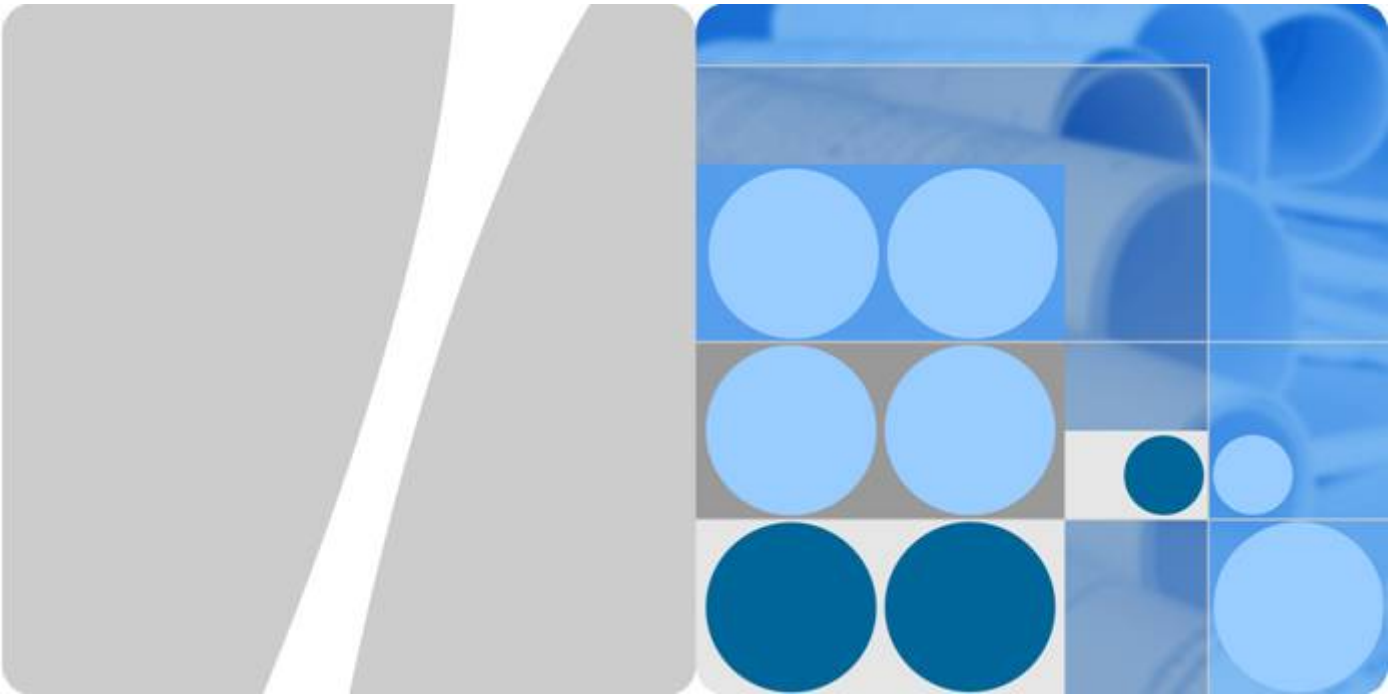


Huawei AR2200-S 系列企业路由器

V200R001C01

配置指南-局域网

文档版本　01

发布日期　2012-01-06

华为技术有限公司

商标声明


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： 4008302118

前 言

读者对象

本文档介绍了 AR2200-S 中局域网的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了以太网的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 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。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

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 (2012-01-06)

第一次正式发布。

目 录

1 链路聚合配置

关于本章

介绍链路聚合的基础知识、配置方法和配置实例。

1.1 链路聚合概述
简要介绍链路聚合的基本概念。

1.2 AR2200-S 支持的链路聚合特性
介绍链路聚合特性在 AR2200-S 中的支持情况。

1.3 配置手工负载分担模式链路聚合
介绍了手工负载分担模式链路聚合配置场景、步骤及注意事项。

1.4 配置静态 LACP 模式链路聚合
介绍了静态 LACP 模式链路聚合配置场景、步骤及注意事项。

1.5 维护
清除 LACP 统计信息、调试链路聚合组、监控链路聚合组运行状况。

1.6 配置举例
介绍了手工负载分担模式和静态 LACP 模式下的典型应用场景举例。

1.1 链路聚合概述

简要介绍链路聚合的基本概念。

链路聚合（Link Aggregation）是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽的一种方法，又称为多接口负载均衡组（Load Sharing Group）或链路聚合组（Link Aggregation Group），相关的协议标准请参考 IEEE802.3ad。

通过在两台设备之间建立链路聚合组，可以提供更高的通讯带宽和更高的可靠性。链路聚合不仅为设备间通信提供了冗余保护，而且不需要对硬件进行升级。

1.2 AR2200-S 支持的链路聚合特性

介绍链路聚合特性在 AR2200-S 中的支持情况。

手工负载分担模式

手工负载分担模式允许在聚合组中手工加入多个成员接口，所有的接口均处于转发状态，分担负载的流量。AR2200-S 支持的负载分担方式包括目的 MAC、源 MAC、源 MAC 异或目的 MAC、源 IP、目的 IP、源 IP 异或目的 IP。

Eth-Trunk 的创建、成员接口的加入都需要手工配置完成，没有 LACP（link Aggregation Control Protocol）协议报文的参与。

手工负载分担模式通常应用在对端设备不支持 LACP 协议的情况下。

静态 LACP 模式

静态 LACP 模式是一种利用 LACP 协议进行聚合参数协商、确定活动接口和非活动接口的链路聚合方式。该模式下，需手工创建 Eth-Trunk，手工加入 Eth-Trunk 成员接口，由 LACP 协议协商确定活动接口和非活动接口。

静态 LACP 模式也称为 M：N 模式。这种方式可以同时实现链路负载分担和链路冗余备份的双重功能。在链路聚合组中 M 条链路处于活动状态，这些链路负责转发数据并进行负载分担，另外 N 条链路处于非活动状态作为备份链路，不转发数据。当 M 条链路中有链路出现故障时，系统会从 N 条备份链路中选择优先级最高的接替出现故障的链路，同时这条替换故障链路的备份链路状态变为活动状态开始转发数据。

静态 LACP 模式与手工负载分担模式的主要区别为：静态 LACP 模式有备份链路，而手工负载分担模式所有成员接口均处于转发状态，分担负载流量。

和静态 LACP 模式相对应的还包括动态 LACP 模式。动态 LACP 模式的链路聚合，从 Eth-Trunk 的创建到加入成员接口都不需要人工的干预，由 LACP 协议自动协商完成。虽然这种方式对于用户来说很简单，但由于这种方式过于灵活，不便于管理，所以 AR2200-S 上不支持动态 LACP 模式链路聚合。

活动接口与非活动接口

处于活动状态并负责转发数据的接口称作活动接口。相反，处于非活动状态禁止转发数据的接口称作非活动接口。根据配置的工作模式不同，角色分工如下：

- 手工负载分担模式。正常情况下，所有的成员接口均为活动接口，除非这些接口出现链路故障。
- 静态 LACP 模式。M 条链路对应的接口为活动接口负责转发数据，N 条链路对应的接口为非活动接口负责冗余备份。

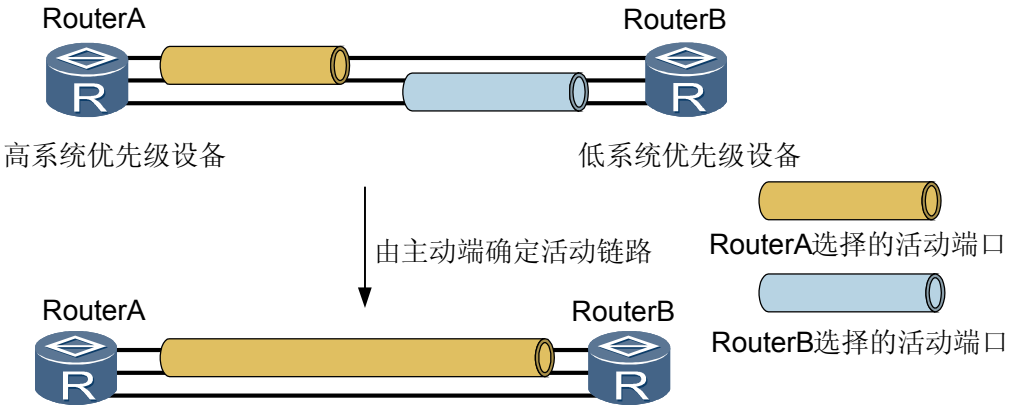
主动端与被动端

在静态 LACP 模式下，聚合组两端的设备中 LACP 优先级较高的一端为主动端，LACP 优先级较低的一端为被动端。

如果两端设备的 LACP 优先级一样时，需要按照系统 MAC 来选择主动端，系统 MAC 小的一端优先。

区分主动端与被动端的目的是为了保证两端设备最终确定的活动接口一致，如果两端都按照本端各自的接口优先级来选择活动接口，两端所确定的活动接口很可能不一致，活动链路也就无法建立。因此首先确定主动端，被动端按照主动端侧的接口优先级来选择活动接口。如图 1-1 所示。

图 1-1 静态 LACP 模式下主动端确定活动链路



1.3 配置手工负载分担模式链路聚合

介绍了手工负载分担模式链路聚合配置场景、步骤及注意事项。

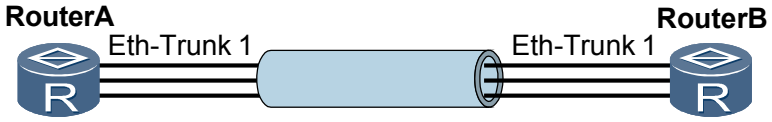
1.3.1 建立配置任务

应用环境

当需要增加两台设备之间的带宽或可靠性，而两台设备中有一台不支持 LACP 协议时，可在 Router 设备上创建手工负载分担模式的 Eth-Trunk，并加入多个成员接口增加设备间的带宽及可靠性。

如图 1-2 所示，RouterA 和 RouterB 之间创建 Eth-Trunk。

图 1-2 手工负载分担模式链路聚合组网图



前置任务

在配置手工负载分担模式链路聚合之前，需完成以下任务：

- 设备正常上电。
- 创建 Eth-Trunk。

数据准备

在配置手工负载分担模式链路聚合之前，需准备以下数据。

序号	数据
1	负载分担模式 Eth-Trunk 的编号
2	成员接口的类型和编号

1.3.2 创建 Eth-Trunk 接口

背景信息

Eth-Trunk 接口可以分为二层 Eth-Trunk 接口和三层 Eth-Trunk 接口，都可以增加带宽、提高可靠性，根据网络中的应用来选择配置二层 Eth-Trunk 接口还是三层 Eth-Trunk 接口。

操作步骤

- 配置二层 Eth-Trunk 接口。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，创建二层 Eth-Trunk 接口。

     缺省情况下，Eth-Trunk 接口处于二层模式。
- 配置三层 Eth-Trunk 接口。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，创建二层 Eth-Trunk 接口。
  3. 执行命令 **undo portswitch**，配置三层 Eth-Trunk 接口。
  4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置三层 Eth-Trunk 接口的 IP 地址。
  5. （可选）执行命令 **mtu** *mtu*，配置三层 Eth-Trunk 接口的 MTU 值。

最大传输单元 MTU（Maximum Transmission Unit）单位为字节，缺省情况下，接口的 MTU 值为 1500。

注意

- 二层 Eth-Trunk 接口下不能配置 **mtu** 命令。
- 直连链路两端接口上的 MTU 值需要一致。如果使用 **mtu** 命令改变接口 MTU 的值，请同时修改与本设备相连的其他设备的 MTU 值，确保两端设备的 MTU 值匹配。否则，可能导致业务中断。
- 使用 **mtu** 命令改变接口最大传输单元 MTU 后，需要重启接口以保证配置的 MTU 生效。先执行 **shutdown** 命令将接口关闭，再执行 **undo shutdown** 命令将接口开启。

----结束

1.3.3 配置 Eth-Trunk 工作模式为手工负载分担模式

背景信息

说明

改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。删除已存在的成员接口请在相应接口视图下执行命令 **undo eth-trunk** 或在 Eth-Trunk 视图下执行命令 **undo trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>。

在需要配置手工负载分担模式 Eth-Trunk 的 AR2200-S 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 eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **mode manual load-balance**，配置当前 Eth-Trunk 工作模式为手工负载分担模式。

缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

如果本端配置手工负载分担模式，则对端设备也必须配置手工负载分担模式。

----结束

1.3.4 向 Eth-Trunk 中加入成员接口

背景信息

在需要配置 Eth-Trunk 成员接口的 AR2200-S 上进行如下配置。

操作步骤

- 在 Eth-Trunk 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>，增加成员接口。
- 在成员接口视图下
  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 **eth-trunk** *trunk-id*，将当前接口加入 Eth-Trunk。

  将成员接口加入 Eth-Trunk 时，需要注意以下问题：
  - 二层 Eth-Trunk 接口下的成员口必须为二层接口，三层 Eth-Trunk 接口下的成员口必须为三层接口。
  - 每个 Eth-Trunk 接口下最多可以包含 8 个成员接口。
  - 成员接口不能配置任何业务和静态 MAC 地址。
  - 成员接口加入 Eth-Trunk 时，必须为缺省的 hybrid 类型接口。
  - Eth-Trunk 接口不能嵌套，即成员接口不能是 Eth-Trunk。
  - 一个以太网接口只能加入到一个 Eth-Trunk 接口，如果需要加入其它 Eth-Trunk 接口，必须先退出原来的 Eth-Trunk 接口。
  - 一个 Eth-Trunk 接口中的成员接口必须是同一类型，例如：FE 口和 GE 口不能加入同一个 Eth-Trunk 接口。
  - 可以将不同接口板上的以太网接口加入到同一个 Eth-Trunk。
  - 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。
  - 当成员接口的速率不一致时，实际使用中速率小的接口可能会出现拥塞，导致丢包。
  - 当成员接口加入 Eth-Trunk 后，学习 MAC 地址时是按照 Eth-Trunk 来学习的，而不是按照成员接口来学习。

----结束

1.3.5 （可选）配置负载分担方式

背景信息

在需要配置 Eth-Trunk 负载分担方式的 AR2200-S 上进行如下配置。

操作步骤

- 对于二层 Eth-trunk 接口：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

  缺省情况下，二层 Eth-Trunk 接口的负载分担模式为 **src-dst-mac**。

Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

说明

目前二层 Eth-Trunk 接口的负载分担模式为全局模式配置，即所有的 Eth-Trunk 接口只能选择同时支持一种负载分担模式。

- 对于三层 Eth-trunk 接口：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

  缺省情况下，三层 Eth-Trunk 接口的负载分担模式为 **src-dst-ip**。

  Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

----结束

1.3.6 （可选）配置活动接口数阈值

背景信息

在需要配置活动接口数阈值的 AR2200-S 上进行如下配置。

操作步骤

- 配置链路聚合带宽的上限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **max bandwidth-affected-linknumber** *link-number*，配置影响链路聚合带宽的接口数上限阈值。

     缺省情况下，链路聚合带宽的上限阈值为 8。

  说明

  - 本端 AR2200-S 设备和对端 AR2200-S 设备的链路聚合带宽的上限阈值可以不同。如果两端配置链路聚合带宽的上限阈值不同，则以上限阈值数值较小的一端为准。
- 配置活动接口数下限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **least active-linknumber** *link-number*，配置活动接口数下限阈值。

     缺省情况下，活动接口数下限阈值为 1。

  配置手工模式活动接口数目下限阈值可以决定 Eth-Trunk 中活动接口数的最小值，如果手工模式下活动接口数目小于该值，Eth-Trunk 的接口状态将变为 DOWN 的状态。

说明

- 本端 AR2200-S 设备和对端 AR2200-S 设备的活动接口数下限阈值可以不同。如果下限阈值不同，以下限阈值数值较大的一端为准。

----结束

1.3.7 检查配置结果

操作步骤

- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口。
- 使用命令 **display eth-trunk** [*trunk-id*]查看 Eth-Trunk 的手工负载分担模式。

----结束

任务示例

如果配置正确，执行命令 **display trunkmembership eth-trunk** 能够看到 Eth-Trunk 的工作模式显示为“Normal”、成员接口数量，成员接口 UP 的数量以及成员接口的信息。

```
<Huawei> display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 0
Operate status: down

Interface Ethernet2/0/1, valid, operate down, weight=1
Interface Ethernet2/0/2, valid, operate down, weight=1
```

执行命令 **display eth-trunk** 查看 Eth-Trunk 的负载分担方式。缺省的情况下，二层 Eth-Trunk 负载分担方式应该显示为“SA-XOR-DA”。

```
<Huawei> display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: down        Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
PortName                Status      Weight
Ethernet2/0/1           Down        1
Ethernet2/0/2           Down        1
```

1.4 配置静态 LACP 模式链路聚合

介绍了静态 LACP 模式链路聚合配置场景、步骤及注意事项。

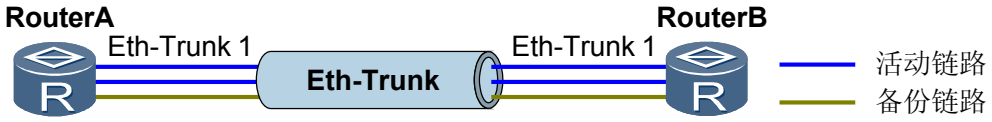
1.4.1 建立配置任务

应用环境

在两台直接相连 Router 设备上配置链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

- 两设备间的链路具有冗余备份的能力，当部分链路故障时使用备份链路替代故障链路，保持数据传输的不中断。
- 活动链路具有负载分担的能力。

图 1-3 静态 LACP 模式链路聚合组网图



前置任务

在配置手工负载分担模式链路聚合之前，需完成以下任务：

- 设备正常上电。
- 创建 Eth-Trunk。

数据准备

在配置静态 LACP 模式链路聚合的基本功能之前，需要准备以下数据。

序号	数据
1	Eth-Trunk 的编号
2	成员接口的类型和编号
3	活动接口上限阈值

1.4.2 创建 Eth-Trunk 接口

背景信息

Eth-Trunk 接口可以分为二层 Eth-Trunk 接口和三层 Eth-Trunk 接口，都可以增加带宽、提高可靠性，根据网络中的应用来选择配置二层 Eth-Trunk 接口还是三层 Eth-Trunk 接口。

操作步骤

- 配置二层 Eth-Trunk 接口。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，创建二层 Eth-Trunk 接口。

     缺省情况下，Eth-Trunk 接口处于二层模式。
- 配置三层 Eth-Trunk 接口。
  1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface eth-trunk** *trunk-id*，创建二层 Eth-Trunk 接口。
3. 执行命令 **undo portswitch**，配置三层 Eth-Trunk 接口。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置三层 Eth-Trunk 接口的 IP 地址。
5. （可选）执行命令 **mtu** *mtu*，配置三层 Eth-Trunk 接口的 MTU 值。

   最大传输单元 MTU（Maximum Transmission Unit）单位为字节，缺省情况下，接口的 MTU 值为 1500。

注意

- 二层 Eth-Trunk 接口下不能配置 **mtu** 命令。
- 直连链路两端接口上的 MTU 值需要一致。如果使用 **mtu** 命令改变接口 MTU 的值，请同时修改与本设备相连的其他设备的 MTU 值，确保两端设备的 MTU 值匹配。否则，可能导致业务中断。
- 使用 **mtu** 命令改变接口最大传输单元 MTU 后，需要重启接口以保证配置的 MTU 生效。先执行 **shutdown** 命令将接口关闭，再执行 **undo shutdown** 命令将接口开启。

----结束

1.4.3 配置 Eth-Trunk 的工作模式为静态 LACP 模式

背景信息

说明

改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。删除已存在的成员接口请在相应接口视图下执行命令 **undo eth-trunk** 或在 Eth-Trunk 视图下执行命令 **undo trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>。

在需要配置静态 LACP 模式 Eth-Trunk 的 AR2200-S 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 eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **mode lacp-static**，配置 Eth-Trunk 的工作模式为静态 LACP 模式。

缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

如果本端配置静态 LACP 模式，则对端设备也必须配置静态 LACP 模式。

----结束

1.4.4 向 Eth-Trunk 中加入成员接口

背景信息

在需要配置 Eth-Trunk 成员接口的 AR2200-S 上进行如下配置。

操作步骤

- 在 Eth-Trunk 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>，增加成员接口。
- 在成员接口视图下
  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 **eth-trunk** *trunk-id*，将当前接口加入 Eth-Trunk。

  将成员接口加入 Eth-Trunk 时，需要注意以下问题：
  - 二层 Eth-Trunk 接口下的成员口必须为二层接口，三层 Eth-Trunk 接口下的成员口必须为三层接口。
  - 每个 Eth-Trunk 接口下最多可以包含 8 个成员接口。
  - 成员接口不能配置任何业务和静态 MAC 地址。
  - 成员接口加入 Eth-Trunk 时，必须为缺省的 hybrid 类型接口。
  - Eth-Trunk 接口不能嵌套，即成员接口不能是 Eth-Trunk。
  - 一个以太网接口只能加入到一个 Eth-Trunk 接口，如果需要加入其它 Eth-Trunk 接口，必须先退出原来的 Eth-Trunk 接口。
  - 一个 Eth-Trunk 接口中的成员接口必须是同一类型，即 FE 口和 GE 口不能加入同一个 Eth-Trunk 接口。
  - 可以将不同接口板上的以太网接口加入到同一个 Eth-Trunk。
  - 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。
  - 当成员接口的速率不一致时，实际使用中速率小的接口可能会出现拥塞，导致丢包。
  - 当成员接口加入 Eth-Trunk 后，学习 MAC 地址时是按照 Eth-Trunk 来学习的，而不是按照成员接口来学习。

----结束

1.4.5 （可选）配置负载分担方式

背景信息

在需要配置 Eth-Trunk 负载分担方式的 AR2200-S 上进行如下配置。

操作步骤

- 对于二层 Eth-trunk 接口：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

缺省情况下，二层 Eth-Trunk 接口的负载分担模式为 **src-dst-mac**。

Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

说明

目前二层 Eth-Trunk 接口的负载分担模式为全局模式配置，即所有的 Eth-Trunk 接口只能选择同时支持一种负载分担模式。

- 对于三层 Eth-trunk 接口：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }，配置 Eth-Trunk 的负载分担模式。

  缺省情况下，三层 Eth-Trunk 接口的负载分担模式为 **src-dst-ip**。

  Eth-Trunk 的负载分担是逐流进行的，本端与对端的负载分担模式可以不一致，两端互不影响。

----结束

1.4.6 （可选）配置活动接口数阈值

背景信息

在需要配置活动接口数阈值的 AR2200-S 上进行如下配置。

操作步骤

- 配置活动接口数上限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。
  3. 执行命令 **max active-linknumber** *link-number* ，配置链路聚合活动接口数上限阈值。

  配置静态 LACP 模式活动接口数目上限阈值可以控制 Eth-Trunk 中活动接口的最大数 M，剩余的成员接口处于备份状态。

  如果未配置上限阈值，Eth-Trunk 最多允许 8 个接口同时处于活动状态。

  说明

  - 活动接口数上限阈值必须大于等于活动接口数下限阈值。
  - 本端 AR2200-S 设备和对端 AR2200-S 设备的活动接口数上限阈值可以不同。如果两端配置活动接口数的上限阈值不同，则以上限阈值数值较小的一端为准。
- 配置活动接口数下限阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

3. 执行命令 **least active-linknumber** *link-number*，配置链路聚合活动接口数下限阈值。

   缺省情况下，活动接口数下限阈值为 1。

配置静态 LACP 模式活动接口数目下限阈值可以决定 Eth-Trunk 中活动接口数的最小值，如果静态模式下活动接口数目小于该值，Eth-Trunk 的接口状态将变为 DOWN 的状态。

说明

- 活动接口数下限阈值必须小于等于活动接口数上限阈值。
- 本端 AR2200-S 设备和对端 AR2200-S 设备的活动接口数下限阈值可以不同。如果下限阈值不同，以下限阈值数值较大的一端为准。

----结束

1.4.7 （可选）配置系统 LACP 优先级

背景信息

在需要配置系统 LACP 优先级的 AR2200-S 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 **lacp priority** *priority*，配置当前 AR2200-S 设备的系统 LACP 优先级。

系统 LACP 优先级值越小优先级越高，缺省情况下，系统 LACP 优先级为 32768。

在两端设备中选择系统 LACP 优先级较小一端作为主动端，如果系统 LACP 优先级相同则选择 MAC 地址较小的一端作为主动端。

----结束

1.4.8 （可选）配置接口 LACP 优先级

背景信息

在需要配置接口 LACP 优先级的 AR2200-S 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** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **lacp priority** *priority*，配置当前接口的 LACP 优先级。

缺省情况下，接口的 LACP 优先级是 32768。

----结束

1.4.9 （可选）使能 LACP 抢占并配置抢占等待时间

背景信息

在需要配置 LACP 抢占的 AR2200-S 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 eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **lacp preempt enable**，使能当前 Eth-Trunk 接口的 LACP 抢占功能。

缺省情况下，LACP 抢占功能处于禁止状态。

说明

为保证 Eth-Trunk 正常工作，要求 Eth-Trunk 两端统一配置使能 LACP 抢占或不使能 LACP 抢占。

步骤 4 执行命令 **lacp preempt delay** *delay-time*，配置当前 Eth-Trunk 接口的 LACP 抢占等待时间。

缺省情况下，LACP 抢占等待时间为 30 秒。

使能 LACP 抢占功能可以保持接口 LACP 优先级最高的接口为活动接口。例如：当一条高优先级的接口因故障切换为非活动状态而后又恢复时，如果使能了抢占，则高优先级的接口将重新成为活动接口；如果未使能抢占，该接口不能重新成为活动接口。

抢占等待时间是指在静态 LACP 模式的 Eth-Trunk 中非活动接口切换为活动接口需要等待的时间。

----结束

1.4.10 （可选）配置接收 LACP 协议报文超时时间

背景信息

在需要配置接收 LACP 协议报文超时时间的 AR2200-S 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 eth-trunk** *trunk-id*，进入 Eth-Trunk 接口视图。

步骤 3 执行命令 **lacp timeout** { **fast** | **slow** }，配置当前接口接收 LACP 协议报文的超时时间。

说明

- 配置此命令后，本端将接收报文的超时时间通过 LACP 报文通知对端。配置为 **fast**，对端发送 LACP 报文的周期为 1 秒。配置为 **slow**，对端发送 LACP 报文的周期为 30 秒。
- LACP 协议报文的超时时间为 LACP 报文发送周期的 3 倍，即：配置为 **fast**，接收 LACP 协议报文的超时时间为 3 秒。配置为 **slow**，接收 LACP 协议报文的超时时间为 90 秒。
- 两端配置的超时时间可以不一致。但为了便于维护，建议用户配置一致的 LCAP 协议报文超时时间。

----结束

1.4.11 检查配置结果

操作步骤

- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口。
- 使用命令 **display eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 查看 Eth-Trunk 信息、活动接口信息以及非活动接口信息。

----结束

任务示例

如果配置正确，执行命令 **display trunkmembership eth-trunk** 能够看到 Eth-Trunk 的工作模式显示为“Static”、成员接口数量，成员接口 UP 的数量以及成员接口的信息。

```
<Huawei> display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Static
Number Of Ports in Trunk = 3
Number Of UP Ports in Trunk = 0
operate status: down
Interface Ethernet2/0/1, valid, operate down, weight=1
Interface Ethernet2/0/2, valid, operate down, weight=1
Interface Ethernet2/0/3, valid, operate down, weight=1
```

通过 **display eth-trunk** 查看 Eth-Trunk 的静态链路聚合方式。配置正确的情况下，静态链路聚合方式应该显示为“STATIC”。

```
<Huawei> display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SIP-XOR-DIP
System Priority: 50         System ID: 000b-09d3-dc62
Least Active-linknumber: 3  Max Active-linknumber: 8
Operate status: down        Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName          Status   PortType PortPri PortNo PortKey PortState  Weight
Ethernet2/0/1          Unselect 100M     10      1547   561     11100000  1
Ethernet2/0/2          Unselect 100M     32768   1548   561     11100010  1
Ethernet2/0/3          Unselect 100M     32768   1549   561     11100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri    SystemID  PortPri PortNo  PortKey   PortState
Ethernet2/0/1          0      0000-0000-0000  0      0      0         11100000
Ethernet2/0/2          0      0000-0000-0000  0      0      0         11100011
Ethernet2/0/3          0      0000-0000-0000  0      0      0         11100011
```

1.5 维护

清除 LACP 统计信息、调试链路聚合组、监控链路聚合组运行状况。

1.5.1 清除 LACP 统计信息

背景信息

注意

清除 LACP 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 在用户视图下使用命令 **reset lacp statistics eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 清除 LACP 收发报文的统计信息。

----结束

1.5.2 调试链路聚合组

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，应及时执行命令 undo debugging all 关闭调试开关。

当链路聚合组出现运行故障时，请在用户视图下执行命令 **debugging** 对链路聚合进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

- 使用命令 **debugging trunk error** 打开 Eth-Trunk 差错信息调试开关。
- 使用命令 **debugging trunk event** 打开 Eth-Trunk 事件通知调试开关。
- 使用命令 **debugging trunk lacp-pdu** 打开 LACP 报文调试开关。
- 使用命令 **debugging trunk lagmsg** 打开 LACP 协议消息调试开关。
- 使用命令 **debugging trunk msg** 打开 Eth-Trunk 消息调试开关。
- 使用命令 **debugging trunk state-machine** 打开 Eth-Trunk 状态机调试开关。
- 使用命令 **debugging trunk updown** 打开 Eth-TrunkUp/Down 信息调试开关。
- 使用命令 **debugging trunk** 打开 Eth-Trunk 信息调试开关。

----结束

1.5.3 监控链路聚合组运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解链路聚合组的运行状况。

操作步骤

- 使用命令 **display eth-trunk** 查看链路聚合组状态信息。
- 使用命令 **display lacp statistics eth-trunk** [*trunk-id* [**interface** *interface-type interface-number*]] 查看 LACP 收发报文统计信息。
- 使用命令 **display trunkmembership eth-trunk** *trunk-id* 查看 Eth-Trunk 的成员接口信息。

----结束

1.6 配置举例

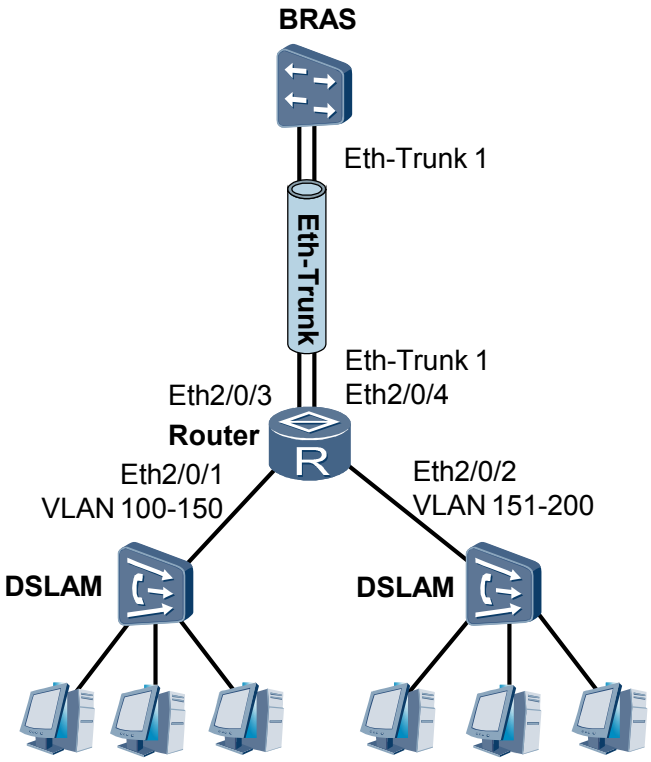
介绍了手工负载分担模式和静态 LACP 模式下的典型应用场景举例。

1.6.1 配置手工负载分担模式链路聚合示例

组网需求

如图 1-4 所示，Router 和 BRAS 之间用 Eth-Trunk 链路连接。要求 Router 和 BRAS 之间的链路有较高的可靠性，并在 Router 上实现数据流量的负载分担。因此需要在 Router 上配置 Eth-Trunk 接口。

图 1-4 配置手工负载分担模式链路聚合组网图



配置思路

采用如下的思路配置负载分担链路聚合：

1. 创建 Eth-Trunk。
2. 加入成员接口。

数据准备

为完成此配置例，需准备的数据：

- 链路聚合组编号。
- Eth-Trunk 的成员接口类型和编号。

操作步骤

步骤 1 创建 Eth-Trunk

创建 Eth-Trunk 1。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface eth-trunk 1
[Router-Eth-Trunk1] quit
```

步骤 2 向 Eth-Trunk 中加入成员接口

将 Eth2/0/3 加入 Eth-Trunk 1。

```
[Router] interface ethernet 2/0/3
[Router-Ethernet2/0/3] eth-trunk 1
[Router-Ethernet2/0/3] quit
```

将 Eth2/0/4 加入 Eth-Trunk 1。

```
[Router] interface ethernet 2/0/4
[Router-Ethernet2/0/4] eth-trunk 1
[Router-Ethernet2/0/4] quit
```

步骤 3 配置 Eth-Trunk 1

配置 Eth-Trunk 1 允许 VLAN100-200 的报文通过。

```
[Router] interface eth-trunk 1
[Router-Eth-Trunk1] port link-type trunk
[Router-Eth-Trunk1] port trunk allow-pass vlan 100 to 200
[Router-Eth-Trunk1] quit
```

步骤 4 验证配置结果

在任意视图下执行 **display trunkmembership eth-trunk** *trunk-id* 命令，检查 Eth-Trunk 1 是否创建成功，及成员接口是否正确加入。

```
[Router] display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of UP Ports in Trunk = 2
operate status: up
Interface Ethernet2/0/3, valid, operate up, weight=1,
Interface Ethernet2/0/4, valid, operate up, weight=1,
```

显示 Eth-Trunk 1 的配置信息。

```
[Router] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL        Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                Status      Weight
Ethernet2/0/3           Up          1
Ethernet2/0/4           Up          1
```

从以上信息看出 Eth-Trunk 1 中包含 2 个成员接口 Eth2/0/3 和 Eth2/0/4。成员接口的状态都为 Up。

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100 to 200
#
interface Ethernet2/0/3
 eth-trunk 1
#
interface Ethernet2/0/4
 eth-trunk 1
#
return
```

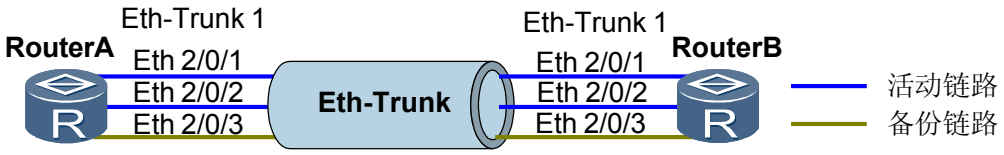
1.6.2 配置静态 LACP 模式链路聚合示例

组网需求

如图 1-5 所示，在两台 Router 设备上配置静态 LACP 模式链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

- 2 条活动链路具有负载分担的能力。
- 两设备间的链路具有 1 条冗余备份链路，当活动链路出现故障链路时，备份链路替代故障链路，保持数据传输的可靠性。

图 1-5 配置静态 LACP 模式链路聚合组网图



配置思路

采用如下的思路配置静态 LACP 模式链路聚合：

1. 在 Router 设备上创建 Eth-Trunk，配置 Eth-Trunk 为静态 LACP 模式。
2. 将成员接口加入 Eth-Trunk。
3. 配置系统优先级确定主动端。
4. 配置活动接口上限阈值。
5. 配置接口优先级确定活动链路。

数据准备

为完成此配置例，需准备如下的数据：

- 两端 Router 设备链路聚合组编号。
- RouterA 系统优先级。
- 活动接口上限阈值。
- 活动接口 LACP 优先级。

操作步骤

步骤 1 创建编号为 1 的 Eth-Trunk，配置它的工作模式为静态 LACP 模式

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] mode lacp-static
[RouterA-Eth-Trunk1] quit
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface eth-trunk 1
[RouterB-Eth-Trunk1] mode lacp-static
[RouterB-Eth-Trunk1] quit
```

步骤 2 将成员接口加入 Eth-Trunk

配置 RouterA。

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] eth-trunk 1
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] eth-trunk 1
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet 2/0/3
[RouterA-Ethernet2/0/3] eth-trunk 1
[RouterA-Ethernet2/0/3] quit
```

配置 RouterB。

```
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] eth-trunk 1
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] eth-trunk 1
[RouterB-Ethernet2/0/2] quit
```

```
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] eth-trunk 1
[RouterB-Ethernet2/0/3] quit
```

步骤 3 在 RouterA 上配置系统优先级为 100，使其成为 LACP 主动端

```
[RouterA] lacp priority 100
```

步骤 4 在 RouterA 上配置活动接口上限阈值为 2

```
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] max active-linknumber 2
[RouterA-Eth-Trunk1] quit
```

步骤 5 在 RouterA 上配置接口优先级确定活动链路

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] lacp priority 100
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] lacp priority 100
[RouterA-Ethernet2/0/2] quit
```

步骤 6 验证配置结果

查看各 Router 设备的 Eth-Trunk 信息，查看链路是否协商成功。

```
[RouterA] display eth-trunk 1
 Eth-Trunk1's state information is:
 Local:
 LAG ID: 1                   WorkingMode: STATIC
 Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
 System Priority: 100        System ID: 00e0-fca8-0417
 Least Active-linknumber: 1   Max Active-linknumber: 2
 Operate status: Up        Number Of Up Port In Trunk: 2
 --------------------------------------------------------------------------------
 ActorPortName          Status    PortType  PortPri   PortNo PortKey   PortState Weight
 Ethernet2/0/1          Selected  100M      100       6145    2865     11111100     1
 Ethernet2/0/2          Selected  100M      100       6146    2865     11111100     1
 Ethernet2/0/3          Unselect  100M      32768     6147    2865     11100000     1

 Partner:
 --------------------------------------------------------------------------------
 PartnerPortName        SysPri    SystemID    PortPri PortNo PortKey   PortState
 Ethernet2/0/1          32768  00e0-fca6-7f85  32768     6145   2609      11111100
 Ethernet2/0/2          32768  00e0-fca6-7f85  32768     6146   2609      11111100
 Ethernet2/0/3          32768  00e0-fca6-7f85  32768     6147   2609      11110000

[RouterB] display eth-trunk 1
 Eth-Trunk1's state information is:
 Local:
 LAG ID: 1                     WorkingMode: STATIC
 Preempt Delay: Disabled       Hash arithmetic: According to SA-XOR-DA
 System Priority: 32768        System ID: 00e0-fca6-7f85
 Least Active-linknumber: 1    Max Active-linknumber: 8
 Operate status: Up            Number Of Up Port In Trunk: 2
 --------------------------------------------------------------------------------
 ActorPortName          Status    PortType  PortPri   PortNo  PortKey   PortState Weight
 Ethernet2/0/1          Selected  100M      32768      6145    2609      11111100     1
 Ethernet2/0/2          Selected  100M      32768      6146    2609      11111100     1
 Ethernet2/0/3          Unselect  100M      32768      6147    2609      11100000     1

 Partner:
 --------------------------------------------------------------------------------
 PartnerPortName        SysPri    SystemID     PortPri  PortNo  PortKey   PortState
 Ethernet2/0/1          100    00e0-fca8-0417  100       6145     2865      11111100
 Ethernet2/0/2          100    00e0-fca8-0417  100       6146     2865      11111100
 Ethernet2/0/3          100    00e0-fca8-0417  32768     6147     2865      11110000
```

通过以上显示信息可以看到，RouterA 的系统优先级为 100，高于 RouterB 的系统优先级。Eth-Trunk 的成员接口中 Ethernet 2/0/1、Ethernet 2/0/2 成为活动接口，处于

“Selected”状态，接口 Ethernet 2/0/2 处于“Unselect”状态，同时实现 M 条链路的负载分担和 N 条链路的冗余备份功能。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 lacp priority 100
#
interface Eth-Trunk1
 mode lacp-static
 max active-linknumber 2
#
interface Ethernet2/0/1
 eth-trunk 1
 lacp priority 100
#
interface Ethernet2/0/2
 eth-trunk 1
 lacp priority 100
#
interface Ethernet2/0/3
 eth-trunk 1
#
return
```

- RouterB 的配置文件

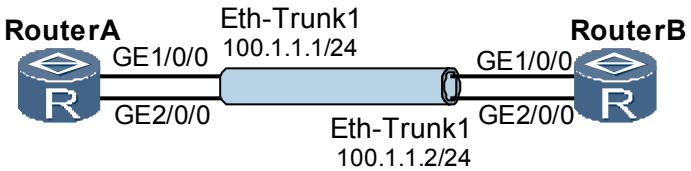
```
#
 sysname RouterB
#
interface Eth-Trunk1
 mode lacp-static
#
interface Ethernet2/0/1
 eth-trunk 1
#
interface Ethernet2/0/2
 eth-trunk 1
#
interface Ethernet2/0/3
 eth-trunk 1
#
return
```

1.6.3 配置三层链路聚合示例

组网需求

RouterA 与 RouterB 之间创建 Eth-Trunk，将两个三层 GE 接口捆绑成一个 Eth-Trunk 接口，可以增加带宽和提高可靠性。

图 1-6 配置三层链路聚合组网图



配置思路

采用如下的思路配置 Eth-Trunk：

1. 创建三层 Eth-Trunk 接口并配置 IP 地址。
2. 把三层 GE 接口加入 Eth-Trunk 接口。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterB 使用三层 GE 接口相连
- RouterA 侧的 Eth-Trunk IP 地址
- RouterB 侧的 Eth-Trunk IP 地址

操作步骤

步骤 1 配置 RouterA

```
<Huawei> system-view
[Huawei] sysname RouterA
```

创建三层 Eth-Trunk 接口，并配置 IP 地址。

```
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] undo portswitch
[RouterA-Eth-Trunk1] ip address 100.1.1.1 24
[RouterA-Eth-Trunk1] quit
```

将三层接口 GE1/0/0、GE2/0/0 加入到 Eth-Trunk 1 中。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] eth-trunk 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] eth-trunk 1
[RouterA-GigabitEthernet2/0/0] quit
```

步骤 2 配置 RouterB

```
<Huawei> system-view
[Huawei] sysname RouterB
```

创建三层 Eth-Trunk 接口，并配置 IP 地址。

```
[RouterB] interface eth-trunk 1
[RouterB-Eth-Trunk1] undo portswitch
[RouterB-Eth-Trunk1] ip address 100.1.1.2 24
[RouterB-Eth-Trunk1] quit
```

将三层接口 GE1/0/0、GE2/0/0 加入到 Eth-Trunk 1 中。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] eth-trunk 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] eth-trunk 1
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 3 检查配置结果

在 RouterA 或 RouterB 上执行 **display interface eth-trunk** 命令，可以看到接口状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Eth-Trunk1 Interface
Route Port,Hash arithmetic : According to SIP-XOR-DIP,The Maximum Transmit Unit
is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc09-9722
Current system time: 2011-4-14 14:51:01
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
-------------------------------------------------
PortName                Status              Weight
-------------------------------------------------
GigabitEthernet1/0/0    UP                  1
GigabitEthernet2/0/0    UP                  1
-------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

RouterA 和 RouterB 的 Eth-Trunk 接口能够互相 Ping 通。

