H3C S5500-HI 系列以太网交换机

二层技术-以太网交换配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20131220
产品版本：Release 52xx 系列

前 言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本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》主要介绍了以太网交换技术的原理及具体配置方法。通过这些技术您可以实现流量控制、流量的负载分担、同一 VLAN 内用户隔离、二层环路消除、VLAN 划分、私网报文穿越公网、修改报文的 VLAN Tag 等功能。

前言部分包含如下内容：

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

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与Release5203 版本相比，新增、修改了部分特性，具体请参见 表 1。
- Release5203 与Release5101 版本相比，新增、修改了部分特性，具体请参见 表 2。

表1 Release5206 与 Release5203 版本间特性差异

配置指导	新增及修改特性
以太网端口	变更特性：显示接口概要信息时，如果某接口的描述信息超过27个字符，不指定description参数时，只显示描述信息中的前27个字符，超出部分不显示；指定description参数时，可以显示全部描述信息
Loopback接口和Null接口	变更特性：显示接口概要信息时，如果某接口的描述信息超过27个字符，不指定description参数时，只显示描述信息中的前27个字符，超出部分不显示；指定description参数时，可以显示全部描述信息
端口批量配置	无

配置指导		新增及修改特性
MAC地址表	MAC地址表配置	无
	MAC Information配置	无
以太网链路聚合		变更特性：显示接口概要信息时，如果某接口的描述信息超过27个字符，不指定description参数时，只显示描述信息中的前27个字符，超出部分不显示；指定description参数时，可以显示全部描述信息
端口隔离		无
生成树		无
BPDU Tunnel		无
VLAN	VLAN配置	变更特性：显示接口概要信息时，如果某接口的描述信息超过27个字符，不指定description参数时，只显示描述信息中的前27个字符，超出部分不显示；指定description参数时，可以显示全部描述信息
	Super VLAN配置	无
	Isolate-user-VLAN配置	无
	Voice VLAN配置	无
GVRP		无
QinQ		无
VLAN映射		无
LLDP		无
业务环回组		无
MVRP		无

表2 Release5203 与 Release5101 版本间特性差异

配置指导		新增及修改特性
以太网端口		无
Loopback接口和Null接口		无
端口批量配置		无
MAC地址表	MAC地址表配置	新增特性： • 关闭基于目的 MAC 地址刷新老化时间 • MAC 地址迁移日志上报
	MAC Information配置	无

配置指导		新增及修改特性
以太网链路聚合		新增特性： • 根据报文的 MPLS 标签进行聚合负载分担 • 配置三层聚合接口下的聚合负载分担类型 • 配置聚合组中最大选中端口数
端口隔离		无
生成树		无
BPDU Tunnel		无
VLAN	VLAN配置	无
	Super VLAN 配置	无
	Isolate-user-VLAN配置	无
	Voice VLAN 配置	新增特性： • 通过 LLDP 自动发现 IP 电话功能 • 指定 LLDP 发布的 Voice VLAN 信息 • 通过 LLDP 动态发布授权 VLAN 功能 修改特性： 设备可配置的Voice VLAN OUI地址从16个变更到128个
GVRP		无
QinQ		无
VLAN映射		无
LLDP		修改特性：LLDP兼容CDP功能中，设备发送的CDP报文新增部分字段（Addresses、Capabilities、Software Version、Platform、Duplex、MTU、System Name）
业务环回组		无
MVRP		MVRP为本版本新增特性

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。

格　式	意　义
[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. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 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。

4. 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。

5. 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 S5500-HI 系列以太网交换机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	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	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
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	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	故障处理手册	指导您快速定位并处理软件故障
	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 以太网端口配置

1.1 端口简介

1.1.1 以太网端口的端口编号规则

本系列交换机的端口均采用 3 位编号方式：interface type A/B/C。

- A：IRF 中成员设备的编号，若未形成 IRF，其取值为 1。
- B：设备上的槽位号。取值为 0，表示设备上固有端口所在的槽位；取值为 1，表示接口模块扩展卡 1 上端口所在的槽位；取值为 2，表示接口模块扩展卡 2 上端口所在的槽位。
- C：某槽位上的端口编号

说明

当设备上插有 GE 接口模块扩展卡时，GE 接口模块扩展卡上的千兆端口在设备上显示为万兆端口。

1.2 以太网端口通用配置

本节将介绍二层以太网端口和三层以太网端口的共有属性及配置。

- 二层以太网端口的特有配置，请参见“1.3 二层以太网端口配置”。
- 三层以太网端口的特有配置，请参见“1.4 三层以太网端口配置”。

1.2.1 管理用以太网口配置

1. 管理用以太网口介绍

该端口采用 RJ-45 连接器，可用来连接后台计算机以进行系统的程序加载、调试等工作。

2. 管理用以太网口基本配置

表1-1 管理用以太网口基本配置

操作	命令	说明
进入系统视图	**system-view**	-
进入管理用以太网口视图	**interface M-GigabitEthernet** *interface-number*	-
设置当前管理用以太网口的描述信息	**description** *text*	可选 缺省情况下，管理用以太网口的描述信息为M-GigabitEthernet0/0/0 Interface
关闭管理用以太网口	**shutdown**	可选 缺省情况下，管理用以太网口处于打开状态

操作	命令	说明
恢复管理用以太网口的缺省配置	**default**	可选

1.2.2 以太网端口基本配置

1. 以太网端口基本配置

设置以太网端口的双工模式时存在三种情况：

- 当希望端口在发送数据包的同时可以接收数据包，可以将端口设置为全双工（**full**）属性；
- 当希望端口同一时刻只能发送数据包或接收数据包时，可以将端口设置为半双工（**half**）属性；
- 当设置端口为自协商（**auto**）状态时，端口的双工状态由本端口和对端端口自动协商而定。

设置以太网端口的速率时，当设置端口速率为自协商（**auto**）状态时，端口的速率由本端口和对端端口双方自动协商而定。对于千兆二层以太网端口，可以根据端口的速率自协商能力，指定自协商速率，让速率在指定范围内协商，具体配置请参见“1.3.3 配置以太网端口自协商速率”。

表1-2 以太网端口基本配置

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
设置当前端口的描述信息	**description** *text*	可选 缺省情况下，端口的描述信息为“*端口名* Interface”，比如：GigabitEthernet1/0/1 Interface
设置以太网端口的双工模式	**duplex** { **auto** | **full** | **half** }	可选 光类型端口和配置了端口速率为1000的以太网电口不支持配置**half**参数 缺省情况下，以太网端口的双工模式为**auto**（自协商）状态
设置以太网端口的速率	**speed** { **10** | **100** | **1000** | **10000** | **auto** }	可选 千兆光口不支持配置**10**和**10000**参数，万兆光口不支持配置**10**和**100**参数，千兆电口不支持配置**10000**参数 缺省情况下，以太网端口的速率为**auto**（自协商）状态
恢复当前端口的缺省配置	**default**	可选

说明

对于光类型端口，配置的速率必须与插入的光模块速率匹配，如插入千兆光模块时，需配置 **speed** 命令的参数为 **1000** 或 **auto**。

1.2.3 关闭以太网端口

在某些特殊情况下（比如切换了端口的速率或双工模式等），端口相关配置不能立即生效，需要关闭和激活端口后，才能生效。

表1-3 关闭以太网端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 在以太网端口视图下的配置，只在当前端口下生效；在端口组视图下的配置在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
关闭当前端口		**shutdown**	必选 缺省情况下，端口处于激活状态

注意

手工关闭端口，即便端口物理上是连通的，也不能转发报文，请谨慎使用本特性。

1.2.4 配置以太网端口的流量控制功能

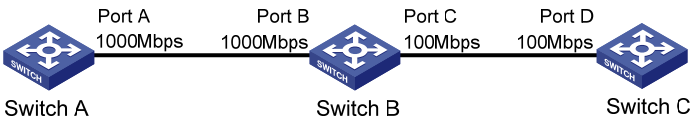
以太网端口流量控制功能的基本原理是：如果本端设备发生拥塞，它将向对端设备发送消息，通知对端设备暂时停止发送报文；而对端设备在接收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生。

流量控制功能通过端口收/发 pause 帧来实现。流量控制的工作模式有两种：

- 收发模式（配置 **flow-control** 命令）：端口既能接收、又能发送 pause 帧；
- 接收模式（配置 **flow-control receive enable** 命令）：端口只能接收、不能发送 pause 帧。

如 图 1-1 所示，当Port A和Port B以 1000 Mbps速率转发报文时，Port C将发生拥塞。为避免报文丢失，在Port A和Port B开启流量控制功能。

图1-1 端口的流量控制



配置 Port B 工作在收发模式、配置 Port A 工作在接收模式：

- 当 Port C 转发报文出现拥塞时，Switch B 会缓冲报文，当缓冲报文达到一定值后，Switch B 知道从 Port B 发往 Port C 的流量过大，超过了 Port C 的转发能力。这时，处于收发模式的 Port B 会向 Port A 发送 pause 帧，通知 Port A 暂时停止发送报文；
- Port A 在接收到该 pause 帧后会暂时停止向 Port B 发送报文，暂停时间长短信息由 pause 帧所携带。当拥塞仍然存在时，Port B 就会一直向 Port A 发送 pause 帧，直至拥塞解除。

因此，如果要应对单向网络拥塞的情况，可以在一端配置 **flow-control receive enable**，在对端配置 **flow-control**；如果要求本端和对端网络拥塞都能处理，则两端都必须配置 **flow-control**。

表1-4 开启以太网端口的流量控制功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
开启以太网端口的流量控制功能	**flow-control**	二者必选其一 缺省情况下，以太网端口的接收流量控制功能处于关闭状态
配置以太网端口的接收流量控制功能	**flow-control receive enable**	

说明

开启或关闭流量控制功能可能会使接口产生 down/up 状态切换，请开启或关闭此功能时做好相关准备。

1.2.5 配置以太网端口down/up状态抑制时间

以太网端口有两种物理连接状态：up 和 down。一般情况下，端口的物理连接状态在 up 与 down 之间切换时，物理层会向系统报告物理端口连接状态的变化。

若在端口上配置了以太网端口 down 状态抑制时间后，每次当端口的物理连接状态从 up 变为 down 时，便触发以太网端口 down 状态抑制机制，在该抑制时间内，系统认为端口仍然处于 up 状态。当 down 状态抑制时间到达后，若端口状态仍然为 down 时，物理层再向系统报告物理连接状态的变化。

若在端口上配置了以太网端口 up 状态抑制时间后，每次当端口的物理连接状态从 down 变为 up 时，便触发以太网端口 up 状态抑制机制，在该抑制时间内，系统认为端口仍然处于 down 状态。当 up 状态抑制时间到达后，若端口状态仍然为 up 时，物理层再向系统报告物理连接状态的变化。

以太网端口 down /up 状态抑制功能用于避免因端口在短时间内频繁改变物理连接状态，给系统带来额外的开销。

表1-5 设置以太网端口 down 状态抑制时间

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
设置以太网端口物理连接状态抑制时间	**link-delay** *delay-time*	必选 缺省情况下，没有使能以太网端口down状态抑制功能

表1-6 设置以太网端口 up 状态抑制时间

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
设置以太网端口up状态抑制时间	**link-delay** *delay-time* **mode up**	必选 缺省情况下，没有使能以太网端口up状态抑制功能

说明

- **link-delay mode up** 和 **link-delay** 命令相互覆盖，即若在同一端口上多次使用这两条命令设置抑制时间，只有最新配置生效。
- **link-delay/link-delay mode up** 命令对自然关闭/开启的端口有效，对手工关闭/开启（使用 **shutdown/undo shutdown** 命令）的端口无效。
- 当在端口上使用 **link-delay** 命令设置了以太网端口 down 状态抑制时间后，若该端口的物理连接状态从 up 变为 down 时，在该设置的抑制时间内使用 **display interface brief** 或 **display interface** 命令将显示该端口一直处于 up 状态。
- 当在端口上使用 **link-delay mode up** 命令设置了以太网端口 up 状态抑制时间后，若该端口的物理连接状态从 down 变为 up 时，在该设置的抑制时间内使用 **display interface brief** 或 **display interface** 命令将显示该端口一直处于 down 状态。

1.2.6 配置以太网端口环回测试功能

用户可以开启以太网端口环回测试功能，检验以太网端口能否正常工作。测试时端口将不能正常转发数据包。以太网端口环回测试功能包括内部环回测试和外部环回测试。

- 内部环回测试：该测试在交换芯片内部建立自环，用以定位芯片内与该端口相关的功能是否出现故障。
- 外部环回测试：该测试需要在以太网端口上接一个自环头，从端口发出的报文通过自环头又环回到该端口，并被该端口接收。用以定位该端口的硬件功能是否出现故障。

表1-7 配置以太网端口环回测试功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置以太网端口进行环回测试	**loopback** { **external** | **internal** }	可选 缺省情况下，以太网端口环回测试功能处于关闭状态

说明

- 端口在手工关闭状态（即端口状态显示为 ADM 或者 Administratively DOWN）下不能进行内部和外部环回测试。
- 以太网端口开启环回测试功能时将工作在全双工状态；关闭环回测试功能后恢复原有配置。
- 环回测试配置是一次性操作，不会被记录在配置文件中。

1.2.7 以太网端口二三层模式切换

本系列交换机的端口比较灵活，可以通过配置来改变其链路模式：在二层模式（bridge）下，该端口作为一个二层以太网端口使用；而在三层模式（route）下，该端口作为一个三层以太网端口使用。

表1-8 切换以太网端口的链路模式

操作		命令	说明
进入系统视图		**system-view**	-
切换以太网端口的链路模式	系统视图下的配置	**port link-mode** { **bridge** | **route** } *interface-list*	二者必选其一
	以太网端口视图下的配置	**interface** *interface-type interface-number* **port link-mode** { **bridge** | **route** }	

注意

- 链路模式切换后，该以太网端口下的所有配置都将恢复到新模式下的缺省配置。
- 以太网端口的链路模式既可以在系统视图下配置也可以在以太网端口视图下配置。当两种视图下配置的链路模式不同时，最新的配置生效。

1.2.8 配置允许长帧通过以太网端口

以太网端口在进行文件传输等大吞吐量数据交换的时候，可能会收到大于标准以太网帧长的长帧，对于这样的长帧，系统会直接丢弃不再进行处理。配置允许长帧通过功能后，当端口收到大于标准长度又在参数指定长度范围内的长帧时，系统会继续处理。

用户可以通过端口下（以太网端口视图或端口组视图下）的配置方式设置允许指定长度的长帧通过以太网端口：

- 在以太网端口视图下执行该命令，则该配置只在当前端口下生效；
- 在端口组视图下执行该命令，则该配置在端口组中的所有端口下生效。

表1-9 配置允许长帧通过以太网端口

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
设置允许长帧通过	**jumboframe enable** [*value*]	必选 缺省情况下，系统允许最大长度为12288字节的帧通过以太网端口。多次执行该命令配置不同的*value*值时，则最新的配置生效

1.2.9 配置以太网端口节能功能

1. 配置down状态接口节能功能

配置 down 状态接口节能功能后，如果在连续一段时间（由芯片规格决定，不能通过命令行配置）内接口状态始终为 down，则系统会自动停止对该接口供电，接口自动进入节能模式；当接口状态变为 up 时，系统会自动对该接口供电，接口自动进入正常模式，从而达到节能的效果。

表1-10 配置 down 状态端口节能功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	必选
配置down状态端口节能功能	**port auto-power-down**	必选 缺省情况下，该功能处于关闭状态

说明

使用开启此功能的端口与其他设备进行对接时，若链路不能正常 UP，可尝试关闭此功能。

2. 使能EEE节能功能

端口使能 EEE（Energy Efficient Ethernet）节能功能后，如果在连续一段时间（由芯片规格决定，不能通过命令行配置）内端口状态始终为 up 且没有收发任何报文，则端口自动进入节能模式；当端口需要收发报文时，端口又自动恢复工作模式，从而达到节能的效果。

表1-11 使能 EEE 节能功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
使能EEE节能功能	**eee enable**	必选 缺省情况下，没有使能EEE节能功能

说明

- 如果当前端口的配置信息为速率 100M 和全双工模式下使用 EEE 功能，该端口在进入节能模式后将不会自动 up，需要将双工模式配置为 auto 方可 up 此端口。
- 开启 EEE 功能可能会降低 STP、Smart Link、Monitor Link、RRPP、以太网链路聚合的收敛性能，建议在配置了上述协议情况下不使用 EEE 节能功能。

1.3 二层以太网端口配置

1.3.1 二层以太网端口配置任务简介

当以太网端口工作在二层模式（bridge）时，可以进行以下配置：

表1-12 二层以太网端口配置任务简介

配置任务	说明	详细配置
配置端口组	可选 二层以太网端口支持	1.3.2
配置以太网端口自协商速率	可选 二层以太网端口支持	1.3.3
配置以太网端口的风暴抑制比	可选 二层以太网端口支持	1.3.4
配置以太网端口统计信息的时间间隔	可选 二层以太网端口支持	1.3.5
配置以太网端口进行环回监测	可选 二层以太网端口支持	1.3.6
配置以太网端口的MDI模式	可选 二层以太网端口支持	1.3.7
检测以太网端口的连接电缆	可选 二层以太网端口支持	1.3.9
配置以太网端口桥功能	可选 二层以太网端口支持	1.3.8
配置以太网端口流量阈值控制功能	可选 二层以太网端口支持	1.3.10

1.3.2 配置端口组

对某些功能（比如“1.3.4 配置以太网端口的风暴抑制比”等），设备支持多种配置方式：用户可以一次配置一个端口，也可以一次配置多个端口。端口组就是为了实现一次可以配置多个端口而产生的。在端口组视图下，用户只需输入一次配置命令，则该端口组内的所有端口都会配置该功能，以减少重复配置工作。

端口组由用户手工创建生成，用户可将多个二层以太网端口手工加入同一个端口组中。

端口组提供了一种批量配置的方式，系统不支持查看、保存端口组本身的配置，但可以通过 **display current-configuration** 或者 **display this** 命令查看成员端口下当前生效配置。

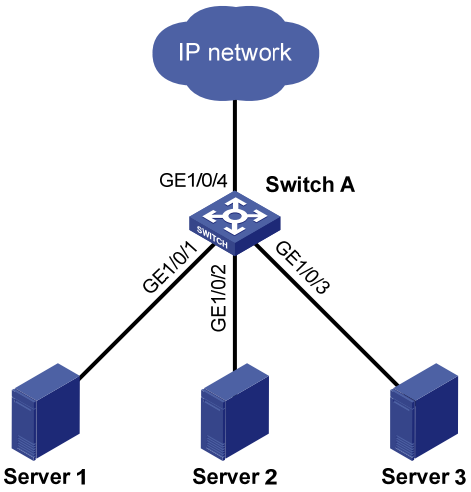
表1-13 配置手工端口组

操作	命令	说明
进入系统视图	**system-view**	-
创建手工端口组，并进入手工端口组视图	**port-group manual** *port-group-name*	必选
添加二层以太网端口到指定手工端口组中	**group-member** *interface-list*	必选 如果使用**group-member** *interface-type interface-start-number* **to** *interface-type interface-end-number*命令形式一次将多个端口加入到指定手工端口组中时，要求本次加入的所有端口的*interface-end-number*必须大于*interface-start-number*
设置允许长帧通过	**jumboframe enable** [*value*]	必选 缺省情况下，系统允许最大长度为12288字节的帧通过以太网端口。多次执行该命令配置不同的*value*值时，则最新的配置生效

1.3.3 配置以太网端口自协商速率

通常情况下，设备以太网端口速率是通过和对端自协商决定的。协商得到的速率可以是端口速率能力范围内的任意一个速率。通过配置自协商速率可以让以太网端口在能力范围内只协商部分速率，从而可以控制速率的协商。

图1-2 以太网端口自协商速率应用示意图



如 图 1-2 所示，服务器群（Server 1、Server 2 和Server 3）通过Switch A与外部网络相连，该服务器群中每台服务器的网卡速率均为 1000Mbps，Switch A与外部网络相连端口GigabitEthernet1/0/4 的速率也为 1000Mbps。如果在Switch A上不指定自协商速率范围，则端口GigabitEthernet1/0/1、GigabitEthernet1/0/2 和GigabitEthernet1/0/3 与各服务器网卡进行速率协商的结果将均为 1000Mbps，这样就可能造成出端口GigabitEthernet1/0/4 的拥塞。在这种情况下，可通过将端口GigabitEthernet1/0/1、GigabitEthernet1/0/2 和GigabitEthernet1/0/3 的自协商速率范围分别设置为 100Mbps，来避免出端口的拥塞

表1-14 配置以太网端口自协商速率

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
设置以太网端口的自协商速率范围	**speed auto** { **10** | **100** | **1000** } *	可选

说明

- 本特性只有具备自协商速率能力的、千兆二层以太网电口支持。
- 如果多次使用 **speed**、**speed auto** 命令设置端口的速率，则最新配置生效。

1.3.4 配置以太网端口的风暴抑制比

用户可以在端口下进行配置，设置端口允许通过的最大广播、组播或未知单播报文流量。当端口上的广播、组播或未知单播流量超过用户设置的值后，系统将丢弃超出广播、组播或未知单播流量限制的报文，从而使端口广播、组播或未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

说明

本特性与端口流量阈值控制功能**storm-constrain**不能同时配置，否则抑制效果不确定。端口流量阈值控制功能的详细描述请参见“1.3.10 配置以太网端口流量阈值控制功能”。

表1-15 配置以太网端口的风暴抑制比

操作		命令	说明
进入系统视图		**system-view**	-
进入以太网端口视图或端口组视图	进入以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 在以太网端口视图下的配置，只在当前端口下生效；在端口组视图下的配置在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置以太网端口的广播风暴抑制比		**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	可选 缺省情况下，所有端口不对广播流量进行抑制
配置以太网端口的组播风暴抑制比例		**multicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	可选 缺省情况下，所有端口不对组播流量进行抑制
配置以太网端口的未知单播风暴抑制比		**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	可选 缺省情况下，所有端口不对未知单播流量进行抑制

说明

如果端口属于某个端口组，在以太网端口视图或端口组视图下多次配置不同的抑制比数值时，则最新的配置生效。

1.3.5 配置以太网端口统计信息的时间间隔

使用以下的配置任务可以设置统计以太网端口报文信息的时间间隔。使用 **display interface** 命令可以显示端口在该间隔时间内统计的报文信息。使用 **reset counters interface** 命令可以清除端口的统计信息。

表1-16 配置以太网端口统计信息的时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置端口统计信息的时间间隔	**flow-interval** *interval*	必选 端口统计信息的缺省时间间隔为300秒

1.3.6 配置以太网端口进行环回监测

端口发生环回是指设备发送出去的报文又回到该设备。环回的存在可能导致广播风暴，使用本特性能够监测设备端口是否存在环回。

根据发生环回时，报文的收、发端口是否相同，端口环回分为单端口环回和多端口环回：

- 单端口环回指的是端口发送出去的报文又从该端口回到设备，报文的接收和发送端口相同，如 图 1-3 所示。
- 多端口环回指的是设备上某端口发送出去的报文又从该设备的另一个端口环回到本设备，如 图 1-4 所示。从设备上Port 1 发送的报文又从Port 2 接收到，则认为Port 1 与Port 2 之间存在环回（接收到环回报文的端口Port 2 为被环回端口）。

图1-3 单端口环回示意图

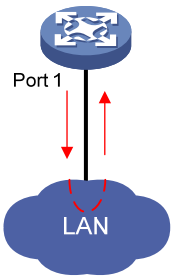
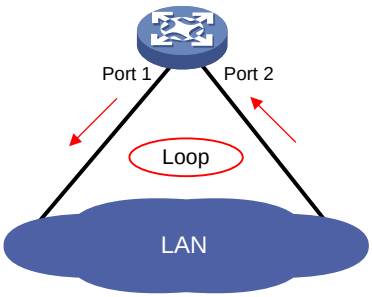


图1-4 多端口环回示意图



当用户开启以太网端口环回监测功能后，如果监测到端口存在环回，设备会根据环回监测动作对报文的接收端口进行相应的操作：

(1) 对于 Access 端口，

- 若端口未配置环回监测动作（未使用 **loopback-detection action** 命令指定监测动作），则将报文的接收端口变为监测受控状态。处于该状态的端口入方向报文将被丢弃，出方向报文不受影响，并生成 Trap 信息和日志信息，同时删除该端口对应的 MAC 地址转发表项；

- 若端口配置了环回监测动作（使用 **loopback-detection action** 命令指定监测动作），则按照环回监测动作对报文的接收端口进行处理，并生成 Trap 信息和日志信息，同时删除该端口对应的 MAC 地址转发表项；

(2) 对于 Trunk 端口和 Hybrid 端口，

- 若端口未配置环回监测动作，则生成 Trap 信息和日志信息。当端口环回监测受控功能也同时开启时（即配置了 **loopback-detection control enable**），则将报文的接收端口变为监测受控状态，处于该状态的端口将不收发任何数据报文，并生成 Trap 信息和日志信息，同时删除该端口对应的 MAC 地址转发表项。
- 若端口配置了环回监测动作，则生成 Trap 信息和日志信息。当端口环回监测受控功能也同时开启时（即配置了 **loopback-detection control enable**），按照环回监测动作对报文的接收端口进行处理，并向终端上报 Trap 信息和日志信息，同时删除该端口对应的 MAC 地址转发表项。

表1-17 配置以太网端口进行环回监测

操作		命令	说明
进入系统视图		**system-view**	-
开启全局的端口环回监测功能		**loopback-detection enable**	必选 缺省情况下，全局的端口环回监测功能处于关闭状态
开启多端口环回监测模式		**loopback-detection multi-port-mode enable**	可选 缺省情况下，多端口环回监测模式处于关闭状态，即设备只能检测到单端口环回
设置端口环回监测的时间间隔		**loopback-detection interval-time** *time*	可选 缺省情况下，端口环回监测的时间间隔为30秒
进入以太网端口视图或端口组视图	进入以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 在以太网端口视图下的配置，只在当前端口下生效；在端口组视图下的配置在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
开启指定端口的环回监测功能		**loopback-detection enable**	必选 缺省情况下，端口环回监测功能处于关闭状态
开启Trunk端口和Hybrid端口的环回监测受控功能		**loopback-detection control enable**	可选 缺省情况下，端口的环回监测受控功能处于关闭状态
配置在Trunk端口和Hybrid端口允许通过的所有VLAN内进行环回监测		**loopback-detection per-vlan enable**	可选 缺省情况下，系统只在Trunk端口和Hybrid端口的缺省VLAN内进行环回监测

操作	命令	说明
配置在发现端口环回后对端口进行的动作	**loopback-detection action { no-learning | semi-block | shutdown }**	可选 缺省情况下，对被环回端口进行的动作为：端口入方向报文将被丢弃，出方向报文不受影响，并生成Trap信息和日志信息，同时删除该端口对应的MAC地址转发表项 如果指定动作为**shutdown**，则被环回的端口会被系统关闭，端口物理状态为Loop down。环回消除后，需要手工执行**undo shutdown**命令才能恢复端口的转发能力

注意

- 只有在系统视图下和指定端口视图下均配置了 **loopback-detection enable** 命令后，才开启端口的环回监测功能。
- 设备在实现多端口环回监测的同时，也可进行单端口环回监测。
- 当在系统视图下配置 **undo loopback-detection enable** 后，所有端口的环回监测功能均被关闭。
- 对于 Trunk 端口或 Hybrid 端口，在指定端口视图下配置了 **loopback-detection control enable** 命令后，该端口的环回监测动作才生效。
- 当使用 **port link-type { access | hybrid | trunk }**命令修改端口的链路类型后，该端口下的 **loopback-detection action** 配置会自动恢复到缺省情况。（**port link-type** 命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“VLAN”）

1.3.7 配置以太网端口的MDI模式

说明

光口不支持本特性。

用于连接以太网设备的双绞线有两种：直通线缆（straight-through cable）和交叉线缆（crossover cable）。为了使以太网端口支持使用这两种线缆，设备实现了三种 MDI（Medium Dependent Interface，介质相关端口）模式：**across**、**normal** 和 **auto**。

物理以太网端口由 8 个引脚组成，缺省情况下，每个引脚都有专门的作用，比如，使用引脚 1 和 2 发送信号，引脚 3 和 6 接收信号。通过设置 MDI 模式，可以改变引脚在通信中的角色。使用 normal 模式时，不改变引脚的角色，即使用引脚 1 和 2 发送信号，使用引脚 3 和 6 接收信号；如果使用 across 模式，会改变引脚的角色，将使用引脚 1 和 2 接收信号，而使用引脚 3 和 6 发送信号。只有将设备的发送引脚连接到对端的接收引脚后才能正常通信，所以 MDI 模式需要和两种线缆配合使用。

- 通常情况下，建议用户使用 **auto** 模式，只有当设备不能获取网线类型参数时，才需要将模式手工指定为 **across** 或 **normal**。
- 当使用直通线缆时，两端设备的 MDI 模式配置不能相同。
- 当使用交叉线缆时，两端设备的 MDI 模式配置必须相同或者至少有一端设置为 auto 模式。

表1-18 配置以太网端口的 MDI 模式

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
设置以太网端口的MDI模式	**mdi** { **across** | **auto** | **normal** }	可选 以太网端口的MDI模式为auto，即通过协商来决定物理引脚的角色（发送报文或接收报文）

1.3.8 配置以太网端口桥功能

缺省情况下，某端口收到数据报文后：

- 对于已知报文（如单播、组播），会查找设备上的 MAC 地址表。若 MAC 地址表中包含与该报文目的 MAC 地址对应的表项，但该表项中的转发出端口是接收该报文的端口，设备将直接丢弃该报文。
- 对于未知报文，交换机会将该报文广播给除接收该报文的端口以外的其他端口。

由此可知，报文的接收端口不能作为该报文的转发端口。若在该端口上使能了端口桥功能后，上述情况下的报文将不会直接被丢弃，而是通过该端口发送出去。

表1-19 配置以太网端口桥功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
配置以太网端口桥功能	**port bridge enable**	必选 缺省情况下，未使能端口桥功能

1.3.9 检测以太网端口的连接电缆

说明

- 光口不支持本特性。
- 在以太网端口上执行该操作会使得已经 up 的链路自动 down、up 一次。

通过以下配置任务，用户可以检测设备上以太网端口连接电缆的当前状况，系统将在 5 秒内返回检测结果。检测内容包括电缆的接收方向、发送方向以及是否存在短路或开路现象，同时可以检测出故障线缆的长度。

表1-20 检测以太网端口的连接电缆

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
对以太网端口连接电缆进行一次检测	**virtual-cable-test**	必选

1.3.10 配置以太网端口流量阈值控制功能

1. 端口流量阈值控制简介

端口流量阈值控制功能用于控制以太网上的报文风暴。启用该功能的端口会定时分别检测到达端口的未知单播报文流量、组播报文流量和广播报文流量。如果某类报文流量超过预先设置的上限阈值时，用户可以通过配置来决定是阻塞该端口还是关闭该端口，以及是否发送 Trap 和 Log 信息。

注意

对于某种类型的报文流量，可以通过该功能或者以太网端口的风暴抑制功能（请参见“1.3.4 配置以太网端口的风暴抑制比”）来进行抑制，但是这两种功能不能同时配置，否则抑制效果不确定。比如，不能同时配置端口的未知单播报文流量阈值控制功能和未知单播风暴抑制功能。

当某种类型的报文流量超过该类报文预设的上限阈值时，系统提供了两种处理方式：

- block 方式：当端口上未知单播、组播或广播报文中某类报文的流量大于其上限阈值时，端口将暂停转发该类报文（其它类型报文照常转发），端口处于阻塞状态，但仍会统计该类报文的流量。当该类报文的流量小于其下限阈值时，端口将自动恢复对此类报文的转发。
- shutdown 方式：当端口上未知单播、组播或广播报文中某类报文的流量大于其上限阈值时，端口将被关闭，系统停止转发所有报文。当该类报文的流量小于其下限阈值时，端口状态不会自动恢复，此时可通过执行 **undo shutdown** 命令或取消端口上流量阈值的配置来恢复。

2. 配置以太网端口流量阈值控制功能

表1-21 配置以太网端口流量阈值控制功能

操作	命令	说明
进入系统视图	**system-view**	-
配置端口流量统计时间间隔	**storm-constrain interval** *seconds*	可选 缺省情况下，端口流量统计时间间隔为10秒
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
开启端口流量阈值控制功能，并设置上限阈值与下限阈值	**storm-constrain** { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *max-pps-values min-pps-values*	必选 缺省情况下，端口不进行流量阈值控制
配置端口流量大于上限阈值的控制动作	**storm-constrain control** { **block** | **shutdown** }	可选 缺省情况下，端口不进行流量阈值控制
配置端口流量超过上限阈值或者从超上限回落到低于下限阈值时输出Trap信息	**storm-constrain enable trap**	可选 缺省情况下，端口流量超过上限阈值或者从超上限回落到低下限阈值输出Trap信息
配置端口流量超过上限阈值或者从超上限回落到低于下限阈值时输出Log信息	**storm-constrain enable log**	可选 缺省情况下，端口流量超过上限阈值或者从超上限回落到低于下限阈值输出Log信息

说明

- 为了保持网络状态的稳定，建议设置的流量统计时间间隔不低于默认值。
- 本特性实现中系统需要一个完整的周期（周期长度为 seconds）来收集流量数据，下一个周期分析数据、采取相应的控制措施。因此，开启端口流量阈值控制功能后，如果某类报文流量超过预先设置的上限阈值，控制动作最短将在一个周期后执行，最长不会超过两个周期。
- 在同一个端口下，可以分别对未知单播、组播和广播报文开启流量阈值控制功能，并设置上限阈值与下限阈值。

1.4 三层以太网端口配置

当以太网端口工作在三层模式（route）时，可以配置三层以太网端口的 MTU 值。

1.4.1 配置三层以太网端口的MTU

MTU（Maximum Transmission Unit，最大传输单元）参数影响 IP 报文的分片与重组。

表1-22 配置三层以太网端口的 MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图	**interface** *interface-type interface-number*	-
设置MTU	**mtu** *size*	可选 缺省情况下，三层以太网端口的MTU均为1500Bytes

1.5 以太网端口显示和维护

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** 命令可以清除端口统计信息。

表1-23 以太网端口显示和维护

操作	命令
显示以太网端口的相关信息 （仅R5206及以上版本支持**description**参数）	**display interface** [*interface-type*] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface** *interface-type interface-number* [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口的报文流量统计信息	**display counters** { **inbound** | **outbound** } **interface** [*interface-type*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示最近一个抽样间隔内处于up状态的端口的报文速率统计信息	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定端口丢弃报文的信息	**display packet-drop interface** [*interface-type* [*interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示所有端口丢弃报文摘要的信息	**display packet-drop summary** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定手工端口组或所有手工端口组的信息	**display port-group manual** [**all** | **name** *port-group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口环回监测功能的开启情况和相关信息	**display loopback-detection** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口流量控制信息	**display storm-constrain** [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除以太网端口的统计信息	**reset counters interface** *interface-type* [*interface-number*]
清除指定端口丢弃报文的统计信息	**reset packet-drop interface** [*interface-type* [*interface-number*]]

