H3C MSR 系列路由器

二层技术-以太网交换配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《二层技术-以太网交换配置指导》主要介绍以太网相关协议原理和配置，包括以太网链路聚合、端口隔离、VLAN、LLDP 等。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 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 | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

3. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

4. 端口编号示例约定

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

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 MAC地址表

说明

该特性仅在安装了二层接口卡的款型和 MSR3600-28/MSR3600-51 的固定二层接口上支持。

1.1 MAC地址表简介

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

1.1.1 MAC地址表项的生成方式

MAC 地址表项的生成方式有两种：自动生成、手工配置。

1. 自动生成MAC地址表项

一般情况下，MAC 地址表是设备通过源 MAC 地址学习过程而自动建立的。设备学习 MAC 地址的过程如下：

- 从某接口（假设为接口 A）收到一个数据帧，设备分析该数据帧的源 MAC 地址（假设为 MAC-SOURCE），并认为目的 MAC 地址为 MAC-SOURCE 的报文可以由接口 A 转发。
- 如果 MAC 地址表中已经包含 MAC-SOURCE，设备将对该表项进行更新。
- 如果 MAC 地址表中尚未包含 MAC-SOURCE，设备则将这个新 MAC 地址以及该 MAC 地址对应的接口 A 作为一个新的表项加入到 MAC 地址表中。

为适应网络拓扑的变化，MAC 地址表需要不断更新。MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称作老化时间。如果在到达生存周期前某表项被刷新，则重新计算该表项的老化时间。

2. 手工配置MAC地址表项

设备通过源 MAC 地址学习自动建立 MAC 地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。如果非法用户将攻击报文的源 MAC 地址伪装成合法用户的 MAC 地址，并从设备的其他接口进入，设备就会学习到错误的 MAC 地址表项，于是将本应转发给合法用户的报文转发给非法用户。

为了提高安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

1.1.2 MAC地址表项的分类

MAC 地址表项分为以下几种：

- 静态 MAC 地址表项：由用户手工配置，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项不老化。静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。
- 动态 MAC 地址表项：包括用户手工配置的以及设备通过源 MAC 地址学习得来的，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项有老化时间。手工配置的动态 MAC 地址表项优先级等于自动生成的 MAC 地址表项。
- 黑洞 MAC 地址表项：由用户手工配置，用于丢弃目的 MAC 地址为指定值的报文（例如，出于安全考虑，可以禁止某个接收报文），表项不老化。

静态 MAC 地址表项和黑洞 MAC 地址表项不会被动态 MAC 地址表项覆盖，而动态 MAC 地址表项可以被静态 MAC 地址表项和黑洞 MAC 地址表项覆盖。

说明

本章节内容只涉及单播的静态、动态和黑洞 MAC 地址表项。有关静态组播 MAC 地址表项的相关介绍和配置内容，请参见“IP 组播配置指导”中的“组播路由与转发”和“IPv6 组播路由与转发”。

1.2 配置MAC地址表

以下配置均为可选配置，且配置过程无先后顺序，用户可以根据实际情况选择配置。

1.2.1 配置MAC地址表项

配置 MAC 地址表项时，需要注意：

- 在手工配置动态 MAC 地址表项时，如果 MAC 地址表中已经存在 MAC 地址相匹配的自动生成表项，但该表项的接口与配置不符，那么该手工配置不生效。
- 如果不保存配置，设备重启后所有手工配置的 MAC 地址表项都会丢失；如果保存配置，设备重启后手工配置的静态 MAC 地址表项和黑洞 MAC 地址表项不会丢失，手工配置的动态 MAC 地址表项会丢失。

配置 MAC 地址表项后，当设备收到的报文的源 MAC 地址与配置表项中的 MAC 地址相同时，不同类型的 MAC 地址表项处理方式不同：

表1-1 不同类型 MAC 地址表项对源 MAC 地址匹配报文的处理方式

MAC 地址表项类型	报文源 MAC 地址与配置表项中的 MAC 地址相同
静态MAC地址表项	• 如果报文入接口与表项中的接口不同，则丢弃该报文 • 如果报文入接口与表项中的接口相同，则转发该报文
动态MAC地址表项	• 如果报文入接口与该表项中的接口不同，则进行 MAC 地址学习，并覆盖该表项 • 如果报文入接口与该表项中的接口相同，则转发该报文，并更新该表项老化时间

1. 配置静态/动态MAC地址表项

(1) 全局配置静态/动态 MAC 地址表项

表1-2 全局配置静态/动态 MAC 地址表项

操作	命令	说明
进入系统视图	**system-view**	-
添加或者修改静态/动态MAC地址表项	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	缺省情况下，系统没有配置任何MAC地址表项 **interface**参数指定的接口必须属于**vlan**参数指定的VLAN，而且该VLAN必须事先创建，否则将配置失败

(2) 接口配置静态/动态 MAC 地址表项

表1-3 接口配置静态/动态 MAC 地址表项

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
在当前接口下添加或者修改静态/动态MAC地址表项	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	缺省情况下，接口下没有配置任何MAC地址表项 当前接口必须属于*vlan-id*参数指定的VLAN，而且该VLAN必须事先创建，否则将配置失败

2. 配置黑洞MAC地址表项

表1-4 配置黑洞 MAC 地址表项

操作	命令	说明
进入系统视图	**system-view**	-
添加或者修改黑洞MAC地址表项	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	缺省情况下，系统没有配置任何MAC地址表项 **vlan**参数指定的VLAN必须事先创建，否则将配置失败

1.2.2 关闭接口MAC地址学习功能

缺省情况下，MAC 地址学习功能处于开启状态。有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。

关闭 MAC 地址学习功能后，不会立即删除已经学习到的动态 MAC 地址表项，需要等待 MAC 地址表项老化时间过后删除。

在开启全局的 MAC 地址学习功能的前提下，用户可以关闭设备上单个接口的 MAC 地址学习功能。

表1-5 关闭接口的 MAC 地址学习功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
关闭接口的MAC地址学习功能	**undo mac-address mac-learning enable**	缺省情况下，接口的MAC地址学习功能处于开启状态

1.2.3 配置动态MAC地址表项的老化时间

当网络拓扑改变后，如果动态 MAC 地址表项不及时更新，会导致用户流量不能正常转发。配置动态 MAC 地址表项的老化时间后，超过老化时间的动态 MAC 地址表项会被自动删除，设备将重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，导致设备广播大量的数据报文，增加网络的负担。

用户需要根据实际情况，配置合适的老化时间。如果网络比较稳定，可以将老化时间配置得长一些或者配置为不老化；否则，可以将老化时间配置得短一些。比如在一个比较稳定的网络，如果长时间没有流量，动态 MAC 地址表项会被全部删除，可能导致设备突然广播大量的数据报文，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设得长一些或不老化，以减少广播，增加网络稳定性和安全性。

动态 MAC 地址表项的老化时间作用于全部接口上。

表1-6 配置动态 MAC 地址表项的老化时间

操作	命令	说明
进入系统视图	**system-view**	-
配置动态MAC地址表项的老化时间	**mac-address timer { aging** *seconds* **| no-aging }**	缺省情况下，动态MAC地址表项的老化时间为300秒

1.3 MAC地址表显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MAC 地址表的运行情况，通过查看显示信息验证配置的效果。

表1-7 MAC 地址表显示和维护

操作	命令
显示MAC地址表信息	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]
显示MAC地址表动态表项的老化时间	**display mac-address aging-time**
显示MAC地址学习功能的使能状态	**display mac-address mac-learning** [**interface** *interface-type interface-number*]

1.4 MAC地址表典型配置举例

1. 组网需求

- 现有一台用户主机，它的 MAC 地址为 000f-e235-dc71，属于 VLAN 1，连接 Device 的 GigabitEthernet2/1/1 端口。为防止假冒身份的非法用户骗取数据，在设备的 MAC 地址表中为该用户主机添加一条静态表项。
- 另有一台用户主机，它的 MAC 地址为 000f-e235-abcd，属于 VLAN 1。由于该用户主机曾经接入网络进行非法操作，为了避免此种情况再次发生，在设备上添加一条黑洞 MAC 地址表项，使该用户主机接收不到报文。
- 配置设备的动态 MAC 地址表项老化时间为 500 秒。

2. 配置步骤

增加一个静态 MAC 地址表项，目的地址为 000f-e235-dc71，出接口为 GigabitEthernet2/1/1，且该接口属于 VLAN 1。

```
<Device> system-view
[Device] mac-address static 000f-e235-dc71 interface gigabitethernet 2/1/1 vlan 1
```

增加一个黑洞 MAC 地址表项，地址为 000f-e235-abcd，属于 VLAN 1。

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

配置动态 MAC 地址表项的老化时间为 500 秒。

```
[Device] mac-address timer aging 500
```

3. 验证配置

查看端口 GigabitEthernet2/1/1 上的静态 MAC 地址表项信息。

```
[Device] display mac-address static interface gigabitethernet 2/1/1
MAC Address      VLAN ID    State           Port/NickName           Aging
000f-e235-dc71   1          Static          GE2/1/1                 N
```

查看黑洞 MAC 地址表信息。

```
[Device] display mac-address blackhole
MAC Address      VLAN ID    State           Port/NickName           Aging
000f-e235-abcd   1          Blackhole       N/A                     N
```

查看动态 MAC 地址表项的老化时间。

```
[Device] display mac-address aging-time
MAC address aging time: 500s.
```

目 录

1 以太网链路聚合

1.1 以太网链路聚合简介

以太网链路聚合通过将多条以太网物理链路捆绑在一起形成一条以太网逻辑链路，实现增加链路带宽的目的，同时这些捆绑在一起的链路通过相互动态备份，可以有效地提高链路的可靠性。

如 图 1-1 所示，Device A与Device B之间通过三条以太网物理链路相连，将这三条链路捆绑在一起，就成为了一条逻辑链路Link aggregation 1。这条逻辑链路的带宽最大可等于三条以太网物理链路的带宽总和，增加了链路的带宽；同时，这三条以太网物理链路相互备份，当其中某条物理链路down，还可以通过其他两条物理链路转发报文。

图1-1 链路聚合示意图

1.1.1 基本概念

1. 聚合组、成员端口和聚合接口

链路捆绑是通过接口捆绑实现的，多个以太网接口捆绑在一起后形成一个聚合组，而这些被捆绑在一起的以太网接口就称为该聚合组的成员端口。每个聚合组唯一对应着一个逻辑接口，称为聚合接口。聚合组与聚合接口的编号是相同的，例如聚合组 1 对应于聚合接口 1。聚合组/聚合接口可以分为以下两种类型：

- 二层聚合组/二层聚合接口：二层聚合组的成员端口全部为二层以太网接口，其对应的聚合接口称为二层聚合接口。
- 三层聚合组/三层聚合接口：三层聚合组的成员端口全部为三层以太网接口，其对应的聚合接口称为三层聚合接口。在创建了三层聚合接口之后，还可继续创建该三层聚合接口的子接口，即三层聚合子接口。

聚合接口的速率和双工模式取决于对应聚合组内的选中端口（请参见“1.1.1 2. 成员端口的状态”）：聚合接口的速率等于所有选中端口的速率之和，聚合接口的双工模式则与选中端口的双工模式相同。

说明

目前，设备仅支持三层链路聚合。

2. 成员端口的状态

聚合组内的成员端口具有以下两种状态：

- 选中（Selected）状态：此状态下的成员端口可以参与数据的转发，处于此状态的成员端口称为“选中端口”。

- 非选中（Unselected）状态：此状态下的成员端口不能参与数据的转发，处于此状态的成员端口称为“非选中端口”。

3. 操作Key

操作 Key 是系统在进行链路聚合时用来表征成员端口聚合能力的一个数值，它是根据成员端口上的一些信息（包括该端口的速率、双工模式等）的组合自动计算生成的，这个信息组合中任何一项的变化都会引起操作 Key 的重新计算。在同一聚合组中，所有的选中端口都必须具有相同的操作 Key。

4. 配置分类

根据对成员端口状态的影响不同，成员端口上的配置可以分为以下两类：

(1) 属性类配置：包含的配置内容如 表 1-1 所示。在聚合组中，只有与对应聚合接口的属性类配置完全相同的成员端口才能够成为选中端口。

表1-1 属性类配置的内容

配置项	内容
端口隔离	端口是否加入隔离组、端口所属的端口隔离组
QinQ配置	端口的QinQ功能开启/关闭状态、VLAN Tag的TPID值、VLAN透传。关于QinQ配置的详细描述请参见“二层技术-以太网交换配置指导”中的“QinQ”
VLAN配置	端口上允许通过的VLAN、端口缺省VLAN、端口的链路类型（即Trunk、Hybrid、Access类型）、VLAN报文是否带Tag配置。有关VLAN配置的详细描述，请参见“二层技术-以太网交换配置指导”中的“VLAN”

说明

- 在聚合接口上所作的属性类配置，将被自动同步到对应聚合组内的所有成员端口上。当聚合接口被删除后，这些配置仍将保留在这些成员端口上。
- 由于成员端口上属性类配置的改变可能导致其选中/非选中状态发生变化，进而对业务产生影响，因此当在成员端口上进行此类配置时，系统将给出提示信息，由用户来决定是否继续执行该配置。

(2) 协议类配置：是相对于属性类配置而言的，包含的配置内容有 MAC 地址学习、生成树等。在聚合组中，即使某成员端口与对应聚合接口的协议配置存在不同，也不会影响该成员端口成为选中端口。

说明

在成员端口上所作的协议类配置，只有当该成员端口退出聚合组后才能生效。

5. 聚合模式

链路聚合分为静态聚合和动态聚合两种模式，它们各自的优点如下所示：

- 静态聚合模式：一旦配置好后，端口的选中/非选中状态就不会受网络环境的影响，比较稳定。
- 动态聚合模式：能够根据对端和本端的信息调整端口的选中/非选中状态，比较灵活。

处于静态聚合模式下的聚合组称为静态聚合组，处于动态聚合模式下的聚合组称为动态聚合组。

1.1.2 静态聚合模式

静态聚合模式的工作机制如下所述。

1. 选择参考端口

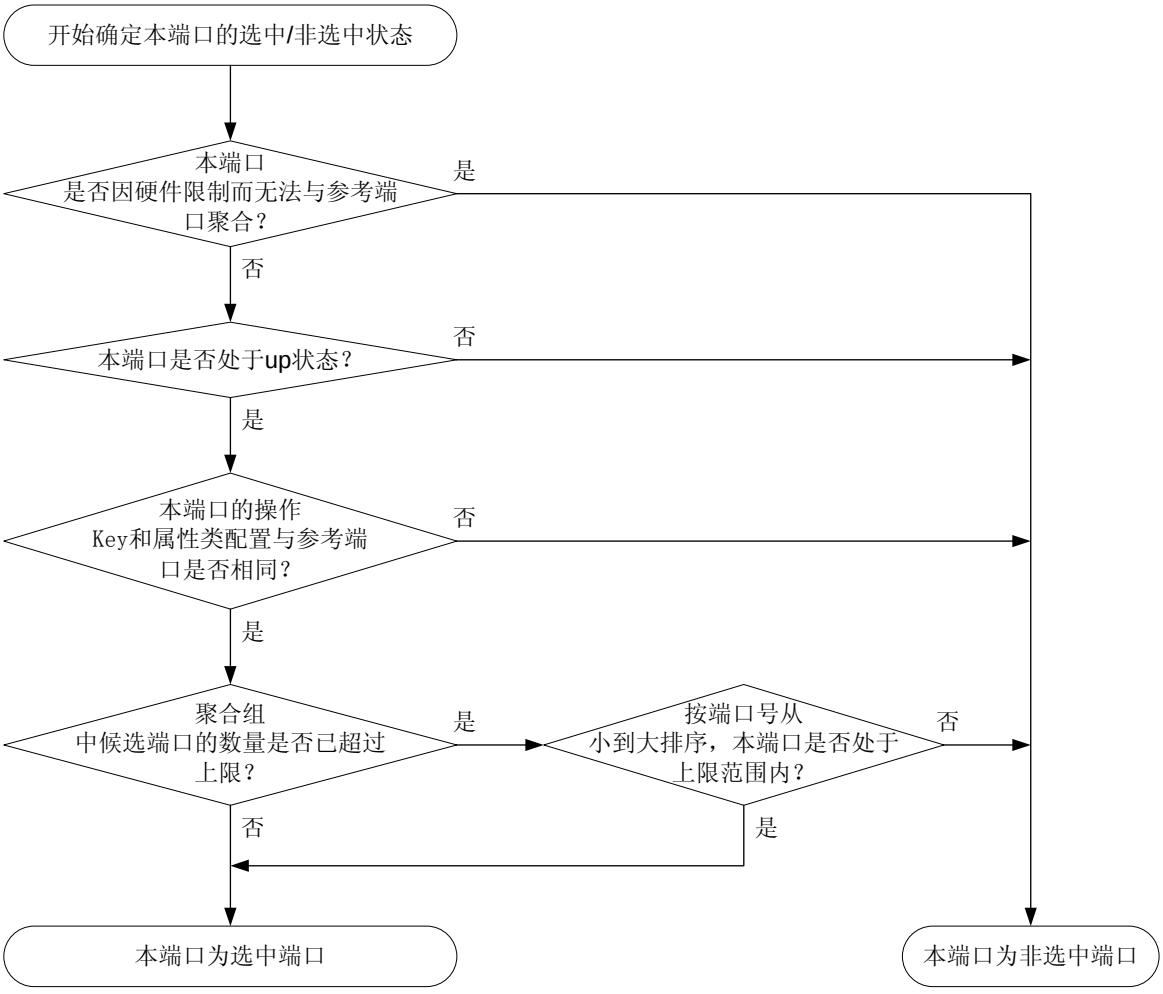
参考端口从本端的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

对于聚合组内处于 up 状态的端口，按照端口的高端口优先级->全双工/高速率->全双工/低速率->半双工/高速率->半双工/低速率的优先次序，选择优先次序最高、且属性类配置与对应聚合接口相同的端口作为参考端口；如果优先次序相同，首先选择原来的选中端口作为参考端口；如果此时有多个端口的优先次序相同且为原来的选中端口，则选择其中端口号最小的端口作为参考端口。

2. 确定成员端口的状态

静态聚合组内成员端口状态的确定流程如 图 1-2 所示。

图1-2 静态聚合组内成员端口状态的确定流程



确定静态聚合组内成员端口状态时，需要注意：

- 当一个成员端口的操作 Key 或属性类配置改变时，其所在静态聚合组内各成员端口的选中/非选中状态可能会发生改变。

- 当静态聚合组内选中端口的数量已达到上限时，后加入的成员端口即使满足成为选中端口的所有条件，也不会立即成为选中端口。这样能够尽量维持当前选中端口上的流量不中断，但是由于设备重启时会重新计算选中端口，因此可能导致设备重启前后各成员端口的选中/非选中状态不一致。

1.1.3 动态聚合模式

动态聚合模式通过 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议实现，LACP 协议的内容及动态聚合模式的工作机制如下所述。

1. LACP协议

基于 IEEE802.3ad 标准的 LACP 协议是一种实现链路动态聚合的协议，运行该协议的设备之间通过互发 LACPDU 来交互链路聚合的相关信息。

动态聚合组内的成员端口可以收发 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元），本端通过向对端发送 LACPDU 通告本端的信息。当对端收到该 LACPDU 后，将其中的信息与所在端其他成员端口收到的信息进行比较，以选择能够处于选中状态的成员端口，使双方可以对各自接口的选中/非选中状态达成一致。

(1) LACP 协议的功能

表1-2 LACP 协议的功能分类

类别	说明
基本功能	利用LACPDU的基本字段可以实现LACP协议的基本功能。基本字段包含以下信息：系统LACP优先级、系统MAC地址、端口优先级、端口编号和操作Key

(2) LACP 工作模式

LACP 工作模式分为 ACTIVE 和 PASSIVE 两种。

如果动态聚合组内成员端口的LACP工作模式为PASSIVE，且对端的LACP工作模式也为PASSIVE时，两端将不能发送 LACPDU。如果两端中任何一端的 LACP 工作模式为 ACTIVE 时，两端将可以发送 LACPDU。

(3) LACP 优先级

根据作用的不同，可以将LACP优先级分为系统LACP优先级和端口优先级两类，如 表 1-3 所示。

表1-3 LACP 优先级的分类

类别	说明	比较标准
系统LACP优先级	用于区分两端设备优先级的高低。当两端设备中的一端具有较高优先级时，另一端将根据优先级较高的一端来选择本端的选中端口，这样便使两端设备的选中端口达成了一致	优先级数值越小，优先级越高
端口优先级	用于区分各成员端口成为选中端口的优先程度	

(4) LACP 超时时间

LACP 超时时间是指成员端口等待接收 LACPDU 的超时时间，在 LACP 超时时间之后，如果本端成员端口仍未收到来自对端的 LACPDU，则认为对端成员端口已失效。

LACP 超时时间同时也决定了对端发送 LACPDU 的速率。LACP 超时有短超时（3 秒）和长超时（90 秒）两种。若 LACP 超时时间为短超时，则对端将快速发送 LACPDU（每 1 秒发送 1 个 LACPDU）；若 LACP 超时时间为长超时，则对端将慢速发送 LACPDU（每 30 秒发送 1 个 LACPDU）。

2. 动态聚合模式的工作机制：

(1) 选择参考端口

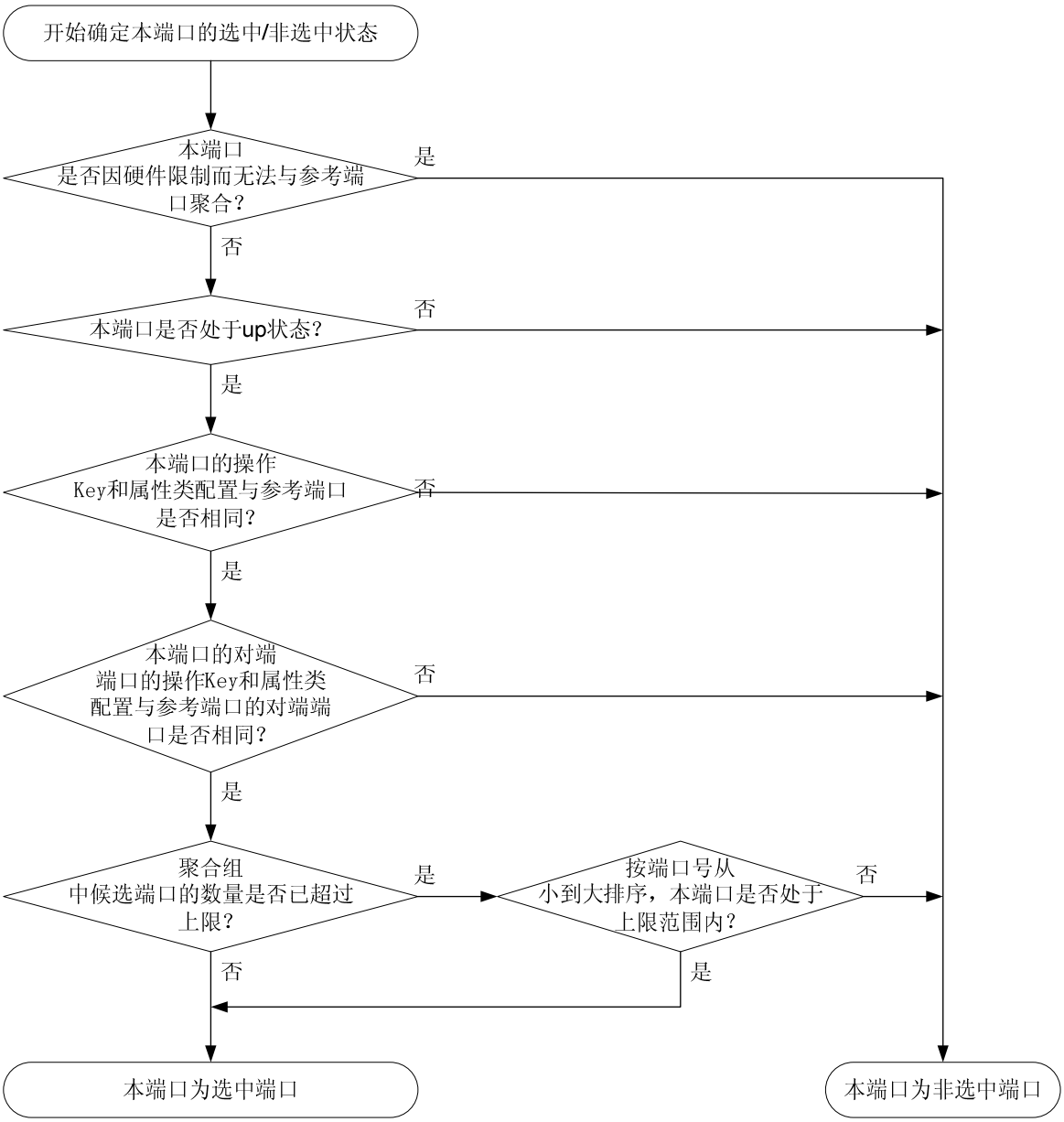
参考端口从聚合链路两端处于 up 状态的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

- 首先，从聚合链路的两端选出设备 ID（由系统的 LACP 优先级和系统的 MAC 地址共同构成）较小的一端：先比较两端的系统 LACP 优先级，优先级数值越小其设备 ID 越小；如果优先级相同再比较其系统 MAC 地址，MAC 地址越小其设备 ID 越小。
- 其次，对于设备 ID 较小的一端，再比较其聚合组内各成员端口的端口 ID（由端口优先级和端口的编号共同构成）：先比较端口优先级，优先级数值越小其端口 ID 越小；如果优先级相同再比较其端口号，端口号越小其端口 ID 越小。端口 ID 最小、且属性类配置与对应聚合接口相同的端口作为参考端口。

(2) 确定成员端口的状态

在设备ID较小的一端，动态聚合组内成员端口状态的确定流程如 图 1-3 所示。

图1-3 动态聚合组内成员端口状态的确定流程



与此同时，设备 ID 较大的一端也会随着对端成员端口状态的变化，随时调整本端各成员端口的状态，以确保聚合链路两端成员端口状态的一致。

确定动态聚合组内成员端口状态时，需要注意：

- 当动态聚合组内同时存在全双工端口和半双工端口时，全双工端口将优先成为选中端口；只有当所有全双工端口都无法成为选中端口，或动态聚合组内只有半双工端口时，才允许从半双工端口中选出一个成为选中端口，且只有一个半双工端口可成为选中端口。
- 当一个成员端口的操作 Key 或属性类配置改变时，其所在动态聚合组内各成员端口的选中/非选中状态可能会发生改变。
- 当本端端口的选中/非选中状态发生改变时，其对端端口的选中/非选中状态也将随之改变。
- 当动态聚合组内选中端口的数量已达到上限时，后加入的成员端口一旦满足成为选中端口的所有条件，就会立刻取代已不满足条件的端口成为选中端口。

1.1.4 聚合负载分担类型

通过采用逐流负载分担类型，按照报文的源/目的服务端口、源/目的 IP 地址标签中的一种或某几种的组合区分流，使属于同一数据流的报文从同一条成员链路上通过。可以实现灵活地对聚合组内流量进行负载分担。

1.2 以太网链路聚合配置任务简介

表1-4 以太网链路聚合配置任务简介

配置任务		说明	详细配置
配置聚合组	配置静态聚合组	二者必选其一	1.3.1
	配置动态聚合组		1.3.2
聚合接口相关配置	配置聚合接口的描述信息	可选	1.4.1
	配置三层聚合接口MTU	可选	1.4.2
	限制聚合组内选中端口的数量	可选	1.4.3
	配置聚合接口的期望带宽	可选	1.4.4
	关闭聚合接口	可选	1.4.5
	恢复聚合接口的缺省配置	可选	1.4.6
配置聚合负载分担		可选	1.5
配置聚合流量重定向功能		可选	1.6