```
[RouterA] ping -a 100.1.1.1 100.1.1.2
  PING 100.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=62 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=62 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=62 ms
  --- 100.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/49/62 ms
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface Eth-Trunk1
 undo portswitch
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 eth-trunk 1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface Eth-Trunk1
 undo portswitch
 ip address 100.1.1.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/0
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 eth-trunk 1
#
return
```

2 透明网桥配置

关于本章

透明网桥是以太网类型局域网中使用最广泛的一种网桥，具有使用方便、易于安装等特点。

2.1 透明网桥概述
从透明网桥的出现、透明网桥的优点到透明网桥如何工作等方面，描述了透明网桥在局域网中的应用。

2.2 AR2200-S 支持的透明网桥
从透明网桥的主要配置场景介绍 AR2200-S 支持的透明网桥特性。理解透明网桥的配置场景后，您可以更快速准确地完成配置任务。

2.3 配置本地同一网段桥接功能
配置本地同一网段桥接功能可以实现同一地理位置相同网段的局域网之间的数据通信。

2.4 配置本地不同网段桥接功能
配置本地不同网段桥接功能可以实现同一地理位置不同网段局域网之间的数据通信。

2.5 配置远程同一网段桥接功能
配置远程同一网段桥接功能可以实现不同地理位置相同网段的局域网之间的数据通信。

2.6 配置远程不同网段桥接功能
配置远程不同网段桥接功能可以实现不同地理位置不同网段局域网之间的数据通信。

2.7 维护
使用清除统计信息命令，帮助定位透明网桥产生的故障原因。

2.8 配置举例
配置举例结合组网需求、配置思路和数据准备，例举了透明网桥的典型应用场景，并提供配置文件。

2.1 透明网桥概述

从透明网桥的出现、透明网桥的优点到透明网桥如何工作等方面，描述了透明网桥在局域网中的应用。

背景

随着各种局域网技术的发展，以太类型局域网以其良好的网络伸缩性以及低成本优势逐步占据了局域网技术的统治地位。在一些小型网络尤其是比较分散的网络中，如何便捷地实现局域网内部、局域网与局域网之间的互通，是一个亟需解决的问题。

通过交换机进行局域网连接，不能够很好地实现不同网段之间的局域网互通，而传统路由器进行局域网互联的方式由于其高成本以及配置复杂等缺点，也难以满足以太局域网互联的需要。

透明网桥（Transparent Bridge）主要应用在以太网环境中，用于连接局域网并在其间传递数据。由于网络中透明网桥的加入以及转发行为对于网络用户来说是透明的，因此被称之为“透明”网桥。

透明网桥不仅可以实现同一网段之间局域网的互通，也很方便实现不同网段之间局域网的互通。采用透明网桥，网络终端用户不需要对设备进行特别配置就能达到拓展网络物理距离、扩大网络规模的目的。透明网桥不仅简单易用，而且成本低，在一些小型网络，尤其是比较分散的网络中得到了广泛地应用。

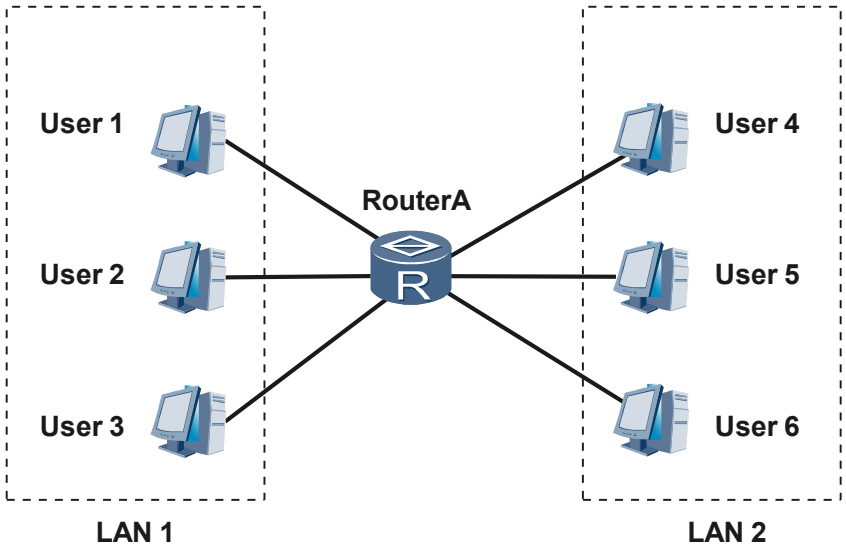
本地桥接功能

透明网桥可以创建不同的网桥组，接口加入到指定网桥组后，流量在网桥组内基于目的MAC 地址进行转发或广播。

一般情况下，网桥获取 MAC 地址和接口的对应关系，生成动态网桥地址表项。管理员也可以手工配置静态地址表项，并且永远不会老化。

如图 2-1 所示，本地六台主机分属于两个不同的 LAN（LAN 1 和 LAN 2）。创建网桥组并将需要互通的局域网的接口加入到相同网桥组中，实现不同 LAN 之间的互通。

图 2-1 透明网桥本地桥接应用组网图



透明网桥的本地桥接成功配置后：

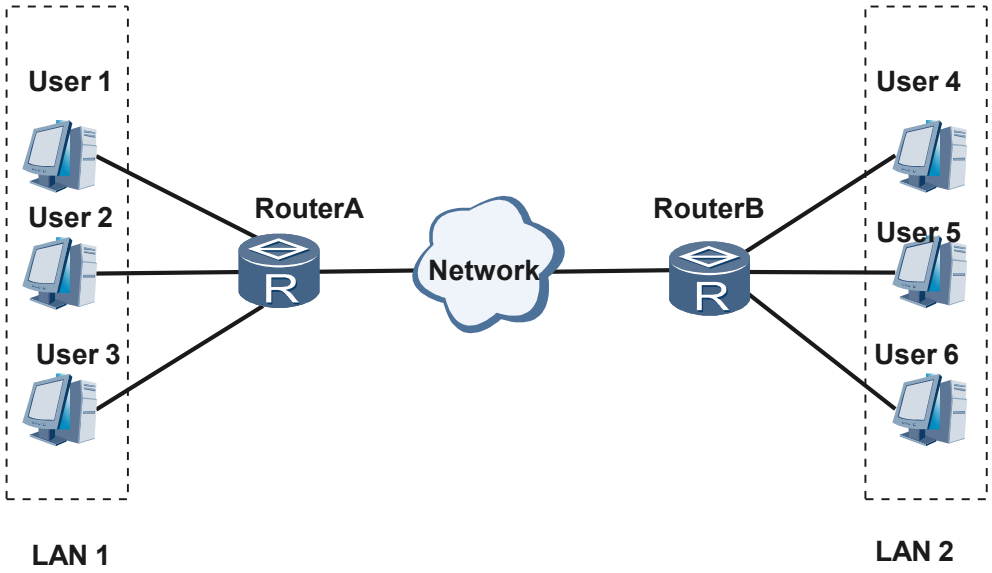
- 网桥组默认支持学习 MAC 地址与端口的映射关系，即 MAC 转发表项。
- 网桥组支持配置静态以及黑洞 MAC 表项。
- 网桥组支持动态 MAC 表项学习使能与禁止。
- 支持配置动态 MAC 表项老化时间。
- 缺省支持对所有报文的桥接功能，包括 IP 以及非 IP 报文。

远程桥接功能

当透明网桥连接的局域网分布在不同地理位置时，需要使能网桥的远程桥接功能实现不同局域网之间的通信。连接两端网桥的中间网络可能是以太网或者非以太网。

如图 2-2 所示，六台主机分属于两个不同的 LAN，其中 User1、User2、User3 属于 LAN 1，User4、User5、User6 属于 LAN 2。两台网桥设备可以通过 Network（包括以太链路、PPP、HDLC、MP、FR、ATM 等链路）连接，使能网桥的远程桥接功能后，LAN 1 和 LAN 2 主机之间可以互通。

图 2-2 透明网桥远程桥接应用组网图



为支持远程桥接功能，透明网桥提供了如下功能：

- 支持以太主接口、以太子接口、VLANIF、VT、Dialer、Serial、ATM 接口、ATM 子接口、FR 接口、FR 子接口、MFR 接口、MLPP 接口加入网桥组；
- 支持以太、PPP、HDLC、FR、ATM 等链路封装协议；
- 支持 802.1Q VLAN ID 透明传输；
- 支持桥接 IP 和非 IP 报文。

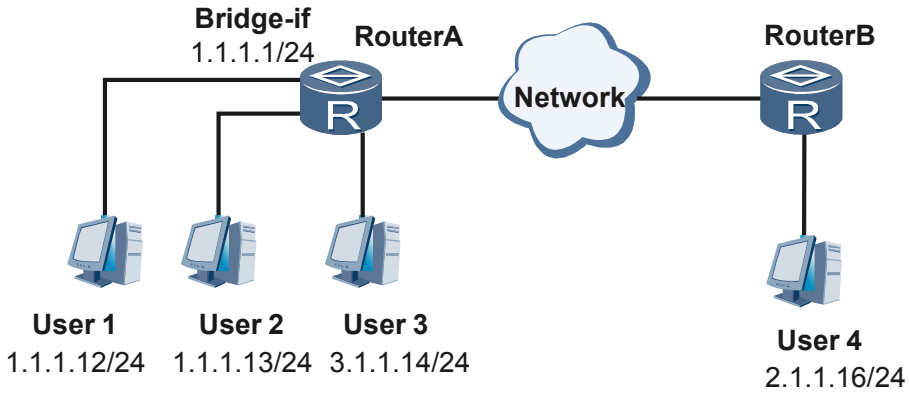
集成路由桥接功能

透明网桥集成路由功能提供了一种结合路由和桥接的转发模式。对于指定的协议数据：

- 如果是在网桥端口之间进行数据通信，则进行桥接转发。
- 如果与非网桥组内的网络（不在同一网段）进行数据通信，则需要进行网络协议的路由转发。

如图 2-3 所示，在 RouterA 上配置网桥组以及网桥组虚接口，网桥组虚接口配置 IP 地址。使能网桥集成路由桥接功能并使能网桥组的 IP 协议数据路由功能，加入网桥组的两台主机 User1 和 User2 可以通过集成路由桥接功能与 User3 互通。两台网桥设备可以通过 Network（包括以太链路、PPP、HDLC、MP、FR、ATM、MFR 等链路）连接，在 RouterA 和 RouterB 上同时配置集成路由功能，并配置网桥组的 IP 协议数据路由功能，可以实现 User1 与 User4 之间的互通。

图 2-3 透明网桥集成路由桥接应用组网图



VLAN ID 透明传输功能

缺省情况下，报文从网桥组接口送出时，VLAN ID 将被去除。为了实现同一 VLAN 之间的互通，不同 VLAN 之间的隔离，可以使能透明网桥 VLAN ID 透明传输功能。

使能透明网桥的 VLAN ID 的透明传输功能后：

- 网桥不会对报文的 VLAN ID 进行任何的修改和去除等操作，从而可以实现 VLAN ID 的透明传输，保证不同 VLAN 之间的隔离、同一 VLAN 之间的互通。
- 加入网桥组的非以太出接口也能转发带有 VLAN ID 的报文，而不会因此丢失 VLAN ID，并且即使加入桥组设备的出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID，从而实现不同 VLAN 的隔离。

2.2 AR2200-S 支持的透明网桥

从透明网桥的主要配置场景介绍 AR2200-S 支持的透明网桥特性。理解透明网桥的配置场景后，您可以更快速准确地完成配置任务。

透明网桥可以实现不同局域网用户之间的相互通信。在进行透明网桥配置时，根据局域网地理位置和所属网段的不同，可以将透明网桥的配置场景分为四种情况，其功能描述及其选择原则如表 2-1 所示。请根据实际的组网环境和需要实现的功能进行选择。

表 2-1 透明网桥的应用场景

需要互通的用户场景	本地同一网段	本地不同网段	远程同一网段	远程不同网段
选择原则	当处于相同地理位置，且属于同一网段的用户可以采用本地桥接功能进行互通。	当处于相同地理位置，且属于不同网段的用户可以采用本地桥接功能和集成路由功能进行互通。	当处于不同地理位置，但属于同一网段的用户可以采用远程桥接功能进行互通。如果需要实现相同 VLAN 之间互通、不同 VLAN 之间隔离时，还需使能 VLAN ID 透明传输功能。	当处于不同地理位置，且属于不同网段的用户可以采用远程桥接功能和集成路由功能进行互通。

2.3 配置本地同一网段桥接功能

配置本地同一网段桥接功能可以实现同一地理位置相同网段的局域网之间的数据通信。

2.3.1 建立配置任务

在进行透明网桥的本地同一网段桥接功能配置之前，需要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，可以帮助您快速、准确地完成配置任务。

应用环境

相同地理位置同一网段的局域网之间如果需要在链路层上互通，可以配置本地同一网段桥接功能来实现。透明网桥可以创建不同的网桥组，接口加入到指定的网桥组后，流量在网桥组内基于目的 MAC 地址进行转发。

前置任务

在配置本地同一网段桥接功能之前，需完成以下任务：

- 配置链路接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置本地同一网段桥接功能之前，需准备以下数据。

序号	数据
1	网桥组的桥组号、（可选）网桥组的静态 MAC 表项、（可选）网桥组的黑洞 MAC 表项、（可选）网桥动态 MAC 表项老化时间
2	加入网桥组中的接口编号。

2.3.2 创建网桥组

网桥组是一个虚拟组，接口加入到网桥组后才能够实现报文转发。

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 **bridge** *bridge-id*，创建网桥组并且进入对应网桥组视图。

如果 *bridge-id* 标识的网桥组已经存在，则直接进入网桥组视图。

网桥组号只在本地设备上有意义，组网时可以与其他设备上的网桥组号相同。

----结束

后续处理

网桥组在默认情况下使能动态地址学习功能，在网络环境比较恶劣（如网络安全性能较差，容易受到攻击），可以关闭网桥的动态 MAC 地址学习功能，采用静态 MAC 表项指导数据转发。请根据需要选择执行以下的一个或多个操作：

- 配置网桥组的静态地址表项。
  - 执行命令 **mac-address static** *mac-address interface-type interface-number* **bridge** *bridge-id*，配置网桥组的静态 MAC 表项。

    缺省情况下，无任何静态 MAC 表项配置。基于同一个网桥组，同一个 MAC 表项只允许一条静态 MAC 表项，重复配置将覆盖已有的配置。
  - （可选）执行命令 **mac-address blackhole** *mac-address* **bridge** *bridge-id*，配置网桥组的黑洞 MAC 表项。

    缺省情况下，无任何黑洞 MAC 表项配置。
- 配置网桥组的动态地址属性。
  - 执行命令 **undo mac-address learning disable**，使能动态 MAC 地址学习功能。

    缺省情况下，已经使能网桥组动态地址学习功能。
  - （可选）执行命令 **mac-address aging-time** *seconds* **bridge**，配置网桥动态 MAC 表项老化时间。

    该配置对设备上所有的网桥组生效。*seconds* 取值范围是 0 或 60 ～ 1000000，0 表示永远不老化。

2.3.3 将本地接口加入到网桥组

将本地接口加入网桥组，实现本地局域网之间的互通。

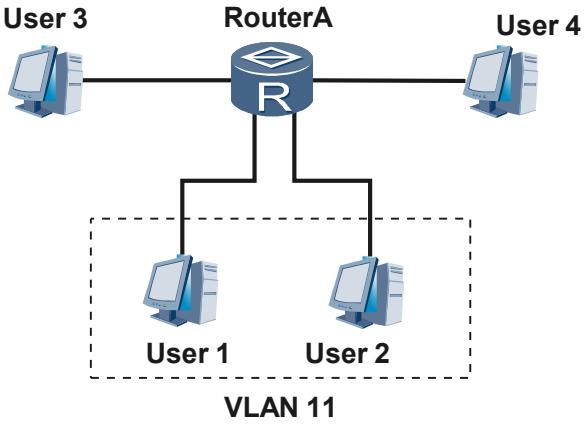
背景信息

网桥组是一个虚拟组，接口加入到网桥组内，能够实现报文在网桥组内转发。

如图 2-4 所示，用户可以通过以下三种方式加入网桥组：

- 用户通过主接口加入网桥组，如 User3。
- 用户通过 VLAN 接入网桥组：在网桥上创建 VLAN，用户加入 VLAN 后，可以通过 VLANIF 接口接入网桥组，如 User1、User2。
- 用户通过以太子接口接入网桥组：同一物理接口下需要通过不同子接口区分不同的流时，可以通过子接口接入网桥组，如 User4。

图 2-4 用户加入网桥组方式



请在设备的用户侧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** *interface-type interface-number*，进入用户侧接口视图。

步骤 3 执行命令 **bridge** *bridge-id*，将接口加入网桥组。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

配置了 QinQ 终结的 Ethernet 子接口和 GE 子接口不支持透明桥接功能。

----结束

2.3.4 （可选）禁止网桥组对指定协议的桥接功能

配置网桥组禁止对指定协议的桥接功能，当网桥组禁止 IP 或其他协议的桥接功能后，对于无法转发的报文，会将其丢弃。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **bridging** { **ip** | **others** } **disable**，禁止网桥组对指定网络协议的桥接功能。

网桥组需要激活对指定网络层协议的桥接功能才能实现报文的转发。缺省情况下，网桥组使能对所有协议的桥接功能。

----结束

2.3.5 检查配置结果

配置透明网桥的本地同一网段桥接功能后，您可以查看到网桥组以及网桥组中接口的流量统计信息。

前提条件

完成本地同一网段桥接功能的相关配置。

操作步骤

- 使用命令 **display bridge** [*bridge-id*] **information**，查看网桥组信息。
- 使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组中相关流量统计信息。

----结束

任务示例

使用命令 **display bridge** [*bridge-id*] **information**，查看网桥组信息。

```
<Huawei> display bridge information

Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet1/0/0 : Up
    Vlanif11 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    Vlanif12 : Up
```

使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组相关流量统计信息。

```
<Huawei> display bridge traffic
Bridge 1 :
 Input  :
        34 total, 0 bpdu, 27 single,
        0 multi, 7 broadcast,
 Output :
```

```
        36 total, 0 bpdu, 28 single,
        0 multi, 8 broadcast,
Bridge 2 :
 Input  :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
 Output :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
```

2.4 配置本地不同网段桥接功能

配置本地不同网段桥接功能可以实现同一地理位置不同网段局域网之间的数据通信。

2.4.1 建立配置任务

在进行透明网桥本地不同网段桥接功能配置之前，需要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，可以帮助您快速、准确地完成配置任务。

应用环境

通常情况下，同一地理位置需要互通的局域网用户在网络层属于同一网段，使能透明网桥的桥接功能便可满足互通。当网桥组内用户需要访问不在同一网段的局域网时，这时仅仅通过链路层桥接无法满足需求，还需要使能透明网桥的集成路由功能。

集成路由功能通过为桥组创建一个路由虚接口（Bridge-if）来实现。

前置任务

在配置本地不同网段桥接功能之前，需完成以下任务：

- 配置链路接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置本地不同网段桥接功能之前，需准备以下数据。

序号	数据
1	网桥组的桥组号。
2	加入网桥组中的接口编号。
3	网桥组虚接口的 IP 地址。

2.4.2 创建网桥组

网桥组是一个虚拟组，接口加入到网桥组后才能够实现报文转发。

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 **bridge** *bridge-id*，创建网桥组并且进入对应网桥组视图。

如果 *bridge-id* 标识的网桥组已经存在，则直接进入网桥组视图。

网桥组号只在本地设备上有意义，组网时可以与其他设备上的网桥组号相同。

----结束

后续处理

网桥组在默认情况下使能动态地址学习功能，在网络环境比较恶劣（如网络安全性能较差，容易受到攻击），可以关闭网桥的动态 MAC 地址学习功能，采用静态 MAC 表项指导数据转发。请根据需要选择执行以下的一个或多个操作：

- 配置网桥组的静态地址表项。
  - 执行命令 **mac-address static** *mac-address interface-type interface-number* **bridge** *bridge-id*，配置网桥组的静态 MAC 表项。

    缺省情况下，无任何静态 MAC 表项配置。基于同一个网桥组，同一个 MAC 表项只允许一条静态 MAC 表项，重复配置将覆盖已有的配置。
  - （可选）执行命令 **mac-address blackhole** *mac-address* **bridge** *bridge-id*，配置网桥组的黑洞 MAC 表项。

    缺省情况下，无任何黑洞 MAC 表项配置。
- 配置网桥组的动态地址属性。
  - 执行命令 **undo mac-address learning disable**，使能动态 MAC 地址学习功能。

    缺省情况下，已经使能网桥组动态地址学习功能。
  - （可选）执行命令 **mac-address aging-time** *seconds* **bridge**，配置网桥动态 MAC 表项老化时间。

    该配置对设备上所有的网桥组生效。*seconds* 取值范围是 0 或 60 ～ 1000000，0 表示永远不老化。

2.4.3 将本地接口加入到网桥组

将本地接口加入网桥组，实现本地局域网之间的互通。

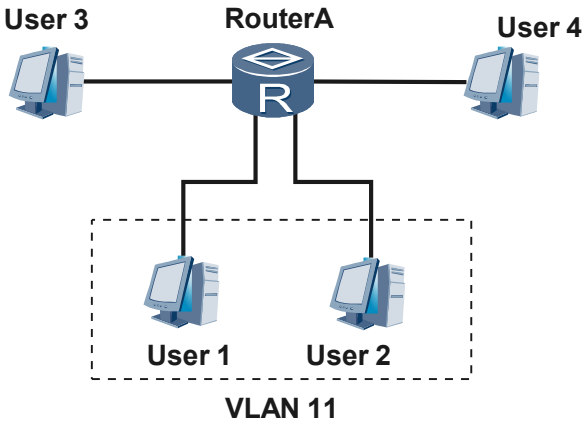
背景信息

网桥组是一个虚拟组，接口加入到网桥组内，能够实现报文在网桥组内转发。

如图 2-5 所示，用户可以通过以下三种方式加入网桥组：

- 用户通过主接口加入网桥组，如 User3。
- 用户通过 VLAN 接入网桥组：在网桥上创建 VLAN，用户加入 VLAN 后，可以通过 VLANIF 接口接入网桥组，如 User1、User2。
- 用户通过以太子接口接入网桥组：同一物理接口下需要通过不同子接口区分不同的流时，可以通过子接口接入网桥组，如 User4。

图 2-5 用户加入网桥组方式



请在设备的用户侧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** *interface-type interface-number*，进入用户侧接口视图。

步骤 3 执行命令 **bridge** *bridge-id*，将接口加入网桥组。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

配置了 QinQ 终结的 Ethernet 子接口和 GE 子接口不支持透明桥接功能。

----结束

2.4.4 配置网桥组虚接口

通过配置网桥组虚接口可以实现不同网段局域网之间的数据通信。

背景信息

网桥组虚接口（Bridge-if）是一个虚拟的选路接口。

对于指定的协议数据，网桥端口之间只能进行网桥组内的桥接转发，如果不同网段的局域网之间需要进行通信，可以在网桥组上创建一个网桥组虚接口实现通信数据的路由转发。

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 bridge-if** *bridge-id*，创建网桥组虚接口并进入虚接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置网桥组虚接口的 IP 地址。

步骤 4 （可选）执行命令 **mac-address** *mac-address*，配置网桥组虚接口的 MAC 地址。

----结束

2.4.5 使能网桥路由功能

配置透明网桥的集成路由功能，可以实现对指定协议的报文进行路由处理。

背景信息

透明网桥集成路由功能提供了一种结合路由和桥接的转发方式。如果未使能透明网桥的集成路由功能，所有的协议数据只能够进行桥接处理，使能透明网桥的集成路由功能后，通过命令配置，灵活实现对指定协议的报文进行路由或桥接处理。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **routing ip**，使能网桥路由功能。

IP 协议报文的路由功能与成员口 IP 互斥，使能 IP 协议报文的路由功能前需要查看成员口是否配置 IP 地址，如果接口有配置 IP 地址，需要取消成员口 IP 地址。

----结束

2.4.6 （可选）禁止网桥组对指定协议的桥接功能

配置网桥组禁止对指定协议的桥接功能，当网桥组禁止 IP 或其他协议的桥接功能后，对于无法转发的报文，会将其丢弃。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **bridging** { **ip** | **others** } **disable**，禁止网桥组对指定网络协议的桥接功能。

网桥组需要激活对指定网络层协议的桥接功能才能实现报文的转发。缺省情况下，网桥组使能对所有协议的桥接功能。

----结束

2.4.7 检查配置结果

配置透明网桥的本地不同网段桥接功能后，您可以查看到网桥组以及网桥组中相关流量统计信息。

前提条件

完成透明网桥本地不同网段桥接功能的相关配置。

操作步骤

- 使用命令 **display interface bridge-if** [*bridge-id*]，查看网桥组虚接口信息。
- 使用命令 **display bridge** [*bridge-id*] **information**，查看对端网桥的网桥组信息。
- 使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组中相关流量统计信息。

----结束

任务示例

使用命令 **display interface bridge-if** [*bridge-id*]，查看网桥的网桥组虚接口信息。

```
<Huawei> display interface bridge-if 1

Bridge-if1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-10-09 18:50:53 UTC-08:00
Description:HUAWEI, AR Series, Bridge-if1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.3/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-0e0b-0100
Physical is BRIDGE-IF
Current system time: 2010-10-11 08:52:21-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 18 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 18 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 396 packets,0 bytes,
           190 unicast,206 broadcast,0 multicast
    Output:731 packets,0 bytes,
           498 unicast,233 broadcast,0 multicast
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看本地网桥的网桥组相关流量统计信息。

```
<Huawei> display bridge traffic
Bridge 1 :
 Input  :
         283 total, 0 bpdu, 11 single,
         271 multi, 1 broadcast,
 Output :
         178 total, 0 bpdu, 11 single,
         166 multi, 1 broadcast,
Bridge 2 :
 Input  :
         0 total, 0 bpdu, 0 single,
         0 multi, 0 broadcast,
 Output :
         0 total, 0 bpdu, 0 single,
         0 multi, 0 broadcast,
```

2.5 配置远程同一网段桥接功能

配置远程同一网段桥接功能可以实现不同地理位置相同网段的局域网之间的数据通信。

2.5.1 建立配置任务

在进行透明网桥的远程同一网段桥接功能配置之前，需要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，可以帮助您快速、准确地完成配置任务。

应用环境

不同地理位置同一网段的局域网之间有链路层互通需求时，可以通过配置透明网桥的远程同一网段桥接功能来实现。如果需要实现相同 VLAN 之间互通、不同 VLAN 之间隔离时，还需使能 VLAN ID 透明传输功能。

前置任务

在配置远程同一网段桥接功能之前，需完成以下任务：

- 配置链路接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置远程同一网段桥接功能之前，需准备以下数据。

序号	数据
1	网桥组的桥组号。
2	加入网桥组中的接口编号。

2.5.2 创建网桥组

网桥组是一个虚拟组，接口加入到网桥组后才能够实现报文转发。

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 **bridge** *bridge-id*，创建网桥组并且进入对应网桥组视图。

如果 *bridge-id* 标识的网桥组已经存在，则直接进入网桥组视图。

网桥组号只在本地设备上有意义，组网时可以与其他设备上的网桥组号相同。

----结束

后续处理

网桥组在默认情况下使能动态地址学习功能，在网络环境比较恶劣（如网络安全性能较差，容易受到攻击），可以关闭网桥的动态 MAC 地址学习功能，采用静态 MAC 表项指导数据转发。请根据需要选择执行以下的一个或多个操作：

- 配置网桥组的静态地址表项。
  - 执行命令 **mac-address static** *mac-address interface-type interface-number* **bridge** *bridge-id*，配置网桥组的静态 MAC 表项。

    缺省情况下，无任何静态 MAC 表项配置。基于同一个网桥组，同一个 MAC 表项只允许一条静态 MAC 表项，重复配置将覆盖已有的配置。
  - （可选）执行命令 **mac-address blackhole** *mac-address* **bridge** *bridge-id*，配置网桥组的黑洞 MAC 表项。

缺省情况下，无任何黑洞 MAC 表项配置。

- 配置网桥组的动态地址属性。
  - 执行命令 **undo mac-address learning disable**，使能动态 MAC 地址学习功能。
    缺省情况下，已经使能网桥组动态地址学习功能。
  - （可选）执行命令 **mac-address aging-time** *seconds* **bridge**，配置网桥动态 MAC 表项老化时间。
    该配置对设备上所有的网桥组生效。*seconds* 取值范围是 0 或 60 ～ 1000000，0 表示永远不老化。

2.5.3 将用户侧接口加入网桥组

将用户侧接口加入网桥组，实现局域网之间的互通。

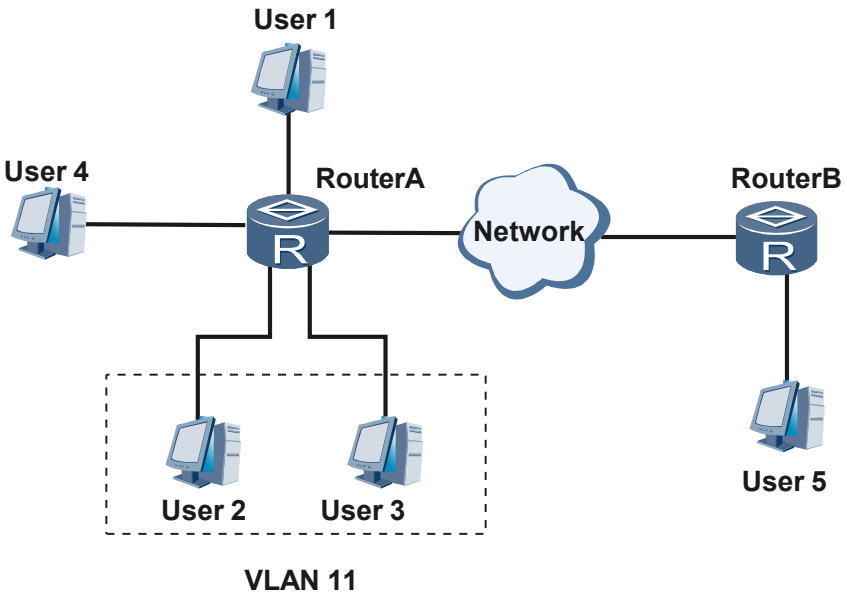
背景信息

网桥组是一个虚拟组，接口加入到网桥组内，能够实现报文在网桥组内转发。

如图 2-6 所示，用户可以通过以下三种方式加入网桥组：

- 用户通过主接口加入网桥组，如 User1。
- 用户通过 VLAN 接入网桥组：在网桥上创建 VLAN，用户加入 VLAN 后，可以通过 VLANIF 接口接入网桥组，如 User2、User3。
- 用户通过以太子接口接入网桥组：同一物理接口下需要通过不同子接口区分不同的流时，可以通过子接口接入网桥组，如 User4。

图 2-6 用户加入网桥组方式



请在设备的用户侧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** *interface-type interface-number*，进入用户侧接口视图。

步骤 3 执行命令 **bridge** *bridge-id*，将接口加入网桥组。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

配置了 QinQ 终结的 Ethernet 子接口和 GE 子接口不支持透明桥接功能。

----结束

2.5.4 将网络侧接口加入网桥组

两台网桥设备通过中间链路相连，可实现不同局域网之间的远程桥接。

背景信息

两台网桥设备通过以太链路、PPP、HDLC、MP、FR、MFR、ATM 等中间链路相连，用于远程连接不同的局域网。

要实现局域网的远程桥接，必须将网桥设备上连接局域网的接口与连接中间链路的接口（即网络侧接口）加入同一个网桥组。

请在中间链路两端的设备上分别进行如下配置。

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** *interface-type interface-number*，进入网络侧接口视图。

步骤 3 请根据中间链路实际情况，进行如下配置：

- 配置以太链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 HDLC 链路支持透明网桥。
  1. 执行命令 **link-protocol hdlc**，封装 HDLC 协议。
  2. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 PPP 链路支持透明网桥。
  1. 执行命令 **link-protocol ppp**，封装 PPP 协议。
  2. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 MP 链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将 VT 接口加入到网桥组中。
  2. 执行命令 **quit**，退出当前视图，返回到系统视图。
  3. 执行命令 **interface** *interface-type interface-number*，进入 MP 链路接口视图。
  4. 执行命令 **link-protocol ppp**，封装 PPP 协议。
  5. 执行命令 **ppp mp virtual-template** *number*，将接口绑定到虚拟接口模板。

- 配置 FR 链路支持透明网桥。
  1. 执行命令 **link-protocol fr**，封装 FR 协议。
  2. 执行命令 **fr dlci** *dlci*，创建帧中继 PVC。
  3. 执行命令 **bridge** *bridge-id*，将帧中继接口加入到网桥组中。
  4. 执行命令 **fr map bridge** *dlci-number* **broadcast**，配置一条转发到网桥的帧中继映射。
- 配置 ATM 链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将 ATM 接口加入到网桥组中。
  2. 执行命令 **pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }，PVC 允许收发桥报文。
  3. 执行命令 **map bridge broadcast** 配置一条转发到网桥的 ATM PVC 映射。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

MFR 接口加入网桥组，如果 MFR 接口下绑定的帧中继接口带宽不一致，数据转发时可能会出现丢包现象。

----结束

2.5.5 （可选）禁止网桥组对指定协议的桥接功能

配置网桥组禁止对指定协议的桥接功能，当网桥组禁止 IP 或其他协议的桥接功能后，对于无法转发的报文，会将其丢弃。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **bridging** { **ip** | **others** } **disable**，禁止网桥组对指定网络协议的桥接功能。

网桥组需要激活对指定网络层协议的桥接功能才能实现报文的转发。缺省情况下，网桥组使能对所有协议的桥接功能。

----结束

2.5.6 （可选）配置 VLAN ID 透明传输功能

通过配置网桥透明传输 VLAN ID，可以实现两个不同局域网的同一 VLAN 内的相互通信。

背景信息

缺省情况下，报文从网桥组接口送出时，VLAN ID 将被去除。加入网桥组的设备出接口配置支持 VLAN ID 透明传输功能后，可以使报文从该接口送出时，不对报文的 VLAN ID 做任何修改，则报文从该接口发出时保留报文入桥时的 VLAN ID。

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 **bridge vlan-transmit enable**，使能网桥组接口透明传输 VLAN ID 功能。

说明

- VLANIF 接口不支持此功能。
- 子接口不建议使用该功能。

步骤 4 执行命令 **quit**，退出当前视图，返回到系统视图。

----结束

2.5.7 检查配置结果

配置透明网桥的远程同一网段桥接功能后，您可以查看到网桥组以及网桥组中相关流量统计信息。

前提条件

完成透明网桥远程同一网段桥接功能的相关配置。

操作步骤

- 使用命令 **display bridge** [*bridge-id*] **information**，查看网桥组信息。
- 使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组中相关流量统计信息。

----结束

任务示例

使用命令 **display bridge** [*bridge-id*] **information**，查看网桥 1 信息。

```
[Huawei] display bridge 1 information

Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet1/0/0 : Up
    GigabitEthernet2/0/0 : Up
```

使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组 1 中相关流量统计信息。

```
[Huawei] display bridge traffic bridge 1
Bridge 1 :
 Input  :
         48 total, 0 bpdu, 11 single,
         36 multi, 1 broadcast,
 Output :
         35 total, 0 bpdu, 11 single,
         23 multi, 1 broadcast,
```

2.6 配置远程不同网段桥接功能

配置远程不同网段桥接功能可以实现不同地理位置不同网段局域网之间的数据通信。

2.6.1 建立配置任务

在进行透明网桥远程不同网段桥接功能配置之前，需要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，可以帮助您快速、准确地完成配置任务。

应用环境

不同地理位置不同网段的局域网需要互通时，这时仅仅通过链路层桥接无法满足需求，还需要使能透明网桥的集成路由功能。

集成路由功能通过为桥组创建一个路由虚接口（Bridge-if）来实现。

当局域网在不同地理位置，且属于不同 IP 子网时，同时使能透明网桥集成路由功能和远程桥接功能，即进行远程不同网段桥接功能配置可以实现上述局域网之间的数据通信。

前置任务

在配置远程不同网段桥接功能之前，需完成以下任务：

- 配置链路接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置远程不同网段桥接功能之前，需准备以下数据。

序号	数据
1	网桥组的桥组号。
2	加入网桥组中的接口编号。
3	网桥组虚接口的 IP 地址。

2.6.2 创建网桥组

网桥组是一个虚拟组，接口加入到网桥组后才能够实现报文转发。

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 **bridge** *bridge-id*，创建网桥组并且进入对应网桥组视图。

如果 *bridge-id* 标识的网桥组已经存在，则直接进入网桥组视图。

网桥组号只在本地设备上有意义，组网时可以与其他设备上的网桥组号相同。

----结束

后续处理

网桥组在默认情况下使能动态地址学习功能，在网络环境比较恶劣（如网络安全性能较差，容易受到攻击），可以关闭网桥的动态 MAC 地址学习功能，采用静态 MAC 表项指导数据转发。请根据需要选择执行以下的一个或多个操作：

- 配置网桥组的静态地址表项。
  - 执行命令 **mac-address static** *mac-address interface-type interface-number* **bridge** *bridge-id*，配置网桥组的静态 MAC 表项。

    缺省情况下，无任何静态 MAC 表项配置。基于同一个网桥组，同一个 MAC 表项只允许一条静态 MAC 表项，重复配置将覆盖已有的配置。
  - （可选）执行命令 **mac-address blackhole** *mac-address* **bridge** *bridge-id*，配置网桥组的黑洞 MAC 表项。

    缺省情况下，无任何黑洞 MAC 表项配置。
- 配置网桥组的动态地址属性。
  - 执行命令 **undo mac-address learning disable**，使能动态 MAC 地址学习功能。

    缺省情况下，已经使能网桥组动态地址学习功能。
  - （可选）执行命令 **mac-address aging-time** *seconds* **bridge**，配置网桥动态 MAC 表项老化时间。

    该配置对设备上所有的网桥组生效。*seconds* 取值范围是 0 或 60 ～ 1000000，0 表示永远不老化。

2.6.3 将用户侧接口加入网桥组

将用户侧接口加入网桥组，实现局域网之间的互通。

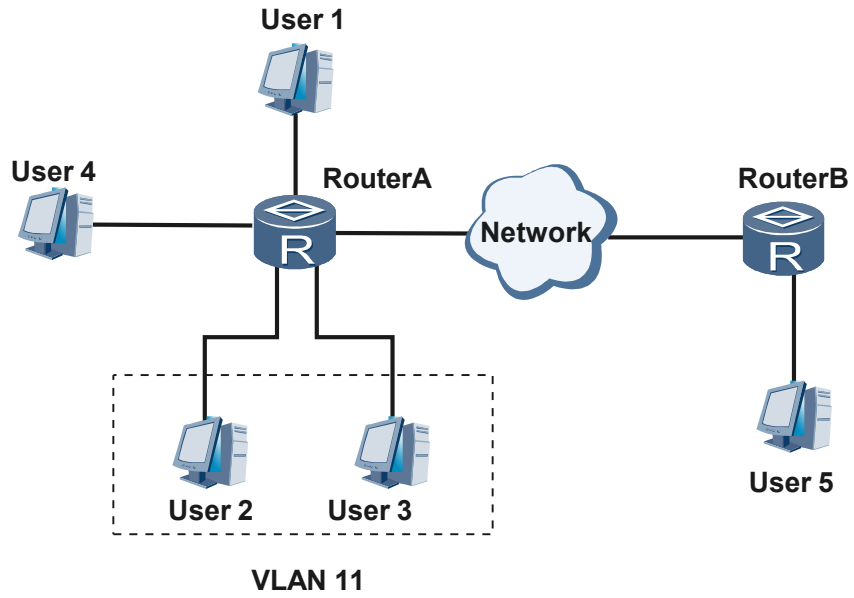
背景信息

网桥组是一个虚拟组，接口加入到网桥组内，能够实现报文在网桥组内转发。

如图 2-7 所示，用户可以通过以下三种方式加入网桥组：

- 用户通过主接口加入网桥组，如 User1。
- 用户通过 VLAN 接入网桥组：在网桥上创建 VLAN，用户加入 VLAN 后，可以通过 VLANIF 接口接入网桥组，如 User2、User3。
- 用户通过以太子接口接入网桥组：同一物理接口下需要通过不同子接口区分不同的流时，可以通过子接口接入网桥组，如 User4。

图 2-7 用户加入网桥组方式



请在设备的用户侧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** *interface-type interface-number*，进入用户侧接口视图。

步骤 3 执行命令 **bridge** *bridge-id*，将接口加入网桥组。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

配置了 QinQ 终结的 Ethernet 子接口和 GE 子接口不支持透明桥接功能。

----结束

2.6.4 将网络侧接口加入网桥组

两台网桥设备通过中间链路相连，可实现不同局域网之间的远程桥接。

背景信息

两台网桥设备通过以太链路、PPP、HDLC、MP、FR、MFR、ATM 等中间链路相连，用于远程连接不同的局域网。

要实现局域网的远程桥接，必须将网桥设备上连接局域网的接口与连接中间链路的接口（即网络侧接口）加入同一个网桥组。

请在中间链路两端的设备上分别进行如下配置。

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** *interface-type interface-number*，进入网络侧接口视图。

步骤 3 请根据中间链路实际情况，进行如下配置：

- 配置以太链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 HDLC 链路支持透明网桥。
  1. 执行命令 **link-protocol hdlc**，封装 HDLC 协议。
  2. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 PPP 链路支持透明网桥。
  1. 执行命令 **link-protocol ppp**，封装 PPP 协议。
  2. 执行命令 **bridge** *bridge-id*，将接口加入到网桥组中。
- 配置 MP 链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将 VT 接口加入到网桥组中。
  2. 执行命令 **quit**，退出当前视图，返回到系统视图。
  3. 执行命令 **interface** *interface-type interface-number*，进入 MP 链路接口视图。
  4. 执行命令 **link-protocol ppp**，封装 PPP 协议。
  5. 执行命令 **ppp mp virtual-template** *number*，将接口绑定到虚拟接口模板。
- 配置 FR 链路支持透明网桥。
  1. 执行命令 **link-protocol fr**，封装 FR 协议。
  2. 执行命令 **fr dlci** *dlci*，创建帧中继 PVC。
  3. 执行命令 **bridge** *bridge-id*，将帧中继接口加入到网桥组中。
  4. 执行命令 **fr map bridge** *dlci-number* **broadcast**，配置一条转发到网桥的帧中继映射。
- 配置 ATM 链路支持透明网桥。
  1. 执行命令 **bridge** *bridge-id*，将 ATM 接口加入到网桥组中。
  2. 执行命令 **pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }，PVC 允许收发桥报文。
  3. 执行命令 **map bridge broadcast** 配置一条转发到网桥的 ATM PVC 映射。

一个网桥组最多只允许 20 个接口加入，不同接口类型可以混合加入到同一个网桥组。不允许二层口加入网桥组。

MFR 接口加入网桥组，如果 MFR 接口下绑定的帧中继接口带宽不一致，数据转发时可能会出现丢包现象。

----结束

2.6.5 配置网桥组虚接口

通过配置网桥组虚接口可以实现不同网段局域网之间的数据通信。

背景信息

网桥组虚接口（Bridge-if）是一个虚拟的选路接口。

对于指定的协议数据，网桥端口之间只能进行网桥组内的桥接转发，如果不同网段的局域网之间需要进行通信，可以在网桥组上创建一个网桥组虚接口实现通信数据的路由转发。

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 bridge-if** *bridge-id*，创建网桥组虚接口并进入虚接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置网桥组虚接口的 IP 地址。

步骤 4 （可选）执行命令 **mac-address** *mac-address*，配置网桥组虚接口的 MAC 地址。

----结束

2.6.6 使能网桥路由功能

配置透明网桥的集成路由功能，可以实现对指定协议的报文进行路由处理。

背景信息

透明网桥集成路由功能提供了一种结合路由和桥接的转发方式。如果未使能透明网桥的集成路由功能，所有的协议数据只能够进行桥接处理，使能透明网桥的集成路由功能后，通过命令配置，灵活实现对指定协议的报文进行路由或桥接处理。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **routing ip**，使能网桥路由功能。

IP 协议报文的路由功能与成员口 IP 互斥，使能 IP 协议报文的路由功能前需要查看成员口是否配置 IP 地址，如果接口有配置 IP 地址，需要取消成员口 IP 地址。

----结束

2.6.7 （可选）禁止网桥组对指定协议的桥接功能

配置网桥组禁止对指定协议的桥接功能，当网桥组禁止 IP 或其他协议的桥接功能后，对于无法转发的报文，会将其丢弃。

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 **bridge** *bridge-id*，进入网桥组视图。

步骤 3 执行命令 **bridging** { **ip** | **others** } **disable**，禁止网桥组对指定网络协议的桥接功能。

网桥组需要激活对指定网络层协议的桥接功能才能实现报文的转发。缺省情况下，网桥组使能对所有协议的桥接功能。

----结束

2.6.8 检查配置结果

配置透明网桥的远程不同网段桥接功能后，您可以查看到网桥组以及网桥组中接口的流量统计信息。

前提条件

完成透明网桥远程不同网段桥接功能的相关配置。

操作步骤

- 使用命令 **display interface bridge-if** [*bridge-id*]，查看网桥组虚接口信息。
- 使用命令 **display bridge** [*bridge-id*] **information**，查看对端网桥的网桥组信息。
- 使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看网桥组相关流量统计信息。

----结束

任务示例

使用命令 **display interface bridge-if** [*bridge-id*]，查看网桥的网桥组虚接口信息。

```
<Huawei> display interface bridge-if 1

Bridge-if1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-10-09 18:50:53 UTC-08:00
Description:HUAWEI, AR Series, Bridge-if1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.3/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-0e0b-0100
Physical is BRIDGE-IF
Current system time: 2010-10-11 08:52:21-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 18 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 18 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 396 packets,0 bytes,
           190 unicast,206 broadcast,0 multicast
     Output:731 packets,0 bytes,
           498 unicast,233 broadcast,0 multicast
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

使用命令 **display bridge** [*bridge-id*] **information**，查看对端网桥的网桥组信息。

```
<Huawei> display bridge information
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : IP
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet1/0/0 : Up
    GigabitEthernet2/0/0 : Up
```

使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看本地网桥的网桥组相关流量统计信息。

```
<Huawei> display bridge traffic
Bridge 1 :
 Input  :
        54 total, 0 bpdu, 50 single,
```

```
        0 multi, 4 broadcast,
 Output :
        52 total, 0 bpdu, 45 single,
        0 multi, 7 broadcast,
Bridge 2 :
 Input  :
        234 total, 0 bpdu, 198 single,
        0 multi, 36 broadcast,
 Output :
        234 total, 0 bpdu, 196 single,
        0 multi, 38 broadcast,
```

使用命令 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，查看对端网桥的网桥组相关流量信息。

```
<Huawei> display bridge traffic
Bridge 2 :
 Input  :
        234 total, 0 bpdu, 198 single,
        0 multi, 36 broadcast,
 Output :
        234 total, 0 bpdu, 196 single,
        0 multi, 38 broadcast,
```

2.7 维护

使用清除统计信息命令，帮助定位透明网桥产生的故障原因。

2.7.1 监控网桥运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解网桥的运行状况。

操作步骤

- 在任意视图下执行 **display bridge traffic** [**bridge** *bridge-id* | **interface** *interface-type interface-number*]，可以查看网桥组相关流量统计信息。
- 在任意视图下执行 **display bridge** [*bridge-id*] **information**，可以查看网桥组信息。
- 在任意视图下执行 **display interface bridge-if** [*bridge-id*]，可以查看网桥组虚接口的使能状态、协议使能状态、接口描述信息和接口 IP 地址等信息。
- 在任意视图下执行 **display mac-address** [*mac-address* | **blackhole** | **static** | **dynamic**] [**bridge** *bridge-id*] [**verbose**]，可以查看指定网桥组的静态、动态或黑洞 mac 地址表项信息。
- 在任意视图下执行 **display mac-address** [*mac-address* | *interface-type interface-number*] **bridge** *bridge-id* [**verbose**]或 **display mac-address** { **static** | **dynamic** } [*interface-type interface-number*] **bridge** *bridge-id* **verbose**，可以查看指定网桥组和接口的静态或动态地址表项信息。

----结束

2.7.2 清除网桥组流量统计信息

清除当前网桥组的流量计数，帮助定位查找网桥组产生故障的原因。

背景信息

需要定位网桥组产生故障的原因时，可以采用清除当前网桥组的流量计数来帮助定位查找。

注意

清除统计信息后，已有的统计信息将无法恢复，请务必仔细确认。

操作步骤

- 请在用户视图下执行 **reset bridge** *bridge-id* **statistics** 命令，清除网桥组流量统计信息。

----结束

2.7.3 清除网桥组虚接口的流量统计信息

清除当前网桥组虚接口的流量计数，帮助定位查找网桥组产生故障的原因。

背景信息

需要定位网桥组产生的故障原因时，可以采用清除当前网桥组虚接口的流量计数来帮助定位查找。

注意

清除统计信息后，已有的统计信息将无法恢复，请务必仔细确认。

操作步骤

- 请在用户视图下执行 **reset counters interface bridge-if** [*bridge-id*]命令，清除网桥组虚接口流量统计信息。

----结束

2.8 配置举例

配置举例结合组网需求、配置思路和数据准备，例举了透明网桥的典型应用场景，并提供配置文件。

2.8.1 配置本地同一网段桥接功能示例

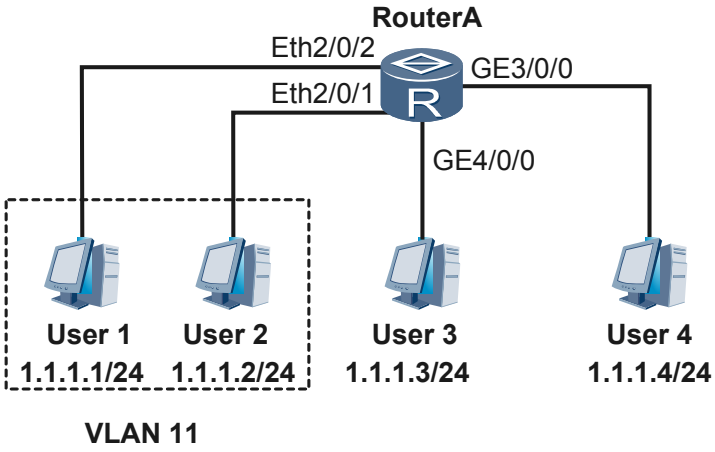
通过配置透明网桥的本地相同网段桥接功能，实现同一网段相同地理位置局域网之间的相互通信。

组网需求

某企业有多个部门，各个部门分散在同一栋大厦的不同楼层。由于业务的发展，同一部门内部的终端、部分部门与部门之间有数据通信的需求。但是部分部门出于安全等需要,需要与其他部门之间进行隔离。对于上述情况，可以采用透明网桥的本地桥接功能，将需要互通的用户加入同一个网桥组，从而实现部门之间的互通或隔离。

如图 2-8 所示，两台主机 User1、User2 属于同一个部门，加入 VLAN 11，User4、User3 属于另外两个不同的部门,User1、User2、User3 之间有互通的需求。在透明网桥上创建网桥组，把需要互通的部门加入相同的网桥组内，即可实现部门之间的互通和隔离。

图 2-8 本地同一网段桥接功能示例组网图



配置思路

采用如下的思路配置透明网桥的本地同一网段桥接功能：

1. 配置网桥组。
2. 将 User1、User2 加入 VLAN 11，通过 VLANIF 接口加入网桥组 1，并将 User3 加入网桥组 1，实现 User1、User2、User3 之间的互通。
3. 将 User4 加入网桥组 2，实现与 User1、User2、User3 之间隔离。

数据准备

为完成此配置，需准备如下数据：

- 网桥设备上用于连接各局域网的接口。
- 互通的各局域网都加入同一个网桥组的桥组号。
- 加入网桥组的 VLAN 编号。

配置过程

1. 创建网桥组 1

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] bridge 1
```

```
[RouterA-bridge1] quit
```

2. 将本地接口 Eth2/0/1 和 Eth2/0/1 加入到 VLAN11

```
[RouterA] vlan 11
[RouterA-vlan11] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1] port default vlan 11
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type access
[RouterA-Ethernet2/0/2] port default vlan 11
[RouterA-Ethernet2/0/2] quit
```

3. 将 VLANIF 接口和本地接口 GE4/0/0 加入网桥组 1

```
[RouterA] interface gigabitethernet 4/0/0
[RouterA-GigabitEthernet4/0/0] bridge 1
[RouterA-GigabitEthernet4/0/0] quit
[RouterA] interface vlanif 11
[RouterA-Vlanif11] bridge 1
[RouterA-Vlanif11] quit
```

4. 创建网桥组 2

```
[RouterA] bridge 2
[RouterA-bridge2] quit
```

5. 将本地接口 GE3/0/0 加入网桥组 2

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] bridge 2
[RouterA-GigabitEthernet3/0/0] quit
```

6. 检查配置结果

   # 上述配置完成后，执行命令 **display bridge information**，可以查看网桥的配置信息。

```
[RouterA] display bridge information
Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet4/0/0 : Up
    Vlanif11 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    GigabitEthernet3/0/0 : Up
```

   # 上述配置完成后，User1、User2 和 User3 可以互相 ping 通；User4 和 User3 不能 ping 通。

配置文件

网桥 RouterA 的配置文件