目　录

1 Loopback接口和NULL接口配置

1.1 Loopback接口

1.1.1 Loopback接口简介

Loopback 接口是一种纯软件性质的虚拟接口。Loopback 接口具有以下特点：

- Loopback 接口创建后除非手工关闭该接口，否则 Loopback 接口物理层状态和链路层协议永远处于 UP 状态。
- Loopback 接口可以配置掩码为全 f 的 IP 地址，以便节约 IP 地址。当配置 IPv4 地址时，子网掩码必须是 32 位的。如果配置的子网掩码不是 32 位的，系统会自动修改为 32；同样，当配置 IPv6 地址时，子网掩码必须是 128 位的。如果配置的掩码不是 128 位的，系统会自动修改为 128。
- Loopback 接口下也可以使能路由协议，可以收发路由协议报文。

鉴于上述特点，Loopback 接口的应用非常广泛，主要表现在：

- 将 Loopback 接口地址设置为该设备产生的 IP 数据包的源地址。因为 Loopback 接口地址稳定且是单播地址，所以通常将 Loopback 接口地址视为设备的标志。在认证或安全等服务器上设置允许或禁止携带 Loopback 接口地址的报文通过，就相当于允许或禁止某台设备产生的报文通过，这样可以简化报文过滤规则。但需要注意的是，将 Loopback 接口地址用于 IP 数据包源地址时，需借助路由配置来确保 Loopback 接口到对端的路由可达。另外，任何送到 Loopback 接口的网络数据报文都会被认为是送往设备本身的，设备将不再转发这些数据包。
- 因为 Loopback 接口状态稳定（永远处于 UP 状态），该接口还常用于动态路由协议。比如，在一些动态路由协议中，当没有配置 Router ID 时，将选取所有 Loopback 接口上数值最大的 IP 地址作为 Router ID。在 BGP 协议中，为了使 BGP 会话不受物理接口故障的影响，可将发送 BGP 报文的源接口配置成 Loopback 接口等。

1.1.2 配置Loopback接口

表1-1 配置 Loopback 接口

操作	命令	说明
进入系统视图	**system-view**	-
创建Loopback接口，并进入Loopback接口视图	**interface loopback** *interface-number*	-
配置当前接口的描述信息	**description** *text*	可选 缺省情况下，接口的描述信息为“*接口名* Interface”
关闭当前接口	**shutdown**	可选 缺省情况下，Loopback接口处于开启状态

操作	命令	说明
恢复当前接口的缺省配置	**default**	可选

说明

在 Loopback 接口上可以配置 IP 地址、IP 路由等参数，具体配置请参见“三层技术-IP 业务配置指导”。

1.2 Null接口

1.2.1 Null接口简介

Null 接口是一种纯软件性质的逻辑接口。它永远处于 up 状态，但不能转发数据包，也不能配置 IP 地址和链路层协议。如果在静态路由中指定到达某一网段的下一跳为 Null 接口时，则任何送到该网段的网络数据报文都会被丢弃，因此设备通过 Null 接口提供了一种过滤报文的简单方法——将不需要的网络流量发送到 Null 接口，从而免去配置 ACL（访问控制列表）的复杂工作。

例如：使用静态路由配置命令“ip route-static 92.101.0.0 255.255.0.0 null 0”将丢弃所有去往网段 92.101.0.0/16 的报文。

1.2.2 配置Null接口

表1-2 配置 Null 接口

操作	命令	说明
进入系统视图	**system-view**	-
进入Null接口视图	**interface null 0**	必选 缺省情况下，设备上已经存在Null0接口，用户不能创建也不能删除
配置当前接口的描述信息	**description** *text*	可选 缺省情况下，接口的描述信息为“*接口名* Interface”
恢复当前接口的缺省配置	**default**	可选

1.3 Loopback接口和Null接口显示和维护

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接口的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除接口统计信息。

表1-3 Loopback 接口和 Null 接口显示和维护

操作	命令
显示Loopback接口的相关信息 （仅R5206及以上版本支持**description**参数）	**display interface** [**loopback**] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface loopback** *interface-number* [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Null接口的状态信息 （仅R5206及以上版本支持**description**参数）	**display interface** [**null**] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface null 0** [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除Loopback接口的统计信息	**reset counters interface** [**loopback** [*interface-number*]]
清除Null接口的统计信息	**reset counters interface** [**null** [**0**]]

目 录

1 端口批量配置

当多个端口需要配置某功能（比如 shutdown）时，需要逐个进入端口视图，在每个端口执行一遍命令，比较繁琐。此时，可以使用端口批量配置功能，达到事半功倍的效果。

1.1 端口批量配置

- 进入端口批量配置视图后，在命令行提示符下输入?，将显示端口列表中第一个端口支持的所有命令。
- 在端口批量配置视图下，只能执行端口列表中第一个端口支持的命令，不能执行第一个端口不支持但其它成员端口支持的命令。
- 在端口批量配置视图下，执行 **display this** 命令，将显示端口列表中第一个端口当前生效的配置。
- 在端口批量配置视图下执行的配置命令，对绑定的所有端口生效。如果某个成员端口不支持该命令，或者命令在某个成员端口下执行失败，系统会给出相应的提示信息，不会影响其他成员端口继续执行该命令。

表1-1 端口批量配置

操作	命令	说明
进入系统视图	**system-view**	-
进入端口批量配置视图	**interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5>	二者选其一 **interface range name**和**interface range**命令都能提供端口批量配置功能，它们的差别在于：**interface range name**命令在绑定端口的时候可以定义一个别名，可以进行多次绑定，给不同的绑定定义不同的别名，以示区别，方便记忆。并且，后续可以使用别名直接进入端口批量配置视图，不再需要输出一长串的端口列表，配置起来更简便。
	interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5>]	

说明

- 聚合口加入批量端口时，建议不要将该聚合口的成员端口也加入，否则在批量端口配置视图下执行某些配置命令时，可能会导致聚合分裂。
- 批量端口包含的端口数量没有上限，仅受系统资源限制。端口数量较多时，在批量端口配置视图下执行命令等待的时间将较长。

目 录

1 MAC地址表配置

说明

- MAC 地址表中对于接口的相关配置，目前只能在二层以太网端口、二层聚合接口等二层接口上进行。
- 本章节内容只涉及单播的静态、动态、黑洞 MAC 地址表项的配置。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“IGMP Snooping”和“MLD Snooping”。有关 VPLS 中 MAC 地址表的相关介绍和配置内容，请参见“MPLS 配置指导”中的“VPLS”。

1.1 MAC地址表简介

MAC 地址表记录了目的 MAC 地址、MAC 地址对应的出接口以及所属的 VLAN ID。在转发数据时，设备根据报文中的目的 MAC 地址查询 MAC 地址表，快速定位出接口，从而减少广播。

通过 **display mac-address** 命令可以查看 MAC 地址表信息，例如：

```
<Sysname> display mac-address
MAC ADDR        VLAN ID   STATE           PORT INDEX              AGING TIME(s)
000f-e201-0101  1         Learned         GigabitEthernet1/0/1    AGING

  ---  1 mac address(es) found  ---
```

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 地址的方法如下：如果从某接口（假设为接口 A）收到一个数据帧，设备就会分析该数据帧的源 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纪录被刷新，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黑客用户的报文，带来了安全隐患。如果黑客用户将攻击报文的源 MAC 地址伪装成合法用户的 MAC 地址，并从设备的其它接口进入，设备就会学习到错误的 MAC 地址表项，于是就会将本应转发给合法用户的报文转发给黑客用户。

为了提高接口安全性，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，从而防止假冒身份的非法用户骗取数据。

1.1.2 MAC地址表项的分类

MAC 地址表项分为：静态 MAC 地址表项、动态 MAC 地址表项和黑洞 MAC 地址表项。

- 静态 MAC 地址表项由用户手工配置，用于目的是某个 MAC 地址的报文从对应端口转发出去，表项不老化。
- 动态 MAC 地址表项包括用户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 地址的报文从对应端口转发出去，表项有老化时间。
- 黑洞 MAC 地址表项用于丢弃源 MAC 地址或目的 MAC 地址为指定值的报文（例如，出于安全考虑，可以屏蔽某个用户接收报文），由用户手工配置，表项不老化。


说明

用户手工配置的静态 MAC 地址表项、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、黑洞 MAC 地址表项覆盖。

1.1.3 基于MAC地址表的报文转发

设备在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

- 单播方式：当 MAC 地址表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文从该表项中的转发出接口发送。
- 广播方式：当设备收到目的地址为全 1 的报文，或 MAC 地址表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外的所有接口进行转发。

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

一般情况下，设备通过源 MAC 地址学习过程自动建立 MAC 地址表。

为了提高接口安全性，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，从而防止假冒身份的非法用户骗取数据。

另外，如果需要丢弃指定源 MAC 地址或目的 MAC 地址的报文，可配置黑洞 MAC 地址表项。

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1-1 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**	-

操作	命令	说明
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*	必选 缺省情况下，系统没有配置任何MAC地址表项

说明

在配置 MAC 地址表项时，命令中 **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，否则将添加失败。

(2) 接口配置静态/动态 MAC 地址表项

表1-2 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**	-
进入二层以太网端口、二层聚合接口视图	**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*	必选 缺省情况下，接口下没有配置任何MAC地址表项

说明

在配置 MAC 地址表项时，当前的接口必须属于命令中 **vlan** 参数指定的 VLAN，而且该 VLAN 必须事先创建，否则将添加失败。

2. 配置黑洞MAC地址表项

表1-3 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*	必选 缺省情况下，系统没有配置任何MAC地址表项

说明

在配置黑洞 MAC 地址表项时，指定的 VLAN 必须事先创建，否则将添加失败。

1.2.2 关闭MAC地址学习功能

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：黑客使用大量源 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。

1. 关闭全局的MAC地址学习功能

关闭全局的 MAC 地址学习功能的同时也就关闭了全部接口的 MAC 地址学习功能。

表1-4 关闭全局 MAC 地址学习功能

操作	命令	说明
进入系统视图	**system-view**	-
关闭全局的MAC地址学习功能	**mac-address mac-learning disable**	必选 缺省情况下，全局的MAC地址学习功能处于开启状态

说明

关闭 MAC 地址学习功能后，已经学习到的 MAC 地址表项将继续有效直至老化。

2. 关闭接口的MAC地址学习功能

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的单个接口或者端口组的 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**	-
开启全局的MAC地址学习功能		**undo mac-address mac-learning disable**	可选 缺省情况下，全局的MAC地址学习功能处于开启状态
进入二层以太网端口、二层聚合接口或者端口组视图	进入二层以太网端口、或者二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口、或者二层聚合接口视图后，下面进行的配置只在当前接口生效；进入端口组视图后，下面进行的配置将在端口组的所有接口生效
	进入端口组视图	**port-group manual** *port-group-name*	
关闭接口的MAC地址学习功能		**mac-address mac-learning disable**	必选 缺省情况下，接口的MAC地址学习功能处于开启状态

说明

- 关闭 MAC 地址学习功能后，已经学习到的 MAC 地址表项将继续有效直至老化。
- 端口组相关的配置请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

3. 关闭VLAN的MAC地址学习功能

用户可以关闭设备上的指定 VLAN 的 MAC 地址学习功能。

表1-6 关闭 VLAN 的 MAC 地址学习功能

操作	命令	说明
进入系统视图	**system-view**	-
开启全局的MAC地址学习功能	**undo mac-address mac-learning disable**	可选 缺省情况下，全局的MAC地址学习功能处于开启状态
进入VLAN视图	**vlan** *vlan-id*	-
关闭VLAN的MAC地址学习功能	**mac-address mac-learning disable**	必选 缺省情况下，VLAN的MAC地址学习功能处于开启状态

说明

关闭 MAC 地址学习功能后，已经学习到的 MAC 地址表项将继续有效直至老化。

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，动态 MAC 地址表项不会及时自动更新。这样，由于设备学习不到新的 MAC 地址，会导致用户流量不能正常转发。因此，需要配置动态 MAC 地址表项老化时间。超出设定的老化时间，动态 MAC 地址表项被自动删除，设备重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。

配置合适的老化时间可以有效利用 MAC 地址老化功能。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，可能导致设备广播大量的数据报文，影响设备的运行性能。

表1-7 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**	-

操作	命令	说明
配置动态MAC地址表项的老化时间	**mac-address timer** { **aging** *seconds* | **no-aging** }	可选 缺省情况下，MAC地址老化时间为300秒

说明

- 动态 MAC 地址表项的老化时间作用于全部接口上，地址老化只对动态的（设备学习到的或者用户配置的动态的）MAC 地址表项起作用。
- 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，被他人侦听，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设成 **no-aging**（不老化），以减少广播，增加网络稳定性和安全性。

1.2.4 关闭基于目的MAC地址刷新老化时间

为适应网络的变化，设备上的动态 MAC 地址表项需要及时老化。因此，每条动态 MAC 地址表项都有一个老化时间。如果在动态 MAC 地址表项的老化时间超时之前，设备收到源 MAC 地址或目的 MAC 地址匹配该表项的报文，则重新计算该表项的老化时间，即缺省情况下设备基于源 MAC 地址和目的 MAC 地址刷新老化时间。

如果希望设备上的动态MAC地址仅基于报文的源MAC地址刷新老化时间，可以关闭基于目的MAC地址刷新老化时间功能。

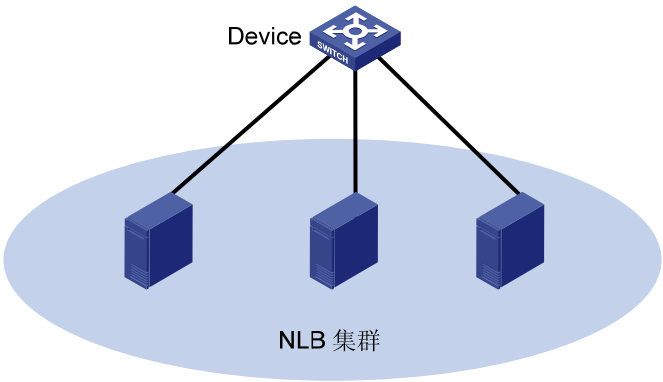
表1-8 关闭基于目的 MAC 地址刷新老化时间配置

操作	命令	说明
进入系统视图	**system-view**	-
关闭目的MAC地址刷新老化时间	**mac-address destination-hit disable**	必选 缺省情况下，基于目的MAC地址刷新老化时间功能处于开启状态

1. 应用举例

微软的网络负载均衡（NLB，Network Load Balancing）功能，是其在 Windows Server 上开发的一个多服务器集群负载均衡特性。

a. NLB 集群



NLB 支持集群内服务器之间的负载分担以及冗余备份，当发生服务器故障时可以支持数据快速切换。为了保证快速切换，NLB 要求交换机将业务流量转发至集群内的所有服务器或指定服务器，然后由各服务器将该服务器不期望的流量过滤掉。

在 NLB 集群的单播模式下，集群服务器加入或者切换时会发送一个以虚拟 MAC 为源 MAC 的报文，交换机会学习到这个虚拟 MAC。之后，服务器不再以此 MAC 为源地址发送报文，但是发往服务器的流量会以这个虚拟 MAC 为目的地址。如果设备的 MAC 地址老化允许目的 MAC 地址刷新老化时间，将导致该虚拟 MAC 无法老化，从而使流量只能发送到该虚拟 MAC 地址表项所在端口，无法发送到所有连接服务器的端口。

此时，可以关闭基于目的 MAC 地址刷新老化时间功能，使该虚拟 MAC 及时老化掉，从而使发往服务器的报文能够到达集群内的所有服务器。

1.2.5 配置端口最多可以学习到的MAC地址数

通过配置二层以太网端口或端口组最多可以学习到的 MAC 地址数，用户可以控制设备维护的 MAC 地址表的表项数量。当接口学习到的 MAC 地址数达到配置的最大值时，该接口将不再对 MAC 地址进行学习。

表1-9 配置接口最多可以学习到的 MAC 地址数

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口、或者端口组视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图后，下面进行的配置只在当前接口生效；进入端口组视图后，下面进行的配置将在端口组的所有接口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置接口最多可以学习到的MAC地址数		**mac-address max-mac-count** *count*	必选 缺省情况下，没有配置以太网端口/端口组最多可以学习到的MAC地址数

说明

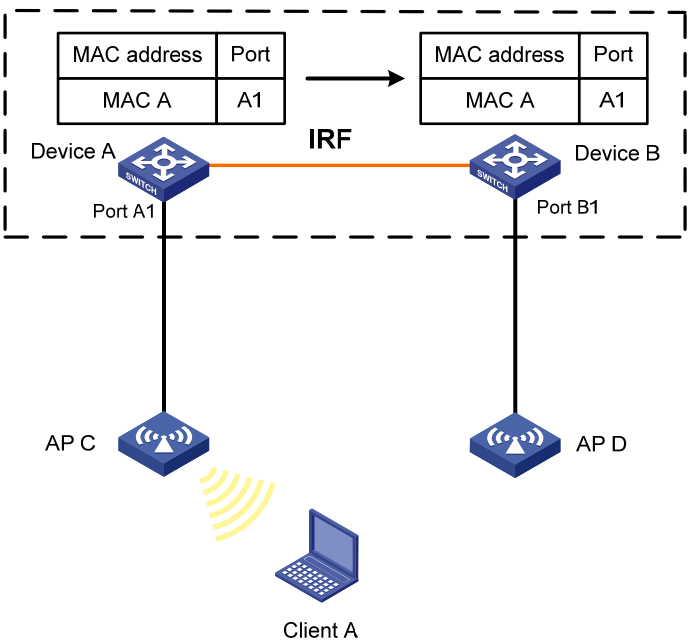
- 二层链路聚合端口不支持配置端口最多可以学习到的 MAC 地址数。
- 当以太网端口被配置为聚合组的成员端口后，如果在这些成员端口上配置端口最多可以学习到的 MAC 地址数，会导致成员端口不能被选中，因此，请不要在聚合组的成员端口上配置端口最多可以学习到的 MAC 地址数。

1.2.6 配置MAC地址漫游功能

如 图 1-1 所示，是MAC地址漫游功能的典型应用场景。Device A和Device B是两台配置了IRF功能的本系列交换机。无线接入点AP C和AP D分别连接到IRF成员设备Device A和Device B。

开启MAC地址漫游功能后，IRF成员设备会将学习到的MAC地址同步给IRF设备内的其他成员设备。如 图 1-1 所示，当Client A通过AP C接入时，Device A会将学习到的Client A的MAC地址同步给IRF设备内的其他成员设备Device B。

图1-1 Client A 通过 AP C 接入时的 MAC 地址表



当用户的接入地点发生变化，例如从AP C的覆盖区域移动到AP D的覆盖区域时，IRF会将Client A的MAC地址重新学习到Device B上，并将更新后的MAC地址同步给IRF设备内的其他成员设备Device A（如 图 1-2 所示），使用户的通信不受任何影响。

图1-2 Client A 移动到通过 AP D 接入时的 MAC 地址表

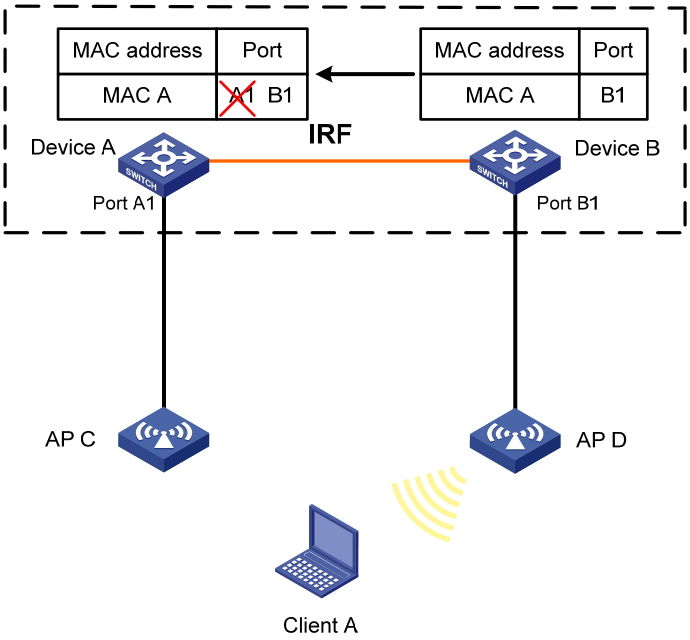


表1-10 配置 MAC 地址漫游功能

操作	命令	说明
进入系统视图	**system-view**	-
配置MAC地址漫游功能	**mac-address mac-roaming enable**	必选 缺省情况下，MAC地址漫游功能处于关闭状态

1.2.7 MAC地址迁移日志上报配置

本功能记录和上报 MAC 地址迁移情况，包括发生迁移的 MAC 地址、该 MAC 地址所在 VLAN ID、迁移的源接口和新接口、最近迁移时间、以及该 MAC 地址一分钟内迁移的次数。

MAC 地址迁移是指：设备从某接口（假设接口 A）学习到某 MAC 地址，之后从另一接口（假设接口 B）接收到了以该 MAC 地址为源 MAC 地址的报文，且接口 B 与接口 A 所属的 VLAN 相同，则该 MAC 地址表项的出接口改为接口 B，即 MAC 地址从接口 A 迁移到接口 B。

当设备作为数据中心接入设备连接服务器时，服务器上虚拟机的迁移会引起设备上 MAC 地址迁移。例如虚拟机从接口 A 连接的服务器迁移到接口 B 连接的服务器，当设备从接口 B 接收到该虚拟机的报文后，该虚拟机的 MAC 地址会从接口 A 迁移到接口 B。通过 MAC 地址迁移日志上报功能可以记录和查看虚拟机的迁移情况。

窍门

如果 MAC 地址迁移频繁出现，且同一 MAC 地址总是在特定的两个接口之间迁移，那么网络中可能存在二层环路。您可以通过 MAC 地址迁移日志上报功能来发现和定位二层环路。

表1-11 配置 MAC 地址迁移日志上报

操作	命令	说明
进入系统视图	**system-view**	-
使能MAC地址迁移日志上报功能	**mac-flapping notification enable**	必选 缺省情况下，MAC地址迁移日志上报功能处于关闭状态

说明

使能本功能后，系统将每分钟上报一次上一分钟发生的 MAC 地址迁移日志。

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1-12 MAC 地址表显示和维护

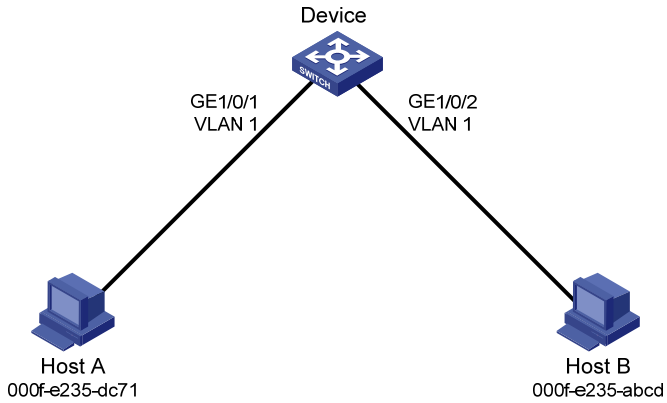
操作	命令
显示MAC地址表信息	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MAC地址表动态表项的老化时间	**display mac-address aging-time** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统或接口MAC地址的学习状态	**display mac-address mac-learning** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MAC地址表的统计信息	**display mac-address statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.4 MAC地址表典型配置举例

1. 组网需求

- 现有一个用户主机 Host A，它的 MAC 地址为 000f-e235-dc71，所属 VLAN 为 VLAN 1，所连的设备接口为 GigabitEthernet1/0/1。为防止 MAC 地址攻击，在设备的 MAC 地址表中为该用户主机添加一条静态表项。
- 另有一个用户主机 Host B，它的 MAC 地址为 000f-e235-abcd，所属 VLAN 为 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. 组网图



3. 配置步骤

增加一个静态 MAC 地址表项。

```
<Sysname> system-view
[Sysname] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

增加一个黑洞 MAC 地址表项。

```
[Sysname] 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。

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

查看以太网端口 GigabitEthernet1/0/1 上的 MAC 地址表信息。

```
[Sysname] display mac-address interface gigabitethernet 1/0/1
MAC ADDR          VLAN ID  STATE            PORT INDEX              AGING TIME(s)
000f-e235-dc71    1        Config static    GigabitEthernet 1/0/1           NOAGED

  ---  1 mac address(es) found  ---
```

查看黑洞 MAC 地址表信息。

```
[Sysname] display mac-address blackhole
MAC ADDR        VLAN ID    STATE            PORT INDEX              AGING TIME(s)
000f-e235-abcd  1          Blackhole        N/A                     NOAGED

  ---  1 mac address(es) found  ---
```

查看动态 MAC 地址表项的老化时间。

```
[Sysname] display mac-address aging-time
Mac address aging time: 500s
```

2 MAC Information配置

2.1 MAC Information简介

2.1.1 MAC Information介绍

在网络监控中，需要对加入和离开网络的用户进行监控。由于 MAC 地址能唯一标识一个网络用户，所以可以通过监控加入和离开网络的 MAC 地址对用户进行跟踪。

通过使用 MAC Information 功能，当二层以太网端口学习到或删除 MAC 地址时会发送 Syslog 或 Trap 信息，通过对 Syslog 和 Trap 信息的分析，监控端可以实现对进入网络的用户进行监控。

2.1.2 MAC Information的工作机制

当设备学习到一条新的 MAC 地址或删除掉一条已有 MAC 地址时，设备将 MAC 地址相关信息写入设备的记录用户信息的缓冲区。当用户设定的发送 MAC 监控 Syslog 或 Trap 的时间间隔到期，设备立即发送记录的 MAC 地址的 Syslog 或 Trap 信息。

说明

- 设备仅记录和发送通过源 MAC 地址学习自动生成的 MAC 地址、通过 MAC 地址认证的 MAC 地址、通过 802.1X 认证的 MAC 地址、Voice Vlan 匹配的 OUI MAC 地址，以及安全 MAC 地址等。对黑洞 MAC 地址、静态 MAC 地址、用户配置的动态 MAC 地址、组播 MAC 地址和本机 MAC 地址不进行记录和发送。
- 关于 MAC 地址认证的详细介绍请参见“安全配置指导”中的“MAC 地址认证”。
- 关于 802.1X 的详细介绍请参见“安全配置指导”中的“802.1X”。
- 关于安全 MAC 地址的详细介绍请参见“安全配置指导”中的“端口安全”。
- 关于 Voice VLAN 和 OUI MAC 地址的详细介绍请参见“二层技术-以太网交换配置指导”中的“Voice VLAN”。

2.2 配置MAC Information功能

2.2.1 使能全局MAC Information功能

表2-1 使能全局 MAC Information 功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能全局MAC Information功能	**mac-address information enable**	必选 缺省情况下，全局MAC Information功能处于关闭状态

2.2.2 使能基于接口的MAC Information功能

表2-2 使能基于接口的 MAC Information 功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
使能基于接口的MAC Information功能	**mac-address information enable** { **added** | **deleted** }	必选 缺省情况下，基于接口的MAC Information功能处于关闭状态

说明

当全局 MAC Information 功能未使能时，即使以太网端口下使能了 MAC Information 功能，MAC Information 功能也处于关闭状态。

2.2.3 配置MAC Information工作模式

表2-3 配置 MAC Information 工作模式

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置MAC Information工作模式	**mac-address information mode** { **syslog** | **trap** }	可选 缺省情况下，MAC变化通知功能采用Trap方式发送

2.2.4 配置发送Syslog或Trap信息的时间间隔

为了防止过多的 Syslog 或 Trap 信息干扰用户，用户可以配置发送 Syslog 或 Trap 信息的时间间隔，当到达时间间隔时再发送 Syslog 或 Trap 信息。

表2-4 配置发送 Syslog 或 Trap 信息的时间间隔

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置发送Syslog或Trap信息的时间间隔	**mac-address information interval** *interval-time*	可选 缺省情况下，发送Syslog或Trap信息的时间间隔为1秒

2.2.5 配置MAC Information缓存队列长度

MAC Information 缓存队列长度是否为 0 对应着不同的处理方式：

- 如果 MAC Information 缓存队列长度为 0，则当学习到或删除掉一条 MAC 地址时会立即发送 Syslog 或 Trap 信息。
- 如果 MAC Information 缓存队列长度不为 0，则将 MAC 地址变化信息存放在缓存队列中。当未达到发送 Syslog 或 Trap 的时间间隔，此时若缓存队列被写满，新的 MAC 地址变化信息将覆盖缓存队列中最后一条写入的信息；当达到发送 Syslog 或 Trap 的时间间隔时，不论此时缓存队列是否已被写满，都发送 Syslog 或 Trap 信息。

表2-5 配置 MAC Information 缓存队列长度

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置MAC Information缓存队列长度	**mac-address information queue-length** *value*	可选 缺省情况下，MAC Information缓存队列长度为50

2.3 MAC Information典型配置举例

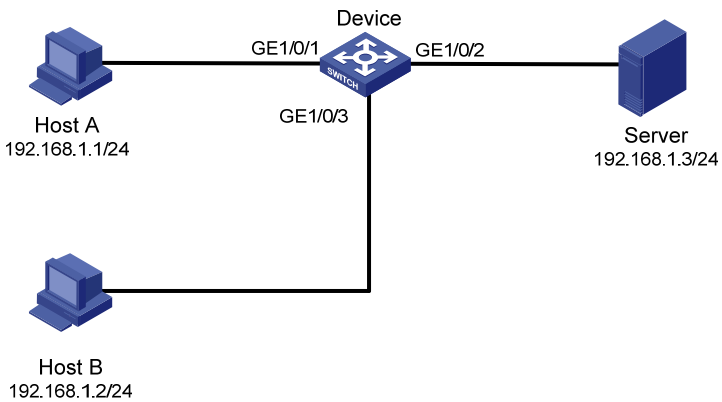
2.3.1 MAC Information典型配置举例

1. 组网需求

- Host A 与远端服务器 Server 通过 Device 相连；
- 在 Device 的 GigabitEthernet1/0/1 上使能 MAC Information 功能，Device 将 MAC 变化信息利用 Syslog 方式通过 GigabitEthernet1/0/3 发送给 Host B，Host B 对接收到的 Syslog 信息进行分析并显示。

2. 组网图

图2-1 MAC Information 典型配置组网图



3. 配置步骤

(1) 配置 Device 可以将 Syslog 发送到 Host B

详细内容请参见“网络管理和监控配置指导”中的“信息中心”。

(2) 使能 MAC Information 功能

全局使能 MAC Information。

```
<Device> system-view
[Device] mac-address information enable
```

配置 MAC Information 工作模式为 Syslog 方式。

```
[Device] mac-address information mode syslog
```

配置接口 GigabitEthernet1/0/1 使能 MAC Information 功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-address information enable added
[Device-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-GigabitEthernet1/0/1] quit
```

配置 MAC Information 缓存队列长度为 100。

```
[Device] mac-address information queue-length 100
```

配置 MAC Information 发送时间间隔为 20 秒。