1.3 配置聚合组

配置聚合组时，需要注意：

- 用户删除聚合接口时，系统将自动删除对应的聚合组，且该聚合组内的所有成员端口将全部离开该聚合组。
- 聚合链路的两端应配置相同的聚合模式。

1.3.1 配置静态聚合组

对于静态聚合模式，用户需要保证在同一链路两端端口的选中/非选中状态的一致性，否则聚合功能无法正常使用。

1. 配置三层静态聚合组

表1-5 配置三层静态聚合组

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建三层聚合接口，并进入三层聚合接口视图	**interface route-aggregation** *interface-number*	创建三层聚合接口后，系统将自动生成同编号的三层聚合组，且该聚合组缺省工作在静态聚合模式下
退回系统视图	**quit**	-
进入三层以太网接口视图	**interface** *interface-type interface-number*	多次执行此步骤可将多个三层以太网接口加入聚合组
将三层以太网接口加入聚合组	**port link-aggregation group** *number*	

1.3.2 配置动态聚合组

对于动态聚合模式，聚合链路两端的设备会自动协商同一链路两端的端口在各自聚合组内的选中/非选中状态，用户只需保证本端聚合在一起的端口的对端也同样聚合在一起，聚合功能即可正常使用。

1. 配置三层动态聚合组

表1-6 配置三层动态聚合组

操作	命令	说明
进入系统视图	**system-view**	-
配置系统的LACP优先级	**lacp system-priority** *system-priority*	缺省情况下，系统的LACP优先级为32768 改变系统的LACP优先级，将会影响到动态聚合组成员的选中/非选中状态
创建三层聚合接口，并进入三层聚合接口视图	**interface route-aggregation** *interface-number*	创建三层聚合接口后，系统将自动生成同编号的三层聚合组，且该聚合组缺省工作在静态聚合模式下
配置聚合组工作在动态聚合模式下	**link-aggregation mode dynamic**	缺省情况下，聚合组工作在静态聚合模式下
退回系统视图	**quit**	-
进入三层以太网接口视图	**interface** *interface-type interface-number*	多次执行此步骤可将多个三层以太网接口加入聚合组
将三层以太网接口加入聚合组	**port link-aggregation group** *number*	
配置当前端口的LACP工作模式为PASSIVE	**lacp mode passive**	二者选其一 缺省情况下，端口的LACP工作模式为ACTIVE
配置当前端口的LACP工作模式为ACTIVE	**undo lacp mode**	
配置端口优先级	**link-aggregation port-priority** *port-priority*	缺省情况下，端口优先级为32768
配置端口的LACP超时时间为短超时（3秒），并使对端快速发送LACPDU	**lacp period short**	缺省情况下，端口的LACP超时时间为长超时（90秒），对端慢速发送LACPDU

1.4 聚合接口相关配置

本节对能够在聚合接口上进行的部分配置进行介绍。除本节所介绍的配置外，能够在三层以太网接口上进行的配置大多数也能在三层聚合接口上进行，具体配置请参见相关的配置指导。

1.4.1 配置聚合接口的描述信息

通过在接口上配置描述信息，可以方便网络管理员根据这些信息来区分各接口的作用。

表1-7 配置聚合接口的描述信息

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口/子接口视图	**interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	-
配置当前接口的描述信息	**description** *text*	缺省情况下，接口的描述信息为“*接口名* Interface”

1.4.2 配置三层聚合接口MTU

MTU（Maximum Transmission Unit，最大传输单元）参数会影响 IP 报文的分片与重组，可以通过下面的配置来改变 MTU 值。

表1-8 配置三层聚合接口 MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口/子接口视图	**interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	-
配置三层聚合接口/子接口的MTU值	**mtu** *size*	缺省情况下，三层聚合接口/子接口的MTU值为1500字节

1.4.3 限制聚合组内选中端口的数量

提示

本端和对端配置的聚合组中的最小/最大选中端口数必须一致。

聚合链路的带宽取决于聚合组内选中端口的数量，用户通过配置聚合组中的最小选中端口数，可以避免由于选中端口太少而造成聚合链路上的流量拥塞。当聚合组内选中端口的数量达不到配置值时，对应的聚合接口将不会 up。具体实现如下：

- 如果聚合组内能够被选中的成员端口数小于配置值，这些成员端口都将变为非选中状态，对应聚合接口的链路状态也将变为 down。
- 当聚合组内能够被选中的成员端口数增加至不小于配置值时，这些成员端口都将变为选中状态，对应聚合接口的链路状态也将变为 up。

当配置了聚合组中的最大选中端口数之后，最大选中端口数将同时受配置值和设备硬件能力的限制，即取二者的较小值作为限制值。用户借此可实现两端口间的冗余备份：在一个聚合组中只添加两个成员端口，并配置该聚合组中的最大选中端口数为 1，这样这两个成员端口在同一时刻就只能有一个成为选中端口，而另一个将作为备份端口。

表1-9 限制聚合组内选中端口的数量

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口	**interface route-aggregation** *interface-number*	-
配置聚合组中的最小选中端口数	**link-aggregation selected-port minimum** *number*	缺省情况下，聚合组中的最小选中端口数不受限制
配置聚合组中的最大选中端口数	**link-aggregation selected-port maximum** *number*	缺省情况下，聚合组中的最大选中端口数仅受设备硬件能力的限制

1.4.4 配置聚合接口的期望带宽

表1-10 配置聚合接口的期望带宽

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口/子接口视图	**interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	-
配置当前接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbit/s）

1.4.5 关闭聚合接口

提示

聚合接口关闭时，聚合组内成员端口上不能配置 **loopback** 命令，同样的，配置有 **loopback** 命令的端口不能加入处于关闭状态的聚合接口。有关 **loopback** 命令的详细介绍，请参见“二层交换-以太网交换命令参考”中的“以太网接口”。

对聚合接口的开启/关闭操作，将会影响聚合接口对应的聚合组内成员端口的选中/非选中状态和链路状态：

- 关闭聚合接口时，将使对应聚合组内所有处于选中状态的成员端口都变为非选中端口，且所有成员端口的链路状态都将变为 down。
- 开启聚合接口时，系统将重新计算对应聚合组内成员端口的选中/非选中状态。

表1-11 关闭聚合接口

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口/子接口视图	**interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	-
关闭当前接口	**shutdown**	缺省情况下，聚合接口为打开状态

1.4.6 恢复聚合接口的缺省配置

通过执行本操作可以将聚合接口下的所有配置都恢复为缺省配置。

表1-12 恢复聚合接口的缺省配置

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口/子接口视图	**interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	-
恢复当前聚合接口的缺省配置	**default**	-

1.5 配置聚合负载分担

聚合负载分担类型支持全局配置或在聚合组内配置两种方式：全局的配置对所有聚合组都有效，而聚合组内的配置只对当前聚合组有效。对于一个聚合组来说，优先采用该聚合组内的配置，只有该聚合组内未进行配置时，才采用全局的配置。

1. 全局配置聚合负载分担类型

表1-13 全局配置聚合负载分担类型

操作	命令	说明
进入系统视图	**system-view**	-
配置全局采用的聚合负载分担类型	**link-aggregation global load-sharing mode** { **destination-ip** | **destination-port** | **source-ip** | **source-port** }	

2. 在聚合组内配置聚合负载分担类型

表1-14 在聚合组内配置聚合负载分担类型

操作	命令	说明
进入系统视图	**system-view**	-
进入三层聚合接口视图	**interface route-aggregation** *interface-number*	-
配置聚合组内采用的聚合负载分担类型	**link-aggregation load-sharing mode** { **destination-ip** | **destination-port** | **source-ip** | **source-port** }	

1.6 配置聚合流量重定向功能

在使能了聚合流量重定向功能后，当关闭聚合组内某选中端口时，系统可以将该端口上的流量重定向到其他选中端口上，从而实现聚合链路上流量的不中断。（MSR 2600/MSR 3600）

在使能了聚合流量重定向功能后，当重启设备上某块有聚合组选中端口的单板时，系统可以将该单板上的流量重定向到其他单板上，从而实现聚合链路上流量的不中断。（MSR 5600）

配置聚合流量重定向功能时，需要注意：

- 必须在聚合链路两端都使能聚合流量重定向功能才能实现聚合链路上流量的不中断。
- 如果同时使能聚合流量重定向功能和生成树功能，在重启单板/设备时会出现少量的丢包，因此不建议同时使能上述两个功能。
- 只有动态聚合组支持聚合流量重定向功能。

表1-15 配置聚合流量重定向功能

操作	命令	说明
进入系统视图	**system-view**	-
使能聚合流量重定向功能	**link-aggregation lacp traffic-redirect-notification enable**	缺省情况下，聚合流量重定向功能处于关闭状态

1.7 以太网链路聚合显示与维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后以太网链路聚合的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除端口的 LACP 和聚合接口上的统计信息。

表1-16 以太网链路聚合显示与维护

操作	命令
显示聚合接口的相关信息	**display interface** [**route-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]
显示本端系统的设备ID	**display lacp system-id**

操作	命令
显示全局或聚合组内采用的聚合负载分担类型	**display link-aggregation load-sharing mode** [**interface** [**route-aggregation** *interface-number*]]
显示成员端口上链路聚合的详细信息	**display link-aggregation member-port** [*interface-list*]
显示所有聚合组的摘要信息	**display link-aggregation summary**
显示已有聚合接口所对应聚合组的详细信息	**display link-aggregation verbose** [**route-aggregation** [*interface-number*]]
清除成员端口上的LACP统计信息	**reset lacp statistics** [**interface** *interface-list*]
清除聚合接口上的统计信息	**reset counters interface** [**route-aggregation** [*interface-number*]]

1.8 以太网链路聚合典型配置举例

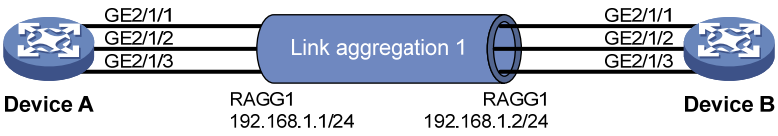
1.8.1 三层静态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的三层以太网接口 GigabitEthernet2/1/1～GigabitEthernet2/1/3 相互连接。
- 在 Device A 和 Device B 上分别配置三层静态链路聚合组，并为对应的三层聚合接口配置 IP 地址和子网掩码。

2. 组网图

图1-4 三层静态聚合配置组网图



3. 配置步骤

(1) 配置 Device A

创建三层聚合接口 1，并为该接口配置 IP 地址和子网掩码。

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

分别将接口 GigabitEthernet2/1/1 至 GigabitEthernet2/1/3 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/1] quit
[DeviceA] interface gigabitethernet 2/1/2
[DeviceA-GigabitEthernet2/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/2] quit
```

```
[DeviceA] interface gigabitethernet 2/1/3
[DeviceA-GigabitEthernet2/1/3] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/3] quit
```

(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

4. 验证配置

查看 Device A 上所有聚合组的详细信息。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE2/1/1          S       32768    1
  GE2/1/2          S       32768    1
  GE2/1/3          S       32768    1
```

以上信息表明，聚合组 1 为负载分担类型的三层静态聚合组，包含有三个选中端口。

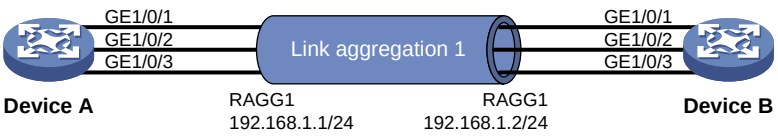
1.8.2 三层动态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的三层以太网接口 GigabitEthernet2/1/1～GigabitEthernet2/1/3 相互连接。
- 在 Device A 和 Device B 上分别配置三层动态链路聚合组，并为对应的三层聚合接口配置 IP 地址和子网掩码。

2. 组网图

图1-5 三层动态聚合配置组网图



3. 配置步骤

(1) 配置 Device A

创建三层聚合接口 1，配置该接口为动态聚合模式，并为其配置 IP 地址和子网掩码。

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
```

```
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

分别将接口 GigabitEthernet2/1/1 至 GigabitEthernet2/1/3 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/1] quit
[DeviceA] interface gigabitethernet 2/1/2
[DeviceA-GigabitEthernet2/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/2] quit
[DeviceA] interface gigabitethernet 2/1/3
[DeviceA-GigabitEthernet2/1/3] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/3] quit
```

(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

4. 验证配置

查看 Device A 上所有聚合组的详细信息。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE2/1/1          S       32768    1         {ACDEF}
  GE2/1/2          S       32768    1         {ACDEF}
  GE2/1/3          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE2/1/1          1       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE2/1/2          2       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE2/1/3          3       32768    1         0x8000, 000f-e267-57ad {ACDEF}
```

以上信息表明，聚合组 1 为负载分担类型的三层动态聚合组，包含有三个选中端口。

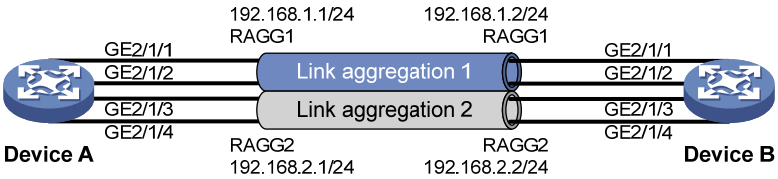
1.8.3 三层聚合负载分担配置举例

1. 组网需求

- Device A 与 Device B 通过各自的三层以太网接口 GigabitEthernet2/1/1～GigabitEthernet2/1/4 相互连接。
- 在 Device A 和 Device B 上分别配置两个三层静态链路聚合组，并为对应的三层聚合接口都配置 IP 地址和子网掩码。
- 通过在聚合组 1 上按照源 IP 地址进行聚合负载分担、在聚合组 2 上按照目的 IP 地址进行聚合负载分担的方式，来实现数据流量在各成员端口间的负载分担。

2. 组网图

图1-6 三层聚合负载分担配置组网图



3. 配置步骤

(1) 配置 Device A

创建三层聚合接口 1，配置该接口对应的聚合组内按照源 IP 地址进行聚合负载分担，并为其配置 IP 地址和子网掩码。

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation load-sharing mode source-ip
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

分别将接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/1] quit
[DeviceA] interface gigabitethernet 2/1/2
[DeviceA-GigabitEthernet2/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet2/1/2] quit
```

创建三层聚合接口 2，配置该接口对应的聚合组内按照目的 IP 地址进行聚合负载分担，并为其配置 IP 地址和子网掩码。

```
[DeviceA] interface route-aggregation 2
[DeviceA-Route-Aggregation2] link-aggregation load-sharing mode destination-ip
[DeviceA-Route-Aggregation2] ip address 192.168.2.1 24
[DeviceA-Route-Aggregation2] quit
```

分别将接口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 加入到聚合组 2 中。

```
[DeviceA] interface gigabitethernet 2/1/3
[DeviceA-GigabitEthernet2/1/3] port link-aggregation group 2
[DeviceA-GigabitEthernet2/1/3] quit
```

```
[DeviceA] interface gigabitethernet 2/1/4
[DeviceA-GigabitEthernet2/1/4] port link-aggregation group 2
[DeviceA-GigabitEthernet2/1/4] quit
```

(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

4. 验证配置

查看 Device A 上所有聚合组的详细信息。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE2/1/1          S       32768    1
  GE2/1/2          S       32768    1

Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE2/1/3          S       32768    2
  GE2/1/4          S       32768    2
```

以上信息表明，聚合组 1 和聚合组 2 都是负载分担类型的三层静态聚合组，各包含有两个选中端口。

查看 Device A 上所有聚合接口所对应聚合组内采用的聚合负载分担类型。

```
[DeviceA] display link-aggregation load-sharing mode interface
Route-Aggregation1 Load-Sharing Mode:
source-ip address

Route-Aggregation2 Load-Sharing Mode:
destination-ip address
```

以上信息表明，三层聚合组 1 按照报文的源 IP 地址进行聚合负载分担，三层聚合组 2 按照报文的目的 IP 地址进行聚合负载分担。

目 录

1 端口隔离

说明

该特性仅在安装了 SIC 4GSW/SIC 4GSWP/DSIC 9FSW/DSIC 9FSWP/HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 接口卡的款型和 MSR 3600-28/MSR 3600-51 的固定二层接口上支持。

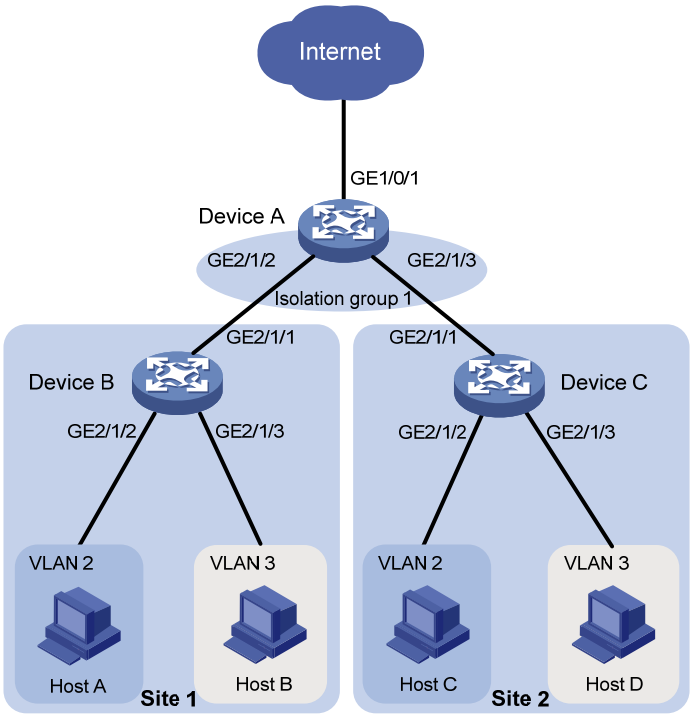
1.1 端口隔离简介

为了实现端口间的二层隔离，可以将不同的端口加入不同的 VLAN，但 VLAN 资源有限。采用端口隔离特性，用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层隔离，而不关心这些端口所属 VLAN，从而节省 VLAN 资源。

隔离组内的端口与未加入隔离组的端口之间二层流量双向互通。

如 图 1-1 所示，Device B和Device C都通过Device A与外部网络相连，Device A分别通过GigabitEthernet2/1/2 和GigabitEthernet2/1/3 连接Device B和Device C，且这两个端口均允许VLAN 2、VLAN 3 的报文通过。将GigabitEthernet2/1/2 和GigabitEthernet2/1/3 加入隔离组 1 后，Device B与Device C之间不能二层互通（属于同一VLAN的Host A和Host C之间、Host B和Host D之间也不能互通）。

图1-1 非隔离 VLAN 示意图



1.2 配置隔离组

设备只支持一个隔离组，由系统自动创建隔离组 1，用户不可删除该隔离组或创建其他的隔离组。隔离组内可以加入的端口数量没有限制。

表1-1 配置隔离组

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	二层以太网接口视图下的配置只对当前端口生效
将当前端口加入到隔离组中	**port-isolate enable**	缺省情况下，当前端口未加入隔离组

1.3 端口隔离显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后端口隔离的运行情况，通过查看显示信息验证配置的效果。

表1-2 端口隔离显示和维护

操作	命令
显示隔离组的信息	**display port-isolate group**

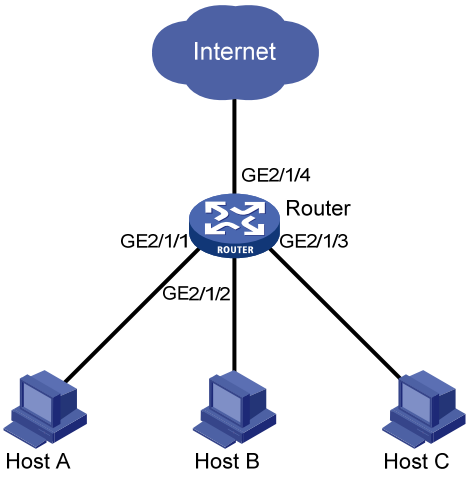
1.4 端口隔离典型配置举例

1. 组网需求

如 图 1-2 所示，小区用户Host A、Host B、Host C分别与Router的端口GigabitEthernet2/1/1、GigabitEthernet2/1/2、GigabitEthernet2/1/3 相连，Router设备通过GigabitEthernet2/1/4 端口与外部网络相连。现需要实现小区用户Host A、Host B和Host C彼此之间二层报文不能互通，但可以和外部网络通信。

2. 组网图

图1-2 端口隔离组网图



3. 配置步骤

将端口 GigabitEthernet2/1/1、GigabitEthernet2/1/2、GigabitEthernet2/1/3 加入隔离组。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] port-isolate enable
[Router-GigabitEthernet2/1/1] quit
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] port-isolate enable
[Router-GigabitEthernet2/1/2] quit
[Router] interface gigabitethernet 2/1/3
[Router-GigabitEthernet2/1/3] port-isolate enable
[Router-GigabitEthernet2/1/3] quit
```

4. 验证配置

显示隔离组中的信息。