```
#
 sysname RouterA
#
bridge 1
bridge 2
#
interface Vlanif11
 bridge 1
```

```
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 11
#
interface GigabitEthernet 4/0/0
 bridge 1
#
interface GigabitEthernet 3/0/0
 bridge 2
#
return
```

2.8.2 配置本地不同网段桥接功能示例

通过配置透明网桥的集成路由桥接功能，实现不同网段局域网之间的相互通信。

组网需求

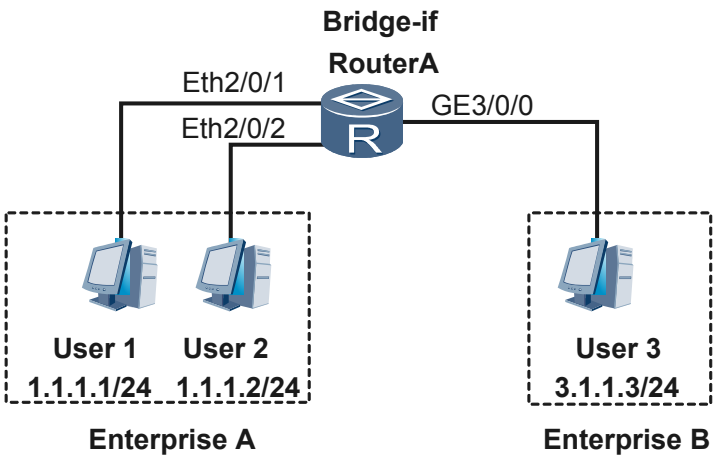
企业 A 由于业务的不断扩展，不仅企业部门之间有相互通信的需求，而且与当地企业 B 有业务往来，需要与企业 B 进行通信。

企业 A 部门之间的通信属于同一网段的局域网通信，可以采用桥接转发；但是企业 A 需要与企业 B 进行通信时，属于不同网段之间的局域网通信，仅仅通过链路层桥接无法满足需求。

为了能够实现该企业 A 内部之间，以及企业 A 与企业 B 之间进行通信，可以同时采用透明网桥的集成路由功能。

如图 2-9 所示，在网桥上配置网桥组以及网桥组虚接口，连接不同企业的接口分别加入到不同的网桥组。创建网桥组虚接口并配置 IP 地址，使能网桥集成路由桥接功能后，企业 A 两台主机即可以通过网桥组虚接口与企业 B 进行通信。

图 2-9 本地不同网段桥接功能组网图



配置思路

采用如下的思路配置透明网桥的集成路由桥接：

1. 在网桥 RouterA 上配置网桥组。
2. 将企业 A 加入到网桥 RouterA 的网桥组中，实现企业 A 内部的互通。
3. 配置并激活网桥 RouterA 集成路由功能，实现企业 A 与企业 B 的互通。

数据准备

为完成此配置，需准备如下数据：

- 网桥设备上用于连接各局域网的接口。
- 互通的各局域网都加入同一个网桥组的桥组号。

配置过程

- 配置本地集成路由功能

  1. 配置网桥 RouterA

     # 创建网桥组 1 并使能桥组的路由桥接功能和 IP 协议数据路由功能。

     ```
     <Huawei> system-view
     [Huawei] sysname RouterA
     [RouterA] bridge 1
     [RouterA-bridge1] routing ip
     [RouterA-bridge1] quit
     ```

     # 将本地接口 Eth2/0/1 和 Eth2/0/2 加入到 VLAN11

     ```
     [RouterA] vlan 11
     [RouterA-vlan11] quit
     [RouterA] interface ethernet 2/0/1
     [RouterA-Ethernet2/0/1] port link-type access
     [RouterA-Ethernet2/0/1] port default vlan 11
     [RouterA-Ethernet2/0/1] quit
     [RouterA] interface ethernet 2/0/2
     [RouterA-Ethernet2/0/2] port link-type access
     [RouterA-Ethernet2/0/2] port default vlan 11
     [RouterA-Ethernet2/0/2] quit
     ```

     # 将 VLANIF 接口加入网桥组 1

     ```
     [RouterA] interface vlanif 11
     [RouterA-Vlanif11] bridge 1
     [RouterA-Vlanif11] quit
     ```

     # 配置与网桥 RouterA 连接的接口 GE3/0/0 的 IP 地址。

     ```
     [RouterA] interface gigabitethernet 3/0/0
     [RouterA-GigabitEthernet3/0/0] ip address 3.1.1.1 255.255.255.0
     [RouterA-GigabitEthernet3/0/0] quit
     ```

     # 创建网桥组虚接口 1，并配置其 IP 地址。

     ```
     [RouterA] interface bridge-if 1
     [RouterA-Bridge-if1] ip address 1.1.1.3 255.255.255.0
     [RouterA-Bridge-if1] quit
     ```

  2. 检查配置结果

     # 完成上述配置后，User1 和 User3 可以互相 ping 通。

配置文件

网桥 RouterA 的配置文件

```
#
 sysname RouterA
#
```

```
bridge 1
 routing ip
#
interface Vlanif11
 bridge 1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 11
#
interface GigabitEthernet3/0/0
 ip address 3.1.1.1 255.255.255.0
#
interface Bridge-if1
 ip address 1.1.1.3 255.255.255.0
#
return
```

2.8.3 配置远程同一网段桥接功能示例

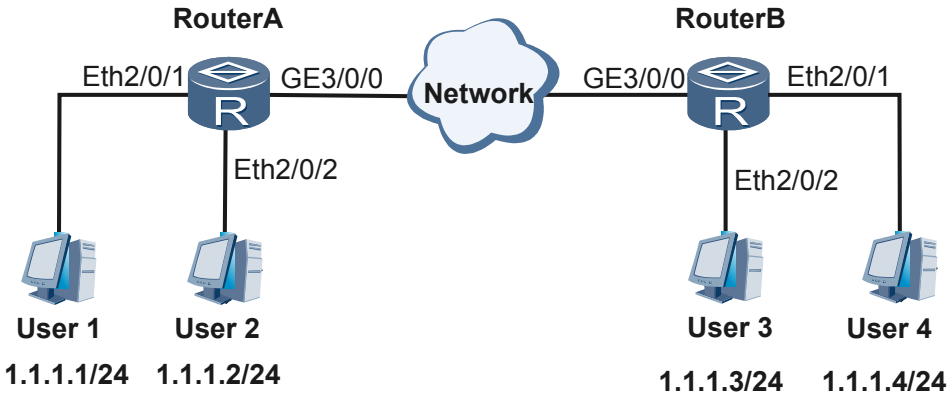
通过配置远程同一网段桥接功能，实现同一网段不同地理位置局域网之间的通信。

组网需求

某企业有多个部门分布在不同的地区，由于业务发展的需要，不同区域的部门内部终端、部分部门与部门之间有数据通信的需求。为了解决不同区域部门之间的互通，可以采用透明网桥的远程桥接功能，实现企业在不同区域部门之间的数据通信需要。

如图 2-10 所示，两个网桥 RouterA 和 RouterB 分布在不同地点，并通过中间链路链接。主机 User1、User2，User3、User4 属于同一网段不同局域网，通过透明网桥的远程桥接功能实现不同地理位置主机之间的互通。

图 2-10 远程同一网段桥接功能组网图



配置思路

在网桥 RouterA 和网桥 RouterB 上采用如下的思路配置透明网桥的远程桥接：

1. 配置网桥组。

2. 将本地用户加入本地网桥组，实现本地局域网之间的互通。
3. 将中间链路接口加入本地网桥组，使能透明网桥的远程桥接，实现不同地理位置的局域网的互通。

数据准备

为完成此配置，需准备如下数据：

- 网桥设备上用于连接各局域网的接口。
- 互通的各局域网都加入同一个网桥组的桥组号。

配置过程

1. 配置网桥 RouterA

   # 创建网桥组 1。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] bridge 1
[RouterA-bridge1] quit
```

   # 将本地接口 Eth2/0/2 和 Eth2/0/1 加入到 VLAN11，实现 User1 和 User2 之间互通。

```
[RouterA] vlan 11
[RouterA-vlan11] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type access
[RouterA-Ethernet2/0/2] port default vlan 11
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1] port default vlan 11
[RouterA-Ethernet2/0/1] quit
```

   # 将 VLANIF 接口加入网桥组 1

```
[RouterA] interface vlanif 11
[RouterA-Vlanif11] bridge 1
[RouterA-Vlanif11] quit
```

   # 将接口 GE3/0/0 加入网桥组 1。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] bridge 1
[RouterA-GigabitEthernet3/0/0] quit
```

2. 配置网桥 RouterB

   # 创建网桥组 1。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] bridge 1
[RouterB-bridge1] quit
```

   # 将本地接口 Eth2/0/2 和 Eth2/0/1 加入到 VLAN11，实现 User3 和 User4 之间互通。

```
[RouterB] vlan 11
[RouterB-vlan11] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] port link-type access
[RouterB-Ethernet2/0/2] port default vlan 11
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port link-type access
[RouterB-Ethernet2/0/1] port default vlan 11
[RouterB-Ethernet2/0/1] quit
```

   # 将 VLANIF 接口加入网桥组 1

```
[RouterB] interface vlanif 11
[RouterB-Vlanif11] bridge 1
[RouterB-Vlanif11] quit
```

将接口 GE3/0/0 加入网桥组 1。

```
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] bridge 1
[RouterB-GigabitEthernet3/0/0] quit
```

3. 检查配置结果

完成上述配置后，User1、User2、User3 和 User4 可以互相 ping 通。

配置文件

网桥 RouterA 的配置文件

```
#
 sysname RouterA
#
bridge 1
#
interface Vlanif11
 bridge 1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 11
#
interface GigabitEthernet3/0/0
 bridge 1
#
return
```

网桥 RouterB 的配置文件

```
#
 sysname RouterB
#
bridge 1
#
interface Vlanif11
 bridge 1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 11
#
interface GigabitEthernet3/0/0
 bridge 1
#
return
```

2.8.4 配置远程不同网段桥接功能示例

通过配置远程不同网段桥接功能，实现远程不同网段局域网之间的相互通信。

组网需求

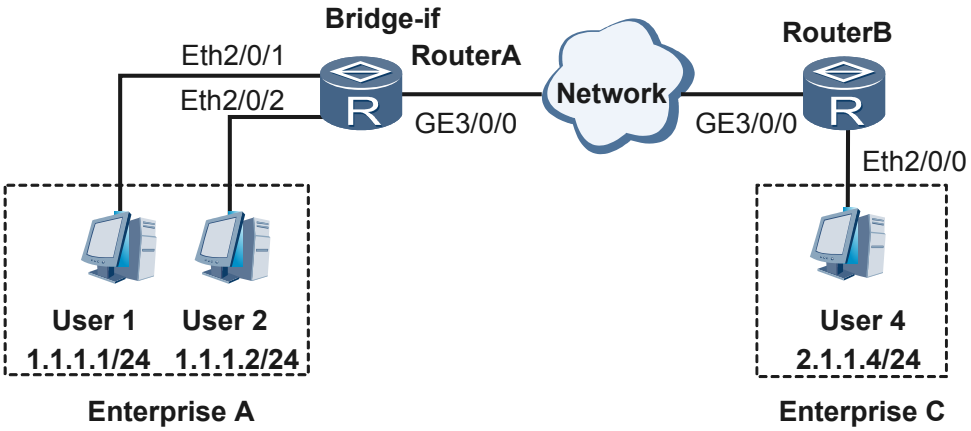
企业 A 由于业务的不断扩展，不仅企业部门之间有相互通信的需求，而且与不在同一地区的企业 C 有业务往来，需要与 C 进行通信。

企业 A 部门之间的通信属于同一网段的局域网通信，可以采用桥接转发；但是企业 A 需要与企业 C 进行通信时，属于不同网段之间的局域网通信，仅仅通过链路层桥接无法满足需求。

为了能够实现该企业 A 内部之间，以及企业 A 与 C 之间进行通信，可以采用透明网桥的远程桥接功能和集成路由功能。

如图 2-11 所示，在网桥上配置网桥组以及网桥组虚接口，连接不同企业的接口分别加入到不同的网桥组。创建网桥组虚接口并配置 IP 地址，使能网桥集成路由桥接功能后，企业 A 两台主机即可以通过网桥组虚接口与外地企业 C 进行通信。

图 2-11 远程不同网段桥接功能组网图



配置思路

采用如下的思路配置透明网桥的集成路由桥接：

1. 在网桥 RouterA 和网桥 RouterB 上配置网桥组。
2. 将企业 A 加入到网桥 RouterA 的网桥组中，实现企业 A 内部的互通。
3. 将连接网桥 RouterA 和网桥 RouterB 的广域网两端链路接口分别加入网桥组。
4. 配置并激活网桥 RouterA 和 RouterB 的集成路由功能，实现企业 A 与企业 C 的互通。

数据准备

为完成此配置，需准备如下数据：

- 网桥设备上用于连接各局域网的接口。
- 互通的各局域网都加入同一个网桥组的桥组号。

配置过程

- 配置本地集成路由功能

  1. 配置网桥 RouterA

     # 创建网桥组 1 和网桥组 2 并使能桥组的路由桥接功能和 IP 协议数据路由功能。

     ```
     <Huawei> system-view
     [Huawei] sysname RouterA
     [RouterA] bridge 1
     [RouterA-bridge1] routing ip
     [RouterA-bridge1] quit
     [RouterA] bridge 2
     [RouterA-bridge2] routing ip
     [RouterA-bridge2] quit
     ```

     # 将本地接口 Eth2/0/1 和 Eth2/0/2 加入到 VLAN11，实现 User1 和 User2 之间互通。

     ```
     [RouterA] vlan 11
     [RouterA-vlan11] quit
     [RouterA] interface ethernet 2/0/1
     [RouterA-Ethernet2/0/1] port link-type access
     [RouterA-Ethernet2/0/1] port default vlan 11
     [RouterA-Ethernet2/0/1] quit
     [RouterA] interface ethernet 2/0/2
     [RouterA-Ethernet2/0/2] port link-type access
     [RouterA-Ethernet2/0/2] port default vlan 11
     [RouterA-Ethernet2/0/2] quit
     ```

     # 将 VLANIF 接口加入网桥组 1

     ```
     [RouterA] interface vlanif 11
     [RouterA-Vlanif11] bridge 1
     [RouterA-Vlanif11] quit
     ```

     # 配置与网桥 RouterA 连接接口 GE3/0/0 加入网桥组 2。

     ```
     [RouterA] interface gigabitethernet 3/0/0
     [RouterA-GigabitEthernet3/0/0] bridge 2
     [RouterA-GigabitEthernet3/0/0] quit
     ```

     # 创建网桥组虚接口 1 和网桥组虚接口 2，并配置其 IP 地址。

     ```
     [RouterA] interface bridge-if 1
     [RouterA-Bridge-if1] ip address 1.1.1.3 255.255.255.0
     [RouterA-Bridge-if1] quit
     [RouterA] interface bridge-if 2
     [RouterA-Bridge-if2] ip address 2.1.1.3 255.255.255.0
     [RouterA-Bridge-if2] quit
     ```

  2. 配置网桥 RouterB

     # 创建网桥组 2 并使能桥组的路由桥接功能和 IP 协议数据路由功能。

     ```
     <Huawei> system-view
     [Huawei] sysname RouterB
     [RouterB] bridge 2
     [RouterB-bridge2] routing ip
     [RouterB-bridge2] quit
     ```

     # 将本地接口 Eth2/0/0 加入到 VLAN11。

     ```
     [RouterB] vlan 11
     [RouterB-vlan11] quit
     [RouterB] interface ethernet 2/0/0
     [RouterB-Ethernet2/0/0] port link-type access
     [RouterB-Ethernet2/0/0] port default vlan 11
     [RouterB-Ethernet2/0/0] quit
     ```

     # 将 VLANIF 接口加入网桥组 2

     ```
     [RouterB] interface vlanif 11
     [RouterB-Vlanif11] bridge 2
     ```

```
[RouterB-Vlanif11] quit
```

配置与网桥 RouterB 连接接口 GE3/0/0 加入网桥组 2。

```
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] bridge 2
[RouterB-GigabitEthernet3/0/0] quit
```

3. 检查配置结果

完成上述配置后，User1 和 User4 可以互相 ping 通。

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
bridge 1
 routing ip
bridge 2
 routing ip
#
interface Vlanif11
 bridge 1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 11
#
interface Bridge-if1
 ip address 1.1.1.3 255.255.255.0
#
interface Bridge-if2
 ip address 2.1.1.3 255.255.255.0
#
interface GigabitEthernet3/0/0
 bridge 2
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
bridge 2
 routing ip
#
interface Vlanif11
 bridge 2
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 11
#
interface GigabitEthernet3/0/0
 bridge 2
#
return
```

2.8.5 配置远程同一网段相同 VLAN 之间互通示例

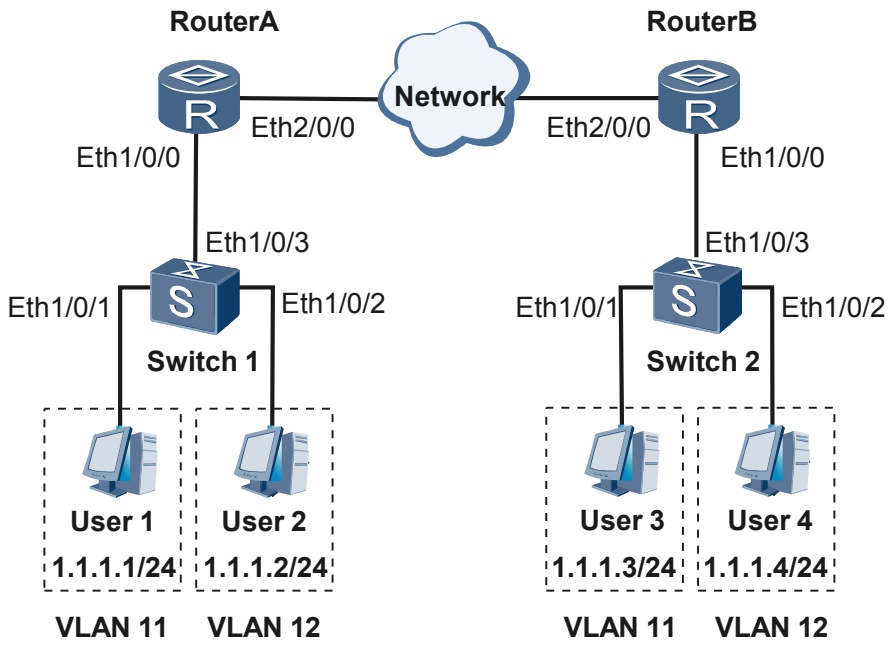
通过配置透明网桥的 VLAN ID 透明传输功能，实现两个不同局域网的同一 VLAN 内的相互通信。

组网需求

某企业有多个部门分布在不同的地区，由于业务发展的需要，不同区域的部门内部终端、部分部门与部门之间有数据通信的需求。为了解决不同区域部门之间的互通，可以采用透明网桥的远程桥接功能，实现企业在不同区域部门之间的数据通信需要。如果由于业务或安全按需要，要实现相同部门（同一 VLAN 内用户）之间的互通、不同部门之间的隔离，则还需要使能透明网桥的透明传输功能。

如图 2-12 所示，主机 User1、User2，User3、User4 属于同一网段不同局域网，其中 User1、User3 属于同一个 VLAN，其中 User2、User4 属于同一个 VLAN。为实现同一 VLAN 之间的通信、不同 VLAN 之间的隔离，可以通过网桥的远程桥接并使能 VLAN ID 透明传输功能，从而实现 User1 只与 User3、User2 只与 User4 进行通信。

图 2-12 远程桥接组网图



配置思路

采用如下的思路配置透明网桥的远程桥接

- 在 Switch1 和 Switch2 上按如下思路进行配置：
  1. 创建 VLAN。
  2. 将接口加入相应的 VLAN。
  3. 配置接口允许带 VLAN11 和 VLAN12 的报文通过。

- 在 RouterA 和 RouterB 上分别按如下思路进行配置：
  1. 配置网桥组。
  2. 将用户侧接口和中间链路接口，即 WAN 侧口 Ethernet1/0/0 和 Ethernet2/0/0 加入同一个网桥组。
  3. 使能用户侧接口和中间链路接口的 VLAN ID 透明传输功能，实现同一 VLAN 之间的互通、不同 VLAN 之间的隔离。

数据准备

为完成此配置，需准备如下数据：

- 交换机连接用户的接口编号。
- 用户加入 VLAN 的 VLAN 编号。
- 网桥设备上用于连接各局域网的接口。
- 互通的各局域网都加入同一个网桥组的桥组号。

配置过程

1. 配置 RouterA

   # 创建网桥组 1。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA-bridge1] bridge 1
[RouterA-bridge1] undo shutdown
[RouterA-bridge1] quit
```

   # 将接口 GE1/0/0 和 GE2/0/0 加入网桥组 1，同时使能 VLAN ID 透传功能。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] bridge 1
[RouterA-GigabitEthernet1/0/0] bridge vlan-transmit enable
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] bridge 1
[RouterA-GigabitEthernet2/0/0] bridge vlan-transmit enable
[RouterA-GigabitEthernet2/0/0] quit
```

2. 配置 Switch1。

   # 创建 VLAN。

```
<Huawei> system-view
[Huawei] sysname Switch1
[Switch1] vlan 11
[Switch1-vlan11] quit
[Switch1] vlan 12
[Switch1-vlan12] quit
```

   # 将接口 Eth1/0/1 和 Eth1/0/2 分别配置接入 VLAN11、VLAN12。

```
[Switch1] interface ethernet 1/0/1
[Switch1-Ethernet1/0/1] port link-type access
[Switch1-Ethernet1/0/1] port default vlan 11
[Switch1-Ethernet1/0/1] quit
[Switch1] interface ethernet 1/0/2
[Switch1-Ethernet1/0/2] port link-type access
[Switch1-Ethernet1/0/2] port default vlan 12
[Switch1-Ethernet1/0/2] quit
```

   # 配置接口 Eth1/0/3 允许携带 VLAN11、VLAN12 的报文通过。

```
[Switch1] interface ethernet 1/0/3
[Switch1-Ethernet1/0/3] port link-type trunk
[Switch1-Ethernet1/0/3] port trunk allow-pass vlan 11 to 12
```

```
[Switch1-Ethernet1/0/3] quit
```

3. 配置 RouterB

   # 创建网桥组 2。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB-bridge2] bridge 2
[RouterB-bridge2] quit
```

   # 将接口 GE1/0/0 和 GE2/0/0 加入网桥组 1，同时使能 VLAN ID 透传功能。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] bridge 2
[RouterB-GigabitEthernet1/0/0] bridge vlan-transmit enable
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] bridge 2
[RouterB-GigabitEthernet2/0/0] bridge vlan-transmit enable
[RouterB-GigabitEthernet2/0/0] quit
```

4. 配置 Switch2

   # 创建 VLAN。

```
<Huawei> system-view
[Huawei] sysname Switch2
[Switch2] vlan 11
[Switch2-vlan11] quit
[Switch2] vlan 12
[Switch2-vlan12] quit
```

   # 将接口 Eth1/0/1 和 Eth1/0/2 分别配置接入 VLAN11、VLAN12。

```
[Switch2] interface ethernet 1/0/1
[Switch2-Ethernet1/0/1] port link-type access
[Switch2-Ethernet1/0/1] port default vlan 11
[Switch2-Ethernet1/0/1] quit
[Switch2] interface ethernet 1/0/2
[Switch2-Ethernet1/0/2] port link-type access
[Switch2-Ethernet1/0/2] port default vlan 12
[Switch2-Ethernet1/0/2] quit
```

   # 配置接口 Eth1/0/3 允许携带 VLAN11、VLAN12 的报文通过。

```
[Switch2] interface ethernet 1/0/3
[Switch2-Ethernet1/0/3] port link-type trunk
[Switch2-Ethernet1/0/3] port trunk allow-pass vlan 11 to 12
[Switch2-Ethernet1/0/3] quit
```

5. 检查配置结果

   完成上述配置后，User1 只与 User3 可以互相 ping 通，User2 只与 User4 可以互相 ping 通。

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 11 to 12
#
bridge 1
#
interface GigabitEthernet1/0/0
 bridge 1
 bridge vlan-transmit enable
#
interface GigabitEthernet2/0/0
 bridge 1
```

```
 bridge vlan-transmit enable
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
 vlan batch 11 to 12
#
bridge 2
#
#
interface GigabitEthernet1/0/0
 bridge 2
 bridge vlan-transmit enable
#
interface GigabitEthernet2/0/0
 bridge 2
 bridge vlan-transmit enable

#
return
```

Switch1 的配置文件

```
#
 sysname Switch1
#
 vlan batch 11 to 12
#
interface Ethernet1/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet1/0/2
 port link-type access
 port default vlan 12
#
interface Ethernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 11 to 12
#
return
```

Switch2 的配置文件

```
#
 sysname Switch2
#
 vlan batch 11 to 12
#
#
interface Ethernet1/0/1
 port link-type access
 port default vlan 11
#
interface Ethernet1/0/2
 port link-type access
 port default vlan 12
#
interface Ethernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 11 to 12
#
return
```

3 VLAN 配置

关于本章

介绍了 VLAN 的基础知识、配置方法和配置实例。

3.1 VLAN 概述
简要介绍 VLAN 的基本概念。

3.2 AR2200-S 支持的 VLAN 特性
介绍 VLAN 特性在 AR2200-S 中的支持情况。

3.3 创建 VLAN
介绍创建一个或多个 VLAN 的过程与步骤。

3.4 配置基于接口划分 VLAN
介绍将 Access 类型、Hybrid 类型、Trunk 类型的接口加入 VLAN 的过程与步骤。

3.5 配置 VLANIF 接口实现三层互通
介绍配置 VLANIF 接口实现三层互通的过程与步骤。

3.6 配置 VLAN 聚合
介绍解决多个 VLAN 占用 IP 地址过多的问题的配置方法。

3.7 配置 MUX VLAN
介绍如何配置 VLAN 内接口隔离。

3.8 配置管理 VLAN
介绍配置管理 VLAN 的配置方法。

3.9 配置举例
介绍 VLAN 的各种组网举例。

3.1 VLAN 概述

简要介绍 VLAN 的基本概念。

VLAN 的定义

在逻辑上将一个局域网 LAN（Local Area Network）划分成多个子集，每个子集形成各自的广播域，即虚拟局域网 VLAN（Virtual Local Area Network）。简单地说，VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。

VLAN 的作用

采用 VLAN 方式进行组网时，将有互通需求的设备划分在同一个 VLAN 内，没有互通需求的设备划分在不同的 VLAN 内。既隔离了广播域，减少了广播风暴，又增强了信息的安全性。

当网络规模越来越庞大时，局部网络出现的故障会影响到整个网络。VLAN 的出现，可以将网络故障限制在 VLAN 范围内，增强了网络的健壮性。

3.2 AR2200-S 支持的 VLAN 特性

介绍 VLAN 特性在 AR2200-S 中的支持情况。

基于接口划分 VLAN

AR2200-S 的接口类型分为三种：

- Access 类型：接口只能加入 1 个缺省 VLAN，一般用于连接用户设备；
- Trunk 类型：接口可以加入多个 VLAN，一般用于网络设备之间连接；
- Hybrid 类型：接口可以加入多个 VLAN，可以用于网络设备之间连接，也可以用于连接用户设备；

  Hybrid 接口和 Trunk 接口的区别在于：
  - Hybrid 接口可以配置成多个 VLAN 的报文发送时不带 Tag 标签；
  - Trunk 接口只能配置成缺省 VLAN 的报文发送时不带 Tag 标签。

接口配置了链路类型和缺省 VLAN 后对收发报文的处理方法如**表 3-1** 所示。

表 3-1 接口收发报文的处理

接口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	对发送报文的处理
Access 接口	接收该报文，并打上缺省 VLAN 的 Tag。	● 当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文。 ● 当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。	去掉 Tag，发送该报文。
Trunk 接口	● 打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文。 ● 打上缺省的 VLAN ID，当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	● 当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文。 ● 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	● 当 VLAN ID 与缺省 VLAN ID 相同时，且是该接口允许通过的 VLAN ID 时：去掉 Tag，发送该报文。 ● 当 VLAN ID 与缺省 VLAN ID 不同时，且是该接口允许通过的 VLAN ID 时：保持原有 Tag，发送该报文。
Hybrid 接口			当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。可以通过 **port hybrid untagged/tagged vlan** 设置发送时是否携带 Tag。

VLAN 聚合

为了在路由器上实现 VLAN 间通信，需要为每个 VLANIF 接口配置一个 IP 地址，以实现 VLAN 间路由。如果 VLAN 很多，将占用许多 IP 地址资源。VLAN 聚合（VLAN aggregation）可以解决多个 VLAN 占用多个 IP 地址的问题。

VLAN 聚合是将多个 VLAN 集中在一起，形成一个 Super-VLAN。组成 Super-VLAN 的 VLAN 被称作 Sub-VLAN。

可以创建一个 VLANIF 接口，使其对应一个 Super-VLAN，只在该接口上配置 IP 地址，不必为每个 Sub-VLAN 分配 IP 地址，所有 Sub-VLAN 共用 IP 网段，从而解决 IP 地址使用效率的问题。

MUX VLAN

MUX VLAN 提供了一种在 VLAN 的接口间进行二层流量隔离机制。比如在企业网络中，企业希望某些部门之间的员工是互相隔离的，某些部门之间的员工是可以互相访问的，并且所有部门的员工都可以访问公司的某些服务器。

MUX VLAN 分为主 VLAN 和从 VLAN，从 VLAN 又分为互通型从 VLAN 和隔离型从 VLAN。

主 VLAN 与从 VLAN 之间可以相互通信，不同从 VLAN 之间不能互相通信。互通型从 VLAN 接口之间可以互相通信，隔离型从 VLAN 接口之间不能互相通信。

当多台设备配置的 MUX VLAN 一致，且设备间允许 MUX VLAN 通过时，可以实现跨设备的 MUX VLAN 功能，功能实现与单台设备的 MUX VLAN 完全一致。

3.3 创建 VLAN

介绍创建一个或多个 VLAN 的过程与步骤。

3.3.1 建立配置任务

应用环境

通过划分 VLAN，将没有互通需求的主机进行隔离，增强网络的安全性、减少广播流量，同时也减少了广播风暴的发生。

前置任务

无

数据准备

在创建 VLAN 之前，需要准备以下数据。

序号	数据
1	VLAN 的编号

3.3.2 创建单个 VLAN

背景信息

请在需要创建 VLAN 的 AR2200-S 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 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 （可选）执行命令 **description** *description*，配置 VLAN 的描述信息。

配置 VLAN 的描述信息主要是为了方便管理和记忆 VLAN。缺省情况下，VLAN 的描述中体现了 VLAN 的编号，例如 VLAN15 的描述信息为：“VLAN 0015”。

----结束

3.3.3 （可选）批量创建 VLAN

背景信息

请在需要创建 VLAN 的 AR2200-S 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 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，批量创建 VLAN。

----结束

3.3.4 检查配置结果

操作步骤

步骤 1 使用命令 **display vlan** [*vlan-id* [**verbose**]] 查看 VLAN 的基本信息。

----结束

任务示例

执行命令 **display vlan**，可以查看到已经创建的 VLAN。

```
<Huawei> display vlan
* : management-vlan
--------------------
The total number of vlans is : 5
VLAN ID Type    Status   MAC Learning Broadcast/Multicast/Unicast Property
--------------------------------------------------------------------------------
1       common  enable   enable       forward   forward   forward default
10      common  enable   enable       forward   forward   forward default
20      common  enable   enable       forward   forward   forward default
30      common  enable   enable       forward   forward   forward default
100     common  enable   enable       forward   forward   forward default
```

执行命令 **display vlan** *vlan-id* **verbose**，可以查看到 VLAN 的描述信息是否配置正确。

```
<Huawei> display vlan 10 verbose
* : Management-VLAN
--------------------
  VLAN ID                    : 10
  VLAN Name                  :
  VLAN Type                  : Common
  Description                : VLAN 0010
  Status                     : Enable
  Broadcast                  : Enable
  MAC Learning               : Enable
```

```
  Smart MAC Learning          : Disable
  Current MAC Learning Result : Enable
  Statistics                  : Disable
  Property                    : Default
  VLAN State                  : Up
  ----------------
  Untagged      Port: Ethernet2/0/0             Ethernet2/0/4

  ----------------
  Active Untag  Port: Ethernet2/0/0             Ethernet2/0/4

-------------------
Interface                   Physical
Ethernet2/0/0               UP
Ethernet2/0/4               DOWN
```

3.4 配置基于接口划分 VLAN

介绍将 Access 类型、Hybrid 类型、Trunk 类型的接口加入 VLAN 的过程与步骤。

3.4.1 建立配置任务

应用环境

通过接口划分 VLAN。将具有相同业务需求的接口划分在一个 VLAN 中，实现不同业务需求的接口互相隔离。例如：接口 1 连接宽带上网用户，接口 2 也连接宽带上网用户，接口 3 连接视频业务，则将接口 1 和接口 2 划分在一个 VLAN 中，接口 3 和接口 1、接口 2 划分在不同的 VLAN 中。

说明

改变接口类型前，需要删除原接口类型下对 VLAN 的配置，即恢复接口只加入 VLAN1 的缺省配置。

前置任务

在配置将接口加入 VLAN 之前，需完成以下任务：

- 创建 VLAN

数据准备

在将接口加入到 VLAN 之前，需要准备以下数据。

序号	数据
1	需要加入 VLAN 的接口的类型和编号
2	VLAN 的编号

3.4.2 将 Access 类型接口加入 VLAN

背景信息

可以通过如下两种方式将 Access 类型接口加入 VLAN。

操作步骤

- VLAN 视图下将 Access 类型接口加入 VLAN。
  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 **port link-type access**，配置接口的类型。

     缺省情况下，接口的链路类型为 Hybrid。
  4. 执行命令 **quit**，退回到系统视图。
  5. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  6. 执行命令 **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>，将 Access 类型的接口加入 VLAN，即接口的缺省 VLAN。

     缺省情况下，所有接口加入的 VLAN 和缺省 VLAN 都为 VLAN1。
- 接口视图下将 Access 类型接口加入 VLAN。
  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 **port link-type access**，配置接口的类型。

     缺省情况下，接口的链路类型为 Hybrid。
  4. 执行命令 **port default vlan** *vlan-id*，将 Access 类型的接口加入 VLAN，即接口的缺省 VLAN。

     缺省情况下，所有接口加入的 VLAN 和缺省 VLAN 都为 VLAN1。

----结束

3.4.3 将 Trunk 类型接口加入 VLAN

背景信息

请在需要将接口加入 VLAN 的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type trunk**，将接口配置成 Trunk 类型接口。

缺省情况下，接口的链路类型为 Hybrid。

步骤 4 执行命令 **port trunk allow-pass vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，将 Trunk 类型接口加入 VLAN。

缺省情况下，Trunk 类型接口加入的 VLAN 为 VLAN1。

----结束

3.4.4 将 Hybrid 类型接口加入 VLAN

背景信息

请在需要将接口加入 VLAN 的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type hybrid**，将接口配置为 Hybrid 类型。

缺省情况下，接口的链路类型为 Hybrid。

步骤 4 根据需要，选择执行以下命令：

- 将 Hybrid 接口以 Tagged 方式加入 VLAN，执行命令 **port hybrid tagged vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>。
- 将 Hybrid 接口以 Untagged 方式加入 VLAN，执行命令 **port hybrid untagged vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>。

缺省情况下，Hybrid 类型接口以 Untagged 方式加入 VLAN1。

----结束

3.4.5 （可选）设置 Trunk 类型接口缺省 VLAN

背景信息

请在需要设置 Trunk 类型接口缺省 VLAN 的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type trunk**，将接口配置成 Trunk 类型接口。

缺省情况下，接口的链路类型为 Hybrid。

步骤 4 执行命令 **port trunk pvid vlan** *vlan-id*，设置 Trunk 类型接口的缺省 VLAN。

缺省情况下，Trunk 类型接口的缺省 VLAN 为 VLAN1。

设置接口缺省 VLAN 后，接口并没有加入该 VLAN，如需转发缺省 VLAN 的报文，还需要将接口加入该 VLAN。

----结束

3.4.6 （可选）设置 Hybrid 类型接口缺省 VLAN

背景信息

请在需要设置 Hybrid 类型接口缺省 VLAN 的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type hybrid**，将接口配置成 Hybrid 类型接口。

缺省情况下，接口的链路类型为 Hybrid。

步骤 4 执行命令 **port hybrid pvid vlan** *vlan-id*，设置 Hybrid 类型接口的缺省 VLAN。

缺省情况下，Hybrid 类型接口的缺省 VLAN 为 VLAN1。

设置接口缺省 VLAN 后，接口并没有加入该 VLAN，如需转发缺省 VLAN 的报文，还需要将接口加入该 VLAN。

----结束

3.4.7 检查配置结果

操作步骤

- 使用命令 **display interface** [*interface-type* [*interface-number*]] 查看接口的 PVID。
- 使用命令 **display vlan** [*vlan-id*] 查看 VLAN 的基本信息。

----结束

任务示例

执行命令 **display interface** [*interface-type* [*interface-number*]]，可以查看到接口 Ethernet2/0/0 的 PVID 为 6。

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port,PVID :    6,The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
Last physical up time   : -
Last physical down time : 2009-04-19 18:25:51
Port Mode: COMMON FIBER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi    : NORMAL
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Total Error:              0

  CRC:                    0,  Giants:                   0
  Jabbers:                0,  Throttles:                0
```

```
  Runts:                    0,  DropEvents:                0
  Alignments:               0,  Symbols:                   0
  Ignoreds:                 0,  Frames:                    0

Output:  0 packets, 0 bytes
  Unicast:                  0,  Multicast:                 0
  Broadcast:                0,  Jumbo:                     0
  Discard:                  0,  Total Error:               0

  Collisions:               0,  ExcessiveCollisions:       0
  Late Collisions:          0,  Deferreds:                 0
  Buffers Purged:           0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

执行命令 **display vlan** [*vlan-id*]，可以查看到接口 Ethernet2/0/1 已加入到 VLAN2 中。

```
<Huawei> display vlan 2
* : management-vlan
----------------------
VLAN ID Type    Status   MAC Learning Broadcast/Multicast/Unicast Property
------------------------------------------------------------
2       common  enable   enable       forward   forward   forward default
----------------
Untagged      Port: Ethernet2/0/1
----------------
Active Untag  Port: Ethernet2/0/1
----------------
Interface                 Physical
Ethernet2/0/1             UP
```

3.5 配置 VLANIF 接口实现三层互通

介绍配置 VLANIF 接口实现三层互通的过程与步骤。

3.5.1 建立配置任务

应用环境

当 AR2200-S 需要与网络层的设备通信时，可以在 AR2200-S 上创建基于 VLAN 的逻辑接口，即 VLANIF 接口。VLANIF 接口是网络层接口，可以配置 IP 地址。借助 VLANIF 接口，AR2200-S 就能与其它网络层的设备互相通信。

前置任务

在配置 VLANIF 接口之前，需完成以下任务：

- 创建 VLAN

数据准备

在配置 VLANIF 接口之前，需要准备以下数据。

序号	数据
1	VLAN 的编号
2	VLANIF 接口的 IP 地址

3.5.2 创建 VLANIF 接口

背景信息

请在需要配置 VLANIF 接口的 AR2200-S 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 **interface vlanif** *vlan-id*，创建 VLANIF 接口并进入 VLANIF 接口视图。

说明

当 VLAN 内存在 UP 的物理端口时，该 VLAN 的 VLANIF 接口才会 UP。

----结束

3.5.3 配置 VLANIF 接口的 IP 地址

背景信息

请在需要配置 VLANIF 接口的 AR2200-S 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 **interface vlanif** *vlan-id*，创建 VLANIF 接口并进入 VLANIF 接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

----结束

3.5.4 （可选）配置 VLANIF 接口的 MTU

背景信息

- 使用 **mtu** 命令改变接口最大传输单元 MTU 后，需要重启接口以保证配置的 MTU 生效。可以先执行 **shutdown** 命令将接口关闭，再执行 **undo shutdown** 命令将接口重启；也可以在接口视图下执行 **restart** 命令重启接口。
- 如果使用 **mtu** 命令改变接口 MTU 的值，请同时修改与本设备相连的其他设备的 MTU 值，确保两端设备的 MTU 值匹配。否则，可能导致业务中断。

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 vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 3 执行命令 **mtu** *mtu*，配置 VLANIF 接口的 MTU。

最大传输单元 MTU（Maximum Transmission Unit）单位为字节，VLANIF 接口 MTU 的取值范围为 46 ～ 1500。缺省值为 1500。

说明

由于 QoS（Quality of Service）队列长度有限，如果 MTU 太小而报文尺寸较大，可能会造成分片过多，报文被 QoS 队列丢弃。为避免这种情况，可适当增大 QoS 队列的长度。

----结束

3.5.5 （可选）配置 VLAN Damping 功能

背景信息

请在 VLANIF 接口上进行以下配置。

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 **interface vlanif** *interface-number*，进入指定的 VLANIF 接口视图。

VLANIF 接口关联的 VLAN 已经创建。

步骤 3 执行命令 **damping time** *delay-time*，设置抑制时间。

取值范围是 0 ～ 20，单位是秒。

缺省情况下，抑制时间为 0 秒，即为不进行抑制。

----结束

3.5.6 检查配置结果

操作步骤

步骤 1 使用命令 **display interface vlanif** [*vlan-id*] 查看 VLANIF 接口的基本配置信息。

----结束

任务示例

执行命令 **display interface vlanif**，可以查看 VLANIF 接口的 IP 地址是否配置正确。

```
<Huawei> display interface vlanif
Vlanif5 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Vlanif5 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
```

```
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-00e1
Current system time: 2011-02-09 19:45:40
    Input bandwidth utilization  : --
    Output bandwidth utilization : --

Vlanif10 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.10.10.20/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-00e1
Current system time: 2011-02-09 19:45:40
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

3.6 配置 VLAN 聚合

介绍解决多个 VLAN 占用 IP 地址过多的问题的配置方法。

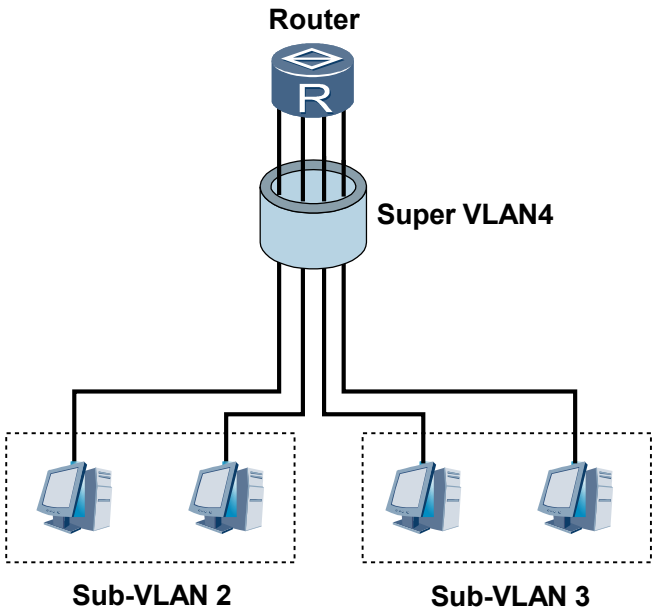
3.6.1 建立配置任务

应用环境

VLAN 聚合（VLAN aggregation）用于解决多个 VLAN 占用多个 IP 地址的问题。

如图 3-1 所示，VLAN 聚合将多个 VLAN 集中在一起，形成一个 super-VLAN。组成 super-VLAN 的 VLAN 被称作 sub-VLAN，所有 sub-VLAN 共用一个 IP 网段。

图 3-1 VLAN 聚合应用场景图



当以太网存在大量 VLAN 时，配置 VLAN 聚合还可以简化配置。

前置任务

在配置 VLAN 聚合之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置 VLAN 聚合之前，需准备以下数据。

序号	数据
1	sub-VLAN 的 VLAN ID 及其包含的端口编号
2	super-VLAN 的 VLAN ID
3	VLANIF 接口的 IP 地址和掩码

3.6.2 配置 Sub-VLAN

背景信息

请在需要实现 VLAN 聚合的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port link-type access**，配置 Access 类型接口。

步骤 4 执行命令 **quit**，退出接口视图。

步骤 5 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 6 执行命令 **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>，配置 VLAN 包含的端口。

----结束

3.6.3 创建 Super-VLAN

背景信息

请在需要实现 VLAN 聚合的 AR2200-S 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 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **aggregate-vlan**，设置该 VLAN 为 super-VLAN。

super-VLAN 与 sub-VLAN 必须使用不同的 VLAN ID，super-VLAN 中不能包含任何物理端口。

步骤 4 执行命令 **access-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，将 sub-VLAN 加入到 super-VLAN 中。

目前 AR2200-S 最多支持 16 个 sub-VLAN 加入到同一 super-VLAN 中。

----结束

3.6.4 配置 VLANIF 接口的 IP 地址

背景信息

请在需要实现 VLAN 聚合的 AR2200-S 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 **interface vlanif** *vlan-id*，创建 VLANIF 接口并进入 VLANIF 接口视图。

由于只能创建 Super-VLAN 对应的 VLANIF 接口，Sub-VLAN 不允许创建对应的 VLANIF 接口。因此，参数 *vlan-id* 是创建 Super-VLAN 时指定的 VLAN ID。

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

VLANIF 接口的 IP 地址所在的网段应包含各 sub-VLAN 用户所在的子网段。

----结束

3.6.5 配置 Super-VLAN 的 Proxy ARP

背景信息

请在需要启动 ARP 代理的 AR2200-S 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 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

参数 *vlan-id* 是创建 Super-VLAN 时指定的 VLAN ID。

步骤 3 执行命令 **arp-proxy inter-sub-vlan-proxy enable**，使能 Sub-VLAN 间的 ARP 代理。

----结束

3.6.6 检查配置结果

操作步骤

- 使用命令 **display vlan** [*vlan-id* [**verbose**]] 查看 VLAN 信息。
- 使用命令 **display interface vlanif** [*vlan-id*] 显示 VLANIF 接口信息。

----结束

任务示例

执行命令 **display vlan verbose**，可以看到 VLAN 类型。例如：

```
<Huawei> display vlan 2 verbose
* : Management-VLAN
----------------------
  VLAN ID                     : 2
  VLAN Name                   :
  VLAN Type                   : Super
  Description                 : VLAN 0002
  Status                      : Enable
  Broadcast                   : Enable
  MAC Learning                : Enable
  Smart MAC Learning          : Disable
  Current MAC Learning Result : Enable
  Statistics                  : Disable
  Property                    : Default
  VLAN State                  : Down
---------------
sub-VLAN List: 20
```

执行命令 **display interface vlanif**，可以看到 VLANIF 接口物理状态、链路协议状态、IP 地址和掩码等信息。例如：

```
<Huawei> display interface vlanif 2
Vlanif2 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Vlanif2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc03-0205
Current system time: 2007-09-09 19:29:45
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

3.7 配置 MUX VLAN

介绍如何配置 VLAN 内接口隔离。

3.7.1 建立配置任务

应用环境

MUX VLAN 提供了一种在 VLAN 的端口间进行二层流量隔离的机制。比如在企业网络中，客户端口可以和服务器端口通讯，但客户端口间不能互相通信。

MUX VLAN 分为主 VLAN 和从 VLAN，从 VLAN 又分为互通型从 VLAN 和隔离型从 VLAN。

主 VLAN 与从 VLAN 之间可以相互通信，不同从 VLAN 之间不能互相通信。互通型从 VLAN 端口之间可以互相通信，隔离型从 VLAN 端口之间不能互相通信。

前置任务

在配置 MUX VLAN 之前，需完成以下任务：

- 创建 VLAN

数据准备

在配置 MUX VLAN 之前，需准备以下数据。

序号	数据
1	主 VLAN 的 VLAN ID 及其包含的端口编号
2	互通型从 VLAN 的 VLAN ID 及其包含的端口编号
3	隔离型从 VLAN 的 VLAN ID 及其包含的端口编号

3.7.2 配置主 VLAN

背景信息

请在需要实现 MUX VLAN 的 AR2200-S 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 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **mux-vlan**，配置 MUX VLAN 的主 VLAN。

目前 AR2200-S 支持配置 128 个主 VLAN，每个主 VLAN 中最多加入 1632 个从 VLAN。

----结束

3.7.3 配置从 VLAN

背景信息

请在需要实现 MUX VLAN 的 AR2200-S 上进行以下配置。

操作步骤

- 配置 MUX VLAN 中的互通型从 VLAN
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入主 VLAN 视图。
  3. 执行命令 **subordinate group** *vlan-id1* [**to** *vlan-id2*]用来配置主 vlan 下的互通型从 vlan。

说明

vlan-id1 和 *vlan-id2* 表示被配置的 VLAN 的编号，整数形式，取值范围是 1 ~ 4094。*vlan-id2* 的取值必须大于 *vlan-id1* 的取值。

- 配置 MUX VLAN 中的隔离型从 VLAN
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入主 VLAN 视图。
  3. 执行命令 **subordinate separate** *vlan-id*，用来配置主 vlan 下的隔离型从 vlan。

----结束

3.7.4 配置接口 MUX VLAN 功能

背景信息

请在需要实现 MUX VLAN 的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port mux-vlan enable**，用来使能端口的 MUX VLAN 功能。

说明

- MAC 地址学习限制可能会影响 MUX VLAN 功能的正常使用。
- 对于同一接口，不支持同时配置接口安全功能和端口使能 MUX-VLAN。

----结束

3.7.5 检查配置结果

操作步骤

步骤 1 使用命令 **display mux-vlan** 查看 VLAN 信息。

----结束

任务示例

执行命令 **display mux-vlan**，可以看到配置的 MUX VLAN。例如：

```
<Huawei> display mux-vlan
Principal Subordinate Type      Interface
------------------------------------------------------------------------------
100       -           principal
100       120         separate    Ethernet2/0/1
100       130         group       Ethernet2/0/2
100       140         group       Ethernet2/0/3
------------------------------------------------------------------------------
```

3.8 配置管理 VLAN

介绍配置管理 VLAN 的配置方法。

3.8.1 建立配置任务

应用环境

接口以 access 类型加入的 VLAN 一般为用户 VLAN，用于管理的 VLAN 一般禁止接口以 access 类型加入。

将 VLAN 配置成管理 VLAN 后，加入该 VLAN 的接口必须为 trunk 或 hybrid 类型，可以提高设备的安全性。

用户一般使用管理 VLAN 的 VLANIF 接口来登录管理设备。

前置任务

在配置管理 VLAN 之前，需要完成以下任务：

- 创建 VLAN

数据准备

在管理 VLAN 之前，需准备以下数据。

序号	数据
1	VLAN 编号

3.8.2 配置管理 VLAN 功能

背景信息

请在需要配置管理 VLAN 的 AR2200-S 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 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **management-vlan**，配置管理 VLAN。