```
[Device] mac-address information interval 20
```

目 录

1 以太网链路聚合配置

1.1 以太网链路聚合简介

以太网链路聚合简称链路聚合，它通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而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间的动态备份，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等于原先三条以太网物理链路的带宽总和，从而达到了增加链路带宽的目的；同时，这三条以太网物理链路相互备份，有效地提高了链路的可靠性。

图1-1 链路聚合示意图

1.1.1 基本概念

2. 聚合组、成员端口和聚合接口

将多个以太网端口捆绑在一起所形成的组合称为聚合组，而这些被捆绑在一起的以太网端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，我们称之为聚合接口。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端口，其对应的聚合接口称为二层聚合接口（Bridge-aggregation Interface，BAGG）。
- 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端口，其对应的聚合接口称为三层聚合接口（Route-aggregation Interface，RAGG）。

说明

- 聚合组与聚合接口的编号是一一对应的，譬如聚合组 1 对应于聚合接口 1。
- 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 3. 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。

---

3. 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用户数据的转发，处于此状态的成员端口简称为“选中端口”。

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

4. 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。

5. 配置分类

根据对成员端口状态的影响不同，我们可以将成员端口上的配置分为以下三类：

(1) 端口属性类配置：包含速率、双工模式和链路状态（up/down）这三项配置内容，是成员端口上最基础的配置内容。

(2) 第二类配置：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第二类配置完全相同的成员端口才能够成为选中端口。

表1-1 第二类配置的内容

配置项	内容
端口隔离	端口是否加入隔离组
QinQ配置	端口的QinQ功能开启/关闭状态、VLAN Tag的TPID值、添加的外层VLAN Tag、内外层VLAN优先级映射关系、不同内层VLAN ID添加外层VLAN Tag的策略、内层VLAN ID替换关系
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）、基于IP子网的VLAN配置、基于协议的VLAN配置、VLAN报文是否带Tag配置
MAC地址学习配置	是否具有MAC地址学习功能

说明

- 在聚合接口上所作的第二类配置，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。
- 由于成员端口上第二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。

(3) 第一类配置：是相对于第二类配置而言的，包含的配置内容有 GVRP、MSTP 等。在聚合组中，即使某成员端口与对应聚合接口的第一类配置存在不同，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第一类配置，只有当该成员端口退出聚合组后才能生效。

6. 参考端口

参考端口从成员端口中选出，其端口属性类配置和第二类配置将作为同一聚合组内的其它成员端口的参照，以确定这些成员端口的状态。

7. LACP协议

基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路聚合控制协议）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（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）来交互链路聚合的相关信息。

(1) LACP 协议的功能

根据所使用的LACPDU字段的不同，可将LACP协议的功能分为基本功能和扩展功能两大类，如 表 1-2 所示。

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、端口聚合优先级、端口编号和操作Key。 动态聚合组内的成员端口会自动使能LACP协议，并通过发送LACPDU向对端通告本端的上述信息。当对端收到该LACPDU后，将其中的信息与本端其它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，从而决定哪些链路可以加入聚合组以及某链路何时可以加入聚合组。
扩展功能	通过对LACPDU的字段进行扩展，可以实现对LACP协议的扩展。譬如，通过在扩展字段中定义一个新的TLV（Type/Length/Value，类型/长度/值）数据域，可以实现IRF（Intelligent Resilient Framework，智能弹性架构）中的LACP MAD（Multi-Active Detection，多Active检测）机制。本系列交换机可以作为成员设备或中间设备来参与LACP MAD。

说明

有关 IRF、成员设备、中间设备和 LACP MAD 机制的详细介绍，请参见“IRF 配置指导”中的“IRF”。

(2) LACP 优先级

根据作用的不同，可以将LACP优先级分为系统LACP优先级和端口聚合优先级两类，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	系统LACP优先级用于区分两端设备优先级的高低。要想使两端设备的选中端口一致，可以使一端具有较高的优先级，另一端则根据优先级较高的一端来选择本端的选中端口	优先级数值越小，优先级越高
端口聚合优先级	端口聚合优先级用于区分各成员端口成为选中端口的优先程度	

(3) 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。在三倍 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 超时时间只有短超时（1 秒）和长超时（30 秒）两种取值。

8. 聚合模式

根据成员端口上是否启用了LACP协议，可以将链路聚合分为静态聚合和动态聚合两种模式，它们各自的特点如 表 1-4 所示。

表1-4 不同聚合模式的特点

聚合模式	成员端口是否开启 LACP 协议	优点	缺点
静态聚合模式	否	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	不能根据对端的状态调整端口的选中/非选中状态，不够灵活
动态聚合模式	是	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	端口的选中/非选中状态容易受网络环境的影响，不够稳定

处于静态聚合模式和动态聚合模式下的聚合组分别称为静态聚合组和动态聚合组，动态聚合组内的选中端口以及处于 up 状态、与对应聚合接口的第二类配置相同的非选中端口均可以收发 LACPDU。

1.1.2 静态聚合模式

在静态聚合模式下，聚合组内的成员端口上不启用 LACP 协议，其端口状态通过手工进行维护。静态聚合模式的工作机制如下：

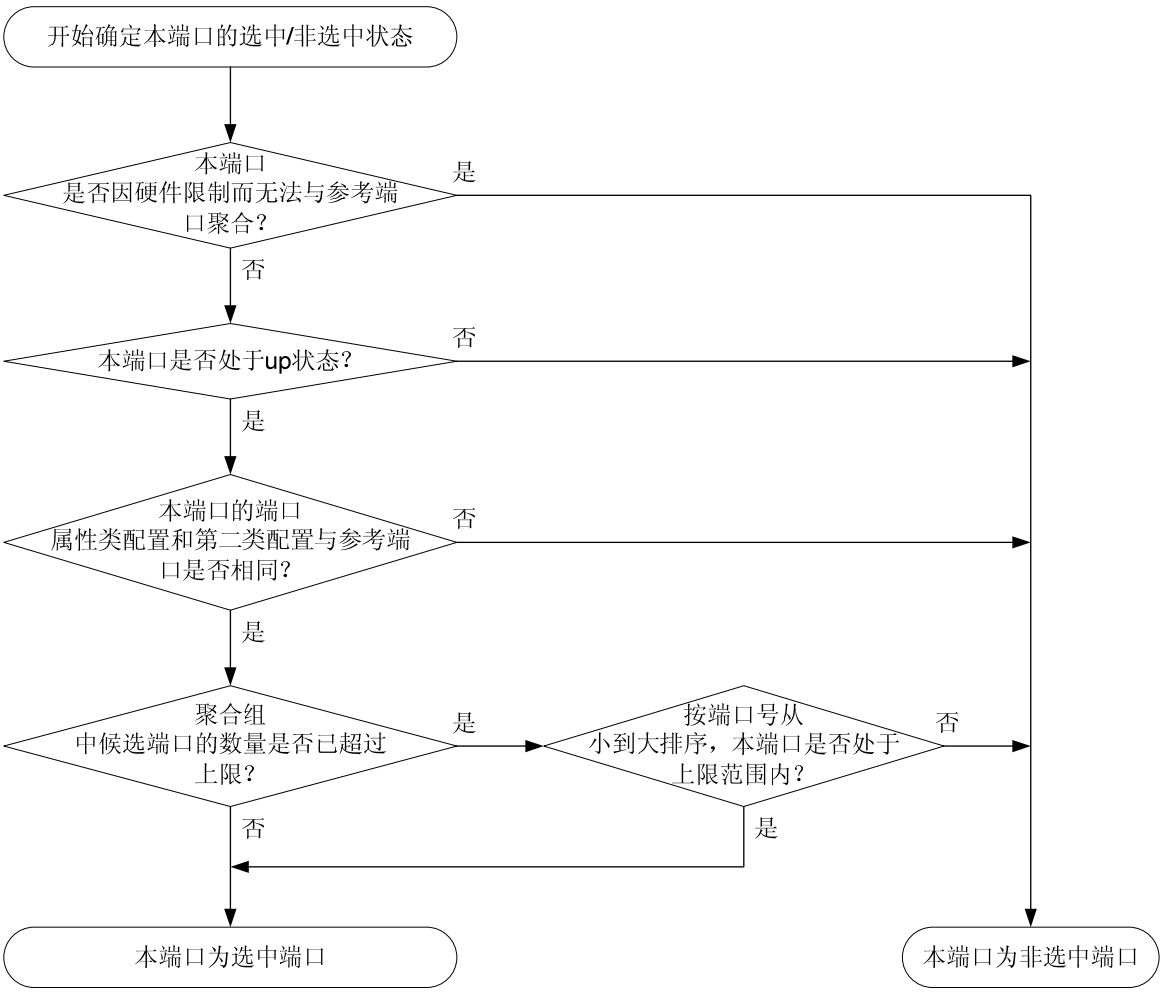
1. 选择参考端口

当聚合组内有处于 up 状态的端口时，先比较端口的聚合优先级，优先级数值最小的端口作为参考端口；如果优先级相同，再按照端口的全双工/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、且第二类配置与对应聚合接口相同的端口作为该组的参考端口；如果优先次序也相同，则选择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



说明

- 当一个成员端口的端口属性类配置或第二类配置改变时，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，也不会立刻成为选中端口。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

在动态聚合模式下，聚合组内的成员端口上均启用 LACP 协议，其端口状态通过该协议自动进行维护。动态聚合模式的工作机制如下：

1. 选择参考端口

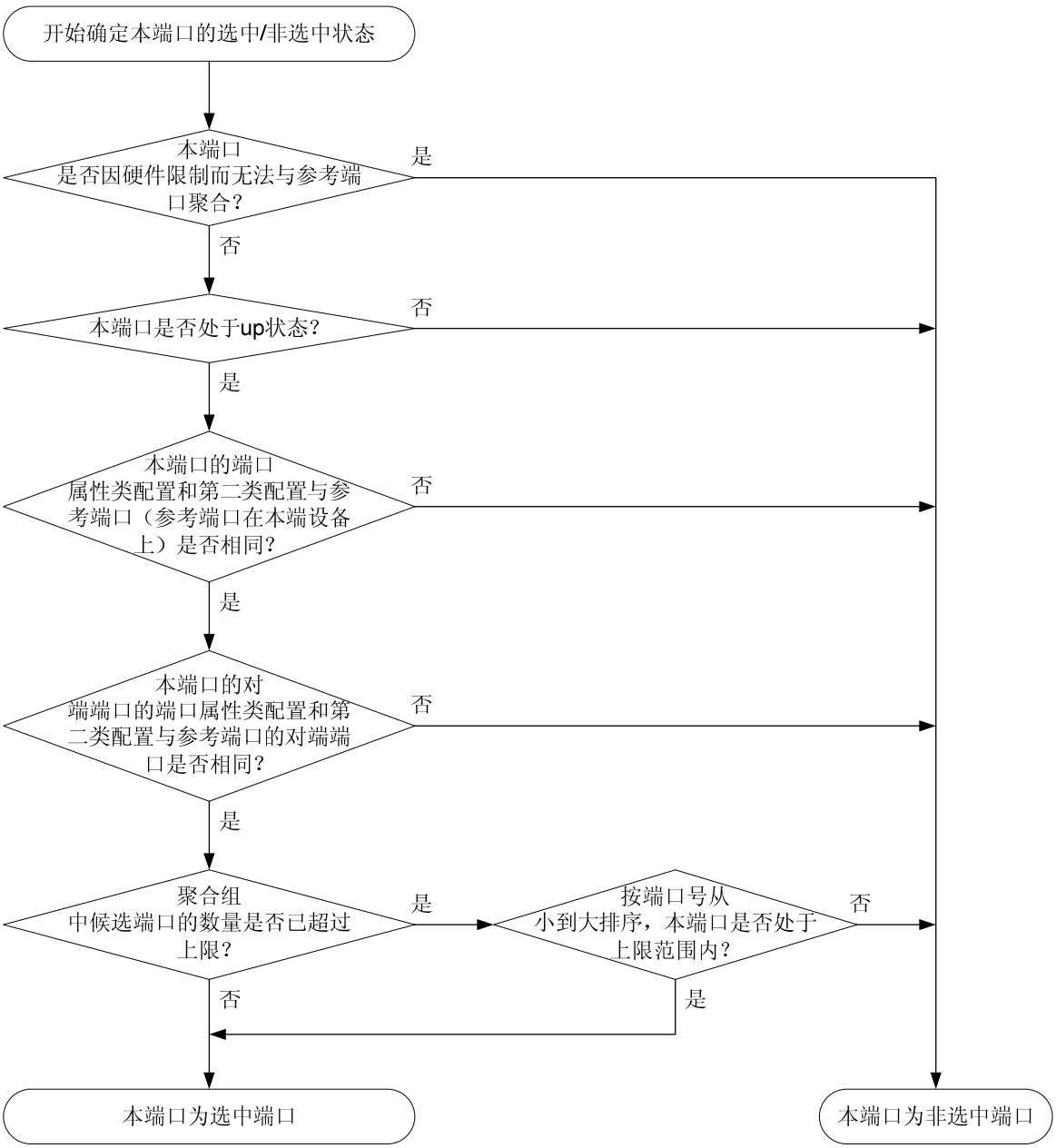
(1) 首先，从聚合链路的两端选出设备 ID（由系统的 LACP 优先级和系统的 MAC 地址共同构成）较小的一端：先比较两端的系统 LACP 优先级，优先级数值越小其设备 ID 越小；如果优先级相同再比较其系统 MAC 地址，MAC 地址越小其设备 ID 越小。

(2) 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（由端口的聚合优先级和端口的编号共同构成）：先比较端口的聚合优先级，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。

说明

- 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。
- 当一个成员端口的端口属性类配置或第二类配置改变时，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

通过采用不同的聚合负载分担类型及其组合，可以灵活地实现对聚合组内流量的负载分担。聚合负载分担的类型包括以下几种：

- 根据报文的源/目的 MAC 地址进行聚合负载分担
- 根据报文的源/目的服务端口号进行聚合负载分担
- 根据报文的入端口进行聚合负载分担
- 根据报文的源/目的 IP 地址进行聚合负载分担
- 根据报文的 MPLS 标签进行聚合负载分担

用户可以指定系统按照上述聚合负载分担类型的其中之一或其组合来进行负载分担，此外用户也可以指定系统按照报文类型（如二层、IPv4、IPv6、MPLS 等）自动选择聚合负载分担的类型。

1.2 以太网链路聚合配置任务简介

表1-5 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
	开启聚合接口链路状态变化Trap功能	可选	1.4.3
	限制聚合组内选中端口的数量	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	配置聚合负载分担类型	可选	1.5.1

配置任务		说明	详细配置
	配置聚合负载分担采用本地转发优先	可选	1.5.2
配置聚合流量重定向功能		可选	1.6

1.3 配置聚合组

请根据需要聚合的以太网端口类型来配置相应类型的聚合组：当需要聚合的是二层以太网端口时，请配置二层聚合组；当需要聚合的是三层以太网端口时，请配置三层聚合组。聚合链路的两端应配置相同的聚合模式。

说明

- 配置或使能了下列功能的端口将不能加入二层聚合组：RRPP（请参见“可靠性配置指导/RRPP”）、MAC 地址认证（请参见“安全配置指导/MAC 地址认证”）、端口安全模式（请参见“安全配置指导/端口安全”）、IP Source Guard 功能（请参见“安全配置指导/IP Source Guard”）、802.1X 功能（请参见“安全配置指导/802.1X”）以及 Portal 免认证规则源接口（请参见“安全配置指导/Portal”）。
- 配置或使能了下列功能的接口将不能加入三层聚合组：IP 地址（请参见“三层技术-IP 业务配置指导/IP 地址”）、DHCP 客户端（请参见“三层技术-IP 业务配置指导/DHCP”）、BOOTP 客户端（请参见“三层技术-IP 业务配置指导/DHCP”）、VRRP 功能（请参见“可靠性配置指导/VRRP”）和 Portal 功能（请参见“安全配置指导/Portal”）。
- 三层聚合接口和该聚合组内所有成员端口与 VPN 实例关联的配置必须保持一致，即三层聚合接口和各成员端口均不与任何 VPN 实例关联或者均与相同的 VPN 实例关联，否则将影响流量的正常转发。关于配置 VPN 与接口关联请参见“MPLS 配置指导/MPLS L3VPN 配置”。

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。

1.3.1 配置静态聚合组

说明

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. 配置二层静态聚合组

表1-6 配置二层静态聚合组

操作	命令	说明
进入系统视图	**system-view**	-
创建二层聚合接口，并进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	必选 创建二层聚合接口后，系统将自动生成同编号的二层聚合组，且该聚合组缺省工作在静态聚合模式下
退回系统视图	**quit**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	必选 多次执行此步骤可将多个二层以太网端口加入聚合组
将二层以太网端口加入聚合组	**port link-aggregation group** *number*	
配置端口的聚合优先级	**link-aggregation port-priority** *port-priority*	可选 缺省情况下，端口的聚合优先级为32768 改变端口的聚合优先级，将会影响到静态聚合组成员端口的选中/非选中状态

2. 配置三层静态聚合组

表1-7 配置三层静态聚合组

操作	命令	说明
进入系统视图	**system-view**	-
创建三层聚合接口，并进入三层聚合接口视图	**interface route-aggregation** *interface-number*	必选 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**	-
进入三层以太网端口视图	**interface** *interface-type interface-number*	必选 多次执行此步骤可将多个三层以太网端口加入聚合组
将三层以太网端口加入聚合组	**port link-aggregation group** *number*	
配置端口的聚合优先级	**link-aggregation port-priority** *port-priority*	可选 缺省情况下，端口的聚合优先级为32768 改变端口的聚合优先级，将会影响到静态聚合组成员端口的选中/非选中状态

1.3.2 配置动态聚合组

说明

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. 配置二层动态聚合组

表1-8 配置二层动态聚合组

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*	可选 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端口的选中/非选中状态
创建二层聚合接口，并进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	必选 创建二层聚合接口后，系统将自动生成同编号的二层聚合组，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**	必选 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**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	必选 多次执行此步骤可将多个二层以太网端口加入聚合组
将二层以太网端口加入聚合组	**port link-aggregation group** *number*	
配置端口的聚合优先级	**link-aggregation port-priority** *port-priority*	可选 缺省情况下，端口的聚合优先级为32768 改变端口的聚合优先级，将会影响到动态聚合组成员端口的选中/非选中状态
配置端口的LACP超时时间为短超时（即1秒）	**lacp period short**	可选 缺省情况下，端口的LACP超时时间为长超时（即30秒）

2. 配置三层动态聚合组

表1-9 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*	可选 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*	必选 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**	必选 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**	-
进入三层以太网端口视图	**interface** *interface-type interface-number*	必选 多次执行此步骤可将多个三层以太网端口加入聚合组
将三层以太网端口加入聚合组	**port link-aggregation group** *number*	
配置端口的聚合优先级	**link-aggregation port-priority** *port-priority*	可选 缺省情况下，端口的聚合优先级为32768 改变端口的聚合优先级，将会影响到动态聚合组成员的选中/非选中状态
配置端口的LACP超时时间为短超时（即1秒）	**lacp period short**	可选 缺省情况下，端口的LACP超时时间为长超时（即30秒）

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。除本节所介绍的以外，能够在二层/三层以太网端口上进行的配置大多数也能在二层/三层聚合接口上进行，具体配置请参见相关的配置手册。

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1-10 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**	-
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一
	进入三层聚合接口视图	**interface route-aggregation** *interface-number*	
配置当前接口的描述信息		**description** *text*	可选 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1-11 配置三层聚合接口 MTU

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

1.4.3 开启聚合接口链路状态变化Trap功能

在聚合接口上开启了接口链路状态变化 Trap 功能后，可以使聚合接口在链路状态发生改变时生成并发送端口 Link up 和 Link down 的 Trap 报文。有关 Trap 的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-12 开启聚合接口状态变化 Trap 功能

操作		命令	说明
进入系统视图		**system-view**	-
开启全局接口链路状态变化Trap功能		**snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *]	可选 缺省情况下，全局接口链路状态变化Trap功能处于开启状态
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一

操作		命令	说明
	进入三层聚合接口视图	**interface route-aggregation** *interface-number*	
开启接口链路状态变化Trap功能		**enable snmp trap updown**	可选 缺省情况下，接口链路状态变化Trap功能处于开启状态

1.4.4 限制聚合组内选中端口的数量

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，从而使流量可以切换到备份链路上。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。

缺省情况下，聚合组内选中端口的最大数量仅受端口硬件能力的限制；在配置了聚合组中的最大选中端口数之后，聚合组内选中端口的最大数量将同时受配置值和端口硬件能力（聚合组内成员端口的数量）的限制，即取二者中较低的值作为限制值。用户利用此特性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，那么在同一时刻这两个成员端口中只能有一个成为选中端口，另一个将作为备份端口。

表1-13 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**	-
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一
	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*	必选 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*	必选 缺省情况下，聚合组中的最大选中端口数仅受端口硬件能力的限制

注意

- 配置聚合组中的最小选中端口数可能导致聚合组内的所有成员端口都变为非选中状态。
- 配置聚合组中的最大选中端口数可能导致聚合组内的部分成员端口变为非选中状态。
- 要求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。

1.4.5 关闭聚合接口

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，且所有成员端口的链路状态都将变为 up。

表1-14 关闭聚合接口

操作		命令	说明
进入系统视图		**system-view**	-
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一
	进入三层聚合接口视图	**interface route-aggregation** *interface-number*	
关闭当前接口		**shutdown**	必选 缺省情况下，聚合接口处于开启状态

1.4.6 恢复聚合接口的缺省配置

通过执行本操作可以将接口下的所有配置都恢复为缺省配置。

表1-15 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**	-
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一
	进入三层聚合接口视图	**interface route-aggregation** *interface-number*	
恢复当前接口的缺省配置		**default**	必选

1.5 配置聚合负载分担

1.5.1 配置聚合负载分担类型

通过改变负载分担的类型，可以灵活地实现聚合组流量的负载分担。用户既可以指定系统按照报文携带的源/目的 MAC 地址、源/目的服务端口、报文入端口、源/目的 IP 地址、MPLS 标签等信息之一或其组合来选择所采用的负载分担类型，也可以指定系统按照报文类型（如二层、IPv4、IPv6、MPLS 等）自动选择所采用的聚合负载分担类型。

用户可以根据需要，选择全局配置或在聚合组内配置聚合负载分担类型。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。对于某聚合组来说，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。

说明

改变负载分担的类型仅对单播报文生效，即可以改变单播报文的聚合负载分担类型。对广播和组播报文无效，其分担类型只能是缺省模式。

1. 全局配置聚合负载分担类型

表1-16 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 load-sharing mode** { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *	必选 缺省情况下，系统按照报文类型自动选择所采用的聚合负载分担类型

说明

目前，在系统视图下进行全局聚合负载分担类型配置，交换机只支持：

- 根据报文类型自动匹配负载分担类型；
- 根据源 IP 地址进行聚合负载分担；
- 根据目的 IP 地址进行聚合负载分担；
- 根据源 MAC 地址进行聚合负载分担；
- 根据目的 MAC 地址进行聚合负载分担；
- 根据源 IP 地址与目的 IP 地址进行聚合负载分担；
- 根据源 IP 地址与源端口进行聚合负载分担；
- 根据目的 IP 地址与目的端口进行聚合负载分担；
- 根据源 IP 地址、源端口、目的 IP 地址与目的端口进行聚合负载分担；
- 根据报文入端口、源 MAC 地址、目的 MAC 地址之间不同的组合进行聚合负载分担。

表1-17 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**	-
进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者必选其一
	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-mac** | **mpls-label1** | **mpls-label2** | **source-ip** | **source-mac** } *	必选 缺省情况下，聚合组内采用的聚合负载分担类型与全局采用的聚合负载分担类型一致 本系列交换机中S5500-28SC-HI和S5500-52SC-HI不支持**mpls-label1**和**mpls-label2**参数

说明

目前，在二层/三层聚合接口视图下进行聚合组的聚合负载分担模式配置，交换机只支持：

- 根据报文类型自动匹配负载分担类型；
- 根据源 IP 地址进行聚合负载分担；
- 根据目的 IP 地址进行聚合负载分担；
- 根据源 MAC 地址进行聚合负载分担；
- 根据目的 MAC 地址进行聚合负载分担；
- 根据 mpls-label1 标签进行聚合负载分担；
- 根据目的 IP 地址与源 IP 地址进行聚合负载分担；
- 根据目的 MAC 地址与源 MAC 地址进行聚合负载分担；
- 根据 mpls-label1 和 mpls-label2 标签进行聚合负载分担。

1.5.2 配置聚合负载分担采用本地转发优先

配置聚合负载分担采用本地转发优先可以降低数据流量对IRF物理端口间链路的冲击，采用与未采用该机制时的聚合负载分担方式如 图 1-4 所示。有关IRF的详细介绍，请参见“IRF配置指导”中的“IRF”。

图1-4 IRF 中设备间聚合负载分担处理流程

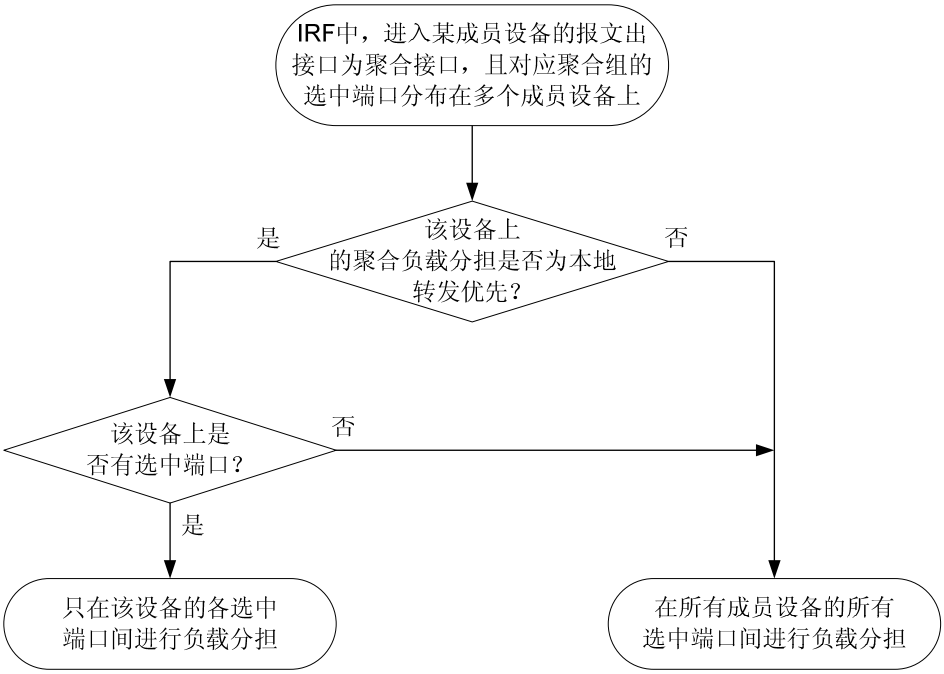


表1-18 配置聚合负载分担采用本地转发优先

操作	命令	说明
进入系统视图	**system-view**	-
配置聚合负载分担采用本地转发优先	**link-aggregation load-sharing mode local-first**	可选 缺省情况下，聚合负载分担采用本地转发优先

注意

聚合负载分担采用本地转发优先仅对已知单播报文生效。

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，当重启 IRF 中的某台成员设备时，系统可以将待重启设备上的聚合成员端口的流量重定向到其它设备上，从而实现聚合链路上流量的不中断。有关IRF的详细介绍，请参见“IRF 配置指导”中的“IRF”。

表1-19 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**	-

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

注意

- 只有动态聚合组支持聚合流量重定向功能，且仅对已知单播报文生效。
- 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 MSTP 功能，在重启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。
- 使能了聚合流量重定向功能后，请勿将配置了物理连接状态抑制的以太网接口加入聚合组。以免聚合组中的选中端口出现异常。有关以太网接口物理连接状态抑制功能请参见“以太网接口命令”中的“**link-delay**”命令。

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1-20 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 （仅R5206及以上版本支持**description**参数）	**display interface** [**bridge-aggregation** | **route-aggregation**] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface** { **bridge-aggregation** | **route-aggregation** } *interface-number* [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示本端系统的设备ID	**display lacp system-id** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
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** [{ **bridge-aggregation** | **route-aggregation** } *interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示成员端口上链路聚合的详细信息	**display link-aggregation member-port** [*interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示所有聚合组的摘要信息	**display link-aggregation summary** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定聚合组的详细信息	**display link-aggregation verbose** [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
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** [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]]

1.8 以太网链路聚合典型配置举例

说明

在聚合组中，只有端口属性类配置（请参见“1.1 5. 配置分类”）和第二类配置（请参见“1.1 5. 配置分类”）都与参考端口（请参见“1.1 6. 参考端口”）相同的成员端口才可以成为选中端口。因此，用户需通过配置使各成员端口的上述配置与参考端口保持一致，而除此以外的其它配置则只需在聚合接口上进行，不必再在成员端口上重复配置。

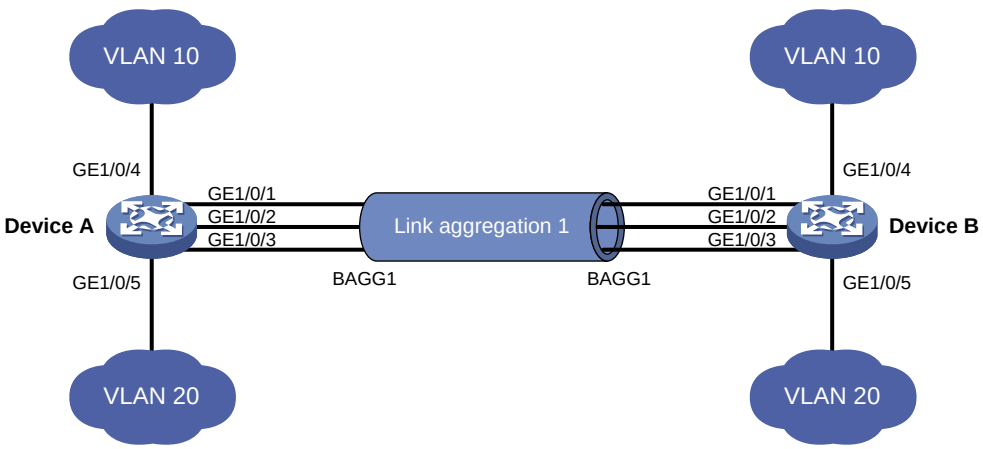
1.8.1 二层静态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的二层以太网端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。
- 在 Device A 和 Device B 上分别配置二层静态链路聚合组，并使两端的 VLAN 10 和 VLAN 20 之间分别互通。
- 通过按照报文的源 MAC 地址和目的 MAC 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1-5 二层静态聚合配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 10，并将端口 GigabitEthernet1/0/4 加入到该 VLAN 中。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
```

```
[DeviceA-vlan10] quit
```
创建 VLAN 20，并将端口 GigabitEthernet1/0/5 加入到该 VLAN 中。
```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```
创建二层聚合接口 1。
```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```
分别将端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。
```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```
配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 10 和 20 的报文通过。
```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
 Please wait... Done.
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[DeviceA-Bridge-Aggregation1] quit
```
配置全局按照报文的源 MAC 地址和目的 MAC 地址进行聚合负载分担。
```
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac
```
(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

(3) 检验配置效果

查看 Device A 上所有聚合组的摘要信息。
```
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

AGG         AGG       Partner ID              Select Unselect   Share
Interface   Mode                              Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1       S         none                    3      0          Shar
```
以上信息表明，聚合组 1 为负载分担类型的二层静态聚合组，包含有三个选中端口。

查看 Device A 上全局采用的聚合负载分担类型。

```
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
  destination-mac address, source-mac address
```

以上信息表明，所有聚合组都按照报文的源 MAC 地址和目的 MAC 地址进行聚合负载分担。

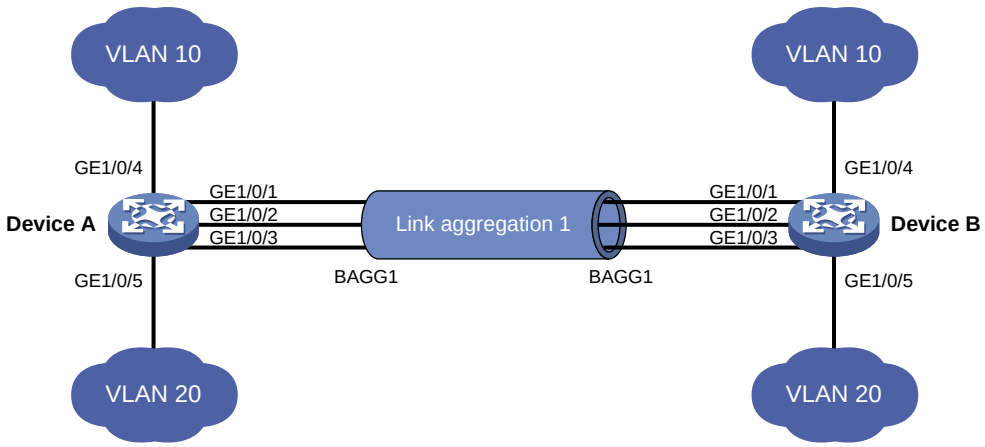
1.8.2 二层动态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的二层以太网端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。
- 在 Device A 和 Device B 上分别配置二层动态链路聚合组，并使两端的 VLAN 10 和 VLAN 20 之间分别互通。
- 通过按照报文的源 MAC 地址和目的 MAC 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 二层动态聚合配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 10，并将端口 GigabitEthernet1/0/4 加入到该 VLAN 中。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/5 加入到该 VLAN 中。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

创建二层聚合接口 1，并配置该接口为动态聚合模式。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
```
分别将端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。
```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```
配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 10 和 20 的报文通过。
```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
 Please wait... Done.
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[DeviceA-Bridge-Aggregation1] quit
```
配置全局按照报文的源 MAC 地址和目的 MAC 地址进行聚合负载分担。
```
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac
```
(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

(3) 检验配置效果

查看 Device A 上所有聚合组的摘要信息。
```
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

AGG         AGG       Partner ID              Select Unselect   Share
Interface   Mode                              Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1       D         0x8000, 000f-e2ff-0002  3      0          Shar
```
以上信息表明，聚合组 1 为负载分担类型的二层动态聚合组，包含有三个选中端口。

查看 Device A 上全局采用的聚合负载分担类型。
```
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
  destination-mac address, source-mac address
```
以上信息表明，所有聚合组都按照报文的源 MAC 地址和目的 MAC 地址进行聚合负载分担。

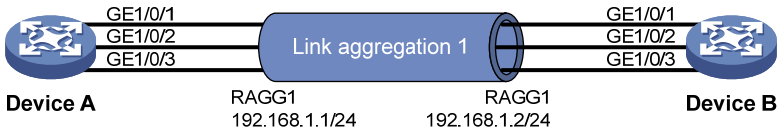
1.8.3 三层静态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的三层以太网端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 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。
- 通过按照报文的源 IP 地址和目的 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分担。

2. 组网图

图1-7 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 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

配置全局按照报文的源 IP 地址和目的 IP 地址进行聚合负载分担。

```
[DeviceA] link-aggregation load-sharing mode source-ip destination-ip
```

(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

(3) 检验配置效果

查看 Device A 上所有聚合组的摘要信息。

```
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
```

```
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

AGG          AGG       Partner ID               Select Unselect   Share
Interface    Mode                               Ports  Ports      Type
--------------------------------------------------------------------------------
RAGG1        S         none                     3      0          Shar
```

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。

查看 Device A 上全局采用的聚合负载分担类型。

```
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
  destination-ip address,  source-ip address
```

以上信息表明，所有聚合组都按照报文的源 IP 地址和目的 IP 地址进行聚合负载分担。

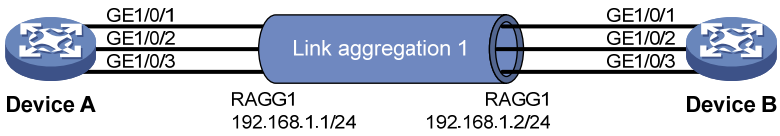
1.8.4 三层动态聚合配置举例

1. 组网需求

- Device A 与 Device B 通过各自的三层以太网端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 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。
- 通过按照报文的源 IP 地址和目的 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分担。

2. 组网图

图1-8 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 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

配置全局按照报文的源 IP 地址和目的 IP 地址进行聚合负载分担。

```
[DeviceA] link-aggregation load-sharing mode source-ip destination-ip
```

(2) 配置 Device B

Device B 的配置与 Device A 相似，配置过程略。

(3) 检验配置效果

查看 Device A 上所有聚合组的摘要信息。

```
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

AGG         AGG       Partner ID              Select Unselect   Share
Interface   Mode                              Ports  Ports      Type
--------------------------------------------------------------------------------
RAGG1       D         0x8000, 000f-e2ff-0002  3      0          Shar
```

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。

查看 Device A 上全局采用的聚合负载分担类型。

```
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
  destination-ip address,  source-ip address
```

以上信息表明，所有聚合组都按照报文的源 IP 地址和目的 IP 地址进行聚合负载分担。

目 录

1 端口隔离配置

1.1 端口隔离简介

为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。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数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

目前：

- 本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它的隔离组。
- 隔离组内可以加入的端口数量没有限制。

端口隔离特性与端口所属的 VLAN 无关。隔离组内的端口和隔离组外属于同一 VLAN 内的端口二层流量双向互通。

1.2 配置隔离组

1.2.1 将端口加入隔离组

表1-1 将端口加入隔离组

操作		命令	说明
进入系统视图		**system-view**	-
进入以太网端口视图/端口组视图/二层聚合接口视图	进入以太网端口视图	**interface** *interface-type interface-number*	三者必选其一 • 进入以太网端口视图后，下面进行的配置只在当前端口下生效 • 进入端口组视图后，下面进行的配置将在端口组中的所有端口下生效 • 在二层聚合接口视图下执行该命令，则该配置将对二层聚合接口以及相应的所有成员端口生效。在配置过程中，如果某个成员端口配置失败，系统会自动跳过该成员端口继续配置其它成员端口；如果二层聚合接口配置失败，则不会再配置成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
将指定端口加入到隔离组中，并作为隔离组中的普通端口		**port-isolate enable**	必选 缺省情况下，隔离组中没有加入任何端口

1.3 隔离组显示和维护

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隔离组的相关信息，通过查看显示信息验证配置的效果。

表1-2 隔离组显示和维护

操作	命令
显示隔离组的信息	**display port-isolate group** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

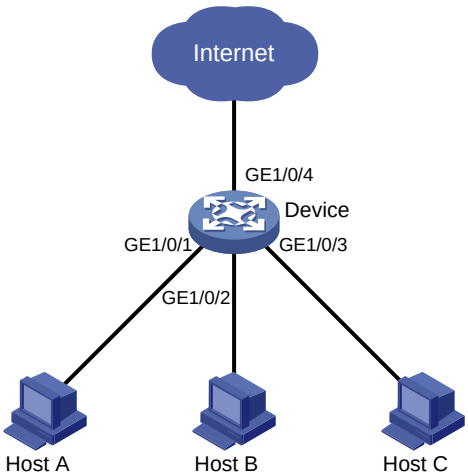
1.4 端口隔离典型配置举例

1. 组网需求

- 小区用户 Host A、Host B、Host C 分别与 Device 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 相连；
- 设备通过 GigabitEthernet1/0/4 端口与外部网络相连；
- 端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 属于同一 VLAN；请实现小区用户 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1-1 配置端口隔离组网图



3. 配置步骤

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 加入隔离组。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable
```