```
[Router] display port-isolate group
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet2/1/1     GigabitEthernet2/1/2     GigabitEthernet2/1/3
```

以上信息显示 Router 上的端口 GigabitEthernet2/1/1、GigabitEthernet2/1/2、GigabitEthernet2/1/3 已经加入隔离组，从而实现二层隔离，分别对应的 Host A、Host B 和 Host C 彼此之间不能 Ping 通。

目 录

1 生成树

说明

该特性仅在安装了二层接口卡的款型和 MSR 3600-28/MSR 3600-51 的固定二层接口上支持。

1.1 生成树简介

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 STP（Spanning Tree Protocol，生成树协议）到 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）和 PVST（Per-VLAN Spanning Tree，每 VLAN 生成树），再到最新的 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。本文将对 STP、RSTP、PVST 和 MSTP 各自的特点及其相互间的关系进行介绍。

1.1.1 STP简介

STP 由 IEEE 制定的 802.1D 标准定义，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路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的报文处理能力下降的问题发生。

STP 包含了两个含义，狭义的 STP 是指 IEEE 802.1D 中定义的 STP 协议，广义的 STP 是指包括 IEEE 802.1D 定义的 STP 协议以及各种在它的基础上经过改进的生成树协议。

1. STP的协议报文

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息。本文中将把生成树协议的协议报文均简称为 BPDU。

STP 通过在设备之间传递 BPDU 来确定网络的拓扑结构。BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。STP 协议的 BPDU 分为以下两类：

- 配置 BPDU（Configuration BPDU）：用来进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU，拓扑变化通知 BPDU）：当拓扑结构发生变化时，用来通知相关设备网络拓扑结构发生变化的报文。

BPDU 中包含有足够的信息来保证设备完成生成树的计算过程，其中包括：

- 根桥（Root Bridge）ID：由根桥的优先级和 MAC 地址组成。
- 根路径开销：到根桥的路径开销。
- 指定桥 ID：由指定桥的优先级和 MAC 地址组成。
- 指定端口 ID：由指定端口的优先级和该端口的全局编号组成。
- Message Age：BPDU 在网络中传播的生存期。

- Max Age：BPDU 在设备中的最大生存期。
- Hello Time：BPDU 的发送周期。
- Forward Delay：端口状态迁移的延迟时间。

2. STP的基本概念

(1) 根桥

树形的网络结构必须有树根，于是 STP 引入了根桥的概念。根桥在全网中有且只有一个，其他设备则称为叶子节点。根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。

在网络初始化过程中，所有设备都视自己为根桥，生成各自的配置 BPDU 并周期性地向外发送；但当网络拓扑稳定以后，只有根桥设备才会向外发送配置 BPDU，其他设备则对其进行转发。

(2) 根端口

所谓根端口，是指非根桥设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

(3) 指定桥与指定端口

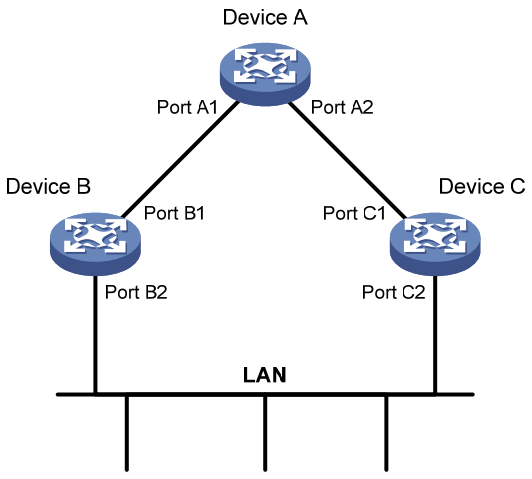
有关指定桥与指定端口的含义，请参见 表 1-1 的说明。

表1-1 指定桥与指定端口的含义

分类	指定桥	指定端口
对于一台设备而言	与本机直接相连并且负责向本机转发BPDU的设备	指定桥向本机转发BPDU的端口
对于一个局域网而言	负责向本网段转发BPDU的设备	指定桥向本网段转发BPDU的端口

如 图 1-1 所示，Device B和Device C与LAN直接相连。如果Device A通过Port A1 向Device B转发BPDU，则Device B的指定桥就是Device A，指定端口就是Device A上的Port A1；如果Device B负责向LAN转发BPDU，则LAN的指定桥就是Device B，指定端口就是Device B上的Port B2。

图1-1 指定桥与指定端口示意图



(4) 路径开销

路径开销是 STP 协议用于选择链路的参考值。STP 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型网络结构。

3. STP的基本原理

STP 算法实现的基本过程如下：

(1) 初始状态

各设备的各端口在初始时会生成以本设备为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

(2) 选择根桥

网络初始化时，网络中所有的 STP 设备都认为自己是“根桥”，根桥 ID 为自身的设备 ID。通过交换 BPDU，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

(3) 选择根端口和指定端口

根端口和指定端口的选择过程如 表 1-2 所示。

表1-2 根端口和指定端口的选择过程

步骤	内容
1	非根桥设备将接收最优BPDU（最优BPDU的选择过程如表1-3所示）的那个端口定为根端口
2	设备根据根端口的BPDU和根端口的路径开销，为每个端口计算一个指定端口BPDU： • 根桥 ID 替换为根端口的 BPDU 的根桥 ID； • 根路径开销替换为根端口 BPDU 的根路径开销加上根端口对应的路径开销； • 指定桥 ID 替换为自身设备的 ID； • 指定端口 ID 替换为自身端口 ID。
3	设备将计算出的BPDU与角色待定端口自己的BPDU进行比较： • 如果计算出的 BPDU 更优，则该端口被确定为指定端口，其 BPDU 也被计算出的 BPDU 替换，并周期性地向外发送； • 如果该端口自己的 BPDU 更优，则不更新该端口的 BPDU 并将该端口阻塞。该端口将不再转发数据，且只接收不发送 BPDU。

说明

当拓扑处于稳定状态时，只有根端口和指定端口在转发用户流量。其他端口都处于阻塞状态，只接收 STP 协议报文而不转发用户流量。

表1-3 最优 BPDU 的选择过程

步骤	内容
1	每个端口将收到的BPDU与自己的BPDU进行比较： • 如果收到的 BPDU 优先级较低，则将其直接丢弃，对自己的 BPDU 不进行任何处理； • 如果收到的 BPDU 优先级较高，则用该 BPDU 的内容将自己 BPDU 的内容替换掉。
2	设备将所有端口的BPDU进行比较，选出最优的BPDU

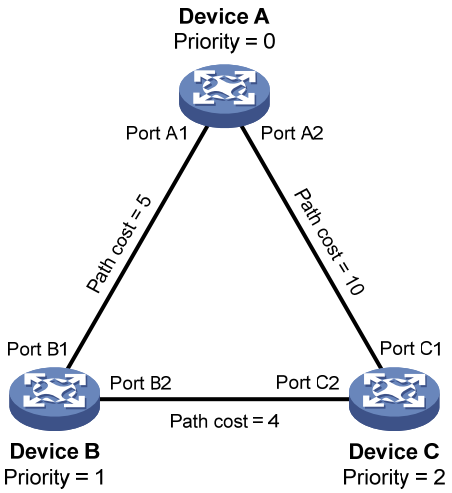
说明

BPDU 优先级的比较规则如下：

- 根桥 ID 较小的 BPDU 优先级较高；
- 若根桥 ID 相同，则比较根路径开销：将 BPDU 中的根路径开销与本端口对应的路径开销相加，二者之和较小的 BPDU 优先级较高；
- 若根路径开销也相同，则依次比较指定桥 ID、指定端口 ID、接收该 BPDU 的端口 ID 等，上述值较小的 BPDU 优先级较高。

一旦根桥、根端口和指定端口选举成功，整个树形拓扑就建立完毕了。下面结合例子说明 STP 算法实现的具体过程。

图1-2 STP 算法实现过程组网图



如 图 1-2 所示，Device A、Device B和Device C的优先级分别为 0、1 和 2，Device A与Device B之间、Device A与Device C之间以及Device B与Device C之间链路的路径开销分别为 5、10 和 4。

(1) 各设备的初始状态

各设备的初始状态如 表 1-4 所示。

表1-4 各设备的初始状态

设备	端口名称	端口的 BPDU
Device A	Port A1	{0，0，0，Port A1}
	Port A2	{0，0，0，Port A2}
Device B	Port B1	{1，0，1，Port B1}
	Port B2	{1，0，1，Port B2}
Device C	Port C1	{2，0，2，Port C1}
	Port C2	{2，0，2，Port C2}

说明

表 1-4 中BPDU各项的具体含义为：{根桥ID，根路径开销，指定桥ID，指定端口ID}。

(2) 各设备的比较过程及结果

各设备的比较过程及结果如 表 1-5 所示。

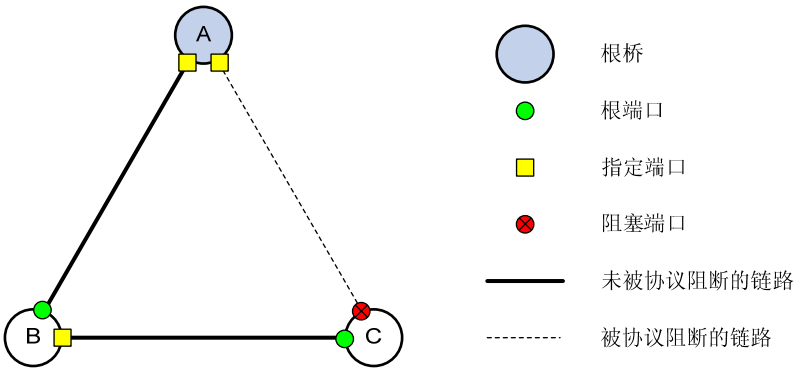
表1-5 各设备的比较过程及结果

设备	比较过程	比较后端口的 BPDU
Device A	• Port A1 收到 Port B1 的 BPDU {1，0，1，Port B1}，发现自己的 BPDU {0，0，0，Port A1}更优，于是将其丢弃。 • Port A2 收到 Port C1 的 BPDU {2，0，2，Port C1}，发现自己的 BPDU {0，0，0，Port A2}更优，于是将其丢弃。 • Device A 发现自己各端口的 BPDU 中的根桥和指定桥都是自己，于是认为自己就是根桥，各端口的 BPDU 都不作任何修改，此后便周期性地向外发送 BPDU。	• Port A1：{0，0，0，Port A1} • Port A2：{0，0，0，Port A2}
Device B	• Port B1 收到 Port A1 的 BPDU {0，0，0，Port A1}，发现其比自己的 BPDU {1，0，1，Port B1}更优，于是更新自己的 BPDU。 • Port B2 收到 Port C2 的 BPDU {2，0，2，Port C2}，发现自己的 BPDU {1，0，1，Port B2}更优，于是将其丢弃。	• Port B1：{0，0，0，Port A1} • Port B2：{1，0，1，Port B2}
	• Device B 比较自己各端口的 BPDU，发现 Port B1 的 BPDU 最优，于是该端口被确定为根端口，其 BPDU 不变。 • Device B 根据根端口的 BPDU 和路径开销，为 Port B2 计算出指定端口的 BPDU {0，5，1，Port B2}，然后与 Port B2 本身的 BPDU {1，0，1，Port B2}进行比较，发现计算出的 BPDU 更优，于是 Port B2 被确定为指定端口，其 BPDU 也被替换为计算出的 BPDU，并周期性地向外发送。	• 根端口 Port B1：{0，0，0，Port A1} • 指定端口 Port B2：{0，5，1，Port B2}
Device C	• Port C1 收到 Port A2 的 BPDU {0，0，0，Port A2}，发现其比自己的 BPDU {2，0，2，Port C1}更优，于是更新自己的 BPDU。 • Port C2 收到 Port B2 更新前的 BPDU {1，0，1，Port B2}，发现其比自己的 BPDU {2，0，2，Port C2}更优，于是更新自己的 BPDU。	• Port C1：{0，0，0，Port A2} • Port C2：{1，0，1，Port B2}

设备	比较过程	比较后端口的 BPDU
	• Device C 比较自己各端口的 BPDU，发现 Port C1 的 BPDU 最优，于是该端口被确定为根端口，其 BPDU 不变。 • Device C 根据根端口的 BPDU 和路径开销，为 Port C2 计算出指定端口的 BPDU {0，10，2，Port C2}，然后与 Port C2 本身的 BPDU {1，0，1，Port B2}进行比较，发现计算出的 BPDU 更优，于是 Port C2 被确定为指定端口，其 BPDU 也被替换为计算出的 BPDU。	• 根端口 Port C1：{0，0，0，Port A2} • 指定端口 Port C2：{0，10，2，Port C2}
	• Port C2 收到 Port B2 更新后的 BPDU {0，5，1，Port B2}，发现其比自己的 BPDU {0，10，2，Port C2}更优，于是更新自己的 BPDU。 • Port C1 收到 Port A2 周期性发来的 BPDU {0，0，0，Port A2}，发现其与自己的 BPDU 一样，于是将其丢弃。	• Port C1：{0，0，0，Port A2} • Port C2：{0，5，1，Port B2}
	• Device C 比较 Port C1 的根路径开销 10（收到的 BPDU 中的根路径开销 0＋本端口所在链路的路径开销 10）与 Port C2 的根路径开销 9（收到的 BPDU 中的根路径开销 5＋本端口所在链路的路径开销 4），发现后者更小，因此 Port C2 的 BPDU 更优，于是 Port C2 被确定为根端口，其 BPDU 不变。 • Device C 根据根端口的 BPDU 和路径开销，为 Port C1 计算出指定端口的 BPDU {0，9，2，Port C1}，然后与 Port C1 本身的 BPDU {0，0，0，Port A2}进行比较，发现本身的 BPDU 更优，于是 Port C1 被阻塞，其 BPDU 不变。从此，Port C1 不再转发数据，直至有触发生成树计算的新情况出现，譬如 Device B 与 Device C 之间的链路 down 掉。	• 阻塞端口 Port C1：{0，0，0，Port A2} • 根端口 Port C2：{0，5，1，Port B2}

经过上述比较过程之后，以Device A为根桥的生成树就确定下来了，其拓扑如 图 1-3 所示。

图1-3 计算后得到的拓扑



说明

为了便于描述，本例简化了生成树的计算过程，实际的过程要更加复杂。

4. STP的BPDU传递机制

STP 的 BPDU 传递机制如下：

- 当网络初始化时，所有的设备都将自己作为根桥，生成以自己为根的 BPDU，并以 Hello Time 为周期定时向外发送。

- 接收到 BPDU 的端口如果是根端口，且接收的 BPDU 比该端口的 BPDU 优，则设备将 BPDU 中携带的 Message Age 按照一定的原则递增，并启动定时器为这条 BPDU 计时，同时将此 BPDU 从设备的指定端口转发出去。
- 如果指定端口收到的 BPDU 比本端口的 BPDU 优先级低时，会立刻发出自己的更好的 BPDU 进行回应。
- 如果某条路径发生故障，则这条路径上的根端口不会再收到新的 BPDU，旧的 BPDU 将会因为超时而被丢弃，设备重新生成以自己为根的 BPDU 并向外发送，从而引发生成树的重新计算，得到一条新的通路替代发生故障的链路，恢复网络连通性。

不过，重新计算得到的新 BPDU 不会立刻就传遍整个网络，因此旧的根端口和指定端口由于没有发现网络拓扑变化，将仍按原来的路径继续转发数据。如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。

5. STP的时间参数

在 STP 的计算过程中，用到了以下三个重要的时间参数：

- Forward Delay：用于确定状态迁移的延迟时间。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新 BPDU 无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。为此，STP 采用了一种状态迁移的机制，新选出的根端口和指定端口要经过 2 倍的 Forward Delay 延时后才能进入转发状态，这个延时保证了新的 BPDU 已经传遍整个网络。
- Hello Time：用于设备检测链路是否存在故障。设备每隔 Hello Time 时间会向周围的设备发送 Hello 报文，以确认链路是否存在故障。
- Max Age：用于判断 BPDU 在设备内的保存时间是否“过时”，设备会将过时的 BPDU 丢弃。

1.1.2 RSTP简介

RSTP 由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时将大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

在 RSTP 中，根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。

在 RSTP 中，指定端口的端口状态快速迁移的条件是：指定端口是边缘端口（即该端口直接与用户终端相连，而没有连接到其他设备或共享网段上）或者指定端口与点对点链路（即两台设备直接相连的链路）相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

1.1.3 PVST简介

STP 和 RSTP 在局域网内的所有网桥都共享一棵生成树，不能按 VLAN 阻塞冗余链路，所有 VLAN 的报文都沿着一棵生成树进行转发。而 PVST 则可以在每个 VLAN 内都拥有一棵生成树，能够有效地提高链路带宽的利用率。PVST 可以简单理解为在每个 VLAN 上运行一个 STP 或 RSTP 协议，不同 VLAN 之间的生成树完全独立。

运行 PVST 的 H3C 设备可以与运行 Rapid PVST 或 PVST 的友商设备互通。当运行 PVST 的 H3C 设备之间互联，或运行 PVST 的 H3C 设备与运行 Rapid PVST 的友商设备互通时，H3C 设备支持像 RSTP 一样的快速收敛。

根据端口类型的不同，PVST 所发送的 BPDU 格式也有所差别：

- 对于 Access 端口，PVST 将根据该 VLAN 的状态发送 STP 格式的 BPDU。
- 对于 Trunk 端口和 Hybrid 端口，PVST 将在 VLAN 1 内根据该 VLAN 的状态发送 STP 格式的 BPDU，而对于其他本端口允许通过的 VLAN，则发送 PVST 格式的 BPDU。

1.1.4 MSTP简介

1. MSTP的产生背景

(1) STP、RSTP 和 PVST 存在的不足

STP 不能快速迁移，即使是在点对点链路或边缘端口，也必须等待两倍的 Forward Delay 的时间延迟，端口才能迁移到转发状态。

RSTP 可以快速收敛，但和 STP 一样还存在如下缺陷：由于局域网内所有 VLAN 都共享一棵生成树，因此所有 VLAN 的报文都沿这棵生成树进行转发，不能按 VLAN 阻塞冗余链路，也无法在 VLAN 间实现数据流量的负载均衡。

对于 PVST 而言，由于每个 VLAN 都需要生成一棵树，因此 PVST BPDU 的通信量将与 Trunk 端口上允许通过的 VLAN 数量成正比。而且当 VLAN 数量较多时，维护多棵生成树的计算量以及资源占用量都将急剧增长，特别是当允许通过很多 VLAN 的 Trunk 端口和 Hybrid 端口的链路状态发生改变时，对应生成树的状态都要重新计算，网络设备的 CPU 将不堪重负。

(2) MSTP 的特点

MSTP 由 IEEE 制定的 802.1s 标准定义，它可以弥补 STP、RSTP 和 PVST 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。MSTP 的特点如下：

- 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。
- MSTP 通过设置 VLAN 与生成树的对应关系表（即 VLAN 映射表），将 VLAN 与生成树联系起来。并通过“实例”的概念，将多个 VLAN 捆绑到一个实例中，从而达到了节省通信开销和降低资源占用率的目的。
- MSTP 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 数据的负载分担。
- MSTP 兼容 STP 和 RSTP，部分兼容 PVST。

2. MSTP的基本概念

图1-4 MSTP 的基本概念示意图

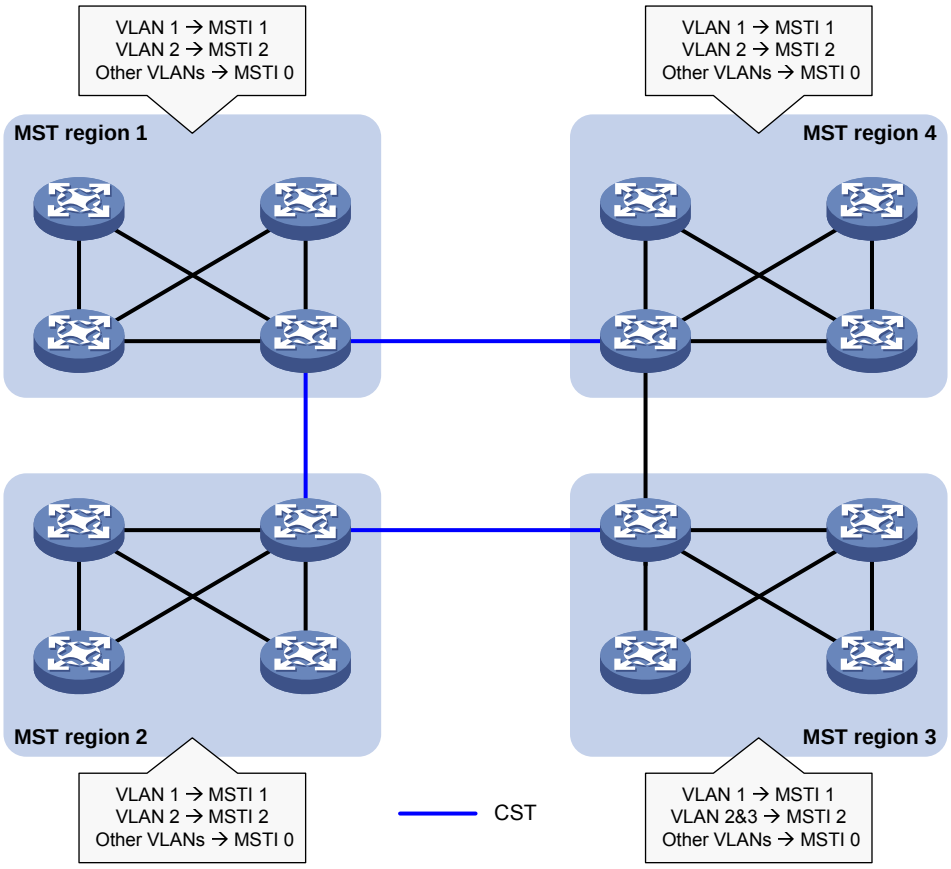
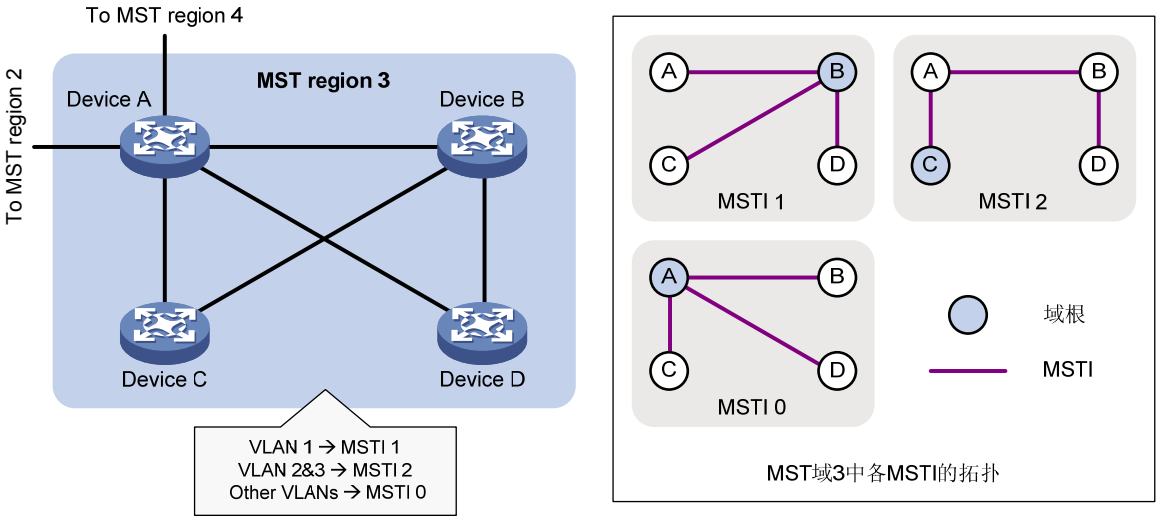


图1-5 MST 域 3 详图



在如 图 1-4 所示的交换网络中有四个MST域，每个MST域都由四台设备构成，所有设备都运行MSTP；为了看清MST域内的情形，我们以MST域 3 为例放大来看，如 图 1-5 所示。下面就结合这两张图来介绍一些MSTP中的基本概念：

(1) MST 域

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台设备以及它们之间的网段所构成。这些设备具有下列特点：

- 都使能了生成树协议。
- 域名相同。
- VLAN 与 MSTI 间映射关系的配置相同。
- MSTP 修订级别的配置相同。
- 这些设备之间有物理链路连通。

一个交换网络中可以存在多个MST域，用户可以通过配置将多台设备划分在一个MST域内。如在 图 1-4 所示的网络中就有MST域 1～MST域 4 这四个MST域，每个域内的所有设备都具有相同的MST域配置。

(2) MSTI

一个MST域内可以通过MSTP生成多棵生成树，各生成树之间彼此独立并分别与相应的VLAN对应，每棵生成树都称为一个MSTI（Multiple Spanning Tree Instance，多生成树实例）。如在 图 1-5 所示的MST域 3 中，包含有三个MSTI：MSTI 1、MSTI 2 和MSTI 0。

(3) VLAN 映射表

VLAN映射表是MST域的一个属性，用来描述VLAN与MSTI间的映射关系。如 图 1-5 中MST域 3 的VLAN映射表就是：VLAN 1 映射到MSTI 1，VLAN 2 和VLAN 3 映射到MSTI 2，其余VLAN映射到MSTI 0。MSTP就是根据VLAN映射表来实现负载分担的。

(4) CST

CST（Common Spanning Tree，公共生成树）是一棵连接交换网络中所有MST域的单生成树。如果把每个MST域都看作一台“设备”，CST就是这些“设备”通过STP协议、RSTP协议计算生成的一棵生成树。如 图 1-4 中的蓝色线条描绘的就是CST。

(5) IST

IST（Internal Spanning Tree，内部生成树）是MST域内的一棵生成树，它是一个特殊的MSTI，通常也称为MSTI 0，所有VLAN缺省都映射到MSTI 0 上。如 图 1-5 中的MSTI 0 就是MST域 3 内的IST。

(6) CIST

CIST（Common and Internal Spanning Tree，公共和内部生成树）是一棵连接交换网络内所有设备的单生成树，所有MST域的IST再加上CST就共同构成了整个交换网络的一棵完整的单生成树，即CIST。如 图 1-4 中各MST域内的IST（即MSTI 0）再加上MST域间的CST就构成了整个网络的CIST。

(7) 域根

域根（Regional Root）就是MST域内IST或MSTI的根桥。MST域内各生成树的拓扑不同，域根也可能不同。如在 图 1-5 所示的MST域 3 中，MSTI 1 的域根为Device B，MSTI 2 的域根为Device C，而MSTI 0（即IST）的域根则为Device A。

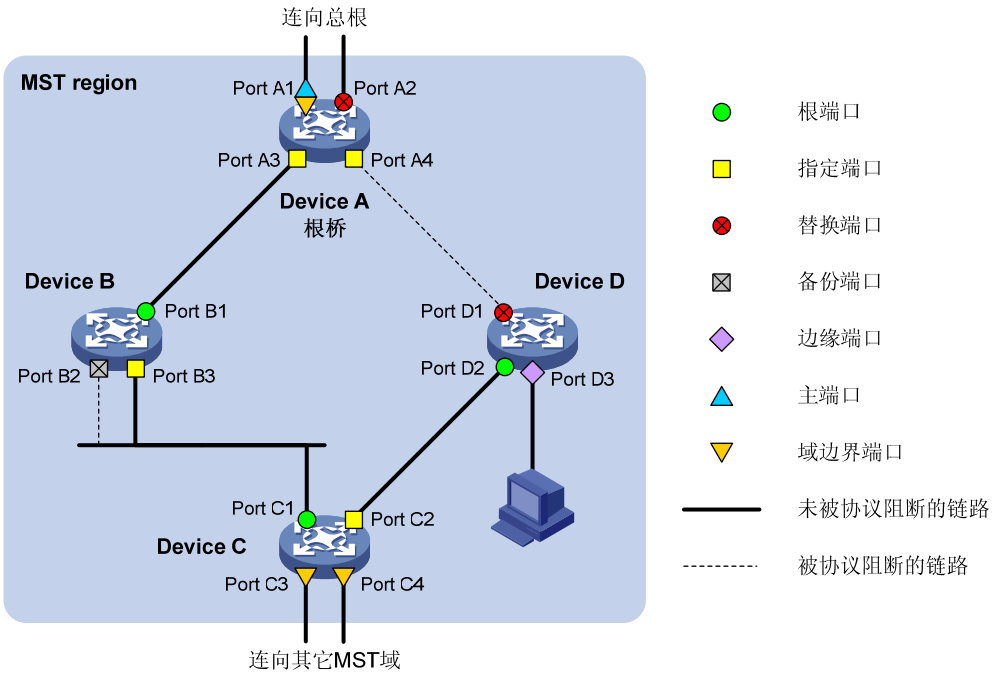
(8) 总根

总根（Common Root Bridge）就是CIST的根桥。如 图 1-4 中CIST的总根就是MST域 1 中的某台设备。

(9) 端口角色

端口在不同的MSTI中可以担任不同的角色。如 图 1-6 所示，在由Device A、Device B、Device C和Device D共同构成的MST域中，Device A的端口Port A1 和Port A2 连向总根方向，Device B的端口Port B2 和Port B3 相连而构成环路，Device C的端口Port C3 和Port C4 连向其他MST域，Device D的端口Port D3 直接连接用户主机。

图1-6 端口角色示意图



如 图 1-6 所示，MSTP计算过程中涉及到的主要端口角色有以下几种：

- 根端口（Root Port）：在非根桥上负责向根桥方向转发数据的端口就称为根端口，根桥上没有根端口。
- 指定端口（Designated Port）：负责向下游网段或设备转发数据的端口就称为指定端口。
- 替换端口（Alternate Port）：是根端口和主端口的备份端口。当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口（Backup Port）：是指定端口的备份端口。当指定端口失效后，备份端口将转换为新的指定端口。当使能了生成树协议的同一台设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 边缘端口（Edge Port）：不与其他设备或网段连接的端口就称为边缘端口，边缘端口一般与用户终端设备直接相连。
- 主端口（Master Port）：是将 MST 域连接到总根的端口（主端口不一定在域根上），位于整个域到总根的最短路径上。主端口是 MST 域中的报文去往总根的必经之路。主端口在 IST/CIST 上的角色是根端口，而在其他 MSTI 上的角色则是主端口。

- 域边界端口（Boundary Port）：是位于 MST 域的边缘、并连接其他 MST 域或 MST 域与运行 STP/RSTP 的区域的端口。主端口同时也是域边界端口。在进行 MSTP 计算时，域边界端口在 MSTI 上的角色与 CIST 的角色一致，但主端口除外——主端口在 CIST 上的角色为根端口，在其他 MSTI 上的角色才是主端口。

(10) 端口状态

MSTP中的端口状态可分为三种，如 表 1-6 所示。同一端口在不同的MSTI中的端口状态可以不同。

表1-6 MSTP 的端口状态

状态	描述
Forwarding	该状态下的端口可以接收和发送BPDU，也转发用户流量
Learning	是一种过渡状态，该状态下的端口可以接收和发送BPDU，但不转发用户流量
Discarding	该状态下的端口可以接收和发送BPDU，但不转发用户流量

端口状态和端口角色是没有必然联系的，表 1-7 给出了各种端口角色能够具有的端口状态（“√”表示此端口角色能够具有此端口状态；“-”表示此端口角色不能具有此端口状态）。

表1-7 各种端口角色具有的端口状态

端口角色 端口状态	根端口/主端口	指定端口	替换端口	备份端口
Forwarding	√	√	-	-
Learning	√	√	-	-
Discarding	√	√	√	√

3. MSTP的基本原理

MSTP 将整个二层网络划分为多个 MST 域，各域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个 MSTI，其中的 MSTI 0 也称为 IST。MSTP 同 STP 一样，使用 BPDU 进行生成树的计算，只是 BPDU 中携带的是设备上 MSTP 的配置信息。

(1) CIST 生成树的计算

通过比较 BPDU 后，在整个网络中选择一个优先级最高的设备作为 CIST 的根桥。在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台设备对待，通过计算在域间生成 CST。CST 和 IST 构成了整个网络的 CIST。

(2) MSTI 的计算

在MST域内，MSTP根据VLAN与MSTI的映射关系，针对不同的VLAN生成不同的MSTI。每棵生成树独立进行计算，计算过程与STP计算生成树的过程类似，请参见“1.1.1 3. STP的基本原理”。

MSTP 中，一个 VLAN 报文将沿着如下路径进行转发：

- 在 MST 域内，沿着其对应的 MSTI 转发；
- 在 MST 域间，沿着 CST 转发。

4. MSTP在设备上的实现

MSTP 同时兼容 STP 和 RSTP。STP 和 RSTP 的协议报文都可以被运行 MSTP 协议的设备识别并应用于生成树计算。设备除了提供 MSTP 的基本功能外，还从用户的角度出发，提供了如下便于管理的特殊功能：

- 根桥保持；
- 根桥备份；
- 根保护功能；
- BPDU 保护功能；
- 环路保护功能；
- 防 TC-BPDU 攻击保护功能；
- 端口角色限制功能；
- TC-BPDU 传播限制功能；
- 支持接口板的热插拔，同时支持主控板与备板的倒换。

1.1.5 协议规范

与生成树相关的协议规范有：

- IEEE 802.1D：Media Access Control (MAC) Bridges
- IEEE 802.1w：Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s：Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees
- IEEE 802.1Q-REV/D1.3：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—Clause 13: Spanning tree Protocols

1.2 生成树配置任务简介

生成树协议包括 STP、RSTP、PVST 和 MSTP 四种类型。在配置生成树之前，首先需明确要使用的生成树协议类型，并规划好各设备在其中的角色（根桥或叶子节点）；然后根据所选择的协议类型及规划好的设备角色，依照本节中的表格进行配置。

1.2.1 STP配置任务简介

表1-8 STP 配置任务简介

配置任务		说明	详细配置
配置根桥	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为STP模式	1.3.1
	配置根桥和备份根桥	可选	1.3.3
	配置设备的优先级	可选	1.3.4
	配置交换网络的网络直径	可选	1.3.6

配置任务		说明	详细配置
	配置生成树的时间参数	可选	1.3.7
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16
配置叶子节点	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为STP模式	1.3.1
	配置设备的优先级	可选	1.3.4
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口的路径开销	可选	1.3.11
	配置端口的优先级	可选	1.3.12
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16
配置生成树保护功能		可选	1.3.20

1.2.2 RSTP配置任务简介

表1-9 RSTP 配置任务简介

配置任务		说明	详细配置
配置根桥	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为RSTP模式	1.3.1
	配置根桥和备份根桥	可选	1.3.3
	配置设备的优先级	可选	1.3.4
	配置交换网络的网络直径	可选	1.3.6
	配置生成树的时间参数	可选	1.3.7
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的链路类型	可选	1.3.13
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16

配置任务		说明	详细配置
配置叶子节点	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为RSTP模式	1.3.1
	配置设备的优先级	可选	1.3.4
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的路径开销	可选	1.3.11
	配置端口的优先级	可选	1.3.12
	配置端口的链路类型	可选	1.3.13
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16
执行mCheck操作		可选	1.3.17
配置生成树保护功能		可选	1.3.20

1.2.3 PVST配置任务简介

表1-10 PVST 配置任务简介

配置任务		说明	详细配置
配置根桥	配置生成树的工作模式	必选 生成树缺省工作在MSTP模式下，通过本配置将其工作模式配置为PVST模式	1.3.1
	配置根桥和备份根桥	可选	1.3.3
	配置设备的优先级	可选	1.3.4
	配置交换网络的网络直径	可选	1.3.6
	配置生成树的时间参数	可选	1.3.7
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的链路类型	可选	1.3.13
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	错误！未找到引用源。

配置任务		说明	详细配置
配置叶子节点	配置生成树的工作模式	必选 生成树缺省工作在MSTP模式下，通过本配置将其工作模式配置为PVST模式	1.3.1
	配置设备的优先级	可选	1.3.4
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的路径开销	可选	1.3.11
	配置端口的优先级	可选	1.3.12
	配置端口的链路类型	可选	1.3.13
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16
执行mCheck操作		可选	1.3.17
配置生成树保护功能		可选	1.3.20

1.2.4 MSTP配置任务简介

表1-11 MSTP 配置任务简介

配置任务		说明	详细配置
配置根桥	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为MSTP模式	1.3.1
	配置MST域	必选	1.3.2
	配置根桥和备份根桥	可选	1.3.3
	配置设备的优先级	可选	1.3.4
	配置MST域的最大跳数	可选	1.3.5
	配置交换网络的网络直径	可选	1.3.6
	配置生成树的时间参数	可选	1.3.7
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的链路类型	可选	1.3.13
	配置端口收发的MSTP报文格式	可选	1.3.14
	打开端口状态变化信息显示开关	可选	1.3.15

配置任务		说明	详细配置
	使能生成树协议	必选	1.3.16
配置叶子节点	配置生成树的工作模式	必选 通过本配置将生成树的工作模式配置为MSTP模式	1.3.1
	配置MST域	必选	1.3.2
	配置设备的优先级	可选	1.3.4
	配置超时时间因子	可选	1.3.8
	配置端口发送BPDU的速率	可选	1.3.9
	配置端口为边缘端口	可选	1.3.10
	配置端口的路径开销	可选	1.3.11
	配置端口的优先级	可选	1.3.12
	配置端口的链路类型	可选	1.3.13
	配置端口收发的MSTP报文格式	可选	1.3.14
	打开端口状态变化信息显示开关	可选	1.3.15
	使能生成树协议	必选	1.3.16
执行mCheck操作		可选	1.3.17
配置摘要侦听功能		可选	1.3.18
配置No Agreement Check功能		可选	1.3.19
配置生成树保护功能		可选	1.3.20

1.3 配置生成树

1.3.1 配置生成树的工作模式

生成树的工作模式有以下几种：

- STP 模式：设备的所有端口都将向外发送 STP BPDU。如果端口的对端设备只支持 STP，可选择此模式。
- RSTP 模式：设备的所有端口都向外发送 RSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 MSTP BPDU，则不会进行迁移。
- PVST 模式：设备的所有端口都向外发送 PVST BPDU，每个 VLAN 对应一棵生成树。进行 PVST 组网时，若网络中所有设备的生成树维护量（使能生成树协议的 VLAN 数×使能生成树协议的端口数）达到一定数量，会导致 CPU 负荷过重，不能正常处理报文，引起网络震荡。
- MSTP 模式：设备的所有端口都向外发送 MSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 RSTP BPDU，则不会进行迁移。

MSTP 模式兼容 RSTP 模式，RSTP 模式兼容 STP 模式，PVST 模式与其他模式的兼容性如下：

- 对于 Access 端口：PVST 模式在任意 VLAN 中都能与其他模式互相兼容。

- 对于 Trunk 端口或 Hybrid 端口：PVST 模式仅在 VLAN 1 中能与其他模式互相兼容。

需要注意的是，在各工作模式下进行配置时，对是否需要指定 MSTI 或 VLAN 的要求不同：

- 在 STP 模式或 RSTP 模式下无需指定 MSTI 和 VLAN，若指定了 MSTI 或 VLAN，则该配置无效。
- 在 PVST 模式下，若指定了 VLAN 则表示针对该 VLAN 进行配置，若未指定 VLAN 则该配置无效。
- 在 MSTP 模式下，若指定了 MSTI 则表示针对该 MSTI 进行配置，若指定 VLAN 则该配置无效；若 MSTI 和 VLAN 均未指定，则表示针对 CIST 进行配置。

表1-12 配置生成树的工作模式

操作	命令	说明
进入系统视图	**system-view**	-
配置生成树的工作模式	**stp mode { mstp | pvst | rstp | stp }**	缺省情况下，生成树的工作模式为MSTP模式

1.3.2 配置MST域

两台或多台使能了生成树协议的设备若要属于同一个 MST 域，必须同时满足以下两个条件：第一是选择因子（取值为 0，不可配）、域名、修订级别和 VLAN 映射表的配置都相同；第二是这些设备之间的链路相通。

在配置 MST 域的相关参数（特别是 VLAN 映射表）时，会引发生成树的重新计算，从而引起网络拓扑的振荡。为了减少网络振荡，新配置的 MST 域参数并不会马上生效，而是在使用 **active region-configuration** 命令激活，或使用命令 **stp global enable** 全局使能生成树协议后才会生效。

配置 MST 域时，需要注意的是，在 STP/RSTP/PVST 模式下，MST 域的相关配置不会生效。

表1-13 配置 MST 域

操作	命令	说明
进入系统视图	**system-view**	-
进入MST域视图	**stp region-configuration**	-
配置MST域的域名	**region-name** *name*	缺省情况下，MST域的域名为设备的MAC地址
配置VLAN映射表	**instance** *instance-id* **vlan** *vlan-id-list*	二者选其一 缺省情况下，所有VLAN都映射到CIST（即MSTI 0）上
	vlan-mapping modulo *modulo*	
配置MSTP的修订级别	**revision-level** *level*	缺省情况下，MSTP的修订级别为0
（可选）显示MST域的预配置信息	**check region-configuration**	-
激活MST域的配置	**active region-configuration**	-

1.3.3 配置根桥和备份根桥

可以通过计算来自动确定生成树的根桥，用户也可以手工将设备配置为指定生成树的根桥或备份根桥：

- 设备在各生成树中的角色互相独立，在作为一棵生成树的根桥或备份根桥的同时，也可以作为其他生成树的根桥或备份根桥；但在同一棵生成树中，一台设备不能既作为根桥，又作为备份根桥。
- 在一棵生成树中，生效的根桥只有一个；当两台或两台以上的设备被指定为同一棵生成树的根桥时，系统将选择 MAC 地址最小的设备作为根桥。
- 可以在每棵生成树中指定多个备份根桥。当根桥出现故障或被关机时，备份根桥可以取代根桥成为指定生成树的根桥；但此时若配置了新的根桥，则备份根桥将不会成为根桥。如果配置了多个备份根桥，则 MAC 地址最小的备份根桥将成为指定生成树的根桥。
- 用户可以为每棵生成树指定一个根桥，而无需关心设备的优先级配置。当设备一旦被配置为根桥或者备份根桥之后，便不能再修改该设备的优先级。也可以通过配置设备的优先级为 0 来实现将当前设备指定为根桥的目的。有关设备优先级的配置，请参见“1.3.4 ”。

1. 配置根桥

请在欲配置为根桥的设备上进行如下配置。

表1-14 配置根桥

操作	命令	说明
进入系统视图	**system-view**	-
配置当前设备为根桥	STP/RSTP模式： **stp root primary**	缺省情况下，设备不是根桥
	PVST模式： **stp vlan** *vlan-id-list* **root primary**	
	MSTP模式： **stp** [**instance** *instance-list*] **root primary**	

2. 配置备份根桥

请在欲配置为备份根桥的设备上进行如下配置。

表1-15 配置备份根桥

操作	命令	说明
进入系统视图	**system-view**	-
配置当前设备为备份根桥	STP/RSTP模式： **stp root secondary**	缺省情况下，设备不是备份根桥
	PVST模式： **stp vlan** *vlan-id-list* **root secondary**	
	MSTP模式： **stp** [**instance** *instance-list*] **root secondary**	

1.3.4 配置设备的优先级

设备的优先级参与生成树计算，其大小决定了该设备是否能够被选作生成树的根桥。数值越小表示优先级越高，通过配置较小的优先级，可以达到指定某台设备成为生成树根桥的目的。可以在不同的生成树中为设备配置不同的优先级。如果设备的优先级相同，则 MAC 地址最小的设备将被选择为根。当指定设备为根桥或者备份根桥之后，不允许再修改该设备的优先级。

表1-16 配置设备的优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置设备的优先级	STP/RSTP模式： **stp priority** *priority*	缺省情况下，设备的优先级为32768
	PVST模式： **stp vlan** *vlan-id-list* **priority** *priority*	
	MSTP模式： **stp** [**instance** *instance-list*] **priority** *priority*	

1.3.5 配置MST域的最大跳数

MST 域的最大跳数限制了 MST 域的规模，在域根上配置的最大跳数将作为该 MST 域的最大跳数。

从 MST 域内的生成树的根桥开始，域内的 BPDU 每经过一台设备的转发，跳数就被减 1；设备将丢弃跳数为 0 的 BPDU，以使处于最大跳数外的设备无法参与生成树的计算，从而限制了 MST 域的规模。

本配置只需在根桥设备上进行，非根桥设备将采用根桥设备的配置值。

用户可以根据设计的 MST 域内拓扑的层数来配置 MST 域的最大跳数，MST 域的最大跳数要大于 MST 域内拓扑的最大层数。

表1-17 配置 MST 域的最大跳数

操作	命令	说明
进入系统视图	**system-view**	-
配置MST域的最大跳数	**stp max-hops** *hops*	缺省情况下，MST域的最大跳数为20

1.3.6 配置交换网络的网络直径

交换网络中任意两台终端设备都通过特定路径彼此相连，这些路径由一系列的设备构成。网络直径就是指对于交换网络中的任意两台网络边缘设备，其中一台经过根桥到达另一台所经过的最大设备数。网络直径越大，说明网络的规模越大。

在配置了网络直径之后，系统会通过计算自动将设备的 Hello Time、Forward Delay 和 Max Age 三个时间参数设置为最优值。在 STP/RSTP/MSTP 模式下，每个 MST 域将被视为一台设备，且网络直径配置只对 CIST 有效（即只能在总根上生效），而对 MSTI 无效。在 PVST 模式下，网络直径的配置只能在指定 VLAN 的根桥上生效。

表1-18 配置交换网络的网络直径

操作	命令	说明
进入系统视图	**system-view**	-
配置交换网络的网络直径	STP/RSTP/MSTP模式： **stp bridge-diameter** *diameter*	缺省情况下，交换网络的网络直径为7
	PVST模式： **stp vlan** *vlan-id-list* **bridge-diameter** *diameter*	

1.3.7 配置生成树的时间参数

在生成树的计算过程中，用到了以下三个时间参数：

(1) Forward Delay：用于确定状态迁移的延迟时间。为了防止产生临时环路，生成树协议在端口由 Discarding 状态向 Forwarding 状态迁移的过程中设置了 Learning 状态作为过渡，并规定状态迁移需要等待 Forward Delay 时间，以保持与远端的设备状态切换同步。

(2) Hello Time：用于检测链路是否存在故障。生成树协议每隔 Hello Time 时间会发送 BPDU，以确认链路是否存在故障。如果设备在 Hello Time 时间内没有收到 BPDU，则会由于消息超时而重新计算生成树。

(3) Max Age：用于确定 BPDU 是否超时。在 MSTP 的 CIST 上，设备根据 Max Age 时间来确定端口收到的 BPDU 是否超时。如果端口收到的 BPDU 超时，则需要对该 MSTI 重新计算。Max Age 时间对 MSTP 的 MSTI 无效。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。上述三个时间参数之间应满足以下关系，否则会引起网络的频繁震荡：

- 2×（Forward Delay－1 秒）≥Max Age
- Max Age≥2×（Hello Time＋1 秒）

配置生成树时间参数时，需要注意：

- Forward Delay 的长短与交换网络的网络直径有关。一般来说，网络直径越大，Forward Delay 就应该越长。如果 Forward Delay 过短，可能引入临时的冗余路径；如果 Forward Delay 过长，网络可能较长时间不能恢复连通。建议用户采用自动计算值。
- 合适的 Hello Time 可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果 Hello Time 过长，在链路发生丢包时，设备会误以为链路出现了故障，从而引发设备重新计算生成树；如果 Hello Time 过短，设备将频繁发送重复的 BPDU，增加了设备的负担，浪费了网络资源。建议用户采用自动计算值。
- 如果 Max Age 过短，设备会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果 Max Age 过长，设备很可能不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力。建议用户采用自动计算值。

通常情况下，不建议通过手工配置直接调整上述三个时间参数。由于这三个时间参数的取值与网络规模有关，生成树协议会自动根据网络直径计算出这三个时间参数的最优值，因此在网络拓扑变化时，建议在设备上通过执行 **stp bridge-diameter** 命令调整网络直径，使设备自动调整这三个时间参数的值。当网络直径取缺省值时，这三个时间参数也分别取其各自的缺省值。

本配置只需在根桥设备上进行，整个交换网络中的所有设备都将采用根桥设备的配置值。

表1-19 配置生成树的时间参数

操作	命令	说明
进入系统视图	**system-view**	-
配置Forward Delay时间参数	STP/RSTP/MSTP模式： **stp timer forward-delay** *time*	缺省情况下，Forward Delay为15秒
	PVST模式： **stp vlan** *vlan-id-list* **timer forward-delay** *time*	
配置Hello Time时间参数	STP/RSTP/MSTP模式： **stp timer hello** *time*	缺省情况下，Hello Time为2秒
	PVST模式： **stp vlan** *vlan-id-list* **timer hello** *time*	
配置Max Age时间参数	STP/RSTP/MSTP模式： **stp timer max-age** *time*	缺省情况下，Max Age为20秒
	PVST模式： **stp vlan** *vlan-id-list* **timer max-age** *time*	

1.3.8 配置超时时间因子

超时时间因子用来确定设备的超时时间：超时时间＝超时时间因子×3×Hello Time。

当网络拓扑结构稳定后，非根桥设备会每隔 Hello Time 时间向周围相连设备转发根桥发出的 BPDU 以确认链路是否存在故障。通常如果设备在 9 倍的 Hello Time 时间内没有收到上游设备发来的 BPDU，就会认为上游设备已经故障，从而重新进行生成树的计算。

有时设备在较长时间内收不到上游设备发来的 BPDU，可能是由于上游设备的繁忙导致的，在这种情况下一般不应重新进行生成树的计算。因此在稳定的网络中，可以通过延长超时时间来减少网络资源的浪费。在一个稳定的网络中，建议将超时时间因子配置为 5～7。

表1-20 配置超时时间因子

操作	命令	说明
进入系统视图	**system-view**	-
配置设备的超时时间因子	**stp timer-factor** *factor*	缺省情况下，设备的超时时间因子为3

1.3.9 配置端口发送BPDU的速率

每 Hello Time 时间内端口能够发送的 BPDU 的最大数目＝端口发送 BPDU 的速率＋Hello Time 时间值。端口发送 BPDU 的速率与端口的物理状态和网络结构有关，用户可以根据实际的网络情况对其进行配置。

端口发送 BPDU 的速率越高，每个 Hello Time 内可发送的 BPDU 数量就越多，占用的系统资源也越多。适当配置发送速率一方面可以限制端口发送 BPDU 的速度，另一方面还可以防止在网络拓扑动荡时，生成树协议占用过多的带宽资源。建议用户采用缺省配置。

表1-21 配置端口的最大发送速率

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的发送BPDU的速率	**stp transmit-limit** *limit*	缺省情况下，端口发送BPDU的速率为10

1.3.10 配置端口为边缘端口

当端口直接与用户终端相连，而没有连接到其他设备或共享网段上，则该端口被认为是边缘端口。网络拓扑变化时，边缘端口不会产生临时环路。

由于设备无法知道端口是否直接与终端相连，所以需要用户手工将端口配置为边缘端口。如果用户将某个端口配置为边缘端口，那么当该端口由阻塞状态向转发状态迁移时，这个端口可以实现快速迁移，而无需等待延迟时间。

对于直接与终端相连的端口，请将该端口设置为边缘端口，同时使能 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。

配置端口为边缘端口时，需要注意：

- 在同一个端口上，不允许同时配置边缘端口和环路保护功能。
- 在设备没有使能 BPDU 保护的情况下，如果被设置为边缘端口的端口上收到来自其他端口的 BPDU，则该端口会重新变为非边缘端口。此时，只有重启端口才能将该端口恢复为边缘端口。

表1-22 配置端口为边缘端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置当前端口为边缘端口	**stp edged-port**	缺省情况下，端口为非边缘端口

1.3.11 配置端口的路径开销

路径开销（Path Cost）是与端口相连的链路速率相关的参数。在支持生成树协议的设备上，端口在不同的 MSTI 中可以拥有不同的路径开销。设置合适的路径开销可以使不同 VLAN 的流量沿不同的物理链路转发，从而实现按 VLAN 负载分担的功能。

设备可以自动计算端口的缺省路径开销，用户也可以直接配置端口的路径开销。

1. 配置缺省路径开销的计算标准

缺省路径开销的计算标准有以下三种，用户可以通过本配置来改变设备自动计算端口的缺省路径开销时所采用的计算标准：

- **dot1d-1998**：表示按照 IEEE 802.1D-1998 标准来计算缺省路径开销。
- **dot1t**：表示按照 IEEE 802.1t 标准来计算缺省路径开销。
- **legacy**：表示按照私有标准来计算缺省路径开销。

需要注意的是，改变缺省路径开销的计算标准，将使端口的路径开销值恢复为缺省值。

表1-23 配置缺省路径开销的计算标准

操作	命令	说明
进入系统视图	**system-view**	-
配置缺省路径开销的计算标准	**stp pathcost-standard { dot1d-1998 | dot1t | legacy }**	缺省情况下，缺省路径开销的计算标准为 **legacy**

链路速率与路径开销值的对应关系如 表 1-24 所示。

表1-24 链路速率与端口路径开销值的对应关系表

链路速率	端口类型	端口的路径开销值		
		IEEE 802.1D-1998	IEEE 802.1t	私有标准
0	-	65535	200,000,000	200,000
10Mbps	单个端口	100	2,000,000	2,000
	聚合接口（含两个选中端口）		1,000,000	1,800
	聚合接口（含三个选中端口）		666,666	1,600
	聚合接口（含四个选中端口）		500,000	1,400
100Mbps	单个端口	19	200,000	200
	聚合接口（含两个选中端口）		100,000	180
	聚合接口（含三个选中端口）		66,666	160
	聚合接口（含四个选中端口）		50,000	140
1000Mbps	单个端口	4	20,000	20
	聚合接口（含两个选中端口）		10,000	18
	聚合接口（含三个选中端口）		6,666	16
	聚合接口（含四个选中端口）		5,000	14

链路速率	端口类型	端口的路径开销值		
		IEEE 802.1D-1998	IEEE 802.1t	私有标准
10Gbps	单个端口	2	2,000	2
	聚合接口（含两个选中端口）		1,000	1
	聚合接口（含三个选中端口）		666	1
	聚合接口（含四个选中端口）		500	1
20Gbps	单个端口	1	1,000	1
	聚合接口（含两个选中端口）		500	1
	聚合接口（含三个选中端口）		333	1
	聚合接口（含四个选中端口）		250	1
40Gbps	单个端口	1	500	1
	聚合接口（含两个选中端口）		250	1
	聚合接口（含三个选中端口）		166	1
	聚合接口（含四个选中端口）		125	1
100Gbps	单个端口	1	200	1
	聚合接口（含两个选中端口）		100	1
	聚合接口（含三个选中端口）		66	1
	聚合接口（含四个选中端口）		50	1

说明

- 在计算聚合接口的路径开销时，IEEE 802.1D-1998 标准不考虑聚合接口所对应聚合组内选中端口的数量；而 IEEE 802.1t 标准则对此予以考虑，其计算公式为：端口的路径开销 = 200000000 ÷ 链路速率（单位为 100Kbps），其中链路速率为聚合接口所对应聚合组内选中端口的速率之和。
- 当端口的链路速率大于 10Gbps、且缺省路径开销的计算标准为IEEE 802.1D-1998 或私有标准时，单个端口和聚合接口的路径开销值都会取所选标准规定的最小值，这将影响转发路径选择的合理性。在这种情况下，建议将缺省路径开销的计算标准配置为IEEE 802.1t，或手工配置端口的路径开销（请参见“1.3.11 2. 配置端口的路径开销”）。

2. 配置端口的路径开销

需要注意的是，当端口的路径开销值改变时，系统将重新计算端口的角色并进行状态迁移。

表1-25 配置端口的路径开销

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置端口的路径开销	STP/RSTP模式： **stp cost** *cost*	缺省情况下，自动按照相应的标准计算各生成树上的路径开销
	PVST模式： **stp vlan** *vlan-id-list* **cost** *cost*	
	MSTP模式： **stp** [**instance** *instance-list*] **cost** *cost*	

3. 配置举例

在 MSTP 模式下，配置按照 IEEE 802.1D-1998 标准来计算缺省路径开销，并配置端口 GigabitEthernet2/1/3 在 MSTI 2 上的路径开销值为 200。

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated.
[Sysname] interface gigabitethernet 2/1/3
[Sysname-GigabitEthernet2/1/3] stp instance 2 cost 200
```