----结束

3.8.3 检查配置结果

操作步骤

步骤 1 使用命令 **display vlan** 查看管理 VLAN 的配置信息。

----结束

任务示例

执行命令 **display vlan**，可以看到管理 VLAN 的配置信息，带有*的 VLAN 为管理 VLAN。例如：

```
<Huawei> display vlan
* : management-vlan
--------------------
The total number of vlans is : 6
VLAN ID Type    Status   MAC Learning Broadcast/Multicast/Unicast Property
--------------------------------------------------------------------------------
1       common  enable   enable       forward   forward   forward default
93      common  enable   enable       forward   forward   forward default
95      common  enable   enable       forward   forward   forward default
100     super   enable   enable       forward   forward   forward default
202     mux     enable   enable       forward   forward   forward default
1000    *common enable   enable       forward   forward   forward default
```

3.9 配置举例

介绍 VLAN 的各种组网举例。

3.9.1 配置基于接口划分 VLAN 示例

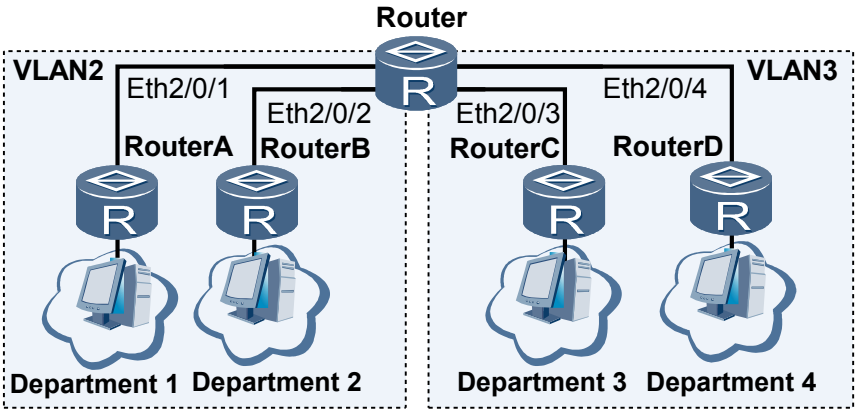
组网需求

某企业有很多部门，要求业务相同部门之间的员工可以互相访问，业务不同部门之间的员工不能互相访问。

如图 3-2 所示，某企业包含 4 个部门。部门 1 通过 RouterA 与 Router 的接口 Eth2/0/1 相连。部门 2 通过 RouterB 与 Router 的接口 Eth2/0/2 相连。部门 3 通过 RouterC 与 Router 的接口 Eth2/0/3 相连。部门 4 通过 RouterD 与 Router 的接口 Eth2/0/4 相连。要求：

- VLAN2 内的部门 1、部门 2 与 VLAN3 内的部门 3、部门 4 互相隔离。
- VLAN2 内的部门 1 与部门 2 可以互相访问。
- VLAN3 内的部门 3 与部门 4 可以互相访问。

图 3-2 配置基于接口划分 VLAN 组网图



配置思路

采用如下的思路配置 VLAN：

1. 创建 VLAN。
2. 将接口加入 VLAN。

数据准备

为完成此配置例，需准备如下的数据：

- 接口 Ethernet2/0/1、Ethernet2/0/2 属于 VLAN2。
- 接口 Ethernet2/0/3、Ethernet2/0/4 属于 VLAN3。

操作步骤

步骤 1 配置 Router

创建 VLAN2。

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] quit
```

将接口 Ethernet2/0/1 的类型为 Trunk，并加入到 VLAN2 中。

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type trunk
[Huawei-Ethernet2/0/1] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/1] quit
```

配置接口 Ethernet2/0/2 的类型为 Trunk，并加入到 VLAN2 中。

```
[Huawei]interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] port link-type trunk
[Huawei-Ethernet2/0/2] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/2] quit
```

创建 VLAN3。

```
[Huawei] vlan 3
[Huawei-vlan3] quit
```

配置接口 Ethernet2/0/3 的类型为 Trunk，并加入到 VLAN3 中。

```
[Huawei] interface ethernet 2/0/3
[Huawei-Ethernet2/0/3] port link-type trunk
[Huawei-Ethernet2/0/3] port trunk allow-pass vlan 3
[Huawei-Ethernet2/0/3] quit
```

将接口 Ethernet2/0/4 的类型为 Trunk，并加入到 VLAN3 中。

```
[Huawei] interface ethernet 2/0/4
[Huawei-Ethernet2/0/4] port link-type trunk
[Huawei-Ethernet2/0/4] port trunk allow-pass vlan 3
[Huawei-Ethernet2/0/4] quit
```

步骤 2 验证配置结果

部门 1、部门 2 所属的 VLAN2 内的任一台主机 ping 部门 3、部门 4 所属的 VLAN3 内的任一台主机，无法 ping 通，证明部门 1、部门 2 与部门 3、部门 4 已实现隔离。

部门 1 的任一台主机 ping 部门 2 的任一台主机，能 ping 通，证明部门 1 与部门 2 已实现互通。

部门 3 的任一台主机 ping 部门 4 的任一台主机，能 ping 通，证明部门 3 与部门 4 已实现互通。

----结束

配置文件

以下仅给出 Router 的配置文件。

```
#
 vlan batch 2 to 3
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface Ethernet2/0/3
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface Ethernet2/0/4
 port link-type trunk
 port trunk allow-pass vlan 3
#
return
```

3.9.2 配置 VLAN 间通过 VLANIF 接口通信示例

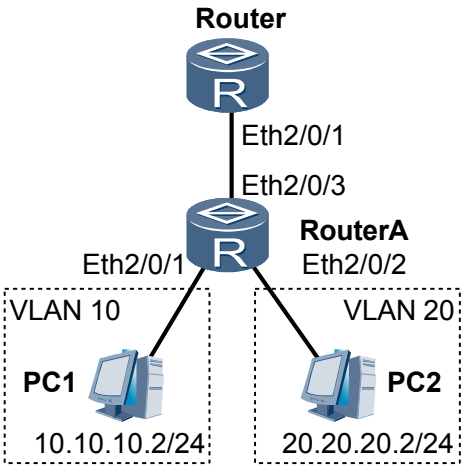
组网需求

如图 3-3 所示，Router 的接口 Eth2/0/1 与 RouterA 上行口相连。

RouterA 的下行接口 Eth2/0/1 加入 VLAN10，下行接口 Eth2/0/2 加入 VLAN20。

要求 VLAN10 内的 PC1 与 VLAN20 内的 PC2 能够互相 PING 通。

图 3-3 配置 VLAN 间通过 VLANIF 接口通信组网图



配置思路

采用如下的思路配置不同 VLAN 通过 Router 互相通信：

1. 配置各以太网接口加入 VLAN。
2. 配置 VLANIF 接口。

数据准备

为完成此配置例，需准备如下的数据：

- 在 Router 上配置接口 Eth2/0/1 加入 VLAN10 和 VLAN20。
- 在 Router 上配置 VLANIF10 的 IP 地址为 10.10.10.1/24。
- 在 Router 上配置 VLANIF20 的 IP 地址为 20.20.20.1/24。
- 在 RouterA 上配置接口 Eth2/0/1 加入 VLAN10。
- 在 RouterA 上配置接口 Eth2/0/2 加入 VLAN20。
- 在 RouterA 上配置接口 Eth2/0/3 加入 VLAN10 和 VLAN20。

操作步骤

步骤 1 配置 Router

创建 VLAN

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

配置接口加入 VLAN

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type trunk
[Router-Ethernet2/0/1] port trunk allow-pass vlan 10 20
[Router-Ethernet2/0/1] quit
```

配置 VLANIF 接口的 IP 地址

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.10.10.1 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 20.20.20.1 24
[Router-Vlanif20] quit
```

步骤 2 配置 RouterA

创建 VLAN

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10 20
```

配置接口加入 VLAN

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1] port default vlan 10
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type access
[RouterA-Ethernet2/0/2] port default vlan 20
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet 2/0/3
[RouterA-Ethernet2/0/3] port link-type trunk
[RouterA-Ethernet2/0/3] port trunk allow-pass vlan 10 20
[RouterA-Ethernet2/0/3] quit
```

步骤 3 检查配置结果

在 VLAN10 中的 PC1 上配置缺省网关为 VLANIF10 接口的 IP 地址 10.10.10.1/24。

在 VLAN20 中的 PC2 上配置缺省网关为 VLANIF20 接口的 IP 地址 20.20.20.1/24。

配置完成后，VLAN10 内的 PC1 与 VLAN20 内的 PC2 能够相互访问。

----结束

配置文件

Router 的配置文件。

```
#
 sysname Router
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

RouterA 的配置文件。

```
#
 sysname RouterA
#
 vlan batch 10 20
#
```

```
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 20
#
interface Ethernet2/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

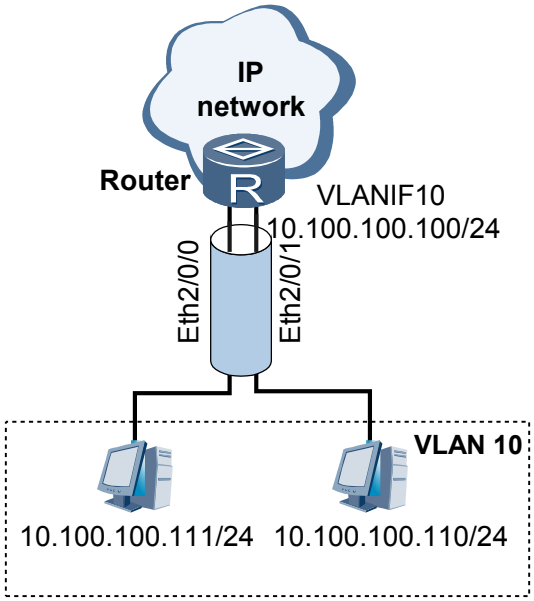
3.9.3 配置 VLAN Damping 示例

组网需求

如图 3-4 所示，VLAN10 中的主机通过 VLANIF10 接口跟 VLAN10 外部的主机通信。

在 VLANIF10 上配置 VLAN Damping，防止 VLANIF 接口状态变化引起网络震荡。

图 3-4 配置 VLAN Damping 组网图



配置思路

采用如下的思路配置 VLAN：

1. 创建 VLAN。
2. 配置接口加入 VLAN。
3. 创建 VLANIF 接口，并配置 IP 地址。
4. 在 VLANIF 接口上配置抑制时间。

数据准备

为完成此配置例，需准备如下的数据。

- VLAN 编号
- 接口编号
- VLANIF 接口编号
- VLANIF 接口的 IP 地址为 10.100.100.100/24
- 抑制时间为 20 秒

操作步骤

步骤 1 创建 VLAN

创建 VLAN 10

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10
```

步骤 2 配置接口加入 VLAN

将 Eth2/0/0 加入 VLAN 10。

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] quit
```

将 Eth2/0/1 加入 VLAN 10。

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 10
[Router-Ethernet2/0/1] quit
```

步骤 3 创建 VLANIF10

创建 VLANIF10，并配置 IP 地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.100.100.100 24
```

步骤 4 配置抑制时间

配置抑制时间为 20 秒。

```
[Router-Vlanif10] damping time 20
```

步骤 5 检查配置结果

在 Router 上执行 **display interface vlanif** 命令，检查配置的抑制时间。

```
<Router> display interface vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2008-01-25 09:05:13
Description:HUAWEI, AR Series, Vlanif10 Interface
Route Port,The Maximum Transmit Unit is 1500, The Holdoff Timer is 20(sec)
Internet Address is 10.100.100.100/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-0005
Current system time: 2008-01-25 09:05:37
```

```
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

----结束

配置文件

```
#
 sysname Router
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.100.100.100 255.255.255.0
 damping time 20
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
#
return
```

3.9.4 配置 VLAN 聚合示例

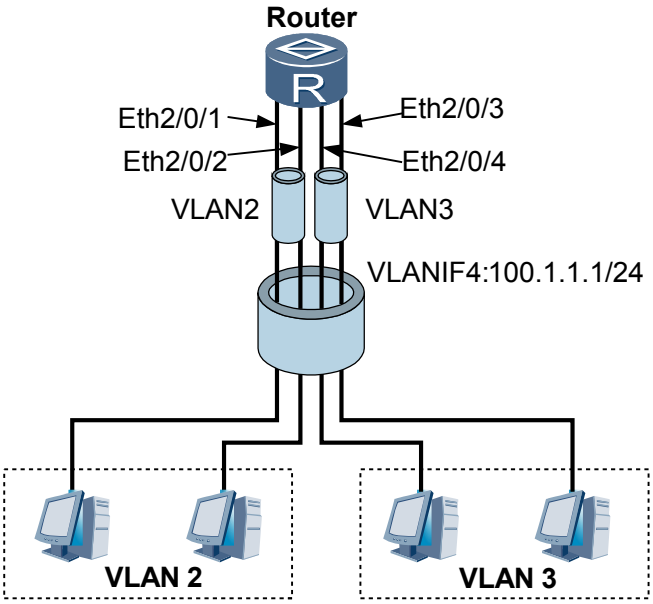
组网需求

如图 3-5 所示，VLAN2 和 VLAN3 组成 super-VLAN：VLAN4。

作为 sub-VLAN 的 VLAN2 和 VLAN3 之间不能互相 ping 通。

配置 Proxy ARP 后，VLAN2 和 VLAN3 之间可以互相 ping 通。

图 3-5 配置 VLAN 聚合组网图



配置思路

采用如下思路配置 VLAN 聚合：

1. 把 Router 接口加入到相应的 sub-VLAN 中。
2. 把 sub-VLAN 聚合为 super-VLAN。
3. 配置 super-VLAN 的 IP 地址。
4. 配置 super-VLAN 的 Proxy ARP。

数据准备

为完成此配置例，需准备如下的数据：

- Eth2/0/1 和 Eth2/0/2 属于 VLAN2
- Eth2/0/3 和 Eth2/0/4 属于 VLAN3
- super-VLAN 的 ID 为 4
- super-VLAN 的 IP 地址为 100.1.1.1

操作步骤

步骤 1 配置接口类型

配置接口 Eth2/0/1 为 Access 类型。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type access
[Huawei-Ethernet2/0/1] quit
```

配置接口 Eth2/0/2 为 Access 类型。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] port link-type access
[Huawei-Ethernet2/0/2] quit
```

配置接口 Eth2/0/3 为 Access 类型。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/3
[Huawei-Ethernet2/0/3] port link-type access
[Huawei-Ethernet2/0/3] quit
```

配置接口 Eth2/0/4 为 Access 类型。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/4
[Huawei-Ethernet2/0/4] port link-type access
[Huawei-Ethernet2/0/4] quit
```

步骤 2 配置 VLAN2

创建 VLAN2。

```
[Huawei] vlan 2
```

向 VLAN2 中加入 Eth2/0/1 和 Eth2/0/2。

```
[Huawei-vlan2] port ethernet 2/0/1 2/0/2
[Huawei-vlan2] quit
```

步骤 3 配置 VLAN3

创建 VLAN3。

```
[Huawei] vlan 3
```

向 VLAN3 中加入 Eth2/0/3 和 Eth2/0/4。

```
[Huawei-vlan3] port ethernet 2/0/3 2/0/4
[Huawei-vlan3] quit
```

步骤 4 配置 VLAN4

配置 super-VLAN。

```
[Huawei] vlan 4
[Huawei-vlan4] aggregate-vlan
[Huawei-vlan4] access-vlan 2 to 3
```

配置 VLANIF。

```
[Huawei] interface vlanif 4
[Huawei-Vlanif4] ip address 100.1.1.1 255.255.255.0
[Huawei-Vlanif4] quit
```

步骤 5 配置 PC

分别为各 PC 配置 IP 地址，并使它们和 VLAN4 处于同一网段。

配置成功后，各 PC 与 Router 之间可以相互 ping 通，但 VLAN2 的 PC 与 VLAN3 的 PC 间不可以相互 ping 通。

步骤 6 配置 Proxy ARP

```
[Huawei] interface vlanif 4
[Huawei-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
```

步骤 7 检查配置结果

配置完成后，VLAN2 的 PC 与 VLAN3 的 PC 间可以相互 ping 通。

----结束

配置文件

Router 的配置文件

```
#
vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
#
interface Vlanif4
 ip address 100.1.1.1 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 2
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 2
#
interface Ethernet2/0/3
```

```
 port link-type access
 port default vlan 3
#
interface Ethernet2/0/4
 port link-type access
 port default vlan 3
#
return
```

3.9.5 配置 MUX VLAN 示例

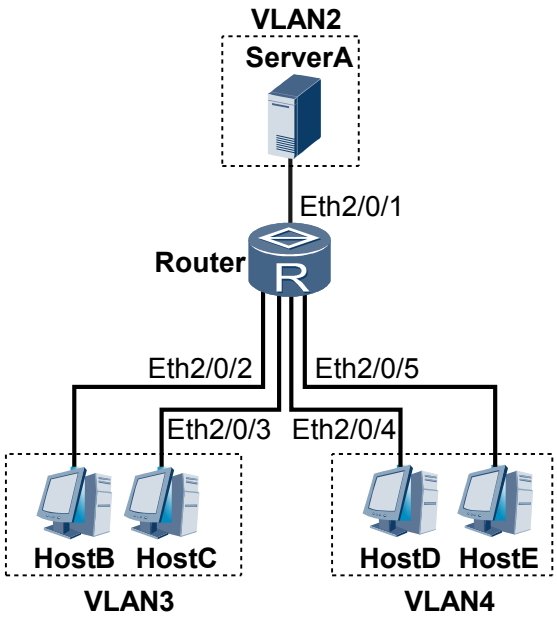
组网需求

在企业网络中，企业希望某些部门之间的员工是互相隔离的，某些部门之间的员工是可以互相访问的，并且所有部门的员工都可以访问公司的服务器。

为了解决上述问题，可在 AR2200-S 上部署 MUX VLAN 功能。将企业服务器划分在主 VLAN 内，需要互相访问的部门员工划分在互通型从 VLAN 内，需要互相隔离的部门员工划分在隔离型从 VLAN 内，即可解决上述问题，且不会耗费大量的 VLAN ID。

如图 3-6 所示，Eth2/0/1 与 ServerA 相连，Eth2/0/2 与 HostB 相连，Eth2/0/3 与 HostC 相连，Eth2/0/4 与 HostD 相连，Eth2/0/5 与 HostE 相连。将 Router 设备上创建 VLAN2 为主 VLAN，加入端口 Eth2/0/1，创建 VLAN3 作为 group VLAN，加入端口 Eth2/0/2 和 Eth2/0/3，创建 VLAN4 作为 separate VLAN，加入端口 Eth2/0/4 和 Eth2/0/5。

图 3-6 配置 MUX-VLAN 组网图



配置思路

采用如下思路配置 MUX-VLAN 功能：

1. 配置主 VLAN 的 MUX-VLAN 功能。

2. 配置 Group-VLAN 功能。
3. 配置 Separate-VLAN 功能。
4. 配置接口加入 VLAN 并使能 MUX-VLAN 功能。

数据准备

为完成此配置例，需准备如下的数据：

- Eth2/0/1 属于 VLAN2
- Eth2/0/2 和 Eth2/0/3 属于 VLAN3
- Eth2/0/4 和 Eth2/0/5 属于 VLAN4

操作步骤

步骤 1 配置 MUX VLAN

创建 VLAN2、VLAN3 和 VLAN4。

```
<Huawei> system-view
[Huawei] vlan batch 2 3 4
[Huawei] quit
```

配置 MUX VLAN 中的主 VLAN 和从 VLAN。

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] mux-vlan
[Huawei-vlan2] subordinate group 3
[Huawei-vlan2] subordinate separate 4
[Huawei-vlan2] quit
```

配置接口加入 VLAN 并使能 MUX VLAN 功能。

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type access
[Huawei-Ethernet2/0/1] port default vlan 2
[Huawei-Ethernet2/0/1] port mux-vlan enable
[Huawei-Ethernet2/0/1] quit
[Huawei] interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] port link-type access
[Huawei-Ethernet2/0/2] port default vlan 3
[Huawei-Ethernet2/0/2] port mux-vlan enable
[Huawei-Ethernet2/0/2] quit
[Huawei] interface ethernet 2/0/3
[Huawei-Ethernet2/0/3] port link-type access
[Huawei-Ethernet2/0/3] port default vlan 3
[Huawei-Ethernet2/0/3] port mux-vlan enable
[Huawei-Ethernet2/0/3] quit
[Huawei] interface ethernet 2/0/4
[Huawei-Ethernet2/0/4] port link-type access
[Huawei-Ethernet2/0/4] port default vlan 4
[Huawei-Ethernet2/0/4] port mux-vlan enable
[Huawei-Ethernet2/0/4] quit
[Huawei] interface ethernet 2/0/5
[Huawei-Ethernet2/0/5] port link-type access
[Huawei-Ethernet2/0/5] port default vlan 4
[Huawei-Ethernet2/0/5] port mux-vlan enable
[Huawei-Ethernet2/0/5] quit
```

步骤 2 检查配置结果

ServerA 和 HostB、HostC、HostD、HostE 都可以互相 ping 通。

HostB 和 HostC 可以互相 ping 通。

HostD 和 HostE 不可以互相 ping 通。

HostB、HostC 和 HostD、HostE 不可以互相 ping 通。

----结束

配置文件

Router 的配置文件

```
#
 sysname Huawei
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate group 3
 subordinate separate 4
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 2
 port mux-vlan enable
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface Ethernet2/0/3
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface Ethernet2/0/4
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface Ethernet2/0/5
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
return
```

3.9.6 配置跨设备 MUX VLAN 示例

组网需求

在企业网络中，企业希望某些部门之间的员工是互相隔离的，某些部门之间的员工是可以互相访问的，并且所有部门的员工都可以访问公司的某些服务器。

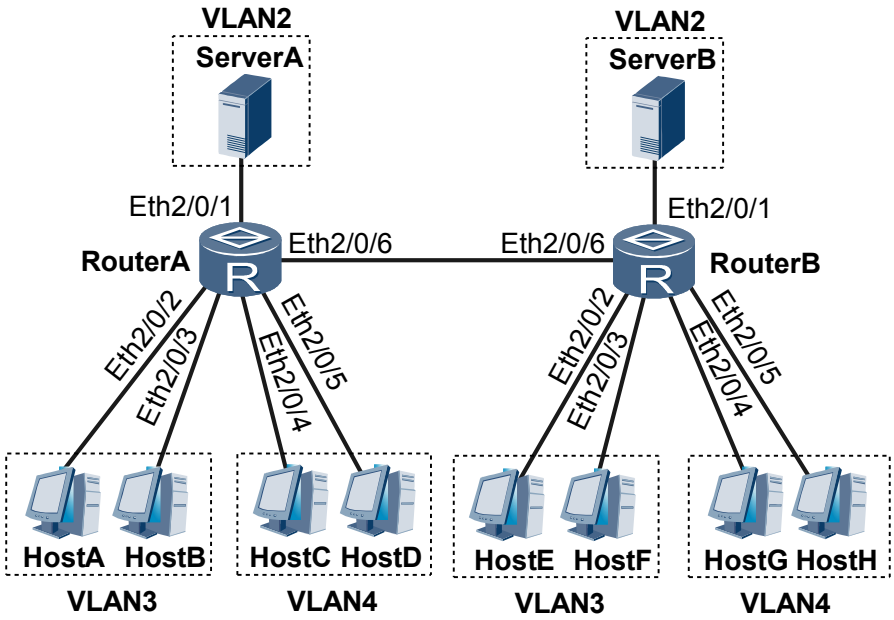
为了解决上述问题，可在 AR2200-S 上部署 MUX VLAN 功能。将企业服务器划分在主 VLAN 内，需要互相访问的部门员工划分在互通型从 VLAN 内，需要互相隔离的部门员工划分在隔离型从 VLAN 内，即可解决上述问题，且不会耗费大量的 VLAN ID。

当企业网络中的服务器和员工分布在多台 AR2200-S 设备上时，可以部署跨设备的 MUX VLAN 功能解决上述问题。

如图 3-7 所示，Eth2/0/1 与服务器相连，Eth2/0/2、Eth2/0/3、Eth2/0/4 和 Eth2/0/5 与主机相连，Router 之间通过 Eth2/0/6 相连。在 Router 设备上创建 VLAN2 为主 VLAN，加入

端口 Eth2/0/1，创建 VLAN3 作为 group VLAN，加入端口 Eth2/0/2 和 Eth2/0/3，创建 VLAN4 作为separate VLAN，加入端口 Eth2/0/4 和 Eth2/0/5，并配置 Eth2/0/6 允许 VLAN2、VLAN3 和 VLAN4 通过。

图 3-7 配置 MUX-VLAN 组网图



配置思路

采用如下思路配置 MUX-VLAN 功能：

1. 配置主 VLAN 的 MUX-VLAN 功能。
2. 配置 Group-VLAN 功能。
3. 配置 Separate-VLAN 功能。
4. 配置接口加入 VLAN 并使能 MUX-VLAN 功能。
5. 配置 Router 之间的接口允许所有 MUX-VLAN 通过。

数据准备

为完成此配置例，需准备如下的数据：

- Eth2/0/1 属于 VLAN2
- Eth2/0/2 和 Eth2/0/3 属于 VLAN3
- Eth2/0/4 和 Eth2/0/5 属于 VLAN4
- Eth2/0/6 允许 VLAN2、VLAN3 和 VLAN4 通过

操作步骤

步骤 1 配置 RouterA 的 MUX VLAN

创建 VLAN2、VLAN3 和 VLAN4。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 2 3 4
[RouterA] quit
```

配置 MUX VLAN 中的主 VLAN 和从 VLAN。

```
<RouterA> system-view
[RouterA] vlan 2
[RouterA-vlan2] mux-vlan
[RouterA-vlan2] subordinate group 3
[RouterA-vlan2] subordinate separate 4
[RouterA-vlan2] quit
```

配置接口 Eth2/0/1 ～ Eth2/0/5 加入 VLAN 并使能 MUX VLAN 功能。

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1] port default vlan 2
[RouterA-Ethernet2/0/1] port mux-vlan enable
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type access
[RouterA-Ethernet2/0/2] port default vlan 3
[RouterA-Ethernet2/0/2] port mux-vlan enable
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet 2/0/3
[RouterA-Ethernet2/0/3] port link-type access
[RouterA-Ethernet2/0/3] port default vlan 3
[RouterA-Ethernet2/0/3] port mux-vlan enable
[RouterA-Ethernet2/0/3] quit
[RouterA] interface ethernet 2/0/4
[RouterA-Ethernet2/0/4] port link-type access
[RouterA-Ethernet2/0/4] port default vlan 4
[RouterA-Ethernet2/0/4] port mux-vlan enable
[RouterA-Ethernet2/0/4] quit
[RouterA] interface ethernet 2/0/5
[RouterA-Ethernet2/0/5] port link-type access
[RouterA-Ethernet2/0/5] port default vlan 4
[RouterA-Ethernet2/0/5] port mux-vlan enable
[RouterA-Ethernet2/0/5] quit
```

配置接口 Eth2/0/6 允许所有 MUX VLAN 通过。

```
[RouterA] interface ethernet 2/0/6
[RouterA-Ethernet2/0/6] port link-type trunk
[RouterA-Ethernet2/0/6] port trunk allow-pass vlan 2 to 4
[RouterA-Ethernet2/0/6] quit
```

步骤 2 配置 RouterB 的 MUX VLAN

创建 VLAN2、VLAN3 和 VLAN4。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan batch 2 3 4
[RouterB] quit
```

配置 MUX VLAN 中的主 VLAN 和从 VLAN。

```
<RouterB> system-view
[RouterB] vlan 2
[RouterB-vlan2] mux-vlan
[RouterB-vlan2] subordinate group 3
[RouterB-vlan2] subordinate separate 4
[RouterB-vlan2] quit
```

配置接口 Eth2/0/1 ～ Eth2/0/5 加入 VLAN 并使能 MUX VLAN 功能。

```
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port link-type access
```

```
[RouterB-Ethernet2/0/1] port default vlan 2
[RouterB-Ethernet2/0/1] port mux-vlan enable
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] port link-type access
[RouterB-Ethernet2/0/2] port default vlan 3
[RouterB-Ethernet2/0/2] port mux-vlan enable
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] port link-type access
[RouterB-Ethernet2/0/3] port default vlan 3
[RouterB-Ethernet2/0/3] port mux-vlan enable
[RouterB-Ethernet2/0/3] quit
[RouterB] interface ethernet 2/0/4
[RouterB-Ethernet2/0/4] port link-type access
[RouterB-Ethernet2/0/4] port default vlan 4
[RouterB-Ethernet2/0/4] port mux-vlan enable
[RouterB-Ethernet2/0/4] quit
[RouterB] interface ethernet 2/0/5
[RouterB-Ethernet2/0/5] port link-type access
[RouterB-Ethernet2/0/5] port default vlan 4
[RouterB-Ethernet2/0/5] port mux-vlan enable
[RouterB-Ethernet2/0/5] quit
```

配置接口 Eth2/0/6 允许所有 MUX VLAN 通过。

```
[RouterB] interface ethernet 2/0/6
[RouterB-Ethernet2/0/6] port link-type trunk
[RouterB-Ethernet2/0/6] port trunk allow-pass vlan 2 to 4
[RouterB-Ethernet2/0/6] quit
```

步骤 3 检查配置结果

所有从 VLAN 中的主机都可以访问主 VLAN 中的 ServerA 和 ServerB。

互通型从 VLAN 中的主机 HostA、HostB、HostE 和 HostF 之间可以互相访问。

隔离型从 VLAN 中的主机 HostC、HostD、HostG 和 HostH 之间不可以互相访问。

互通型从 VLAN 中的主机和隔离型从 VLAN 中的主机之间也不可以互相访问。

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate group 3
 subordinate separate 4
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 2
 port mux-vlan enable
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
```

```
interface Ethernet2/0/3
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface Ethernet2/0/4
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface Ethernet2/0/5
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface Ethernet2/0/6
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate group 3
 subordinate separate 4
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 2
 port mux-vlan enable
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface Ethernet2/0/3
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface Ethernet2/0/4
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface Ethernet2/0/5
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface Ethernet2/0/6
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
return
```

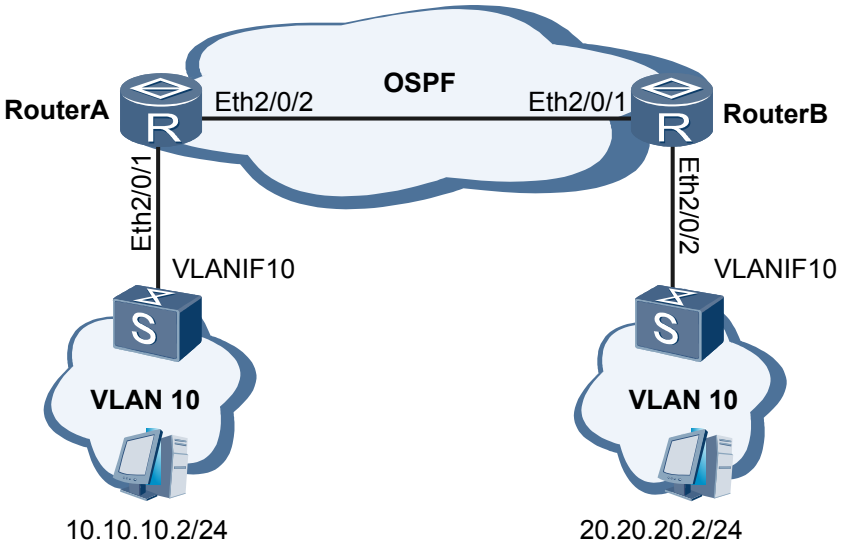
3.9.7 配置通过 VLANIF 接口跨越三层网络通信示例

组网需求

如图 3-8 所示，RouterA 和 RouterB 分别下挂 VLAN10 的二层网络，RouterA 和 RouterB 之间通过三层网络互通，三层网络采用 OSPF 协议。

要求两个二层网络的 PC 实现二层隔离三层互通。

图 3-8 配置通过 VLANIF 接口跨越三层网络通信组网图



配置思路

采用如下的思路配置通过 VLANIF 接口跨越三层网络通信：

1. 配置接口所属的 VLAN。
2. 配置 VLANIF 接口的 IP 地址。
3. 配置 OSPF 基本功能。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 的接口 Eth2/0/1 加入 VLAN 10，VLANIF10 的 IP 地址为 10.10.10.1/24。
- RouterB 的接口 Eth2/0/2 加入 VLAN 10，VLANIF10 的 IP 地址为 20.20.20.1/24。
- RouterA 的接口 Eth2/0/2 加入 VLAN 30，VLANIF30 的 IP 地址为 30.30.30.1/24。
- RouterB 的接口 Eth2/0/1 加入 VLAN 30，VLANIF30 的 IP 地址为 30.30.30.2/24。
- RouterA 下挂的二层网络中 PC 的 IP 地址为 10.10.10.2/24。
- RouterB 下挂的二层网络中 PC 的 IP 地址为 20.20.20.2/24。

操作步骤

步骤 1 配置 RouterA

创建 VLAN

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10 30
```

配置接口加入 VLAN

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan 10
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type trunk
[RouterA-Ethernet2/0/2] port trunk allow-pass vlan 30
[RouterA-Ethernet2/0/2] quit
```

配置 VLANIF 接口的 IP 地址

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 10.10.10.1 24
[RouterA-Vlanif10] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 30.30.30.1 24
[RouterA-Vlanif30] quit
```

配置 OSPF 基本功能

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 30.30.30.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
```

步骤 2 配置 RouterB

创建 VLAN

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan batch 10 30
```

配置接口加入 VLAN

```
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] port link-type trunk
[RouterB-Ethernet2/0/2] port trunk allow-pass vlan 10
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port link-type trunk
[RouterB-Ethernet2/0/1] port trunk allow-pass vlan 30
[RouterB-Ethernet2/0/1] quit
```

配置 VLANIF 接口的 IP 地址

```
[RouterB] interface vlanif 10
[RouterB-Vlanif10] ip address 20.20.20.1 24
[RouterB-Vlanif10] quit
[RouterB] interface vlanif 30
[RouterB-Vlanif30] ip address 30.30.30.2 24
[RouterB-Vlanif30] quit
```

配置 OSPF 基本功能

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 20.20.20.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 30.30.30.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

步骤 3 检查配置结果

RouterA 下挂的二层网络中 PC 上配置缺省网关为 VLANIF10 接口的 IP 地址 10.10.10.1/24。

RouterB 下挂的二层网络中 PC 上配置缺省网关为 VLANIF10 接口的 IP 地址 20.20.20.1/24。

配置完成后，两个二层网络的 PC 实现二层隔离三层互通。

----结束

配置文件

RouterA 的配置文件。

```
#
 sysname RouterA
#
 router id 1.1.1.1
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif30
 ip address 30.30.30.1 255.255.255.0
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.10.10.0 0.0.0.255
  network 30.30.30.0 0.0.0.255
#
return
```

RouterB 的配置文件。

```
#
 sysname RouterB
#
 router id 2.2.2.2
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 20.20.20.1 255.255.255.0
#
interface Vlanif30
 ip address 30.30.30.2 255.255.255.0
#
interface Ethernet2/0/1
```

```
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 20.20.20.0 0.0.0.255
  network 30.30.30.0 0.0.0.255
#
return
```

4 Voice VLAN 配置

关于本章

介绍配置 Voice VLAN 的过程与步骤。

4.1 Voice VLAN 概述
简要介绍 Voice VLAN 的概念。

4.2 AR2200-S 支持的 Voice VLAN 特性
介绍 Voice VLAN 特性在 AR2200-S 中的支持情况。

4.3 配置 Voice VLAN
介绍配置 Voice VLAN 的过程与步骤。

4.4 配置举例
介绍 Voice VLAN 的各种组网举例。

4.1 Voice VLAN 概述

简要介绍 Voice VLAN 的概念。

网络中有 HSI（High Speed Internet）、VoIP（Voice over IP）和 IPTV（Internet Protocol Television）等各种数据流，其中用户对语音通话质量较敏感，为保证用户的语音通话质量，需要提高语音数据流的传输优先级和指定独有传输路径。

Voice VLAN 是为用户的语音数据流划分的 VLAN。用户通过创建 Voice VLAN 并将连接语音设备的接口加入到 Voice VLAN 中，使语音数据流集中在 Voice VLAN 中进行传输。采用 Voice VLAN 的方式，还可以提高语音数据流的传输优先级，便于对语音数据流进行有针对性的 QoS（Quality of Service）配置，以保证通话质量。

4.2 AR2200-S 支持的 Voice VLAN 特性

介绍 Voice VLAN 特性在 AR2200-S 中的支持情况。

语音数据流的识别方式

AR2200-S 根据进入接口数据流中的源 MAC 地址来判断该数据流是否为语音数据流，当源 MAC 地址匹配系统配置的 OUI（Organizationally Unique Identifier）地址时，认为该数据流为语音数据流。

OUI 地址一般配置为 MAC 地址的前 24 位，是 IEEE（Institute of Electrical and Electronics Engineers）为不同设备供应商分配的一个全球唯一的标识符，从 OUI 地址可以判断出该设备是哪一个厂商的产品。

AR2200-S 支持配置 16 个 OUI 地址，并且可以通过设定不同的 MAC 地址掩码来调节匹配深度。

接口加入 Voice VLAN 的模式

用户可以根据每个连接语音设备接口中数据流的实际情况，设定接口加入 Voice VLAN 的模式。

- 自动模式

  自动模式下配置了 Voice VLAN 功能后，当语音设备发出的报文中源 MAC 地址匹配配置的 OUI 地址时，系统会将连接语音设备的接口自动加入到 Voice VLAN 中。如果配置了 Voice VLAN 的设备在到达老化时间后未收到任何来自该语音设备的语音报文，连接语音设备的接口将自动从 Voice VLAN 中退出。
- 手动模式

  手动模式下配置了 Voice VLAN 功能后，必须通过手动将连接语音设备的接口加入到 Voice VLAN 中，这样才能保证接口正常转发 Voice VLAN 的语音报文。

Voice VLAN 的工作模式

说明

建议用户尽量不要在 Voice VLAN 中传输非语音数据流。如确有此需要，请确认 Voice VLAN 工作在普通模式。

为满足用户对 Voice VLAN 中传输数据的不同需求，如表 4-1 所示，Voice VLAN 的工作模式可以分为安全模式和普通模式。

表 4-1 不同的 Voice VLAN 模式下处理报文的方式

Voice VLAN 模式	处理方式
安全模式	判断该报文源 MAC 地址是否为 OUI 地址： ● 是，则修改报文优先级并进行转发。 ● 否，则不修改优先级并禁止在 Voice VLAN 内转发。
普通模式	判断该报文源 MAC 地址是否为 OUI 地址： ● 是，则修改报文优先级并进行转发。 ● 否，则不修改优先级并允许在 Voice VLAN 内转发。

说明

当源 MAC 地址为 OUI 地址时，将自动修改报文中的两个优先级，以提高语音数据的传输质量：

- CoS（802.1p）优先级将被自动调整为 6。
- DSCP 优先级将被自动调整为 46。

4.3 配置 Voice VLAN

介绍配置 Voice VLAN 的过程与步骤。

4.3.1 建立配置任务

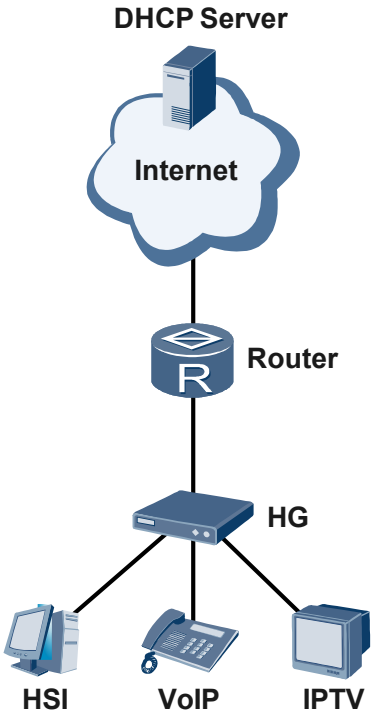
在进行 Voice VLAN 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 4-1 所示 HSI（High Speed Internet）、VoIP（Voice over IP）和 IPTV（Internet Protocol Television）通过家庭网关 HG（Home Gateway）接入 Router。用户对语音通话质量较敏感，需要提高语音数据流的传输优先级，以保证用户的通话质量。

可在 Router 上配置 Voice VLAN 功能解决此问题。

图 4-1 Voice VLAN 应用场景图



当 Router 配置 Voice VLAN 功能后，会根据进入接口数据流的源 MAC 地址来判断该数据流是否为语音数据流。当源 MAC 地址匹配系统设置的语音设备 OUI 地址时，则认为是语音数据流。Router 接收到语音数据流后将修改语音数据流的传输优先级，并且在 Voice VLAN 内进行传输，以保证用户的通话质量。

前置任务

在配置 Voice VLAN 之前，需完成以下任务：

- 创建 VLAN

数据准备

在配置 Voice VLAN 之前，请根据网络规划，准备以下数据。

序号	数据
1	Voice VLAN 的 VLAN 编号
2	使能 Voice VLAN 功能的接口类型和接口编号
3	接口加入 Voice VLAN 的模式
4	OUI 的地址和掩码地址
5	（可选）Voice VLAN 的老化时间
6	（可选）Voice VLAN 的工作模式

4.3.2 使能接口的 Voice VLAN 功能

当 AR2200-S 配置 Voice VLAN 功能后，会根据进入接口数据流的源 MAC 地址来判断该数据流是否为语音数据流。当源 MAC 地址匹配系统设置的语音设备 OUI 地址时，则认为是语音数据流。AR2200-S 接收到语音数据流后将修改语音数据流的传输优先级，并且在 Voice VLAN 内进行传输，以保证用户的通话质量。

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 **voice-vlan** *vlan-id* **enable**，配置指定 VLAN 为 Voice VLAN，同时使能接口的 Voice VLAN 功能。

缺省情况下，接口的 Voice VLAN 功能处于去使能状态。

说明

- 为保证各种功能的正常使用，请为 Voice VLAN、接口的缺省 VLAN 分配不同的 VLAN ID。
- 如果要删除被设置为 Voice VLAN 的 VLAN，需要先使用 **undo voice-vlan enable** 命令去使能 Voice VLAN 功能后，才能够删除该 VLAN。
- 一个接口只能有一个 VLAN 被设置为 Voice VLAN。

----结束

4.3.3 配置 Voice VLAN 的 OUI 地址

AR2200-S 根据进入接口数据流中的源 MAC 地址来判断该数据流是否为语音数据流，当源 MAC 地址匹配系统配置的 OUI（Organizationally Unique Identifier）地址时，认为该数据流为语音数据流。

背景信息

OUI 地址一般配置为 MAC 地址的前 24 位，是 IEEE（Institute of Electrical and Electronics Engineers）为不同设备供应商分配的一个全球唯一的标识符，从 OUI 地址可以判断出该设备是哪一个厂商的产品。AR2200-S 支持配置 OUI 地址的掩码，用户可以通过设定不同的掩码来调节路由器对 MAC 地址匹配的深度。

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 **voice-vlan mac-address** *mac-address* **mask** *oui-mask* [**description** *text*]，配置 Voice VLAN 的 OUI 地址。

缺省情况下，没有配置 MAC 地址为 OUI 地址。

AR2200-S 支持配置 16 个 OUI 地址，当 OUI 地址大于 16 个时，将无法配置。

----结束

4.3.4 （可选）配置接口加入 Voice VLAN 的模式

AR2200-S 接口加入 Voice VLAN 的模式为自动模式或手动模式。

背景信息

- 自动模式下配置了 Voice VLAN 功能后，当语音设备发出的报文中源 MAC 地址匹配配置的 OUI 地址时，系统会将连接语音设备的接口自动加入到 Voice VLAN 中。如果配置了 Voice VLAN 的设备在到达老化时间后未收到任何来自该语音设备的语音报文，连接语音设备的接口将自动从 Voice VLAN 中退出。
- 手动模式下配置了 Voice VLAN 功能后，必须通过手动将连接语音设备的接口加入到 Voice VLAN 中，这样才能保证接口正常转发 Voice VLAN 的语音报文。

操作步骤

- 接口自动模式加入 Voice VLAN
  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。

     不支持 access 类型接口在自动模式下加入 Voice VLAN。
  3. 执行命令 **voice-vlan mode auto**，配置接口加入 Voice VLAN 的模式为自动模式。

     缺省情况下，接口加入 Voice VLAN 的模式为自动模式。
- 接口手动模式加入 Voice VLAN
  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 **voice-vlan mode manual**，配置接口加入 Voice VLAN 的模式为手动模式。

     缺省情况下，接口加入 Voice VLAN 的模式为自动模式。
  4. 手动将接口加入到 Voice VLAN 中：
     - 如果接口为 Access 类型，请参见 **3.4.2 将 Access 类型接口加入 VLAN**。
     - 如果接口为 Trunk 类型，请参见 **3.4.3 将 Trunk 类型接口加入 VLAN**。
     - 如果接口为 Hybrid 类型，请参见 **3.4.4 将 Hybrid 类型接口加入 VLAN**。

----结束

4.3.5 （可选）配置 Voice VLAN 的 802.1p 和 DSCP 优先级

通过配置 Voice VLAN 的 802.1p 和 DSCP 优先级，提高用户部署语音业务的灵活性。

背景信息

Voice-VLAN 特性的 802.1p 和 DSCP 优先级缺省值为 6 和 46，用户可以动态配置这两个参数，满足自由规划网络语音流量优先级的需求。

说明

- 802.1p 优先级就是 802.1Q VLAN 帧中的 PRI（Priority）字段值，长度为 3 比特，用于交换设备阻塞时，优先发送优先级高的数据包。
- IPv4 的数据报文头部里的 TOS（Type of Service）字节中的 6 位作为 DSCP（DiffServ Code Point）。DSCP 是 DiffServ 的信令，用于 IP 网络的 QoS 保证。网关的流量控制器的操作只决定于这 6 个比特。

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 **voice-vlan remark** { **8021p** *8021p-value* | **dscp** *dscp-value* } *，配置 Voice VLAN 的 802.1p 和 DSCP 优先级。

缺省情况下，Voice VLAN 的 802.1p 优先级是 6，DSCP 优先级是 46。

----结束

4.3.6 （可选）配置 Voice VLAN 的老化时间

Voice VLAN 的老化时间只对接口以自动模式加入 Voice VLAN 的方式有效，对以手动模式加入 Voice VLAN 的方式无效。

背景信息

如果配置了 Voice VLAN 的设备在到达老化时间后未收到任何来自该语音设备的语音报文，连接语音设备的接口将自动从 Voice VLAN 中退出。如果使能了 Voice VLAN 功能的接口再次收到该语音设备发出的语音报文，连接语音设备的接口将再次自动加入 Voice VLAN。

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 **voice-vlan aging-time** *minutes*，配置 Voice VLAN 的老化时间。

缺省情况下，老化时间为 1440 分钟。

----结束

4.3.7 （可选）配置 Voice VLAN 的工作模式

网络中有各种数据流，为满足用户对 Voice VLAN 中传输数据的不同需求，Voice VLAN 在接口下定义了安全模式和普通模式两种工作模式。

背景信息

- 安全模式下使能了 Voice VLAN 的接口对每一个进入 Voice VLAN 的报文都进行源 MAC 地址匹配检查，丢弃不能匹配 OUI 地址的报文。即，当 Voice VLAN 工作在安全模式时，使能了 Voice VLAN 的接口只允许该 Voice VLAN 的语音报文通过，不允许其他报文通过。安全模式用于防止 Voice VLAN 受到恶意数据流量的攻击，但是检查报文的工作会占用一定的系统资源。
- 普通模式下使能了 Voice VLAN 的接口允许 Voice VLAN 同时传输语音数据流和业务数据流。对每一个进入 Voice VLAN 的报文不进行源 MAC 地址匹配检查，容易受到恶意数据流量的攻击。

操作步骤

- 安全模式
  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 **voice-vlan security enable**，配置 Voice VLAN 的工作模式为安全模式。

   缺省情况下，Voice VLAN 的工作模式为安全模式。

- 普通模式
  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 **undo voice-vlan security enable**，配置 Voice VLAN 的工作模式为普通模式。

     缺省情况下，Voice VLAN 的工作模式为安全模式。

----结束

4.3.8 （可选）使能接口与其他厂商语音设备的互通功能

一些厂商的 IP 电话上电时，不会发送 DHCP 报文申请 IP 地址，而是发送该厂商私有协议报文申请 IP 地址。为了与这些厂商的语音设备互通，用户可以使能 Voice VLAN legacy 功能，使华为数据通信设备能够识别其他厂商的私有协议报文，实现互通。

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 **voice-vlan legacy enable**，使能接口与其他厂商的语音设备互通功能。

缺省情况下，没有使能接口与其他厂商的语音设备互通功能。

----结束

4.3.9 检查配置结果

Voice VLAN 配置成功后，您可以查看到 Voice VLAN 的 OUI 地址、工作状态、安全模式、老化时间和使能了 Voice VLAN 功能接口的配置信息。

操作步骤

- 使用命令 **display voice-vlan oui**，查看当前系统配置的 OUI 地址、OUI 地址掩码和描述信息。
- 使用命令 **display voice-vlan** [*vlan-id*] **status**，查看当前 Voice VLAN 的工作状态、安全模式、老化时间等信息。

----结束

任务示例

执行命令 **display voice-vlan oui**，可以查看到 Voice VLAN 的 OUI 地址是否配置正确。

```
<Huawei> display voice-vlan oui
-----------------------------------------------
OuiAddress       Mask            Description
-----------------------------------------------
0022-0033-0044   ffff-ff00-0000
```