显示隔离组中的信息。

```
<Device> display port-isolate group
```

```
Port-isolate group information:
Uplink port support: NO
Group ID: 1
Group members:
   GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
```

目 录

1 生成树配置

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。

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 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：配置消息在网络中传播的生存期；
- Max Age：配置消息在设备中的最大生存期；
- Hello Time：配置消息的发送周期；
- 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（Root Bridge）的概念。根桥在全网中有且只有一个，其它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，其它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

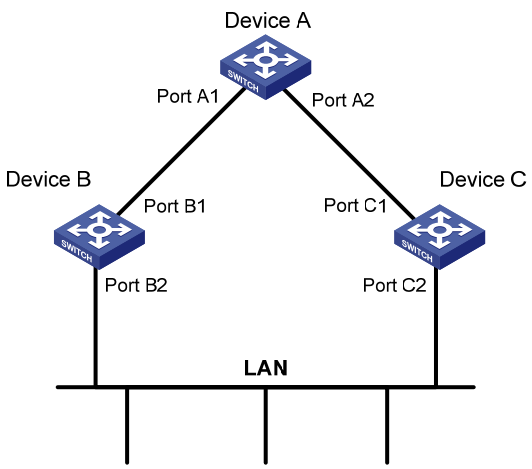
指定桥与指定端口的含义，请参见 表 1-1 的说明。

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配置消息的设备	指定桥向本机转发配置消息的端口
对于一个局域网而言	负责向本网段转发配置消息的设备	指定桥向本网段转发配置消息的端口

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转发配置消息，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转发配置消息，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配置消息，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。通过交换配置消息，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配置消息（最优配置消息的选择过程如表1-3所示）的那个端口定为根端口
2	设备根据根端口的配置消息和根端口的路径开销，为每个端口计算一个指定端口配置消息： • 根桥 ID 替换为根端口的配置消息的根桥 ID； • 根路径开销替换为根端口配置消息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	设备将计算出的配置消息与角色待定端口自己的配置消息进行比较： • 如果计算出的配置消息更优，则该端口被确定为指定端口，其配置消息也被计算出的配置消息替换，并周期性地向外发送； • 如果该端口自己的配置消息更优，则不更新该端口的配置消息并将该端口阻塞。该端口将不再转发数据，且只接收不发送配置消息。

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。其它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 最优配置消息的选择过程

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

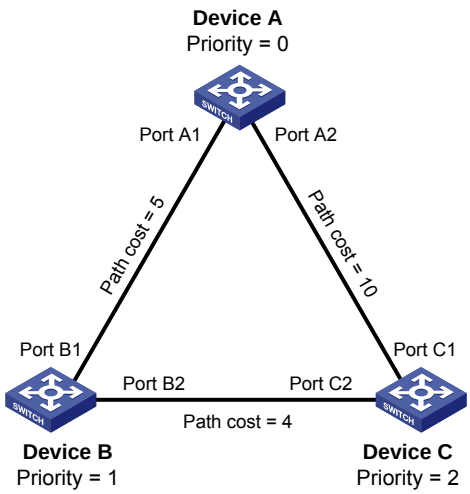
说明

配置消息优先级的比较规则如下：

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

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	端口的配置消息
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 配置消息中各项的具体含义为：{根桥ID，根路径开销，指定桥ID，指定端口ID}。

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

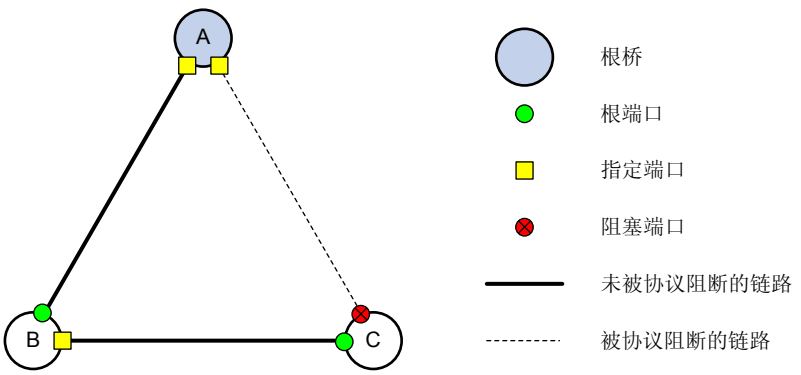
设备	比较过程	比较后端口的配置消息
	• Device C 比较自己各端口的配置消息，发现 Port C1 的配置消息最优，于是该端口被确定为根端口，其配置消息不变。 • Device C 根据根端口的配置消息和路径开销，为 Port C2 计算出指定端口的配置消息{0，10，2，Port C2}，然后与 Port C2 本身的配置消息{1，0，1，Port B2}进行比较，发现计算出的配置消息更优，于是 Port C2 被确定为指定端口，其配置消息也被替换为计算出的配置消息。	• 根端口 Port C1：{0，0，0，Port A2} • 指定端口 Port C2：{0，10，2，Port C2}
	• Port C2 收到 Port B2 更新后的配置消息{0，5，1，Port B2}，发现其比自己的配置消息{0，10，2，Port C2}更优，于是更新自己的配置消息。 • Port C1 收到 Port A2 周期性发来的配置消息{0，0，0，Port A2}，发现其与自己的配置消息一样，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（收到的配置消息中的根路径开销 0＋本端口所在链路的路径开销 10）与 Port C2 的根路径开销 9（收到的配置消息中的根路径开销 5＋本端口所在链路的路径开销 4），发现后者更小，因此 Port C2 的配置消息更优，于是 Port C2 被确定为根端口，其配置消息不变。 • Device C 根据根端口的配置消息和路径开销，为 Port C1 计算出指定端口的配置消息{0，9，2，Port C1}，然后与 Port C1 本身的配置消息{0，0，0，Port A2}进行比较，发现本身的配置消息更优，于是 Port C1 被阻塞，其配置消息不变。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}

说明

表 1-5 配置消息中各项的具体含义为：{根桥ID，根路径开销，指定桥ID，指定端口ID}。

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的配置消息传递机制

STP 的配置消息传递机制如下：

- 当网络初始化时，所有的设备都将自己作为根桥，生成以自己为根的配置消息，并以 Hello Time 为周期定时向外发送。
- 接收到配置消息的端口如果是根端口，且接收的配置消息比该端口的配置消息优，则设备将配置消息中携带的 Message Age 按照一定的原则递增，并启动定时器为这条配置消息计时，同时将此配置消息从设备的指定端口转发出去。
- 如果指定端口收到的配置消息比本端口的配置消息优先级低时，会立刻发出自己的更好的配置消息进行回应。
- 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配置消息，旧的配置消息将会因为超时而被丢弃，设备重新生成以自己为根的配置消息并向外发送，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，重新计算得到的新配置消息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配置消息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配置消息已经传遍整个网络。
- 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：用于判断配置消息在设备内的保存时间是否“过时”，设备会将过时的配置消息丢弃。

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。

说明

- 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，而没有连接到其它设备或共享网段上）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。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，而对于其它本端口允许通过的 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，但是和 STP 一样存在以下缺陷：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 端口的状态发生改变时，所有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。

2. MSTP的基本概念

图1-4 MSTP 的基本概念示意图

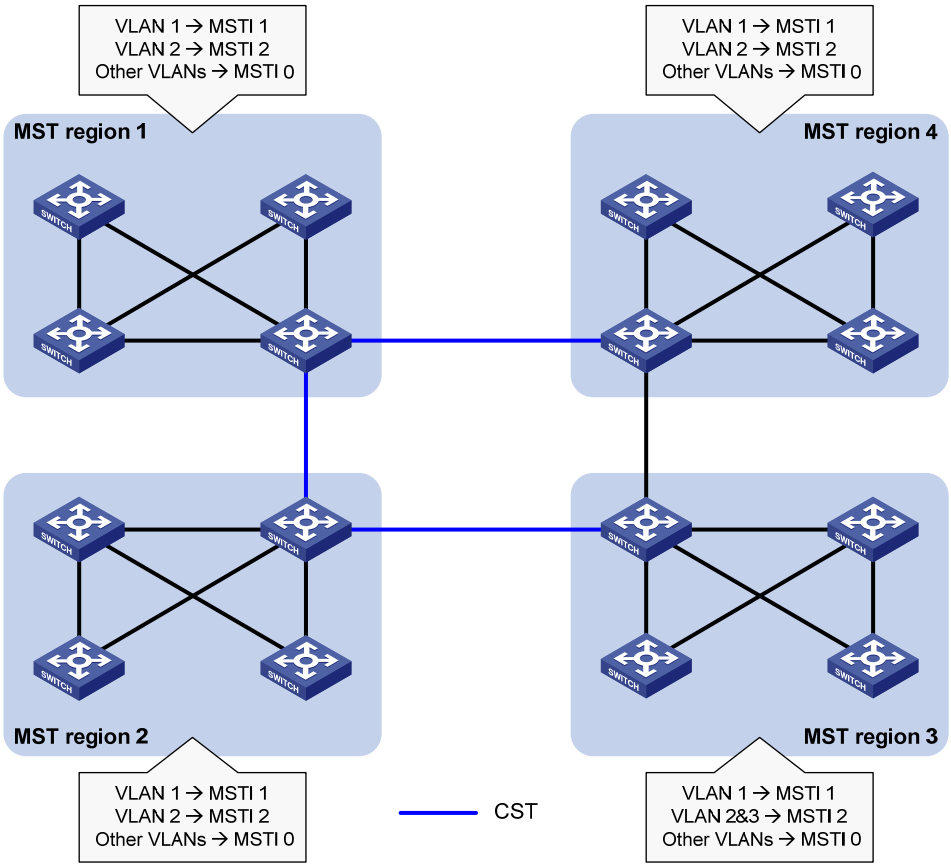
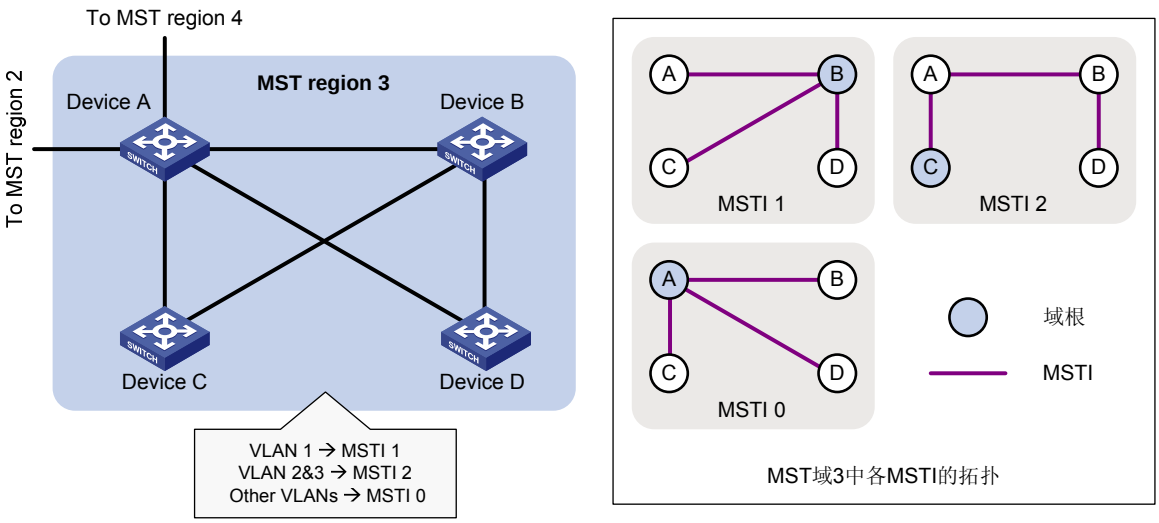


图1-5 MST 域 3 详图



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。

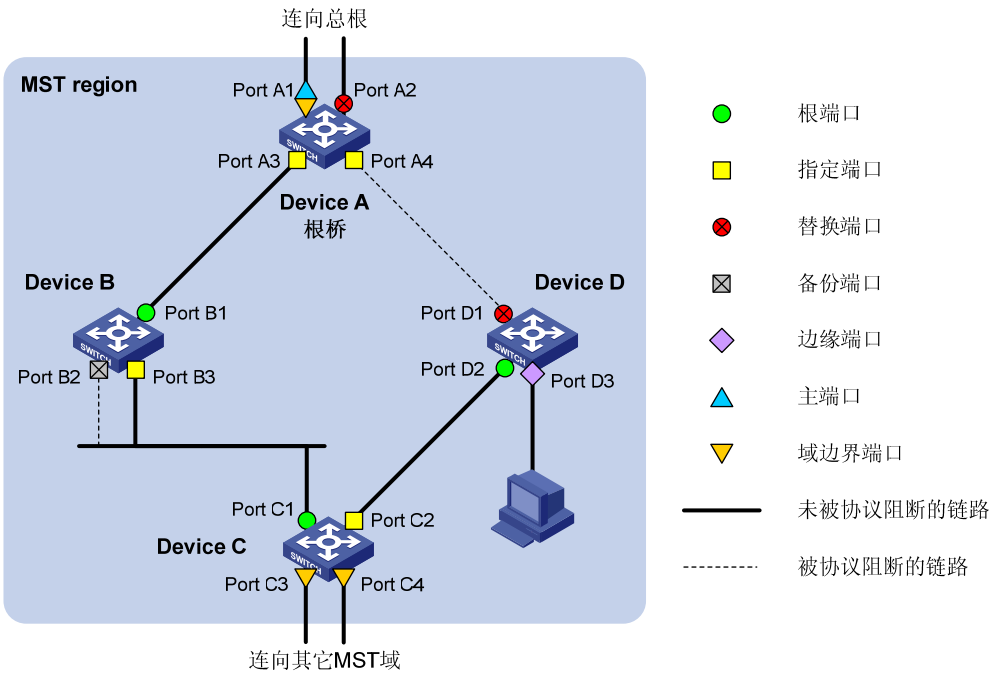
(8) 总根

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 连向其它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）：不与其它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，而在其它 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、并连接其它 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，在其它 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。

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

说明

同一端口在不同的 MSTI 中的端口状态可以不同。

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，使用配置消息进行生成树的计算，只是配置消息中携带的是设备上 MSTP 的配置信息。

(1) CIST 生成树的计算

通过比较配置消息后，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；
- BPDU 拦截功能。

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

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，依照以下表格进行配置。

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 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
	配置端口的最大发送速率	可选	1.3.9

配置任务		说明	详细配置
	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
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
	配置端口的最大发送速率	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
	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
配置TC Snooping功能		可选	1.3.20
配置生成树保护功能		可选	1.3.21

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 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
	配置端口的最大发送速率	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
	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 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
	配置端口的最大发送速率	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TC Snooping功能		可选	1.3.20
配置生成树保护功能		可选	1.3.21

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
	配置端口的最大发送速率	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 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
	配置端口的最大发送速率	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	1.3.21

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	可选 生成树缺省即工作在MSTP模式下	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
	配置端口的最大发送速率	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
	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	可选 生成树缺省即工作在MSTP模式下	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
	配置端口的最大发送速率	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TC Snooping功能		可选	1.3.20
配置生成树保护功能		可选	1.3.21

说明

- 当同时使能 GVRP 和生成树协议时，GVRP 报文将沿 CIST 传播。因此当同时使能了 GVRP 和生成树协议时，如果希望通过 GVRP 在网络中发布某个 VLAN，则配置生成树协议的 VLAN 映射表时要保证将该 VLAN 映射到 CIST 上。有关 GVRP 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“GVRP”。
- 生成树协议与以下功能互斥：业务环回功能、RRPP 功能、Smart Link 功能和 STP 协议的 BPDU Tunnel 功能。
- 对于生成树的相关配置来说：系统视图下的配置在全局生效；二层以太网端口下的配置只对当前端口生效；端口组视图下的配置对当前端口组中的所有端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。
- 在二层聚合接口上使能生成树协议后，生成树的相关计算只在二层聚合接口上进行，聚合成员端口不再参与生成树计算。二层聚合接口的所有选中成员端口上生成树协议的使能/关闭状态以及端口转发状态与二层聚合接口保持一致。尽管聚合成员端口不参与生成树计算，但端口上的生成树相关配置仍然保留，当端口退出聚合组时，该端口将采用这些配置参与生成树计算。

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四种：

- STP 模式：设备的各端口都将向外发送 STP BPDU。如果端口的对端设备只支持 STP，可选择此模式。
- RSTP 模式：设备的各端口都向外发送 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。
- MSTP 模式：设备的各端口都向外发送 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。
- PVST 模式：设备的各端口都向外发送 PVST BPDU，每个 VLAN 维护一棵生成树。不同型号的设备可维护的 VLAN 数目（假设为 n，S5500-HI 系列交换机为 128）不同，当使用不同型号的设备进行 PVST 组网时，网络中维护有生成树的 VLAN 总数请勿超过最小的 n 值，否则将导致网络故障。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 的友商设备互通时支持像 RSTP 一样的快速收敛。

MSTP 模式兼容 RSTP 模式，RSTP 模式兼容 STP 模式，而 PVST 模式与其它模式的兼容性如下：

- 对于 Access 端口：PVST 模式在任意 VLAN 中都能与其它模式互相兼容。
- 对于 Trunk 端口或 Hybrid 端口：PVST 模式仅在 VLAN 1 中能与其它模式互相兼容。

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 { stp | rstp | mstp | pvst }**	必选 缺省情况下，生成树的工作模式为MSTP模式

1.3.2 配置MST域

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*	可选 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-list*	二者可选其一 缺省情况下，所有VLAN都映射到CIST（即MSTI 0）上
	vlan-mapping modulo *modulo*	

操作	命令	说明
配置MSTP的修订级别	**revision-level** *level*	可选 缺省情况下，MSTP的修订级别为0
显示MST域的预配置信息	**check region-configuration**	可选
激活MST域的配置	**active region-configuration**	必选
显示当前生效的MST域配置信息	**display stp region-configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图执行

说明

- 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 enable** 使能生成树协议后才会生效。
- 在 PVST 模式下，系统会自动将 VLAN 与 MSTI 进行映射。由于设备在 PVST 模式下支持的 MSTI 数量比在 MSTP 模式下多，因此当由 PVST 模式切换到 MSTP 模式时，多出的 MSTI（按 MSTI 的编号由小到大确定）的映射关系配置将被自动清除，此后即使再切换回 PVST 模式，被清除的这些配置也不会自动恢复。为了避免这种情况，在 PVST 模式下不建议手工配置 VLAN 与 MSTI 的映射关系。

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，也可以作为其它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。

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**	必选 缺省情况下，设备不是根桥
配置当前设备为根桥（PVST模式）	**stp vlan** *vlan-list* **root primary**	
配置当前设备为根桥（MSTP模式）	**stp** [**instance** *instance-id*] **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**	必选 缺省情况下，设备不是备份根桥
配置当前设备为备份根桥（PVST模式）	**stp vlan** *vlan-list* **root secondary**	
配置当前设备为备份根桥（MSTP模式）	**stp** [**instance** *instance-id*] **root secondary**	

说明

- 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 配置设备的优先级”。

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。

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*	必选 缺省情况下，设备的优先级为32768
配置设备的优先级（PVST模式）	**stp vlan** *vlan-list* **priority** *priority*	
配置设备的优先级（MSTP模式）	**stp** [**instance** *instance-id*] **priority** *priority*	

注意

- 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。
- 在生成树根桥的选择过程中，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。

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，域内的配置消息（即 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 的配置消息，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。

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*	必选 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。网络直径就是指交换网络中任意两台终端设备间的最大设备数。网络直径越大，说明网络的规模越大。

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*	必选 缺省情况下，交换网络的网络直径为7
配置交换网络的网络直径（PVST模式）	**stp vlan** *vlan-list* **bridge-diameter** *diameter*	

说明

- 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根桥上生效。

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 时间会发送配置消息，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：用于确定配置消息是否超时。在 MSTP 的 CIST 以及 PVST 的各 VLAN 上，设备根据 Max Age 时间来确定端口收到的配置消息是否超时。如果端口收到的配置消息超时，则需要对该 MSTI 重新计算。Max Age 时间对 MSTP 的 MSTI 无效。

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：

(1) 2×（Forward Delay－1 秒）≥Max Age

(4) Max Age ≥2×（Hello Time＋1 秒）

通常情况下，不建议通过本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，因此建议通过调整网络直径，使生成树协议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*	可选 缺省情况下，Forward Delay为15秒
配置Forward Delay时间参数（PVST模式）	**stp vlan** *vlan-list* **timer forward-delay** *time*	
配置Hello Time时间参数（STP/RSTP/MSTP模式）	**stp timer hello** *time*	可选 缺省情况下，Hello Time为2秒
配置Hello Time时间参数（PVST模式）	**stp vlan** *vlan-list* **timer hello** *time*	

操作	命令	说明
配置Max Age时间参数（STP/RSTP/MSTP模式）	**stp timer max-age** *time*	可选 缺省情况下，Max Age为20秒
配置Max Age时间参数（PVST模式）	**stp vlan** *vlan-list* **timer max-age** *time*	

- 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。建议用户采用缺省值。
- 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配置消息，增加了设备的负担，浪费了网络资源。建议用户采用缺省值。
- 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。建议用户采用缺省值。

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*	必选 缺省情况下，设备的超时时间因子为3

1.3.9 配置端口的最大发送速率

端口的最大发送速率是指每Hello Time时间内端口能够发送的BPDU最大数目。端口的最大发送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。

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的最大发送速率		**stp transmit-limit** *limit*	必选 缺省情况下，端口的最大发送速率为10

说明

最大发送速率越高，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。适当配置最大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。

1.3.10 配置端口为边缘端口

当端口直接与用户终端相连，而没有连接到其它设备或共享网段上，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。

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置当前端口为边缘端口		**stp edged-port enable**	必选 缺省情况下，端口为非边缘端口

说明

- 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它端口的 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。
- 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。
- 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。

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。

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 }**	必选 缺省情况下，缺省路径开销的计算标准为私有标准

注意

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。

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

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
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
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

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

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一

操作		命令	说明
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的路径开销（STP/RSTP模式）		**stp cost** *cost*	必选 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
配置端口的路径开销（PVST模式）		**stp vlan** *vlan-list* **cost** *cost*	
配置端口的路径开销（MSTP模式）		**stp [instance** *instance-id* **] cost** *cost*	

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。

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 GigabitEthernet1/0/3 在 MSTI 2 上的路径开销值为 200。

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 cost 200
```

在 PVST 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 GigabitEthernet1/0/3 在 PVST VLAN 20～30 上的路径开销均为 2000。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp pathcost-standard dot1d-1998
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] 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。

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的优先级（STP/RSTP模式）		**stp port priority** *priority*	必选 缺省情况下，端口的优
配置端口的优先级（PVST模式）		**stp vlan** *vlan-list* **port priority** *priority*	

操作	命令	说明
配置端口的优先级（MSTP模式）	**stp** [**instance** *instance-id*] **port priority** *priority*	先级为128

说明

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。

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。

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型		**stp point-to-point** { **auto** | **force-false** | **force-true** }	必选 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

说明

- 如果某端口是二层聚合接口或其工作在全双工模式下，则可以将该端口配置为与点对点链路相连。通常建议使用缺省配置，由系统进行自动检测。
- 在 MSTP 模式或 PVST 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 MSTI 或 VLAN 都有效。
- 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。

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收发的 MSTP 报文格式，使端口只收发与所配格式相符的 MSTP 报文，实现与对端发送所配置格式报文的设备互通。

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口收发的MSTP报文格式		**stp compliance { auto | dot1s | legacy }**	必选 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

说明

- 设备提供了 MSTP 报文格式不兼容保护功能：在 MSTP 模式下，当端口上配置的收发 MSTP 报文格式不是 **auto** 时，如果端口收到了与所配格式不符的报文，该端口将成为指定端口，其状态将保持在 Discarding，以防止出现环路。
- 设备提供了 MSTP 报文格式频繁切换保护功能：设备运行过程中，如果端口收到的 MSTP 报文格式频繁变化，则表明组网中 MSTP 报文格式的配置出现了错误，此时在 MSTP 模式下会把该端口关闭以进行保护。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”。

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**	必选 缺省情况下，端口状态变化信息显示开关处于开启状态
打开端口状态变化信息显示开关（PVST模式）	**stp port-log vlan** *vlan-list*	

操作	命令	说明
打开端口状态变化信息显示开关（MSTP模式）	**stp port-log instance** { *instance-id* | **all** }	

1.3.16 使能生成树协议

只有使能了生成树协议，生成树的其它配置才会生效。

1. 使能生成树协议（STP/RSTP/MSTP模式）

在 STP/RSTP/MSTP 模式下，须保证全局和端口上的生成树协议均处于使能状态。

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 enable**	必选 缺省情况下，全局生成树协议处于关闭状态
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
在端口上使能生成树协议		**stp enable**	可选 缺省情况下，所有端口上的生成树协议均处于使能状态

2. 使能生成树协议（PVST模式）

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。

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 enable**	必选 缺省情况下，全局生成树协议处于关闭状态
在VLAN中使能生成树协议		**stp vlan** *vlan-list* **enable**	必选 缺省情况下，VLAN上生成树协议处于使能状态
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	

操作	命令	说明
在端口上使能生成树协议	**stp enable**	可选 缺省情况下，所有端口上的生成树协议均处于使能状态

说明

- 可以通过 **undo stp enable** 命令关闭特定端口的生成树协议，使这些端口不参与生成树计算，以节省设备的 CPU 资源。
- 在 PVST 模式下，全局使能生成树协议后，设备会默认使能已创建的前 n 个 VLAN（n 为设备支持的 PVST 实例数，S5500-HI 系列交换机为 128）上的生成树协议，此时如果需要再使能其它指定 VLAN 的生成树协议，需先关闭某些 VLAN 的生成树协议，然后再在指定的 VLAN 上使能生成树协议。如果设备上创建的 VLAN 总数没有超过 n，则不存在这种情况。

1.3.17 执行mCheck操作

MSTP 的工作模式有 STP 模式、RSTP 模式、MSTP 模式和 PVST 模式四种。在运行 MSTP、RSTP 或 PVST 的设备上，若某端口连接着运行 STP 协议的设备，该端口会自动迁移到 STP 模式；但在下列两种情况下，该端口将无法自动迁移回到原有模式，而需要通过执行 mCheck 操作将其手工迁移回原有模式：

- 运行 STP 协议的设备被关机或撤走；
- 运行 STP 协议的设备切换为 MSTP 模式、RSTP 模式或 PVST 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/MSTP/PVST 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/MSTP/PVST 协议，除了要在设备 B 上配置生成树的工作模式为 RSTP/MSTP/PVST 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。

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 mcheck**	必选

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**	-
进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
在端口上执行mCheck操作	**stp mcheck**	必选

注意

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

1.3.18 配置摘要侦听功能

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。

1. 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。

2. 配置摘要侦听功能

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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	

配置步骤	命令	说明
在端口上使能摘要侦听功能	**stp config-digest-snooping**	必选 缺省情况下，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 config-digest-snooping**	必选 缺省情况下，摘要侦听功能处于关闭状态

注意

- 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，禁止修改 MST 域配置中 VLAN 与 MSTI 的映射关系，禁止执行 **undo stp region-configuration** 命令取消当前域配置，但可以修改域配置中的域名和修订级别。
- 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。

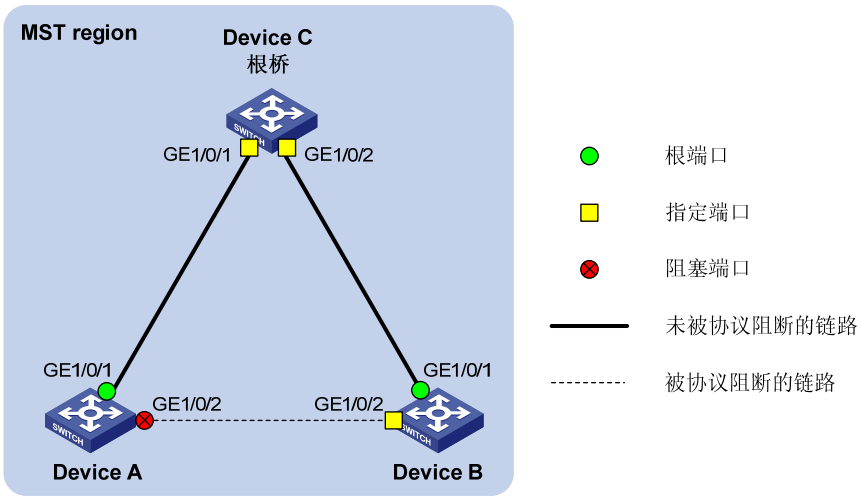
3. 摘要侦听功能配置举例

(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 GigabitEthernet1/0/1 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 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] stp config-digest-snooping
```