在 PVST 模式下，配置设备按照 IEEE 802.1D-1998 标准来计算缺省路径开销，并配置端口 GigabitEthernet2/1/3 在 PVST VLAN 20～30 上的路径开销为 2000。

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated
[Sysname] interface gigabitethernet 2/1/3
[Sysname-GigabitEthernet2/1/3] stp vlan 20 to 30 cost 2000
```

1.3.12 配置端口的优先级

端口优先级是确定该端口是否会被选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。在支持生成树协议的设备上，端口可以在不同的生成树中拥有不同的优先级，同一端口可以在不同的生成树中担任不同的角色，从而使不同 VLAN 的数据沿不同的物理路径传播，实现按 VLAN 进行负载分担的功能。用户可以根据组网的实际需要来设置端口的优先级。

需要注意的是，当端口的优先级改变时，系统将重新计算端口的角色并进行状态迁移。

表1-26 配置端口的优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的优先级	STP/RSTP模式： **stp port priority** *priority*	缺省情况下，端口的优先级为128

操作	命令	说明
	PVST模式： **stp vlan** *vlan-id-list* **port priority** *priority*	
	MSTP模式： **stp** [**instance** *instance-list*] **port priority** *priority*	

1.3.13 配置端口的链路类型

点对点链路是两台设备之间直接连接的链路。与点对点链路相连的两个端口如果为根端口或者指定端口，则端口可以通过传送同步报文（Proposal 报文和 Agreement 报文）快速迁移到转发状态，减少了不必要的转发延迟时间。

在 PVST 或 MSTP 模式下，如果某端口被配置为与点对点链路（或非点对点链路）相连，那么该配置对该端口所属的所有 VLAN 或 MSTI 都有效。

需要注意的是，如果某端口被配置为与点对点链路相连，但与该端口实际相连的物理链路不是点对点链路，则有可能引入临时回路。

表1-27 配置端口的链路类型

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型	**stp point-to-point** { **auto** | **force-false** | **force-true** }	缺省情况下，端口的链路类型为**auto**，即由系统自动检测与本端口相连的链路是否为点对点链路

1.3.14 配置端口收发的MSTP报文格式

端口可以收发的 MSTP 报文格式有两种：

- **dot1s**：符合 802.1s 协议的标准格式；
- **legacy**：与非标准格式兼容的格式。

端口默认配置为自动识别方式（**auto**），即可以自动识别这两种格式的 MSTP 报文，并根据识别结果确定发送报文的格式，从而实现与对端设备的互通。

用户也可以通过配置改变端口发送的 MSTP 报文格式，使端口只发送与所配格式相符的 MSTP 报文，实现与对端只识别特定格式报文的设备互通。

当端口处于 auto 模式时，默认发送 802.1s 标准的报文。在此模式下，为避免因收到不同格式的 MSTP 报文而导致端口发送的报文格式频繁变化，端口一旦收到私有格式报文就将一直以该格式发送报文。若想使该端口恢复发送 802.1s 标准的报文，可对其依次执行关闭/开启操作。

需要注意的是，如果当前配置的 MSTI 大于 48，端口将只发送 802.1s 标准的 MSTP 报文。

表1-28 配置端口收发的 MSTP 报文格式

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口收发的MSTP报文格式	**stp compliance** { **auto** | **dot1s** | **legacy** }	缺省情况下，端口会自动识别收到的MSTP报文格式并根据识别结果确定发送的报文格式

1.3.15 打开端口状态变化信息显示开关

在使能了生成树协议的大型网络中，用户可以通过打开端口状态变化信息显示开关，使系统输出端口状态变化的相关信息，方便用户对端口状态进行实时监控。

表1-29 打开端口状态变化信息显示开关

操作	命令	说明
进入系统视图	**system-view**	-
打开端口状态变化信息显示开关	STP/RSTP模式： **stp port-log instance 0**	缺省情况下，端口状态变化信息显示开关处于关闭状态
	PVST模式： **stp port-log vlan** *vlan-id-list*	
	MSTP模式： **stp port-log** { **all** | **instance** *instance-list* }	

1.3.16 使能生成树协议

只有使能了生成树协议，生成树的其他配置才会生效。在 STP/RSTP/MSTP 模式下，必须保证全局和端口上的生成树协议均处于使能状态；在 PVST 模式下，必须保证全局、VLAN 和端口上的生成树协议均处于使能状态。

需要注意的是，可以通过 **undo stp enable** 命令关闭指定端口的生成树协议，使其不参与生成树计算，以节省设备的 CPU 资源。但必须保证指定的端口关闭生成树协议后，网络中不能出现环路。

表1-30 使能生成树协议（STP/RSTP/MSTP 模式）

操作	命令	说明
进入系统视图	**system-view**	-
全局使能生成树协议	**stp global enable**	缺省情况下，生成树协议的全局状态为关闭
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
在端口上使能生成树协议	**stp enable**	缺省情况下，所有端口上的生成树协议均处于使能状态

表1-31 使能生成树协议（PVST 模式）

操作	命令	说明
进入系统视图	**system-view**	-
全局使能生成树协议	**stp global enable**	缺省情况下，生成树协议的全局状态为关闭
在VLAN中使能生成树协议	**stp vlan** *vlan-id-list* **enable**	缺省情况下，生成树协议在VLAN中为使能状态
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
在端口上使能生成树协议	**stp enable**	缺省情况下，所有端口上的生成树协议均处于使能状态

1.3.17 执行mCheck操作

生成树的工作模式有 STP 模式、RSTP 模式、PVST 模式和 MSTP 模式四种。在运行 RSTP、PVST 或 MSTP 的设备上，若某端口连接着运行 STP 协议的设备，该端口收到 STP 报文后会自动迁移到 STP 模式；但当对端运行 STP 协议的设备关机或撤走，而该端口又无法感知的情况下，该端口将无法自动迁移回原有模式，此时需要通过执行 mCheck 操作将其手工迁移回原有模式。

当运行 STP 的设备 A、未使能生成树协议的设备 B 和运行 RSTP/PVST/MSTP 的设备 C 三者顺次相连时，设备 B 将透传 STP 报文，设备 C 上连接设备 B 的端口将迁移到 STP 模式。在设备 B 上使能生成树协议后，若想使设备 B 与设备 C 之间运行 RSTP/PVST/MSTP 协议，除了要在设备 B 上配置生成树的工作模式为 RSTP/PVST/MSTP 外，还要在设备 B 与设备 C 相连的端口上都执行 mCheck 操作。

可以在全局或在端口上执行 mCheck 操作。

执行 mCheck 操作时，需要注意，只有当生成树的工作模式为 RSTP 模式、PVST 模式或 MSTP 模式时执行 mCheck 操作才有效。

1. 全局执行mCheck操作

表1-32 全局执行 mCheck 操作

操作	命令	说明
进入系统视图	**system-view**	-
全局执行mCheck操作	**stp global mcheck**	-

2. 在端口上执行mCheck操作

表1-33 在端口上执行 mCheck 操作

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
在端口上执行mCheck操作	**stp mcheck**	-

1.3.18 配置摘要侦听功能

1. 功能简介

根据 IEEE 802.1s 规定，只有在 MST 域配置（包括域名、修订级别和 VLAN 映射关系）完全一致的情况下，相连的设备才被认为是在同一个域内。当设备使能了生成树协议以后，设备之间通过识别 BPDU 数据报文内的配置 ID 来判断相连的设备是否与自己处于相同的 MST 域内；配置 ID 包含域名、修订级别、配置摘要等内容，其中配置摘要长 16 字节，是由 HMAC-MD5 算法将 VLAN 与 MSTI 的映射关系加密计算而成。

在网络中，由于一些厂商的设备在对生成树协议的实现上存在差异，即用加密算法计算配置摘要时采用私有的密钥，从而导致即使 MST 域配置相同，不同厂商的设备之间也不能实现在 MST 域内的互通。

通过在我方设备与对生成树协议的实现存在差异的第三方厂商设备相连的端口上使能摘要侦听功能，可以实现我方设备与这些厂商设备在 MST 域内的完全互通。

2. 配置限制和指导

- 摘要侦听功能在端口生效后，由于不再通过配置摘要的比较计算来判断是否在同一个域内，因此需要保证互连设备的域配置中 VLAN 与 MSTI 映射关系的配置相同。
- 全局使能摘要侦听功能后，如果要修改 VLAN 与 MSTI 间的映射关系，或执行 **undo stp region-configuration** 命令取消当前域配置，均可能因与邻接设备的 VLAN 和 MSTI 映射关系不一致而导致环路或流量中断，因此请谨慎操作。
- 只有当全局和端口上都使能了摘要侦听功能后，该功能才能生效。使能摘要侦听功能时，建议先在所有与第三方厂商设备相连的端口上使能该功能，再全局使能该功能，以一次性让所有端口的配置生效，从而减少对网络的冲击。
- 请不要在 MST 域的边界端口上使能摘要侦听功能，否则可能会导致环路。
- 建议配置完摘要侦听功能后再使能生成树协议。在网络稳定的情况下不要进行摘要侦听功能的配置，以免造成临时的流量中断。

3. 配置准备

我方设备与第三方厂商设备相连，网络配置正确，生成树协议正常运行。

4. 配置步骤

只有当我方设备与对生成树协议的实现存在差异的第三方厂商设备（即采用私有密钥来计算配置摘要）互连时，才有必要配置本功能。

表1-34 配置摘要侦听功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-

配置步骤	命令	说明
在端口上使能摘要侦听功能	**stp config-digest-snooping**	缺省情况下，端口上的摘要侦听功能处于关闭状态
退回系统视图	**quit**	-
全局使能摘要侦听功能	**stp global config-digest-snooping**	缺省情况下，摘要侦听功能处于全局关闭状态

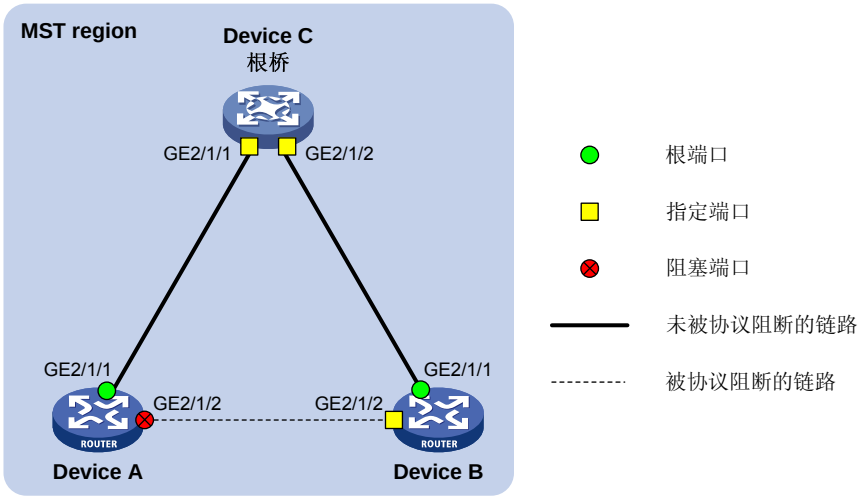
5. 配置举例

(1) 组网需求

- Device A 和 Device B 分别与对生成树协议的实现存在差异的第三方厂商设备 Device C 相连并配置在同一域内。
- 分别在 Device A 和 Device B 各自与 Device C 相连的端口上使能摘要侦听功能，实现 Device A、Device B 和 Device C 在 MST 域内的互通。

(2) 组网图

图1-7 摘要侦听功能配置组网图



(3) 配置步骤

在 Device A 的端口 GigabitEthernet2/1/1 上使能摘要侦听功能，并全局使能摘要侦听功能。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] stp config-digest-snooping
[DeviceA-GigabitEthernet2/1/1] quit
[DeviceA] stp global config-digest-snooping
```