执行命令 **display voice-vlan 10 status**，可以查看到 Voice VLAN10 的工作状态、安全模式和老化时间是否配置正确。

```
<Huawei> display voice-vlan 10 status
Voice VLAN Configurations:
------------------------------------------------
Voice VLAN ID            : 10
Voice VLAN status        : Enable
Voice VLAN aging time    : 4000(minutes)
Voice VLAN 802lp remark  : 6
Voice VLAN dscp remark   : 46
------------------------------------------------------------
Port Information:
------------------------------------------------------------
Port                     Add-Mode  Security-Mode  Legacy
------------------------------------------------------------
Ethernet2/0/1            Auto      Security       Disable
```

4.4 配置举例

介绍 Voice VLAN 的各种组网举例。

4.4.1 配置自动模式下的 Voice VLAN 示例

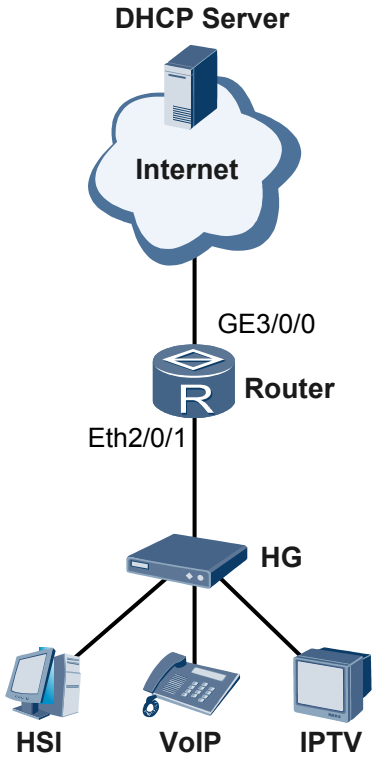
该组网的特点是使能了 Voice VLAN 功能的接口以自动模式加入 Voice VLAN。自动模式下配置了 Voice VLAN 功能后，当语音设备发出的报文中源 MAC 地址匹配配置的 OUI 地址时，系统会将连接语音设备的接口自动加入到 Voice VLAN 中。如果配置了 Voice VLAN 的设备在到达老化时间后未收到任何来自该语音设备的语音报文，连接语音设备的接口将自动从 Voice VLAN 中退出。

组网需求

网络中有 HSI、VoIP 和 IPTV 等数据流，用户对语音通话质量较敏感，需要提高语音数据流的传输优先级，以保证用户的通话质量。

如图 4-2 所示，Router 配置 Voice VLAN 功能后，根据进入接口 Ethernet2/0/1 的数据流源 MAC 地址来判断是否为语音数据流，是则修改报文优先级且在 Voice VLAN 内传输，不是则不修改报文优先级且在普通 VLAN 内传输，要求接口 Ethernet2/0/1 能自动加入和退出 Voice VLAN，并通过 Router 的 GE3/0/0 接口连接到 WAN 侧网络。

图 4-2 配置自动模式下的 Voice VLAN 的组网图



配置思路

采用如下的思路配置自动模式下的 Voice VLAN：

1. 在 Router 上创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 Router 访问 WAN 侧网络。
2. 使能接口的 Voice VLAN 功能，并配置 Voice VLAN。
3. 配置流策略，并在语音入接口绑定流策略。

数据准备

为完成此配置例，需准备如下的数据：

- 创建 Voice VLAN2 和 IP 电话申请 IP 地址的 VLAN6，VLANIF 2 的 IP 地址为 192.168.2.1/24。
- OUI 地址为 0011-2200-0000，掩码地址为 ffff-ff00-0000。
- Voice VLAN 的老化时间为 100min。
- 接口 Ethernet2/0/1 的缺省 VLAN 为 VLAN6。
- Router 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24
- 源 MAC 地址为 0011-2200-0000 或 VLAN 的 ID 为 2 的语音报文重标记后的 DSCP 优先级为 46。
- 需要应用流策略的接口类型、方向和编号：Router 上接口 Ethernet2/0/1 的入方向。

操作步骤

步骤 1 配置 Router 的 VLAN 和接口

创建 VLAN2、VLAN6

```
<Huawei> system-view
[Huawei] vlan batch 2 6
```

配置接口类型和缺省 VLAN

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port hybrid pvid vlan 6
[Huawei-Ethernet2/0/1] port hybrid untagged vlan 6
[Huawei-Ethernet2/0/1] quit
```

创建 VLANIF 2，并为 VLANIF 2 配置 IP 地址 192.168.2.1/24

```
[Huawei] interface vlanif 2
[Huawei-Vlanif2] ip address 192.168.2.1 24
[Huawei-Vlanif2] quit
```

配置 GE3/0/0 的 IP 地址为 192.168.4.1/24。

```
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[Router-GigabitEthernet3/0/0] quit
```

步骤 2 配置 Router 的 Voice VLAN 功能

配置接口 Voice VLAN 功能

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] voice-vlan 2 enable
```

配置接口加入 Voice VLAN 的模式

```
[Huawei-Ethernet2/0/1] voice-vlan mode auto
[Huawei-Ethernet2/0/1] quit
```

配置 OUI 地址

```
[Huawei] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

配置 Voice VLAN 的老化时间

```
[Huawei] voice-vlan aging-time 100
```

配置 Voice VLAN 的工作模式

```
[Huawei-Ethernet2/0/1] voice-vlan security enable
```

步骤 3 配置流策略，并在语音出接口绑定流策略。

在 Router 上创建并配置流分类 c1。

```
[Router] traffic classifier c1 operator and
[Router-classifier-c1] if-match source-mac 0011-2200-0000 mac-address-mask ffff-ff00-0000
[Router-classifier-c1] if-match vlan-id 2
[Router-classifier-c1] quit
```

在 Router 上创建并配置流行为 b1，重标记用户报文的优先级。

```
[Router] traffic behavior b1
[Router-behavior-b1] remark dscp 46
[Router-behavior-b1] quit
```

在 Router 上创建流策略 p1，将流分类和对应的流行为进行绑定并将流策略应用到接口 Ethernet2/0/1 的入方向上，对报文进行重标记。

```
[Router] traffic policy p1
[Router-trafficpolicy-p1] classifier c1 behavior b1
[Router-trafficpolicy-p1] quit
[Router] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] traffic-policy p1 inbound
[Huawei-Ethernet2/0/1] quit
[Router] quit
```

步骤 4 检查配置结果

执行命令 **display voice-vlan oui**，查看 Voice VLAN 的 OUI 地址是否配置正确。

```
<Huawei> display voice-vlan oui
-------------------------------------------------
OuiAddress       Mask            Description
-------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

执行命令 **display voice-vlan 2 status**，查看 Voice VLAN 的工作状态、安全模式和老化时间是否配置正确。

```
<Huawei> display voice-vlan 2 status
Voice VLAN Configurations:
-------------------------------------------------
Voice VLAN ID            :  2
Voice VLAN status        : Enable
Voice VLAN aging time    : 100(minutes)
Voice VLAN 802.1p remark  : 6
Voice VLAN dscp remark   : 46
-------------------------------------------------------------
Port Information:
-------------------------------------------------------------
Port                     Add-Mode  Security-Mode  Legacy
-------------------------------------------------------------
Ethernet2/0/1            Auto      Security       Disable
```

执行命令 **display traffic policy user-defined**，查看流策略的配置信息。

```
<Router> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Marking:
        Remark DSCP 46
```

----结束

配置文件

Router 的配置文件。

```
#
sysname Huawei
#
 vlan batch 2 6
#
 voice-vlan aging-time 100
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
traffic classifier c1 operator and
 if-match source-mac 0011-2200-0000 mac-address-mask ffff-ff00-0000
 if-match vlan-id 2
#
traffic behavior b1
```

```
 remark dscp 46
#
traffic policy p1
 classifier c1 behavior b1
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet2/0/1
 port hybrid pvid vlan 6
 port hybrid untagged vlan 6
 voice-vlan 2 enable
 traffic-policy p1 inbound
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

4.4.2 配置手动模式下的 Voice VLAN 示例

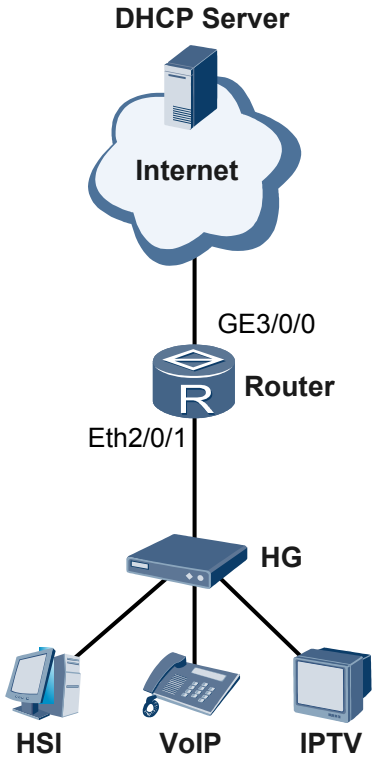
该组网的特点是使能了 Voice VLAN 功能的接口以手动模式加入 Voice VLAN。手动模式下配置了 Voice VLAN 功能后，必须通过手动将连接语音设备的接口加入到 Voice VLAN 中，这样才能保证接口正常转发 Voice VLAN 的语音报文。

组网需求

网络中有 HSI、VoIP 和 IPTV 等数据流，用户对语音通话质量较敏感，需要提高语音数据流的传输优先级，以保证用户的通话质量。

如图 4-3 所示，Router 配置 Voice VLAN 功能后，根据进入接口 Ethernet2/0/1 的数据流源 MAC 地址来判断是否为语音数据流，是则修改报文优先级且在 Voice VLAN 内传输，不是则不修改报文优先级且在普通 VLAN 内传输，要求接口 Ethernet2/0/1 需要通过手动加入和退出 Voice VLAN，并通过 Router 的 GE3/0/0 接口连接到 WAN 侧网络。

图 4-3 配置手动模式下的 Voice VLAN 的组网图



配置思路

采用如下的思路配置手动模式下的 Voice VLAN：

1. 在 Router 上创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 Router 访问 WAN 侧网络。
2. 使能接口的 Voice VLAN 功能，并配置 Voice VLAN。
3. 配置流策略，并在语音入接口绑定流策略。

数据准备

为完成此配置例，需准备如下的数据：

- 创建 Voice VLAN2 和 IP 电话申请 IP 地址的 VLAN6，VLANIF 2 的 IP 地址为 192.168.2.1/24。
- OUI 地址为 0011-2200-0000，掩码地址为 ffff-ff00-0000。
- 接口 Ethernet2/0/1 的缺省 VLAN 为 VLAN6。
- Router 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24
- 源 MAC 地址为 0011-2200-0000 或 VLAN 的 ID 为 2 的语音报文重标记后的 DSCP 优先级为 46。
- 需要应用流策略的接口类型、方向和编号：Router 上接口 Ethernet2/0/1 的入方向。

操作步骤

步骤 1 配置 Router 的 VLAN 和接口

创建 VLAN2、VLAN6

```
<Huawei> system-view
[Huawei] vlan batch 2 6
```

配置接口类型和缺省 VLAN

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port hybrid pvid vlan 6
[Huawei-Ethernet2/0/1] port hybrid untagged vlan 6
[Huawei-Ethernet2/0/1] quit
```

创建 VLANIF 2，并为 VLANIF 2 配置 IP 地址 192.168.2.1/24

```
[Huawei] interface vlanif 2
[Huawei-Vlanif2] ip address 192.168.2.1 24
[Huawei-Vlanif2] quit
```

配置 GE3/0/0 的 IP 地址为 192.168.4.1/24。

```
[Huawei] interface gigabitethernet 3/0/0
[Huawei-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[Huawei-GigabitEthernet3/0/0] quit
```

步骤 2 配置 Router 的 Voice VLAN 功能

配置接口 Voice VLAN 功能

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] voice-vlan 2 enable
```

配置接口加入 Voice VLAN 的模式

```
[Huawei-Ethernet2/0/1] voice-vlan mode manual
[Huawei-Ethernet2/0/1] port hybrid tagged vlan 2
[Huawei-Ethernet2/0/1] quit
```

配置 OUI 地址

```
[Huawei] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

配置 Voice VLAN 的工作模式

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] voice-vlan security enable
```

步骤 3 配置流策略，并在语音出接口绑定流策略。

在 Router 上创建并配置流分类 c1。

```
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match source-mac 0011-2200-0000 mac-address-mask ffff-ff00-0000
[Huawei-classifier-c1] if-match vlan-id 2
[Huawei-classifier-c1] quit
```

在 Router 上创建并配置流行为 b1，重标记用户报文的优先级。

```
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark dscp 46
[Huawei-behavior-b1] quit
```

在 Router 上创建流策略 p1，将流分类和对应的流行为进行绑定并将流策略应用到接口 Ethernet2/0/1 的入方向上，对报文进行重标记。

```
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] traffic-policy p1 inbound
[Huawei-Ethernet2/0/1] quit
[Huawei] quit
```

步骤 4 检查配置结果

执行命令 **display voice-vlan oui**，查看 Voice VLAN 的 OUI 地址是否配置正确。

```
<Huawei> display voice-vlan oui
------------------------------------------------
OuiAddress       Mask            Description
------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

执行命令 **display voice-vlan 2 status**，查看 Voice VLAN 的工作状态、安全模式和老化时间是否配置正确。

```
<Huawei> display voice-vlan 2 status
Voice VLAN Configurations:
------------------------------------------------
Voice VLAN ID            :  2
Voice VLAN status        : Enable
Voice VLAN aging time    : 1440(minutes)
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
------------------------------------------------------------
Port Information:
------------------------------------------------------------
Port                     Add-Mode  Security-Mode  Legacy
------------------------------------------------------------
Ethernet2/0/1            Manual    Security       Disable
```

执行命令 **display traffic policy user-defined**，查看流策略的配置信息。

```
<Huawei> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Marking:
        Remark DSCP 46
```

----结束

配置文件

Router 的配置文件。

```
#
 vlan batch 2 6
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
traffic classifier c1 operator and
 if-match source-mac 0011-2200-0000 mac-address-mask ffff-ff00-0000
 if-match vlan-id 2
#
traffic behavior b1
 remark dscp 46
#
traffic policy p1
 classifier c1 behavior b1
```

```
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet2/0/1
 port hybrid pvid vlan 6
 port hybrid tagged vlan 2
 port hybrid untagged vlan 6
 voice-vlan 2 enable
 voice-vlan mode manual

 traffic-policy p1 inbound
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

5 GVRP 配置

关于本章

介绍了 GVRP 的基础知识、GVRP 配置方法和配置实例。

5.1 GVRP 概述
简要介绍 GVRP 和 GARP 的基本概念。

5.2 AR2200-S 支持的 GVRP 特性
介绍 GVRP 特性在 AR2200-S 中的支持情况。

5.3 配置 GVRP 功能
介绍配置 GVRP 功能的过程与步骤。

5.4 维护
介绍清除 GARP 统计信息的方法。

5.5 配置举例
介绍了 GVRP 的典型组网配置。

5.1 GVRP 概述

简要介绍 GVRP 和 GARP 的基本概念。

GVRP 简介

GARP VLAN 注册协议 GVRP（GARP VLAN Registration Protocol）是通用属性注册协议 GARP（Generic Attribute Registration Protocol）的一种应用，下面先介绍一下 GARP 的相关内容。

GARP 简介

GARP 提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息（如 VLAN、组播地址等）。

GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用实体称为 GARP 应用，GVRP 就是 GARP 的一种应用。当 GARP 应用实体存在于设备的某个接口上时，该接口对应于一个 GARP 应用实体。

- GARP 消息和定时器
  - GARP 消息

    GARP 成员之间的信息交换借助于消息的传递来完成，主要有三类消息起作用，分别为 Join 消息、Leave 消息和 LeaveAll 消息。
    - 当一个 GARP 应用实体希望其它设备注册自己的属性信息时，它将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GARP 应用实体进行注册时，它也会向外发送 Join 消息。
    - 当一个 GARP 应用实体希望其它设备注销自己的属性信息时，它将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性后，它也会向外发送 Leave 消息。
    - 每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GARP 应用实体将对外发送 LeaveAll 消息，LeaveAll 消息用来注销所有的属性，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。

    Join 消息、Leave 消息与 LeaveAll 消息配合确保信息的重新注册或注销。

    通过消息交互，所有待注册的属性信息可以传播到同一局域网配置了 GARP 的所有设备上。
  - GARP 定时器

    GARP 消息发送的时间间隔是通过定时器来实现的，GARP 定义了四种定时器，用于控制 GARP 消息的发送周期：
    - Hold 定时器：当 GARP 应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条 Join 消息对外发送，而是启动 Hold 定时器，当该定时器超时后，GARP 应用实体将此时段内收到的所有注册信息放在同一个 Join 消息中向外发送，从而节省带宽资源。
    - Join 定时器：GARP 应用实体可以通过将每个 Join 消息向外发送两次来保证消息的可靠传输，在第一次发送的 Join 消息没有得到回复的时候，GARP 应用实体会第二次发送 Join 消息。两次 Join 消息发送之间的时间间隔用 Join 定时器来控制。

- Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 消息，则注销该属性信息。
- LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

说明

- GARP 定时器的值将应用于所有在同一局域网内运行的 GARP 应用（如 GVRP）。
- Hold 定时器、Join 定时器和 Leave 定时器的值可以在每个接口单独进行设置；而 LeaveAll 定时器只需在设备的全局进行设置即可，设置完成后，该值将在设备的所有接口上生效。
- 在全网有多台设备的情况下，各个设备的 LeaveAll 定时器的取值可能不相同，但各设备都将以全网最小的 LeaveAll 定时器为准发送 LeaveAll 消息。因为每次发送 LeaveAll 消息时，当其它设备接收到之后都会清零 LeaveAll 定时器，因此即使全网存在很多不同的 LeaveAll 定时器，也只有最小的那个 LeaveAll 定时器起作用。

- GARP 运行过程

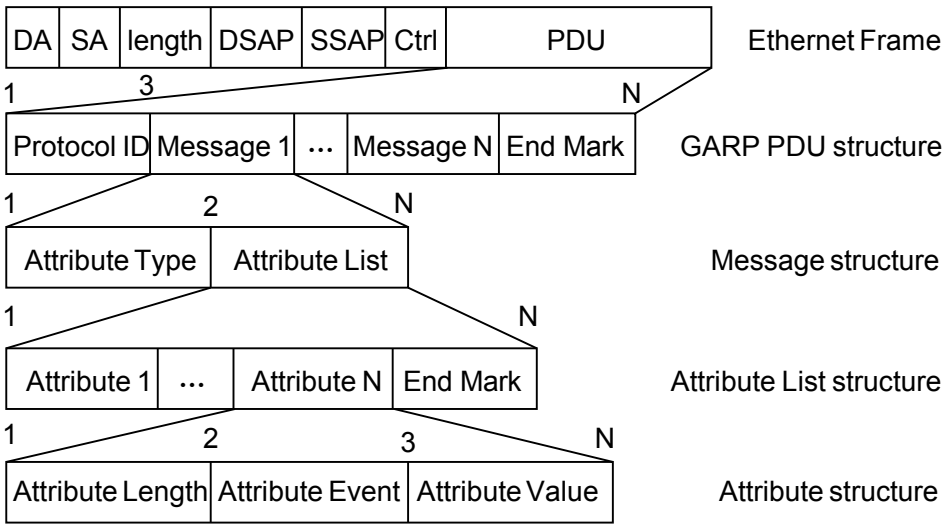
  通过 GARP 机制，一个 GARP 成员上的配置信息会迅速传播到整个局域网。GARP 成员可以是终端工作站或网桥。GARP 成员通过声明或回收声明来通知其它的 GARP 成员注册或注销自己的属性信息，并根据其它 GARP 成员的声明或回收声明注册或注销对方的属性信息。当接口接收到一个属性声明时，该接口将注册该属性，如果接口接收到回收属性的声明，该接口将注销该属性。

  GARP 应用实体的协议数据报文以特定的组播 MAC 地址为目的 MAC。设备在接收到 GARP 应用实体的报文后，会根据其目的 MAC 地址加以区分并交给不同的 GARP 应用（如 GVRP）去处理。

- GARP 的报文格式

  GARP 的报文格式如图 5-1 所示。

图 5-1 GARP 报文格式



各个字段的说明如下表所示。

字段	含义	取值
Protocol ID	协议 ID。	取值为 1。
Message	消息，每个 Message 由 Attribute Type、Attribute List 构成。	-
Attribute Type	属性类型，由具体的 GARP 的应用定义。	对于 GVRP，属性类型为 0x01，表示属性取值为 VLAN ID。
Attribute List	属性列表，由多个属性构成。	-
Attribute	属性，每个属性由 Attribute Length、Attribute Event、Attribute Value 构成。	-
Attribute Length	属性长度。	取值 2 ～ 255，单位为字节。
Attribute Event	属性描述的事件。	● 0：LeaveAll Event ● 1：JoinEmpty Event ● 2：JoinIn Event ● 3：LeaveEmpty Event ● 4：LeaveIn Event ● 5：Empty Event
Attribute Value	属性取值。	GVRP 的属性取值为 VLAN ID，但 LeaveAll 属性的 Attribute Value 值无效。
End Mark	结束标志、GARP 的 PDU 的结尾标志。	以 0x00 取值表示。

5.2 AR2200-S 支持的 GVRP 特性

介绍 GVRP 特性在 AR2200-S 中的支持情况。

GVRP 是 GARP 的一种应用。它基于 GARP 的工作机制，维护设备中的 VLAN 动态注册信息，并传播该信息到其它的设备中。

设备启动 GVRP 特性后，能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个接口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以便使同一局域网内所有设备的 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

GVRP 的接口注册模式有三种：

- Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动创建的那部分。
- Forbidden 模式：禁止该接口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何的 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN1。

说明

AR2200-S 的 GVRP 特性在定时器使用默认值时最多支持 256 个动态 VLAN，在定时器使用推荐值时最多支持 4094 个动态 VLAN。

GVRP 功能只能运行在接口 PVID VLAN 对应的实例上，并且在该实例上被 MSTP 等生成树协议阻塞的接口不能收发 GVRP 报文。

5.3 配置 GVRP 功能

介绍配置 GVRP 功能的过程与步骤。

5.3.1 建立配置任务

应用环境

在某些复杂的二层网络中，配置 GVRP 功能可以使接口动态加入或退出 VLAN 以简化配置。

前置任务

在配置 GVRP 功能之前，需完成以下任务：

- 接口已加入所有 VLAN。

数据准备

在配置 GVRP 功能之前，需准备以下数据。

序号	数据
1	（可选）GVRP 接口的注册模式
2	（可选）GARP 定时器时长

5.3.2 使能 GVRP 功能

背景信息

请在需要使能 GVRP 功能的 AR2200-S 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 **gvrp**，使能全局 GVRP 功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **port link-type trunk**，配置接口为 Trunk 类型。

步骤 5 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，配置接口加入 VLAN。

步骤 6 执行命令 **gvrp**，使能接口 GVRP 功能。

缺省情况下，全局和接口的 GVRP 功能都处于关闭状态。

说明

- 在开启接口 GVRP 功能之前，必须先开启全局 GVRP 功能。
- 开启接口 GVRP 功能必须在 Trunk 接口操作。

----结束

5.3.3 （可选）配置 GVRP 接口注册模式

背景信息

GVRP 的接口注册模式有三种：

- Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动创建的那部分。
- Forbidden 模式：禁止该接口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何的 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN1。

请在需要配置 GVRP 接口注册模式的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **gvrp registration** { **fixed** | **forbidden** | **normal** }，配置 GVRP 接口注册模式。

缺省情况下，GVRP 接口注册模式为 **normal**。

说明

配置 GVRP 接口注册模式之前，需要先使能接口的 GVRP 功能。

----结束

5.3.4 （可选）配置 GARP 定时器功能

背景信息

每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其他 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

在全网有多台设备的情况下，各个设备的 LeaveAll 定时器的取值可能不相同，但每台设备都将以全网最小的 LeaveAll 定时器为准发送 LeaveAll 消息。因为每次 LeaveAll 定时器超时后发送 LeaveAll 消息，其它的设备接收到之后都会清零 LeaveAll 定时器，因此即使全网存在很多不同的 LeaveAll 定时器，也只有最小的那个 LeaveAll 定时器起作用。

使用命令 **garp timer** 设置接口的 GARP 定时器时，需要注意以下几点：

- **undo garp timer** 命令用来恢复接口的 GARP 定时器的值为缺省值。如果缺省值不满足取值范围的要求，则 **undo garp timer** 命令无效。
- 各个定时器的取值范围会由于其他定时器取值的改变而改变。如果用户想要设置的定时器的值不在当前可以设置的取值范围内，可以通过改变相关定时器的取值实现。
- 如果用户想恢复各定时器的值为缺省值，可以先恢复 **Hold** 定时器的值为缺省值，然后再依次恢复 **Join**、**Leave**、**LeaveAll** 定时器的值为缺省值。

说明

在实际组网中，建议用户将 GVRP 定时器配置为以下的推荐值:

- GARP Hold 定时器：100 厘秒（1 秒钟）
- GARP Join 定时器：600 厘秒（6 秒钟）
- GARP Leave 定时器：3000 厘秒（30 秒钟）
- GARP LeaveAll 定时器：12000 厘秒（2 分钟）

当动态 VLAN 超过 100 个或运行 GVRP 的网络超过 3 台设备时，需将定时器配置为推荐值。当动态 VLAN 数或设备数增加时，定时器的时间也需要相应的增加。

请在需要配置 GARP 定时器的 AR2200-S 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 **garp timer leaveall** *timer-value*，配置 GARP 的 LeaveAll 定时器的值。

缺省情况下，LeaveAll 定时器的值为 1000 厘秒，即 10 秒。

由于接口 Leave 定时器的值受全局 LeaveAll 定时器的值限制，所以在配置 LeaveAll 定时器的值时，需要保证设备上所有配置 GARP 定时器的接口都是处于正常工作状态。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **garp timer** { **hold** | **join** | **leave** } *timer-value*，配置接口 **Hold** 定时器、**Join** 定时器、**Leave** 定时器的值。

缺省情况下，**Hold** 定时器的值为 40 厘秒，**Join** 定时器的值为 80 厘秒，**Leave** 定时器的值为 240 厘秒。

----结束

5.3.5 检查配置结果

操作步骤

- 使用命令 **display gvrp status** 查看全局 GVRP 的开启或关闭状态信息。
- 使用命令 **display gvrp statistics** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]查看接口的 GVRP 统计信息。
- 使用命令 **display garp timer** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]查看 GARP 定时器的值。

----结束

任务示例

执行命令 **display gvrp status**，查看全局 GVRP 的使能情况。

```
<Huawei> display gvrp status
 Info: GVRP is enabled.
```

执行命令 **display gvrp statistics**，查看接口的 GVRP 统计信息，其中包括：GVRP 状态、GVRP 注册失败次数、上一个 GVRP 数据单元源 MAC 地址和接口 GVRP 注册类型。

```
<Huawei> display gvrp statistics

  GVRP statistics on port Ethernet2/0/1
    GVRP status                     : Enabled
    GVRP registrations failed       : 0
    GVRP last PDU origin            : 0000-0000-0000
    GVRP registration type          : Normal
```

执行命令 **display garp timer interface ethernet 2/0/1**，查看指定接口 GARP 定时器的值。

```
<Huawei> display garp timer interface ethernet 2/0/1
  GARP timers on port Ethernet2/0/1
    GARP JoinTime                : 20 centiseconds
    GARP LeaveTime               : 60 centiseconds
    GARP LeaveAllTime            : 1000 centiseconds
    GARP HoldTime                : 10 centiseconds
```

5.4 维护

介绍清除 GARP 统计信息的方法。

5.4.1 清除 GARP 统计信息

背景信息

注意

清除 GARP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在用户视图下使用命令 **reset garp statistics** [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]清除接口的 GARP 统计信息。

----结束

5.5 配置举例

介绍了 GVRP 的典型组网配置。

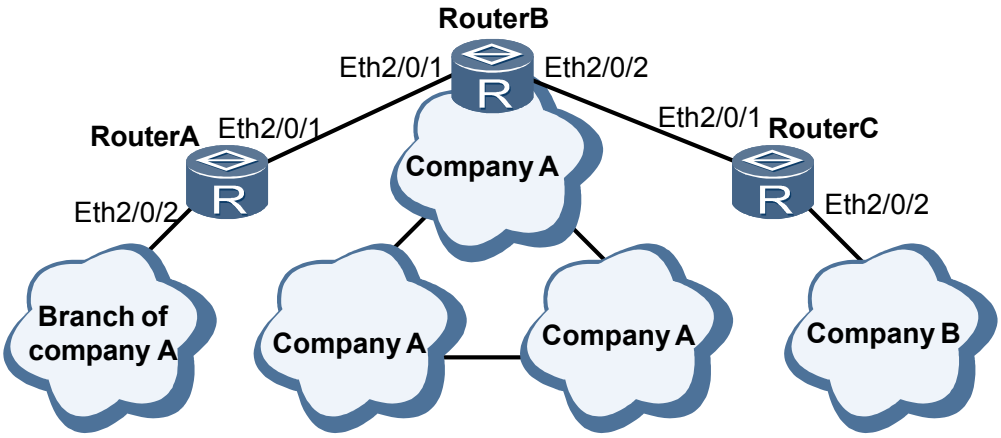
5.5.1 配置 GVRP 示例

组网需求

如图 5-2 所示，公司 A 的分公司与总部通过 RouterA 和 RouterB 互通，公司 A 的所有路由器配置 GVRP 功能并配置接口注册模式为 Normal，以简化配置。

公司 B 通过 RouterB 和 RouterC 与公司 A 互通，公司 B 的所有路由器配置 GVRP 功能并将与公司 A 相连的接口的注册模式配置为 Fixed，以控制只允许公司 B 配置的 VLAN 通过。

图 5-2 配置 GVRP 的组网图



配置思路

采用如下的思路配置 GVRP：

1. 全局使能 GVRP 功能。
2. 配置接口类型为 Trunk 类型。
3. 使能接口的 GVRP 功能。
4. 配置接口注册模式。

数据准备

为完成此配置例，需准备如下的数据：

- 在 RouterA、RouterB 和 RouterC 上配置接口允许所有 VLAN 通过。
- 在 RouterA 和 RouterB 上配置接口的注册模式为 Normal。
- 在 RouterC 上配置接口 Ethernet2/0/1 的注册模式为 Fixed，配置接口 Ethernet2/0/2 的注册模式为 Normal。
- 在 RouterC 上创建属于公司 B 的 VLAN101 ～ VLAN200。

操作步骤

步骤 1 配置路由器 RouterA

创建 VLAN101 ～ VLAN200。

```
<RouterA> system-view
[RouterA] vlan batch 101 to 200
```

全局使能 GVRP 功能。

```
[RouterA] gvrp
```

配置接口为 Trunk 类型，并允许所有 VLAN 通过。

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan all
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type trunk
[RouterA-Ethernet2/0/2] port trunk allow-pass vlan all
[RouterA-Ethernet2/0/2] quit
```

使能接口的 GVRP 功能，并配置接口注册模式。

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] gvrp
[RouterA-Ethernet2/0/1] gvrp registration normal
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] gvrp
[RouterA-Ethernet2/0/2] gvrp registration normal
[RouterA-Ethernet2/0/2] quit
```

RouterB 配置与 RouterA 配置类似，这里不再赘述。

步骤 2 配置路由器 RouterC

创建 VLAN101 ～ VLAN200。

```
<RouterC> system-view
[RouterC] vlan batch 101 to 200
```

全局使能 GVRP 功能。

```
[RouterC] gvrp
```

配置接口为 Trunk 类型，并允许所有 VLAN 通过。

```
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] port link-type trunk
[RouterC-Ethernet2/0/1] port trunk allow-pass vlan all
[RouterC-Ethernet2/0/1] quit
[RouterC] interface ethernet 2/0/2
```

```
[RouterC-Ethernet2/0/2] port link-type trunk
[RouterC-Ethernet2/0/2] port trunk allow-pass vlan all
[RouterC-Ethernet2/0/2] quit
```

使能接口的 GVRP 功能，并配置接口注册模式。

```
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] gvrp
[RouterC-Ethernet2/0/1] gvrp registration fixed
[RouterC-Ethernet2/0/1] quit
[RouterC] interface ethernet 2/0/2
[RouterC-Ethernet2/0/2] gvrp
[RouterC-Ethernet2/0/2] gvrp registration normal
[RouterC-Ethernet2/0/2] quit
```

步骤 3 验证配置结果

配置完成后，公司 A 的分公司用户可以与总部互通，公司 A 属于 VLAN101 ～ VLAN200 的用户可以与公司 B 用户互通。

在 RouterA 上使用命令 **display gvrp status**，查看全局 GVRP 的使能情况，结果如下：

```
<RouterA> display gvrp status
 Info: GVRP is enabled.
```

在 RouterA 上使用命令 **display gvrp statistics**，查看接口的 GVRP 统计信息，其中包括：GVRP 状态、GVRP 注册失败次数、上一个 GVRP 数据单元源 MAC 地址和接口 GVRP 注册类型，结果如下：

```
<RouterA> display gvrp statistics interface ethernet 2/0/1
 GVRP statistics on port Ethernet2/0/1
 GVRP status                   : Enabled
 GVRP registrations failed     : 0
 GVRP last PDU origin          : 0001-0001-0001
 GVRP registration type        : Normal
```

RouterB 和 RouterC 的查看方法与 RouterA 类似，这里不再赘述。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 101 to 200
#
 gvrp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 vlan batch 101 to 200
```

```
#
 gvrp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 vlan batch 101 to 200
#
 gvrp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
 gvrp registration fixed
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

6 MAC 表配置

关于本章

介绍了 MAC 表的基础知识、配置方法和配置实例。

6.1 MAC 表概述
简要介绍 MAC 表的基本概念。

6.2 AR2200-S 支持的 MAC 表特性
介绍 MAC 表特性在 AR2200-S 中的支持情况。

6.3 配置 MAC 表
介绍配置静态、黑洞、动态 MAC 表的过程与步骤。

6.4 配置接口安全
介绍接口安全的配置过程与步骤。

6.5 配置 MAC 地址学习限制
介绍基于接口和 VLAN 的 MAC 表配置过程与步骤。

6.6 配置 MAC 地址漂移检测功能
介绍 MAC 地址漂移检测功能的配置方法。

6.7 配置丢弃全 0 非法 MAC 地址报文
介绍配置丢弃全 0 非法 MAC 地址报文的过程与步骤。

6.8 维护
介绍维护 MAC 表的相关命令和方法。

6.9 配置举例
介绍 MAC 表的各种组网举例。

6.1 MAC 表概述

简要介绍 MAC 表的基本概念。

AR2200-S 的每个线路处理板 LPU（Line Processing Unit）内存有一张 MAC 地址表，简称 MAC 表。MAC 表用于存放 AR2200-S 所学习到的其它设备的 MAC 地址、VLAN 编号和出接口（即发送该数据的接口）。在转发数据时，AR2200-S 根据数据帧中的目的 MAC 地址和 VLAN 编号查询 MAC 表，快速定位出接口，从而减少广播。

为了提高接口的安全性，防止假冒身份的非法用户接入，网络管理员可手工配置静态 MAC 表项，将用户设备与接口绑定。

6.2 AR2200-S 支持的 MAC 表特性

介绍 MAC 表特性在 AR2200-S 中的支持情况。

MAC 表项的分类

MAC 表项分为动态 MAC 表项、静态 MAC 表项、黑洞 MAC 表项、安全动态 MAC 表项和 Sticky MAC 表项。

- 动态 MAC 表项：自动学习接口接收到的报文的源 MAC 地址而建立的 MAC 地址表项，表项会老化。
- 静态 MAC 表项：由用户手工配置的 MAC 地址表项，表项不老化。
- 黑洞 MAC 表项：由用户手工配置的 MAC 地址表项，用于丢弃含有特定目的 MAC 或源 MAC 地址的数据帧，表项不老化。
- 安全动态 MAC 表项：接口使能接口安全功能后学习到的 MAC 地址表项，表项可以设置为老化或不老化。
- Sticky MAC 表项：接口使能 Sticky MAC 功能后学习到的 MAC 地址表项，表项不老化。

接口安全和 Sticky MAC

接口安全功能是将路由器接口学习到的 MAC 地址变为安全动态 MAC 地址，安全动态 MAC 地址缺省情况下不会被老化，可以通过设置安全动态 MAC 地址老化时间使其变为可老化的 MAC 地址，设备重启后安全动态 MAC 地址会丢失，需要重新学习。

Sticky MAC 功能是将路由器接口学习到的 MAC 地址变为 Sticky MAC，Sticky MAC 不会被老化，手动保存后设备重启 Sticky MAC 也不会丢失。

接口安全和 Sticky MAC 功能都可以通过配置阻止其他非信任的 MAC 主机通过本接口和路由器通信，增强设备安全性。

MAC 地址学习限制

由于 MAC 表的容量是有限的，当黑客伪造大量源 MAC 地址不同的报文并发送给 AR2200-S 后，AR2200-S 的 MAC 表就可能被填满。当 AR2200-S 的 MAC 表被填满后，即使它再收到正常的报文，也无法学习到报文中的源 MAC 地址。

AR2200-S 支持基于接口和 VLAN 的 MAC 地址学习限制功能。当学习到的 MAC 表项已达到最大数目，则设置对接收到的报文进行丢弃或转发，并设置是否进行告警，以提

醒网络管理员，从而灵活控制接入用户的数量，并防止黑客通过 MAC 地址攻击用户设备或网络。

6.3 配置 MAC 表

介绍配置静态、黑洞、动态 MAC 表的过程与步骤。

6.3.1 建立配置任务

应用环境

在以下情况，需要配置静态、黑洞 MAC 表项或调整动态表项老化时间，以满足不同的需求。

- 携带特定目的 MAC 地址的报文由指定接口转发。
- 为了防止无用的 MAC 地址表项占用 MAC 表，也为了防止黑客通过 MAC 地址攻击用户设备或网络，丢弃目的 MAC 或源 MAC 地址为特定值的报文。
- 为了避免 MAC 地址表项爆炸式增长，改变动态 MAC 表项的老化时间。

前置任务

无

数据准备

在配置 MAC 表之前，需要准备以下数据。

序号	数据
1	（可选）目的 MAC 地址、出接口号、目的设备出接口所属的 VLAN 编号
2	（可选）动态 MAC 表项的老化时间

6.3.2 创建静态 MAC 表项

背景信息

请在需要配置 MAC 表的 AR2200-S 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 **mac-address static** *mac-address interface-type interface-number* { **vlan** *vlan-id* | **bridge** *bridge-id* }，添加静态 MAC 表项。

----结束

6.3.3 创建黑洞 MAC 表项

背景信息

请在需要配置 MAC 表的 AR2200-S 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 **mac-address blackhole** *mac-address* { **vlan** *vlan-id* | **bridge** *bridge-id* }，添加黑洞 MAC 表项。

----结束

6.3.4 （可选）配置动态 MAC 表项的老化时间

背景信息

请在需要配置 MAC 表的 AR2200-S 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 **mac-address aging-time** *aging-time*，配置动态 MAC 表项的老化时间。

缺省情况下，动态 MAC 表项的老化时间为 300 秒。

----结束

6.3.5 （可选）配置禁止 MAC 地址学习

背景信息

请在 AR2200-S 上进行以下配置。

操作步骤

- 接口视图下配置禁止 MAC 地址学习。
  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 **mac-address learning disable** [**action** { **discard** | **forward** }]，在接口上禁止 MAC 地址学习功能。

     缺省情况下，接口的 MAC 地址学习功能是使能的。

     关闭 MAC 地址学习功能的缺省动作为 **forward**，即对报文按照 MAC 地址表项进行转发。当配置动作为 **discard** 时，会对报文的源 MAC 地址进行匹配，

当接口和 MAC 地址与 MAC 地址表项匹配时，则对该报文进行转发。当接口和 MAC 地址与 MAC 地址表项不匹配时，则丢弃该报文。

- VLAN 视图下配置禁止 MAC 地址学习。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  3. 执行命令 **mac-address learning disable**，在 VLAN 上禁止 MAC 地址学习功能。

     缺省情况下，VLAN 的 MAC 地址学习功能是使能的。

----结束

6.3.6 检查配置结果

操作步骤

- 使用命令 **display mac-address** 查看所有 MAC 表项信息。
- 使用命令 **display mac-address static** [**vlan** *vlan-id*]查看静态 MAC 表项信息。
- 使用命令 **display mac-address dynamic** [*slot-id*] [*interface-type interface-number* | **vlan** *vlan-id*]查看动态 MAC 表项信息。
- 使用命令 **display mac-address blackhole** [**vlan** *vlan-id*]查看黑洞 MAC 表项信息。
- 使用命令 **display mac-address aging-time** 查看动态 MAC 表项的老化时间。
- 使用命令 **display mac-address summary** 查看所有 MAC 地址表项的数目。

----结束

任务示例

执行命令 **display mac-address**，可以查看所有 MAC 表项对应的目的 MAC 地址、出接口号、出接口所属 VLAN 的编号是否配置正确。

```
<Huawei> display mac-address
------------------------------------------------------------------------------
MAC Address       VLAN/Bridge           Learned-From          Type
------------------------------------------------------------------------------
0000-3333-3333       2/-                Eth2/0/2              static
00e0-1234-5678       2/-                -                     blackhole

------------------------------------------------------------------------------
Total items displayed = 2
```

执行命令 **display mac-address static**，可以查看静态 MAC 表项对应的目的 MAC 地址、出接口号、出接口所属 VLAN 的编号是否配置正确。

```
<Huawei> display mac-address static
------------------------------------------------------------------------------
MAC Address       VLAN/Bridge           Learned-From          Type
------------------------------------------------------------------------------
0000-3333-3333       2/-                Eth2/0/2              static

------------------------------------------------------------------------------
Total items displayed = 1
```

执行命令 **display mac-address dynamic**，可以查看动态 MAC 表项对应的目的 MAC 地址、出接口号、出接口所属 VLAN 的编号是否配置正确。

```
<Huawei> display mac-address dynamic
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge             Learned-From               Type
--------------------------------------------------------------------------------
00e0-fc01-0005       1/-                  Eth2/0/1                    dynamic

--------------------------------------------------------------------------------
Total items displayed = 1
```

执行命令 **display mac-address blackhole**，可以查看黑洞 MAC 表项对应的目的 MAC 地址、出接口号、出接口所属 VLAN 的编号是否配置正确。

```
<Huawei> display mac-address blackhole
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge             Learned-From               Type
--------------------------------------------------------------------------------
00e0-1234-5678       2/-                  -                          blackhole

--------------------------------------------------------------------------------
Total items displayed = 1
```

执行命令 **display mac-address aging-time**，可以查看动态 MAC 表项的老化时间是否配置正确。

```
<Huawei> display mac-address aging-time
Aging time: 300 seconds
```

执行命令 **display mac-address summary**，可以查看所有 MAC 地址表项的数目。

```
<Huawei> display mac-address summary
Mac Item of Lan Switch
------------------------------------------------------------------
Slot Total Blackhole Static DynLoc DynRmt Secure Sticky Block Authen
------------------------------------------------------------------
0        2         1      1      0      0      0      0     0      0
------------------------------------------------------------------
sum:     2         1      1      0      0      0      0     0      0

Mac Item of Transparent Bridge
--------------------------------
Total  Blackhole  Static  Dynamic
--------------------------------
0              0       0        0
```

6.4 配置接口安全

介绍接口安全的配置过程与步骤。

6.4.1 建立配置任务

应用环境

接口安全功能可以通过配置阻止其他非信任的 MAC 主机通过本接口和路由器通信，主要应用在对接入用户的安全性要求较高的网络中。

前置任务

无

数据准备

在配置接口安全功能之前，需要准备以下数据。

序号	数据
1	接口类型和接口编号
2	接口安全 MAC 学习数量
3	（可选）接口安全保护动作

6.4.2 使能接口安全功能

背景信息

使能接口安全功能后，接口学习到的 MAC 地址为安全动态 MAC 地址，安全动态 MAC 地址不会被老化，设备重启后安全动态 MAC 地址会丢失，需要重新学习。

接口安全的其他配置需要使能接口安全后才可以配置，如安全保护动作、安全 MAC 学习限制数量、Sticky MAC 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port-security enable**，使能接口安全功能。

缺省情况下，AR2200-S 的接口未使能接口安全功能。

说明

对于同一接口，不支持同时配置接口安全功能和端口使能 MUX-VLAN。

----结束

6.4.3 使能接口 Sticky MAC 功能

背景信息

Sticky MAC 的主要作用是将接口学习到的动态 MAC 地址转换成静态 MAC 地址，可以理解为将 MAC 地址黏在接口上。当接口学习的最大 MAC 数量达到上限后，不再学习新的 MAC 地址，只允许这些 Sticky MAC 和路由器通信。这样一可以避免在设备重启后动态 MAC 丢失需要重新学习，二可以阻止其他非信任的 MAC 主机通过本接口和路由器通信。

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 **port-security mac-address sticky**，使能接口 Sticky MAC 功能。

缺省情况下，接口未使能 Sticky MAC 功能。

步骤 4 （可选）执行命令 **port-security mac-address sticky** *mac-address* **vlan** *vlan-id*，手动配置一条 **sticky-mac** 表项。

----结束

6.4.4 （可选）配置接口安全 MAC 学习限制数量

背景信息

- 在没有使能 Sticky MAC 功能时，本配置任务用于限制接口学习的安全动态 MAC 地址数量。
- 在使能 Sticky MAC 功能后，本配置任务用于限制接口学习的 Sticky MAC 数量。

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 **port-security max-mac-num** *max-number*，配置接口安全 MAC 学习限制数量。

使能接口安全功能后，缺省情况下，接口学习的 MAC 地址限制数量为 1。

----结束

6.4.5 （可选）配置接口安全保护动作

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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置接口安全保护动作。

缺省情况下，接口安全保护动作为 **restrict**。

----结束

6.4.6 （可选）配置接口安全动态 MAC 地址的老化时间

背景信息

使能接口安全功能后，接口学习到的 MAC 地址为安全动态 MAC 地址，缺省情况下安全动态 MAC 地址不会被老化。

若用户只在一段时间内信任该接口学习到的 MAC 地址，则可以配置接口安全动态 MAC 地址的老化时间。使接口学习到的安全动态 MAC 地址变为可以老化的 MAC 地址。

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 **port-security aging-time** *aging-time*，配置接口学习到的安全动态 MAC 地址的老化时间。

使能接口安全功能后，缺省情况下，接口学习的安全动态 MAC 地址不老化。

说明

使能接口安全功能后，才能配置安全动态 MAC 地址的老化时间。

----结束

6.4.7 检查配置结果

操作步骤

- 使用命令 **display current-configuration interface** *interface-type interface-number* 查看接口配置信息。
- 使用命令 **display mac-address** 查看安全动态 MAC 和 Sticky MAC 表项。

----结束

任务示例

执行命令 **display mac-address**，可以查看安全动态 MAC 和 Sticky MAC 表项。

```
<Huawei> display mac-address sticky
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge           Learned-From          Type
--------------------------------------------------------------------------------
0000-1111-3333       2/-                Eth0/0/2              sticky

--------------------------------------------------------------------------------
Total items displayed = 1
```

6.5 配置 MAC 地址学习限制

介绍基于接口和 VLAN 的 MAC 表配置过程与步骤。

6.5.1 建立配置任务

应用环境

限制 MAC 地址的学习主要应用于接入用户已固定，但易受黑客攻击的网络环境，如小区用户、缺乏安全管理的企业内部网。

前置任务

无

数据准备

在配置 MAC 地址学习限制之前，需要准备以下数据。

序号	数据
1	（可选）基于接口、VLAN 的 MAC 地址学习限制规则

6.5.2 配置基于接口的 MAC 地址学习限制规则

背景信息

请在需要限制 MAC 表的表项的 AR2200-S 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 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **mac-limit maximum** *max-number*，限制接口的 MAC 地址学习数量。

缺省情况下，不限制 MAC 地址学习数量。

步骤 4 执行命令 **mac-limit action** { **discard** | **forward** }，配置当 MAC 地址数量达到限制后，对报文应采取的动作。

缺省情况下，对超过 MAC 地址学习限制的报文采取直接丢弃的动作。

步骤 5 执行命令 **mac-limit alarm** { **disable** | **enable** }，配置当 MAC 地址数量达到限制后是否进行告警。

缺省情况下，对超过 MAC 地址学习限制的报文进行告警。

----结束

6.5.3 配置基于 VLAN 的 MAC 地址学习限制规则

背景信息

请在需要限制 MAC 表的表项的 AR2200-S 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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **mac-limit maximum** *max-number*，限制 VLAN 上的 MAC 地址学习数量。

缺省情况下，不限制 MAC 地址学习数量。

步骤 4 执行命令 **mac-limit alarm** { **disable** | **enable** }，配置当 MAC 地址数量达到限制后是否进行告警。

缺省情况下，对超过 MAC 地址学习限制的报文进行告警。

----结束

6.5.4 检查配置结果

操作步骤

步骤 1 使用命令 **display mac-limit** [*interface-type interface-number* | **vlan** *vlan-id*] 查看 MAC 地址学习限制规则。

----结束

任务示例

执行命令 **display mac-limit**，可以查看 MAC 地址学习限制的配置是否正确。