在 Device B 的端口 GigabitEthernet1/0/1 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 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] stp config-digest-snooping
```

1.3.19 配置No Agreement Check功能

RSTP 和 MSTP 的指定端口快速迁移机制使用两种协议报文：

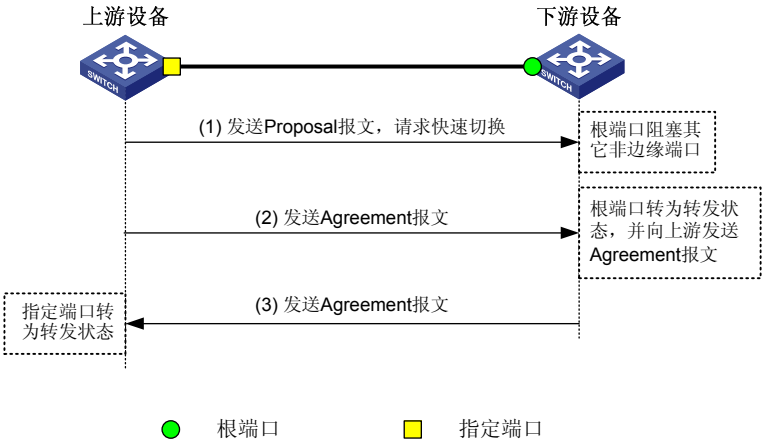
- Proposal 报文：指定端口请求快速迁移的报文。
- Agreement 报文：同意对端进行快速迁移的报文。

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。

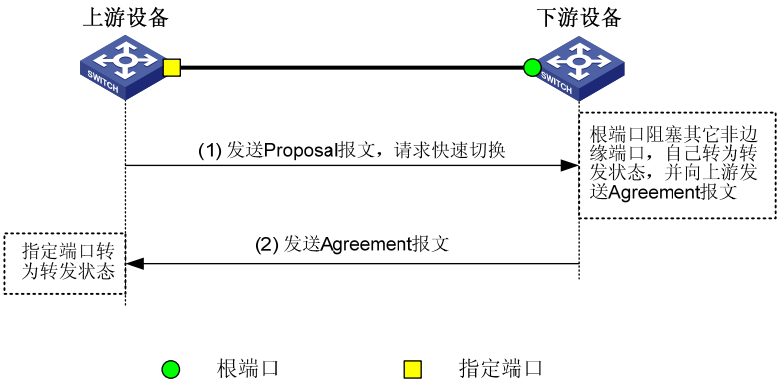
如 图 1-8 所示，是MSTP的指定端口快速迁移机制。

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。

1. 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。

2. 配置No Agreement Check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**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能No Agreement Check功能		**stp no-agreement-check**	必选 缺省情况下，No Agreement Check功能处于关闭状态

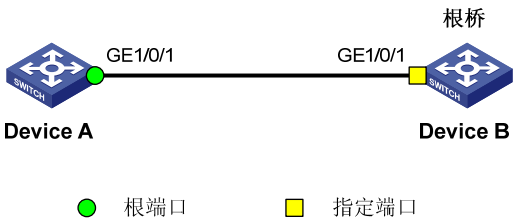
3. No Agreement Check功能配置举例

(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

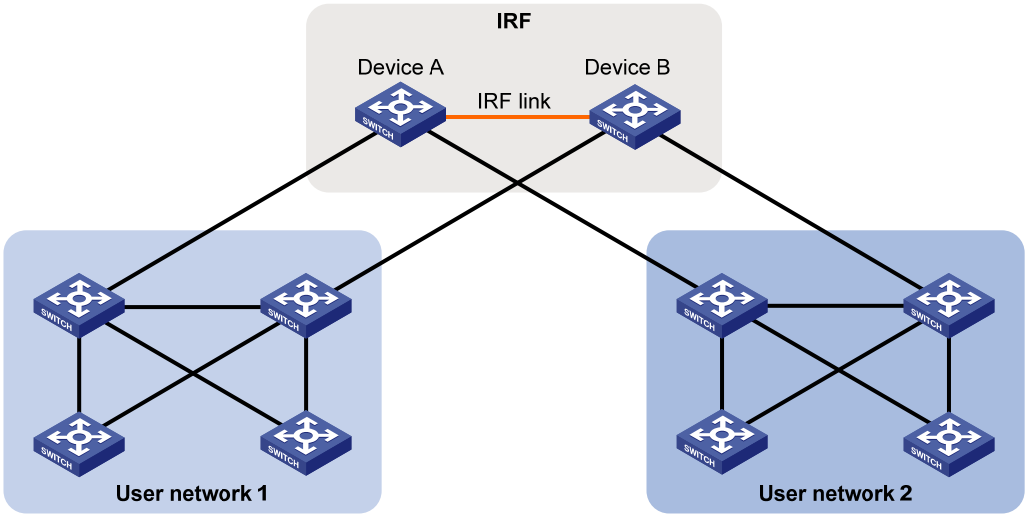
在 Device A 的端口 GigabitEthernet1/0/1 上使能 No Agreement Check 功能。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

1.3.20 配置TC Snooping功能

TC Snooping功能的典型应用环境如 图 1-11 所示。在该组网中，由Device A和Device B组成的IRF设备未使能生成树协议，而用户网络 1 和 2 中的所有设备均使能了生成树协议。用户网络 1 和 2 均通过双上行链路与IRF设备相连以提高链路可靠性，BPDU在每个用户网络中都能够被IRF设备进行透明传输。

图1-11 TC Snooping 功能典型应用组网图



在该组网中，当 IRF 设备和用户网络的拓扑结构发生改变时，由于 IRF 设备对 BPDU 进行了透明传输而不参与生成树计算，因而其本身可能需经过较长时间才能重新学到正确的 MAC 地址表项和 ARP 表项，在此期间可能导致网络中断。为了避免这种情况，可以通过在 IRF 设备上使能 TC Snooping 功能，使其在收到 TC-BPDU（网络拓扑发生变化的通知报文）后，主动更新接收该报文的端口所属的 VLAN 所对应的 MAC 地址表和 ARP 表，从而保证业务流量的正常转发。

说明

- 有关 MAC 地址表的详细介绍，请参见“二层技术-以太网交换配置指导”中的“MAC 地址表”。
- 有关 ARP 表的详细介绍，请参见“三层技术-IP 业务配置指导”中的“ARP”。

表1-36 配置 TC Snooping 功能

操作	命令	说明
进入系统视图	**system-view**	-
全局关闭生成树协议	**undo stp enable**	必选 缺省情况下，生成树协议在全局处于关闭状态
使能TC Snooping功能	**stp tc-snooping**	必选 缺省情况下，TC Snooping功能处于关闭状态

说明

- 由于 TC Snooping 功能与生成树协议互斥，因此在使能 TC Snooping 功能之前必须全局关闭生成树协议。
- 由于 BPDU Tunnel 功能比 TC Snooping 功能的优先级高，因此若某端口使能了生成树协议的 BPDU Tunnel 功能，TC Snooping 功能将不会在该端口上生效。有关 BPDU Tunnel 功能的详细介绍，请参见“二层技术-以太网交换配置指导”中的“BPDU Tunnel”。
- TC Snooping 功能不支持 PVST 格式的 TC-BPDU，因此在 PVST 组网环境下 TC Snooping 功能不生效。

1.3.21 配置生成树保护功能

生成树保护功能有以下几种：

- BPDU 保护功能
- 根保护功能
- 环路保护功能
- 防 TC-BPDU 攻击保护功能
- BPDU 拦截功能

1. 配置准备

生成树协议在设备上已经正确配置。

2. 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；当这些端口接收到配置消息（即 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 的配置消息。如果有人伪造配置消息恶意攻击设备，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配置消息，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。被关闭的端口在端口状态检测定时器超时后将被重新激活。有关端口状态检测定时器的详细介绍，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。

表1-37 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**	必选 缺省情况下，BPDU保护功能处于关闭状态

说明

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“二层技术-以太网交换配置指导”中的“以太网端口”。

3. 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配置消息，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 优先级更高的配置消息，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配置消息时，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。

表1-38 配置根保护功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口的根保护功能		**stp root-protection**	必选 缺省情况下，端口上的根保护功能处于关闭状态

说明

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。

4. 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它阻塞端口的状态。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。

表1-39 配置环路保护功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口的环路保护功能		**stp loop-protection**	必选 缺省情况下，端口的环路保护功能处于关闭状态

说明

- 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。

5. 配置防TC-BPDU攻击保护功能

设备在接收到 TC-BPDU（网络拓扑发生变化的通知报文）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。

通过在设备上使能防 TC-BPDU 攻击保护功能，可以避免频繁地刷新转发地址表项。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。

表1-40 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 enable**	可选 缺省情况下，防TC-BPDU攻击保护功能处于使能状态
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*	可选 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

说明

建议不要关闭防 TC-BPDU 攻击保护功能。

6. 配置BPDU拦截功能

在使能了生成树协议的网络中，由于设备收到 BPDU 后会进行 STP 计算并向其它设备转发，因此恶意用户可借此进行 BPDU 攻击：通过不停地发送 BPDU，使网络中的所有设备都不停地进行 STP 计算，从而导致设备的 CPU 占用率过高或 BPDU 的协议状态错误等问题。

为了避免这种情况，用户可以在端口上配置 BPDU 拦截功能。使能了该功能的端口将不再接收任何 BPDU，从而能够防止设备遭受 BPDU 攻击，保证 STP 计算的正确性。

表1-41 配置 BPDU 拦截功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
使能端口的BPDU拦截功能	**bpdu-drop any**	必选 缺省情况下，端口的BPDU拦截功能处于关闭状态

说明

开启 BPDU 拦截功能的端口，对收到的 802.1X 报文也会进行丢弃，因此请不要同时开启端口的 BPDU 拦截功能和 802.1X 功能。关于 802.1X 功能请参见“安全配置指导”中的“802.1X”。

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** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口上的BPDU统计信息	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示被生成树保护功能down掉的端口信息	**display stp down-port** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示生成树端口角色计算的历史信息	**display stp** [**instance** *instance-id* | **vlan** *vlan-id*] **history** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示生成树所有端口收发的TC或TCN报文数	**display stp** [**instance** *instance-id* | **vlan** *vlan-id*] **tc** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示生成树的状态和统计信息	**display stp** [**instance** *instance-id* | **vlan** *vlan-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示当前生效的MST域配置信息	**display stp region-configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示所有生成树的根桥信息	**display stp root** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
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

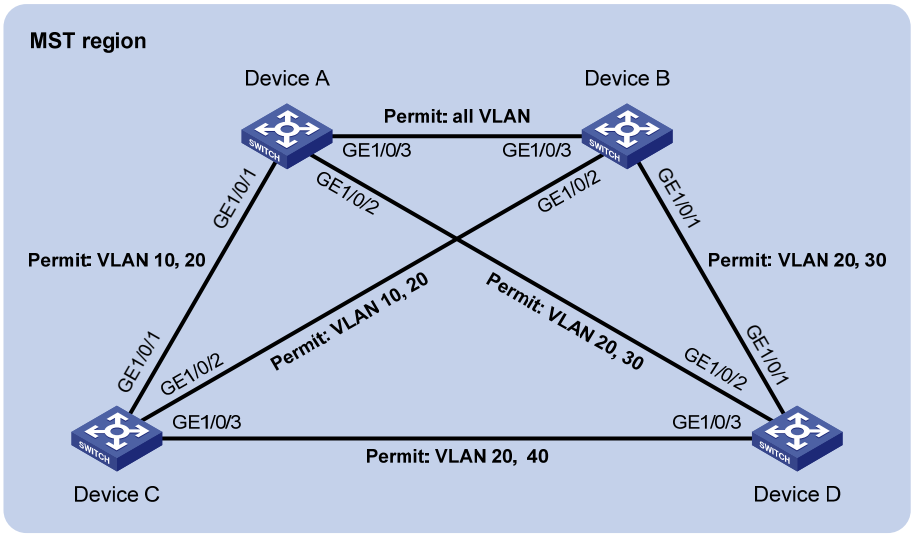
1.5.1 MSTP典型配置举例

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1-12 MSTP 典型配置组网图



3. 配置步骤

(1) 配置 VLAN 和端口

请按照 图 1-12 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 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 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 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 enable
```

(6) 检验配置效果

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
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        ALTE  DISCARDING    NONE
   0        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   3        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   3        GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
```

查看 Device B 上生成树的简要信息。

```
[DeviceB] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
   3        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   3        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

查看 Device C 上生成树的简要信息。

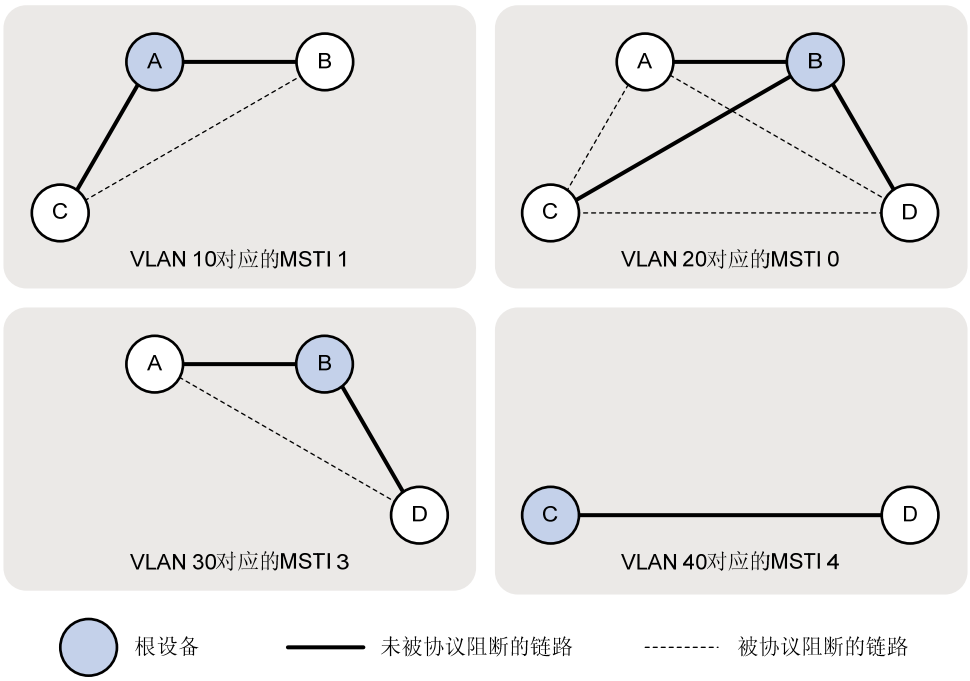
```
[DeviceC] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/2        ROOT  FORWARDING    NONE
   0        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   4        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   0        GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   0        GigabitEthernet1/0/3        ALTE  DISCARDING    NONE
   3        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   3        GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   4        GigabitEthernet1/0/3        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 1-13 所示。

图1-13 各 VLAN 所对应 MSTI 的拓扑图



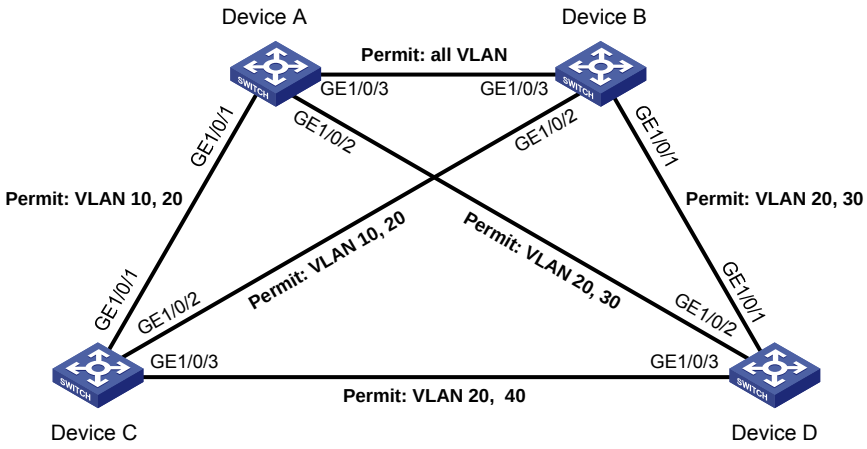
1.5.2 PVST典型配置举例

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、VLAN 20、VLAN 30 和 VLAN 40 的报文分别按照其各自 VLAN 所对应的生成树转发。
- 由于 VLAN 10、VLAN 20 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 VLAN 10 和 VLAN 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1-14 PVST 典型配置组网图



3. 配置步骤

(1) 配置 VLAN 和端口

请按照 图 1-14 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 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 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 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 enable
[DeviceD] stp vlan 20 30 40 enable
```

(6) 检验配置效果

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      Port                        Role  STP State     Protection
   10      GigabitEthernet1/0/1        DESI  DISCARDING    NONE
   10      GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   20      GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   20      GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   20      GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   30      GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   30      GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
```

查看 Device B 上生成树的简要信息。

```
[DeviceB] display stp brief
 VLAN      Port                        Role  STP State     Protection
   10      GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   10      GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
   20      GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   20      GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   20      GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
   30      GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   30      GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

查看 Device C 上生成树的简要信息。

```
[DeviceC] display stp brief
 VLAN      Port                        Role  STP State     Protection
   10      GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   10      GigabitEthernet1/0/2        ALTE  FORWARDING    NONE
   20      GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   20      GigabitEthernet1/0/2        ALTE  FORWARDING    NONE
   20      GigabitEthernet1/0/3        DESI  DISCARDING    NONE
   40      GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

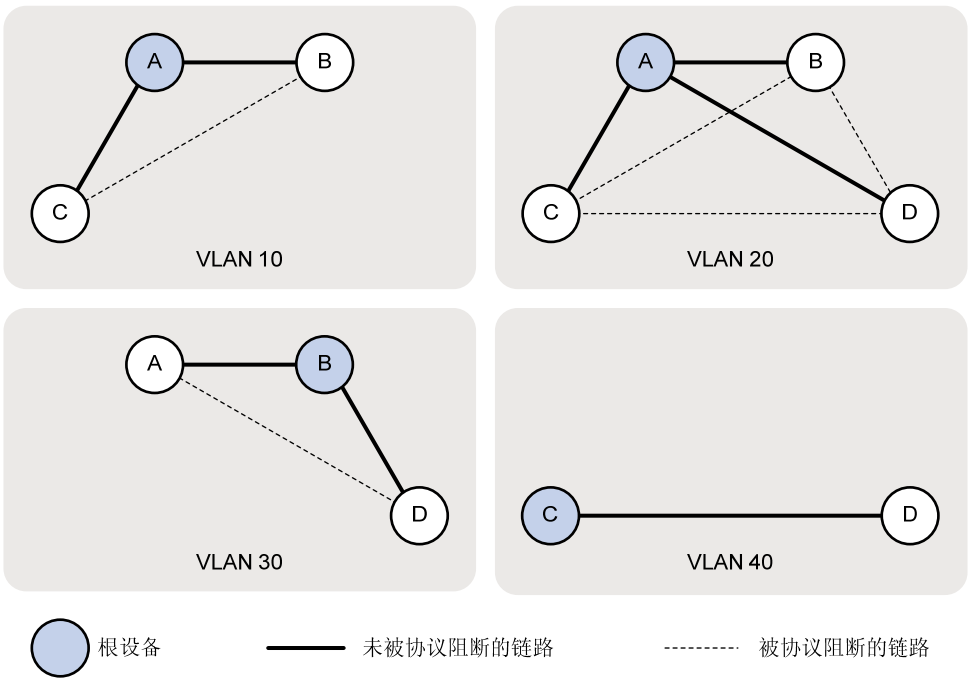
查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
 VLAN      Port                        Role  STP State     Protection
   20      GigabitEthernet1/0/1        ALTE  FORWARDING    NONE
```

```
20      GigabitEthernet1/0/2          ROOT  DISCARDING    NONE
20      GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
30      GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
30      GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
40      GigabitEthernet1/0/3          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 1-15 所示。

图1-15 各 VLAN 所对应生成树的拓扑图



目 录

1 BPDU Tunnel配置

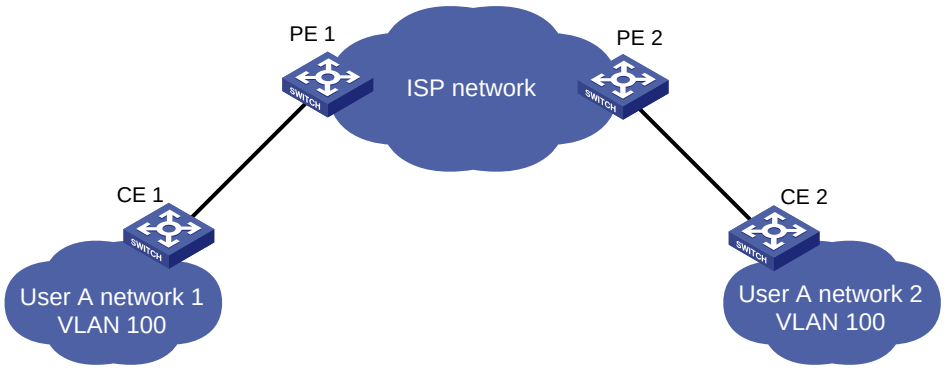
1.1 BPDU Tunnel简介

BPDU Tunnel 是一种二层隧道技术，它使不同地域私网用户的二层协议报文，可以通过运营商网络内的指定通道进行透明传输。

1.1.1 BPDU Tunnel的产生背景

在实际组网中，用户经常利用运营商提供的专线来构建自己的二层网络，这使同一用户私网的不同部分可能分布在运营商公网的两侧。如 图 1-1 所示，用户A拥有属于相同VLAN的两台设备CE 1 和 CE 2，该用户的网络分为网络 1 和网络 2，二者通过运营商网络相连接。当网络 1 和网络 2 中共同运行某种二层协议（如STP协议）时，要求网络 1 和网络 2 中的二层协议报文能够穿越运营商网络，以完成二层协议的计算（如生成树的计算）。但是，当CE发送的二层协议报文到达PE时，由于PE无法识别该报文来自用户网络还是运营商网络，因此会将其上送给CPU进行处理。这样，用户网络与运营商网络的二层协议计算将相互影响，用户网络就无法独立完成二层协议的计算。

图1-1 BPDU Tunnel 应用环境



为了解决上述问题，就要求在运营商网络中能够透传用户网络的二层协议报文。利用 BPDU Tunnel 功能，即可实现上述要求，具体过程如下：

(1) PE 1 将 CE 1 发来的二层协议报文进行封装，将其目的 MAC 地址替换成一个特定的组播 MAC 地址，然后在运营商网络中进行转发；

(2) 封装好的二层协议报文（称为 BPDU Tunnel 报文）被转发至运营商网络另一端的 PE 2，解封装后被还原为原始的目的 MAC 地址，并发送给 CE 2。

说明

目前，H3C 设备支持以下协议的 BPDU Tunnel 功能：

- CDP（Cisco Discovery Protocol，思科发现协议）
- DLDP（Device Link Detection Protocol，设备链路检测协议）
- EOAM（Ethernet Operation, Administration and Maintenance，以太网操作、管理和维护）
- GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）
- HGMP（HW Group Management Protocol，HW 组管理协议）
- LACP（Link Aggregation Control Protocol，链路聚合控制协议）
- LLDP（Link Layer Discovery Protocol，链路层发现协议）
- PAGP（Port Aggregation Protocol，端口聚合协议）
- PVST（Per VLAN Spanning Tree，每 VLAN 生成树）
- STP（Spanning Tree Protocol，生成树协议）
- UDLD（Uni-directional Link Direction，单向链路检测）
- VTP（VLAN Trunking Protocol，VLAN 中继协议）

1.1.2 BPDU Tunnel的实现

各协议的 BPDU Tunnel 实现基本类似，下面以 STP 协议为例介绍 BPDU Tunnel 的实现过程。

说明

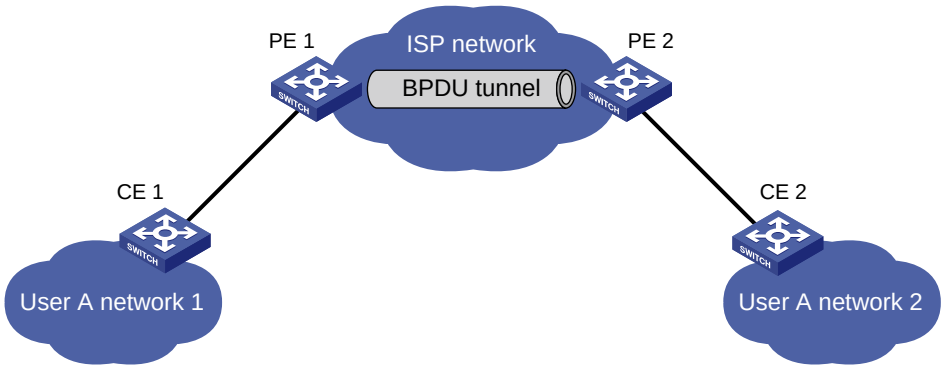
- 本文中的 STP 是指广义的 STP 协议，包括 STP、RSTP 和 MSTP。
- STP 协议通过在设备之间传递 BPDU（Bridge Protocol Data Unit，桥协议数据单元）报文来确定网络的拓扑结构，详情请参见“二层技术-以太网交换配置指导”中的“生成树”。

为避免环路，用户需要在私网中启用 STP 功能，当一侧私网发生拓扑变化时，会发送 BPDU 报文给另一侧私网，否则将无法完成在整个用户私网内的生成树计算。但由于 BPDU 报文是二层组播报文，所有开启 STP 功能的设备都会接收并处理该报文，因此若用户私网和运营商网络的生成树一起计算将导致每个网络都无法生成正确的生成树。

BPDU Tunnel 功能可以解决上述问题，它可使运行 STP 功能的用户私网和运营商网络拥有各自的生成树，互不干扰，它具有下列作用：

- 对 BPDU 报文进行透明传输。可以使同一个用户网络的 BPDU 报文在运营商网络内指定的 VLAN 中进行广播，使得在不同地域的同一个用户网络可以跨越运营商网络进行统一的生成树计算。
- 同时，由于不同用户网络的 BPDU 报文在运营商网络的不同 VLAN 中进行广播，所以不同用户网络的 BPDU 报文相互隔离，可以独立进行生成树计算。

图1-2 BPDU Tunnel 组网示意图



如 图 1-2 所示，上部为运营商网络，下部为用户A的网络。其中，用户A的网络根据地域的不同又分为网络 1 和网络 2。通过在运营商网络两端的边缘设备PE 1 和PE 2 上配置BPDU Tunnel功能，可实现网络 1 和网络 2 之间的BPDU报文在运营商网络中的透明传输，且这两个网络的生成树通过独立计算后生成。举例来说，假设BPDU报文由网络 1 发往网络 2：

(1) 在运营商网络的输入端，PE 1 将来自 CE 1 的 BPDU 报文的目的 MAC 地址 0x0180-C200-0000 修改为特殊的组播 MAC 地址（假设为缺省的 0x010F-E200-0003）。在运营商网络中，修改后的 BPDU 报文（即 BPDU Tunnel 报文）被当作数据报文在用户所属的 VLAN 中进行转发。

(2) 在运营商网络的输出端，PE 2 将目的 MAC 地址为 0x010F-E200-0003 的报文识别出来，将其目的 MAC 地址还原为 0x0180-C200-0000，然后将还原后的 BPDU 报文转发给 CE 2。

说明

用户必须通过配置保证用户网络携有 VLAN Tag 的 BPDU 报文在运营商网络中进行透明传输的过程中，其 VLAN Tag 不能被改变也不能被去掉，否则设备将无法正确透传用户网络的 BPDU 报文。

1.2 配置BPDU Tunnel

1.2.1 配置准备

在配置 BPDU Tunnel 之前，需完成以下任务：

- 在配置某个协议的 BPDU Tunnel 功能前，应在用户网络中启用该协议。
- 在 PE 设备欲配置 BPDU Tunnel 功能的端口上和与其相连的 CE 设备的端口上，应配置相同的 VLAN 属性。
- 运营商网络中各设备间相连的端口均应配置为 Trunk 类型，并允许所有 VLAN 的报文通过。

1.2.2 使能BPDU Tunnel功能

用户可在不同视图下使能不同协议的 BPDU Tunnel 功能。

说明

- 二层以太网端口视图下的配置只对当前端口有效；端口组视图下的配置对当前端口组中的所有端口有效；二层聚合接口视图下的配置只对当前接口有效。
- 在端口上使能 DLDP、EOAM、GVRP、HGMP、LLDP 或 STP 协议的 BPDU Tunnel 功能之前，必须在该端口上关闭相应的协议。由于 PVST 协议是一种特殊的 STP 协议，因此在端口上使能

PVST 协议的 BPDU Tunnel 功能之前，也必须在该端口上关闭 STP 协议并使能 STP 协议的 BPDU Tunnel 功能。

- 不允许在二层聚合组的成员端口上使能 DLDP、EOAM、LACP、LLDP、PAGP 或 UDLD 协议的 BPDU Tunnel 功能，否则系统将提示出错。

1. 二层以太网端口视图或端口组视图下的配置

表1-1 以太网端口视图或端口组视图下的配置

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能指定协议的BPDU Tunnel功能		**bpdu-tunnel dot1q** { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }	必选 缺省情况下，各协议的BPDU Tunnel功能均处于关闭状态

2. 二层聚合接口视图下的配置

表1-2 二层聚合接口视图下的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	-
使能指定协议的BPDU Tunnel功能	**bpdu-tunnel dot1q** { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** }	必选 缺省情况下，各协议的BPDU Tunnel功能均处于关闭状态

1.2.3 配置BPDU Tunnel报文组播目的MAC

BPDU Tunnel 报文缺省采用的组播目的 MAC 地址为 0x010F-E200-0003，用户可以根据需要将其修改为 0x0100-0CCD-CDD0、0x0100-0CCD-CDD1 或 0x0100-0CCD-CDD2。

表1-3 配置 BPDU Tunnel 报文组播目的 MAC

操作	命令	说明
进入系统视图	**system-view**	-
配置BPDU Tunnel报文的组播目的MAC地址	**bpdu-tunnel tunnel-dmac** *mac-address*	可选 缺省情况下，BPDU Tunnel报文的组播目的MAC地址为0x010F-E200-0003

说明

在运营商网络边缘设备上所配置的 BPDU Tunnel 报文的组播目的 MAC 地址必须一致，否则设备将无法正确识别 BPDU Tunnel 报文。

1.3 BPDU Tunnel典型配置举例

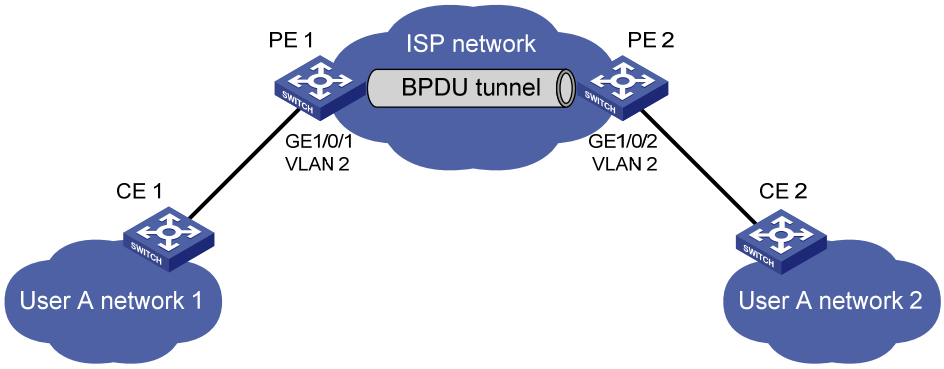
1.3.1 STP协议BPDU Tunnel配置举例

1. 组网需求

- CE 1 和 CE 2 为用户 A 的处于不同地域网络的边缘设备，PE 1 和 PE 2 为运营商网络的边缘设备。
- PE 与 CE 间相连的端口均为属于 VLAN 2 的 Access 端口；而运营商网络中各设备间相连的端口均为 Trunk 类型，并允许所有 VLAN 的报文通过。
- 用户 A 的网络中已启用 MSTP 功能，要求通过配置使 CE 1 和 CE 2 可以跨越运营商网络进行统一的生成树计算，其中 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

2. 组网图

图1-3 STP 协议 BPDU Tunnel 配置组网图



3. 配置步骤

(1) 配置 PE 1

配置 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<PE1> system-view
[PE1] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/1 端口使用 VLAN 2 对用户报文进行传输。

```
[PE1] vlan 2
[PE1-vlan2] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port access vlan 2
```

在端口 GigabitEthernet1/0/1 上关闭 STP 协议，并使能 STP 协议的 BPDU Tunnel 功能。

```
[PE1-GigabitEthernet1/0/1] undo stp enable
[PE1-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

(2) 配置 PE 2

配置 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<PE2> system-view
[PE2] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/2 端口使用 VLAN 2 对用户报文进行传输。

```
[PE2] vlan 2
[PE2-vlan2] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port access vlan 2
```

在端口 GigabitEthernet1/0/2 上关闭 STP 协议，并使能 STP 协议的 BPDU Tunnel 功能。

```
[PE2-GigabitEthernet1/0/2] undo stp enable
```

```
[PE2-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
```

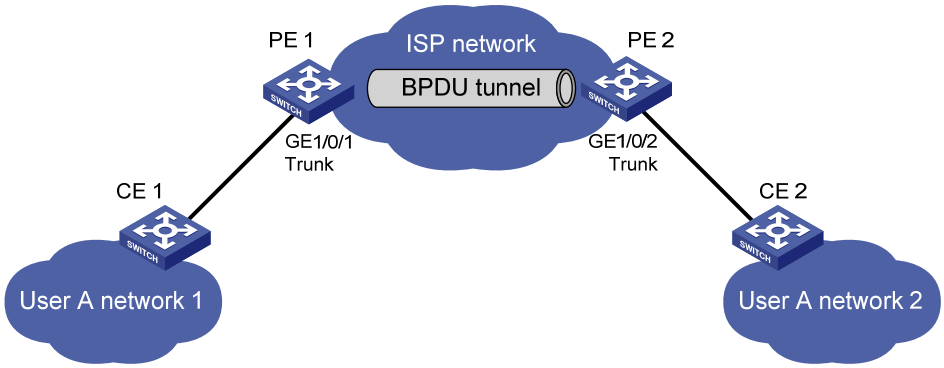
1.3.2 PVST协议BPDU Tunnel配置举例

1. 组网需求

- CE 1 和 CE 2 为用户 A 的处于不同地域网络的边缘设备，PE 1 和 PE 2 为运营商网络的边缘设备。
- PE 与 CE 间相连的端口以及运营商网络中各设备间相连的端口均为 Trunk 类型，并允许所有 VLAN 的报文通过。
- 用户 A 网络的 VLAN 1～4094 内已启用 PVST 功能，要求通过配置使 CE 1 和 CE 2 可以跨越运营商网络进行统一的 PVST 计算，其中 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

2. 组网图

图1-4 PVST 协议 BPDU Tunnel 配置组网图



3. 配置步骤

(1) 配置 PE 1

配置 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<PE1> system-view
[PE1] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/1 端口为 Trunk 端口，并允许所有 VLAN 通过。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上关闭 STP 协议，并分别使能 STP 协议和 PVST 协议的 BPDU Tunnel 功能。

```
[PE1-GigabitEthernet1/0/1] undo stp enable
[PE1-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
[PE1-GigabitEthernet1/0/1] bpdu-tunnel dot1q pvst
```

(2) 配置 PE 2

配置 BPDU Tunnel 报文的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<PE2> system-view
[PE2] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/2 端口为 Trunk 端口，并允许所有 VLAN 通过。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/2 上关闭 STP 协议，并分别使能 STP 协议和 PVST 协议的 BPDU Tunnel 功能。

```
[PE2-GigabitEthernet1/0/2] undo stp enable
[PE2-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
[PE2-GigabitEthernet1/0/2] bpdu-tunnel dot1q pvst
```

目 录

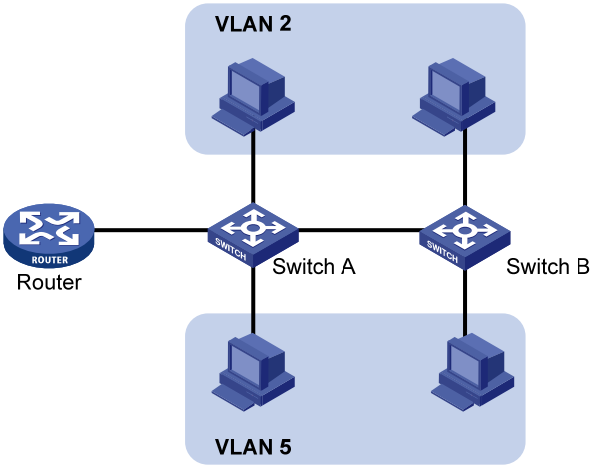
1 VLAN配置

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，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现LAN互联虽然可以解决冲突（Collision）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LAN划分成多个虚拟的LAN——VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文被限制在一个VLAN内，如 图 1-1 所示。

图1-1 VLAN 示意图



VLAN 的划分不受物理位置的限制：不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户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 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 内的用户不能和其它 VLAN 内的用户直接通信，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。用 VLAN 可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

1.1.2 VLAN原理

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。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。

IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案，对带有 VLAN 标识的报文结构进行了统一规定。

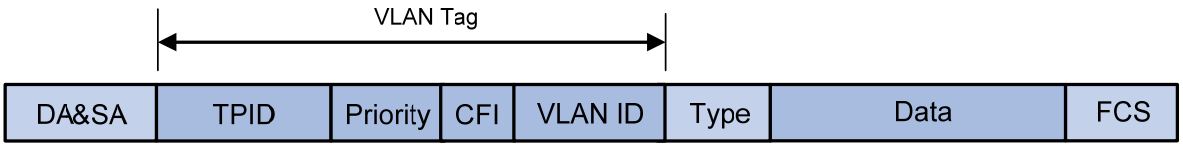
传统的以太网数据帧在目的MAC地址和源MAC地址之后封装的是上层协议的类型字段，如 图 1-2 所示。

图1-2 传统以太网帧封装格式

其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。

IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

图1-3 VLAN Tag 的组成字段



如 图 1-3 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 用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。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 表示报文的 802.1P 优先级，长度为 3bit。
- CFI 字段标识 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 1bit，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，缺省取值为 0。
- VLAN ID 标识该报文所属 VLAN 的编号，长度为 12bit，取值范围为 0～4095。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

- 这里的帧格式以 Ethernet II 型封装为例，以太网还支持 802.2 LLC、802.2 SNAP 和 802.3 raw 封装格式。对于这些封装格式的报文，也会添加 VLAN Tag 字段，用来区分不同 VLAN 的报文。
- 对于多 VLAN Tag 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 VLAN划分

VLAN 根据划分方式不同可以分为不同类型，下面列出了几种最常见的 VLAN 类型：

- 基于端口的 VLAN
- 基于 MAC 地址的 VLAN
- 基于协议的 VLAN
- 基于 IP 子网的 VLAN

- 基于策略的 VLAN
- 其它 VLAN

本章将分别介绍基于端口的 VLAN、基于 MAC 地址的 VLAN、基于协议的 VLAN 和基于 IP 子网的 VLAN。如果某个接口下同时使能以上四种 VLAN，则缺省情况下 VLAN 的匹配将按照 MAC VLAN、IP 子网 VLAN、协议 VLAN、端口 VLAN 的先后顺序进行。

1.1.4 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**	-
创建一个VLAN并进入VLAN视图，或批量创建VLAN	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	可选 缺省情况下，系统只有一个缺省VLAN（VLAN 1）
进入VLAN视图	**vlan** *vlan-id*	必选 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*	可选 缺省情况下，VLAN的名称为该VLAN的VLAN ID，如“VLAN 0001”
配置当前VLAN的描述信息	**description** *text*	可选 缺省情况下，VLAN的描述字符串为该VLAN的VLAN ID，如“VLAN 0001”

说明

- VLAN 1 为系统缺省 VLAN，用户不能手工创建和删除。
- 保留 VLAN 是系统为实现特定功能预留的 VLAN，用户也不能手工创建和删除。
- 协议保留的 VLAN、Voice VLAN、管理 VLAN、动态学习到的 VLAN、配置有 QoS 策略的 VLAN、Smart Link 的控制 VLAN、RRPP 的控制 VLAN、远程镜像 VLAN 等，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