在 Device B 的端口 GigabitEthernet2/1/1 上使能摘要侦听功能，并全局使能摘要侦听功能。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] stp config-digest-snooping
[DeviceB-GigabitEthernet2/1/1] quit
```

```
[DeviceB] stp global config-digest-snooping
```

1.3.19 配置No Agreement Check功能

1. 功能简介

RSTP 和 MSTP 的指定端口快速迁移机制使用两种协议报文：

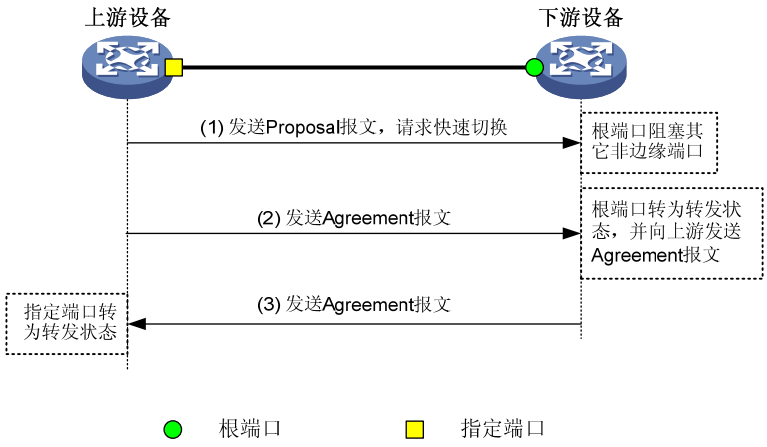
- Proposal 报文：指定端口请求快速迁移的报文。
- Agreement 报文：同意对端进行快速迁移的报文。

RSTP 和 MSTP 均要求上游设备的指定端口在接收到下游设备的 Agreement 报文后才能进行快速迁移。不同之处如下：

- 对于 MSTP，上游设备先向下游设备发送 Agreement 报文，而下游设备的根端口只有在收到了上游设备的 Agreement 报文后才会向上游设备回应 Agreement 报文。
- 对于 RSTP，下游设备无需等待上游设备发送 Agreement 报文就可向上游设备发送 Agreement 报文。

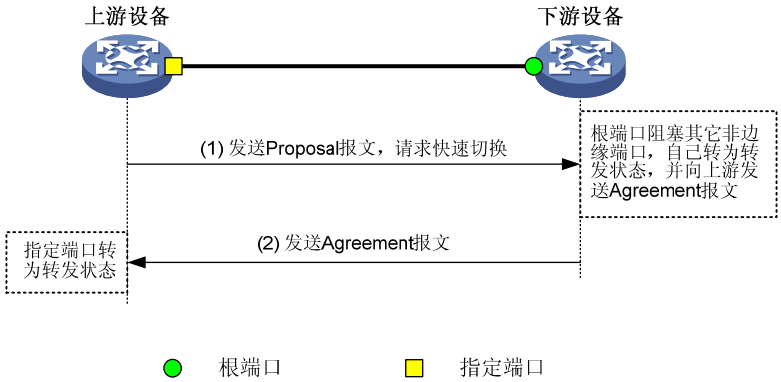
如 图 1-8 所示，是MSTP的指定端口快速迁移机制。

图1-8 MSTP 指定端口快速迁移机制



如 图 1-9 所示，是RSTP的指定端口快速迁移机制。

图1-9 RSTP 指定端口快速迁移机制



当我方设备与作为上游设备且与对生成树协议的实现存在差异的第三方厂商设备互联时，二者在快速迁移的配合上可能会存在一定的限制。例如：上游设备指定端口的状态迁移实现机制与 RSTP 类似；而下游设备运行 MSTP 并且不工作在 RSTP 模式时，由于下游设备的根端口接收不到上游设备的 Agreement 报文，它不会向上游设备发 Agreement 报文，所以上游设备的指定端口无法实现状态的快速迁移，只能在 2 倍的 Forward Delay 延时后变成转发状态。

通过在我方设备与对生成树协议的实现存在私有性差异的上游第三方厂商设备相连的端口上使能 No Agreement Check 功能，可避免这种情况的出现，使得上游的第三方厂商设备的指定端口能够进行状态的快速迁移。

2. 配置准备

- 设备与作为上游设备且支持生成树协议的第三方厂商设备互连，并且端口之间为点对点链路。
- 为我方设备与第三方厂商设备配置相同的域名、域配置修订级别和VLAN与MSTI的映射关系，以确保它们在同一个域内。

3. 配置功能

请在设备的根端口上进行如下配置，且本功能只有在根端口上配置才会生效。

表1-35 配置 No Agreement Check 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能No Agreement Check功能	**stp no-agreement-check**	缺省情况下，No Agreement Check功能处于关闭状态

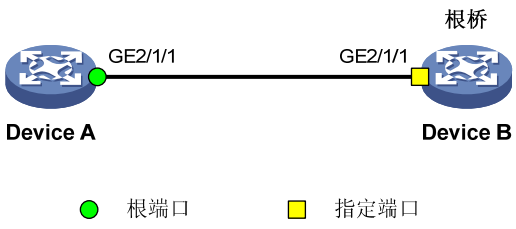
4. 配置举例

(1) 组网需求

- Device A 与对生成树协议的实现存在差异的第三方厂商设备 Device B 互连并配置在同一域内。
- Device B 作为域根，Device A 作为下游设备。

(2) 组网图

图1-10 No Agreement Check 功能配置组网图



(3) 配置步骤

在 Device A 的端口 GigabitEthernet2/1/1 上使能 No Agreement Check 功能。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] stp no-agreement-check
```

1.3.20 配置生成树保护功能

生成树保护功能包括以下几种：

- BPDU 保护功能
- 根保护功能
- 环路保护功能
- 端口角色限制功能
- TC-BPDU 传播限制功能
- 防 TC-BPDU 攻击保护功能

1. 配置BPDU保护功能

对于接入层设备，接入端口一般直接与用户终端（如 PC）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接收到 BPDU 时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。这些端口正常情况下应该不会收到 STP 的 BPDU。如果有人伪造 BPDU 恶意攻击设备，就会引起网络震荡。

生成树协议提供了 BPDU 保护功能来防止这种攻击：设备上使能了 BPDU 保护功能后，如果边缘端口收到了 BPDU，系统就将这些端口关闭，同时通知网管这些端口已被生成树协议关闭。被关闭的端口在经过一定时间间隔之后将被重新激活，这个时间间隔就是定时检测时间间隔。有关定时检测时间间隔的详细介绍，请参见“基础配置指导”中的“设备管理”。

请在有边缘端口的设备上进行如下配置。

需要注意的是，BPDU 保护功能对使能了环回测试功能的端口无效。有关环回测试功能的相关介绍，请参见“接口管理配置指导”中的“以太网接口”。

表1-36 配置 BPDU 保护功能

操作	命令	说明
进入系统视图	**system-view**	-
使能BPDU保护功能	**stp bpdu-protection**	缺省情况下，BPDU保护功能处于关闭状态

2. 配置根保护功能

生成树的根桥和备份根桥应该处于同一个域内，特别是对于 CIST 的根桥和备份根桥，网络设计时一般会把 CIST 的根桥和备份根桥放在一个高带宽的核心域内。但是，由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥有可能会收到优先级更高的 BPDU，这样当前合法根桥会失去根桥的地位，引起网络拓扑结构的错误变动。这种不合法的变动，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，导致网络拥塞。

为了防止这种情况发生，生成树协议提供了根保护功能：对于使能了根保护功能的端口，其在所有 MSTI 上的端口角色只能为指定端口。一旦该端口收到某 MSTI 优先级更高的 BPDU，立即将该 MSTI 端口设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在 2 倍的 Forward Delay 时间内没有收到更优的 BPDU 时，端口会恢复原来的正常状态。

请在设备的指定端口上进行如下配置。

需要注意的是，在同一个端口上，不允许同时配置根保护功能和环路保护功能。

表1-37 配置根保护功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能端口的根保护功能	**stp root-protection**	缺省情况下，端口上的根保护功能处于关闭状态

3. 配置环路保护功能

依靠不断接收上游设备发送的 BPDU，设备可以维持根端口和其他阻塞端口的状态。但是由于链路拥塞或者单向链路故障，这些端口会收不到上游设备的 BPDU，此时下游设备会重新选择端口角色，收不到 BPDU 的下游设备端口会转变为指定端口，而阻塞端口会迁移到转发状态，从而交换网络中会产生环路。环路保护功能会抑制这种环路的产生。

在使能了环路保护功能的端口上，其所有 MSTI 的初始状态均为 Discarding 状态：如果该端口收到了 BPDU，这些 MSTI 可以进行正常的状态迁移；否则，这些 MSTI 将一直处于 Discarding 状态以避免环路的产生。

请在设备的根端口和替换端口上进行如下配置。

配置环路保护功能时，需要注意：

- 请不要在与用户终端相连的端口上使能环路保护功能，否则该端口会因收不到 BPDU 而导致其所有 MSTI 将一直处于 Discarding 状态。
- 在同一个端口上，不允许同时配置边缘端口和环路保护功能，或者同时配置根保护功能和环路保护功能。

表1-38 配置环路保护功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能端口的环路保护功能	**stp loop-protection**	缺省情况下，端口的环路保护功能处于关闭状态

4. 配置端口角色限制功能

用户接入网络中设备桥 ID 的变化会引起核心网络生成树拓扑的改变。为了避免这种情况，可以在端口上使能端口角色限制功能，此后当该端口收到最优根消息时将不再当选为根端口，而是成为替换端口。

请在与用户接入网络相连的端口上进行如下配置。

需要注意的是，使能端口角色限制功能后可能影响生成树拓扑的连通性，请慎重配置。

表1-39 配置端口角色限制功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能端口角色限制功能	**stp role-restriction**	缺省情况下，端口角色限制功能处于关闭状态

5. 配置TC-BPDU传播限制功能

用户接入网络的拓扑改变会引起核心网络的转发地址更新，当用户接入网络的拓扑因某种原因而不稳定时，就会对核心网络形成冲击。为了避免这种情况，可以在端口上使能 TC-BPDU 传播限制功能，此后当该端口收到 TC-BPDU 时，不会再向其他端口传播。

请在与用户接入网络相连的端口上进行如下配置。

需要注意的是，使能 TC-BPDU 传播限制功能后，当拓扑改变时原有转发地址表项可能无法更新，请慎重配置。

表1-40 配置 TC-BPDU 传播限制功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能TC-BPDU传播限制功能	**stp tc-restriction**	缺省情况下，TC-BPDU传播限制功能处于关闭状态

6. 配置防TC-BPDU攻击保护功能

设备在收到 TC-BPDU 后，会执行转发地址表项的刷新操作。在有人伪造 TC-BPDU 恶意攻击设备时，设备短时间内会收到很多的 TC-BPDU，频繁的刷新操作给设备带来很大负担，给网络的稳定带来很大隐患。而通过在设备上使能防 TC-BPDU 攻击保护功能，就可以避免转发地址表项的频繁刷新。

当使能了防 TC-BPDU 攻击保护功能后，如果设备在单位时间（固定为十秒）内收到 TC-BPDU 的次数大于 **stp tc-protection threshold** 命令所指定的最高次数（假设为 N 次），那么该设备在这段时间之内将只进行 N 次刷新转发地址表项的操作，而对于超出 N 次的那些 TC-BPDU，设备会在这段时间过后再统一进行一次地址表项刷新的操作，这样就可以避免频繁地刷新转发地址表项。

建议不要关闭防 TC-BPDU 攻击保护功能。

表1-41 配置防 TC-BPDU 攻击保护功能

操作	命令	说明
进入系统视图	**system-view**	-
使能防TC-BPDU攻击保护功能	**stp tc-protection**	缺省情况下，防TC-BPDU攻击保护功能处于使能状态

操作	命令	说明
（可选）配置在单位时间（固定为十秒）内，设备收到TC-BPDU后立即刷新转发地址表项的最高次数	**stp tc-protection threshold** *number*	缺省情况下，在单位时间（固定为十秒）内，设备收到TC-BPDU后立即刷新转发地址表项的最高次数为6

1.4 生成树显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令都可以显示配置后生成树的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除生成树的统计信息。

表1-42 生成树显示和维护

操作	命令
显示被生成树保护功能阻塞的端口信息	**display stp abnormal-port**
显示端口上的BPDU统计信息	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-list*]]
显示被生成树保护功能down掉的端口信息	**display stp down-port**
显示生成树端口角色计算的历史信息（MSR 2600/MSR 3600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history**
显示生成树端口角色计算的历史信息（MSR 5600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]
显示生成树所有端口收发的TC或TCN报文数（MSR 2600/MSR 3600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc**
显示生成树所有端口收发的TC或TCN报文数（MSR 5600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]
显示生成树的状态和统计信息（MSR 2600/MSR 3600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list*] [**brief**]
显示生成树的状态和统计信息（MSR 5600）	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
显示当前生效的MST域配置信息	**display stp region-configuration**
显示所有生成树的根桥信息	**display stp root**
清除生成树的统计信息	**reset stp** [**interface** *interface-list*]

1.5 生成树典型配置举例

1.5.1 MSTP典型配置举例

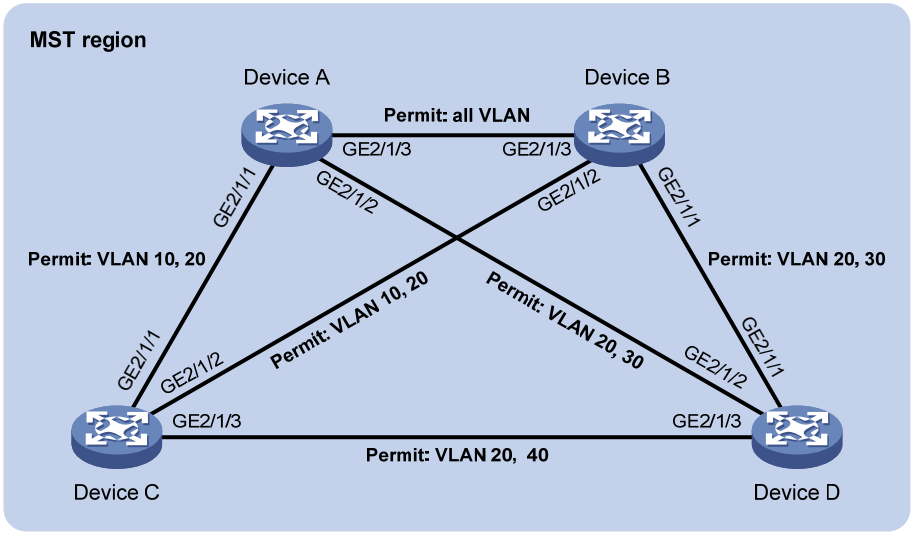
1. 组网需求

- 网络中所有设备都属于同一个 MST 域。Device A 和 Device B 为汇聚层设备，Device C 和 Device D 为接入层设备。

- 通过配置 MSTP，使不同 VLAN 的报文按照不同的 MSTI 转发：VLAN 10 的报文沿 MSTI 1 转发，VLAN 30 沿 MSTI 3 转发，VLAN 40 沿 MSTI 4 转发，VLAN 20 沿 MSTI 0 转发。
- 由于 VLAN 10 和 VLAN 30 在汇聚层设备终结、VLAN 40 在接入层设备终结，因此配置 MSTI 1 和 MSTI 3 的根桥分别为 Device A 和 Device B，MSTI 4 的根桥为 Device C。

2. 组网图

图1-11 MSTP 典型配置组网图



3. 配置步骤

(1) 配置 VLAN 和端口

请按照 图 1-11 在Device A和Device B上分别创建VLAN 10、20 和 30，在Device C上创建VLAN 10、20 和 40，在Device D上创建VLAN 20、30 和 40；将各设备的各端口配置为Trunk端口并允许相应的VLAN通过，具体配置过程略。

(2) 配置 Device A

配置 MST 域的域名为 example，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
[DeviceA-mst-region] revision-level 0
```

激活 MST 域的配置。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

配置本设备为 MSTI 1 的根桥。

```
[DeviceA] stp instance 1 root primary
```

全局使能生成树协议。

```
[DeviceA] stp global enable
```

(3) 配置 Device B

配置 MST 域的域名为 example，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
[DeviceB-mst-region] revision-level 0
```

激活 MST 域的配置。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

配置本设备为 MSTI 3 的根桥。

```
[DeviceB] stp instance 3 root primary
```

全局使能生成树协议。

```
[DeviceB] stp global enable
```

(4) 配置 Device C

配置 MST 域的域名为 example，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
[DeviceC-mst-region] revision-level 0
```

激活 MST 域的配置。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

配置本设备为 MSTI 4 的根桥。

```
[DeviceC] stp instance 4 root primary
```

全局使能生成树协议。

```
[DeviceC] stp global enable
```

(5) 配置 Device D

配置 MST 域的域名为 example，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
[DeviceD-mst-region] revision-level 0
```

激活 MST 域的配置。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

全局使能生成树协议。

```
[DeviceD] stp global enable
```

4. 验证配置

说明

在本例中，假定 Device B 的根桥 ID 最小，因此该设备将在 MSTI 0 中被选举为根桥。

当网络拓扑稳定后，通过使用 **display stp brief** 命令可以查看各设备上生成树的简要信息。例如：

查看 Device A 上生成树的简要信息。

```
[DeviceA] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet2/1/1        ALTE  DISCARDING    NONE
 0           GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 0           GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
 1           GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 1           GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 3           GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 3           GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
```

查看 Device B 上生成树的简要信息。

```
[DeviceB] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 0           GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 0           GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 1           GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 1           GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
 3           GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 3           GigabitEthernet2/1/3        DESI  FORWARDING    NONE
```

查看 Device C 上生成树的简要信息。

```
[DeviceC] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 0           GigabitEthernet2/1/2        ROOT  FORWARDING    NONE
 0           GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 1           GigabitEthernet2/1/1        ROOT  FORWARDING    NONE
 1           GigabitEthernet2/1/2        ALTE  DISCARDING    NONE
 4           GigabitEthernet2/1/3        DESI  FORWARDING    NONE
```

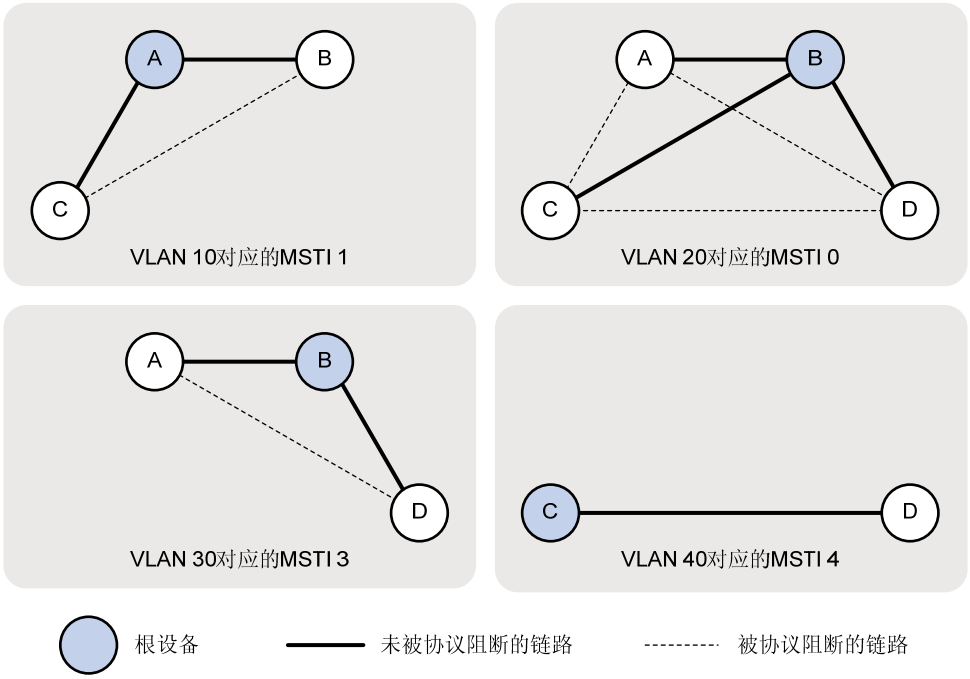
查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet2/1/1        ROOT  FORWARDING    NONE
 0           GigabitEthernet2/1/2        ALTE  DISCARDING    NONE
 0           GigabitEthernet2/1/3        ALTE  DISCARDING    NONE
```

```
3           GigabitEthernet2/1/1          ROOT  FORWARDING    NONE
3           GigabitEthernet2/1/2          ALTE  DISCARDING    NONE
4           GigabitEthernet2/1/3          ROOT  FORWARDING    NONE
```

根据上述显示信息，可以绘出各VLAN所对应MSTI的拓扑，如 图 1-12 所示。

图1-12 各 VLAN 所对应 MSTI 的拓扑图



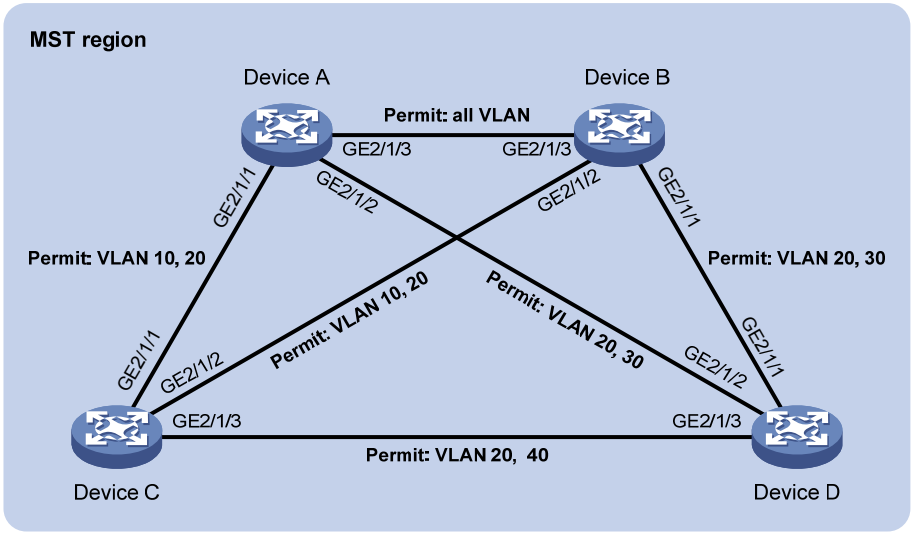
1.5.2 PVST典型配置举例

1. 组网需求

- Device A 和 Device B 为汇聚层设备，Device C 和 Device D 为接入层设备。
- 通过配置 PVST，使 VLAN 10、20、30 和 40 中的报文分别按照其各自 VLAN 所对应的生成树转发。
- 由于 VLAN 10、20 和 30 在汇聚层设备终结、VLAN 40 在接入层设备终结，因此配置 VLAN 10 和 20 的根桥为 Device A，VLAN 30 的根桥为 Device B，VLAN 40 的根桥为 Device C。

2. 组网图

图1-13 PVST 典型配置组网图



3. 配置步骤

(1) 配置 VLAN 和端口

请按照 图 1-13 在Device A和Device B上分别创建VLAN 10、20 和 30，在Device C上创建VLAN 10、20 和 40，在Device D上创建VLAN 20、30 和 40；将各设备的各端口配置为Trunk端口并允许相应的VLAN通过，具体配置过程略。

(2) 配置 Device A

配置生成树的工作模式为 PVST 模式。

