate Interface	基本速率接口
C		
CBQ	Class Based Queue	基于类的队列
CD	Carrier Detect	载波检测
CHAP	Challenge Handshake Authentication Protocol	盘问握手验证协议
CON	Console (port)	控制台端口
cPOS	channelized-POS	通道化的 POS
CQ	Custom Queueing	定制队列
CRC	Cyclic Redundancy Check	循环冗余校验（法）
D		
DCC	Data Communication Channel	数据通信信道
DCE	Data Circuit-terminating Equipment	数据电路终接设备
DD	Database Description	数据库描述
DES	Data Encryption Standard	数据加密标准
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
DOD	Downstream-on-Demand	下游按需标签分配
DOS	Denial of Service	拒绝服务
DTE	Data Terminal Equipment	数据终端设备
DU	Downstream Unsolicited	下游自主标签分配
E		
EIA	Electronics Industry Association	电子工业协会
ESP	Encapsulating Security Payload	封装安全载荷
F		

FEC	Forward Error Correction	前向纠错
FIFO	First In First Out	先入先出
FLASH	FLASH memory	闪存存储器/闪存
FR	Frame Relay	帧中继
FRR	Fast Reroute	快速重路由
FTP	File Transfer Protocol	文件传输协议
G		
GE	Gigabit Ethernet	千兆比特以太网
GNS	Get Nearest Server	请求最近的服务器
GRE	Generic Routing Encapsulation	通用路由封装协议
H		
HDLC	High level Data Link Control	高级数据链路控制（规程）
HTTP	Hyper Text Transport Protocol	超级文本传送协议
I		
IBGP	Internal BGP	域内 BGP
ICMP	Internet Control Message Protocol	因特网控制消息协议
ID	IDentification	识别
IETF	Internet Engineering Task Force	因特网工程任务组
IF	Information Frame	信息帧
IGP	Interior Gateway Protocol	内部网关协议
IKE	Internet Key Exchange	因特网密钥交换协议
IP	Internet Protocol	互联网协议
IPHC	IP Header compression	IP 头压缩
IPoA	Internet Protocols over ATM	ATM 承载 IP 协议
IPoEoA	IP over Ethernet over AAL5	AAL5 上承载以太网帧
IPSec	Internet Protocol SECurity extensions	IP 协议安全扩展

ISDN	Integrated Services Digital Network	综合业务数字网
IS-IS	Intermediate System-Intermediate System	中间系统到中间系统
ISP	Internet Service Provider	因特网服务运营商
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	国际电信联盟-电信标准部
L		
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
L2VPN	Layer 2 VPN	二层 VPN
L3VPN	Layer 3 VPN	三层 VPN
LAN	Local Area Network	局域网
LDP	Label Distribution Protocol	标签分发协议
LLC2	Logical Link Control, Type 2	第二类逻辑链路控制
LOG	Call Logging	呼叫登录
LR	Limit Rate	接口限速
LSP	Label Switch Path	标签交换路径
LSPAGENT	Label Switch Path Agent	LSP 代理
LSPM	Label Switch Path Management	LSP 管理
M		
MAC	Medium Access Control	介质访问控制
MD5	Message Digest 5	一种 Hash 算法
MFR	Multiple Frame Relay	多帧中继接口
MIB	Management Information Base	管理信息库
MODEM	Modulator DEModulator	调制解调器
MPLS	Multi-Protocol Label Switching	多协议标签交换
MSDP	Multicast Source Discovery Protocol	组播源发现协议
MTU	Maximum Transmission Unit	最大传输单元

N

NAT	Network Address Translation	网络地址转换（板）
NDA	NetStream Data Analyzer	网络流数据分析器
NetBIOS	Network Basic Input/Output System	网络基本输入/输出系统
NLRI	Network Layer Reachable Information	网络层可达信息
NMS	Network Management System	网络管理系统
NQA	Network Quality Analysis	网络质量分析
NRZ	Non Return to Zero	非归零码
NRZI	Non Return to Zero Inverted	不归零反转
NSC	NetStream Collector	网络流数据收集器
NTP	Network Time Protocol	网络时间协议

O

OSI	Open System Interconnection	开放系统互连（模型）
OSPF	Open Shortest Path First	开放最短路径优先

P

PAD	Packet Assembler/Disassembler	报文分组组装器/拆卸器
PAP	Password Authentication Protocol	密码验证协议
PC	Personal Computer	个人计算机
PDU	Protocol Data Unit	协议数据单元
PHY	Physical Sublayer & Physical Layer	物理子层，物理层
POS	Packet Over SDH/SONET	SDH/SONET 承载包
PPP	Point-to-Point Protocol	点到点协议
PPPoA	PPP over ATM	ATM 网承载 PPP 协议
PPPoE	PPP over Ethernet	以太网承载 PPP 协议
PQ	Priority Queue	优先队列
PRI	Primary Rate Interface	基群速率接口

PSTN	Public Switched Telephone Network	公用交换电话网
PU	Payload Unit	净负载单元
PVC	Permanent Virtual Circuit	永久虚电路
Q		
QoS	Quality of Service	服务质量
R		
RADIUS	Remote Authentication Dial in User Service	远端用户拨入鉴权服务
REJ	REJect(ion)	拒绝
RFC	Request for Comments	请求评议
RIP	Routing Information Protocol	路由信息协议
RM	Resource Management	资源管理
RMON	remote network monitoring	远端监视
RSA	Revest, Shamir and Adleman	RSA 加密系统
RTT	Round Trip Time	环回往返时间
S		
SAP	Service Advertising Protocol	服务公告协议
SDLC	Synchronous Data Link Control	同步数据链路控制
SLIP	Serial Line Internet Protocol	串行线路因特网协议
SLA	Service Level Agreement	服务等级协议
SNA	Systems Network Architecture	系统网络结构体系
SNAP	Sub Network Access Point	子网接入点
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSP	Service Switching Point	业务交换点
STM-1	SDH Transport Module -1	SDH 传输模块 -1
T		

TCP	Transmission Control Protocol	传输控制协议
TE	Traffic Engineering	流量工程
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TOS	Type of Service	服务类型
TTL	Time To Live	生存时间
U		
UDP	User Datagram Protocol	用户数据报协议
URL	Universal Resource Locator;	通用资源定位器
USM	User Security Mode	用户安全模型
UTC	Universal Coordinated Time	国际协调时间
V		
VACM	View-based Access Control Model	基于视图的访问控制模型
VIU	Versatile Interface Unit	通用接口单元
VLAN	Virtual Local Area Network	虚拟局域网
VOS	Virtual Operating System	虚拟操作系统
VPDN	Virtual Private Dial Network	虚拟私有拨号网
VPN	Virtual Private Network	虚拟专用网
VRP	Versatile Routing Platform	通用路由平台
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议
W		
WAN	Wide Area Network	广域网
WFQ	Weighted Fair Queuing	加权公平排队
WRED	Weighted Random Early Detection	加权随机早期检测
WWW	World Wide Web	全球超媒体信息网（万维网）
X		
XOT	X.25 Over TCP	TCP 承载 X.25 报文