1.3.1 VLAN接口简介

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。

1.3.2 配置VLAN接口基本属性

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**	-
创建VLAN接口并进入VLAN接口视图	**interface vlan-interface** *vlan-interface-id*	必选 • 空配置启动时，使用软件功能缺省值，设备上没有任何 VLAN 接口 • 缺省配置启动时，使用软件功能出厂值，设备上已创建 VLAN1 接口 关于空配置启动和缺省配置启动，请参见“基础配置指导”中的“配置文件管理” 如果该VLAN接口已经存在，则直接进入该VLAN接口视图
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	可选 • 空配置启动时，使用软件功能缺省值，没有配置 VLAN 接口的 IP 地址 • 缺省配置启动时，使用软件功能出厂值，VLAN1 接口使用 DHCP 方式自动获取 IP 地址
配置当前VLAN接口的描述信息	**description** *text*	可选 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*	可选 缺省情况下，VLAN接口的MTU值为1500字节
恢复VLAN接口的缺省配置	**default**	可选
打开VLAN接口	**undo shutdown**	可选 缺省情况下，未手工关闭VLAN接口。此时VLAN接口状态受VLAN中端口状态的影响，即：当VLAN中所有以太网端口状态均为down时，VLAN接口为down状态，即关闭状态；当VLAN中有一个或一个以上的以太网端口处于up状态时，则VLAN接口处于up状态。 如果将VLAN接口的状态通过**shutdown**命令设置为DOWN(Administratively)，则VLAN接口的状态始终为DOWN(Administratively)，不受VLAN中端口状态的影响


说明

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。

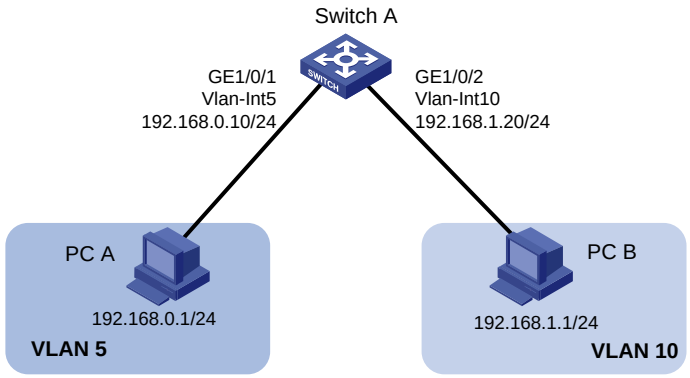
1.3.3 VLAN接口配置举例

1. 组网需求

如 图 1-4 所示，PC A、PC B与Switch A组网。其中PC A、PC B分别属于VLAN 5、VLAN 10，且处于不同网段，不能直接通信。通过在Switch A上创建并配置VLAN接口，实现不同网段的PC A与PC B跨VLAN三层互通。

2. 组网图

图1-4 通过 VLAN 接口实现 VLAN 间互通



3. 配置步骤

(1) 配置 Switch A

创建 VLAN 5，并向 VLAN 5 中添加端口 GigabitEthernet1/0/1。

```
<SwitchA> system-view
[SwitchA] vlan 5
[SwitchA-vlan5] port GigabitEthernet 1/0/1
```

创建 VLAN 10，并向 VLAN 10 中添加端口 GigabitEthernet1/0/2。

```
[SwitchA-vlan5] vlan 10
[SwitchA-vlan10] port GigabitEthernet 1/0/2
[SwitchA-vlan10] quit
```

创建 Vlan-interface5，并配置其 IP 地址为 192.168.0.10/24。

```
[SwitchA] interface vlan-interface 5
[SwitchA-Vlan-interface5] ip address 192.168.0.10 24
[SwitchA-Vlan-interface5] quit
```

创建 Vlan-interface10，并配置其 IP 地址为 192.168.1.20/24。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 192.168.1.20 24
[SwitchA-Vlan-interface10] return
```

(2) 配置 PC A

将其默认网关配为 192.168.0.10。

(3) 配置 PC B

将其默认网关配为 192.168.1.20。

4. 显示与验证

(1) PC A 与 PC B 可以相互 ping 通。

(2) 通过查看显示信息验证配置是否成功。

查看 Switch A 上三层接口的 IP 基本配置信息，验证以上配置是否生效。

```
<SwitchA> display ip interface brief
```

```
*down: administratively down
(s): spoofing
Interface                  Physical Protocol IP Address      Description
Vlan-interface5            up       up       192.168.0.10    Vlan-inte...
Vlan-interface10           up       up       192.168.1.20    Vlan-inte...
```

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，端口就可以转发指定 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 连接：端口发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的终端设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk 连接：端口发出去的报文，端口缺省 VLAN 内的报文不带 Tag，其它 VLAN 内的报文都必须带 Tag。通常用于网络传输设备之间的互连。
- Hybrid 连接：端口发出去的报文可根据需要设置某些 VLAN 内的报文带 Tag，某些 VLAN 内的报文不带 Tag。Hybrid 类型端口既可以用于网络传输设备之间的互连，又可以直接连接终端设备。

2. 端口缺省VLAN

除了可以设置端口允许通过的 VLAN，还可以设置端口的缺省 VLAN，即 PVID（Port VLAN ID，端口 VLAN ID）。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

- 当Voice VLAN工作模式为自动模式时，不能将缺省VLAN设置为Voice VLAN。有关Voice VLAN的相关内容，请参见“4 Voice VLAN配置”。
- 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。

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	为报文添加缺省VLAN的Tag	• 当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文 • 当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文	去掉Tag，发送该报文
Trunk端口	• 当缺省 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文，给报文添加缺省 VLAN 的 Tag • 当缺省 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文 • 当 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当 VLAN ID 与缺省 VLAN ID 相同，且是该端口允许通过的 VLAN ID 时：去掉 Tag，发送该报文 • 当 VLAN ID 与缺省 VLAN ID 不同，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			当报文中携带的VLAN ID是该端口允许通过的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，另一种是在二层以太网端口视图/端口组视图/二层聚合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*	必选 如果指定的VLAN不存在，则该命令先完成VLAN的创建，然后再进入该VLAN的视图
向当前VLAN中添加一个或一组Access端口	**port** *interface-list*	必选 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（在二层以太网端口视图/端口组视图/二层聚合接口视图）

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	四者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效 • 二层聚合接口视图下的配置对当前二层聚合接口及其所有成员端口都生效，若配置二层聚合接口时失败，则不再配置其成员端口，若配置某成员端口时失败，系统会自动跳过该成员端口继续配置其它成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型为Access类型		**port link-type access**	可选 缺省情况下，端口的链路类型为Access类型
将当前Access端口加入到指定VLAN		**port access vlan** *vlan-id*	可选 缺省情况下，所有Access端口均属于且只属于VLAN 1

说明

- 在将 Access 端口加入到指定 VLAN 之前，要加入的 VLAN 必须已经存在。
- 在 VLAN 视图下向 VLAN 中添加端口时，只能添加二层以太网端口。

1.4.3 配置基于Trunk端口的VLAN

Trunk 端口可以允许多个 VLAN 通过，只能在二层以太网端口视图/端口组视图/二层聚合接口视图下进行配置。

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**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	四者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效 • 二层聚合接口视图下的配置对当前二层聚合接口及其所有成员端口都生效，若配置二层聚合接口时失败，则不再配置其成员端口，若配置某成员端口时失败，系统会自动跳过该成员端口继续配置其它成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型为Trunk类型		**port link-type trunk**	必选 缺省情况下，所有端口的链路类型均为Access类型

操作	命令	说明
允许指定的VLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	必选 缺省情况下，Trunk端口只允许VLAN 1的报文通过
设置Trunk端口的缺省VLAN	**port trunk pvid vlan** *vlan-id*	可选 缺省情况下，Trunk端口的缺省VLAN为VLAN 1

- Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其它类型端口。例如：Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 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。

1.4.4 配置基于Hybrid端口的VLAN

Hybrid 端口可以允许多个 VLAN 通过，只能在二层以太网端口视图/端口组视图/二层聚合接口视图下进行配置。

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**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	四者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效 • 二层聚合接口视图下的配置对当前二层聚合接口及其所有成员端口都生效，若配置二层聚合接口时失败，则不再配置其成员端口，若配置某成员端口时失败，系统会自动跳过该成员端口继续配置其它成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
允许指定的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	必选 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）
设置Hybrid端口的缺省VLAN		**port hybrid pvid vlan** *vlan-id*	可选 缺省情况下，Hybrid端口的缺省VLAN为VLAN 1

说明

- Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其它类型端口。例如：Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 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。

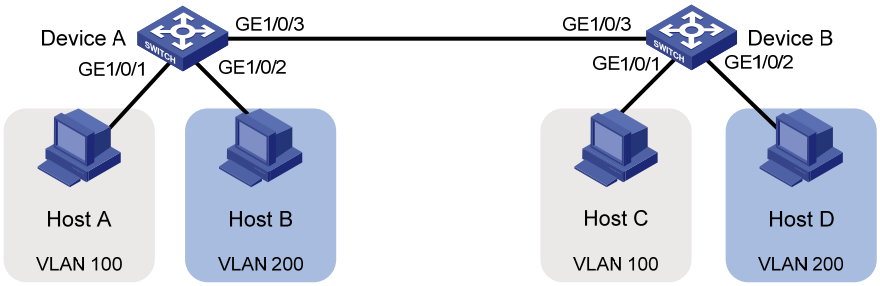
1.4.5 基于端口的VLAN典型配置举例

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1-5 基于端口的 VLAN 组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 100，并将 GigabitEthernet1/0/1 加入 VLAN 100。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

创建 VLAN 200，并将 GigabitEthernet1/0/2 加入 VLAN 200。

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

为了使 Device A 上 VLAN 100 和 VLAN 200 的报文能发送给 Device B，将 GigabitEthernet1/0/3 的链路类型配置为 Trunk，并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
Please wait... Done.
```

(2) Device B 上的配置与 Device A 上的配置完全一样，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. 显示与验证

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

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
 VLAN ID: 100
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0100
 Name: VLAN 0100
Tagged   Ports:
    GigabitEthernet1/0/3
 Untagged Ports:
    GigabitEthernet1/0/1
[DeviceA-GigabitEthernet1/0/3] display vlan 200
 VLAN ID: 200
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0200
 Name: VLAN 0200
Tagged   Ports:
    GigabitEthernet1/0/3
 Untagged Ports:
    GigabitEthernet1/0/2
```

1.5 配置基于MAC的VLAN

1.5.1 基于MAC的VLAN简介

基于 MAC 划分 VLAN 是 VLAN 的另一种划分方法。它按照报文的源 MAC 地址来定义 VLAN 成员，将指定报文加入该 VLAN 的 Tag 后发送。该功能通常会和安全（比如 802.1X）技术联合使用，以实现终端的安全、灵活接入。

1. 手动配置静态MAC VLAN

手动配置静态 MAC VLAN 常用于 VLAN 中用户相对较少的网络环境。在该方式下，用户需要手动配置 MAC VLAN 表项，使能基于 MAC 地址的 VLAN 功能，并将端口加入 MAC VLAN。其原理为：

- 当端口收到的报文为 Untagged 报文时，根据报文的源 MAC 匹配 MAC VLAN 表项。首先进行模糊匹配，即查询表中 MASK 不是全 F 的表项，将源 MAC 和 MASK 相与后与 MAC VLAN 表项中的 MAC 地址匹配，如果完全相同，则模糊匹配成功，给报文添加表项中指定的 VLAN ID 并转发该报文；如果模糊匹配失败，则进行精确匹配，即查询表中 MASK 为全 F 的表项，如果报文中的源 MAC 与 MAC VLAN 表项中的 MAC 地址完全相同，则精确匹配成功，给报文添加表项中指定的 VLAN ID 并转发该报文；如果没有找到匹配 MAC VLAN 表项，则继续按照其它原则（如 IP 子网、协议等）进行匹配，如果匹配成功，则转发报文，如果匹配均失败，则给报文添加端口的缺省 VLAN ID 并转发该报文。

- 当端口收到的报文为 Tagged 报文时，如果报文的 VLAN ID 在该端口允许通过的 VLAN ID 列表里，则转发该报文；如果报文的 VLAN ID 不在端口允许通过的 VLAN ID 列表里，则丢弃该报文。

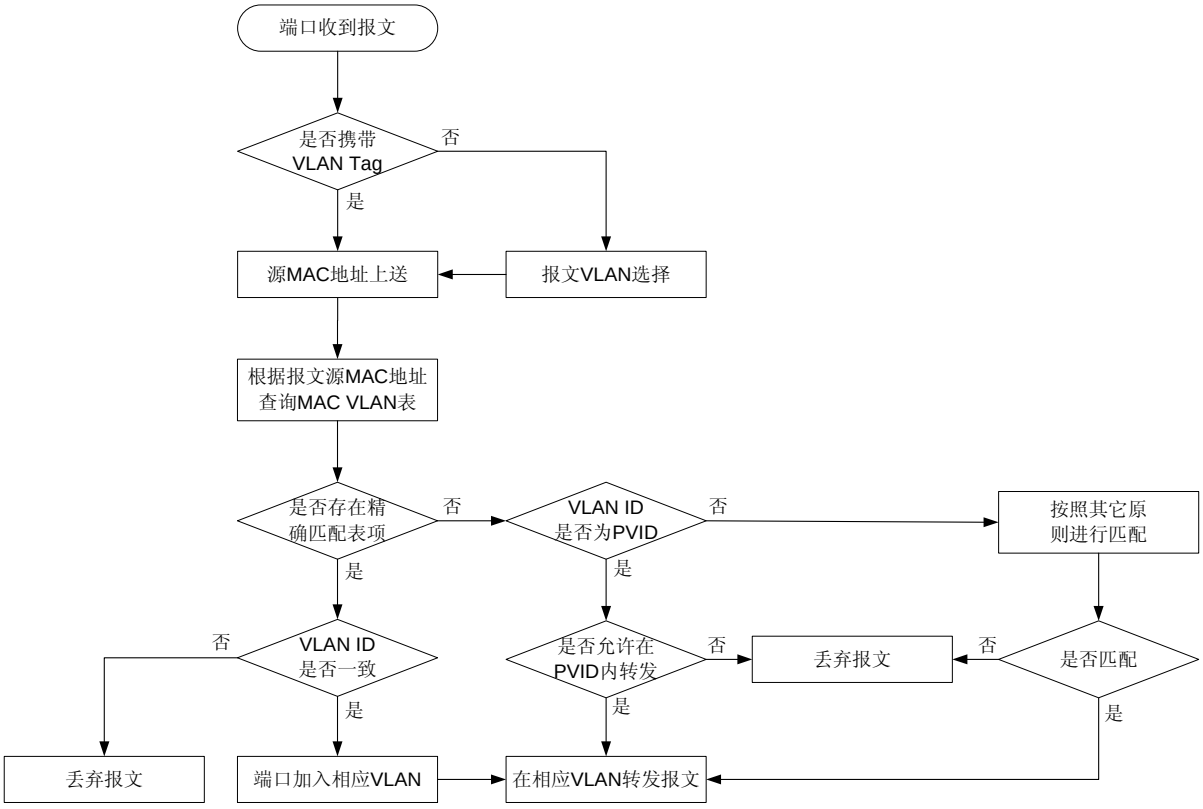
2. 动态触发端口加入静态MAC VLAN

手动配置静态 MAC VLAN 时，用户需要把端口分别加入相应的 MAC VLAN，当用户不能确定从哪些端口收到指定 VLAN 的报文时，就不能把相应端口加入到 MAC VLAN，在这种情况下，手动配置静态 MAC VLAN 无法满足用户的需求。此时可以动态触发端口加入静态 MAC VLAN。在该方式下，用户在配置 MAC VLAN 表项后，需要在端口上使能基于 MAC 的 VLAN 功能和 MAC VLAN 动态触发功能。其原理为：

端口在收到报文时，首先判断报文是否携带 VLAN Tag，若带 Tag，则直接上送报文源 MAC 地址；若不带 Tag，则先进行报文 VLAN 选择（按照基于 MAC 的 VLAN->基于 IP 子网的 VLAN->基于协议的 VLAN->基于端口的 VLAN 的优先次序为该 Untagged 报文添加对应的 Tag，并获取该 Tag），再上送报文的源 MAC 地址。然后根据报文的源 MAC 查询 MAC VLAN 表项：

- 如果报文源 MAC 地址与 MAC VLAN 表项中的 MAC 地址精确匹配，检查报文的 VLAN ID 是否与对应表项中的 VLAN ID 一致，若一致，通过此报文动态触发端口加入相应 VLAN，同时转发报文，否则丢弃该报文。
- 如果报文源MAC地址与MAC VLAN表项的MAC地址不精确匹配，当报文VLAN ID为端口PVID，判断端口是否允许报文在PVID内转发，若允许，则在PVID中转发该报文，否则丢弃该报文。当报文VLAN ID不为端口PVID，报文继续按照其它原则（如IP子网、协议等）进行匹配，若匹配成功，则转发该报文；若匹配均失败，则丢弃该报文。处理流程如 图 1-6 所示：

图1-6 动态触发端口加入静态 MAC VLAN 的处理



说明

- 在端口加入 MAC VLAN 表项中相应的 VLAN 时，若端口未配置允许该 VLAN 通过，则端口自动以 Untagged 方式加入该 VLAN。
- 如果用户在同一端口上同时使能了手动配置 MAC VLAN 和动态触发端口加入 MAC VLAN，此时该端口选择使用后者的功能。
- 当端口收到的报文与 MAC VLAN 表项匹配，对该报文进行转发时，根据 MAC VLAN 的优先级（MAC 地址对应 VLAN 的 802.1p 优先级）高低来决定报文的转发策略。

3. 动态MAC VLAN

动态 MAC VLAN 需要和接入认证（比如基于 MAC 地址的 802.1X 认证）配合使用，以实现终端的安全、灵活接入。用户在设备上配置动态 MAC VLAN 功能以后，还需要在接入认证服务器上配置用户名和 VLAN 的绑定关系。

如果用户发起认证请求，接入认证服务器先对用户名和密码进行验证，如果验证通过，服务器下发VLAN信息。此时设备根据请求报文的源MAC地址和下发的VLAN信息生成MAC VLAN表项，并将 MAC VLAN 添加到端口允许通过的 VLAN 列表中。用户下线后，设备自动删除 MAC VLAN 表项，并将 MAC VLAN 从端口允许通过的 VLAN 列表中删除。

说明

接入认证的相关内容请参见“安全配置指导”中的“802.1X”、“MAC 地址认证”和“Portal”。

1.5.2 配置基于MAC的VLAN

说明

- 基于 MAC 的 VLAN 功能只能在 Hybrid 端口配置。
- Super VLAN 不能作为 MAC VLAN 表项中的 VLAN。
- 基于 MAC 的 VLAN 动态触发使能后，报文会上送 CPU 处理。由于该处理的优先级最高，会导致 MAC 地址最大学习数和 MAC 地址禁止学习功能不生效，因此不建议 MAC VLAN 动态触发功能和上述两个功能同时使用。
- 基于 MAC 的 VLAN 动态触发功能不和 802.1X 和 MAC 认证功能同时使用。
- 基于 MAC 的 VLAN 动态触发功能要求源 MAC 所匹配的 VLAN 必须是静态 VLAN 才能完成触发功能。
- 基于 MAC 的 VLAN 功能主要用于在用户的接入设备的下行端口上进行配置，因此不和聚合功能同时使用。
- 配置 MSTP 多实例情况下，如果端口在要加入的 VLAN 对应的 MSTP 实例中是阻塞状态，则端口会丢弃收到的报文，造成 MAC 地址不能上送，不能完成动态触发功能。基于 MAC 的动态 VLAN 的使用场景为接入侧，不建议和多实例 MSTP 同时使用。
- 配置 PVST 情况下，如果端口要加入的 VLAN 不为端口允许通过的 VLAN，则端口处于阻塞状态，会丢弃收到的报文，造成 MAC 地址不能上送，不能完成动态触发功能。基于 MAC 的动态 VLAN 的使用场景为接入侧，不建议和 PVST 同时使用。
- 配置 MAC-VLAN 表项时，如果指定了 MAC 地址对应 VLAN 的 802.1p 优先级，则用户还需要在相应端口视图下执行 **qos trust dot1p** 命令，使该端口信任报文的 802.1p 优先级，该配置才能生效。关于 **qos trust dot1p** 命令的详细介绍请参见“ACL 和 QoS 命令参考”中的“优先级映射配置命令”。

表1-8 手工配置静态 MAC VLAN

操作		命令	说明
进入系统视图		**system-view**	-
配置MAC地址与VLAN关联		**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *priority*]	必选
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
允许基于MAC的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	必选 缺省情况下，所有Hybrid端口只允许VLAN 1通过
使能基于MAC地址划分VLAN的功能		**mac-vlan enable**	必选 缺省情况下，未使能基于MAC地址划分VLAN的功能

操作	命令	说明
配置VLAN匹配优先级	**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	可选 缺省情况下，优先根据单个MAC地址来匹配VLAN

表1-9 动态触发端口加入静态 MAC VLAN

操作	命令	说明
进入系统视图	**system-view**	-
配置MAC地址与VLAN关联	**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**priority** *priority*]	必选 使能MAC VLAN的动态触发功能后，只有端口接收的报文的源MAC地址匹配了Mask为全F的MAC VLAN表项，才会动态触发该端口加入相应VLAN
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型为Hybrid类型	**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
使能基于MAC地址划分VLAN的功能	**mac-vlan enable**	必选 缺省情况下，未使能基于MAC地址划分VLAN的功能
使能MAC VLAN的动态触发功能	**mac-vlan trigger enable**	必选 缺省情况下，未使能MAC VLAN的动态触发功能。
配置VLAN匹配优先级	**vlan precedence mac-vlan**	可选 缺省情况下，优先根据单个MAC地址来匹配VLAN
配置PVID禁止功能	**port pvid disable**	可选 缺省情况下，对于没有匹配到MAC VLAN表项的未知源MAC会在PVID内进行转发通过

说明

使用 **mac-vlan trigger enable** 命令配置 MAC VLAN 的动态触发功能后，建议用户配置 **vlan precedence mac-vlan** 使报文优先根据单个 MAC 地址来匹配 VLAN，请不要配置 **vlan precedence ip-subnet-vlan** 命令使报文优先匹配 IP 子网-VLAN 表，该配置不能生效。

表1-10 配置动态 MAC VLAN

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
允许基于MAC的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	必选 缺省情况下，所有Hybrid端口只允许VLAN 1通过
使能基于MAC地址划分VLAN的功能		**mac-vlan enable**	必选 缺省情况下，未使能基于MAC地址划分VLAN的功能
配置认证功能	配置802.1X	请参见“安全命令参考”中的“802.1X”	三者至少选其一
	配置MAC地址认证	请参见“安全命令参考”中的“MAC地址认证”	
	配置Portal	请参见“安全命令参考”中的“Portal”	

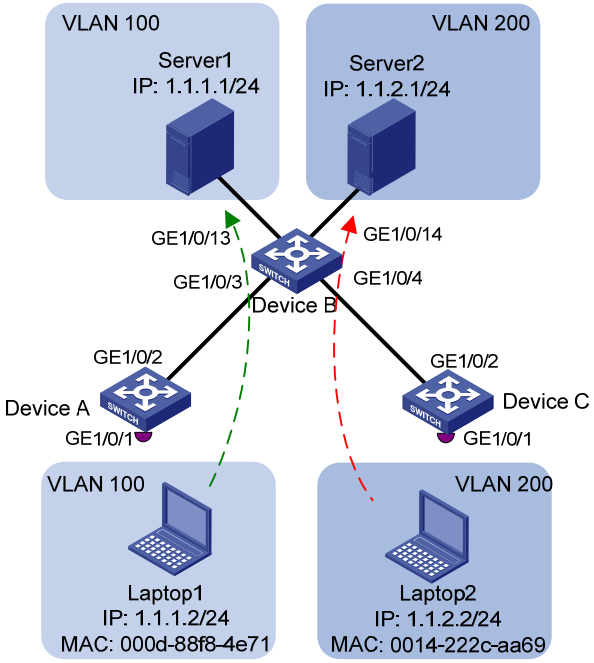
1.5.3 基于MAC的VLAN典型配置举例

1. 组网需求

- 如 图 1-7 所示，Device A和Device C的GigabitEthernet1/0/1 端口分别连接到两个会议室，Laptop1 和Laptop2 是会议用笔记本电脑，会在两个会议室间移动使用。
- Laptop1 和Laptop2 分别属于两个部门，两个部门间使用VLAN 100 和VLAN 200 进行隔离。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即Server1 和 Server2。
- Laptop1 和 Laptop2 的 MAC 地址分别为 000d-88F8-4E71 和 0014-222C-AA69。

2. 组网图

图1-7 基于 MAC 的 VLAN 组网图



3. 配置思路

- 创建 VLAN 100、VLAN 200。
- 配置 Device A 和 Device C 的上行端口为 Trunk 端口，并允许 VLAN 100 和 VLAN 200 的报文通过。
- 配置 Device B 的下行端口为 Trunk 端口，并允许 VLAN 100 和 VLAN 200 的报文通过；上行端口分别加入 VLAN 100、VLAN 200。
- Laptop1 和 Laptop2 的 MAC 地址分别与 VLAN 100、VLAN 200 关联。

4. 配置步骤

(1) Device A 的配置

创建 VLAN 100 和 VLAN 200。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 200
[DeviceA-vlan200] quit
```

将 Laptop1 的 MAC 地址与 VLAN 100 关联，Laptop2 的 MAC 地址与 VLAN 200 关联。

```
[DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200
```

配置终端的接入端口：Laptop1 和 Laptop2 均可能从 GigabitEthernet1/0/1 接入，将 GigabitEthernet1/0/1 的端口类型配置为 Hybrid，并使其在发送 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag；开启 GigabitEthernet1/0/1 端口的 MAC-VLAN 功能。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] mac-vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

为了终端能够访问 Server1 和 Server2，需要将上行端口 GigabitEthernet1/0/2 的端口类型配置为 Trunk，并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) Device B 的配置

创建 VLAN 100 和 VLAN 200，并将 GigabitEthernet1/0/13 加入 VLAN 100，GigabitEthernet 1/0/14 加入 VLAN 200。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/13
[DeviceB-vlan100] quit
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/14
[DeviceB-vlan200] quit
```

配置 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 端口为 Trunk 端口，均允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/4] quit
```

(3) Device C 的配置

Device C 的配置与 Device A 完全一致，这里不再赘述。

5. 显示与验证

(1) Laptop1 只能访问 Server1，不能访问 Server2；Laptop2 只能访问 Server2，不能访问 Server1。

(2) 在 Device A 和 Device C 上可以查看到 Laptop1 和 VLAN 100、Laptop2 和 VLAN 200 的静态 MAC VLAN 地址表项已经生成。

```
[DeviceA] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC ADDR         MASK             VLAN ID   PRIO   STATE
  ------------------------------------------------------------
  000d-88f8-4e71   ffff-ffff-ffff   100       0      S
  0014-222c-aa69   ffff-ffff-ffff   200       0      S

  Total MAC VLAN address count:2
```

6. 配置注意事项

- 基于 MAC 的 VLAN 只能在 Hybrid 端口上配置。
- 基于 MAC 的 VLAN 的配置主要用于在用户的接入设备的下行端口上进行配置，因此不能与聚合功能同时使用。

1.6 配置基于协议的VLAN

1.6.1 基于协议的VLAN简介

说明

基于协议的 VLAN 只对 Hybrid 端口配置才有效。

基于协议的 VLAN 是根据端口接收到的报文所属的协议（族）类型以及封装格式来给报文分配不同的 VLAN ID。可用来划分 VLAN 的协议有 IP、IPX、AT（AppleTalk，Apple 计算机网络协议），封装格式有 Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP 等。

“协议类型 + 封装格式”又称为协议模板，一个协议 VLAN 下可以绑定多个协议模板，不同的协议模板再用协议索引（*protocol-index*）来区分。因此，一个协议模板可以用“协议 *vlan-id* + *protocol-index*”来唯一标识。然后通过命令行将“协议 *vlan-id* + *protocol-index*”和端口绑定。这样，对于从端口接收到 Untagged 报文（没有携带 VLAN 标记的报文）会做如下处理：

- 如果该报文携带的协议类型和封装格式与“协议 *vlan-id* + *protocol-index*”标识的协议模板相匹配，则为其打上协议 *vlan-id*。
- 如果该报文携带的协议类型和封装格式与“协议 *vlan-id* + *protocol-index*”标识的协议模板不匹配，则为其打上端口的缺省 VLAN ID。

对于端口接收到的 Tagged 报文（携带 VLAN 标记的报文），处理方式和基于端口的 VLAN 一样：如果端口允许携带该 VLAN 标记的报文通过，则正常转发；如果不允许，则丢弃该报文。

此特性主要应用于将网络中提供的服务类型与 VLAN 相绑定，方便管理和维护。

1.6.2 配置基于协议的VLAN

表1-11 配置基于协议的 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	必选 如果指定的VLAN不存在，则该命令先完成VLAN的创建，然后再进入该VLAN的视图
配置基于协议的VLAN，并指定协议模板	**protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }	必选 缺省情况下，没有配置任何协议模板
退出VLAN视图	**quit**	-

操作		命令	说明
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	四者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效 • 二层聚合接口视图下的配置对当前二层聚合接口及其所有成员端口都生效，若配置二层聚合接口时失败，则不再配置其成员端口，若配置某成员端口时失败，系统会自动跳过该成员端口继续配置其它成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
允许基于协议的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	必选 缺省情况下，所有Hybrid端口只允许VLAN 1通过
配置Hybrid端口与基于协议的VLAN关联		**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	必选

注意

- 在使用 **protocol-vlan mode llc** 命令配置自定义协议模板时，命令中的 *dsap-id* 和 *ssap-id* 不能同时设置成 0xe0，同时设置为 0xe0 对应的是 ipx llc 协议模板；*dsap-id* 和 *ssap-id* 也不能同时设置成 0xff，同时设置为 0xff 对应的是 ipx raw 协议模板。
- 在使用 **mode** 参数配置协议 VLAN 时，如果将 ethernetii 型报文的 etype 参数值配置为 0x0800、0x8137、0x809b、0x86dd，则分别与 ipv4、ipx、appletalk 和 ipv6 协议模板相同，因此不允许配置 ethernetii 报文的 etype 参数为这四个数值。
- 协议VLAN特性要求Hybrid入端口的报文格式为Untagged的，而自动模式下的Voice VLAN只支持Hybrid端口对Tagged的语音流进行处理（详情请参见“4 Voice VLAN配置”），因此，不能将某个VLAN同时设置为协议VLAN和Voice VLAN。

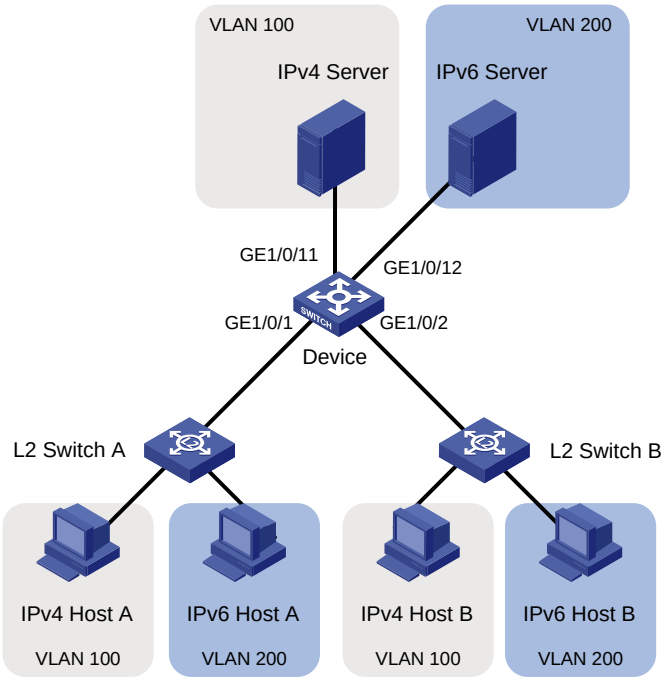
1.6.3 基于协议的VLAN典型配置举例

1. 组网需求

实验室网络中大部分主机运行 IPv4 网络协议，另外为了教学需要还布置了 IPv6 实验局，因此，同时有些主机运行着 IPv6 网络协议。为了避免互相干扰，现要求基于网络协议将 IPv4 流量和 IPv6 流量二层互相隔离。

2. 组网图

图1-8 基于协议的 VLAN 组网图



3. 配置思路

创建 VLAN 100 及 VLAN 200。让 VLAN 100 与 IPv4 协议绑定，VLAN 200 与 IPv6 协议绑定，通过协议 VLAN 来实现 IPv4 流量和 IPv6 流量二层互相隔离。

4. 配置步骤

(1) 配置 Device

创建 VLAN 100，将端口 GigabitEthernet1/0/11 加入 VLAN 100。

```
<Device> system-view
[Device] vlan 100
[Device-vlan100] description protocol VLAN for IPv4
[Device-vlan100] port gigabitethernet 1/0/11
[Device-vlan100] quit
```

创建 VLAN 200，将端口 GigabitEthernet1/0/12 加入 VLAN 200。

```
[Device] vlan 200
[Device-vlan200] description protocol VLAN for IPv6
[Device-vlan200] port gigabitethernet 1/0/12
```

在 VLAN 200 和 VLAN 100 视图下，分别为 IPv4 和 IPv6 协议创建协议模板。

```
[Device-vlan200] protocol-vlan 1 ipv6
[Device-vlan200] quit
[Device] vlan 100
[Device-vlan100] protocol-vlan 1 ipv4
[Device-vlan100] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并在转发 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type hybrid
[Device-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
 Please wait... Done.
```

配置端口 GigabitEthernet1/0/1 与 VLAN 100 的协议模板 1（即 IPv4 协议模板）、VLAN 200 的协议模板 1（即 IPv6 协议模板）进行绑定。

```
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet1/0/2 为 Hybrid 端口，在转发 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag，与 VLAN 100 的协议模板 1（即 IPv4 协议模板）、VLAN 200 的协议模板 1（即 IPv6 协议模板）进行绑定。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-type hybrid
[Device-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
 Please wait... Done.
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
```

(2) L2 Switch A 和 L2 Switch B 采用缺省配置。

(3) 将 IPv4 Host A、IPv4 Host B 和 IPv4 Server 配置在一个网段，比如 192.168.100.0/24；将 IPv6 Host A、IPv6 Host B 和 IPv6 Server 配置在一个网段，比如 2001::1/64。

5. 显示与验证

(1) VLAN 100 内的主机和服务器能够互相 ping 通；VLAN 200 内的主机和服务器能够互相 ping 通。但 VLAN 100 内的主机/服务器和 VLAN 200 内的主机/服务器会 ping 失败。

(2) 通过查看 Device 上的显示信息，验证配置是否生效。

查看 Device 上协议 VLAN 的配置。

```
[Device-GigabitEthernet1/0/2] display protocol-vlan vlan all
 VLAN ID:100
    Protocol Index      Protocol Type
 ============================================================
          1              ipv4
 VLAN ID:200
    Protocol Index      Protocol Type
 ============================================================
          1              ipv6
```