```
<DeviceA> system-view
[DeviceA] stp mode pvst
```

配置本设备为 VLAN 10 和 VLAN 20 的根桥。

```
[DeviceA] stp vlan 10 20 root primary
```

全局使能生成树协议，并使能 VLAN 10、20 和 30 中的生成树协议。

```
[DeviceA] stp global enable
[DeviceA] stp vlan 10 20 30 enable
```

(3) 配置 Device B

配置生成树的工作模式为 PVST 模式。

```
<DeviceB> system-view
[DeviceB] stp mode pvst
```

配置本设备为 VLAN 30 的根桥。

```
[DeviceB] stp vlan 30 root primary
```

全局使能生成树协议，并使能 VLAN 10、20 和 30 中的生成树协议。

```
[DeviceB] stp global enable
[DeviceB] stp vlan 10 20 30 enable
```

(4) 配置 Device C

配置生成树的工作模式为 PVST 模式。

```
<DeviceC> system-view
[DeviceC] stp mode pvst
```
配置本设备为生成树 VLAN 40 的根桥。
```
[DeviceC] stp vlan 40 root primary
```
全局使能生成树协议，并使能 VLAN 10、20 和 40 中的生成树协议。
```
[DeviceC] stp global enable
[DeviceC] stp vlan 10 20 40 enable
```
(5) 配置 Device D

配置生成树的工作模式为 PVST 模式。
```
<DeviceD> system-view
[DeviceD] stp mode pvst
```
全局使能生成树协议，并使能 VLAN 20、30 和 40 中的生成树协议。
```
[DeviceD] stp global enable
[DeviceD] stp vlan 20 30 40 enable
```
4. 验证配置

当网络拓扑稳定后，通过使用 **display stp brief** 命令可以查看各设备上生成树的简要信息。例如：

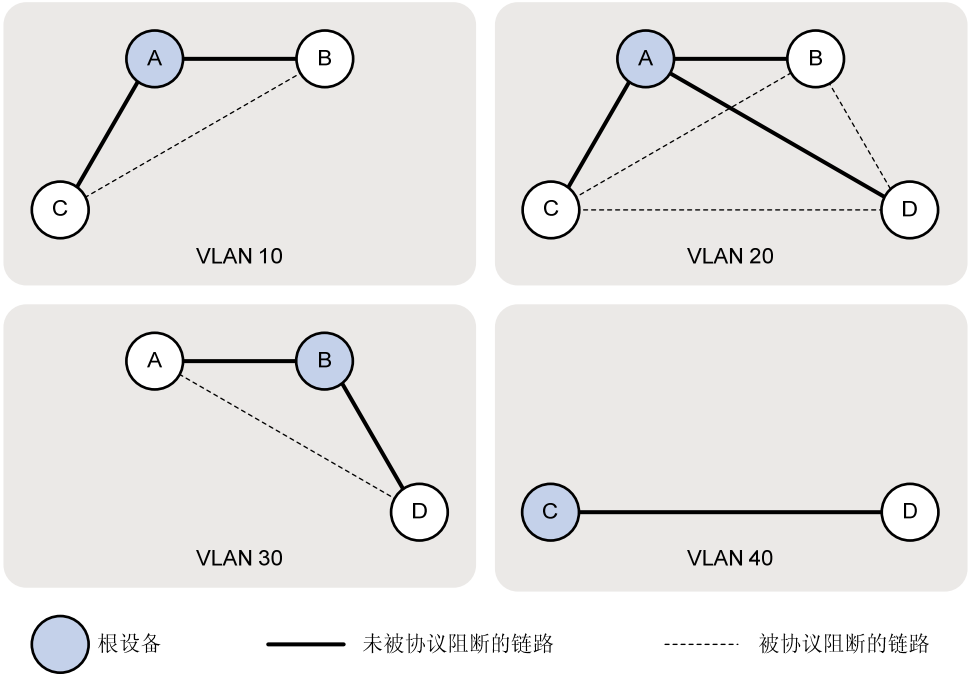
查看 Device A 上生成树的简要信息。
```
[DeviceA] display stp brief
 VLAN ID     Port                        Role  STP State     Protection
 10          GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 10          GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 20          GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 20          GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 20          GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 30          GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 30          GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
```
查看 Device B 上生成树的简要信息。
```
[DeviceB] display stp brief
 VLAN ID     Port                        Role  STP State     Protection
 10          GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 10          GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
 20          GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 20          GigabitEthernet2/1/2        DESI  FORWARDING    NONE
 20          GigabitEthernet2/1/3        ROOT  FORWARDING    NONE
 30          GigabitEthernet2/1/1        DESI  FORWARDING    NONE
 30          GigabitEthernet2/1/3        DESI  FORWARDING    NONE
```
查看 Device C 上生成树的简要信息。
```
[DeviceC] display stp brief
 VLAN ID     Port                        Role  STP State     Protection
 10          GigabitEthernet2/1/1        ROOT  FORWARDING    NONE
 10          GigabitEthernet2/1/2        ALTE  DISCARDING    NONE
 20          GigabitEthernet2/1/1        ROOT  FORWARDING    NONE
 20          GigabitEthernet2/1/2        ALTE  DISCARDING    NONE
 20          GigabitEthernet2/1/3        DESI  FORWARDING    NONE
 40          GigabitEthernet2/1/3        DESI  FORWARDING    NONE
```

查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 20          GigabitEthernet2/1/1          ALTE  DISCARDING    NONE
 20          GigabitEthernet2/1/2          ROOT  FORWARDING    NONE
 20          GigabitEthernet2/1/3          ALTE  DISCARDING    NONE
 30          GigabitEthernet2/1/1          ROOT  FORWARDING    NONE
 30          GigabitEthernet2/1/2          ALTE  DISCARDING    NONE
 40          GigabitEthernet2/1/3          ROOT  FORWARDING    NONE
```

根据上述显示信息，可以绘出各VLAN所对应生成树的拓扑，如 图 1-14 所示。

图1-14 各 VLAN 所对应生成树的拓扑图



目 录

1 环路检测

1.1 环路检测简介

1.1.1 环路检测产生背景

网络连接错误或配置错误都容易导致二层网络中出现转发环路，使设备对广播、组播以及未知单播报文进行重复发送，造成网络资源的浪费甚至导致网络瘫痪。为了能够及时发现二层网络中的环路，以避免对整个网络造成严重影响，需要提供一种检测机制，使网络中出现环路时能及时通知用户检查网络连接和配置情况，这种机制就是环路检测机制。当网络中出现环路时，环路检测机制通过生成日志信息（请参见“网络管理和监控配置指导”中的“信息中心”）来通知用户，并可根据用户事先的配置来选择是否关闭出现环路的端口。

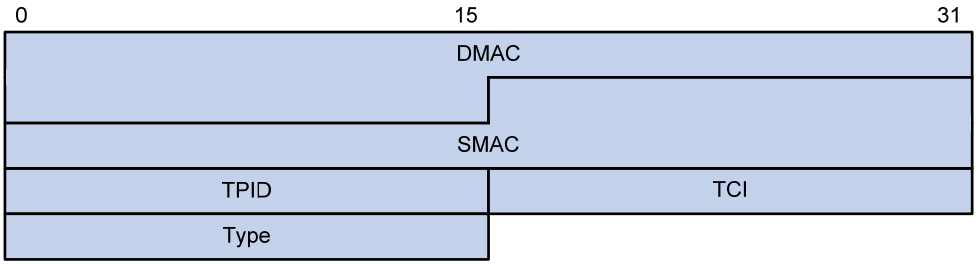
1.1.2 环路检测报文

设备通过发送环路检测报文并检测其是否返回本设备（不要求收、发端口为同一端口）以确认是否存在环路，若某端口收到了由本设备发出的环路检测报文，就认定该端口所在链路存在环路。

提示

环路检测通常工作在特定的 VLAN 内，但也可能因 QinQ 等特性的配置错误而导致 VLAN 间的环路（即尽管发出和收到的报文所携带的 VLAN 信息不同，但仍认为存在环路）。有关 QinQ 的详细介绍，请分别参见“二层技术-以太网交换配置指导”中的“QinQ”。

图1-1 环路检测报文以太网头的封装格式

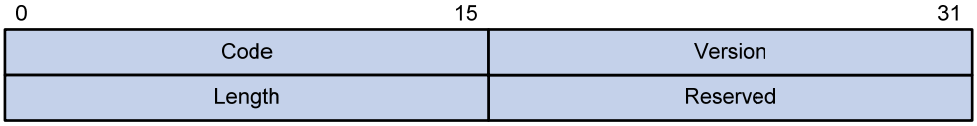


如 图 1-1 所示，为环路检测报文以太网头的封装格式，其中各字段的解释如下：

- DMAC：报文的目的 MAC 地址，使用组播 MAC 地址 010F-E200-0007。当设备使能了环路检测功能时，会将该目的地址的报文上送 CPU 处理，并在收到该报文的 VLAN 内将原始报文广播一份。
- SMAC：报文的源 MAC 地址，采用发送该报文的设备的桥 MAC。
- TPID：VLAN 标签的类型，取值为 0x8100。
- TCI：VLAN 标签的具体值，具体内容为优先级、VLAN ID 等。

- Type：协议类型，取值为 0x8918。

图1-2 环路检测报文内部头的封装格式



如 图 1-2 所示，为环路检测报文的内部头的封装格式，其中各字段的解释如下：

- Code：协议子类型，取值为 0x0001，表示环路检测协议。
- Version：版本，取值为 0x0000，目前保留。
- Length：报文长度（包括环路检测报文的头部，但不包括以太网头部）。
- Reserved：保留字段。

环路检测报文的内容以TLV（Type/Length/Value，类型/长度/值）格式进行封装，环路检测支持的TLV类型如 表 1-1 所示。

表1-1 环路检测支持的 TLV 类型

TLV 名称	说明	携带要求
End of PDU	结束TLV，用来标志PDU结束	可选
Device ID	设备标识TLV，表示发送设备的桥MAC地址	必须
Port ID	端口标识TLV，用来标识PDU发送端的端口索引	可选
Port Name	端口名称TLV，用来标识PDU发送端的端口名称	可选
System Name	系统名称TLV，表示设备的名称	可选
Chassis ID	框号TLV，表示发送端口所在的框号	可选
Slot ID	槽位号TLV，表示发送端口所在的槽位号	可选
Sub Slot ID	子槽位号TLV，表示发送端口所在的子槽位号	可选

1.1.3 环路检测运行机制

1. 环路检测时间间隔

由于网络时刻处于变化中，因此环路检测是一个持续的过程，它以一定的时间间隔发送环路检测报文来确定各端口是否出现环路、以及存在环路的端口上是否已消除环路等，这个时间间隔就称为环路检测的时间间隔。

2. 环路检测处理模式

环路检测的处理模式是指当系统检测到端口出现环路时的处理方式，包括以下几种：

- Block 模式：当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址并将端口的入方向阻塞。

- No-learning 模式：当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址。
- Shutdown 模式：当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。被关闭的端口将在 **shutdown-interval** 命令（请参考“基础配置命令参考”中的“设备管理”）所配置的时间之后自动恢复。

缺省情况下，系统不采用上述任何一种模式，当系统检测到端口出现环路时，除了生成日志信息外不对该端口进行任何处理。

3. 端口状态自动恢复

在 Block 模式和 No-learning 模式下，当设备检测到某端口出现环路后，若在三倍的环路检测时间间隔内仍未收到环路检测报文，就认为该端口上的环路已消除，自动将该端口恢复为正常转发状态，并通知给用户。这个过程就是端口状态的自动恢复过程。

在 Shutdown 模式下，出现环路的端口先被自动关闭，然后在 **shutdown-interval** 命令所配置的时间之后自动恢复。如果此时环路尚未消除，该端口将被再次关闭，然后恢复……如此往复直至环路消除。

提示

当网络中存在环路时，为防止大量报文的冲击，设备会丢弃部分报文。而如果环路检测报文也被丢弃，设备在端口状态自动恢复功能的作用下会误判定环路已消除。在这种情况下，建议将环路检测的处理模式配置为 Shutdown 模式，或当设备提示出现环路时通过手工排查来消除环路。

1.2 环路检测配置任务简介

表1-2 环路检测配置任务简介

配置任务	说明	详细配置
使能环路检测功能	必选	1.3.1
配置环路检测处理模式	可选	1.3.2
配置环路检测时间间隔	可选	1.3.3

1.3 配置环路检测

1.3.1 使能环路检测功能

用户可以在系统视图下全局使能环路检测功能，也可以在接口视图下使能当前端口的环路检测功能。系统视图下的配置对指定 VLAN 中的所有端口都有效，而接口视图下的配置则只对当前端口有效（该端口必须属于所指定的 VLAN，否则配置无效），且接口视图下的配置优先级较高。

1. 全局使能环路检测功能

表1-3 全局使能环路检测功能

操作	命令	说明
进入系统视图	**system-view**	-
全局使能环路检测功能	**loopback-detection global enable vlan** { *vlan-list* | **all** }	缺省情况下，环路检测功能处于全局关闭状态

2. 在端口上使能环路检测功能

表1-4 在端口上使能环路检测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
在端口上使能环路检测功能	**loopback-detection enable vlan** { *vlan-list* | **all** }	缺省情况下，端口上的环路检测功能处于关闭状态

1.3.2 配置环路检测处理模式

用户可以在系统视图下全局配置环路检测的处理模式，也可以在接口视图下配置当前端口的环路检测处理模式。系统视图下的配置对所有端口都有效，接口视图下的配置则只对当前端口有效，且接口视图下的配置优先级较高。

1. 全局配置环路检测处理模式

表1-5 全局配置环路检测处理模式

操作	命令	说明
进入系统视图	**system-view**	-
全局配置环路检测的处理模式	**loopback-detection global action shutdown**	缺省情况下，当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息

2. 在二层以太网接口上配置环路检测处理模式

表1-6 在二层以太网接口上配置环路检测处理模式

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
在端口上配置环路检测的处理模式	**loopback-detection action** { **block** | **no-learning** | **shutdown** }	缺省情况下，当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息

1.3.3 配置环路检测时间间隔

当使能了环路检测功能后，系统开始以一定的时间间隔发送环路检测报文，该间隔越长耗费的系统性能越少，该间隔越短环路检测的灵敏度越高。用户可以通过本配置调整发送环路检测报文的时间间隔，以在系统性能和环路检测的灵敏度之间进行平衡。

表1-7 配置环路检测时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
配置环路检测的时间间隔	**loopback-detection interval-time** *interval*	缺省情况下，环路检测的时间间隔为30秒

1.4 环路检测显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后环路检测的运行情况，通过查看显示信息验证配置的效果。

表1-8 环路检测显示和维护

操作	命令
显示环路检测的配置和运行情况	**display loopback-detection**

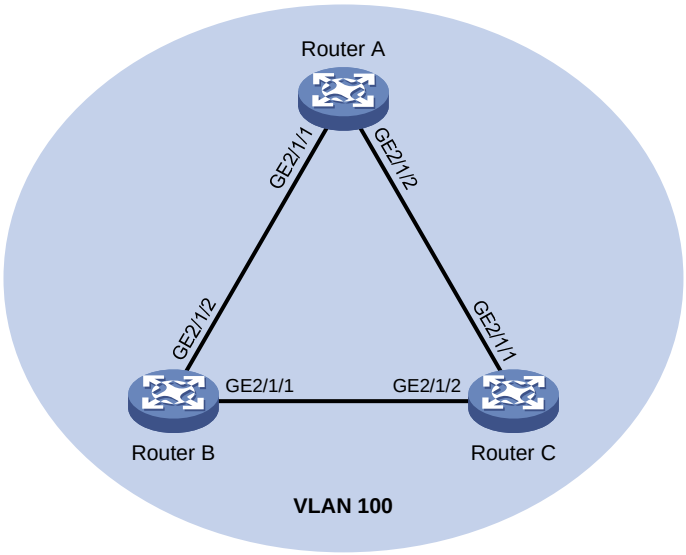
1.5 环路检测典型配置举例

1. 组网需求

- 三台设备 Router A、Router B 和 Router C 组成一个物理上的环形网络。
- 通过在 Router A 上配置环路检测功能，使系统能够自动关闭 Router A 上出现环路的端口，并通过打印日志信息来通知用户检查网络。

2. 组网图

图1-3 环路检测典型组网图



3. 配置步骤

(1) 配置 Router A

创建 VLAN 100，并全局使能该 VLAN 内的环路检测功能。

```
<RouterA> system-view
[RouterA] vlan 100
[RouterA-vlan100] quit
[RouterA] loopback-detection global enable vlan 100
```

配置端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] port link-type trunk
[RouterA-GigabitEthernet2/1/1] port trunk permit vlan 100
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] port link-type trunk
[RouterA-GigabitEthernet2/1/2] port trunk permit vlan 100
[RouterA-GigabitEthernet2/1/2] quit
```

全局配置环路检测的处理模式为 Shutdown 模式。

```
[RouterA] loopback-detection global action shutdown
```

配置环路检测的时间间隔为 35 秒。

```
[RouterA] loopback-detection interval-time 35
```

(2) 配置 Router B

创建 VLAN 100。

```
<RouterB> system-view
[RouterB] vlan 100
[RouterB-vlan100] quit
```

配置端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] port link-type trunk
[RouterB-GigabitEthernet2/1/1] port trunk permit vlan 100
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] port link-type trunk
[RouterB-GigabitEthernet2/1/2] port trunk permit vlan 100
[RouterB-GigabitEthernet2/1/2] quit
```

(3) 配置 Router C

创建 VLAN 100。

```
<RouterC> system-view
[RouterC] vlan 100
[RouterC-vlan100] quit
```

配置端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] port link-type trunk
[RouterC-GigabitEthernet2/1/1] port trunk permit vlan 100
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] port link-type trunk
[RouterC-GigabitEthernet2/1/2] port trunk permit vlan 100
[RouterC-GigabitEthernet2/1/2] quit
```

4. 验证配置

当配置完成后，系统在一个环路检测时间间隔内在 Router A 的端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 上都检测到了环路，于是将这两个端口自动关闭，并打印了如下日志信息：

```
[RouterA]
%Feb 24 15:04:29:663 2013 RouterA LPDT/4/LPDT_LOOPED: Loopback exists on
GigabitEthernet2/1/1.
%Feb 24 15:04:29:667 2013 RouterA LPDT/4/LPDT_LOOPED: Loopback exists on
GigabitEthernet2/1/2.
%Feb 24 15:04:44:243 2013 RouterA LPDT/5/LPDT_RECOVERED: Loopback on GigabitEthernet2/1/1
recovered.
%Feb 24 15:04:44:248 2013 RouterA LPDT/5/LPDT_RECOVERED: Loopback on GigabitEthernet2/1/2
recovered.
```

使用 **display loopback-detection** 命令可以查看 Router A 上环路检测的配置和运行情况：

显示 Router A 上环路检测的配置和运行情况。

```
[RouterA] display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 35 second(s).
No loopback is detected.
```

由此可见，Router A 上并未显示在端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 上检测到环路，这是由于环路检测功能运行在 Shutdown 模式下，端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 上出现环路后均已被自动关闭，因此这两个端口上的环路已消除。此时，使用 **display interface** 命令分别查看 Router A 上端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 的状态信息：

显示 Router A 上端口 GigabitEthernet2/1/1 的状态信息。

```
[RouterA] display interface gigabitethernet 2/1/1
```

```
GigabitEthernet2/1/1 current state: DOWN (Loopback detection down)
...
```

显示 Router A 上端口 GigabitEthernet2/1/2 的状态信息。

```
[RouterA] display interface gigabitethernet 2/1/2
GigabitEthernet2/1/2 current state: DOWN (Loopback detection down)
...
```

由此可见，端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 均已被环路检测模块自动关闭。

目 录

1 VLAN

说明

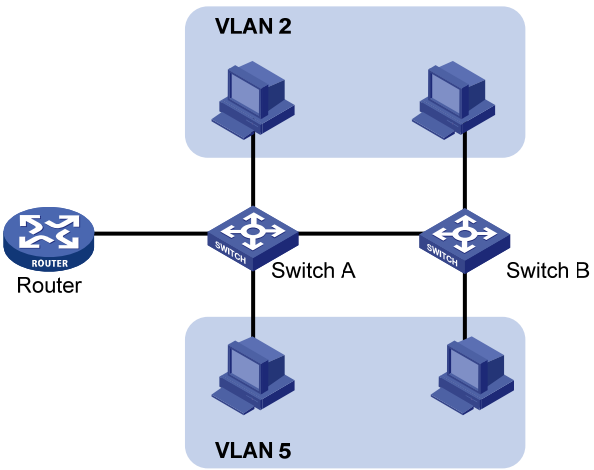
该特性仅在安装了二层接口卡的款型和 MSR 3600-28/MSR 3600-51 的固定二层接口上支持。

1.1 VLAN简介

1.1.1 VLAN概述

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域。当网络中主机数目较多时会导致冲突严重、广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理LAN划分成多个逻辑的LAN——VLAN。处于同一VLAN的主机能直接互通，而处于不同VLAN的主机则不能直接互通。这样，广播报文被限制在同一个VLAN内，即每个VLAN是一个广播域。如 图 1-1 所示，VLAN 2 内的主机可以互通，但与VLAN 5 内的主机不能互通。

图1-1 VLAN 示意图



VLAN 的划分不受物理位置的限制：物理位置不在同一范围的主机可以属于同一个 VLAN；一个 VLAN 包含的主机可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 根据划分方式不同可以分为不同类型。基于端口划分 VLAN 是其中最简单、最有效的 VLAN 划分方式。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。本章将介绍基于端口的 VLAN。

VLAN 的优点如下：

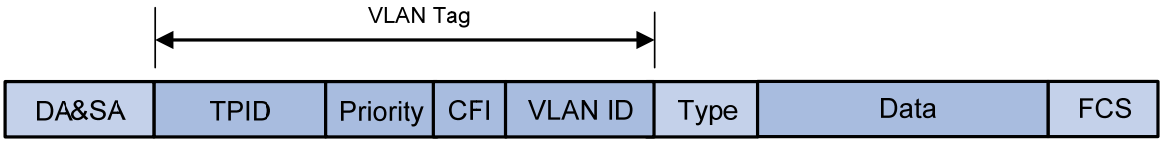
- 限制广播域。广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。

- 增强局域网的安全性。VLAN 间的二层报文是相互隔离的，即一个 VLAN 内的主机不能和其他 VLAN 内的主机直接通信，如果不同 VLAN 要进行通信，则需通过路由器或三层交换机等三层设备。
- 灵活构建虚拟工作组。通过 VLAN 可以将不同的主机划分到不同的工作组，同一工作组的主机可以位于不同的物理位置，网络构建和维护更方便灵活。

1.1.2 VLAN报文封装

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。IEEE 802.1Q 协议规定，在以太网报文的目的 MAC 地址和源 MAC 地址字段之后、协议类型字段之前加入 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

图1-2 VLAN Tag 的组成字段



如 图 1-2 所示，VLAN Tag包含四个字段，分别是TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和VLAN ID。

- TPID：用来表示报文是否带有 VLAN Tag，长度为 16 比特，缺省情况下，TPID 取值为 0x8100，但各设备厂商可以自定义该字段的值。当邻居设备将 TPID 值配置为非 0x8100 时，为了能够识别这样的报文，实现互通，必须在本设备上修改 TPID 值，确保和邻居设备的 TPID 值配置一致。如果报文的 TPID 值为配置值或 0x8100，则该报文被认为带有 VLAN Tag。配置 TPID 值的相关命令请参见“二层技术-以太网交换命令参考”中的“QinQ”。
- Priority：用来表示报文的 802.1p 优先级，长度为 3 比特，相关内容请参见“ACL 和 QoS 配置指导”中的“附录”。
- CFI：用来表示 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1 比特。取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装。在以太网中，CFI 取值为 0。
- VLAN ID：用来表示该报文所属 VLAN 的编号，长度为 12 比特。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1～4094。

网络设备根据报文是否携带VLAN Tag以及携带的VLAN Tag信息，来对报文进行处理，利用VLAN ID来识别报文所属的VLAN。详细的处理方式请参见“1.4.1 基于端口的VLAN简介”。

说明

- 以太网支持 Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式，本文以 Ethernet II 型封装为例。802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式添加 VLAN Tag 字段的方式请参见相关协议规范。
- 对于带有多层 VLAN Tag 的报文，设备会根据其最外层 VLAN Tag 进行处理，而内层 VLAN Tag 会被视为报文的普通数据部分。

1.1.3 协议规范

与 VLAN 相关的协议规范有：

- IEEE 802.1Q：IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 配置VLAN基本属性

表1-1 配置 VLAN 基本属性

配置	命令	说明
进入系统视图	**system-view**	-
（可选）创建一个VLAN并进入VLAN视图，或批量创建VLAN	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	缺省情况下，系统只有一个缺省VLAN（VLAN 1）
进入VLAN视图	**vlan** *vlan-id*	批量创建VLAN时，为必选；否则，无需执行本命令
指定当前VLAN的名称	**name** *text*	缺省情况下，VLAN的名称为“VLAN *vlan-id*”，其中*vlan-id*为该VLAN的编号。例如，VLAN 100的名称为“VLAN 0100”
配置当前VLAN的描述信息	**description** *text*	缺省情况下，VLAN的描述信息为“VLAN *vlan-id*”，其中*vlan-id*为该VLAN的编号。例如，VLAN 100的描述信息为“VLAN 0100”

说明

- VLAN 1 为系统缺省 VLAN，用户不能手工创建和删除。
- 动态学习到的 VLAN、配置有 QoS 策略的 VLAN、被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

1.3 配置VLAN接口基本属性

不同 VLAN 间的主机不能直接通信，通过在设备上配置 VLAN 接口，可以实现 VLAN 间的三层互通。

VLAN 接口是一种三层的虚拟接口，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该 IP 地址即可作为本 VLAN 内网络设备的网关地址，对需要跨网段的报文进行基于 IP 地址的三层转发。

配置 VLAN 接口基本属性时，需要注意，在创建 VLAN 接口之前，对应的 VLAN 必须已经存在，否则将不能创建指定的 VLAN 接口。

表1-2 配置 VLAN 接口基本属性

配置	命令	说明
进入系统视图	**system-view**	-

配置	命令	说明
创建VLAN接口并进入VLAN接口视图	**interface vlan-interface** *vlan-interface-id*	如果该VLAN接口已经存在，则直接进入该VLAN接口视图 缺省情况下，未创建VLAN接口
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，未配置VLAN接口的IP地址
配置当前VLAN接口的描述信息	**description** *text*	缺省情况下，VLAN接口的描述信息为该VLAN接口的接口名，如“Vlan-interface1 Interface”
配置VLAN接口的MTU值	**mtu** *size*	缺省情况下，VLAN接口的MTU值为1500
配置VLAN接口的MAC地址	**mac-address** *mac-address*	缺省情况下，VLAN接口未配置MAC地址
（可选）配置VLAN接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbit/s）
（可选）恢复当前VLAN接口的缺省配置	**default**	-
（可选）取消手工关闭VLAN接口	**undo shutdown**	缺省情况下，未手工关闭VLAN接口

1.4 配置基于端口的VLAN

1.4.1 基于端口的VLAN简介

基于端口划分 VLAN 是最简单、最有效的 VLAN 划分方法。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。

1. 端口的链路类型

根据端口在转发报文时对 VLAN Tag 的不同处理方式，可将端口的链路类型分为三种：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。

2. 端口缺省VLAN

除了可以设置端口允许通过的 VLAN 外，还可以设置端口的缺省 VLAN，即端口 VLAN ID（Port VLAN ID，PVID）。在缺省情况下，所有端口的缺省 VLAN 均为 VLAN 1，但用户可以根据需要进行配置。

- Access 端口的缺省 VLAN 就是它所在的 VLAN。
- Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置缺省 VLAN。

- 当执行 **undo vlan** 命令删除的 VLAN 是某个端口的缺省 VLAN 时，对 Access 端口，端口的缺省 VLAN 会恢复到 VLAN 1；对 Trunk 或 Hybrid 端口，端口的缺省 VLAN 配置不会改变，即它们可以使用已经不存在的 VLAN 作为缺省 VLAN。

说明

- 建议本端设备端口的缺省 VLAN ID 和相连的对端设备端口的缺省 VLAN ID 保持一致。
- 建议保证端口的缺省 VLAN 为端口允许通过的 VLAN。如果端口不允许某 VLAN 通过，但是端口的缺省 VLAN 为该 VLAN，则端口会丢弃收到的该 VLAN 的报文或者不带 VLAN Tag 的报文。

3. 端口对报文的处理方式

在配置了端口链路类型和缺省VLAN后，端口对报文的接收和发送的处理有几种不同情况，具体情况请参看 表 1-3。

表1-3 不同链路类型端口收发报文的差异

端口类型	对接收报文的处理		对发送报文的处理
	当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
Access端口	为报文添加端口缺省VLAN的Tag	• 当报文的 VLAN ID 与端口的缺省 VLAN ID 相同时，接收该报文 • 当报文的 VLAN ID 与端口的缺省 VLAN ID 不同时，丢弃该报文	去掉Tag，发送该报文
Trunk端口	• 当端口的缺省 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文，给报文添加端口缺省 VLAN 的 Tag • 当端口的缺省 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当报文的 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文 • 当报文的 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当报文的 VLAN ID 与端口的缺省 VLAN ID 相同，且是该端口允许通过的 VLAN ID 时：去掉 Tag，发送该报文 • 当报文的 VLAN ID 与端口的缺省 VLAN ID 不同，且是该端口允许通过的 VLAN ID 时：保持原有 Tag，发送该报文
Hybrid端口			当报文的VLAN ID是端口允许通过的VLAN ID时，发送该报文，并可以通过**port hybrid vlan**命令配置端口在发送该VLAN（包括缺省VLAN）的报文时是否携带Tag

1.4.2 配置基于Access端口的VLAN

配置基于 Access 端口的 VLAN 有两种方法：一种是在 VLAN 视图下进行配置，另一种是在接口视图下进行配置。

表1-4 配置基于 Access 端口的 VLAN（在 VLAN 视图下）

配置	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
向当前VLAN中添加一个或一组Access端口	**port** *interface-list*	缺省情况下，系统将所有端口都加入到VLAN 1

表1-5 配置基于 Access 端口的 VLAN（在接口视图下）

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	进入二层以太网接口视图后，下面进行的配置只在当前接口下生效
配置端口的链路类型为Access类型	**port link-type access**	缺省情况下，端口的链路类型为Access
将当前Access端口加入到指定VLAN	**port access vlan** *vlan-id*	缺省情况下，所有Access端口都属于VLAN 1 在将Access端口加入到指定VLAN之前，该VLAN必须已经存在

1.4.3 配置基于Trunk端口的VLAN

Trunk 端口可以允许多个 VLAN 通过，只能在接口视图下进行配置。

配置基于 Trunk 端口的 VLAN 时，需要注意：

- Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其他类型端口。
- 配置缺省 VLAN 后，必须使用 **port trunk permit vlan** 命令配置允许缺省 VLAN 的报文通过，出接口才能转发缺省 VLAN 的报文。

表1-6 配置基于 Trunk 端口的 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	进入二层以太网接口视图后，下面进行的配置只在当前接口下生效
配置端口的链路类型为Trunk类型	**port link-type trunk**	缺省情况下，端口的链路类型为Access类型
允许指定的VLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-id-list* | **all** }	缺省情况下，Trunk端口只允许VLAN 1的报文通过
（可选）设置Trunk端口的缺省VLAN	**port trunk pvid vlan** *vlan-id*	缺省情况下，Trunk端口的缺省VLAN为VLAN 1

1.4.4 配置基于Hybrid端口的VLAN

Hybrid 端口可以允许多个 VLAN 通过，只能在接口视图下进行配置。

配置基于 Hybrid 端口的 VLAN 时，需要注意：

- Hybrid 端口和 Trunk 端口之间不能直接切换，只能先设为 Access 端口，再设置为其他类型端口。
- 在设置允许指定的 VLAN 通过 Hybrid 端口之前，允许通过的 VLAN 必须已经存在。
- 配置缺省 VLAN 后，必须使用 **port hybrid vlan** 命令配置允许缺省 VLAN 的报文通过，出接口才能转发缺省 VLAN 的报文。

表1-7 配置基于 Hybrid 端口的 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	进入二层以太网接口视图后，下面进行的配置只在当前接口下生效
配置端口的链路类型为Hybrid类型	**port link-type hybrid**	缺省情况下，端口的链路类型为Access类型
允许指定的VLAN通过当前Hybrid端口	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	缺省情况下，Hybrid端口只允许VLAN 1的报文以Untagged方式通过（即VLAN 1的报文从该端口发送出去后不携带VLAN Tag）
（可选）配置Hybrid端口的缺省VLAN	**port hybrid pvid vlan** *vlan-id*	缺省情况下，Hybrid端口的缺省VLAN为该端口在链路类型为Access时的所属VLAN

1.5 配置VLAN组

VLAN组是一组VLAN的集合。VLAN组内可以添加多个VLAN列表，一个VLAN列表表示一组VLAN ID连续的VLAN。

认证服务器可以通过下发 VLAN 组名的方式为通过认证的 802.1X 用户下发一组授权 VLAN。有关 802.1X 的详细介绍，请参见“安全配置指导”中的“802.1X”。

表1-8 配置 VLAN 组

操作	命令	说明
进入系统视图	**system-view**	-
创建一个VLAN组，并进入VLAN组视图	**vlan-group** *group-name*	缺省情况下，不存在任何VLAN组
在当前VLAN组内添加VLAN成员	**vlan-list** *vlan-id-list*	缺省情况下，当前VLAN组中不存在任何VLAN列表

1.6 VLAN显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 VLAN 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 VLAN 接口统计信息。

表1-9 VLAN 显示和维护

操作	命令
显示VLAN接口相关信息	**display interface** [**vlan-interface**] [**brief** [**down**]] **display interface** [**vlan-interface** [*interface-number*]] [**brief** [**description**]]
显示VLAN相关信息	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
显示创建的VLAN组及其VLAN成员列表	**display vlan-group** [*group-name*]
显示设备上当前存在的Hybrid或Trunk端口	**display port** { **hybrid** | **trunk** }
清除VLAN接口的统计信息	**reset counters interface vlan-interface** [*vlan-interface-id*]

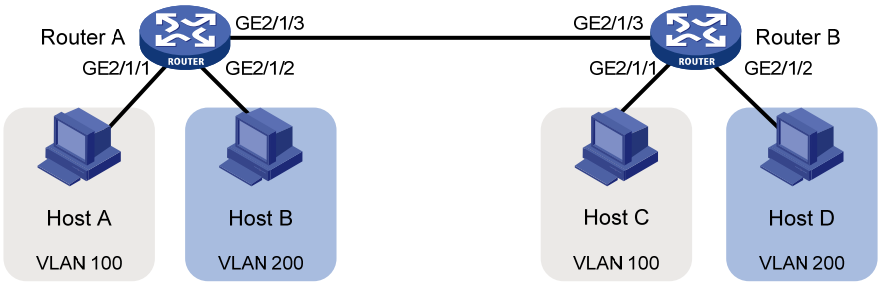
1.7 基于端口的VLAN典型配置举例

1. 组网需求

- Host A 和 Host C 属于部门 A，但是通过不同的设备接入公司网络；Host B 和 Host D 属于部门 B，也通过不同的设备接入公司网络。
- 为了通信的安全性，也为了避免广播报文泛滥，公司网络中使用 VLAN 技术来隔离部门间的二层流量。其中部门 A 使用 VLAN 100，部门 B 使用 VLAN 200。
- 现要求不管是否使用相同的设备接入公司网络，同一 VLAN 内的主机能够互通，即 Host A 和 Host C 能够互通，Host B 和 Host D 能够互通。

2. 组网图

图1-3 基于端口的 VLAN 组网图



3. 配置步骤

(1) 配置 Router A

创建 VLAN 100，并将 GigabitEthernet2/1/1 加入 VLAN 100。