```
<Huawei> display mac-limit
------------------------------------------------------------------------------
PORT                      VLAN      Maximum      Action      Alarm
------------------------------------------------------------------------------
Eth2/0/2                   -          100          discard     enable

------------------------------------------------------------------------------
```

6.6 配置 MAC 地址漂移检测功能

介绍 MAC 地址漂移检测功能的配置方法。

6.6.1 建立配置任务

应用环境

MAC 地址漂移检测功能可以检测指定 VLAN 下的所有 MAC 地址是否发生漂移。若 MAC 地址发生漂移则执行阻断接口或上报告警等处理动作，可以阻断网络环路和防止网络攻击。

前置任务

无

数据准备

在配置 MAC 地址漂移检测功能之前，需要准备以下数据：

序号	数据
1	MAC 地址漂移检测的 VLAN 编号
2	接口的阻断时间
3	指定接口永久阻断的重试次数

6.6.2 配置 MAC 地址漂移检测

背景信息

配置 MAC 地址漂移检测功能可以检测指定 VLAN 下的所有的 MAC 地址是否发生漂移。当 MAC 地址发生漂移时，可根据需求配置阻断接口或 MAC 地址、或者上报告警。

请在需要配置 MAC 地址漂移检测功能的 AR2200-S 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 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。

步骤 3 执行命令 **loop-detect eth-loop** { [**block-mac**] **block-time** *block-time* **retry-times** *retry-times* | **alarm-only** }，配置 MAC 地址漂移检测功能。

当系统检测到 VLAN 内有 MAC 地址发生漂移时，可以进行以下处理动作：

- 接口阻断或 MAC 地址阻断。当检测到 MAC 地址发生漂移则执行接口阻断或 MAC 地址阻断动作。当指定 **block-mac** 参数时，将不阻断整个接口，而是按照发生漂移的 MAC 地址进行流量阻断。
- 发送告警。当检测到 MAC 地址发生漂移时只给网管发送告警。

----结束

6.6.3 解除接口阻断或 MAC 地址阻断

背景信息

当系统检测到某 VLAN 内有 MAC 地址发生漂移且发生漂移的接口或 MAC 地址被永久阻断时，只能通过配置解除指定 VLAN 下的接口阻断或 MAC 地址阻断来恢复到正常状态。

请在需要解除指定 VLAN 下接口或 MAC 地址阻断的 AR2200-S 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 **reset loop-detect eth-loop vlan** *vlan-id* { **all** | **interface** { *interface-type interface-number* } | **mac-address** *mac-address* }，配置解除指定 VLAN 下的接口阻断或 MAC 地址阻断。

执行 **reset loop-detect eth-loop** 命令解除指定 VLAN 下的接口阻断或 MAC 地址阻断前，应当先执行 **display loop-detect eth-loop** 命令查看 MAC 地址漂移检测信息，根据检测信息进行相应的解除阻断配置。

----结束

6.6.4 检查配置结果

操作步骤

步骤 1 使用命令 **display loop-detect eth-loop** [**vlan** *vlan-id*]来查看指定 VLAN 下 MAC 地址漂移的检测信息。

----结束

任务示例

执行命令 **display loop-detect eth-loop**，可以查看指定 VLAN 下检测 MAC 地址漂移的配置信息、永久阻断的接口信息和 MAC 地址信息。

```
<Huawei> display loop-detect eth-loop
VLAN            Block-time      RetryTimes      Block-action
--------------- --------------- --------------- ---------------
111             111             1               block-port
628             118             1               block-mac

Total items:2

Blocked ports:

Total items:0

PortName                 Vlan      Status          Expire(s)       Leave times
------------------------ --------  --------------  --------------  --------------

Blocked Mac Address:

Total items:2

Mac Address              Vlan      Status          Expire(s)       Leave times
------------------------ --------  --------------  --------------  --------------
0000-1111-01aa           628       Block forever       -               -
0000-1111-01b2           628       Block forever       -               -
```

6.7 配置丢弃全 0 非法 MAC 地址报文

介绍配置丢弃全 0 非法 MAC 地址报文的过程与步骤。

6.7.1 建立配置任务

应用环境

当 AR2200-S 收到报文的源 MAC 地址或目的 MAC 地址为全 0 非法 MAC 地址时，可以配置此功能将该报文丢弃。

前置任务

无

数据准备

无

6.7.2 配置丢弃全 0 非法 MAC 地址报文功能

背景信息

在需要配置丢弃全 0 非法 MAC 地址报文的 AR2200-S 设备上进行如下配置。

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 **drop illegal-mac enable**，配置 AR2200-S 设备丢弃全 0 非法 MAC 地址报文。

缺省情况下，AR2200-S 设备没有配置丢弃全 0 非法 MAC 地址报文的功能。

----结束

6.7.3 配置重新触发新告警

背景信息

当 AR2200-S 收到第一个源 MAC 或目的 MAC 地址为全 0 非法 MAC 地址的报文时，会对该报文进行丢弃，并向网管上报一条告警。后继收到相同报文时，只会丢弃，不会再上报告警。执行本命令，可重新触发新告警。

在需要重新触发新告警的 AR2200-S 设备上进行如下配置。

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 **drop illegal-mac alarm**，配置重新触发新告警。

缺省情况下，设备已经配置了重新触发新告警功能。

----结束

6.7.4 检查配置结果

操作步骤

步骤 1 使用 **display current-configuration** 命令查看 AR2200-S 设备是否配置丢弃全 0 非法 MAC 地址报文的功能。

----结束

任务示例

执行命令 **display current-configuration**，查看 AR2200-S 设备是否配置丢弃全 0 非法 MAC 地址报文的功能。

```
<Huawei> display current-configuration | include drop
#
 drop illegal-mac alarm
 drop illegal-mac enable
#
```

6.8 维护

介绍维护 MAC 表的相关命令和方法。

6.8.1 调试 MAC 表

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 MAC 表运行故障时，请在用户视图下执行 **debugging** 命令对 MAC 地址表进行调试，查看调试信息，定位故障并分析故障原因。

操作步骤

步骤 1 使用命令 **debugging ethernet packet mac** { **dest_mac** *mac-address* | **src_mac** *mac-address* }打开源 MAC 地址或目的 MAC 地址为指定值的以太网报文的调试信息开关。

----结束

6.9 配置举例

介绍 MAC 表的各种组网举例。

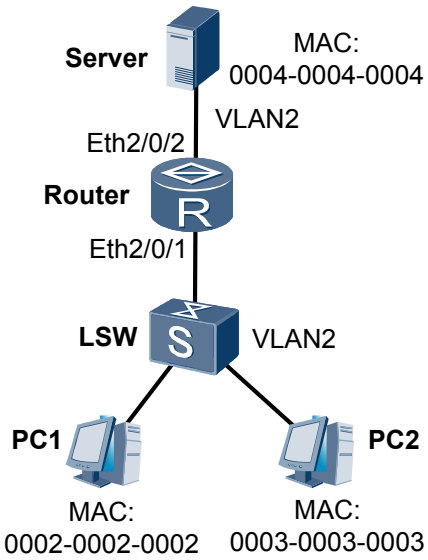
6.9.1 配置 MAC 表示例

组网需求

如图 6-1 所示，用户主机 PC1 和 PC2 的 MAC 地址分别为 0002-0002-0002 和 0003-0003-0003，通过 LSW 连接 Router。连接 Router 的接口为 Ethernet2/0/1，该接口所属 VLAN 为 VLAN2。Server 服务器的 MAC 地址为 0004-0004-0004，连接 Router 的接口为 Ethernet2/0/2，该接口所属 VLAN 为 VLAN2。

- 为防止 MAC 地址攻击，在 Router 的 MAC 表中为该用户主机添加一条静态表项。配置 Router 的动态 MAC 表项老化时间为 500s。
- 为防止假冒 Server 的 MAC 地址窃取重要用户信息，在 Router 上配置静态 MAC 地址转发功能。

图 6-1 配置 MAC 表组网图



配置思路

采用如下的思路配置 MAC 表：

1. 创建 VLAN，并将接口加入到 VLAN 中。
2. 添加静态 MAC 表。
3. 配置动态 MAC 表的老化时间。

数据准备

为完成此配置例，需准备如下的数据：

- PC1 的 MAC 地址为 0002-0002-0002。
- PC2 的 MAC 地址为 0003-0003-0003。
- Server 的 MAC 地址为 0004-0004-0004。
- Router 所属 VLAN 为 VLAN2。
- 与 LSW 相连的 Router 的接口为 Ethernet2/0/1。
- 与 Server 相连的 Router 的接口为 Ethernet2/0/2。
- Router 的动态 MAC 表项老化时间为 500s。

操作步骤

步骤 1 添加静态 MAC 地址表项

创建 VLAN2，将接口 Ethernet2/0/1、Ethernet2/0/2 加入 VLAN2。

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] quit
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port hybrid tagged vlan 2
[Huawei-Ethernet2/0/1] quit
[Huawei] interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] port hybrid pvid vlan 2
[Huawei-Ethernet2/0/2] port hybrid untagged vlan 2
[Huawei-Ethernet2/0/2] quit
```

配置静态 MAC 地址表项。

```
[Huawei] mac-address static 0002-0002-0002 ethernet 2/0/1 vlan 2
[Huawei] mac-address static 0003-0003-0003 ethernet 2/0/1 vlan 2
[Huawei] mac-address static 0004-0004-0004 ethernet 2/0/2 vlan 2
```

步骤 2 配置动态表项老化时间

```
[Huawei] mac-address aging-time 500
```

步骤 3 验证配置结果

在任意视图下执行 **display mac-address** 命令，查看静态 MAC 表是否添加成功。

```
[Huawei] display mac-address static vlan 2
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge             Learned-From               Type
--------------------------------------------------------------------------------
0002-0002-0002       2/-                  Eth2/0/1                   static
0003-0003-0003       2/-                  Eth2/0/1                   static
0004-0004-0004       2/-                  Eth2/0/2                   static

--------------------------------------------------------------------------------
Total items displayed = 3
```

在任意视图下执行 **display mac-address aging-time** 命令，查看动态表项老化时间是否配置成功。

```
[Huawei] display mac-address aging-time
  Aging time: 500 seconds
```

----结束

配置文件

以下仅给出 Router 的配置文件。

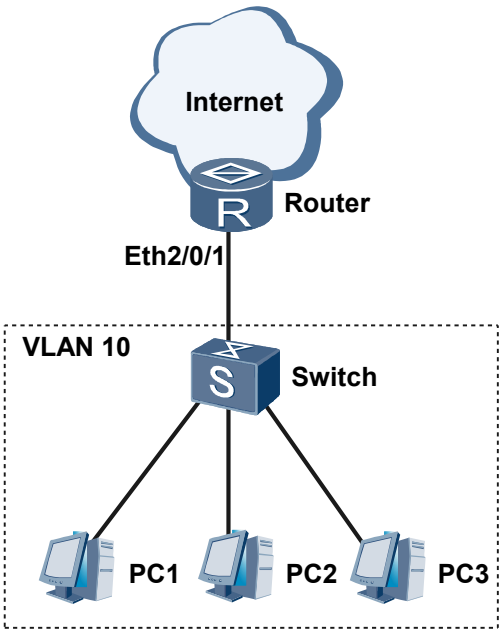
```
#
 vlan batch 2
#
 mac-address aging-time 500
#
interface Ethernet2/0/1
 port hybrid tagged vlan 2
#
interface Ethernet2/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
 mac-address static 0002-0002-0002 Ethernet2/0/1 vlan 2
 mac-address static 0003-0003-0003 Ethernet2/0/1 vlan 2
 mac-address static 0004-0004-0004 Ethernet2/0/2 vlan 2
#
return
```

6.9.2 配置接口安全示例

组网需求

如图 6-2 所示，公司为了提高信息安全，将 Router 连接员工 PC 侧的接口使能了接口安全功能，并且设置了接口学习 MAC 地址数的上限为信任的设备总数，这样其他外来人员使用自己带来的 PC 无法访问公司的网络。

图 6-2 配置接口安全示例组网图



配置思路

采用如下的思路配置接口安全：

1. 创建 VLAN，并配置接口的链路类型为 Trunk。
2. 使能接口安全功能。
3. 使能接口 Sticky MAC 功能。
4. 配置接口安全功能的保护动作。
5. 配置接口 MAC 地址学习限制数。

数据准备

为完成此配置例，需准备如下的数据：

- 接口允许通过的 VLAN 编号。
- Router 连接 PC 的接口类型和编号。
- 接口安全功能的保护动作。
- 接口 MAC 地址学习限制数。

操作步骤

步骤 1 创建 VLAN，并配置接口的链路类型

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type trunk
[Huawei-Ethernet2/0/1] port trunk allow-pass vlan 10
```

步骤 2 配置接口安全功能

使能接口安全功能。

```
[Huawei-Ethernet2/0/1] port-security enable
```

使能接口 Sticky MAC 功能。

```
[Huawei-Ethernet2/0/1] port-security mac-address sticky
```

配置接口安全功能的保护动作。

```
[Huawei-Ethernet2/0/1] port-security protect-action protect
```

配置接口 MAC 地址学习限制数。

```
[Huawei-Ethernet2/0/1] port-security max-mac-num 4
```

其他接口如需使能接口安全功能，请重复上述配置。

步骤 3 验证配置结果

将 PC1 换成其他设备，无法访问公司网络。

----结束

配置文件

以下仅给出 Router 的配置文件。

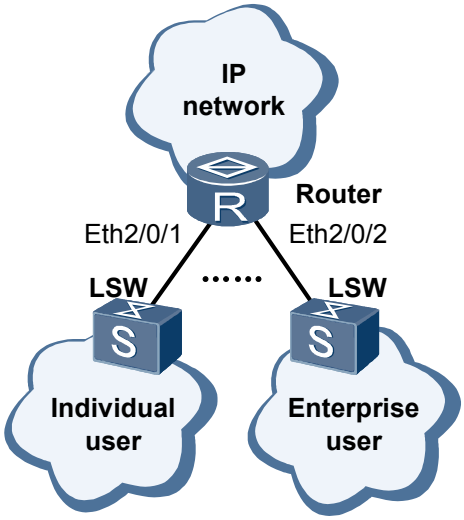
```
#
 vlan batch 10
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 port-security enable
 port-security protect-action protect
 port-security mac-address sticky
 port-security max-mac-num 4
#
return
```

6.9.3 配置基于接口的 MAC 地址学习限制示例

组网需求

如图 6-3 所示，Router 通过接口 Ethernet2/0/1、Ethernet2/0/2 与 LSW 连接，个人用户和企业用户通过 LSW 与 Router 连接。为防止 MAC 地址攻击，控制接入用户数量，对接口 Ethernet2/0/1、Ethernet2/0/2 进行 MAC 地址学习的限制。

图 6-3 配置基于接口的 MAC 地址学习限制组网图



配置思路

采用如下的思路配置基于接口的 MAC 地址学习限制：

1. 配置接口的 MAC 地址学习限制。
2. 配置 MAC 地址学习限制的动作。

数据准备

为完成此配置例，需准备如下的数据：

- 接口 Ethernet2/0/1 的 MAC 地址学习限制数为 4。
- 接口 Ethernet2/0/2 的 MAC 地址学习限制数为 100。
- MAC 地址学习限制的动作为丢弃并告警。

操作步骤

步骤 1 配置 MAC 地址学习限制

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] mac-limit maximum 4 action discard alarm enable
[Huawei-Ethernet2/0/1] quit
[Huawei] interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] mac-limit maximum 100 action discard alarm enable
[Huawei-Ethernet2/0/2] quit
```

步骤 2 验证配置结果

在任意视图下执行 **display mac-limit** 命令，查看 MAC 地址学习限制规则是否配置成功。

```
<Huawei> display mac-limit
------------------------------------------------------------------------
PORT                    VLAN      Maximum      Action      Alarm
------------------------------------------------------------------------
Eth2/0/1                -         4            discard     enable
```

```
Eth2/0/2                -          100          discard     enable
------------------------------------------------------------------------------
```

----结束

配置文件

以下仅给出 Router 的配置文件。

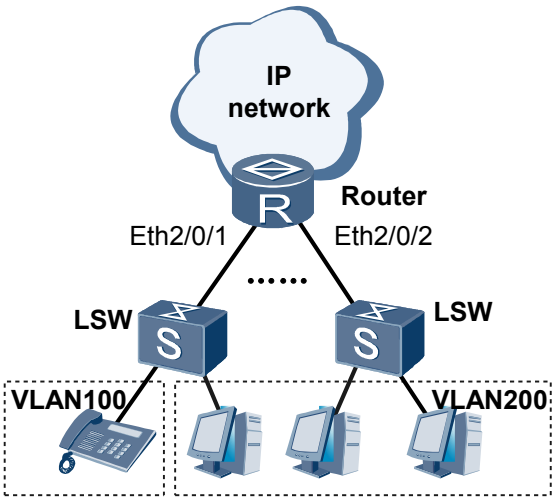
```
#
 sysname Huawei
#
interface Ethernet2/0/1
 mac-limit maximum 4
#
interface Ethernet2/0/2
 mac-limit maximum 100
#
return
```

6.9.4 配置基于 VLAN 的 MAC 地址学习限制示例

组网需求

如图 6-4 所示，Router 通过接口 Ethernet2/0/1、Ethernet2/0/2 与 LSW 连接，用户网络通过 LSW 与 Router 连接。用户网络主要由 IP 电话用户和 PC 上网用户组成。IP 电话用户相对较少，分布在 VLAN100 中。PC 上网用户分布相对较多，分布在 VLAN200 中。为防止 MAC 地址攻击，控制接入用户占用 MAC 地址表项目空间，对 VLAN200 内的 PC 上网用户进行 MAC 地址学习的限制。

图 6-4 配置基于 VLAN 的 MAC 地址学习限制组网图



配置思路

采用如下的思路配置基于 VLAN 的 MAC 地址学习限制：

1. 创建 VLAN，并将接口加入到 VLAN 中。
2. 配置 VLAN 的 MAC 地址学习限制。

数据准备

为完成此配置例，需准备如下的数据：

- 接口 Ethernet2/0/1 所属 VLAN 为 VLAN100、VLAN200。
- 接口 Ethernet2/0/2 所属 VLAN 为 VLAN200。
- VLAN200 的最大 MAC 地址学习数量设置为 500 和发送告警。

操作步骤

步骤 1 配置基于 VLAN 的 MAC 地址学习限制

将 Ethernet2/0/1、Ethernet2/0/2 加入 VLAN。

```
<Huawei> system-view
[Huawei] vlan batch 100 200
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type trunk
[Huawei-Ethernet2/0/1] port trunk allow-pass vlan 100 200
[Huawei-Ethernet2/0/1] quit
[Huawei] interface ethernet 2/0/2
[Huawei-Ethernet2/0/2] port link-type trunk
[Huawei-Ethernet2/0/2] port trunk allow-pass vlan 200
[Huawei-Ethernet2/0/2] quit
```

在 VLAN200 上配置 MAC 地址学习限制规则：最多可以学习 500 个 MAC 地址，超过最大 MAC 地址学习数量的报文继续转发但不加入 MAC 地址表，并进行告警提示。

```
[Huawei] vlan 200
[Huawei-vlan200] mac-limit maximum 500 alarm enable
[Huawei-vlan200] quit
```

步骤 2 验证配置结果

在任意视图下执行 **display mac-limit** 命令，查看 MAC 地址学习限制规则是否配置成功。

```
<Huawei> display mac-limit
------------------------------------------------------------------------------
PORT                    VLAN      Maximum      Action      Alarm
------------------------------------------------------------------------------
-                       200       500          forward     enable

------------------------------------------------------------------------------
```

----结束

配置文件

以下仅给出 Router 的配置文件。

```
#
 sysname Huawei
#
 vlan batch 100 200
#
vlan 200
 mac-limit maximum 500
#
```

```
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
return
```

7 STP/RSTP 配置

关于本章

STP（Spanning Tree Protocol，生成树协议）将环形网络修剪成为一个无环的树型网络，避免报文在环形网络中的增生和无限循环；RSTP（Rapid Spanning Tree Protocol，快速生成树协议）在 STP 基础上实现了快速收敛，并增加了边缘端口的概念及保护功能。

7.1 STP/RSTP 概述
STP/RSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，解决交换网络中的环路问题。

7.2 AR2200-S 支持的 STP/RSTP 特性
配置 STP/RSTP 时，您将接触到基本功能、拓扑收敛、保护功能以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

7.3 配置 STP/RSTP 基本功能
对于一个存在环路的以太网，通过给网络中的交换设备配置 STP/RSTP 基本功能，STP/RSTP 协议阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。

7.4 配置 STP/RSTP 影响拓扑收敛的参数
基于 STP 没有对拓扑是否已经收敛制定反馈机制，RSTP 在 STP 基础上实现了快速收敛。

7.5 配置 RSTP 保护功能
华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

7.6 维护 STP/RSTP
STP/RSTP 相关维护命令，包括清除 STP/RSTP 的统计数据。

7.7 配置举例
配置举例结合组网需求、配置思路和数据准备来了解实际网络中 STP/RSTP 的应用场景，并提供配置文件。

7.1 STP/RSTP 概述

STP/RSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，解决交换网络中的环路问题。

STP/RSTP 概述

在一个复杂的网络环境中，难免会出现环路。并且，由于冗余备份的需要，网络设计者都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样，偶然或必然中都会导致环路产生。

环路会产生广播风暴，最终导致整个网络资源被耗尽，网络瘫痪不可用。环路还会引起 MAC 地址表震荡导致 MAC 地址表项被破坏。

为了破除环路，可以采用数据链路层协议 STP，运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

但是，STP 拓扑收敛速度慢，IEEE 于 2001 年发布的 802.1W 标准定义了 RSTP，RSTP 在 STP 基础上进行了改进，实现了网络拓扑快速收敛。

STP/RSTP 相关概念

- 根桥

  树形网络结构必须有树根，于是 STP/RSTP 引入了根桥（Root Bridge）概念。

  对于一个 STP/RSTP 网络，根桥有且只有一个，它是整个网络的逻辑中心，但不一定是物理中心。但是根据网络拓扑的变化，根桥可能改变。

- ID

  ID 分为：桥 ID 即 BID（Bridge ID）和端口 ID 即 PID（Port ID）。

  - BID：桥 ID

    IEEE 802.1D 标准中规定 BID 是由 2 字节的桥优先级（Bridge Priority）与桥 MAC 地址构成，即 BID（8 字节）= 桥优先级（2 字节）+ 桥 MAC（6 字节）。

    在 STP 网络中，桥 ID 最小的设备会被选举为根桥。在华为公司的设备上，桥优先级支持手工配置。

  - PID：端口 ID

    PID 由两部分构成的，即 PID（16 位）= 端口优先级（4 位）+ 端口号（12 位）。

    PID 只在某些情况下对选择指定端口有作用，即在选择指定端口时，两个端口的根路径开销和发送交换设备 BID 都相同的情况下，比较端口的 PID，PID 小者为指定端口。如图 7-1 所示，设备 S2 的端口 A 和端口 B 的根路径开销和发送交换设备 BID 都相同，所以进行 PID 的比较，端口 A 的 PID 小，则该端口为所在网段的指定端口。在华为公司的设备上，端口优先级支持手工配置。

- 路径开销

  路径开销是一个端口量，是 STP/RSTP 协议用于选择链路的参考值。STP/RSTP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树形网络结构。

在一个 STP/RSTP 网络中，某端口到根桥累计的路径开销就是所经过的各个桥上的各端口的路径开销累加而成，这个值叫做根路径开销。

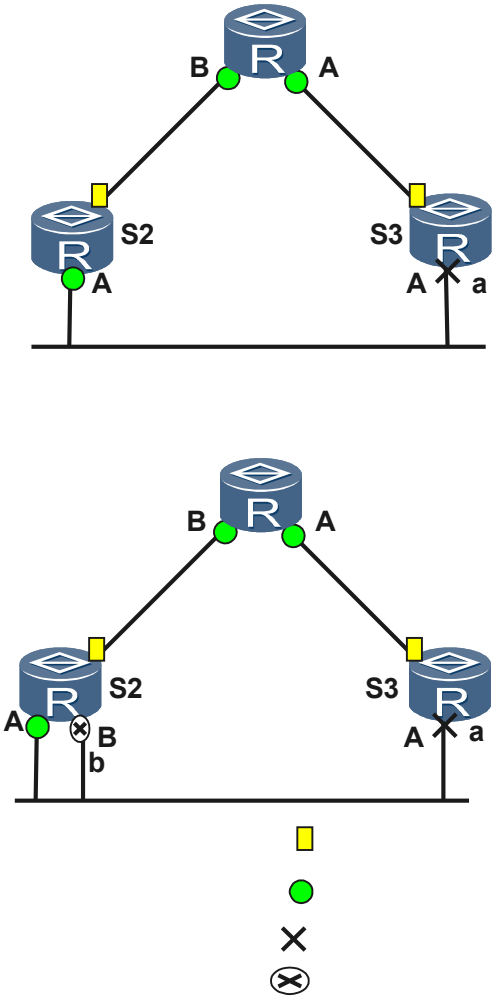
- 端口角色
  - STP 端口
    - 根端口

      所谓根端口就是去往根桥路径最近的端口，根端口负责向根桥方向转发数据，根端口的选择标准是依据根路径开销判定。在一台设备上所有使能 STP 的端口中，根路径开销最小者，就是根端口。在一个运行 STP/RSTP 协议的设备上根端口有且只有一个，而且根桥上没有根端口。
    - 指定端口

      对一台交换设备而言，它的指定端口是向下游交换设备转发 BPDU 报文的端口。根桥的所有端口都是指定端口。在环网的每一网段都会选举出一个指定端口，在一个网段上拥有指定端口的交换设备被称作该网段的指定桥。
  - RSTP 端口

    RSTP 在 STP 基础上新增加了 2 种端口角色：Alternate 端口和 Backup 端口。通过端口角色的增补，简化了生成树协议的理解及部署。

图 7-1 端口角色示意图



如图 7-1 所示，RSTP 的端口角色共有 4 种：根端口、指定端口、Alternate 端口和 Backup 端口。

根端口和指定端口的作用同 STP 协议中定义，Alternate 端口和 Backup 端口的描述如下：

- 从配置 BPDU 报文发送角度来看：
  - Alternate 端口是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。
  - Backup 端口是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。
- 从用户流量角度来看：
  - Alternate 端口作为根端口的备份端口，提供了从指定桥到根的另一条可切换路径。
  - Backup 端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。

- 端口状态
  - STP 端口状态

    运行 STP 协议的设备上端口状态如表 7-1 所示。

表 7-1 STP 端口状态

端口状态	目的	说明
Forwarding	端口既转发用户流量也转发 BPDU 报文。	只有根端口或指定端口才能进入 Forwarding 状态。
Learning	设备会根据收到的用户流量构建 MAC 地址表，但不转发用户流量。	过渡状态，增加 Learning 状态防止临时环路。
Listening	确定端口角色，将选举出根桥、根端口和指定端口。	过渡状态。
Blocking	端口仅仅接收并处理 BPDU，不转发用户流量。	阻塞端口的最终状态。
Disabled	端口不仅不转发 BPDU 报文，也不转发用户流量。	端口状态为 Down。

  - RSTP 端口状态

    RSTP 在 STP 基础上进行了端口状态的改进，如表 7-2 所示。

表 7-2 RSTP 端口状态

端口状态	说明
Forwarding	在这种状态下，端口既转发用户流量又接收/发送 BPDU 报文。

端口状态	说明
Learning	这是一种过渡状态。在 Learning 下，交换设备会根据收到的用户流量，构建 MAC 地址表，但不转发用户流量，所以叫做学习状态。 Learning 状态的端口接收/发送 BPDU 报文，不转发用户流量。
Discarding	Discarding 状态的端口只接收 BPDU 报文。

注意

华为公司数据通信设备缺省情况处于 MSTP 模式，当从 MSTP 模式切换到 STP 模式，运行 STP 协议的设备上端口支持的端口状态仍然保持和 MSTP 支持的端口状态一样（MSTP 端口状态与 RSTP 端口状态相同），支持的状态仅包括 Forwarding、Learning 和 Discarding，如表 7-2 所示。

- 三种定时器
  - Hello Timer

    通过设置 Hello Timer 定时器时间的大小控制 BPDU 发送间隔。
  - Forward Delay Timer

    通过设置 Forward Delay Timer 定时器时间的大小控制端口在 Listening 和 Learing 状态的持续时间。
  - Max Age

    通过设置 Max Age 定时器时间的大小控制存储 BPDU 的超时时间，超时认为根桥连接失败。

三种生成树协议的比较

对于 STP/RSTP/MSTP 三种生成树协议，特点与场景比较如表 7-3 所示。

表 7-3 STP/RSTP/MSTP 特点与场景比较

生成树协议	特点	应用场景	注意事项
STP	形成一棵无环路的树：解决广播风暴并实现冗余备份。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。	**说明** ● 若当前交换设备既支持 STP 又支持 RSTP，建议选择使用 RSTP。 ● 若当前交换设备既支持 STP/RSTP 又支持 MSTP，建议选择使用 MSTP，详见 **MSTP 配置**。
RSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。		

生成树协议	特点	应用场景	注意事项
MSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。 ● 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。	

7.2 AR2200-S 支持的 STP/RSTP 特性

配置 STP/RSTP 时，您将接触到基本功能、拓扑收敛、保护功能以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

STP/RSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。

为了满足特殊场合的应用和功能扩展，STP/RSTP 还支持如下功能：

- RSTP 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。
- RSTP 提供如表 7-4 所示的各种保护功能。
- 为了实现与其他制造商设备的互通，需要在华为公司运行 STP/RSTP 的设备上配置合适的参数，以确保通信畅通。

表 7-4 RSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

保护功能	场景	配置影响
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

7.3 配置 STP/RSTP 基本功能

对于一个存在环路的以太网，通过给网络中的交换设备配置 STP/RSTP 基本功能，STP/RSTP 协议阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。

通过给交换设备配置 STP/RSTP 的工作模式后，启动 STP/RSTP，STP/RSTP 便开始进行生成树计算，将网络修剪成树状，破除环路。但是，若网络规划者需要人为干预生成树计算的结果，可以采取以下方式：

- 配置交换设备的优先级数值：数值越小，交换设备的优先级越高，成为根桥的可能性越大；数值越大，交换设备的优先级越低，成为根桥的可能性越小。
- 配置端口路径开销数值：在同一种计算方法下，数值越小，端口到根桥的路径开销越小，成为根端口的可能性就越大；数值越大，端口到根桥的路径开销越大，成为根端口的可能性越小。
- 配置端口的优先级数值：数值越小，端口成为指定端口的可能性就越大；数值越大，端口成为指定端口的可能性越小。

7.3.1 建立配置任务

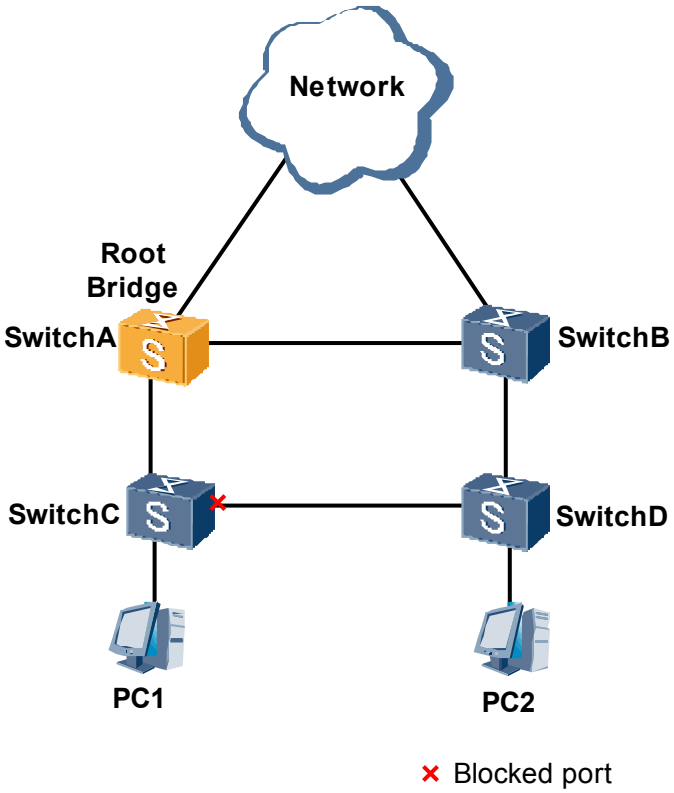
在配置 STP/RSTP 基本功能前，请认真了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。网络规划者规划好网络后，可在网络中部署 STP/RSTP 协议预防环路。当网络中存在环路，STP/RSTP 通过阻塞某个端口以达到破除环路的目的。

如图 7-2 所示，S1、S2、S3 和 S4 构成环形网络，通过在环形网络中运行 STP/RSTP 以破除环路，提高网络的可靠性。

图 7-2 环形网络示意图



说明

若当前设备既支持 STP 又支持 RSTP，建议选择使用 RSTP。

前置任务

在配置 STP/RSTP 基本功能之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up

数据准备

在配置 STP/RSTP 基本功能之前，需要准备以下数据。

序号	数据
1	（可选）当前交换设备的优先级数值
2	（可选）端口优先级数值
3	（可选）端口的路径开销值

7.3.2 配置 STP/RSTP 工作模式

在配置 STP/RSTP 基本功能前需要选择 STP/RSTP 工作模式，RSTP 兼容 STP。

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 **stp mode** { **stp** | **rstp** }，配置交换设备的 STP/RSTP 工作模式。

默认情况下，交换设备会运行 MSTP 模式，MSTP 模式兼容 STP 和 RSTP 模式。

在只运行 STP 的环形网络中，交换设备可选择 STP 模式；在只运行 RSTP 的环形网络中，交换设备可选择 RSTP 模式。其他情况，建议选择默认情况 MSTP 模式。

----结束

7.3.3 （可选）配置交换设备优先级

在环形网络中，选举其中的一个交换设备作为根桥，用户可以通过配置交换设备的优先级人为影响根桥的选择，交换设备优先级值越小，则交换设备在环网中的优先级越高，成为根桥的可能性越大。

背景信息

在一个运行 STP/RSTP 的网络中，有且仅有一个根桥，它是整棵生成树的逻辑中心。在进行根桥的选择时，一般会希望选择性能高、网络层次高的交换设备作为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此需要配置优先级以保证该设备成为根桥。

对于网络中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

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 **stp priority** *priority*，配置交换设备在系统中的优先级。

缺省情况下，交换设备的优先级取值是 32768。

说明

- 如果为当前设备配置系统优先级目的是配置当前设备为根桥设备，则可以直接选择执行命令 **stp root primary**，配置后该设备优先级数值自动为 0。
- 执行命令 **stp root secondary** 可以配置当前交换设备为备份根桥设备，配置后该设备优先级数值自动为 4096。

  同一台交换设备不能既作为根桥又作为备用根桥。
- 如果已经通过执行命令 **stp root primary** 或命令 **stp root secondary** 指定当前设备为根桥设备或备份根桥设备，需要改变当前设备的优先级则需要执行 **undo stp root** 去使能根交换设备或者备份根交换设备功能，然后执行命令 **stp priority** *priority* 配置新的优先级数值。

----结束

7.3.4 （可选）配置端口路径开销

在一台设备所有使能 STP/RSTP 的端口中，到根桥的路径开销最小者，就是根端口，用户可以通过配置交换设备到根桥的路径开销人为影响根端口的选择。

背景信息

路径开销是一个端口量，是 STP/RSTP 协议用于选择链路的参考值。

端口路径开销值取值范围由路径开销计算方法决定，当确定路径开销计算方法后，如果端口所处链路的速率值越大，则建议将该端口的路径开销值在指定范围内设置越小。

以华为的私有计算方法为例，不同速率的端口路径开销的缺省值不同，具体参见表 7-5。

表 7-5 端口所对应的链路速率与端口路径开销值对应表

链路速率	推荐值	推荐取值范围	值域
10Mbit/s	2000	200 ～ 20000	1 ～ 200000
100Mbit/s	200	20 ～ 2000	1 ～ 200000
1Gbit/s	20	2 ～ 200	1 ～ 200000
10Gbit/s	2	2 ～ 20	1 ～ 200000
10Gbit/s 以上	1	1 ～ 2	1 ～ 200000

存在环路的网络环境中，对于链路速率值相对较小的端口，建议将其路径开销值配置相对较大，以使其在生成树算法中被选举成为阻塞端口，阻塞其所在链路。

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 **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }，配置端口路径开销计算方法。

缺省情况下，路径开销值的计算方法为 IEEE 802.1t 标准方法。

同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 4 执行命令 **stp cost** *cost*，设置当前端口的路径开销值。

- 使用华为的私有计算方法时参数 *cost* 取值范围是 1 ～ 200000。
- 使用 IEEE 802.1d 标准方法时取值范围是 1 ～ 65535。
- 使用 IEEE 802.1t 标准方法时取值范围是 1 ～ 2000,000,00。

----结束

7.3.5 （可选）配置端口优先级

通过端口的根路径开销、发送交换设备的 BID 及端口 ID 为每个连接选举出一个指定端口。交换设备的端口优先级值越小，则在生成树算法中进行指定端口选举时，该端口被指定为指定端口的机率越大；否则，该端口在生成树算法中被阻塞的机率越大。

背景信息

在参与 STP/RSTP 生成树计算时，对于处在环路中的交换设备端口，其优先级的高低会影响到是否被选举为指定端口，详见 **STP/RSTP 概述**。

在根路径开销及发送交换设备的 BID 相同的情况下，如果希望将环路中的某交换设备的端口阻塞从而破除环路，则可将其端口优先级值设置比缺省值大，使得在选举过程中成为被阻塞的端口。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp port priority** *priority*，配置端口的优先级。

缺省情况下，交换设备端口的优先级取值是 128。

----结束

7.3.6 启用 STP/RSTP

使能 STP/RSTP 功能后，生成树算法才开始计算。

背景信息

在环形网络中一旦启用 STP/RSTP，STP/RSTP 便立即开始进行生成树计算。而且，诸如交换设备的优先级、端口优先级等参数都会影响到生成树的计算，在计算过程中这些参数的变动可能会导致网络震荡。为了保证生成树计算过程快速而且稳定，必须在交换设备及其端口进行必要的基本配置以后才能启用 STP/RSTP。

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 **stp enable**，使能交换设备的 STP/RSTP 功能。

缺省情况下，设备使能 STP/RSTP 功能。

----结束

7.3.7 检查配置结果

STP/RSTP 基本功能配置成功后，可查看生成树算法计算的结果是否符合要求，如：端口角色、端口状态等。

前提条件

已经完成 STP/RSTP 基本功能的配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息与统计信息。

----结束

任务示例

执行命令 **display stp**，可以查看生成树的工作模式、根桥、根桥优先级、收敛方式、路径开销缺省值的计算方法和根端口路径开销值等信息。例如：

```
<Huawei> display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :32768.00e0-4e1f-b200
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .00e0-e70a-4d00 / 20
CIST RegRoot/IRPC   :32768.00e0-4e1f-b200 / 0
CIST RootPortId     :128.1
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:26m:16s
----[Port1(Ethernet2/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)  :Config=auto / Active=20
 Designated Bridge/Port   :0.00e0-e70a-4d00 / 128.5
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :1
 TC or TCN received  :0
 BPDU Sent           :4
         TCN: 0, Config: 0, RST: 4, MST: 0
 BPDU Received       :22
         TCN: 0, Config: 0, RST: 22, MST: 0
----[Port2(Ethernet2/0/3)][DISCARDING]----
 Port Protocol       :enabled
 Port Role           :Alternate Port
 Port Priority       :160
 Port Cost(Legacy)   :Config=auto / Active=20
 Designated Bridge/Port   :4096.00e0-6606-be00 / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 14s FwDly 10s RemHop 0
 TC or TCN send      :1
 TC or TCN received  :0
 BPDU Sent           :2
         TCN: 0, Config: 0, RST: 2, MST: 0
 BPDU Received       :22
         TCN: 0, Config: 0, RST: 22, MST: 0
```

7.4 配置 STP/RSTP 影响拓扑收敛的参数

基于 STP 没有对拓扑是否已经收敛制定反馈机制，RSTP 在 STP 基础上实现了快速收敛。

STP 不能实现快速收敛，但是诸如网络直径、Hello Time 定时器、Max Age 定时器、Forward Delay 定时器等参数会影响其收敛速度。RSTP 在 STP 基础上进行改进之后，实现快速收敛。对于 STP/RSTP 影响拓扑收敛的参数，除了上述系统参数外，还有端口的链路类型、端口是否支持快速迁移机制、BPDU 的最大发送数目等端口参数。

对于运行 STP/RSTP 的设备，配置参数情况详见**表 7-6**。

表 7-6 影响 STP/RSTP 拓扑收敛的参数

参数类型	参数含义	涉及命令	说明
系统参数	网络直径和定时器（Hello Time、Forward Delay 和 Max Age）以及 Hello Time 定时器与倍数参数形成的超时时间	● stp bridge-diameter *diameter* ● stp timer hello *hello-time* ● stp timer forward-delay *forward-delay* ● stp timer max-age *max-age* ● stp timer-factor *factor*	建议直接通过配置网络直径控制定时器时间的大小，交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。然后通过 stp timer-factor *factor* 配置超时时间。
端口参数	端口的链路类型	● stp point-to-point { **auto** | **force-false** | **force-true** }	点对点链路帮助实现快速收敛。 ● 如果当前端口工作在全双工模式，则当前端口相连的链路是点对点链路。 ● 如果当前端口工作在半双工模式，可强制链路类型为点对点链路。 ● 其他情况选择端口自动识别是否与点对点链路相连。
	端口迁移到 RSTP 模式	● stp mcheck	在运行 RSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。 当端口无法自动迁回 RSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 RSTP 模式。

参数类型	参数含义	涉及命令	说明
	端口在每个 Hello Time 时间内 BPDU 的最大发送数目	● stp transmit-limit *packet-number*	适当的配置端口在每个 Hello time 时间内 BPDU 的最大发送数目，可以限制端口发送 BPDU 的速度，防止网络拓扑震荡时 RSTP 占用过多的带宽资源。
	边缘端口的设置	● stp edged-port **enable**	与终端相连的端口不用参与 STP/RSTP 计算，将该端口配置成边缘端口，该端口便不再参与计算。 在设备上配置 BPDU 保护功能后，边缘端口收到 BPDU 报文会被 Shutdown，可以实现端口在一定的延迟时间后自动恢复为 Up 状态。

7.4.1 建立配置任务

在进行 STP/RSTP 影响快速收敛的参数配置前，请认真了解各项配置的应用环境、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

在运行 RSTP 的网络环境中，快速收敛机制的实现需要配置一些影响快速收敛的参数，配置合适的参数后才能实现最佳快速收敛效果。

说明

因为本配置任务中所包含的命令缺省情况下也能完成 RSTP 的快速收敛，所以本配置任务所包含的所有配置过程，以及配置过程中包含的所有配置步骤都是可选的，可根据实际需要选择配置其中的部分内容。

前置任务

在配置 STP/RSTP 影响拓扑收敛的参数前，需完成以下任务：

- **配置 STP/RSTP 基本功能**

数据准备

在配置 STP/RSTP 影响拓扑收敛的参数之前，需要准备以下数据。

序号	数据
1	网络直径
2	Hello Time 时间、Forward Delay 时间、Max Age 时间、超时时间（3 x hello time x time factor）

序号	数据
3	端口的链路类型
4	端口是否使用普通的快速迁移机制
5	端口是否需要迁移回 RSTP 模式
6	BPDU 的最大发送数目值
7	端口是否需要设置为边缘端口
8	如果端口为边缘端口，是否需要配置其在 Shutdown 后自动恢复功能
9	端口是否需要清除生成树的统计信息
10	如果端口为边缘端口，是否需要配置端口为 BPDU filter 端口

7.4.2 配置系统参数

影响 STP/RSTP 拓扑收敛的系统参数有网络直径、Hello Time 定时器、未收到上游的 BPDU 就重新开始生成树计算的超时时间（3 x hello time x time factor）等，配置合适的系统参数，实现最快的拓扑收敛。

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 **stp bridge-diameter** *diameter*，配置网络直径。

缺省情况下，网络直径为 7。

- 快速生成树是在整个交换网络应用单生成树实例，不能解决由于网络规模增大带来的性能降低问题，网络直径不要超过 7。
- 建议通过执行命令 **stp bridge-diameter** *diameter* 配置网络直径去配置 Forward Delay 时间、Hello Time 时间以及 Max Age 时间，因为交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。

步骤 3 执行命令 **stp timer-factor** *factor*，配置未收到上游的 BPDU 就重新开始生成树计算的超时时间。

缺省情况下，交换设备未收到上游的 BPDU 就重新开始生成树计算的超时时间是 Hello Timer 的 9 倍。

步骤 4 （可选）若当前设备是网络边缘设备，可选择执行如下命令中的一个或多个：

- 执行命令 **stp edged-port default**，配置当前设备上所有端口为边缘端口。

  缺省情况下，端口为非边缘端口。

  在网络边缘设备上配置该命令，使端口不再参与生成树计算，从而帮助加快网络拓扑的收敛时间以及加强网络的稳定性。
- 执行命令 **stp bpdu-filter default**，配置当前设备上所有端口为 BPDU filter 端口。

  缺省情况下，端口为非 BPDU filter 端口。

在网络边缘设备上配置该命令，使边缘端口不处理、不发送 BPDU 报文，该端口即为 BPDU filter 端口。

警告

在系统视图下同时执行命令 **stp bpdu-filter default** 和 **stp edged-port default** 后，设备上所有的端口不会主动发送 BPDU 报文，且均不会主动与对端设备直连端口协商，所有端口均处于转发状态。这将可能导致网络成环，引起广播风暴，请用户慎用。

步骤 5 （可选）若需要对 Forward Delay 时间、Hello Time 时间以及 Max Age 时间直接进行配置，则分别进行如下操作：

- 执行命令 **stp timer forward-delay** *forward-delay*，配置交换设备的 Forward Delay 时间。

  缺省情况下，交换设备的 Forward Delay 时间是 1500 厘秒。
- 执行命令 **stp timer hello** *hello-time*，配置交换设备的 Hello Time 时间。

  缺省情况下，交换设备的 Hello Time 时间是 200 厘秒。
- 执行命令 **stp timer max-age** *max-age*，配置交换设备的 Max Age 时间。

  缺省情况下，交换设备的 Max Age 时间是 2000 厘秒。

说明

根交换设备的 Hello Time、Forward Delay 以及 Max Age 三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡。

- 2 × (Forward Delay – 1.0 second) >= Max Age
- Max Age >= 2 × (Hello Time + 1.0 second)

----结束

7.4.3 配置端口参数

影响 RSTP 拓扑快速收敛的端口参数主要有自动识别端口的链路类型是否为点到点链路、BPDU 的最大发送数目等。配置合适的端口参数，实现 RSTP 最快的拓扑收敛。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 （可选）执行命令 **stp point-to-point** { **auto** | **force-false** | **force-true** }，配置指定端口的链路类型。

缺省情况下，指定端口自动识别是否与点对点链路相连，点对点链路支持快速收敛。

- 如果当前以太网端口工作在全双工模式，则当前端口相连的链路是点到点链路，选择参数 **force-true** 实现快速收敛。
- 如果当前以太网端口工作在半双工模式，可通过执行命令 **stp point-to-point force-true** 强制链路类型为点对点链路，实现快速收敛。

步骤 4 执行命令 **stp mcheck**，执行 MCheck 操作。

在运行 RSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 RSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 RSTP 模式：

- 运行 STP 的交换设备被关机或移走
- 运行 STP 的交换设备切换为 RSTP 模式

说明

在系统视图下执行命令 **stp mcheck**，所有端口都将执行 MCheck 操作。

步骤 5 执行命令 **stp transmit-limit** *packet-number*，配置端口在每个 Hello Time 时间内 BPDU 的最大发送数目。

缺省情况下，端口在每个 Hello Time 时间内 BPDU 的最大发送数目为 147。

步骤 6 （可选）执行命令 **stp edged-port enable**，将端口配置成边缘端口。

若设备与终端相连，则相连的端口为边缘端口，可执行本操作将该端口配置成边缘端口。

缺省情况下，端口为非边缘端口。

若当前端口已经配置为边缘端口，端口仍然会发送 BPDU 报文，这可能导致 BPDU 报文发送到其他网络，引起其他网络产生震荡。此时可以通过执行命令 **stp bpdu-filter** 使边缘端口不处理、不发送 BPDU 报文，该端口即为 BPDU filter 端口。

警告

如果端口上配置命令 **stp bpdu-filter**，端口将不处理、不发送 BPDU 报文。该端口将无法成功与对端设备直连端口协商 STP 协议状态，请慎用。

步骤 7 执行命令 **quit**，退回到系统视图。

步骤 8 （可选）执行命令 **error-down auto-recovery cause** *cause-item* **interval** *interval-value*，使能处于 error-down 状态的边缘端口状态自动恢复为 Up 的功能，同时设置接口状态自动恢复为 Up 的延迟时间。

此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

----结束

后续处理

当生成树的拓扑结构发生改变时，和它建立映射关系的 VLAN 的转发路径也将发生变化。此时，交换设备的 ARP 表中与这些 VLAN 相关的表项也需要更新。根据对 ARP 表项的处理方式不同，STP/RSTP 的收敛方式分为 fast 和 normal 两种：