查看 Device 端口上已配置的协议 VLAN 的相关信息。

```
[Device-GigabitEthernet1/0/2] display protocol-vlan interface all
 Interface: GigabitEthernet 1/0/1
   VLAN ID   Protocol Index      Protocol Type
 ============================================================
     100          1               ipv4
     200          1               ipv6
 Interface: GigabitEthernet 1/0/2
   VLAN ID   Protocol Index      Protocol Type
 ============================================================
     100          1               ipv4
     200          1               ipv6
```

6. 配置注意事项

基于协议的 VLAN 只对 Hybrid 端口配置才有效。

1.7 配置基于IP子网的VLAN

1.7.1 基于IP子网的VLAN简介

基于 IP 子网的 VLAN 是根据报文源 IP 地址及子网掩码来进行划分的。设备从端口接收到 Untagged 报文后，会根据报文的源地址来确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。

此特性主要用于将指定网段或 IP 地址发出的报文在指定的 VLAN 中传送。

1.7.2 配置基于IP子网的VLAN

说明

基于 IP 子网的 VLAN 只对 Hybrid 端口配置有效。

表1-12 配置基于 IP 子网的 VLAN

操作		命令	说明
进入系统视图		**system-view**	-
进入VLAN视图		**vlan** *vlan-id*	-
配置IP子网与当前VLAN关联		**ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]	必选 配置的IP网段或IP地址不能是组播网段或组播地址
退回系统视图		**quit**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	四者必选其一 • 二层以太网端口视图下的配置只对当前端口生效 • 端口组视图下的配置对当前端口组中的所有端口生效 • 二层聚合接口视图下的配置对当前二层聚合接口及其所有成员端口都生效，若配置二层聚合接口时失败，则不再配置其成员端口，若配置某成员端口时失败，系统会自动跳过该成员端口继续配置其它成员端口
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	必选 缺省情况下，所有端口的链路类型均为Access类型
允许基于IP子网的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	必选 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
配置Hybrid端口和基于IP子网的VLAN关联		**port hybrid ip-subnet-vlan vlan** *vlan-id*	必选 缺省情况下，Hybird端口和基于IP子网的VLAN没有任何关联关系

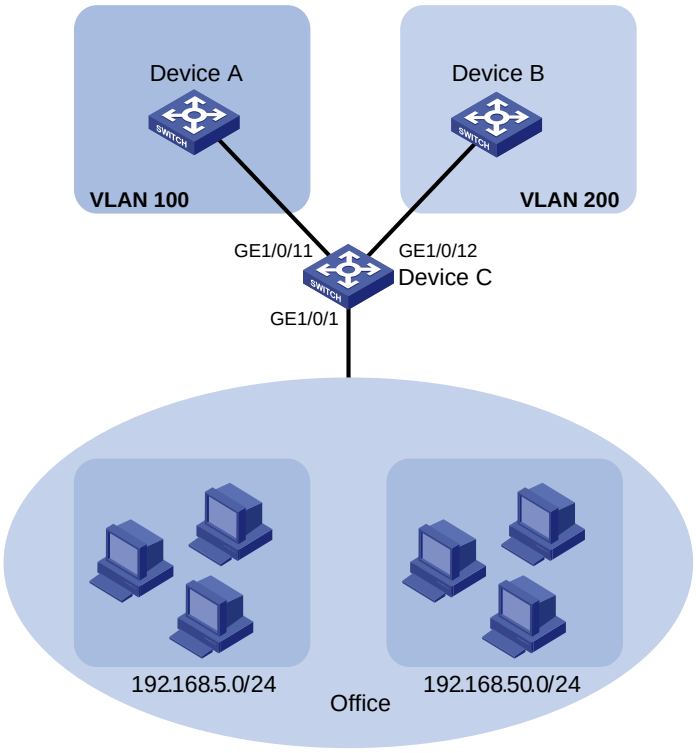
1.7.3 基于IP子网的VLAN典型配置举例

1. 组网需求

如 图 1-9 所示，办公区的主机属于不同的网段 192.168.5.0/24 和 192.168.50.0/24，Device C在收到来自办公区主机的报文时，根据报文的源IP地址，使来自不同网段主机的报文分别在指定的VLAN中传输。

2. 组网图

图1-9 基于 IP 子网的 VLAN 组网图



3. 配置思路

创建 VLAN100、VLAN200，配置子网与 VLAN 的关联关系，并配置端口与 VLAN 的关联关系。

4. 配置步骤

```
<DeviceC> system-view
```

配置子网 192.168.5.0/24 与 VLAN 100 关联。

```
[DeviceC] vlan 100
[DeviceC-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
[DeviceC-vlan100] quit
```

配置子网 192.168.50.0/24 与 VLAN 200 关联。

```
[DeviceC] vlan 200
[DeviceC-vlan200] ip-subnet-vlan ip 192.168.50.0 255.255.255.0
[DeviceC-vlan200] quit
```

配置端口 GigabitEthernet 1/0/11，使其允许通过 VLAN 100 的报文。

```
[DeviceC] interface gigabitethernet 1/0/11
[DeviceC-GigabitEthernet1/0/11] port link-type hybrid
[DeviceC-GigabitEthernet1/0/11] port hybrid vlan 100 tagged
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/11] quit
```

配置端口 GigabitEthernet 1/0/12，使其允许通过 VLAN 200 的报文。

```
[DeviceC] interface gigabitethernet 1/0/12
[DeviceC-GigabitEthernet1/0/12] port link-type hybrid
[DeviceC-GigabitEthernet1/0/12] port hybrid vlan 200 tagged
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/12] quit
```

配置端口 GigabitEthernet 1/0/1，使其和基于 IP 子网的 VLAN 100、VLAN 200 关联。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
[DeviceC-GigabitEthernet1/0/1] return
```

5. 显示与验证

查看所有 VLAN 的 IP 子网信息。

```
<Device C> display ip-subnet-vlan vlan all
VLAN ID:  100
 Subnet Index      IP Address      Subnet Mask
 ---------------------------------------------------
       0          192.168.5.0     255.255.255.0
VLAN ID:  200
 Subnet Index      IP Address      Subnet Mask
 ---------------------------------------------------
       0          192.168.50.0    255.255.255.0
```

查看端口 GigabitEthernet 1/0/1 上所配置的 IP 子网 VLAN 信息。

```
<DeviceC> display ip-subnet-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet-Index    IP ADDRESS        NET MASK
  ---------------------------------------------------
   100           0          192.168.5.0     255.255.255.0
   200           0         192.168.50.0     255.255.255.0
```

6. 配置注意事项

基于 IP 子网的 VLAN 只对 Hybrid 端口配置才有效。

1.8 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** 命令可以清除接口统计信息。

表1-13 VLAN 显示和维护

操作	命令
显示VLAN相关信息	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示VLAN接口相关信息（仅R5206及以上版本支持**description**参数）	**display interface** [**vlan-interface**] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface vlan-interface** *vlan-interface-id* [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备上当前存在的Hybrid或Trunk端口	**display port** { **hybrid** | **trunk** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示MAC-VLAN表项	**display mac-vlan { all | dynamic | mac-address** *mac-address* [**mask** *mac-mask*] **| static | vlan** *vlan-id* **}** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示所有使能了MAC VLAN功能的接口	**display mac-vlan interface** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定VLAN上配置的协议信息及协议的索引	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定端口上已配置的协议VLAN的相关信息	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定VLAN上配置的IP子网VLAN信息及IP子网的索引	**display ip-subnet-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定端口上配置的IP子网VLAN信息及IP子网的索引	**display ip-subnet-vlan interface {** *interface-type interface-number1* [**to** *interface-type interface-number2*] **| all }** [**| { begin | exclude | include }** *regular-expression*]
清除接口的统计信息	**reset counters interface vlan-interface** [*vlan-interface-id*]

2 Super VLAN配置

2.1 Super VLAN简介

随着网络的发展，网络地址资源日趋紧张，为了节省 IP 地址，Super VLAN 的概念被提出来。Super VLAN 又称为 VLAN 聚合（VLAN Aggregation），其原理是一个 Super VLAN 和多个 Sub VLAN 关联，Super VLAN 内不能加入物理端口，但可以创建对应的 VLAN 接口，VLAN 接口下可以配置 IP 地址；Sub VLAN 可以加入物理端口，但不能创建对应的 VLAN 接口，所有 Sub VLAN 内的端口共用 Super VLAN 的 VLAN 接口 IP 地址，不同 Sub VLAN 之间二层相互隔离。当 Sub VLAN 内的用户需要进行三层通信时，将使用 Super VLAN 的 IP 地址作为网关地址，这样多个 Sub VLAN 共享一个网关地址，从而节省了 IP 地址资源。

为了实现 Sub VLAN 之间的三层互通，在创建好 Super VLAN 和 VLAN 接口之后，用户需要开启设备的本地代理功能：

- 对于 IPv4 网络环境，用户需要在 Super VLAN 的 VLAN 接口上开启本地代理 ARP 功能，Super VLAN 利用本地代理 ARP 可以进行 ARP 请求和响应报文的转发与处理，从而实现了 Sub VLAN 之间的三层互通。
- 对于 IPv6 网络环境，用户需要在 Super VLAN 的 VLAN 接口上开启本地代理 ND 功能，Super VLAN 利用本地代理 ND 可以进行 ND 请求和响应报文的转发与处理，从而实现了 Sub VLAN 之间的三层互通。

2.2 配置Super VLAN功能

Super VLAN 功能的配置包括三个必选步骤：

(1) 配置 Sub VLAN，主要是创建 Sub VLAN。

(2) 配置 Super VLAN，主要是创建 Super VLAN，并将 Super VLAN 和 Sub VLAN 关联起来。

(3) 配置 Super VLAN 对应的 VLAN 接口，该接口主要用于接入用户和 Sub VLAN 之间的通信。

1. 配置Sub VLAN

表2-1 配置 Sub VLAN

配置	命令	说明
进入系统视图	**system-view**	-
创建VLAN用作Sub VLAN，并进入VLAN视图	**vlan** *vlan-id*	必选 如果指定的VLAN不存在，则该命令先完成VLAN的创建，然后再进入该VLAN的视图

2. 配置Super VLAN

表2-2 配置 Super VLAN

配置	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	必选 如果指定的VLAN不存在，则该命令先完成VLAN的创建，然后再进入该VLAN的视图

配置	命令	说明
设置VLAN类型为Super VLAN	**supervlan**	必选 缺省情况下，用户创建的VLAN不是Super VLAN类型的VLAN
配置Super VLAN和Sub VLAN间的映射关系	**subvlan** *vlan-list*	必选 *vlan-list*必须是当前已创建的准备用作Sub VLAN的VLAN

说明

- 一个 VLAN 不能同时设置为 Super VLAN 和 Sub VLAN。
- 当端口上使能了动态触发端口加入 MAC VLAN 功能，此时 MAC VLAN 表项中的 VLAN 不能配置为 Super VLAN。
- 当 VLAN 类型为 Isolate-user-VLAN，或配置了该 VLAN 和 Secondary VLAN 间的映射关系，则该 VLAN 不能配置为 Super VLAN。

3. 配置Super VLAN对应的VLAN接口

表2-3 配置 Super VLAN 对应的 VLAN 接口

配置	命令	说明
进入系统视图	**system-view**	-
创建VLAN接口，并进入VLAN接口视图	**interface vlan-interface** *vlan-interface-id*	必选 *vlan-interface-id*的值必须等于Super VLAN ID
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	二者必选其一 缺省情况下，没有配置VLAN接口的IP地址
	ipv6 address { *ipv6-address* { *prefix-length* | **link-local** } | *ipv6-address*/*prefix-length* [**anycast** | **eui-64**] | **auto** [**link-local**] }	
开启本地代理ARP功能	**local-proxy-arp enable**	二者必选其一 缺省情况下，本地代理ARP功能和本地代理ND功能均处于关闭状态
开启本地代理ND功能	**local-proxy-nd enable**	

说明

- 以上步骤中配置的 VLAN 接口的 IP 地址就是对应的 Super VLAN 的 IP 地址。
- 本地代理 ARP 功能的相关介绍请参见“三层技术-IP 业务配置指导”中的“ARP”；**local-proxy-arp enable** 命令的相关描述请参见“三层技术-IP 业务命令参考”中的“代理 ARP”。
- 本地代理 ND 功能的相关介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”；**local-proxy-nd enable** 命令的相关描述请参见“三层技术-IP 业务命令参考”中的“IPv6 基础”。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。Guest VLAN 的相关内容请参见“安全配置指导”中的“802.1X”。
- 在 Super VLAN 下可以配置二层组播功能，但是该配置将不会生效。
- 在 Super VLAN 对应的 VLAN 接口下可以配置 DHCP、三层组播、动态路由等功能，但是只有 DHCP 的配置生效，其它配置将不会生效。
- 在 Super VLAN 对应的 VLAN 接口下配置 VRRP 功能后，会对网络性能造成影响，建议不要这样配置。VRRP 的详细描述请参见“可靠性配置指导”中的“VRRP”。

2.3 Super 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 Super VLAN 的运行情况，通过查看显示信息验证配置的效果。

表2-4 Super VLAN 显示和维护

操作	命令
显示Super VLAN和Sub VLAN之间的映射关系	**display supervlan** [*supervlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

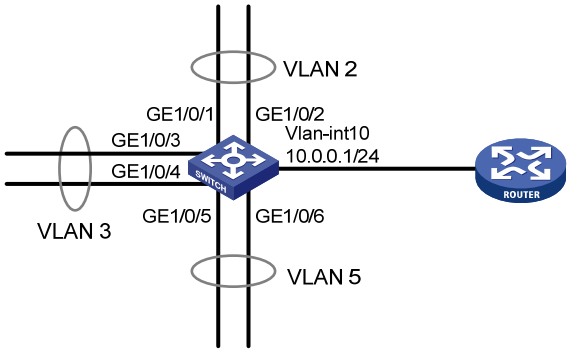
2.4 Super VLAN典型配置举例

1. 组网需求

- 创建 Super VLAN 10，VLAN 接口的 IP 地址为 10.0.0.1/24。
- 创建 Sub VLAN：VLAN 2、VLAN 3、VLAN 5。
- 端口 GigabitEthernet1/0/1 和端口 GigabitEthernet1/0/2 属于 VLAN 2，端口 GigabitEthernet1/0/3 和端口 GigabitEthernet1/0/4 属于 VLAN 3，端口 GigabitEthernet1/0/5 和端口 GigabitEthernet1/0/6 属于 VLAN 5。
- 各 Sub VLAN 的用户之间能够满足二层隔离和三层互通。

2. 组网图

图2-1 配置 Super-vlan 组网图



3. 配置步骤

创建 VLAN 10，配置 VLAN 接口的 IP 地址为 10.0.0.1/24。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 10.0.0.1 255.255.255.0
```

为实现 Super VLAN 特性，开启设备的本地代理功能。

```
[Sysname-Vlan-interface10] local-proxy-arp enable
[Sysname-Vlan-interface10] quit
```

创建 VLAN 2，并添加端口 GigabitEthernet1/0/1 和端口 GigabitEthernet1/0/2。

```
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Sysname-vlan2] quit
```

创建 VLAN 3，并添加端口 GigabitEthernet1/0/3 和端口 GigabitEthernet1/0/4。

```
[Sysname] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/3 gigabitethernet 1/0/4
[Sysname-vlan3] quit
```

创建 VLAN 5，并添加端口 GigabitEthernet1/0/5 和端口 GigabitEthernet1/0/6。

```
[Sysname] vlan 5
[Sysname-vlan5] port gigabitethernet 1/0/5 gigabitethernet 1/0/6
[Sysname-vlan5] quit
```

指定 VLAN 10 为 Super VLAN，VLAN 2、VLAN 3 和 VLAN 5 为 Sub VLAN。

```
[Sysname] vlan 10
[Sysname-vlan10] supervlan
[Sysname-vlan10] subvlan 2 3 5
[Sysname-vlan10] quit
[Sysname] quit
```

4. 显示和验证

查看 Super VLAN 的相关信息，验证以上配置是否生效。

```
<Sysname> display supervlan
 SuperVLAN ID :  10
 SubVLAN ID :  2-3 5

 VLAN ID: 10
 VLAN Type: static
 It is a Super VLAN.
```

```
Route Interface: configured
IPv4 Address: 10.0.0.1
IPv4 Subnet Mask: 255.255.255.0
Description: VLAN 0010
Name: VLAN 0010
Tagged   Ports: none
Untagged Ports: none

VLAN ID: 2
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IPv4 Address: 10.0.0.1
IPv4 Subnet Mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/1     GigabitEthernet1/0/2

VLAN ID: 3
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IPv4 Address: 10.0.0.1
IPv4 Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/3     GigabitEthernet1/0/4

VLAN ID: 5
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IPv4 Address: 10.0.0.1
IPv4 Subnet Mask: 255.255.255.0
Description: VLAN 0005
Name: VLAN 0005
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/5     GigabitEthernet1/0/6
```

3 Isolate-user-VLAN配置

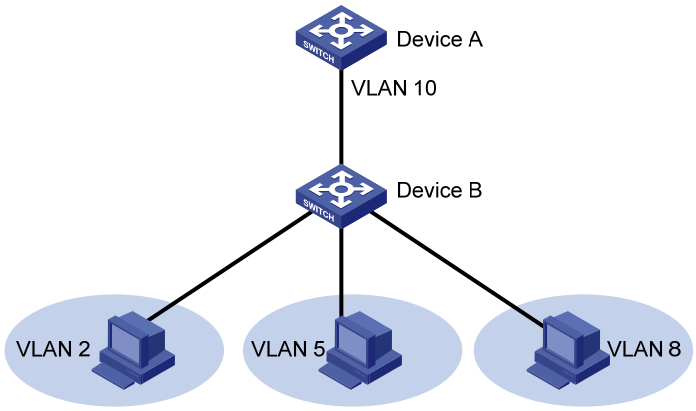
3.1 Isolate-user-VLAN简介

Isolate-user-VLAN采用两层VLAN结构，它在同一台设备上设置Isolate-user-VLAN和Secondary VLAN两类VLAN。

- Isolate-user-VLAN用于上行，不同的Secondary VLAN关联到同一个Isolate-user-VLAN。上行连接的设备只知道Isolate-user-VLAN，而不必关心Secondary VLAN，简化了网络配置，节省了VLAN资源。
- Secondary VLAN用于连接用户，Secondary VLAN之间二层报文互相隔离。如果希望实现同一Isolate-user-VLAN下Secondary VLAN用户之间报文的互通，可以通过配置上行设备（如 图 3-1 中Device A）的本地ARP代理功能来实现三层报文的互通。
- 一个Isolate-user-VLAN可以和多个Secondary VLAN相对应。Isolate-user-VLAN下面的Secondary VLAN对上行设备不可见。

如下图所示，设备Device B上启动了Isolate-user-VLAN功能。其中VLAN 10是Isolate-user-VLAN；VLAN 2、VLAN 5、VLAN 8是Secondary VLAN；VLAN 2、VLAN 5、VLAN 8都映射到VLAN 10；VLAN 2、VLAN 5、VLAN 8对Device A不可见。

图3-1 Isolate-user-VLAN示意图



3.2 配置Isolate-user-VLAN

Isolate-user-VLAN配置主要包括下面几个步骤：

(1) 配置Isolate-user-VLAN。

(2) 配置Secondary VLAN。

(3) 配置Isolate-user-VLAN和Secondary VLAN间的映射关系。

(4) 配置上行/下行端口：配置上行端口（如 图 3-1 中Device B上与Device A相连的端口）在指定VLAN中工作在promiscuous模式，可以实现上行端口加入指定的Isolate-user-VLAN和及同步加入对应的Secondary VLAN的功能；配置下行端口（如 图 3-1 中Device B上与用户相连的端口）工作在host模式，可以实现下行端口同步加入Secondary VLAN对应的Isolate-user-VLAN的功能。有关promiscuous/host模式的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”的相关命令。

表3-1 配置 Isolate-user-VLAN

操作		命令	说明
进入系统视图		**system-view**	-
创建Isolate-user-VLAN，并进入VLAN视图		**vlan** *vlan-id*	-
设置VLAN类型为Isolate-user-VLAN		**isolate-user-vlan enable**	必选 缺省情况下，用户创建的VLAN不是Isolate-user-VLAN类型的VLAN
退回系统视图		**quit**	-
创建Secondary VLAN		**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	必选
设置同一Secondary VLAN内各端口二层隔离		**isolated-vlan enable**	可选 缺省情况下，同一Secondary VLAN内的端口能够二层互通 当同一Secondary VLAN内各端口的工作模式均为host模式，且Isolate-user-VLAN和Secondary VLAN建立映射关系后才能生效
退回系统视图		**quit**	-
配置Isolate-user-VLAN和Secondary VLAN间的映射关系		**isolate-user-vlan** *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]	必选 缺省情况下，用户创建的Isolate-user-VLAN和Secondary VLAN没有任何映射关系
配置Isolate-user-VLAN上行端口	进入二层以太网端口视图或二层聚合接口视图	**Interface** *interface-type interface-number* **Interface bridge-aggregation** *interface-number*	二者必选其一
	配置上行端口在指定VLAN中工作在promiscuous模式	**port isolate-user-vlan** *vlan-id* **promiscuous**	必选 缺省情况下，端口既不工作在promiscuous模式也不工作在host模式
退回系统视图		**quit**	-
配置Isolate-user-VLAN下行端口	进入二层以太网端口视图或二层聚合接口视图	**Interface** *interface-type interface-number* **Interface bridge-aggregation** *interface-number*	二者必选其一
	设置端口的链路类型	**port link-type** { **access** | **hybrid** | **trunk** }	-
	将下行端口加入到Secondary VLAN中	当端口类型为Access时： **port access vlan** *vlan-id* 当端口类型为Hybrid时： **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } 当端口类型为Trunk时： **port trunk permit vlan** { *vlan-list* | **all** }	三者必选其一

操作		命令	说明
	配置下行端口工作在host模式	**port isolate-user-vlan host**	必选 缺省情况下，端口不工作在host模式

说明

- 如果 Isolate-user-VLAN 中的用户需要与其它网络进行三层互通，则需要在设备上创建 Isolate-user-VLAN 接口和 Secondary VLAN 接口，并在 Isolate-user-VLAN 接口上配置网关的 IP 地址，Secondary VLAN 接口上不需要配置 IP 地址。
- 业务环回组成员端口不能配置为 isolate-user-vlan 上行端口（promiscuous 端口）或下行端口（host 端口），有关业务环回组的详细介绍请参见“二层技术-以太网交换配置指导”中的“业务环回组配置”。

3.3 Isolate-user-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 Isolate-user-VLAN 的运行情况，通过查看显示信息验证配置的效果。

表3-2 Isolate-user-VLAN 显示和维护

操作	命令
显示Isolate-user-VLAN和Secondary VLAN的映射关系	**display isolate-user-vlan** [*isolate-user-vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

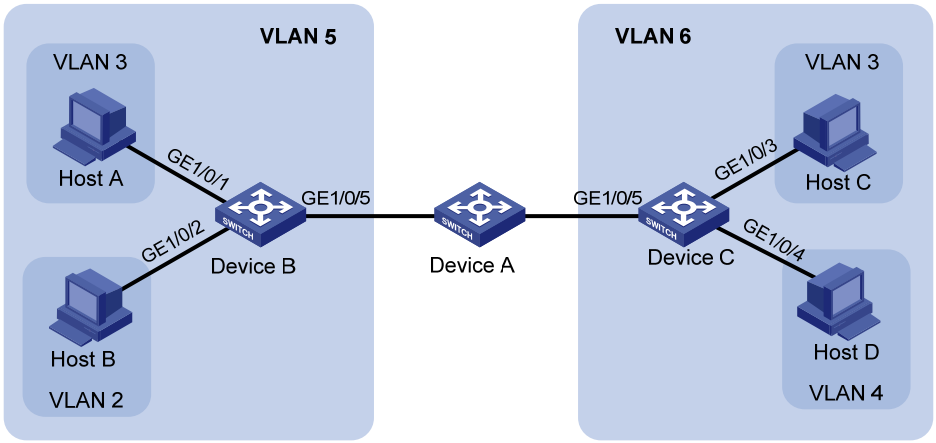
3.4 Isolate-user-VLAN典型配置举例

1. 组网需求

- Device A 下接 Device B、Device C。
- Device B 上的 VLAN 5 为 Isolate-user-VLAN，包含上行端口 GigabitEthernet1/0/5 和两个 Secondary VLAN（VLAN 2 和 VLAN 3），VLAN 2 包含端口 GigabitEthernet1/0/2，VLAN 3 包含端口 GigabitEthernet1/0/1。
- Device C 上的 VLAN 6 为 Isolate-user-VLAN，包含上行端口 GigabitEthernet1/0/5 和两个 Secondary VLAN（VLAN 3 和 VLAN 4），VLAN 3 包含端口 GigabitEthernet1/0/3，VLAN 4 包含端口 GigabitEthernet1/0/4。
- 从 Device A 看，下接的 Device B 只有一个 VLAN（VLAN 5），下接的设备 C 只有一个 VLAN（VLAN 6）。

2. 组网图

图3-2 配置 Isolate-user-VLAN 组网图



3. 配置步骤

下面只列出 Device B 和 Device C 的配置过程。

(1) 配置 Device B

配置 VLAN 5 为 Isolate-user-VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] quit
```

创建 Secondary VLAN。

```
[DeviceB] vlan 2 to 3
```

配置 Isolate-user-VLAN 和 Secondary VLAN 间的映射关系。

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

配置上行端口 GigabitEthernet 1/0/5 在 VLAN 5 中工作在 promiscuous 模式。

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port isolate-user-vlan 5 promiscuous
[DeviceB-GigabitEthernet1/0/5] quit
```

将下行端口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 分别添加到 VLAN 3、VLAN 2，并配置它们工作在 host 模式。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 3
[DeviceB-GigabitEthernet1/0/1] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

(2) 配置 Device C

配置 VLAN 6 为 Isolate-user-VLAN。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] isolate-user-vlan enable
[DeviceC-vlan6] quit
```

创建 Secondary VLAN。

```
[DeviceC] vlan 3 to 4
```

配置 Isolate-user-VLAN 和 Secondary VLAN 间的映射关系。

```
[DeviceC] isolate-user-vlan 6 secondary 3 to 4
```

配置上行端口 GigabitEthernet 1/0/5 在 VLAN 6 中工作在 promiscuous 模式。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port isolate-user-vlan 6 promiscuous
[DeviceC-GigabitEthernet1/0/5] quit
```

将下行端口 GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 分别添加到 VLAN 3、VLAN 4，并配置它们工作在 host 模式。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 3
[DeviceC-GigabitEthernet1/0/3] port isolate-user-vlan host
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] port access vlan 4
[DeviceC-GigabitEthernet1/0/4] port isolate-user-vlan host
[DeviceC-GigabitEthernet1/0/4] quit
```

4. 显示与验证

显示 Device B 上的 Isolate-user-VLAN 配置情况。

```
[DeviceB] display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 5
 Secondary VLAN ID : 2-3

 VLAN ID: 5
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: not configured
 Description: VLAN 0005
 Name：VLAN 0005
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1           GigabitEthernet1/0/2           GigabitEthernet1/0/5

 VLAN ID: 2
 VLAN Type: static
 Isolate-user-VLAN type : secondary
 Route Interface: not configured
 Description: VLAN 0002
 Name：VLAN 0002
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/2           GigabitEthernet1/0/5