```
<RouterA> system-view
[RouterA] vlan 100
[RouterA-vlan100] port gigabitethernet 2/1/1
[RouterA-vlan100] quit
```

创建 VLAN 200，并将 GigabitEthernet2/1/2 加入 VLAN 200。

```
[RouterA] vlan 200
[RouterA-vlan200] port gigabitethernet 2/1/2
[RouterA-vlan200] quit
```

为了使 Router A 上 VLAN 100 和 VLAN 200 的报文能发送给 Router B，将 GigabitEthernet2/1/3 的链路类型配置为 Trunk，并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] port link-type trunk
[RouterA-GigabitEthernet2/1/3] port trunk permit vlan 100 200
```

(2) Router B 上的配置与 Router A 上的配置相同，不再赘述。

(3) 将 Host A 和 Host C 配置在一个网段，比如 192.168.100.0/24；将 Host B 和 Host D 配置在一个网段，比如 192.168.200.0/24。

4. 验证配置

(1) Host A 和 Host C 能够互相 ping 通，但是均不能 ping 通 Host B。Host B 和 Host D 能够互相 ping 通，但是均不能 ping 通 Host A。

(2) 通过查看显示信息验证配置是否成功。

查看 Router A 上 VLAN 100 和 VLAN 200 的配置信息，验证以上配置是否生效。

```
[RouterA-GigabitEthernet2/1/3] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet2/1/3
 Untagged ports:
    GigabitEthernet2/1/1
[RouterA-GigabitEthernet2/1/3] display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet2/1/3
 Untagged ports:
    GigabitEthernet2/1/2
```

目 录

1 QinQ

说明

该特性仅在安装了 HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 接口卡的款型上支持。

1.1 QinQ简介

IEEE 802.1Q 定义的 VLAN ID 域有 12 个比特，最多可以提供 4094 个 VLAN。但在实际应用中，尤其是在城域网中，需要大量的 VLAN 来隔离用户，4094 个 VLAN 远远不能满足需求。QinQ 使整个网络最多可以提供 4094×4094 个 VLAN，满足了城域网对 VLAN 数量的需求。

QinQ 是 802.1Q in 802.1Q 的简称，是基于 IEEE 802.1Q 技术的一种比较简单的二层 VPN 协议。通过将一层 VLAN Tag 封装到私网报文上，使其携带两层 VLAN Tag 穿越运营商的骨干网络（又称公网），从而使运营商能够利用一个 VLAN 为包含多个 VLAN 的用户网络提供服务。

QinQ 具备以下优点：

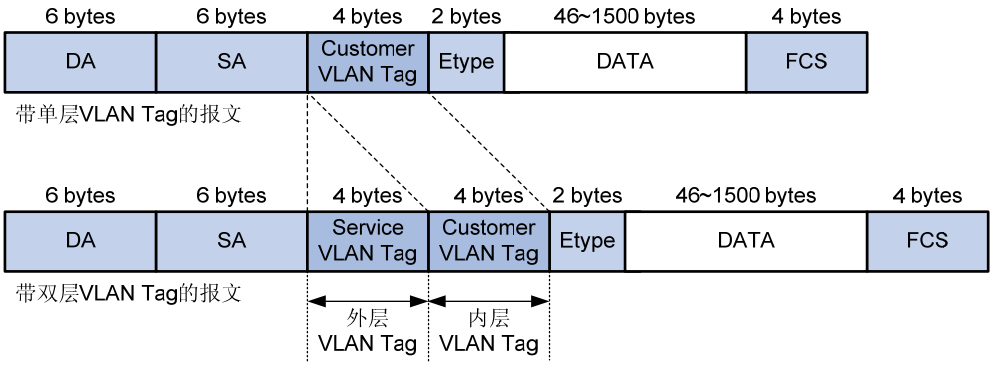
- 缓解公网 VLAN 资源日益紧缺的问题。
- 用户可以规划自己的私网 VLAN，不会导致与公网 VLAN 冲突。
- 为用户提供了一种简单、灵活的二层 VPN 解决方案。
- 当运营商进行 VLAN 规划时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

1.1.1 QinQ的工作原理

如 图 1-1 所示，QinQ报文在运营商网络中传输时带有双层VLAN Tag：

- 内层 VLAN Tag：为用户的私网 VLAN Tag，对应图中的 Customer VLAN Tag（简称 CVLAN）。设备依靠该 Tag 在私网中传送报文。
- 外层 VLAN Tag：为运营商分配给用户的公网 VLAN Tag，对应图中的 Service VLAN Tag（简称 SVLAN）。设备依靠该 Tag 在公网中传送 QinQ 报文。

图1-1 QinQ 的报文结构

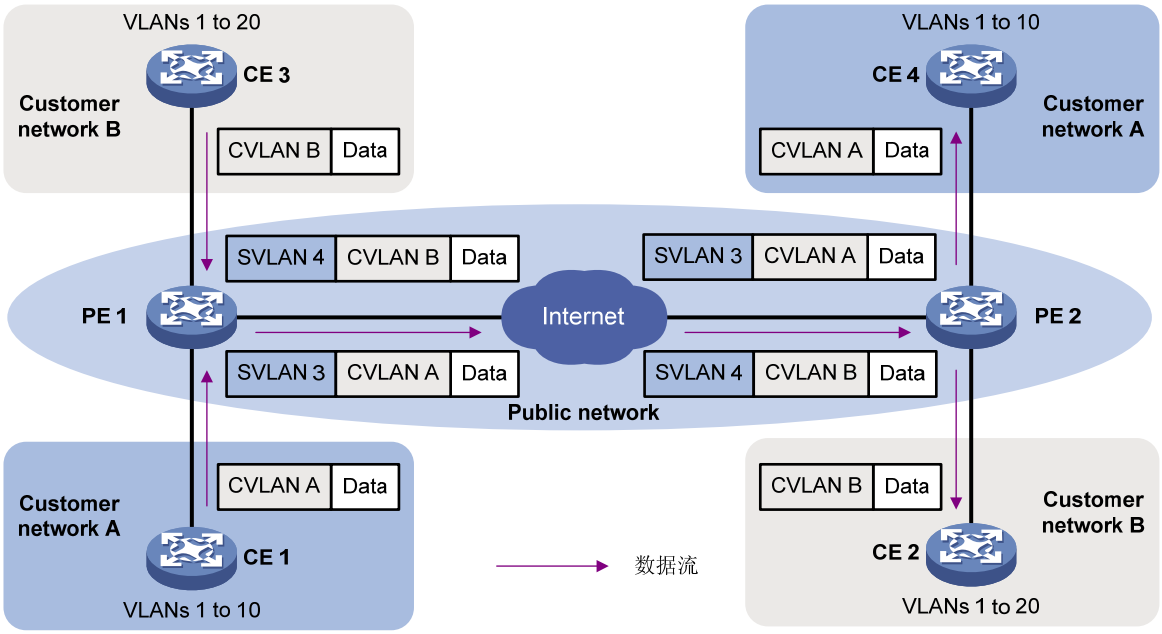


说明

接口的 MTU（Maximum Transmission Unit，最大传输单元）值默认为 1500 字节。由于为报文加上外层 VLAN Tag 后，报文长度将增加 4 个字节，因此建议用户适当增加运营商网络中各接口的 MTU 值（至少为 1504 字节）。有关接口 MTU 值的相关配置，请参见“接口管理配置指导”中的“以太网接口”。

在公网的传输过程中，设备只根据外层 VLAN Tag 转发报文，而内层 VLAN Tag 将被当作报文的数据部分进行传输。

图1-2 QinQ 典型应用组网图



如 图 1-2 所示，用户网络A和B的私网VLAN分别为VLAN 1～10 和VLAN 1～20。运营商为用户网络A和B分配的公网VLAN分别为VLAN 3 和VLAN 4。

(1) 当用户网络 A 和 B 中带私网 VLAN Tag 的报文进入运营商网络时，报文外面就会被分别封装上 VLAN 3 和 VLAN 4 的公网 VLAN Tag。

(2) 来自不同用户网络的报文在运营商网络中传输时被隔离，即使这些用户网络各自的 VLAN 范围存在重叠，因为分配到的公网 VLAN 不同，在运营商网络中传输时也不会产生冲突。

(3) 当报文穿过运营商网络，到达运营商网络另一侧 PE（Provider Edge，服务提供商网络边缘）设备后，报文被剥离公网 VLAN Tag，然后再传送给用户网络的 CE（Customer Edge，用户网络边缘）设备。

1.1.2 QinQ的实现方式

当端口上配置了 QinQ 功能后，不论从该端口收到的报文是否带有 VLAN Tag，设备都会为该报文添加本端口缺省 VLAN 的 Tag：

- 如果收到的是带有 VLAN Tag 的报文，该报文就成为带两层 Tag 的报文；

- 如果收到的是不带 VLAN Tag 的报文，该报文就成为带有本端口缺省 VLAN Tag 的报文。

1.1.3 协议规范

与 QinQ 相关的协议规范有：

- IEEE 802.1Q：IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks
- IEEE 802.1ad：IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks-Amendment 4: Provider Bridges

1.2 配置QinQ功能

QinQ 功能应在 PE 设备的用户网络侧接口上进行配置。

1.2.1 使能QinQ功能

使能了 QinQ 功能的端口将为其收到的报文添加该端口缺省 VLAN 的 Tag。

表1-1 使能 QinQ 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能端口的QinQ功能	**qinq enable**	缺省情况下，端口的QinQ功能处于关闭状态

1.3 配置VLAN Tag的TPID值

TPID（Tag Protocol Identifier，标签协议标识符）值可以用来判断报文中是否带有 VLAN Tag。例如，在设备上配置用户 VLAN Tag 和运营商 VLAN Tag 的 TPID 值分别为 0x8200 和 0x9100，如果该设备收到的报文实际携带的内、外层 VLAN Tag 的 TPID 值分别为 0x8100 和 0x9100，由于该报文外层 VLAN Tag 的 TPID 值与配置值相同，而内层 VLAN Tag 的 TPID 值与配置值不同，该设备会认为该报文只携带运营商 VLAN Tag，而没有携带用户 VLAN Tag；对于该设备收到的只带有一层 VLAN Tag 的报文，如果该 VLAN Tag 的 TPID 值不为 0x9100，则该设备会认为该报文没有携带 VLAN Tag。

第三方厂商的设备可能将 QinQ 报文外层 VLAN Tag 的 TPID 设为不同的值。为了与这些厂商的设备兼容，用户可以通过修改 TPID 值，使发送到的 QinQ 报文携带的 TPID 值与第三方厂商的相同，从而实现与这些厂商的设备互通。

VLAN Tag 的 TPID 值有全局配置和端口上的配置两种方式。其中，全局配置对所有端口都有效，端口上的配置对一个或多个端口有效。对于某个端口来说，优先采用端口上的配置，然后才采用全局配置。

VLAN Tag 的 TPID 值应在 PE 设备的运营商网络侧的接口上进行配置。

1. 全局配置VLAN Tag的TPID值

表1-2 全局配置 VLAN Tag 的 TPID 值

操作	命令	说明
进入系统视图	**system-view**	-
配置内层VLAN Tag的TPID值	**qinq ethernet-type customer-tag** *hex-value*	缺省情况下，内层VLAN Tag的TPID值都为0x8100

2. 在端口上配置VLAN Tag的TPID值

表1-3 在端口上配置 VLAN Tag 的 TPID 值

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
配置外层VLAN Tag的TPID值	**qinq ethernet-type service-tag** *hex-value*	缺省情况下，外层VLAN Tag的TPID值为0x8100

1.4 配置外层VLAN Tag的802.1p优先级

对于携带两层 VLAN Tag 的报文，如果需要修改外层 VLAN Tag 的 802.1p 优先级，可以通过 QoS 策略实现以下两种功能中的一种：

- 根据内层 VLAN Tag 的 802.1p 优先级或内层 VLAN ID 来标记外层 VLAN Tag 的 802.1p 优先级。
- 将内层 VLAN Tag 的 802.1p 优先级复制为外层 VLAN Tag 的 802.1p 优先级。

配置外层 VLAN Tag 的 802.1p 优先级前，需要注意：

- 在未进行本配置时，端口会将内层 VLAN Tag 的 802.1p 优先级复制为外层 VLAN Tag 的 802.1p 优先级。
- 不可以在一台设备上先为报文添加外层 VLAN Tag，再修改该 VLAN Tag 的 802.1p 优先级。
- 有关 QoS 策略相关命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”；有关优先级信任模式的配置，请参见“ACL 和 QoS 配置指导”中的“优先级映射”。

表1-4 配置外层 VLAN Tag 的 802.1p 优先级

操作		命令	说明
进入系统视图		**system-view**	-
定义类，并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配报文的规则	定义匹配内层VLAN ID的规则	**if-match customer-vlan-id** *vlan-id-list*	二者选其一

操作		命令	说明
	定义匹配内层VLAN Tag的802.1p优先级的规则	**if-match customer-dot1p** *dot1p-value*&<1-8>	
退回系统视图		**quit**	-
定义流行为，并进入流行为视图		**traffic behavior** *behavior-name*	-
重标记外层VLAN Tag的802.1p优先级		**remark dot1p** *dot1p-value*	
退回系统视图		**quit**	-
定义策略，并进入策略视图		**qos policy** *policy-name*	-
在策略中，将之前定义的类和流行为进行绑定，组成QoS策略		**classifier** *classifier-name* **behavior** *behavior-name*	-
退回系统视图		**quit**	-
进入二层以太网接口		**interface** *interface-type interface-number*	-
在端口的入方向应用QoS策略		**qos apply policy** *policy-name* **inbound**	-

1.5 QinQ显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示使能了 QinQ 功能的端口，通过查看显示信息验证配置的效果。

表1-5 QinQ 显示和维护

操作	命令
显示使能了QinQ功能的端口	**display qinq** [**interface** *interface-type interface-number*]

1.6 QinQ典型配置举例

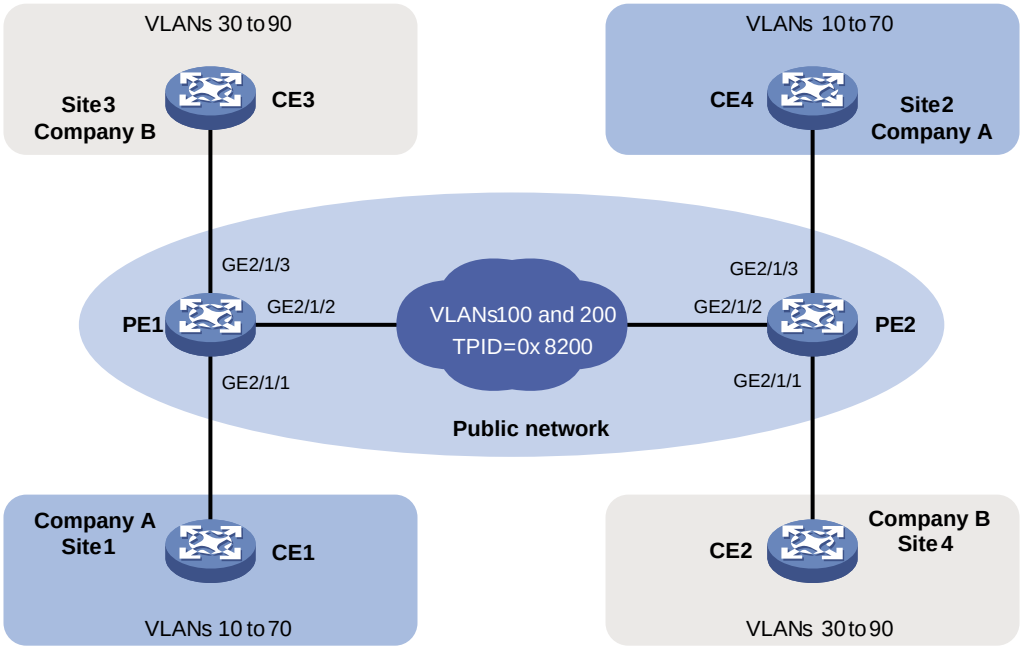
1.6.1 QinQ配置举例

1. 组网需求

- 公司 A 的两个分支机构 Site 1 和 Site 2 通过运营商网络进行通信，该公司各业务使用的 VLAN 为 VLAN 10～70；公司 B 的两个分支机构 Site 3 和 Site 4 也通过运营商网络进行通信，该公司各业务使用的 VLAN 为 VLAN 30～90。
- PE 1 和 PE 2 为运营商网络的边缘设备，且二者通过 TPID 值为 0x8200 的第三方厂商设备进行连接。
- 通过配置，利用运营商提供的 VLAN 100 使公司 A 的两个分支机构之间实现互通，利用运营商提供的 VLAN 200 使公司 B 的两个分支机构之间实现互通。

2. 组网图

图1-3 QinQ 配置组网图



3. 配置步骤

(1) 配置 PE 1

- 配置端口 GigabitEthernet2/1/1

配置端口为 Trunk 端口，且允许 VLAN 100 和 VLAN 10～70 的报文通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] port link-type trunk
[PE1-GigabitEthernet2/1/1] port trunk permit vlan 100 10 to 70
```

配置端口的缺省 VLAN 为 VLAN 100。

```
[PE1-GigabitEthernet2/1/1] port trunk pvid vlan 100
```

使能端口的 QinQ 功能。

```
[PE1-GigabitEthernet2/1/1] qinq enable
[PE1-GigabitEthernet2/1/1] quit
```

- 配置端口 GigabitEthernet2/1/2

配置端口为 Trunk 端口，且允许 VLAN 100 和 VLAN 200 的报文通过。

```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] port link-type trunk
[PE1-GigabitEthernet2/1/2] port trunk permit vlan 100 200
```

配置外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet2/1/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet2/1/2] quit
```

- 配置端口 GigabitEthernet2/1/3

配置端口为 Trunk 端口，且允许 VLAN 200 和 VLAN 30～90 的报文通过。

```
[PE1] interface gigabitethernet 2/1/3
[PE1-GigabitEthernet2/1/3] port link-type trunk
[PE1-GigabitEthernet2/1/3] port trunk permit vlan 200 30 to 90
```

配置端口的缺省 VLAN 为 VLAN 200。

```
[PE1-GigabitEthernet2/1/3] port trunk pvid vlan 200
```

使能端口的 QinQ 功能。

```
[PE1-GigabitEthernet2/1/3] qinq enable
[PE1-GigabitEthernet2/1/3] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet2/1/1

配置端口为 Trunk 端口，且允许 VLAN 200 和 VLAN 30～90 的报文通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] port link-type trunk
[PE2-GigabitEthernet2/1/1] port trunk permit vlan 200 30 to 90
```

配置端口的缺省 VLAN 为 VLAN 200。

```
[PE2-GigabitEthernet2/1/1] port trunk pvid vlan 200
```

使能端口的 QinQ 功能。

```
[PE2-GigabitEthernet2/1/1] qinq enable
[PE2-GigabitEthernet2/1/1] quit
```

- 配置端口 GigabitEthernet2/1/2

配置端口为 Trunk 端口，且允许 VLAN 100 和 VLAN 200 的报文通过。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] port link-type trunk
[PE2-GigabitEthernet2/1/2] port trunk permit vlan 100 200
```

配置外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet2/1/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet2/1/2] quit
```

- 配置端口 GigabitEthernet2/1/3

配置端口为 Trunk 端口，且允许 VLAN 100 和 VLAN 10～70 的报文通过。

```
[PE2] interface gigabitethernet 2/1/3
[PE2-GigabitEthernet2/1/3] port link-type trunk
[PE2-GigabitEthernet2/1/3] port trunk permit vlan 100 10 to 70
```

配置端口的缺省 VLAN 为 VLAN 100。

```
[PE2-GigabitEthernet2/1/3] port trunk pvid vlan 100
```

使能端口的 QinQ 功能。

```
[PE2-GigabitEthernet2/1/3] qinq enable
[PE2-GigabitEthernet2/1/3] quit
```