- fast：ARP 表将需要更新的表项直接删除。
- normal：ARP 表中需要更新的表项快速老化。

  交换设备将 ARP 表中这些表项的剩余存活时间置为 0，对这些表项进行老化处理。如果配置的 ARP 老化探测次数大于零，则 ARP 对这些表项进行老化探测。

这两种方式对 MAC 表项的处理方式相同，都是直接删除。

在系统视图下执行命令 **stp converge** { **fast** | **normal** }，可配置端口的收敛方式。

缺省情况下，端口的 STP/RSTP 收敛方式为 normal。

说明

建议选择 normal 收敛方式。若选择 fast 方式，频繁的 ARP 表项删除可能会导致主控板和接口板 CPU 占用率高达 100%，报文处理超时导致网络震荡。

7.4.4 检查配置结果

在配置 STP/RSTP 影响拓扑收敛的参数后，可以查看配置是否生效。

前提条件

已经完成影响拓扑收敛的参数配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息与统计信息。

----结束

任务示例

执行命令 **display stp**，可以查看生成树的 Hello Time 定时器时间、Max Age 定时器时间、Forward Delay 定时器时间、端口在每个 Hello Time 时间内发送 BPDU 的最大数目以及自动检测与该端口相连的链路是否是点到点链路等信息。例如：

```
<Huawei> display stp interface ethernet 2/0/1
----[CIST][Port8(Ethernet2/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=199
 Designated Bridge/Port   :32768.0010-1220-0100 / 128.8
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :2
 TC or TCN received  :2
 BPDU Sent           :10
         TCN: 0, Config: 0, RST: 10, MST: 0
 BPDU Received       :25
         TCN: 0, Config: 0, RST: 25, MST: 0
```

7.5 配置 RSTP 保护功能

华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

7.5.1 建立配置任务

在进行 RSTP 保护功能配置前，请认真了解各项配置的应用环境、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

RSTP 提供如表 7-7 所示的各种保护功能。

表 7-7 RSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 Shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的 BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

前置任务

在配置 RSTP 保护功能之前，需要完成以下任务：

- **配置 RSTP 基本功能**

  说明

  在配置 BPDU 保护功能前，需要在交换设备上配置边缘端口。

数据准备

在配置 RSTP 保护功能之前，需要准备以下数据。

序号	数据
1	启动 Root 保护功能的端口号
2	启动环路保护功能的端口号

7.5.2 配置交换设备的 BPDU 保护功能

交换设备上启动 BPDU 保护功能后，如果边缘端口收到 BPDU，交换设备将关闭这些端口，同时通知网管系统。

背景信息

边缘端口直接和用户终端相连，正常情况下，边缘端口不会收到 BPDU 报文。如果攻击者伪造 BPDU 恶意攻击交换设备，当边缘端口接收到 BPDU 报文时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。通过使能 BPDU 保护可以防止伪造 BPDU 恶意攻击。

说明

请在有边缘端口的交换设备上进行以下配置。

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 **stp bpdu-protection**，配置交换设备边缘端口的 BPDU 保护功能。

缺省情况下，交换设备的 BPDU 保护功能处于禁用状态。

----结束

后续处理

如果用户希望被 Shutdown 的边缘端口可自动恢复，可通过配置使能端口自动恢复功能，并设置延迟时间，即在系统视图下执行命令 **error-down auto-recovery cause bpdu-protection interval** *interval-value*，使能接口管理状态自动恢复为 Up 的功能，并设置接口自动恢复为 Up 的延时时间使被关闭的端口经过延时时间后能够自动恢复。对于参数 **interval** *interval-value*，取值范围是 30 ～ 86400，单位是秒，配置时需要注意两点：

- 此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

- 取值越小表示接口的管理状态自动恢复为 Up 的延迟时间越短，接口 Up/Down 状态震荡频率越高。
- 取值越大表示接口的管理状态自动恢复为 Up 的延迟时间越长，接口流量中断时间越长。

7.5.3 配置交换设备的 TC 保护功能

启用 TC 保护功能后，在单位时间内，交换设备处理 TC 类型 BPDU 报文的次数可配置，以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护交换设备的目的。

背景信息

如果攻击者伪造拓扑变化 BPDU 报文恶意攻击交换设备，交换设备短时间内会收到很多拓扑变化 BPDU 报文，频繁的删除操作会给设备造成很大的负担，也给网络的稳定带来很大隐患。

启用 TC 保护功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

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 **stp tc-protection**，使能交换设备对 TC 类型 BPDU 报文的保护功能。

缺省情况下，交换设备的 TC 保护功能处于关闭状态。

步骤 3 执行命令 **stp tc-protection threshold** *threshold*，配置交换设备在收到 TC 类型 BPDU 报文后，单位时间内，处理 TC 类型 BPDU 报文并立即刷新转发表项的阈值。

说明

单位时间的取值与 RSTP 的 Hello Time 一致，可以通过执行命令 stp timer hello *hello-time* 进行配置。

----结束

7.5.4 配置端口的 Root 保护功能

在交换设备上配置 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

背景信息

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换设备有可能会收到优先级更高的 BPDU 报文，使得合法根交换设备失去根交换设备的地位，引起网络拓扑结构的错误变动。这种不合法的拓扑变化，可能会导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。为了防止这种情况发生，可在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

说明

Root 保护是指定端口上的特性。当端口的角色是指定端口时，配置的 Root 保护功能才生效。若在其他类型的端口上配置 Root 保护功能，Root 保护功能不会生效。

请在根交换设备上进行以下配置。

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 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp root-protection**，配置交换设备的 Root 保护功能。

缺省情况下，端口的 Root 保护功能处于去使能状态。

----结束

7.5.5 配置端口的环路保护功能

环路保护功能会抑制由于链路拥塞等原因产生的环路。

背景信息

在运行 RSTP 协议的网络中，根端口和其他阻塞端口状态是依靠不断接收来自上游交换设备的 BPDU 维持。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换设备的 BPDU 时，交换设备会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。为了防止以上情况发生，可部署环路保护功能。

在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 BPDU，端口状态才恢复正常为 Forwarding 状态。

说明

由于 Alternate 端口是根端口的备份端口，如果交换设备上有 Alternate 端口，需要在根端口和 Alternate 端口上同时配置环路保护。

在交换设备的根端口和 Alternate 端口上进行以下的配置。

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*，进入根端口或 Alternate 端口的接口视图。

步骤 3 执行命令 **stp loop-protection**，配置交换设备根端口或 Alternate 端口的环路保护功能。

缺省情况下，端口的环路保护功能处于关闭状态。

----结束

7.5.6 检查配置结果

完成 RSTP 保护功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 RSTP 保护功能的所有配置。

操作步骤

- 使用命令 **display stp** [**interface** *interface-type interface-number*] [**brief**]，查看生成树的状态信息，包括是否使能交换设备的 BPDU 保护功能、其他保护类型等信息。

----结束

任务示例

执行命令 **display stp**，可以查看生成树运行的工作模式、是否使能 BPDU 保护功能以及在指定端口是否配置 Root 保护功能。例如：

```
<Huawei> display stp interface ethernet 2/0/1
----[CIST][Port8(Ethernet2/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=199
 Designated Bridge/Port   :32768.0010-1220-0100 / 128.8
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :Root
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :2
 TC or TCN received  :2
 BPDU Sent           :10
         TCN: 0, Config: 0, RST: 10, MST: 0
 BPDU Received       :25
         TCN: 0, Config: 0, RST: 25, MST: 0
```

7.6 维护 STP/RSTP

STP/RSTP 相关维护命令，包括清除 STP/RSTP 的统计数据。

7.6.1 清除 STP/RSTP 统计信息

通过 **reset** 命令可以将 STP/RSTP 统计计数置 0，便于重新统计。

背景信息

注意

清除 STP/RSTP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 STP/RSTP 的统计信息后，请在用户视图下执行以下命令。

操作步骤

步骤 1 执行命令 **reset stp** [**interface** *interface-type interface-number*] **statistics**，清除生成树的统计信息。

----结束

7.7 配置举例

配置举例结合组网需求、配置思路和数据准备来了解实际网络中 STP/RSTP 的应用场景，并提供配置文件。

7.7.1 配置 STP 功能示例

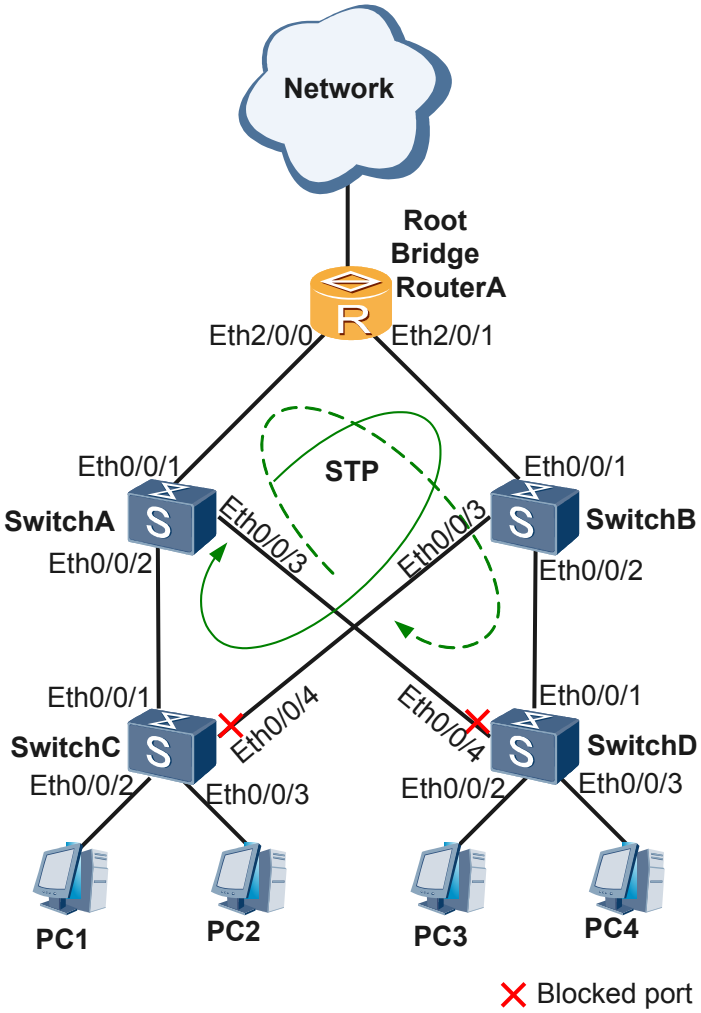
通过本示例，了解 STP 的基本功能，帮助您配置 STP 基本功能。

组网需求

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可以在网络中部署 STP 协议预防环路。当网络中存在环路，STP 通过阻塞某个端口以达到破除环路的目的。如图 7-3 所示，当前网络中存在环路，RouterA、SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 STP，通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

图 7-3 配置 STP 功能组网图



配置思路

采用以下思路配置 STP 功能：

1. 在处于环形网络中的交换设备上配置 STP 基本功能，包括：
   a. 配置环网中的设备生成树协议工作在 STP 模式。
   b. 配置根桥和备份根桥设备。
   c. 配置端口的路径开销值，实现将该端口阻塞。
   d. 使能 STP，实现破除环路，包括：
      - 设备全局使能 STP。
      - 除与终端设备相连的端口外，其他端口使能 STP。

      说明

      与 PC 机相连的端口不用参与 STP 计算，建议将其去使能 STP。

数据准备

为完成此配置举例，需要准备如下的数据：

- 各设备端口号，如图 7-3 所示
- 根桥配置为 RouterA，备份根桥配置为 SwitchA
- 需阻塞的端口的路径开销值是 200000

操作步骤

步骤 1 配置 STP 基本功能

1. 配置环网中的设备生成树协议工作在 STP 模式

   # 配置 RouterA 的 STP 工作模式。

   ```
   <Huawei> system-view
   [Huawei] sysname RouterA
   [RouterA] stp mode stp
   ```

   # 配置交换设备 SwitchA，SwitchB, SwitchC 和 SwitchD 的 STP 工作模式。

   说明

   - 本示例中交换机设备以华为 2300 系列进行配置，在实际场景中，请参考具体交换机设备的配置手册。

2. 配置根桥和备份根桥设备

   # 配置 RouterA 为根桥。

   ```
   [RouterA] stp root primary
   ```

   # 配置 SwitchA 为备份根桥。

3. 配置端口的路径开销值，实现将该端口阻塞

   说明

   - 端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为私有计算方法为例，配置被阻塞的端口的路径开销值为 200000。
   - 如实际场景中的交换机设备为非华为设备，请遵循“同一网络内所有交换设备的端口路径开销应使用相同计算方法”的原则进行配置。配置其他计算方法，请查阅 STP 路径开销列表。

   # 配置 RouterA 的端口路径开销缺省值的计算方法为华为私有计算方法。

   ```
   [RouterA] stp pathcost-standard legacy
   ```

   # 配置 SwitchA、SwitchB、SwitchC 和 SwitchD 的端口路径开销缺省值的计算方法为华为的私有计算方法。

   # 如图 7-3 所示，配置 SwitchC 和 SwitchD 的 Eth0/0/4 路径开销值为 200000。

4. 使能 STP，实现破除环路

   - 将与 PC 机相连的端口去使能 STP

     # 对交换机设备 SwitchC 和 SwitchD 上和 PC 相连的端口进行配置，执行去使能 STP。

   - 设备全局使能 STP

     # 设备 RouterA 全局使能 STP。

     ```
     [RouterA] stp enable
     ```

     # 为其他交换机设备配置全局使能 STP。

   - 除与终端设备相连的端口外，其他端口使能 STP

     # 设备 RouterA 端口 Ethernet2/0/0 和 Ethernet2/0/1 使能 STP。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] stp enable
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] stp enable
[RouterA-Ethernet2/0/1] quit
```

设备 SwitchA，SwitchB，SwitchC 和 SwitchD 除与终端设备 PC 相连的端口外，其他端口使能 STP。

步骤 2 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

在 RouterA 上执行 **display stp brief** 命令，查看端口状态，结果如下：

```
[RouterA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet2/0/0              DESI  FORWARDING      NONE
   0    Ethernet2/0/1              DESI  FORWARDING      NONE
```

将 RouterA 配置为根桥后，与 SwitchA 和 SwitchB 相连的端口 Ethernet2/0/0 和 Ethernet2/0/1 在生成树计算中被选举为指定端口。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 stp mode stp
 stp instance 0 root primary
 stp pathcost-standard legacy
#
interface Ethernet2/0/0
#
interface Ethernet2/0/1
#
return
```

- SwitchA 的配置文件

```
#
 stp mode stp
 stp instance 0 root secondary
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
return
```

- SwitchB 的配置文件

```
#
 stp mode stp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
```

```
#
return
```

- SwitchC 的配置文件

```
#
 stp mode stp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
stp disable
#
interface Ethernet0/0/3
stp disable
#
interface Ethernet0/0/4
stp instance 0 cost 200000
#
return
```

- SwitchD 的配置文件

```
#
 stp mode stp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
stp disable
#
interface Ethernet0/0/3
stp disable
#
interface Ethernet0/0/4
stp instance 0 cost 200000
#
return
```

7.7.2 配置 RSTP 功能示例

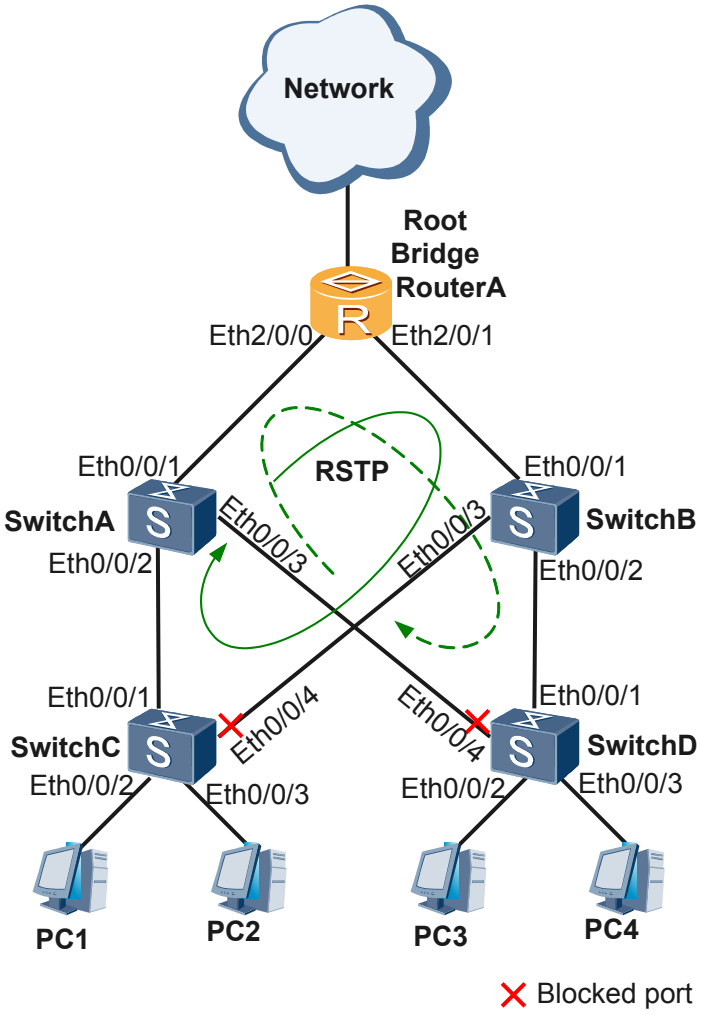
通过本示例，了解 RSTP 的基本功能，帮助您配置 RSTP 基本功能。

组网需求

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可以在网络中部署 RSTP 协议预防环路。当网络中存在环路，RSTP 通过阻塞某个端口以达到破除环路的目的。如图 7-4 所示，当前网络中存在环路，RouterA、SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 RSTP，通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

图 7-4 配置 RSTP 功能组网图



配置思路

采用以下思路配置 RSTP 功能：

1. 在处于环形网络中的交换设备上配置 RSTP 基本功能，包括：
   a. 配置环网中的设备生成树协议工作在 RSTP 模式。
   b. 配置根桥和备份根桥设备。
   c. 配置端口的路径开销值，实现将该端口阻塞。
   d. 使能 RSTP，实现破除环路，包括：
      - 设备全局使能 RSTP。
      - 除与终端设备相连的端口外，其他端口使能 RSTP。

      说明

      与 PC 机相连的端口不用参与 RSTP 计算，建议将其去使能 RSTP。
2. 配置保护功能，实现对设备或链路的保护。例如：在根桥设备的指定端口配置根保护功能。

数据准备

为完成此配置举例，需要准备如下的数据：

- 各设备端口号，如图 7-4 所示
- 根桥配置为 RouterA，备份根桥配置为 SwitchA
- 需阻塞的端口的路径开销值是 200000

操作步骤

步骤 1 配置 RSTP 基本功能

1. 配置环网中的设备生成树协议工作在 RSTP 模式

   # 配置 RouterA 的 RSTP 工作模式。

   ```
   <Huawei> system-view
   [Huawei] sysname RouterA
   [RouterA] stp mode rstp
   ```

   # 配置交换设备 SwitchA，SwitchB, SwitchC 和 SwitchD 的 RSTP 工作模式。

   说明

   - 本示例中交换机设备以华为 2300 系列进行配置，在实际场景中，请参考具体交换机设备的配置手册。

2. 配置根桥和备份根桥设备

   # 配置 RouterA 为根桥。

   ```
   [RouterA] stp root primary
   ```

   # 配置 SwitchA 为备份根桥。请参阅具体交换机设备的配置手册，配置设备为备份根桥。

3. 配置端口的路径开销值，实现将该端口阻塞

   说明

   - 端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为私有计算方法为例，配置将被阻塞的端口的路径开销值为 200000。
   - 如实际场景中的交换机设备为非华为设备，请遵循“同一网络内所有交换设备的端口路径开销应使用相同计算方法”的原则进行配置。配置其他计算方法，请查阅 STP 路径开销列表。

   # 配置 RouterA 的端口路径开销缺省值的计算方法为华为私有计算方法。

   ```
   [RouterA] stp pathcost-standard legacy
   ```

   # 配置 SwitchA、SwitchB、SwitchC 和 SwitchD 的端口路径开销缺省值的计算方法为华为的私有计算方法。

   # 如图 7-4 所示，配置 SwitchC 和 SwitchD 的 Eth0/0/4 路径开销值为 200000。

4. 使能 RSTP，实现破除环路

   - 将与 PC 机相连的端口去使能 RSTP

     # 对交换机设备 SwitchC 和 SwitchD 上和 PC 相连的端口进行配置，执行去使能 RSTP。

   - 设备全局使能 RSTP

     # 设备 RouterA 全局使能 RSTP。

     ```
     [RouterA] stp enable
     ```

     # 为其他交换机设备配置全局使能 RSTP。

   - 除与终端设备相连的端口外，其他端口使能 RSTP

设备 RouterA 端口 Ethernet2/0/0 和 Ethernet2/0/1 使能 RSTP。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] stp enable
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] stp enable
[RouterA-Ethernet2/0/1] quit
```

设备 SwitchA，SwitchB，SwitchC 和 SwitchD 除与终端设备相连的端口外，其他端口使能 RSTP。

步骤 2 配置保护功能

在根桥 RouterA 的端口 Eth2/0/0 和 Eth2/0/1 上启动根保护。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] stp root-protection
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] stp root-protection
[RouterA-Ethernet2/0/1] quit
```

步骤 3 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

在 RouterA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[RouterA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet2/0/0               DESI  FORWARDING      ROOT
   0    Ethernet2/0/1               DESI  FORWARDING      ROOT
```

将 RouterA 配置为根桥后，与 SwitchA 和 SwitchB 相连的端口 Ethernet2/0/0 和 Ethernet2/0/1 在生成树计算中被选举为指定端口。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 stp mode rstp
 stp instance 0 root primary
 stp pathcost-standard legacy

#
interface Ethernet2/0/0
 stp root-protection
#
interface Ethernet2/0/1
 stp root-protection
#
return
```

- SwitchA 的配置文件

```
#
 stp mode rstp
 stp instance 0 root secondary
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
```

```
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
return
```

- SwitchB 的配置文件

```
#
 stp mode rstp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
return
```

- SwitchC 的配置文件

```
#
 stp mode rstp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
stp disable
#
interface Ethernet0/0/3
stp disable
#
interface Ethernet0/0/4
stp instance 0 cost 200000
#
return
```

- SwitchD 的配置文件

```
#
 stp mode rstp
 stp pathcost-standard legacy
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
stp disable
#
interface Ethernet0/0/3
stp disable
#
interface Ethernet0/0/4
stp instance 0 cost 200000
#
return
```

8 MSTP 配置

关于本章

MSTP（Multiple Spanning Tree Protocol，多生成树协议）将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

8.1 MSTP 概述
MSTP 功能兼容 STP 和 RSTP 功能，同时弥补 STP 和 RSTP 的缺陷。MSTP 既可以快速收敛，又能为冗余链路提供更好的负载分担。

8.2 AR2200-S 支持的 MSTP 特性
配置 MSTP 时，您将接触到基本功能、拓扑收敛、保护功能以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

8.3 配置 MSTP 基本功能
在 STP/RSTP 基本功能实现基础上，MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立，实现用户流量与业务流量的分离，达到网络负载均衡的目的。

8.4 配置 MSTP 影响拓扑收敛的参数
MSTP 兼容实现了 RSTP 的快速收敛机制。在以下影响 MSTP 拓扑收敛的参数中选择合适的参数，配置后实现最快的拓扑收敛速度。

8.5 配置 MSTP 保护功能
华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

8.6 配置 MSTP 支持和其他制造商设备互通的参数
为了实现与其他制造商设备的互通，需要在华为公司运行 MSTP 的设备上配置一些参数，以确保通信畅通。这些参数包括收发 BPDU 报文的协议格式、MSTP 报文的协议格式和使能摘要监听功能。

8.7 维护 MSTP
MSTP 相关维护命令，包括清除 MSTP 的统计数据。

8.8 配置举例

配置举例结合组网需求、配置思路和数据准备来了解实际网络中 MSTP 的应用场景，并提供配置文件。

8.1 MSTP 概述

MSTP 功能兼容 STP 和 RSTP 功能，同时弥补 STP 和 RSTP 的缺陷。MSTP 既可以快速收敛，又能为冗余链路提供更好的负载分担。

MSTP 背景

STP 和 RSTP 是用于局域网中预防和消除环路的协议，运行 STP/RSTP 协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成处理能力下降。

STP 和 RSTP 存在同一个缺陷：由于局域网内所有的 VLAN 共享一棵生成树，因此无法在 VLAN 间实现数据流量的负载均衡，链路被阻塞后将不承载任何流量，造成带宽浪费，还有可能造成部分 VLAN 的报文无法转发。

为了弥补 STP 和 RSTP 的缺陷，IEEE 于 2002 年发布的 802.1S 标准定义了 MSTP。MSTP 兼容 STP 和 RSTP，既可以快速收敛，又提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

STP/RSTP/MSTP 三种生成树协议的特点与应用场景比较如**表 8-1** 所示。

表 8-1 三种生成树协议的比较

生成树协议	特点	应用场景	注意事项
STP	形成一棵无环路的树：解决广播风暴并实现冗余备份。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。	**说明** ● 若当前交换设备只支持 STP，建议选择使用 STP，详见 **STP/RSTP 配置**。 ● 若当前交换设备既支持 STP 又支持 RSTP，建议使用 RSTP，详见 **STP/RSTP 配置**。 ● 若当前交换设备既支持 STP/RSTP 又支持 MSTP，建议选择使用 MSTP。
RSTP	● 形成一棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。		
MSTP	● 形成一棵或多棵无环路的树：解决广播风暴并实现冗余备份。 ● 对拓扑是否已经收敛制定反馈机制，实现了快速收敛。 ● 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。	

MSTP 概述

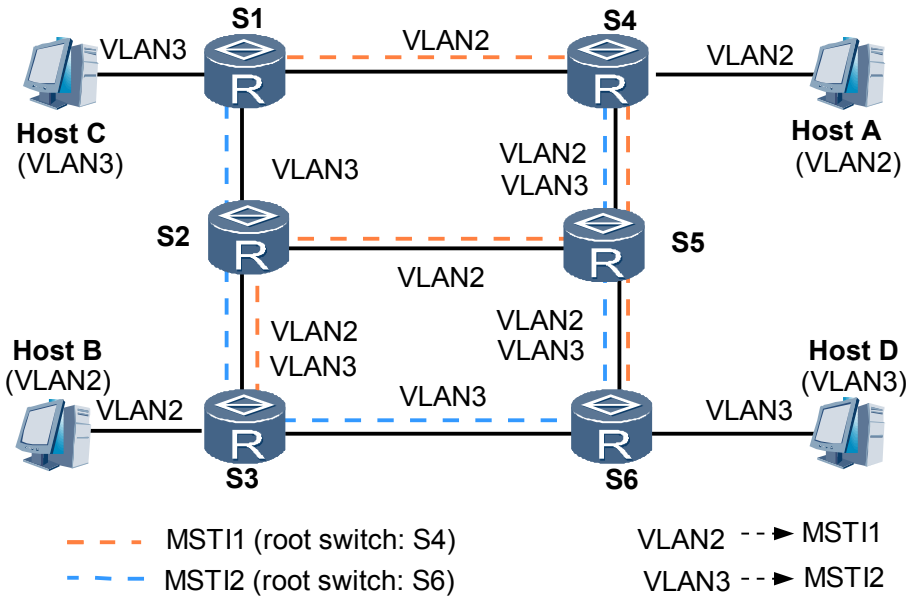
在一个复杂的网络环境中，难免会出现环路；并且，由于冗余备份的需要，网络设计者都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样，偶然或必然中都会存在环路。

环路会产生广播风暴，最终导致整个网络资源被耗尽，网络瘫痪不可用。环路还会引起MAC 地址表震荡导致 MAC 地址表项被破坏。

MSTP 兼容 STP 和 RSTP，通过多实例能实现对业务流量和用户流量的隔离，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

现将 MSTP 应用于图 8-1 中的局域网，应用后生成 MSTI 如图 8-1 所示。

图 8-1 MST 域内的多棵生成树示意图



- MSTI1 以 S4 为根交换设备，转发 VLAN2 的报文。
- MSTI2 以 S6 为根交换设备，转发 VLAN3 的报文。

这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负载分担。

MSTP 基本概念

- MST 域（MST Region）

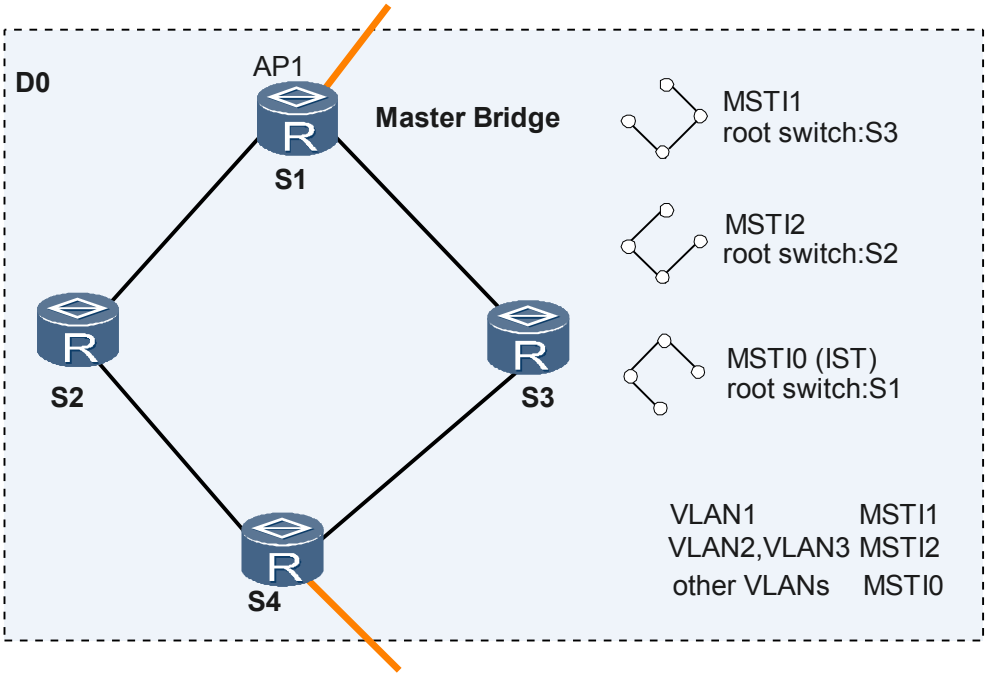
  MST 域是多生成树域（Multiple Spanning Tree Region），由交换网络中的多台交换设备以及它们之间的网段所构成。这些设备具有下列特点：

  - 都启动了 MSTP。
  - 具有相同的域名。
  - 具有相同的 VLAN 到生成树实例映射配置。
  - 具有相同的 MSTP 修订级别配置。

一个局域网可以存在多个 MST 域，各 MST 域之间在物理上直接或间接相连。用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

如图 8-2 所示的 MST Region D0 中由交换设备 S1、S2、S3 和 S4 构成，域中有 3 个 MSTI。

图 8-2 MST Region 的基本概念示意图



- VLAN 映射表

  VLAN 映射表是 MST 域的属性，它描述了 VLAN 和 MSTI 之间的映射关系。

  如图 8-2 所示，MST 域 D0 的 VLAN 映射表是：

  - VLAN1 映射到 MSTI1
  - VLAN2 和 VLAN3 映射到 MSTI2
  - 其余 VLAN 映射到 MSTI0

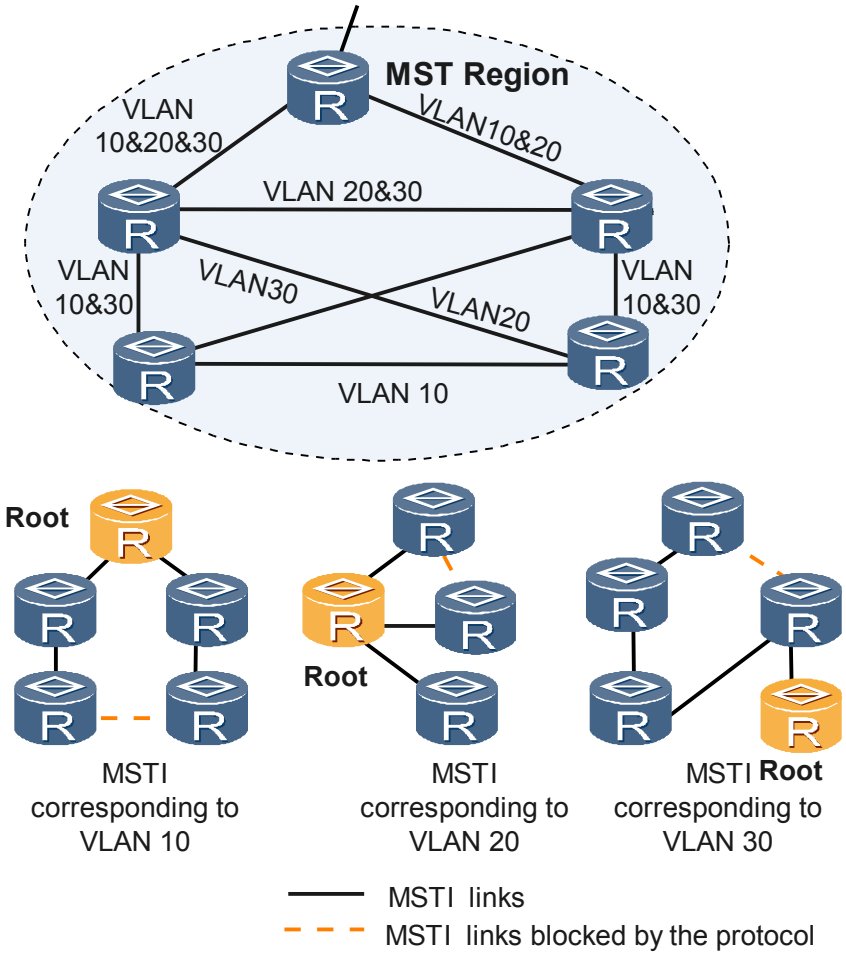
- 域根

  域根（Regional Root）分为 IST（Internal Spanning Tree）域根和 MSTI 域根。

  IST 域根如图 8-4 所示，在 B0、C0 和 D0 中，IST 生成树中距离总根（CIST Root）最近的交换设备是 IST 域根。

  一个 MST 域内可以生成多棵生成树，每棵生成树都称为一个 MSTI。MSTI 域根是每个多生成树实例的树根。如图 8-3 所示，域中不同的 MSTI 有各自的域根。

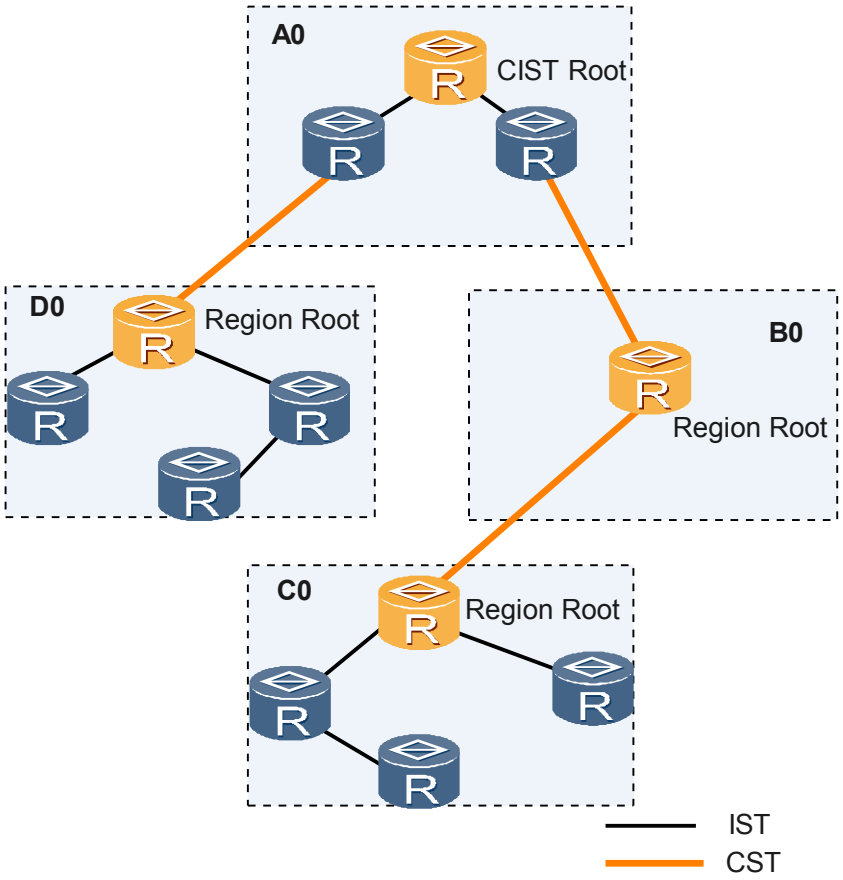
图 8-3 MSTI 的基本概念示意图



MSTI 之间彼此独立，MSTI 可以与一个或者多个 VLAN 对应。但一个 VLAN 只能与一个 MSTI 对应。

- 总根

图 8-4 MSTP 网络基本概念示意图



如图 8-4 所示，总根是 CIST（Common and Internal Spanning Tree）的根桥。总根是区域 A0 中的某台设备。

- CST

  公共生成树 CST（Common Spanning Tree）是连接交换网络内所有 MST 域的一棵生成树。

  如果把每个 MST 域看作是一个节点，CST 就是这些节点通过 STP 或 RSTP 协议计算生成的一棵生成树。

  如图 8-4 所示，较粗的线条连接各个域构成 CST。

- IST

  内部生成树 IST（Internal Spanning Tree）是各 MST 域内的一棵生成树。

  IST 是一个特殊的 MSTI，MSTI 的 ID 为 0，通常称为 MSTI0。

  IST 是 CIST 在 MST 域中的一个片段。

  如图 8-4 所示，较细的线条在域中连接该域的所有交换设备构成 IST。

- CIST

  公共和内部生成树 CIST 是通过 STP 或 RSTP 协议计算生成的，连接一个交换网络内所有交换设备的单生成树。

  如图 8-4 所示，所有 MST 域的 IST 加上 CST 就构成一棵完整的生成树，即 CIST。

- SST

构成单生成树 SST（Single Spanning Tree）有两种情况：

- 运行 STP 或 RSTP 的交换设备只能属于一个生成树。
- MST 域中只有一个交换设备，这个交换设备构成单生成树。

如图 8-4 所示，B0 中的交换设备就是一棵单生成树。

- 端口角色

MSTP 在 RSTP 的基础上新增了 2 种端口，MSTP 的端口角色共有 7 种：根端口、指定端口、Alternate 端口、Backup 端口、边缘端口、Master 端口和域边缘端口。

根端口、指定端口、Alternate 端口、Backup 端口和边缘端口的作用同 RSTP 协议中定义，MSTP 中定义的所有端口角色如表 8-2 所示。

说明

除边缘端口外，其他端口角色都参与 MSTP 的计算过程。

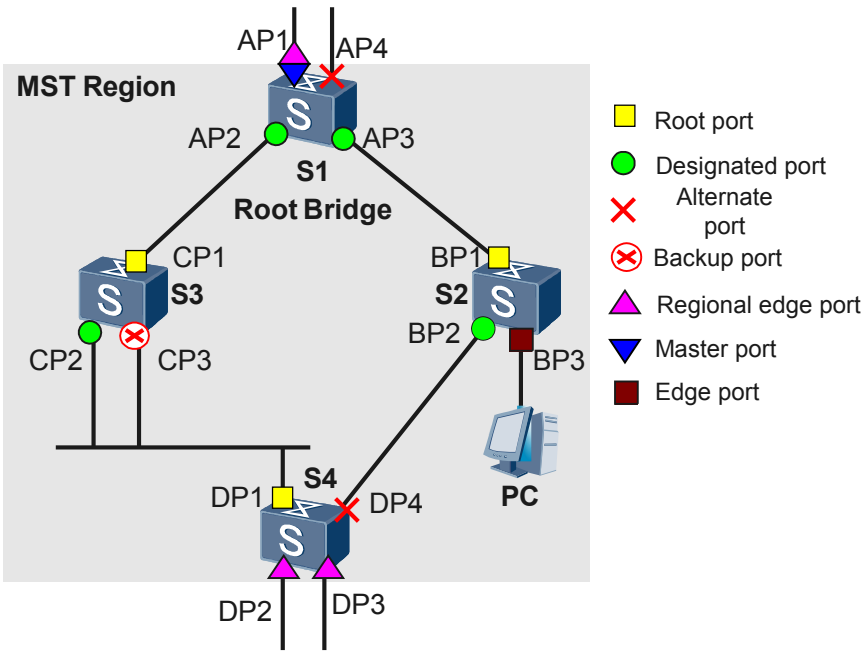
同一端口在不同的生成树实例中可以担任不同的角色。

表 8-2 端口角色

端口角色	说明
根端口	在非根桥上，离根桥最近的端口是本交换设备的根端口。根交换设备没有根端口。 根端口负责向树根方向转发数据。 如图 8-5 所示，S1 为根桥，CP1 为 S3 的根端口，BP1 为 S2 的根端口，DP1 为 S4 的根端口。
指定端口	对一台交换设备而言，它的指定端口是向下游交换设备转发 BPDU 报文的端口。 如图 8-5 所示，AP2 和 AP3 为 S1 的指定端口，BP2 为 S2 的指定端口，CP2 为 S3 的指定端口。
Alternate 端口	● 从配置 BPDU 报文发送角度来看，Alternate 端口就是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。 ● 从用户流量角度来看，Alternate 端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口。 如图 8-5 所示，BP2 和 AP4 为 Alternate 端口。
Backup 端口	● 从配置 BPDU 报文发送角度来看，Backup 端口就是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。 ● 从用户流量角度来看，Backup 端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。 如图 8-5 所示，CP3 为 Backup 端口。
Master 端口	Master 端口是 MST 域和总根相连的所有路径中最短路径上的端口。 Master 端口是域中的报文去往总根的必经之路。 Master 端口是特殊域边缘端口，Master 端口在 IST/CIST 上的角色是 Root Port，在其它各实例上的角色都是 Master 端口。 如图 8-5 所示，交换设备 S1、S2、S3、S4 和它们之间的链路构成一个 MST 域，S1 交换设备的端口 AP1 在域内的所有端口中到总根的路径开销最小，所以 AP1 为 Master 端口。

端口角色	说明
域边缘端口	域边缘端口是指位于 MST 域的边缘并连接其它 MST 域或 SST 的端口。 进行 MSTP 计算时，域边缘端口在 MSTI 上的角色和 CIST 实例的角色保持一致。即如果边缘端口在 CIST 实例上的角色是 Master 端口（连接域到总根的端口），则它在域内所有 MSTI 上的角色也是 Master 端口。 如图 8-5 所示，MST 域内的 AP1、DP2 和 DP3 都和其它域直接相连，它们都是本 MST 域的边缘端口。 如图 8-5，AP1 是域边缘端口，它在 CIST 上的角色是 Master 端口，则 AP1 在 MST 域内所有生成树实例上的角色都是 Master 端口。
边缘端口	如果指定端口位于整个域的边缘，不再与任何交换设备连接，这种端口叫做边缘端口。 边缘端口一般与用户终端设备直接连接。 如图 8-5 所示，BP3 为边缘端口。

图 8-5 端口角色示意图



- 端口状态

  MSTP 定义的端口状态与 RSTP 协议中定义相同，如表 8-3 所示。

表 8-3 端口状态

端口状态	说明
Forwarding	在这种状态下，端口既转发用户流量又接收/发送 BPDU 报文。
Learning	这是一种过渡状态。在 Learning 下，交换设备会根据收到的用户流量，构建 MAC 地址表，但不转发用户流量，所以叫做学习状态。 Learning 状态的端口接收/发送 BPDU 报文，不转发用户流量。
Discarding	Discarding 状态的端口只接收 BPDU 报文。

端口状态和端口角色是没有必然联系的，表 8-4 显示了各种端口角色能够具有的端口状态。

表 8-4 端口角色

端口状态	根端口/Master 端口	指定端口	域边缘端口	Alternate 端口	Backup 端口
Forwarding	Yes	Yes	Yes	No	No
Learning	Yes	Yes	Yes	No	No
Discarding	Yes	Yes	Yes	Yes	Yes

Yes：表示端口支持的状态。

No：表示端口不支持的状态。

8.2 AR2200-S 支持的 MSTP 特性

配置 MSTP 时，您将接触到基本功能、拓扑收敛、保护功能以及与其他制造商设备互通等概念，理解这些概念后，您可以更快速准确地完成配置任务。

MSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。同时，MSTP 引入多实例，通过将不同 VLAN 映射到不同实例中，实现不同 VLAN 的流量负载分担。MSTP 的基本配置思路如下：

1. 在环形网络中，划分域，在域中配置不同的实例。
2. 为各个实例选出其中的一个交换设备作为根桥（Root bridge）。
3. 在各个实例中，计算出其他交换设备到根桥的最短路径，为每个非根交换设备选举一个根端口。

4. 在各个实例中，通过端口 ID 为每个连接选举出一个指定端口。

根据不同的组网情况，可能还会涉及到 Backup 端口、Master 端口等端口角色的确认，详见 **MSTP 端口描述**。

为了满足特殊场合的应用和扩展功能，MSTP 还支持如下功能：

- MSTP 通过 Proposal/Agreement 机制等实现快速收敛。
- MSTP 提供如**表 8-5** 所示的保护功能。
- 为了实现与其他制造商设备的互通，需要在华为公司运行 MSTP 的设备上配置合适的参数，以确保通信畅通。

表 8-5 MSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的 BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

8.3 配置 MSTP 基本功能

在 STP/RSTP 基本功能实现基础上，MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立，实现用户流量与业务流量的分离，达到网络负载均衡的目的。

通过给交换设备配置 MSTP 的工作模式、配置域并激活后，启动 MSTP，MSTP 便开始进行生成树计算，将网络修剪成树状，破除环路。但是，若网络规划者需要人为干预生成树计算的结果，可以采取以下方式：

- 配置交换设备在指定生成树实例中的优先级数值：数值越小，交换设备在该生成树实例中的优先级越高，成为根桥的可能性越大；数值越大，交换设备在该生成树实例中的优先级越低，成为根桥的可能性越小。
- 配置端口在指定生成树实例中的路径开销数值：在同一种计算方法下，数值越小，端口在该生成树实例中到根桥的路径开销越小，成为根端口的可能性就越大；数值越大，端口在该生成树实例中到根桥的路径开销越大，成为根端口的可能性越小。
- 配置端口在指定生成树实例中的优先级数值：数值越小，端口在该生成树实例中成为指定端口的可能性就越大；数值越大，端口在该生成树实例中成为指定端口的可能性越小。

8.3.1 建立配置任务

配置 MSTP 基本功能前，请认真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，可以帮助您快速、准确地完成配置任务。

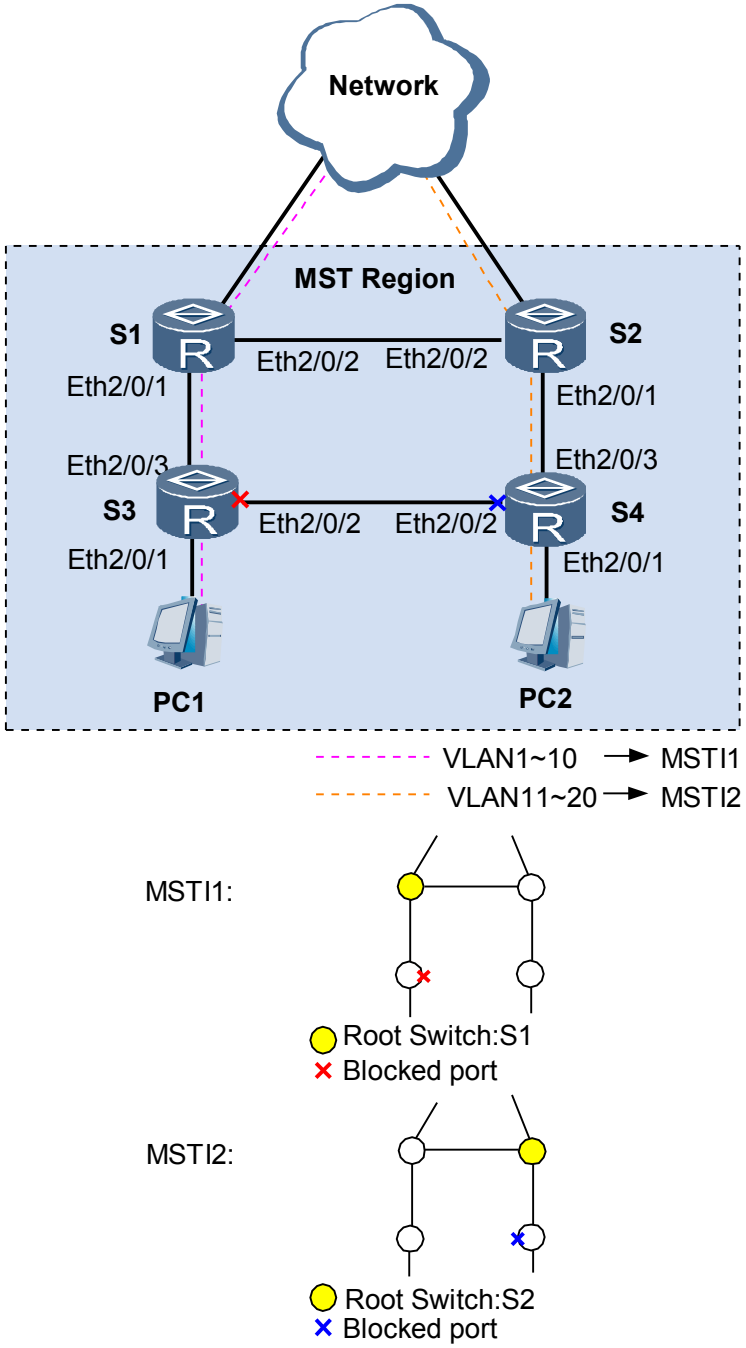
应用环境

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。

网络规划者规划好网络后，可在网络中部署 MSTP 协议预防环路。当网络中存在环路，MSTP 通过阻塞某个或某些端口以达到破除环路的目的，同时通过配置多实例实现多个 VLAN 的流量负载分担。

如图 8-6 所示，S1、S2、S3 和 S4 都支持 MSTP。现通过配置实例 MSTI1 和 MSTI2，然后设置各实例的根桥设备和阻塞口，完成对 VlAN1 ～ 10 和 VLAN11 ～ 20 流量的负载分担。

图 8-6 配置 MSTP 的基本功能组网图



说明

如果当前设备支持 MSTP，建议使用 MSTP。

前置任务

在配置 MSTP 基本功能前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up

数据准备

在配置 MSTP 基本功能之前，需要准备以下数据。

序号	数据
1	MSTP 工作模式
2	交换设备所属 MST 域的域名、多生成树实例和 VLAN 的映射关系、MST 域的 MSTP 修订级别
3	（可选）生成树实例 ID
4	（可选）交换设备在指定多生成树实例中的优先级
5	（可选）端口在指定多生成树实例中的优先级
6	（可选）端口在指定生成树实例中的路径开销

8.3.2 配置 MSTP 工作模式

在配置 MSTP 基本功能前需要选择 MSTP 工作模式，MSTP 兼容 STP/RSTP。

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 **stp mode mstp**，配置交换设备的 MSTP 工作模式。

缺省情况下，交换设备的工作模式为 MSTP。

因为 STP 和 MSTP 不能互相识别报文，而 MSTP 和 RSTP 可以互相识别报文，所以若工作在 MSTP 工作模式下，交换设备会设置所有和运行 STP 的交换设备直接相连的端口工作在 STP 模式下，其他端口工作在 MSTP 模式下，实现运行不同生成树协议的设备之间的互通。

----结束

8.3.3 配置 MST 域并激活

通过 MSTP 把一个交换网络划分成多个 MST 域。在完成配置 MST 域名、配置多生成树实例与 VLAN 的映射关系和配置 MST 域的 MSTP 修订级别后激活 MST 域完成对 MST 域的配置。

背景信息

MST 域即多生成树域，是由交换网络中的多台交换设备以及它们之间的网段所构成。这些交换设备启动 MSTP 后，具有相同域名、相同 VLAN 到生成树映射配置和相同 MSTP 修订级别配置，并且物理上直接相连。一个交换网络可以存在多个 MST 域，用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

注意

只要两台交换设备的以下配置相同，这两台交换设备就属于同一个 MST 域。

- MST 域的域名。
- 多生成树实例和 VLAN 的映射关系。
- MST 域的修订级别。

请在需要加入 MST 域的交换设备上进行以下配置。

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 **stp region-configuration**，进入 MST 域视图。

步骤 3 执行命令 **region-name** *name*，配置 MST 域的域名。

缺省情况下，MST 域的域名等于交换设备主控板上管理网口的 MAC 地址。

步骤 4 选择执行以下两个步骤中的其中一个，配置多生成树实例与 VLAN 的映射关系。

- 执行命令 **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10>，配置多生成树实例和 VLAN 的映射关系。
- 执行命令 **vlan-mapping modulo** *modulo*，配置多生成树实例和 VLAN 按照缺省算法自动分配映射关系。

缺省情况下，MST 域内所有的 VLAN 都映射到生成树实例 0。

说明

- 命令 **vlan-mapping modulo** *modulo* 实现的自动分配机制很难刚好满足实际的多生成树实例与 VLAN 的映射关系，建议使用命令 **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10>配置多生成树实例和 VLAN 的映射关系。
- **vlan-mapping modulo** *modulo* 是指 VLAN ID 减 1 后除以 modulo 值的余数再加 1，即(VLAN ID-1)%modulo+1。通过此算法来分配到对应的实例中，即余数加 1 为几就将此 VLAN 分配到实例几中。

步骤 5（可选）执行命令 **revision-level** *level*，配置 MST 域的 MSTP 修订级别。

缺省情况下，MSTP 域的 MSTP 修订级别为 0。

当设备所在域的 MSTP 修订级别不为 0，则需要执行本操作。

说明

由于 MST 域相关参数（特别是 VLAN 映射表）的变化会引起 MSTP 重新计算生成树，从而引起网络拓扑振荡。因此，在完成配置 MST 域名、配置多生成树实例与 VLAN 的映射关系和配置 MST 域的 MSTP 修订级别后，建议在 MST 域视图下执行命令 check region-configuration 确定未生效的域参数配置是否正确。在确认域参数无误后，执行命令 active region-configuration 激活新的 MST 域配置。

步骤 6 执行命令 **active region-configuration**，激活 MST 域的配置，使域名、VLAN 映射表和 MSTP 修订级别生效。

如果不执行本操作，以上配置的域名、VLAN 映射表和 MSTP 修订级别无法生效。

如果在启动 MSTP 特性后又修改了交换设备的 MST 域相关参数，可以通过执行命令 active region-configuration 激活 MST 域，使修改后的参数生效。

----结束

8.3.4 （可选）配置交换设备在指定生成树实例中的优先级

交换设备在指定生成树实例中的优先级值越小，则交换设备的优先级越高，成为该生成树实例根桥的可能性越大。

背景信息

在一个生成树实例中，有且仅有一个根桥，它是该生成树实例的逻辑中心。在进行根桥的选择时，一般会希望选择性能高、网络层次高的交换设备作为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此需要配置优先级以保证该设备成为根桥。

对于生成树实例中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

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 **stp** [**instance** *instance-id*] **priority** *priority*，配置交换设备在指定生成树实例中的优先级。

缺省情况下，交换设备的优先级取值是 32768。

如果不指定 **instance**，则配置交换设备在实例 0 中的优先级。

说明

- 如果为当前设备配置系统优先级目的是配置当前设备为根桥设备，则可以直接选择执行命令 **stp** [instance *instance-id*] root primary，配置后该设备优先级数值自动为 0。
- 执行命令 **stp** [instance *instance-id*] root secondary 可以配置当前交换设备为备份根桥设备，配置后该设备优先级数值自动为 4096。

  同一台交换设备不能既作为根桥又作为备用根桥。
- 如果已经通过执行命令 **stp** [instance *instance-id*] root primary 或 **stp** [instance *instance-id*] root secondary 指定当前设备为根桥设备或备份根桥设备，需要改变当前设备的优先级则需要执行 undo stp [instance *instance-id*] root 去使能根交换设备或者备份根交换设备功能，然后执行命令 **stp** [instance *instance-id*] priority *priority* 配置新的优先级数值。

----结束

8.3.5 （可选）配置端口在指定生成树实例中的路径开销

端口路径开销会影响指定生成树实例中根端口的选择，在该实例中，某台设备所有端口到达根桥路径开销最小者，就是根端口。

背景信息

路径开销是一个端口量，是 MSTP 协议用于选择链路的参考值。

端口的路径开销是生成树计算的重要依据，在不同生成树实例中为同一端口配置不同的路径开销值，可以使不同 VLAN 的流量沿不同的物理链路转发，实现按 VLAN 的负载分担功能。

以华为的私有计算方法为例，不同速率的端口路径开销的缺省值不同，具体参见下表。

表 8-6 端口所对应的链路速率与端口路径开销值对应表

链路速率	推荐值	推荐取值范围	值域
10Mbit/s	2000	200-20000	1-200000
100Mbit/s	200	20-2000	1-200000
1Gbit/s	20	2-200	1-200000
10Gbit/s	2	2-20	1-200000
10Gbit/s 以上	1	1-2	1-200000

存在环路的网络环境中，对于链路速率值相对较小的端口，建议将其路径开销值配置相对较大，以使其在生成树算法中被选举成为阻塞端口，阻塞其所在链路。

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 **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }，配置端口路径开销计算方法。

缺省情况下，路径开销缺省值的计算方法为 IEEE 802.1t 标准方法。

同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 4 执行命令 **stp instance** *instance-id* **cost** *cost*，设置当前端口在指定生成树实例中的路径开销值。

- 使用华为的私有计算方法时参数 *cost* 取值范围是 1 ～ 200000。
- 使用 IEEE 802.1d 标准方法时取值范围是 1 ～ 65535。
- 使用 IEEE 802.1t 标准方法时取值范围是 1 ～ 2000,000,00。

----结束

8.3.6 （可选）配置端口在指定生成树实例中的优先级

交换设备的端口优先级值越小，被指定为指定端口的机率越大；端口优先级值越大，则该端口被阻塞的机率越大。

背景信息

在参与 MSTP 生成树计算时，对于处在生成树实例中的交换设备端口，其优先级的高低会影响到是否被选举为指定端口。

在根路径开销及发送交换设备的 BID 相同的情况下，如果希望将生成树实例中的某交换设备的端口阻塞从而破除环路，则可将其端口优先级值设置比缺省值大，使得在选举过程中成为被阻塞的端口。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp instance** *instance-id* **port priority** *priority*，配置端口在指定生成树实例中的优先级。

缺省情况下，端口的优先级数值为 128。

优先级数值的取值范围是 0 ～ 240，步长为 16，即取值为 0、16、32 等。

----结束

8.3.7 启用 MSTP

当交换设备配置 MSTP 基本功能后，交换设备 MSTP 使能，MSTP 功能才能生效。

背景信息

在环形网络中一旦启用 MSTP，MSTP 便立即开始进行生成树计算。而且，诸如交换设备的优先级、端口优先级等参数都会影响到生成树的计算，在计算过程中这些参数的变动可能会导致网络震荡。为了保证生成树计算过程快速而且稳定，必须在对交换设备及其端口进行必要的基本配置以后才能启用 MSTP。

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 **stp enable**，使能交换设备的 MSTP 功能。

缺省情况下，设备使能 MSTP 功能。

----结束

8.3.8 检查配置结果

完成 MSTP 基本功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 基本功能的配置。

操作步骤

- 使用命令 **display stp** [**instance** *instance-id*][**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。
- 执行命令 **display stp region-configuration**，查看已经生效的 MST 域的配置信息。
- 执行命令 **display stp region-configuration digest** ，查看已经生效的 MST 域配置的摘要。

----结束

任务示例

执行命令 **display stp**，可以查看生成树的工作模式、交换设备优先级、路径开销缺省值的计算方法和根端口路径开销值等信息。例如：

```
<Huawei> display stp instance 0 interface ethernet 2/0/1
-------[CIST Global Info][ Mode MSTP ]-------
CIST Bridge         :32768.00e0-fc0e-a421
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc0e-a421 / 0
CIST RegRoot/IRPC   :32768.00e0-fc0e-a421 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :8
STP Converge Mode   :Normal
Time since last TC  :0 days 23h:9m:30s
----[Port3(Ethernet2/0/1)] [ FORWARDING ]----
 Port Protocol       :Enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=100 / Active=100
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
```

执行命令 **display stp region-configuration**，可以查看已经生效的 MST 域的域名、MST 域的修订级别和 MST 域的生成树实例和 VLAN 之间的映射关系。例如：

```
<Huawei> display stp region-configuration
Oper Configuration
   Format selector :0
   Region name     :huawei
   Revision level  :0
   Instance   Vlans Mapped
      0       21 to 4094
      1        1 to 10
      2       11 to 20
```

执行命令 **display stp region-configuration digest**，可以查看已经生效的 MST 域的域名、MST 域的修订级别和 MST 域的配置摘要。例如：

```
<Huawei> display stp region-configuration digest
Oper Configuration
   Format selector :0
   Region name     :huawei
   Revision level  :0
   Digest          :0x5F762D9A46311EFFB7A488A3267FCA9F
```

8.4 配置 MSTP 影响拓扑收敛的参数

MSTP 兼容实现了 RSTP 的快速收敛机制。在以下影响 MSTP 拓扑收敛的参数中选择合适的参数，配置后实现最快的拓扑收敛速度。

8.4.1 建立配置任务

配置 MSTP 影响拓扑收敛的参数前，请认真了解各项配置的应用环境、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

在运行 MSTP 的网络环境中，快速收敛机制的实现需要配置影响快速收敛的参数，配置合适的参数后才能实现最佳快速收敛效果。

说明

因为本配置任务中所包含的命令缺省情况下也能完成 MSTP 的快速收敛，所以本配置任务所包含的所有配置过程，以及配置过程中包含的所有配置步骤都是可选的，可根据实际需要选择配置其中的部分内容。

前置任务

在配置 MSTP 影响拓扑收敛的参数之前，需要完成以下任务：

- 配置 MSTP 基本功能

数据准备

在配置影响拓扑收敛的参数之前，需要准备以下数据。

序号	数据
1	网络直径
2	Hello Time 时间、Forward Delay 时间、Max Age 时间、超时时间（3 x hello time x time factor）
3	MST 域的最大跳数
4	端口的链路类型
5	端口是否使用普通的快速迁移机制
6	端口是否需要迁移回 RSTP 模式
7	BPDU 的最大发送数目值
8	端口是否需要设置为边缘端口
9	如果端口为边缘端口，是否需要配置其在 Shutdown 后自动恢复功能
10	端口是否需要清除生成树的统计信息
11	如果端口为边缘端口，是否需要配置端口为 BPDU filter 端口

8.4.2 配置系统参数

影响 MSTP 拓扑收敛的系统参数有网络直径、Hello Time 定时器与倍数参数形成的超时时间（3 x hello time x time factor）等，配置合适的系统参数，实现最快的拓扑收敛。

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 **stp bridge-diameter** *diameter*，配置网络直径。

缺省情况下，网络直径为 7。

- 快速生成树是在整个交换网络应用单生成树实例，不能解决由于网络规模增大带来的性能降低问题，网络直径不要超过 7。
- 建议通过执行命令 **stp bridge-diameter** *diameter* 配置网络直径去配置 Forward Delay 时间、Hello Time 时间以及 Max Age 时间，因为交换设备会自动根据网络直径计算出 Forward Delay 时间、Hello Time 时间以及 Max Age 时间的较优值。

步骤 3 执行命令 **stp timer-factor** *factor*，配置未收到上游的 BPDU 就重新开始生成树计算的超时时间。

缺省情况下，交换设备未收到上游的 BPDU 就重新开始生成树计算的超时时间是 Hello Timer 的 9 倍。

步骤 4 （可选）若当前设备是网络边缘设备，可选择执行如下命令中的一个或多个：

- 执行命令 **stp edged-port default**，配置当前设备上所有端口为边缘端口。

  缺省情况下，端口为非边缘端口。

  在网络边缘设备上配置该命令，使端口不再参与生成树计算，从而帮助加快网络拓扑的收敛时间以及加强网络的稳定性。
- 执行命令 **stp bpdu-filter default**，配置当前设备上所有端口为 BPDU filter 端口。

  缺省情况下，端口为非 BPDU filter 端口。

  在网络边缘设备上配置该命令，使边缘端口不处理、不发送 BPDU 报文，该端口即为 BPDU filter 端口。

警告

在系统视图下同时执行命令 **stp bpdu-filter default** 和 **stp edged-port default** 后，设备上所有的端口不会主动发送 BPDU 报文，且均不会主动与对端设备直连端口协商，所有端口均处于转发状态。这将可能导致网络成环，引起广播风暴，请用户慎用。

步骤 5 （可选）若需要对 Forward Delay 时间、Hello Time 时间以及 Max Age 时间直接进行配置，则分别进行如下操作：

- 执行命令 **stp timer forward-delay** *forward-delay*，配置交换设备的 Forward Delay 时间。

  缺省情况下，交换设备的 Forward Delay 时间是 1500 厘秒。
- 执行命令 **stp timer hello** *hello-time*，配置交换设备的 Hello Time 时间。

  缺省情况下，交换设备的 Hello Time 时间是 200 厘秒。
- 执行命令 **stp timer max-age** *max-age*，配置交换设备的 Max Age 时间。

  缺省情况下，交换设备的 Max Age 时间是 2000 厘秒。

说明

根交换设备的 Hello Time、Forward Delay 以及 Max Age 三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡。

- 2 × (Forward Delay – 1.0 second) >= Max Age
- Max Age >= 2 × (Hello Time + 1.0 second)

步骤 6 执行命令 **stp max-hops** *hop*，配置 MST 域的最大跳数。

缺省情况下，MST 域的最大跳数为 20。

步骤 7 执行命令 **stp mcheck**，执行 MCheck 操作。

在运行 MSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 MSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 MSTP 模式：

- 运行 STP 的交换设备被关机或移走
- 运行 STP 的交换设备切换为 MSTP 模式

说明

在系统视图下执行命令 **stp mcheck**，所有端口都将执行 MCheck 操作。

----结束

8.4.3 配置端口参数

影响 MSTP 拓扑收敛的端口参数有端口的链路类型、BPDU 的最大发送数目等。配置合适的端口参数，实现最快的拓扑收敛。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 （可选）执行命令 **stp point-to-point** { **auto** | **force-false** | **force-true** }，配置指定端口的链路类型。

缺省情况下，指定端口自动识别是否与点对点链路相连，点对点链路支持快速收敛。

- 如果当前以太网端口工作在全双工模式，则当前端口相连的链路是点到点链路，选择参数 **force-true** 实现快速收敛。
- 如果当前以太网端口工作在半双工模式，可通过执行命令 **stp point-to-point force-true** 强制链路类型为点对点链路，实现快速收敛。

步骤 4 执行命令 **stp mcheck**，执行 MCheck 操作。

在运行 MSTP 的交换设备上，如果某个端口和另一台运行 STP 的交换设备连接，则该端口会自动迁移到 STP 工作模式。

以下情况端口无法自动迁回 MSTP 模式，需要在端口上执行 MCheck 操作，将端口手动迁移到 MSTP 模式：

- 运行 STP 的交换设备被关机或移走

- 运行 STP 的交换设备切换为 MSTP 模式

步骤 5 执行命令 **stp transmit-limit** *packet-number*，配置端口在每个 Hello Time 时间内 BPDU 的最大发送数目。

缺省情况下，端口在每个 Hello Time 时间内 BPDU 的最大发送数目为 147。

步骤 6 （可选）执行命令 **stp edged-port enable**，将端口配置成边缘端口。

若设备与终端相连，则相连的端口为边缘端口，可执行本操作将该端口配置成边缘端口。

缺省情况下，端口为非边缘端口。

若当前端口已经配置为边缘端口，端口仍然会发送 BPDU 报文，这可能导致 BPDU 报文发送到其他网络，引起其他网络产生震荡。此时可以通过执行命令 **stp bpdu-filter** 使边缘端口不处理、不发送 BPDU 报文，该端口即为 BPDU filter 端口。

警告

如果端口上配置命令 **stp bpdu-filter**，端口将不处理、不发送 BPDU 报文。该端口将无法成功与对端设备直连端口协商 STP 协议状态，请慎用。

步骤 7 执行命令 **quit**，退回到系统视图。

步骤 8 （可选）执行命令 **error-down auto-recovery cause** *cause-item* **interval** *interval-value*，使能处于 error-down 状态的边缘端口状态自动恢复为 Up 的功能，同时设置接口状态自动恢复为 Up 的延迟时间。

此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

----结束

后续处理

当生成树的拓扑结构发生改变时，和它建立映射关系的 VLAN 的转发路径也将发生变化。此时，交换设备的 ARP 表中与这些 VLAN 相关的表项也需要更新。根据对 ARP 表项的处理方式不同，MSTP 的收敛方式分为 fast 和 normal 两种：

- fast：ARP 表将需要更新的表项直接删除。
- normal：ARP 表中需要更新的表项快速老化。

  交换设备将 ARP 表中这些表项的剩余存活时间置为 0，对这些表项进行老化处理。如果配置的 ARP 老化探测次数大于零，则 ARP 对这些表项进行老化探测。

  这两种方式对 MAC 表项的处理方式相同，都是直接删除。

在系统视图下执行命令 **stp converge** { **fast** | **normal** }，可配置端口的收敛方式。

缺省情况下，端口的 MSTP 收敛方式为 normal。

说明

建议选择 normal 收敛方式。若选择 fast 方式，频繁的 ARP 表项删除可能会导致主控板和接口板 CPU 占用率高达 100%，报文处理超时导致网络震荡。

8.4.4 检查配置结果

完成影响 MSTP 拓扑快速收敛的参数配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成对设备影响 MSTP 拓扑快速收敛的所有参数配置。

操作步骤

- 执行命令 **display stp** [**instance** *instance-id*] [**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。

----结束

任务示例

执行命令 **display stp**，可以查看生成树的 Hello Time、Forward Delay 以及 Max Age 三个时间参数，MST 域的最大跳数，端口在每个 Hello Time 时间内发送 BPDU 的最大数目，自动检测与该端口相连的链路是否是点到点链路等信息。例如：

```
<Huawei> display stp instance 0 interface ethernet 2/0/1
-------[CIST Global Info][ Mode MSTP ]-------
CIST Bridge         :32768.00e0-fc0e-a421
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc0e-a421 / 0
CIST RegRoot/IRPC   :32768.00e0-fc0e-a421 / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :8
STP Converge Mode   :Normal
Time since last TC  :0 days 23h:9m:30s
----[Port3(Ethernet2/0/1)] [ FORWARDING ]----
 Port Protocol       :Enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=100 / Active=100
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 BPDU Sent           :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
```

8.5 配置 MSTP 保护功能

华为公司的数据通信设备支持以下保护功能，用户可根据实际环境任选其中一个或多个保护功能配置。

8.5.1 建立配置任务

配置 MSTP 保护功能前，请认真了解此特性的应用环境、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

MSTP 提供如表 8-7 所示的各种保护功能。

表 8-7 MSTP 保护功能

保护功能	场景	配置影响
BPDU 保护	边缘端口在收到 BPDU 以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击交换设备，就会引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 shutdown，但是边缘端口属性不变，同时通知网管系统。
TC 保护	交换设备在接收到拓扑变化报文后，会执行 MAC 地址表项和 ARP 表项的删除操作，如果频繁操作则会对 CPU 的冲击很大。	启用防 TC-BPDU 报文攻击功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。
Root 保护	由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的 BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。
环路保护	当出现链路拥塞或者单向链路故障，根端口和 Alternate 端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate 端口老化，将迁移到 Forwarding 状态，这样会产生环路。	在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 RST BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

说明

正常启动后，设备默认存在 ID 为 0 的 MSTP 进程，系统视图和接口视图中的 MSTP 相关配置都属于此进程。

前置任务

在配置交换设备的 MSTP 保护功能之前，需要完成以下任务：

- 配置 MSTP 基本功能

  说明

  在配置 BPDU 保护功能前，需要在交换设备上配置边缘端口。

数据准备

在配置交换设备的 MSTP 保护功能之前，需要准备以下数据。

序号	数据
1	启动 Root 保护功能的端口号
2	启动环路保护功能的端口号

8.5.2 配置交换设备的 BPDU 保护功能

交换设备上启动 BPDU 保护功能后，如果边缘端口收到 BPDU，交换设备将关闭这些端口，同时通知网管系统。

背景信息

边缘端口直接和用户终端相连，正常情况下，边缘端口不会收到 BPDU 报文。如果攻击者伪造 BPDU 恶意攻击交换设备，当边缘端口接收到 BPDU 报文时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。通过使能 BPDU 保护可以防止伪造 BPDU 恶意攻击。

说明

请在有边缘端口的交换设备上进行以下配置。

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 **stp bpdu-protection**，配置交换设备的 BPDU 保护功能。

缺省情况下，交换设备的 BPDU 保护功能处于去使能状态。

----结束

后续处理

如果用户希望被 Shutdown 的边缘端口可自动恢复，可通过配置使能端口自动恢复功能，并设置延迟时间，即在系统视图下执行命令 **error-down auto-recovery cause bpdu-protection interval** *interval-value*，使能接口管理状态自动恢复为 Up 的功能，并设置接口自动恢复为 Up 的延时时间使被关闭的端口经过延时时间后能够自动恢复。对于参数 **interval** *interval-value*，取值范围是 30 ～ 86400，单位是秒，配置时需要注意两点：

- 此命令的恢复时间没有缺省值，当用户配置该命令时，必须指定恢复延迟时间。

- 取值越小表示接口的管理状态自动恢复为 Up 的延迟时间越短，接口 Up/Down 状态震荡频率越高。
- 取值越大表示接口的管理状态自动恢复为 Up 的延迟时间越长，接口流量中断时间越长。

8.5.3 配置交换设备的 TC 保护功能

启用 TC 保护功能后，在单位时间内，MSTP 进程处理 TC 类型 BPDU 报文的次数可配置，以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护交换设备的目的。

背景信息

如果攻击者伪造拓扑变化 BPDU 报文恶意攻击交换设备，交换设备短时间内会收到很多拓扑变化 BPDU 报文，频繁的删除操作会给设备造成很大的负担，也给网络的稳定带来很大隐患。

启用 TC 保护功能后，在单位时间内，交换设备处理拓扑变化报文的次数可配置。如果在单位时间内，交换设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

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 **stp tc-protection**，使能 MSTP 进程对 TC 类型 BPDU 报文的保护功能。

缺省情况下，交换设备的 TC 保护功能处于去使能状态。

步骤 3 执行命令 **stp tc-protection threshold** *threshold*，配置 MSTP 进程在收到 TC 类型 BPDU 报文后，单位时间内，处理 TC 类型 BPDU 报文并立即刷新转发表项的阈值。

说明

单位时间的取值与 MSTP 的 Hello Time 一致，可以通过执行命令 **stp timer hello** *hello-time* 进行配置。

----结束

8.5.4 配置端口的 Root 保护功能

在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

背景信息

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换设备有可能会收到优先级更高的 BPDU 报文，使得合法根交换设备失去根交换设备的地位，引起网络拓扑结构的错误变动。这种不合法的拓扑变化，可能会导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。为了防止这种情况发生，可在交换设备上部署 Root 保护功能，通过维持指定端口的角色来保护根交换设备的地位。

说明

Root 保护是指定端口上的特性。当端口在所有实例中都是指定端口时，配置的 Root 保护功能才能起到保护根交换设备的目的。若在其他类型的端口上配置 Root 保护功能，Root 保护功能不会生效。

在 MST 域中的根交换设备上进行以下配置。

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 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp root-protection**，配置交换设备的 Root 保护功能。

缺省情况下，端口的 Root 保护功能处于关闭状态。

----结束

8.5.5 配置端口的环路保护功能

环路保护功能会抑制由于链路拥塞等原因产生的环路。

背景信息

在运行 MSTP 协议的网络中，根端口和其他阻塞端口状态是依靠不断接收来自上游交换设备的 BPDU 维持。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换设备的 BPDU 时，交换设备会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。为了防止以上情况发生，可部署环路保护功能。

在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 BPDU 时，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 BPDU，端口状态才恢复正常为 Forwarding 状态。

说明

由于 Alternate 端口是根端口的备份端口，如果交换设备上有 Alternate 端口，需要在根端口和 Alternate 端口上同时配置环路保护。

在 MST 域中交换设备的根端口和 Alternate 端口上进行以下的配置。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp loop-protection**，配置交换设备根端口的环路保护功能。

缺省情况下，端口的环路保护功能处于关闭状态。

----结束

8.5.6 检查配置结果

完成 MSTP 保护功能配置后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 保护功能的所有配置。

操作步骤

- 执行命令 **display stp [instance** *instance-id* **] [interface** { *interface-type interface-number* } **] [brief]**，查看生成树的状态信息与统计信息。

----结束

任务示例

执行命令 **display stp**，可以查看是否使能交换设备的 BPDU 保护功能，保护类型等信息。例如：

```
<Huawei> display stp instance 0 interface ethernet 2/0/1
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge          :32768.00e0-fc0e-a421
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :32768.00e0-fc0e-a421 / 0
CIST RegRoot/IRPC    :32768.00e0-fc0e-a421 / 0
CIST RootPortId      :0.0
BPDU-Protection      :Enabled
TC or TCN received   :8
STP Converge Mode    :Fast
Time since last TC   :0 days 23h:9m:30s
----[Port3(Ethernet2/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=100 / Active=100
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :Root
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 BPDU Sent           :43
          TCN: 0, Config: 0, RST: 0, MST: 43
 BPDU Received       :3
          TCN: 0, Config: 0, RST: 0, MST: 3
```

8.6 配置 MSTP 支持和其他制造商设备互通的参数

为了实现与其他制造商设备的互通，需要在华为公司运行 MSTP 的设备上配置一些参数，以确保通信畅通。这些参数包括收发 BPDU 报文的协议格式、MSTP 报文的协议格式和使能摘要监听功能。

8.6.1 建立配置任务

配置 MSTP 支持和其他制造商设备互通的参数前，请认真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，可以帮助您快速、准确地完成配置任务。

应用环境

在运行 MSTP 的网络中，因为协议格式不一致、BPDU 报文密钥不一致等原因会导致设备无法正常互通，在这种情况下，需要配置 MSTP 支持和其他制造商设备互通的参数来实现互通。

前置任务

在配置 MSTP 支持和其他制造商设备互通的参数之前，需要完成以下任务：

- 配置 MSTP 基本功能

数据准备

在配置 MSTP 支持和其他制造商设备互通的参数之前，需要准备以下数据。

序号	数据
1	收发 MSTP 协议报文的格式

8.6.2 配置端口 Proposal/Agreement 机制的迁移方式

为了实现华为公司的数据通信与其他制造商设备互通，需要根据其他制造商设备的 P/A 机制选择端口的快速迁移方式。

背景信息

Proposal/Agreement 机制，目前交换设备的端口支持以下两种方式：

- 增强方式：当前接口在计算同步标志位时计算根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口。
  - 上游设备继续发送 Agreement 报文，下游设备接收到后，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。
- 普通方式：当前接口在计算同步标志位时忽略根端口。
  - 上游设备发送 Proposal 报文，请求进行快速迁移，下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口，根端口转为 Forwarding 状态。
  - 下游设备回应 Agreement 报文，上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。

华为数据通信设备和其他制造商的设备进行互通时，需要根据其他制造商设备的 Proposal/Agreement 机制，选择接口使用增强的快速迁移机制还是普通的快速迁移机制。

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 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp no-agreement-check**，配置端口使用普通的快速迁移方式。

缺省情况下，端口使用增强的快速迁移机制。

----结束

8.6.3 配置端口收发 MSTP 协议的报文格式

MSTP 协议报文收发模式包括协议格式自适应、标准 IEEE 802.1s 报文和私有协议报文三种模式，默认情况下为自适应模式。

背景信息

MSTP 协议报文存在两种格式，一种为 dot1s，即 IEEE802.1s 规定的报文格式，另一种为 legacy，是一种私有报文格式。配置 MSTP 协议报文格式自适应的功能，即根据收到的 MSTP 协议报文格式自动切换接口支持的 MSTP 协议报文格式，使报文格式与对端匹配。

操作步骤

步骤 1 在 MST 域中的交换设备上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp compliance** { **auto** | **dot1s** | **legacy** }，配置端口协议报文格式。

缺省情况下，MSTP 报文收发格式为 auto 模式。

说明

如果直连的接口上一端配置 dot1s，而另一端配置 legacy，是不能协商成功的。

----结束

8.6.4 使能摘要监听功能

当华为设备与其他制造商的设备互连时，在域名、修订级别、VLAN mapping 表全都一致的情况下，由于双方 BPDU 报文密钥不一致，会导致两台设备不能正常互通，在这种情况下，需要在交换设备上使能摘要监听功能。

背景信息

在 MST 域中的交换设备上进行以下配置，实现华为设备的 BPDU 报文密钥与其他制造商设备的 BPDU 报文密钥一致。

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*，进入参与生成树协议计算的以太接口视图。

步骤 3 执行命令 **stp config-digest-snoop**，使能端口上配置摘要监听的功能。

----结束

8.6.5 检查配置结果

完成 MSTP 支持和其他制造商设备互通的配置参数后，通过检查配置结果可以查看是否生效。

前提条件

已经完成 MSTP 支持和其他制造商设备互通的所有参数配置。

操作步骤

- 执行命令 **display stp** [**instance** *instance-id*] [**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。

----结束

任务示例

执行命令 **display stp**，可以查看生成树运行的工作模式、交换设备收发 BPDU 报文的协议格式、交换设备收发 MSTP 协议报文的格式以及端口是否配置摘要监听功能等。例如：

```
<Huawei> display stp instance 0 interface ethernet 2/0/1
-------[CIST Global Info][ Mode MSTP ]-------
CIST Bridge           :32768.00e0-fc0e-a421
Bridge Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :32768.00e0-fc0e-a421 / 0
CIST RegRoot/IRPC     :32768.00e0-fc0e-a421 / 0
CIST RootPortId       :0.0
BPDU-Protection       :Disabled
TC or TCN received    :8
STP Converge Mode     :Normal
Time since last TC    :0 days 23h:9m:30s
----[Port3(Ethernet2/0/1)] [ FORWARDING ]----
 Port Protocol         :Enabled
 Port Role             :CIST Designated Port
 Port Priority         :128
 Port Cost(Dot1T )     :Config=100 / Active=100
 Designated Bridge/Port     :32768.00e0-fc0e-a421 / 128.1229
 Port Edged            :Config=disabled / Active=disabled
 Point-to-point        :Config=auto / Active=true
 Transit Limit         :3 packets/hello-time
 Protection Type       :None
 Config-digest-snoop:snooped=false
 Port Stp Mode         :MSTP
 Port Protocol Type    :Config=auto / Active= dot1s
 PortTimes             :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 BPDU Sent             :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 BPDU Received         :0
          TCN: 0, Config: 0, RST: 0, MST: 0
```

在参与生成树协议计算的以太接口视图下执行命令 **display this**，可以查看配置的端口快速迁移方式。例如：

```
[Huawei-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 portswitch
 undo shutdown
```

```
 stp no-agreement-check
return
```

8.7 维护 MSTP

MSTP 相关维护命令，包括清除 MSTP 的统计数据。

8.7.1 清除 MSTP 统计信息

通过 reset 命令可以将 MSTP 统计计数置 0，便于重新统计。

背景信息

注意

清除 MSTP 的统计信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除 MSTP 的统计信息后，请在用户视图下执行以下命令。

操作步骤

步骤 1 执行命令 **reset stp** [**interface** *interface-type interface-number*] **statistics**，清除生成树的统计信息。

----结束

8.8 配置举例

配置举例结合组网需求、配置思路和数据准备来了解实际网络中 MSTP 的应用场景，并提供配置文件。

8.8.1 配置 MSTP 功能示例

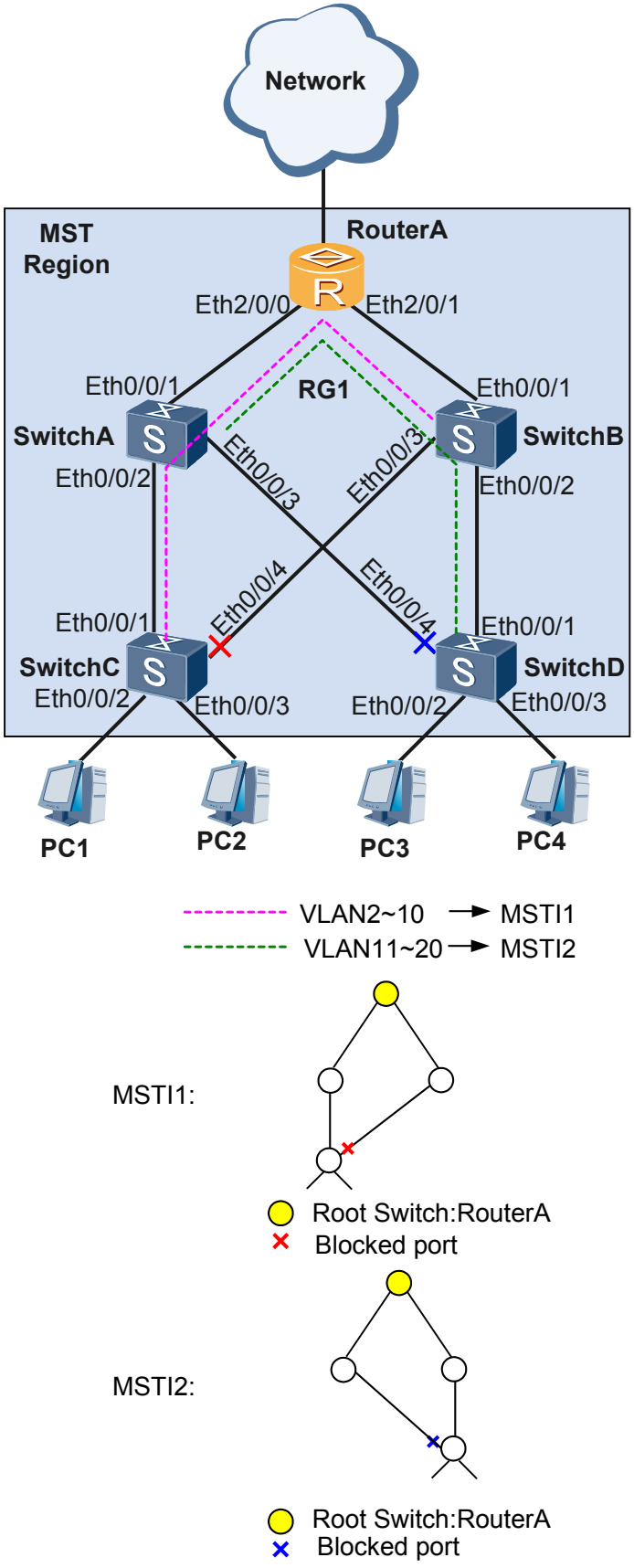
通过本示例，了解 MSTP 的基本功能，帮助您配置 MSTP 基本功能。

组网需求

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 桥表项被破坏。网络规划者规划好网络后，可以在网络中部署 MSTP 协议预防环路。MSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。

如图 8-7 所示，为实现 VLAN2 ～ 10 和 VLAN11 ～ 20 的流量负载分担，MSTP 引入了多实例。MSTP 可设置 VLAN 映射表，把 VLAN 和生成树实例联系起来。图 8-7 中 RouterA、SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 MSTP。

图 8-7 配置 MSTP 功能组网图



配置思路

采用以下思路配置 MSTP 功能：

1. 在处于环形网络中的交换设备上配置 MSTP 基本功能，包括：
   a. 配置环网中的设备生成树协议工作在 MSTP 模式。
   b. 配置 MST 域并创建多实例，实现流量的负载分担。
   c. 在 MST 域内，配置各实例的根桥与备份根桥。
   d. 配置各实例中某端口的路径开销值，实现将该端口阻塞。
   e. 使能 MSTP，实现破除环路，包括：
      - 设备全局使能 MSTP。
      - 除与终端设备相连的端口外，其他端口使能 MSTP。

      说明

      与 PC 机相连的端口不用参与 MSTP 计算，建议将其去使能 MSTP。
2. 配置保护功能，实现对设备或链路的保护。例如：在各实例的根桥设备指定端口配置根保护功能。
3. 配置设备的二层转发功能。

数据准备

为完成此配置举例，需要准备如下的数据：

- 域名为 RG1
- 实例为 MSTI1 和 MSTI2
- 各设备端口号如图 8-7 所示，实例 MSTI1 的根桥为 RouterA，备份根桥为 SwitchA；实例 MSTI2 的根桥为 RouterA，备份根桥为 SwitchB
- 图 8-7 所示实例 MSTI1 和实例 MSTI2 被阻塞的端口路径开销值为 200000
- VLAN 号是 2 ～ 20
- PC1 和 PC2 所属 VLAN 为 10，PC3 和 PC4 所属 VLAN 为 20
- SwitchC 端口加入 VLAN2 ～ 10，SwitchD 端口加入 VLAN11 ～ 20，其他交换设备端口加入 VLAN2 ～ 20

操作步骤

步骤 1 配置 MSTP 基本功能

1. 配置环网中的设备生成树协议工作在 MSTP 模式

   # 配置 RouterA 的 MSTP 工作模式，MSTP 为设备缺省工作模式。

   ```
   <Huawei> system-view
   [Huawei] sysname RouterA
   [RouterA] stp mode mstp
   ```

   # 配置交换设备 SwitchA，SwitchB, SwitchC 和 SwitchD 的 MSTP 工作模式。

   说明

   - 本示例中交换机设备以华为 2300 系列进行配置，在实际场景中，请参考具体交换机设备的配置手册。

2. 配置环网中的设备到域名为 RG1 的域内，创建实例 MSTI1 映射 VLAN2 ～ 10，创建实例 MSTI2 映射 VLAN11 ～ 20。

   # 配置 RouterA 的 MST 域。

   ```
   [RouterA] stp region-configuration
   [RouterA] region-name RG1
   [RouterA] instance 1 vlan 2 to 10
   [RouterA] instance 2 vlan 11 to 20
   [RouterA] active region-configuration
   [RouterA] quit
   ```

   # 配置交换设备 SwitchA、SwitchB、SwitchC 和 SwitchD 的 MST 域。域名为 RG1，创建实例 MSTI1 映射 VLAN2 ～ 10，创建实例 MSTI2 映射 VLAN11 ～ 20。

3. 在域 RG1 内，配置 MSTI1 与 MSTI2 的根桥与备份根桥

   # 配置 MSTI1 的根桥为 RouterA。

   ```
   [RouterA] stp instance 1 root primary
   ```

   # 配置 MSTI1 的备份根桥为 SwitchA。

   # 配置 MSTI2 的根桥为 RouterA。

   ```
   [RouterA] stp instance 2 root primary
   ```

   # 配置 MSTI2 的备份根桥为 SwitchB。

4. 配置实例 MSTI1 和 MSTI2 中需被阻塞的端口的路径开销值大于缺省值，实现将该端口阻塞

   说明

   - 端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为私有计算方法为例，配置将被阻塞的端口的路径开销值为 200000。
   - 如实际场景中的交换机设备为非华为设备，请遵循“同一网络内所有交换设备的端口路径开销应使用相同计算方法”的原则进行配置。配置其他计算方法，请查阅 STP 路径开销列表。

   # 配置 RouterA 的端口路径开销缺省值的计算方法为华为私有计算方法。

   ```
   [RouterA] stp pathcost-standard legacy
   ```

   # 配置 SwitchA、SwitchB、SwitchC 和 SwitchD 的端口路径开销缺省值的计算方法为华为的私有计算方法。

   # 如**图 8-7**，配置 SwitchC 的端口 Eth0/0/4 在实例 1 中的路径开销值为 200000。

   # 如**图 8-7**，配置 SwitchD 的端口 Eth0/0/4 在实例 2 中的路径开销值为 200000。

5. 使能 MSTP，实现破除环路

   - 将与 PC 终端相连的端口去使能 MSTP

     # 如**图 8-7**，配置交换机设备 SwitchC 的端口，Eth0/0/2 和 Eth0/0/3，去使能 MSTP。

     # 如**图 8-7**，配置交换机设备 SwitchD 的端口，Eth0/0/2 和 Eth0/0/3，去使能 MSTP。

   - 设备全局使能 MSTP

     # 设备 RouterA 全局使能 MSTP。

     ```
     [RouterA] stp enable
     ```

     # 为交换机设备 SwitchA，SwitchB，SwitchC 和 SwitchD 全局使能 MSTP。

   - 除与 PC 终端相连的端口外，端口使能 MSTP

     # 设备 RouterA 端口 Eth2/0/0 和 Eth2/0/1 使能 MSTP。

     ```
     [RouterA] interface ethernet 2/0/0
     [RouterA-Ethernet2/0/0] stp enable
     [RouterA-Ethernet2/0/0] quit
     ```

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] stp enable
[RouterA-Ethernet2/0/1] quit
```

如图 8-7，交换机设备 SwitchA，SwitchB，SwitchC 和 SwitchD 除与 PC 终端相连的端口外，其他端口使能 MSTP。

步骤 2 配置保护功能

在根桥 RouterA 的端口 Eth2/0/0 和 Eth2/0/1 上启动根保护。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] stp root-protection
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] stp root-protection
[RouterA-Ethernet2/0/1] quit
```

步骤 3 配置处于环网中的设备的二层转发功能

- 在交换设备 RouterA、SwitchA、SwitchB、SwitchC 和 SwitchD 上创建 VLAN

  # 在 RouterA 上创建 VLAN2 ～ 20。

  ```
  [RouterA] vlan batch 2 to 20
  ```

  # 在交换机 SwitchA 和 SwitchB 上创建 VLAN2 ～ 20。

  # 在交换机 SwitchC 上创建 VLAN2 ～ 10。

  # 在交换机 SwitchD 上创建 VLAN11 ～ 20。

- 将交换设备上接入环路中的端口加入 VLAN

  # 将 RouterA 的端口 Eth2/0/0 和 Eth2/0/1 加入 VLAN2 ～ 20。

  ```
  [RouterA] interface ethernet 2/0/0
  [RouterA-Ethernet2/0/0] port link-type trunk
  [RouterA-Ethernet2/0/0] port trunk allow-pass vlan 2 to 20
  [RouterA-Ethernet2/0/0] quit
  [RouterA] interface ethernet 2/0/1
  [RouterA-Ethernet2/0/1] port link-type trunk
  [RouterA-Ethernet2/0/1] port trunk allow-pass vlan 2 to 20
  [RouterA-Ethernet2/0/1] quit
  ```

  # 将 SwitchA 的端口 Eth0/0/1、Eth0/0/2 和 Eth0/0/3 加入 VLAN2 ～ 20。

  # 将 SwitchB 的端口 Eth0/0/1、Eth0/0/2 和 Eth0/0/3 加入 VLAN2 ～ 20。

  # 将 SwitchC 的端口 Eth0/0/1、Eth0/0/2、Eth0/0/3、Eth0/0/4 加入 VLAN2 ～ 10。

  # 将 SwitchD 的端口 Eth0/0/1、Eth0/0/2、Eth0/0/3、Eth0/0/4 加入 VLAN11 ～ 20。

步骤 4 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

在 RouterA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[RouterA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet2/0/0               DESI  FORWARDING      NONE
   0    Ethernet2/0/1               DESI  FORWARDING      NONE
   1    Ethernet2/0/0               DESI  FORWARDING      ROOT
   1    Ethernet2/0/1               DESI  FORWARDING      ROOT
   2    Ethernet2/0/0               DESI  FORWARDING      ROOT
   2    Ethernet2/0/1               DESI  FORWARDING      ROOT
```

在 MSTI1 中，由于 RouterA 是根桥，RouterA 的端口 Eth2/0/0 和 Eth2/0/1 成为指定端口。在 MSTI2 中，RouterA 同样是根桥，RouterA 的端口 Eth2/0/0 和 Eth2/0/1 是指定端口。

在 SwitchA 查看端口状态和端口的保护类型。在 MSTI1 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/2 和端口 Eth0/0/3 成为指定端口。在 MSTI2 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/2 和端口 Eth0/0/3 成为指定端口。

在 SwitchB 查看端口状态和端口的保护类型。在 MSTI1 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/2 和端口 Eth0/0/3 成为指定端口。在 MSTI2 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/2 和端口 Eth0/0/3 成为指定端口。

在 SwitchC 查看端口状态和端口的保护类型。在 MSTI1 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/4 被阻塞。在 MSTI2 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/4 成为指定端口。

在 SwitchD 查看端口状态和端口的保护类型。在 MSTI1 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/4 成为指定端口。在 MSTI2 中，端口 Eth0/0/1 成为根端口，端口 Eth0/0/4 被阻塞。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 2 to 20
#
 stp instance 1 root primary
 stp instance 2 root primary
 stp pathcost-standard legacy
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 10
  instance 2 vlan 11 to 20
  active region-
configuration
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
 stp root-protection
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
 stp root-protection
#
return
```

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2 to 20
#
 stp instance 1 root secondary
 stp pathcost-standard legacy
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 10
  instance 2 vlan 11 to 20
  active region-
configuration
#
```

```
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface Ethernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface Ethernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2 to 20
#
 stp instance 2 root secondary
 stp pathcost-standard legacy
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 10
  instance 2 vlan 11 to 20
  active region-
configuration
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface Ethernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface Ethernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 2 to 10
#
 stp pathcost-standard legacy
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 10
  instance 2 vlan 11 to 20
  active region-
configuration
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 10
#
interface Ethernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 10
 stp disable
#
interface Ethernet0/0/3
 port link-type trunk
```

```
 port trunk allow-pass vlan 2 to 10
 stp disable
#
interface Ethernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 2 to 10
 stp instance 1 cost 200000
#
return
```

- SwitchD 的配置文件

```
#
 sysname SwitchD
#
 vlan batch 11 to 20
#
 stp pathcost-standard legacy
#
 stp region-configuration
  region-name RG1
  instance 1 vlan 2 to 10
  instance 2 vlan 11 to 20
  active region-
configuration
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11 to 20
#
interface Ethernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 11 to 20
 stp disable
#
interface Ethernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 11 to 20
 stp disable
#
interface Ethernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 11 to 20
 stp instance 2 cost 200000
#
return
```