(3) 配置第三方厂商设备

对于 PE 1 与 PE 2 之间的第三方厂商设备，其关键配置如下：在连通 PE 1 与 PE 2 的端口上，都允许 VLAN 100 和 VLAN 200 的报文携带 VLAN Tag 通过。

目 录

1 LLDP

1.1 LLDP简介

1.1.1 LLDP产生背景

目前，网络设备的种类日益繁多且各自的配置错综复杂，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。

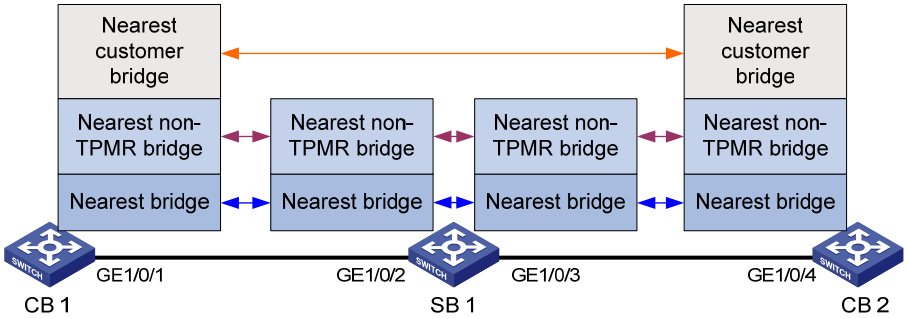
LLDP（Link Layer Discovery Protocol，链路层发现协议）就是在这样的背景下产生的，它提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。有关 MIB 的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

1.1.2 LLDP基本概念

1. LLDP代理

LLDP代理是LLDP协议运行实体的一个抽象映射。一个接口下，可以运行多个LLDP代理。目前LLDP定义的代理类型包括：Nearest Bridge（最近桥代理）、Nearest Customer Bridge（最近客户桥代理）和Nearest non-TPMR Bridge（最近非TPMR桥代理）。其中TPMR（Two-Port MAC Relay，双端口MAC中继），是一种只有两个可供外部访问桥端口的桥，支持MAC桥的功能子集。TPMR对于所有基于帧的介质无关协议都是透明的，但如下协议除外：以TPMR为目的地址的协议、以保留MAC地址为目的地址但TPMR定义为不予转发的协议。LLDP在相邻的代理之间进行协议报文交互，并基于代理创建及维护邻居信息。如 图 1-1 所示，是LLDP不同类型的代理邻居关系示意图。其中，CB（Customer Bridge，客户桥）和SB（Service Bridge，服务桥）表示LLDP的两种桥模式。

图1-1 LLDP 邻居关系示意图

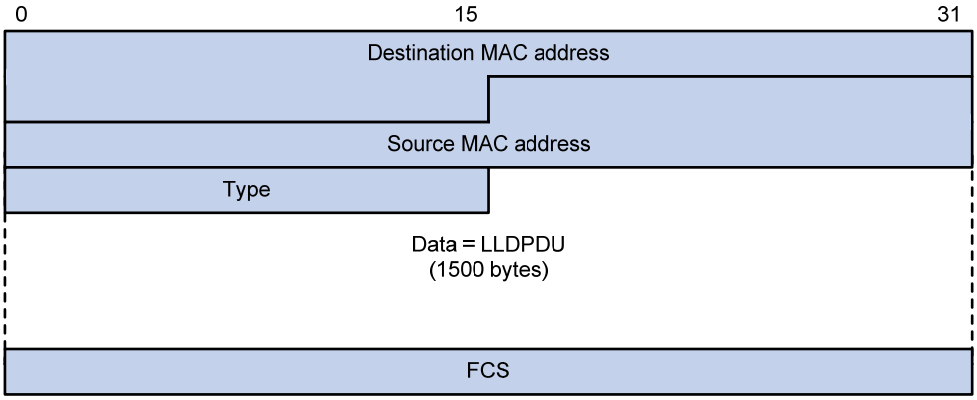


2. LLDP报文

封装有 LLDPDU 的报文称为 LLDP 报文，其封装格式有两种：Ethernet II 和 SNAP（Subnetwork Access Protocol，子网访问协议）。

(1) Ethernet II 格式封装的 LLDP 报文

图1-2 Ethernet II 格式封装的 LLDP 报文

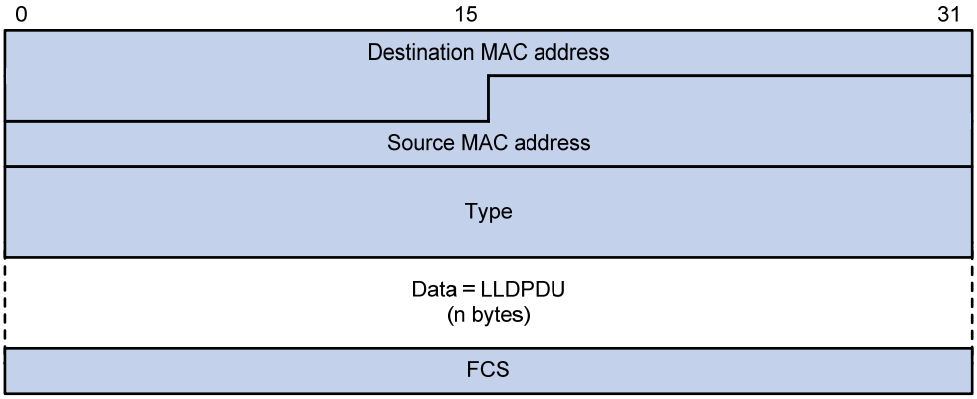


如 图 1-2 所示，是以Ethernet II格式封装的LLDP报文，其中各字段的含义如下：

- Destination MAC address：目的 MAC 地址。为区分同一接口下不同类型代理发送及接收的 LLDP 报文，LLDP 协议规定了不同的组播 MAC 地址作为不同类型代理的 LLDP 报文的目的 MAC 地址。其中固定的组播 MAC 地址 0x0180-C200-000E 供最近桥代理类型的 LLDP 报文使用，0x0180-C200-0000 供最近客户桥代理类型的 LLDP 报文使用，0x0180-C200-0003 供最近非 TPMR 桥代理类型的 LLDP 报文使用。
- Source MAC address：源 MAC 地址，为端口 MAC 地址。
- Type：报文类型，为 0x88CC。
- Data：数据内容，为 LLDPDU。
- FCS：帧检验序列，用来对报文进行校验。

(2) SNAP 格式封装的 LLDP 报文

图1-3 SNAP 格式封装的 LLDP 报文



如 图 1-3 所示，是以SNAP格式封装的LLDP报文，其中各字段的含义如下：

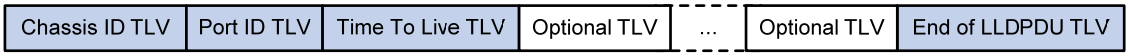
- Destination MAC address：目的 MAC 地址，与 Ethernet II 格式封装的 LLDP 报文目的 MAC 地址相同。
- Source MAC address：源 MAC 地址，为端口 MAC 地址。

- Type：报文类型，为 0xAAAA-0300-0000-88CC。
- Data：数据内容，为 LLDPDU。
- FCS：帧检验序列，用来对报文进行校验。

3. LLDPDU

LLDPDU 就是封装在 LLDP 报文数据部分的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV 格式，再由若干个 TLV 组合成一个 LLDPDU 封装在 LLDP 报文的数据部分进行传送。

图1-4 LLDPDU 的封装格式



如 图 1-4 所示，蓝色的Chassis ID TLV、Port ID TLV、Time To Live TLV和End of LLDPDU TLV这四种TLV是每个LLDPDU都必须携带的，其余的TLV则为可选携带。每个LLDPDU最多可携带 32 种TLV。

4. TLV

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery，链路层发现协议媒体终端发现） TLV。

基本 TLV 是网络设备管理基础的一组 TLV，802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

(1) 基本 TLV

在基本TLV中，有几种TLV对于实现LLDP功能来说是必选的，即必须在LLDPDU中发布，如 表 1-1 所示。

表1-1 基本 TLV

TLV 名称	说明	是否必须发布
Chassis ID	发送设备的桥MAC地址	是
Port ID	标识LLDPDU发送端的端口。如果LLDPDU中携带有LLDP-MED TLV，其内容为端口的MAC地址；否则，其内容为端口的名称	是
Time To Live	本设备信息在邻居设备上的存活时间	是
End of LLDPDU	LLDPDU的结束标识，是LLDPDU的最后一个TLV	是
Port Description	端口的描述	否
System Name	设备的名称	否
System Description	系统的描述	否
System Capabilities	系统的主要功能以及已使能的功能项	否
Management Address	管理地址，以及该地址所对应的接口号和OID（Object Identifier，对象标识符）	否

(2) 802.1 组织定义 TLV

IEEE 802.1 组织定义TLV的内容如 表 1-2 所示。

表1-2 IEEE 802.1 组织定义的 TLV

TLV 名称	说明
Port VLAN ID	端口的PVID（Port VLAN ID）
Port And Protocol VLAN ID	端口的PPVID（Port and Protocol VLAN ID）
VLAN Name	端口所属VLAN的名称
Protocol Identity	端口所支持的协议类型
Link Aggregation	端口是否支持链路聚合以及是否已使能链路聚合
Management VID	管理VLAN
VID Usage Digest	包含VLAN ID使用摘要的数据
ETS Configuration	增强传输选择（Enhanced Transmission Selection）配置
ETS Recommendation	增强传输选择推荐
PFC	基于优先级的流量控制（Priority-based Flow Control）
APP	应用协议（Application Protocol）

说明

- 目前，H3C 设备不支持发送 Protocol Identity TLV 和 VID Usage Digest TLV，但可以接收这两种类型的 TLV。
- 三层以太网接口仅支持 Link Aggregation TLV。

(3) 802.3 组织定义 TLV

IEEE 802.3 组织定义TLV的内容如 表 1-3 所示。

表1-3 IEEE 802.3 组织定义的 TLV

TLV 名称	说明
MAC/PHY Configuration/Status	端口支持的速率和双工状态、是否支持端口速率自动协商、是否已使能自动协商功能以及当前的速率和双工状态
Power Via MDI	端口的供电能力，包括PoE（Power over Ethernet，以太网供电）的类型（包括PSE（Power Sourcing Equipment，供电设备）和PD（Powered Device，受电设备）两种）、PoE端口的远程供电模式、是否支持PSE供电、是否已使能PSE供电以及供电方式是否可控、设备类型、功率来源、功率优先级、PD请求功率值、PSE分配功率值
Maximum Frame Size	端口支持的最大帧长度，取端口配置的MTU（Maximum Transmission Unit，最大传输单元）
Power Stateful Control	端口的电源状态控制，包括PSE/PD所采用的电源类型、供/受电的优先级以及供/受电的功率

说明

Power Stateful Control TLV 是在 IEEE P802.3at D1.0 版本中被定义的，之后的版本不再支持该 TLV。H3C 设备只有在收到 Power Stateful Control TLV 后才会发送该类型的 TLV。

(4) LLDP-MED TLV

LLDP-MED TLV为VoIP（Voice over IP，在IP网络上传送语音）提供了许多高级的应用，包括基本配置、网络策略配置、地址信息以及目录管理等，满足了语音设备的不同生产厂商在投资收效、易部署、易管理等方面的要求，并解决了在以太网中部署语音设备的问题，为语音设备的生产者、销售者以及使用者提供了便利。LLDP-MED TLV的内容如 表 1-4 所示。

表1-4 LLDP-MED TLV

TLV 名称	说明
LLDP-MED Capabilities	网络设备所支持的LLDP-MED TLV类型
Network Policy	网络设备或终端设备上端口的VLAN类型、VLAN ID以及二三层与具体应用类型相关的优先级等
Extended Power-via-MDI	网络设备或终端设备的扩展供电能力，对Power Via MDI TLV进行了扩展
Hardware Revision	终端设备的硬件版本
Firmware Revision	终端设备的固件版本
Software Revision	终端设备的软件版本
Serial Number	终端设备的序列号
Manufacturer Name	终端设备的制造厂商名称
Model Name	终端设备的模块名称
Asset ID	终端设备的资产标识符，以便目录管理和资产跟踪
Location Identification	网络设备的位置标识信息，以供终端设备在基于位置的应用中使用

说明

如果禁止发布 802.3 的组织定义的 MAC/PHY Configuration/Status TLV，则 LLDP-MED TLV 将不会被发布，不论其是否被允许发布；如果禁止发布 LLDP-MED Capabilities TLV，则其他 LLDP-MED TLV 将不会被发布，不论其是否被允许发布。

5. 管理地址

管理地址是供网络管理系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，从而有利于网络拓扑的绘制，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 中向外发布。

1.1.3 LLDP工作机制

1. LLDP的工作模式

在指定类型的 LLDP 代理下，LLDP 有以下四种工作模式：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

2. LLDP报文的发送机制

在指定类型 LLDP 代理下，当端口工作在 TxRx 或 Tx 模式时，设备会周期性地向邻居设备发送 LLDP 报文。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，使用令牌桶机制对 LLDP 报文发送作限速处理。有关令牌桶的详细介绍，请参见“QoS 配置指导”中的“令牌桶”。

当设备的工作模式由 Disable/Rx 切换为 TxRx/Tx，或者发现了新的邻居设备（即收到一个新的 LLDP 报文且本地尚未保存发送该报文设备的信息）时，该设备将自动启用快速发送机制，即将 LLDP 报文的发送周期设置为快速发送周期，并连续发送指定数量的 LLDP 报文后再恢复为正常的发送周期。

3. LLDP报文的接收机制

当端口工作在 TxRx 或 Rx 模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 Time To Live TLV 中 TTL（Time To Live，生存时间）的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

1.1.4 协议规范

与 LLDP 相关的协议规范有：

- IEEE 802.1AB-2005：Station and Media Access Control Connectivity Discovery
- IEEE 802.1AB 2009：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices
- IEEE Std 802.1Qaz™-2011：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes
- IEEE 802.3AT-2009

1.2 LLDP配置任务简介

表1-5 LLDP 配置任务简介

配置任务		说明	详细配置
配置LLDP基本功能	使能LLDP功能	必选	1.3.1

配置任务		说明	详细配置
	配置LLDP桥模式	可选	1.3.2
	配置LLDP工作模式	可选	1.3.3
	配置接口初始化延迟时间	可选	1.3.4
	配置轮询功能	可选	1.3.5
	配置允许发布的TLV类型	可选	1.3.6
	配置管理地址及其封装格式	可选	1.3.7
	调整LLDP相关参数	可选	1.3.8
	配置LLDP报文的封装格式	可选	1.3.9
配置LLDP Trap和LLDP-MED Trap功能		可选	1.5

1.3 配置LLDP基本功能

1.3.1 使能LLDP功能

只有当全局和接口上都使能了 LLDP 功能后，该功能才会生效。

表1-6 使能 LLDP 功能

操作	命令	说明
进入系统视图	**system-view**	-
全局使能LLDP功能	**lldp global enable**	缺省情况下，LLDP全局为关闭状态
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
在接口上使能LLDP功能	**lldp enable**	缺省情况下，LLDP功能在接口上处于使能状态

1.3.2 配置LLDP桥模式

LLDP 可配置桥模式有 service-bridge（服务桥模式）和 customer-bridge（客户桥模式）两种。

- 工作于服务桥模式时，设备可支持最近桥代理和最近非 TPMR 桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。
- 工作于客户桥模式时，设备可支持最近桥代理、最近非 TPMR 桥代理和最近客户桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。

表1-7 配置 LLDP 桥模式

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置LLDP桥模式	**lldp mode service-bridge**	缺省情况下，LLDP工作在客户桥模式

1.3.3 配置LLDP工作模式

LLDP 的工作模式分为以下四种：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

表1-8 配置 LLDP 工作模式

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
配置LLDP的工作模式	在二层以太网接口视图下： **lldp admin-status { disable | rx | tx | txrx }** 在三层以太网接口视图下： **lldp [agent { nearest-customer | nearest-nontpmr }] admin-status { disable | rx | tx | txrx }** 在三层聚合接口视图下： **lldp agent { nearest-customer | nearest-nontpmr } admin-status { disable | rx | tx | txrx }**	缺省情况下，最近桥代理类型的LLDP工作模式为TxRx，最近客户桥代理和最近非TPMR桥代理类型的LLDP工作模式为Disable 以太网接口视图下，未指定agent参数时，表示配置最近桥代理的工作模式 聚合接口视图下，只支持配置最近桥客户桥代理和最近非TPMR代理的工作模式

1.3.4 配置接口初始化延迟时间

当接口上 LLDP 的工作模式发生变化时，接口将对协议状态机进行初始化操作，通过配置接口初始化的延迟时间，可以避免由于工作模式频繁改变而导致接口不断地进行初始化。

表1-9 配置接口初始化延迟时间

操作	命令	说明
进入系统视图	**system-view**	-
配置接口初始化的延迟时间	**lldp timer reinit-delay** *delay*	缺省情况下，接口初始化的延迟时间为2秒

1.3.5 配置轮询功能

在使能了轮询功能后，LLDP 将以轮询间隔周期性地查询本设备的相关配置是否发生改变，如果发生改变将触发 LLDP 报文的发送，以将本设备的配置变化迅速通知给其他设备。

表1-10 配置轮询功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
使能轮询功能并配置轮询间隔	在二层以太网接口视图下： **lldp check-change-interval** *interval* 在三层以太网接口视图下： **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval* 在三层聚合接口视图下： **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*	缺省情况下，轮询功能处于关闭状态

1.3.6 配置允许发布的TLV类型

表1-11 配置允许发布的 TLV 类型

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
配置接口上允许发布的TLV类型（二层以太网接口视图）	**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [m*vlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }	缺省情况下，最近桥代理允许发布除Location-id TLV、Port And Protocol VLAN ID TLV、VLAN Name TLV和Management VLAN ID TLV之外所有类型的TLV

操作	命令	说明
配置接口上允许发布的TLV类型（三层以太网接口视图）	**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } **lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }	缺省情况下： • 最近桥代理允许发布除Network Policy TLV之外所有类型的TLV，其中IEEE 802.1组织定义的TLV只支持Link Aggregation TLV； • 最近非TPMR桥代理不发布任何TLV； • 最近客户桥代理允许发布基本TLV和IEEE 802.1组织定义TLV，其中IEEE 802.1组织定义的TLV只支持Link Aggregation TLV。
配置接口上允许发布的TLV类型（三层聚合接口视图）	**lldp agent** { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }	缺省情况下： • 不存在最近桥代理； • 最近非TPMR桥代理不发布任何TLV； • 最近客户桥代理只允许发布基本TLV。

1.3.7 配置管理地址及其封装格式

管理地址被封装在Management Address TLV中向外发布，封装格式可以是数字或字符串。如果邻居将管理地址以字符串格式封装在TLV中，用户可在本地设备上也将封装格式改为字符串，以保证与邻居设备的正常通信。

表1-12 配置管理地址及其封装格式

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
允许在LLDP报文中发布管理地址并配置所发布的管理地址	在二层以太网接口视图下： **lldp tlv-enable basic-tlv management-address-tlv** [*ip-address*] 在三层以太网接口视图下： **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] 在三层聚合接口视图下： **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv management-address-tlv** [*ip-address*]	缺省情况下，最近桥代理和最近客户桥代理类型的LLDP允许在LLDP报文中发布管理地址，最近非TPMR桥代理类型LLDP不允许在LLDP报文中发布管理地址

操作	命令	说明
配置管理地址在TLV中的封装格式为字符串格式	在二层以太网接口视图下： **lldp management-address-format string** 在三层以太网接口视图下： **lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format string** 在三层聚合接口视图下： **lldp agent { nearest-customer | nearest-nontpmr } management-address-format string**	缺省情况下，管理地址在TLV中的封装格式为数字格式

1.3.8 调整LLDP相关参数

LLDP 报文所携 Time To Live TLV 中 TTL 的值用来设置邻居信息在本地设备上的老化时间，由于 TTL＝Min（65535，（TTL 乘数×LLDP 报文的发送间隔＋1）），即取 65535 与（TTL 乘数×LLDP 报文的发送间隔＋1）中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。

表1-13 调整 LLDP 相关参数

操作	命令	说明
进入系统视图	**system-view**	-
配置TTL乘数	**lldp hold-multiplier** *value*	缺省情况下，TTL乘数为4
配置LLDP报文的发送间隔	**lldp timer tx-interval** *interval*	缺省情况下，LLDP报文的发送间隔为30秒
配置LLDP报文发包限速的令牌桶大小	**lldp max-credit** *credit-value*	缺省情况下，发包限速令牌桶大小为5
配置快速发送LLDP报文的个数	**lldp fast-count** *count*	缺省情况下，快速发送LLDP报文的个数为4个
配置快速发送LLDP报文的间隔	**lldp timer fast-interval** *interval*	缺省情况下，快速发送LLDP报文的发送间隔为1秒

1.3.9 配置LLDP报文的封装格式

LLDP 报文的封装格式有 Ethernet II 和 SNAP 两种：

- 当采用 Ethernet II 封装格式时，使能了 LLDP 功能的接口所发送的 LLDP 报文将以 Ethernet II 格式封装。
- 当采用 SNAP 封装格式时，使能了 LLDP 功能的接口所发送的 LLDP 报文将以 SNAP 格式封装。

需要注意的是，LLDP 早期版本要求只有配置为相同的封装格式才能处理该格式的 LLDP 报文，因此为了确保与运行 LLDP 早期版本的设备稳定通信，建议配置为与之相同的封装格式。

表1-14 配置 LLDP 报文的封装格式

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
配置LLDP报文的封装格式为SNAP格式	在二层以太网接口视图下： **lldp encapsulation snap** 在三层以太网接口视图下： **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap** 在三层聚合接口视图下： **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**	缺省情况下，LLDP报文的封装格式为Ethernet II格式

1.4 配置LLDP兼容CDP功能

1.4.1 配置准备

在配置 LLDP 兼容 CDP 功能之前，需完成以下任务：

- 全局使能 LLDP 功能。
- 在设备与 IP 电话相连接的接口上使能 LLDP 功能，并配置接口的 LLDP 工作模式为 TxRx。

1.4.2 配置LLDP兼容CDP功能

LLDP 兼容 CDP 功能有以下两种工作模式：

- TxRx：既发送也接收 CDP 报文。
- Disable：既不发送也不接收 CDP 报文。

要使 LLDP 兼容 CDP 功能生效，必须先在全局使能 LLDP 兼容 CDP 功能，并将 LLDP 兼容 CDP 功能的工作模式配置为 TxRx。

提示

由于 CDP 报文所携 Time To Live TLV 中 TTL 的最大值为 255，而 CDP 报文的发送间隔由 LLDP 报文的发送间隔控制，因此为保证 LLDP 兼容 CDP 功能的正常运行，建议配置 LLDP 报文的发送间隔值不大于实际 TTL 的 1/3。

表1-15 配置 LLDP 兼容 CDP 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能LLDP兼容CDP功能	**lldp compliance cdp**	缺省情况下，LLDP兼容CDP功能处于关闭状态

操作	命令	说明
进入二层/三层以太网接口视图	**interface** *interface-type interface-number*	-
配置LLDP兼容CDP功能的工作模式为TxRx	**lldp compliance admin-status cdp txrx**	缺省情况下，LLDP兼容CDP功能的工作模式为Disable

1.5 配置LLDP Trap和LLDP-MED Trap功能

使能 LLDP Trap 或 LLDP-MED Trap 功能后，设备可以通过向网管系统发送 Trap 信息以通告如发现新的 LLDP 邻居或 LLDP-MED 邻居、与原来邻居的通信链路发生故障等重要事件。

LLDP Trap 和 LLDP-MED Trap 信息的发送间隔是指设备向网管系统发送 Trap 信息的最小时间间隔，通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。

表1-16 配置 LLDP Trap 和 LLDP-MED Trap 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二/三层以太网接口或三层聚合接口视图	**interface** *interface-type interface-number*	
使能LLDP Trap功能	在二层以太网接口视图下： **lldp notification remote-change enable** 在三层以太网接口视图下： **lldp [agent { nearest-customer | nearest-nontpmr }] notification remote-change enable** 在三层聚合接口视图下： **lldp agent { nearest-customer | nearest-nontpmr } notification remote-change enable**	缺省情况下，LLDP Trap功能处于关闭状态
使能LLDP-MED Trap功能	在二/三层以太网接口视图下： **lldp notification med-topology-change enable**	缺省情况下，LLDP-MED Trap功能处于关闭状态
退回系统视图	**quit**	-
（可选）配置LLDP Trap和LLDP-MED Trap信息的发送间隔	**lldp timer notification-interval** *interval*	缺省情况下，LLDP Trap和LLDP-MED Trap信息的发送间隔均为30秒

1.6 LLDP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 LLDP 的运行情况，通过查看显示信息验证配置的效果。

表1-17 LLDP 显示和维护

操作	命令
显示LLDP本地信息	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
显示由邻居设备发来的LLDP信息	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]
显示LLDP的统计信息	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]
显示LLDP的状态信息	**display lldp status** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]
显示接口上可发送的可选TLV信息	**display lldp tlv-config** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

1.7 LLDP典型配置举例

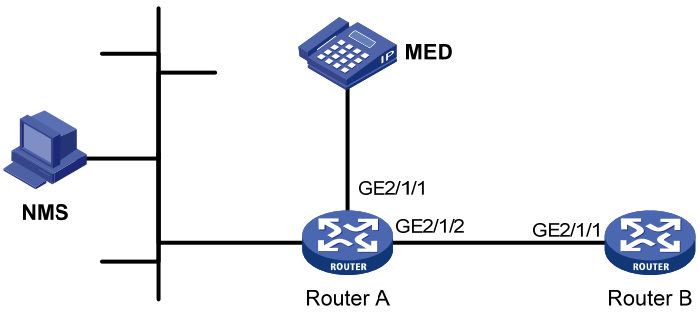
1.7.1 LLDP基本功能配置举例

1. 组网需求

- NMS（Network Management System，网络管理系统）通过以太网与 Router A 相连，Router A 通过接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 分别与 MED 设备和 Router B 相连。
- 通过在 Router A 和 Router B 上配置 LLDP 功能，使 NMS 可以对 Router A 与 MED 设备之间、以及 Router A 与 Router B 之间链路的通信情况进行判断。

2. 组网图

图1-5 LLDP 基本功能配置组网图



3. 配置步骤

(1) 配置 Router A

全局使能 LLDP 功能。

```
<RouterA> system-view
[RouterA] lldp global enable
```

在接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 上分别使能 LLDP 功能（此步骤可省略，LLDP 功能在接口上缺省使能），并配置 LLDP 工作模式为 Rx。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] lldp enable
[RouterA-GigabitEthernet2/1/1] lldp admin-status rx
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] lldp enable
[RouterA-GigabitEthernet2/1/2] lldp admin-status rx
[RouterA-GigabitEthernet2/1/2] quit
```

(2) 配置 Router B

全局使能 LLDP 功能。

```
<RouterB> system-view
[RouterB] lldp global enable
```

在接口 GigabitEthernet2/1/1 上使能 LLDP 功能（此步骤可省略，LLDP 功能在接口上缺省使能），并配置 LLDP 工作模式为 Tx。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] lldp enable
[RouterB-GigabitEthernet2/1/1] lldp admin-status tx
[RouterB-GigabitEthernet2/1/1] quit
```

4. 验证配置

显示 Router A 上全局和所有接口的 LLDP 状态信息。

```
[RouterA] display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet2/1/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
```

```
Number of sent optional TLV    : 21
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet2/1/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 3

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
```

```
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

由此可见，Router A 的接口 GigabitEthernet2/1/1 上连接了一个 MED 邻居设备，GigabitEthernet2/1/2 上则连接了一个非 MED 邻居设备，且这两个接口的 LLDP 工作模式都为 Rx，即只接收而不发送 LLDP 报文。

将 Router A 和 Router B 间的链路断掉后，再显示 Router A 上所有接口的 LLDP 状态信息。

```
[RouterA] display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet2/1/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disabl
```

```
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet2/1/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

由此可见，Router A 的接口 GigabitEthernet2/1/2 上已经没有任何邻居设备了。