 VLAN ID: 3
 VLAN Type: static
 Isolate-user-VLAN type : secondary
 Route Interface: not configured
 Description: VLAN 0003
 Name：VLAN 0003
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1           GigabitEthernet1/0/5
```

4 Voice VLAN配置

4.1 Voice VLAN简介

随着语音技术的日益发展，语音设备应用越来越广泛，尤其在宽带小区，网络中经常同时存在语音数据和业务数据两种流量。通常，语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

Voice VLAN 是为用户的语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，系统自动为语音报文修改 QoS（Quality of Service，服务质量）参数，来提高语音数据报文优先级、保证通话质量。

说明

常见的语音设备有 IP 电话、IAD（Integrated Access Device，综合接入设备）等。本文中以 IP 电话为例进行说明。

当 IP 电话接入设备时，需要设备完成以下两个任务：

(1) 识别 IP 电话，获取 IP 电话的 MAC，从而进行安全认证及提高语音报文的优先级；

(2) 将 Voice VLAN 信息通告给 IP 电话，IP 电话能够根据收到的 Voice VLAN 信息完成自动配置，使 IP 电话发出的语音报文在 Voice VLAN 内传输。

4.2 设备识别IP电话的方法

4.2.1 OUI地址

设备可以根据进入端口的数据报文中的源 MAC 地址字段来判断该数据流是否为语音数据流。源 MAC 地址符合系统设置的语音设备 OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流。

用户可以预先设置OUI地址，也可以使用缺省的OUI地址作为判断标准。设备缺省的OUI地址如 表4-1 所示。目前本系列设备支持配置 128 个OUI地址。

表4-1 设备缺省的 OUI 地址

序号	OUI 地址	生产厂商
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	00D0-1E00-0000	Pingtel phone
5	0060-B900-0000	Philips/NEC phone
6	00E0-7500-0000	Polycom phone
7	00E0-BB00-0000	3Com phone

说明

- 通常意义下，OUI 地址指的是 MAC 地址的前 24 位（二进制），是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。本文中的 OUI 地址有别于通常意义的 OUI 地址，它是设备判断收到的报文是否为语音报文的依据，是 **voice vlan mac-address** 命令中的 *mac-address* 和 *oui-mask* 参数相与的结果。
- 设备缺省的 OUI 地址可以手工删除，删除之后也可再次手工添加。

4.2.2 通过LLDP自动识别IP电话

通过设备上配置的OUI地址识别IP电话的方法受限于设备上可配置的OUI地址的数量，并且当网络中IP电话数量众多时，管理员的配置工作量较大。如果IP电话支持LLDP功能，可以配置LLDP自动识别IP电话功能。有关该功能的详细介绍，请参见“4.6 通过LLDP自动发现IP电话功能”。

4.3 设备将Voice VLAN信息通告给IP电话

4.3.1 设备通告Voice VLAN信息的方法

如果 IP 电话支持 LLDP，设备可以通过 LLDP 报文中的 LLDP-MED TLV 将 Voice VLAN 信息通告给 IP 电话。

如果 IP 电话只支持 CDP，不支持 LLDP，可以通过配置 LLDP 兼容 CDP 功能使设备将 Voice VLAN 信息封装在 CDP 报文中通告给 IP 电话。

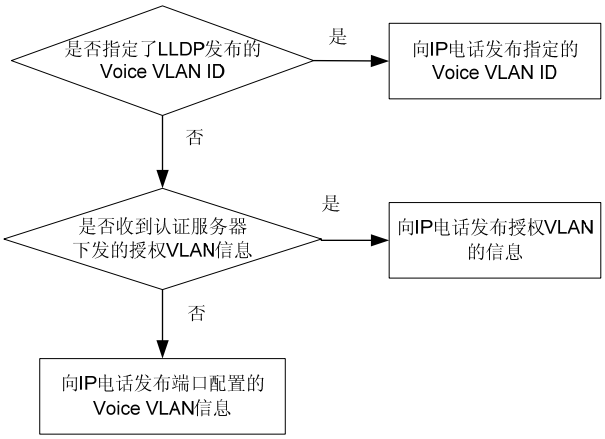
有关 LLDP 和 LLDP 兼容 CDP 的详细信息，请参见“二层技术-以太网交换配置指导”中的“LLDP”。

4.3.2 设备获取Voice VLAN信息的方法

- 端口配置Voice VLAN，请参见“4.5 端口配置Voice VLAN”。
- 当IP电话配合认证功能使用时，可以将授权VLAN信息通告给IP电话，请参见“4.8 通过LLDP动态发布授权VLAN功能”。
- 指定LLDP发布的Voice VLAN信息，请参见“4.7 指定LLDP发布的Voice VLAN信息”。

这三种方法的通告顺序如 图 4-1 所示。

图4-1 设备向 IP 电话发布 Voice VLAN 信息的过程

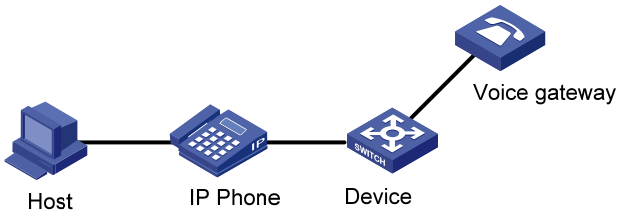


4.4 IP电话的接入方式

1. 主机和IP电话串联接入

如 图 4-2 所示，主机连接到IP电话，IP电话连接到接入设备。在串联接入的环境下，需要将主机和IP电话划分到不同的VLAN，且需要IP电话能发出携带VLAN Tag的报文，从而区分业务数据流和语音数据流。同时，端口需要允许Voice VLAN和PVID的报文通过。

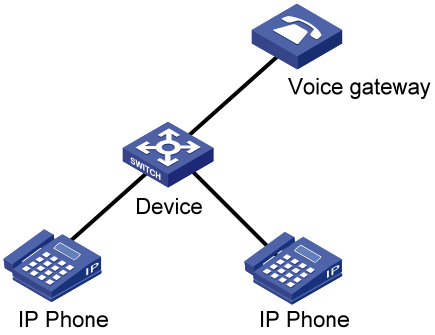
图4-2 主机与 IP 电话串联接入组网图



2. IP电话单独接入

如 图 4-3 所示，IP电话单独接入设备。单独接入适用于IP电话发出Untagged语音报文的情况，此时需要配置Voice VLAN为PVID并配置端口允许PVID的报文通过。

图4-3 IP 电话单独接入组网图



4.5 端口配置Voice VLAN

4.5.1 Voice VLAN的自动模式和手动模式

Voice VLAN 的工作模式包括自动模式和手动模式，这个自动和手动指的是端口加入 Voice VLAN 的方式。

1. 自动模式

自动模式适用于PC-IP电话串联接入（端口同时传输语音数据和普通业务数据）的组网方式，如 图 4-2 所示。

系统利用 IP 电话上电时发出的协议报文，通过识别报文的源 MAC，匹配 OUI 地址。匹配成功后，系统将自动把语音报文的入端口加入 Voice VLAN，并下发 ACL 规则、配置报文的优先级。用户可以在设备上设置 Voice VLAN 的老化时间，当在老化时间内，系统没有从入端口收到任何语音报文时，系统将把该端口从 Voice VLAN 中删除。端口的添加/删除到 Voice VLAN 的过程由系统自动实现。当 Voice VLAN 正常工作时，如果遇到设备重新启动的情况，为保证已经建立的语音连接能够正常工作，系统会在重新启动完成后，将配置为自动模式的端口重新加入 Voice VLAN，而不需要再次通过语音流触发。

2. 手动模式

手动模式适用于IP电话单独接入（端口仅传输语音报文）的组网方式，如 图 4-3 所示。该组网方式可以使该端口专用于传输语音数据，最大限度避免业务数据对语音数据传输的影响。

手动模式下，需要通过手工把 IP 电话接入端口加入 Voice VLAN 中。再通过识别报文的源 MAC，匹配 OUI 地址。匹配成功后，系统将下发 ACL 规则、配置报文的优先级。端口的添加/删除到 Voice VLAN 的过程由管理员手动实现。

3. Voice VLAN工作模式和IP电话的配合

IP电话类型较多，有些电话能发出携带VLAN Tag的报文，有些电话只能发出Untagged报文。因此需要用户保证端口的链路类型与IP电话能够匹配，不同Voice VLAN工作模式下的详细配合关系请见 表 4-2 和 表 4-3：

- IP 电话发送 Tagged 语音数据

表4-2 不同类型端口支持 Tagged 语音数据配置要求

Voice VLAN 工作模式	端口类型	是否支持 Tagged 语音数据	配置要求
自动模式	Access	不支持	-
	Trunk	支持	缺省VLAN不能为Voice VLAN
	Hybrid		
手工模式	Access	不支持	-
	Trunk	支持	缺省VLAN不能为Voice VLAN，需要配置端口允许Voice VLAN的报文通过
	Hybrid	支持	缺省VLAN不能为Voice VLAN，需要配置端口允许Voice VLAN的报文携带Tag通过

- IP 电话发送 Untagged 语音数据

当 IP 电话发送 Untagged 语音数据，则端口的 Voice VLAN 工作模式只能为手工模式，不能为自动模式。

表4-3 不同类型端口支持 Untagged 语音数据配置要求

Voice VLAN 工作模式	端口类型	是否支持 Untagged 语音数据	配置要求
自动模式	Access	不支持	-
	Trunk		
	Hybrid		
手工模式	Access	支持	将缺省VLAN配置为Voice VLAN
	Trunk	支持	接入端口的缺省VLAN必须是Voice VLAN，且接入端口允许该VLAN通过
	Hybrid	支持	接入端口的缺省VLAN必须是Voice VLAN，且允许Voice VLAN的报文不带Tag通过

注意

- 如果用户的 IP Phone 发出的是 Tagged 语音流，且接入的端口上使能了 802.1X 认证和 Guest VLAN/Auth-Fail VLAN/Critical VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Guest VLAN/Auth-Fail VLAN/Critical VLAN 分配不同的 VLAN ID。
- 如果用户的 IP Phone 发出的是 Untagged 语音流，为实现 Voice VLAN 功能，只能将接入端口的缺省 VLAN 配置为 Voice VLAN，此时将不能实现 802.1X 认证功能。

4.5.2 Voice VLAN的安全模式和普通模式

根据使能了 Voice VLAN 功能的端口对接收到的数据包的过滤机制又可以将 Voice VLAN 的工作模式分为普通模式和安全模式：

- 普通模式下，端口加入 Voice VLAN 后，设备对于接收的语音报文不再一一进行识别，凡是带有 Voice VLAN Tag 的报文，设备将不再检查其源 MAC 地址是否为语音设备的 OUI 地址，均接收并在 Voice VLAN 中转发。对于缺省 VLAN 就是 Voice VLAN 的手工模式端口，会导致任意的 Untagged 报文都可以在 Voice VLAN 中传输。这样的处理方式很容易使 Voice VLAN 收到恶意用户的流量攻击。恶意用户可以构造大量带有 Voice VLAN Tag 或 Untagged 的报文，占用 Voice VLAN 的带宽，影响正常的语音通信。
- 安全模式下，设备将对每一个要进入 Voice VLAN 传输的报文进行源 MAC 匹配检查，对于不能匹配 OUI 地址的报文，则将其丢弃。

对于比较安全的网络，用户可以配置 Voice VLAN 的普通模式，以减少检查报文的工作对系统资源的占用。

窍门

建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。如确有此需要，请确认 Voice VLAN 的安全模式已关闭。

表4-4 Voice VLAN 的安全/普通模式对报文的处理

Voice VLAN 工作模式	报文类型	处理方式
安全模式	Untagged报文	当该报文源MAC地址是可识别的OUI地址时，允许该报文在Voice VLAN内传输，否则将该报文丢弃
	带有Voice VLAN Tag的报文	
	带有其他VLAN Tag的报文	根据指定端口是否允许该VLAN通过来对报文进行转发和丢弃的处理，不受Voice VLAN安全/普通模式的影响
普通模式	Untagged报文	不对报文的源MAC地址进行检查，所有报文均可以在Voice VLAN内进行传输
	带有Voice VLAN Tag的报文	
	带有其他VLAN Tag的报文	根据指定端口是否允许该VLAN通过来对报文进行转发和丢弃的处理，不受Voice VLAN安全/普通模式的影响

4.5.3 配置准备

(1) 创建 VLAN

配置 Voice VLAN 之前，须先创建对应的 VLAN。

(2) 确定语音报文的 QoS 优先级

配置语音报文的QoS优先级，需要关闭接口上的Voice VLAN功能。当Voice VLAN使能时，不允许修改语音报文的QoS优先级。语音报文的QoS优先级的配置请参见 4.5.4 配置语音报文的QoS优先级。

(3) 确定将要配置的 Voice VLAN 的工作模式

- 配置自动模式的Voice VLAN，请参见 4.5.5 配置自动模式下的Voice VLAN；
- 配置手动模式的Voice VLAN，请参见 4.5.6 配置手动模式下的Voice VLAN。

4.5.4 配置语音报文的QoS优先级

Voice VLAN 在实现中，通过提高语音报文的 QoS 优先级（CoS 和 DSCP 值）来保证语音通信的质量。语音报文会自带 QoS 优先级，通过配置，用户可以选择在语音报文通过设备时修改或者不修改报文的 QoS 优先级。

表4-5 配置语音报文的 QoS 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置接口信任语音报文的优先级，即接口不会修改Voice VLAN内语音报文自带的CoS和DSCP值	**voice vlan qos trust**	二者任选其一 缺省情况下，接口会将Voice VLAN内语音报文的CoS值修改为6，DSCP值修改为46 在同一接口多次执行这两条命令，则最新配置将覆盖旧配置，最新的配置生效
将Voice VLAN内语音报文的CoS和DSCP修改为指定值	**voice vlan qos** *cos-value dscp-value*	

注意

- 在 Voice VLAN 使能的情况下，不允许配置/修改语音报文的 QoS 优先级。必须禁用 Voice VLAN 后，才能配置/修改。
- 在 S5500-28SC-HI 和 S5500-52SC-HI 交换机上，如果设备上配置了匹配语音报文的 QoS 策略并进行了应用，则该语音报文的优先级不能被 Voice VLAN 功能修改。

4.5.5 配置自动模式下的Voice VLAN

说明

- 自动模式下的Voice VLAN只支持Hybrid端口对Tagged的语音流进行处理，而协议VLAN特性要求Hybrid入端口的报文格式为Untagged的（详情请参见“1.6.2 配置基于协议的VLAN”），因此，不能将某个VLAN同时设置为Voice VLAN和协议VLAN。
- 配置 MSTP 多实例情况下，如果端口在要加入的 Voice VLAN 对应的 MSTP 实例中是阻塞状态，则端口会丢弃收到的报文，造成 MAC 地址不能上送，不能完成动态触发功能。自动模式 Voice VLAN 的使用场景为接入侧，不建议和多实例 MSTP 同时使用。
- 配置 PVST 情况下，如果端口要加入的 Voice VLAN 不为端口允许通过的 VLAN，则端口处于阻塞状态，会丢弃收到的报文，造成 MAC 地址不能上送，不能完成动态触发功能。自动模式 Voice VLAN 的使用场景为接入侧，不建议和 PVST 同时使用。

表4-6 配置自动模式下的 Voice VLAN

操作	命令	说明
进入系统视图	**system-view**	-
设置Voice VLAN的老化时间	**voice vlan aging** *minutes*	可选 缺省情况下，老化时间为1440分钟，老化时间只对自动模式下的端口有效
使能Voice VLAN的安全模式	**voice vlan security enable**	可选 缺省情况下，Voice VLAN工作在安全模式
设置Voice VLAN识别的OUI地址	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	可选 Voice VLAN启动后将有缺省的OUI地址，请参见“表4-1设备缺省的OUI地址”
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型	**port link-type trunk** **port link-type hybrid**	二者必选其一
设置端口Voice VLAN的工作模式为自动模式	**voice vlan mode auto**	可选 缺省情况下，Voice VLAN工作在自动模式 各个端口Voice VLAN的工作模式相互独立，不同的端口可以设置成不同的模式
使能端口的Voice VLAN功能	**voice vlan** *vlan-id* **enable**	必选 缺省情况下，端口没有使能Voice VLAN功能

4.5.6 配置手动模式下的Voice VLAN

表4-7 配置手动模式下的 Voice VLAN

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
使能Voice VLAN的安全模式		**voice vlan security enable**	可选 缺省情况下，Voice VLAN工作在安全模式
设置Voice VLAN识别的OUI地址		**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	可选 Voice VLAN启动后将有缺省的OUI地址，请参见“表4-1设备缺省的OUI地址”
进入二层以太网端口视图		**interface** *interface-type interface-number*	-
配置端口的Voice VLAN工作模式为手动模式		**undo voice vlan mode auto**	必选 缺省情况下，端口的Voice VLAN工作在自动模式
将手动模式端口加入Voice VLAN	Access端口	请参见“1.4.2 配置基于Access端口的VLAN”	三者必选其一 将Access端口加入Voice VLAN后，Voice VLAN会自动成为Access端口的缺省VLAN
	Trunk端口	请参见“1.4.3 配置基于Trunk端口的VLAN”	
	Hybrid端口	请参见“1.4.4 配置基于Hybrid端口的VLAN”	
设置Voice VLAN为端口的缺省VLAN	Trunk端口	请参见“1.4.3 配置基于Trunk端口的VLAN”	可选 当输入的语音流是Untagged语音流时，需要进行该项配置；当输入的语音流是Tagged语音流时，不能将Voice VLAN设置为端口的缺省VLAN
	Hybrid端口	请参见“1.4.4 配置基于Hybrid端口的VLAN”	
使能端口的Voice VLAN功能		**voice vlan** *vlan-id* **enable**	必选 缺省情况下，端口没有使能Voice VLAN功能

说明

- 同一设备同一时刻可以给不同的端口配置不同的 Voice VLAN，但一个端口只能配置一个 Voice VLAN，而且这些 VLAN 必须是已经存在的静态 VLAN。
- 不允许在聚合组的成员端口上使能 Voice VLAN 功能。有关聚合组的成员端口的详细介绍，请参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- 当端口使能了 Voice VLAN 并工作在手工模式时，必须手工将端口加入 Voice VLAN，才能保证 Voice VLAN 功能生效。

4.6 通过LLDP自动发现IP电话功能

传统的 Voice VLAN 是通过手工配置的 OUI 地址作为 IP 电话的匹配规则和接入条件，由于可配置的 OUI 地址数量有限，这种方式限制了可接入网络的 IP 电话的类型（将源 MAC 匹配同一 OUI 地址的 IP 电话视为一个类型）。

在设备上配置了通过 LLDP 自动发现 IP 电话功能后，设备将通过 LLDP 自动发现对端设备，并与对端设备通过 LLDP 的 TLV 进行信息交互。如果通过端口收到的 LLDP System Capabilities TLV

中的信息发现对端设备具有电话能力，则认为对端设备是 IP 电话并将设备上配置的 Voice VLAN 信息通过 LLDP 发送给对端设备。这种方式使接入网络的 IP 电话类型不再受限于 OUI 地址的数量。

在完成 IP 电话的发现过程后，端口将继续完成 Voice VLAN 的其余功能，即端口将自动加入 Voice VLAN，并提高从该 IP 电话发出的语音数据的优先级。为防止 IP 电话无法通过端口上配置的认证功能，设备还会将 IP 电话的 MAC 地址添加到 MAC 地址表中。

4.6.1 配置准备

在配置通过 LLDP 自动发现 IP 电话功能之前，需完成以下任务：

- 在全局和端口使能 LLDP 功能。
- 完成 Voice VLAN 功能的配置。

4.6.2 配置通过LLDP自动发现IP电话功能

表4-8 配置通过 LLDP 自动发现 IP 电话功能

操作	命令	说明
进入系统视图	**system-view**	-
配置通过 LLDP 自动发现 IP 电话功能	**voice vlan track lldp**	必选 缺省情况下，通过 LLDP 自动发现 IP 电话功能处于关闭状态

注意

- 通过 LLDP 自动发现 IP 电话功能只能与 Voice VLAN 自动模式配合使用，不能与手动模式配合使用。
- 设备开启了通过 LLDP 自动发现 IP 电话功能后，每个端口最多可以接入 5 台 IP 电话。
- 通过 LLDP 自动发现 IP 电话功能与 LLDP 兼容 CDP 功能不能同时配置。

4.7 指定LLDP发布的Voice VLAN信息

4.7.1 简介

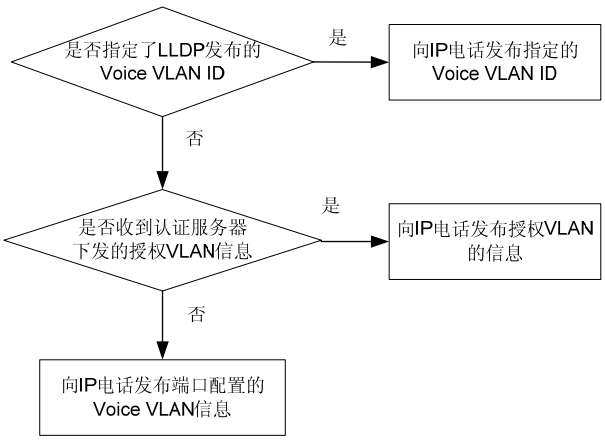
说明

指定 LLDP 发布的 Voice VLAN 信息功能适用于与支持 LLDP 协议的 IP 电话配合使用，配置 LLDP 兼容 CDP 功能之后，也可以与支持 CDP 的 IP 电话配合使用，请确认对端 IP 电话的支持情况。

当有 IP 电话接入设备时，需要设备将 Voice VLAN 信息通告给 IP 电话，使 IP 电话完成 Voice VLAN 的自动配置，从而在 Voice VLAN 中转发语音数据流。开启 LLDP 功能后，设备通过 LLDP-MED 中的 Network Policy TLV 将 Voice VLAN 信息发布给 IP 电话。

通过配置本功能，可以指定 LLDP 向 IP 电话发布的 Voice VLAN 信息。配置本功能后，设备向 IP 电话发布 Voice VLAN 信息的过程如下：

图4-4 设备向 IP 电话发布 Voice VLAN 信息的过程



IP 电话根据收到的信息（VLAN ID、是否携带 Tag、优先级信息）完成自动配置：

- 如果IP电话根据设备通过命令行指定的Voice VLAN信息完成自动配置，会发送携带指定VLAN Tag的报文，语音数据流将在指定VLAN中转发。在设备上通过命令行指定LLDP发布的Voice VLAN信息的配置方法见 4.7.2 。
- 如果IP电话根据认证服务器下发的授权VLAN信息完成自动配置，会发送携带授权VLAN Tag的报文，语音数据流将在授权VLAN中转发。相关内容见 4.8 通过LLDP动态发布授权VLAN功能。
- 如果 IP 电话根据设备接入端口配置的 Voice VLAN 信息完成自动配置，语音数据流将在端口上配置的 Voice VLAN 中转发，是否携带 Tag 由端口上 Voice VLAN 的配置决定。

说明

LLDP-MED Network Policy TLV 中的信息可以通过 **display lldp local-information** 显示信息中的 MED information 相关字段查看。

4.7.2 配置指定LLDP发布的Voice VLAN信息

表4-9 配置指定 LLDP 发布的 Voice VLAN 信息

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置指定 LLDP 发布的 Voice VLAN 信息		**lldp voice-vlan** *vlan-id*	必选 缺省情况下，LLDP 发布端口配置的 Voice VLAN 信息

说明

- 当设备配置 LLDP 兼容 CDP 功能之后，在发送给 IP 电话的 CDP 报文中也发送指定的 Voice VLAN ID，此时本功能也可以与支持 CDP 的 IP 电话配合使用。
- 设备发送给 IP 电话的 LLDP 报文中包含优先级信息，CDP 报文中不包含优先级信息。
- 端口上配置 Voice VLAN 时，设备通过软件学习 MAC 地址；通过 **lldp voice-vlan** 命令指定 Voice VLAN 时，设备通过硬件学习 MAC 地址。

4.8 通过LLDP动态发布授权VLAN功能

说明

- 本功能适用于与支持 LLDP 协议的 IP 电话配合使用，请确认对端 IP 电话是否支持 LLDP 功能。
- 如果设备配置 802.1X 功能对接入设备进行认证，请确认接入的 IP 电话是否支持进行 802.1X 认证。

通过 LLDP 动态发布授权 VLAN 功能是指 LLDP 在配合 802.1X 认证或者 MAC 地址认证使用时，会将服务器下发的授权 VLAN 的信息通过 LLDP-MED Network Policy TLV 发送给通过认证的邻居 IP 电话。同时，设备连接 IP 电话的端口会加入授权 VLAN。

IP 电话根据认证服务器下发的授权 VLAN 信息完成自动配置后，会发送携带授权 VLAN Tag 的报文，语音数据流将在授权 VLAN 中转发。

本功能无配置命令，仅需完成以下功能的配置：

- 请在全局和端口上开启 LLDP 功能。
- 完成安全认证功能的配置，使 IP 电话能够通过安全认证。
- 在服务器上配置给通过认证的 IP 电话下发的授权 VLAN。

说明

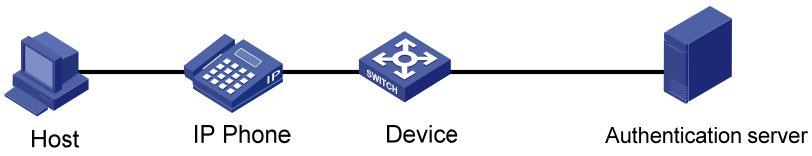
- 有关 802.1X 和 MAC 地址认证的内容请参见“安全配置指导”中的对应章节。
- 授权 VLAN 相关信息请参见“安全配置指导”中“802.1X 配置”中 1.2 节 802.1X 扩展功能部分的支持 VLAN 下发章节和“MAC 地址认证配置“中 1.1.4.1 下发 VLAN 章节。

4.8.1 使用 802.1X对IP电话进行认证应用举例

如 图 4-5 的组网中，在Device上配置 802.1X对主机和IP电话进行认证（IP电话需要支持 802.1X功能）。在认证服务器上配置给主机下发Untag类型授权VLAN，给IP电话下发Tag类型授权VLAN。主机和IP电话通过认证后，设备连接IP电话的端口会以Untag方式加入主机所在授权VLAN，以Tag方式加入IP电话所在授权VLAN。同时，设备发给IP电话的LLDP-MED TLV中携带下发给IP电话的授权VLAN信息，使IP电话发出的语音报文携带Tag在授权VLAN内转发。

需要注意的是，由于 802.1X 协议定义的 EAPOL 报文不带 VLAN Tag，因此当服务器上指定了给 IP 电话下发带 Tag 的授权 VLAN 时，需要在设备连接 IP 电话的端口上配置端口发送 802.1X 协议报文不带 Tag（**dot1x eapol untag**）。

图4-5 使用 802.1X 对 IP 电话进行认证



说明

目前仅 802.1X 认证支持下发带 Tag 类型授权 VLAN。

4.9 Voice 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 Voice VLAN 的运行情况，通过查看显示信息验证配置的效果。

表4-10 Voice VLAN 显示和维护

操作	命令
显示Voice VLAN的状态	**display voice vlan state** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统当前支持的OUI地址	**display voice vlan oui** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

4.10 Voice VLAN典型配置举例

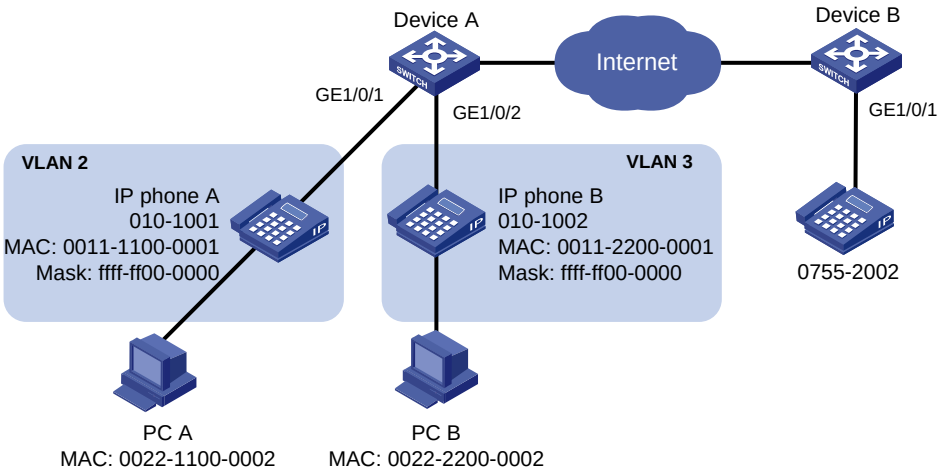
4.10.1 自动模式下Voice VLAN的配置举例

1. 组网需求

- IP phone A 的 MAC 地址为 0011-1100-0001，下行连接 PC A（MAC 地址为 0022-1100-0002），上行连接到 Device A 的 GigabitEthernet1/0/1 端口。
- IP phone B 的 MAC 地址为 0011-2200-0001，下行连接 PC B（MAC 地址为 0022-2200-0002），上行连接到 Device A 的 GigabitEthernet1/0/2 端口。
- Device A 使用 Voice VLAN 2 传输 IP phone A 产生的语音报文；使用 Voice VLAN 3 传输 IP phone B 产生的语音报文。
- GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 工作在自动模式，如果它们在 30 分钟内没有收到语音流，就将相应的 Voice VLAN 老化。

2. 组网图

图4-6 配置自动模式下 Voice VLAN 组网图



3. 配置步骤

创建 VLAN 2 和 VLAN 3。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
 Please wait... Done.
```

设置 Voice VLAN 的老化时间为 30 分钟。

```
[DeviceA] voice vlan aging 30
```

由于 GigabitEthernet1/0/1 端口可能会同时收到语音和数据两种流量，为了保证语音报文的质量以及带宽的高效利用，设置 Voice VLAN 工作在安全模式，即 Voice VLAN 只用于传输语音报文。（此步骤可省略，缺省情况下，Voice VLAN 工作在安全模式）

```
[DeviceA] voice vlan security enable
```

设置允许通过的 OUI 地址为 MAC 地址前缀为 0011-1100-0000 和 0011-2200-0000，即当报文的前缀为 0011-1100-0000 或 0011-2200-0000 时，Device A 会把它当成语音报文来处理。

```
[DeviceA] voice vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone
A
[DeviceA] voice vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone
B
```

将端口 GigabitEthernet1/0/1 设定为 Hybrid 端口。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

将端口 GigabitEthernet1/0/1 上 Voice VLAN 的工作模式设置为自动模式。（可选，缺省情况下，端口的 Voice VLAN 工作在自动模式。）

```
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

使能端口 Voice VLAN 功能。

```
[DeviceA-GigabitEthernet1/0/1] voice vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在 GigabitEthernet1/0/2 上进行相应的配置。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
[DeviceA-GigabitEthernet1/0/2] voice vlan mode auto
[DeviceA-GigabitEthernet1/0/2] voice vlan 3 enable
```

4. 显示和验证

显示当前系统支持的 OUI 地址、OUI 地址掩码和描述信息。

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-1100-0000  ffff-ff00-0000  IP phone A
0011-2200-0000  ffff-ff00-0000  IP phone B
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

显示当前 Voice VLAN 的状态。

```
<DeviceA> display voice vlan state
 Maximum of Voice VLANs: 128
 Current Voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled port and its mode:
PORT                        VLAN        MODE        COS        DSCP
 ------------------------------------------------------------------------
GigabitEthernet1/0/1          2           AUTO        6          46
GigabitEthernet1/0/2          3           AUTO        6          46
```

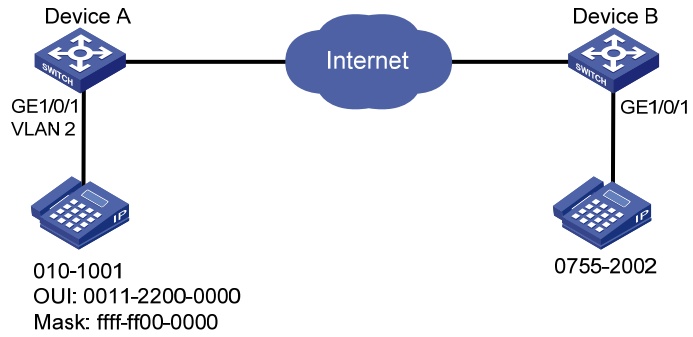
4.10.2 手动模式下Voice VLAN的配置举例

1. 组网需求

- 创建 VLAN 2 为 Voice VLAN，只允许语音报文通过。
- IP Phone 类型为 Untagged，接入端口是 Hybrid 类型端口 GigabitEthernet1/0/1。
- 端口 GigabitEthernet1/0/1 工作在手动模式，且允许 OUI 地址是 0011-2200-0000、掩码是 ffff-ff00-0000 的语音报文通过，描述字符为 test。

2. 组网图

图4-7 配置手动模式下 Voice VLAN 组网图



3. 配置步骤

设置 Voice VLAN 为安全模式，使得 Voice VLAN 端口只允许合法的语音报文通过。（可选，系统缺省为安全模式）

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

```
[DeviceA] voice vlan security enable
```

设置 OUI 地址 0011-2200-0000 是 Voice VLAN 的合法地址。

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

创建 VLAN 2。

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

设置端口 GigabitEthernet1/0/1 工作在手动模式。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice vlan mode auto
```

设置端口 GigabitEthernet1/0/1 为 Hybrid 类型。

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

设置 Voice VLAN 是端口 GigabitEthernet1/0/1 的缺省 VLAN，且在该端口允许通过的 Untagged VLAN 列表中。

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

使能端口 GigabitEthernet1/0/1 的 Voice VLAN 功能。

```
[DeviceA-GigabitEthernet1/0/1] voice vlan 2 enable
```

4. 显示与验证

显示当前系统支持的 OUI 地址、OUI 地址掩码和描述信息。

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-2200-0000  ffff-ff00-0000  test
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

显示当前 Voice VLAN 的状态。

```
<DeviceA> display voice vlan state
Maximum of Voice VLANs: 128
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE        COS        DSCP
 ------------------------------------------------------------------------
 GigabitEthernet1/0/1        2           MANUAL       6          46
```

目 录

1 GVRP配置

1.1 GVRP简介

GARP（Generic Attribute Registration Protocol，通用属性注册协议）作为一个属性注册协议的载体，可以用来传播属性。遵循 GARP 协议的应用实体称为 GARP 应用，GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）就是 GARP 的应用之一，用于注册和注销 VLAN 属性。下面首先了解一下 GARP 的相关内容。

1.1.1 GARP简介

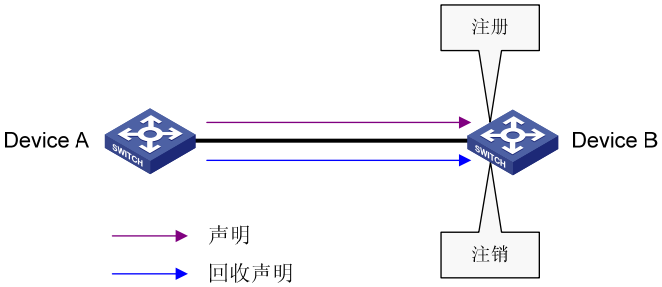
GARP 提供了一种机制，用于协助同一局域网内各成员之间分发、传播和注册某种信息（如 VLAN、组播地址等）。

1. GARP实现机制

设备上每一个参与协议的端口都可以视为一个应用实体，当 GARP 应用（如 GVRP）在端口上启动之后，该端口就可视为一个 GARP 应用实体。

通过GARP机制，一个GARP应用实体上的配置信息会迅速传遍整个局域网。如 图 1-1 所示，GARP应用实体通过发送出的声明或回收声明来通知其它GARP应用实体来注册或注销自己的属性信息，并根据其它实体发来的声明或回收声明来注册或注销对方的属性信息。

图1-1 GARP 实现机制示意图



譬如，GVRP 协议实现 VLAN 属性注册和注销的方式如下：

- 当端口收到一个 VLAN 属性的声明时，该端口将注册该声明中所包含的 VLAN 属性（即，该端口加入到该 VLAN 中）。
- 当端口收到一个 VLAN 属性的回收声明时，该端口将注销该声明中所包含的 VLAN 属性（即，该端口退出该 VLAN）。

2. GARP消息

GARP 应用实体之间的信息交换借助于传递各种消息来完成，主要包括 Join 消息、Leave 消息和 LeaveAll 消息，它们通过互相配合来确保信息的注册或注销。由于 GVRP 基于 GARP 实现，因此，GVRP 也是通过 GARP 消息进行信息交互的。

(1) Join 消息

当一个 GARP 应用实体希望其它 GARP 实体注册自己的属性信息时，它会发送 Join 消息；当收到来自其它实体的 Join 消息或由于本实体静态配置了某些属性而需要其它实体进行注册时，它也会发送 Join 消息。Join 消息又分为 JoinEmpty 和 JoinIn 两种，二者的区别如下：

- JoinEmpty：用于声明一个本身没有注册的属性。
- JoinIn：用于声明一个本身已经注册的属性。

(2) Leave 消息

当一个 GARP 应用实体希望其它 GARP 实体注销自己的属性信息时，它会发送 Leave 消息；当收到来自其它实体的 Leave 消息或由于本实体静态注销了某些属性而需要其它实体进行注销时，它也会发送 Leave 消息。Leave 消息又分为 LeaveEmpty 和 LeaveIn 两种，二者的区别如下：

- LeaveEmpty：用于注销一个本身没有注册的属性。
- LeaveIn：用于注销一个本身已经注册的属性。

(3) LeaveAll 消息

每个 GARP 应用实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，它就会发送 LeaveAll 消息来注销所有的属性，从而使其它 GARP 实体重新注册属性信息；当收到来自其它实体的 LeaveAll 消息时，它也会发送 LeaveAll 消息。在发送 LeaveAll 消息同时重新启动 LeaveAll 定时器，开始新的一轮循环。

3. GARP定时器

GARP 定义了四种定时器，用于控制各种 GARP 消息的发送。

说明

- GARP 定时器值的改变将应用于同一局域网内所有运行的 GARP 应用（如 GVRP）上。
- 设备的每个端口上都独立维护自己的 Hold 定时器、Join 定时器和 Leave 定时器，而每台设备则只在全局维护一个 LeaveAll 定时器。
- Hold定时器、Join定时器、Leave定时器和LeaveAll定时器的取值范围之间存在着相互制约的关系，具体情况请参见 表 1-5。

---

(1) Hold 定时器

Hold 定时器用来控制 GARP 消息（包括 Join 消息和 Leave 消息）的发送。当 GARP 应用实体的属性改变或收到来自其它实体的 GARP 消息时，不会立即将该消息发送出去，而是在 Hold 定时器超时后，将此时段内待发送的所有 GARP 消息封装成尽可能少的报文发送出去，这样就减少了报文的发送数量，从而节省了带宽资源。

(2) Join 定时器

Join 定时器用来控制 Join 消息的发送。为了保证 Join 消息能够可靠地传输到其它实体，GARP 应用实体在发出 Join 消息后将等待一个 Join 定时器的时间间隔：如果在该定时器超时前收到了其它实体发来的 JoinIn 消息，它便不会重发该 Join 消息；否则，它将重发一次该 Join 消息。

说明

并非每个属性都有自己的 Join 定时器，而是每个 GARP 应用实体共用一个。因此，Join 定时器应该足够大，以保证所有属性能够在一次声明过程中全部发送出去。

---

(3) Leave 定时器

Leave 定时器用来控制属性的注销。当 GARP 应用实体希望其它实体注销自己的某属性信息时会发送 Leave 消息，收到该消息的实体将启动 Leave 定时器，只有在该定时器超时前没有收到该属性信息的 Join 消息，该属性信息才会被注销。

(4) LeaveAll 定时器

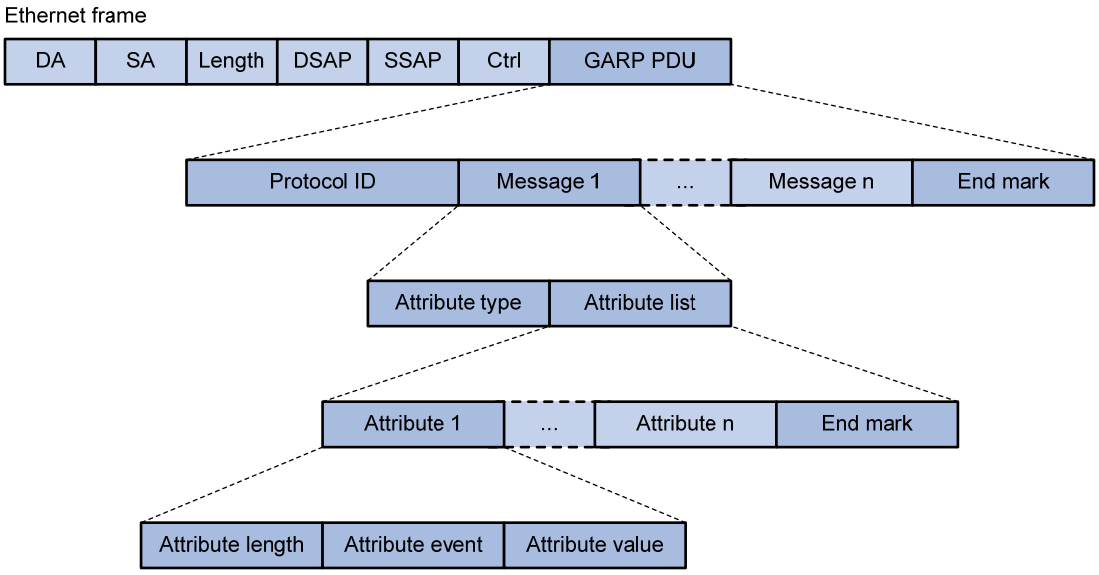
每个 GARP 应用实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，GARP 应用实体就会对外发送 LeaveAll 消息，从而使其它实体重新注册属性信息。随后再重新启动 LeaveAll 定时器，开始新一轮的循环。收到 LeaveAll 消息的实体将重新启动所有的定时器，其中也包括 LeaveAll 定时器。

说明

- 每一次 LeaveAll 定时器超时，都会引起全网所有属性的注销。由于其影响范围很广，所以 LeaveAll 定时器的值不能太小，其取值必须大于所有端口上 Leave 定时器的值，并建议用户配置的 LeaveAll 定时器值不要小于其缺省值（即 1000 厘秒）。
- 尽管全网各设备上 LeaveAll 定时器的值有可能不同，但这些设备都将以 LeaveAll 定时器的全网最小值为周期来发送 LeaveAll 消息。这是由于各设备在收到 LeaveAll 消息后都会清零自己的 LeaveAll 定时器，而只有具备最小 LeaveAll 定时器值的设备才来得及将 LeaveAll 消息发出，因此实际上只有具备全网最小值的 LeaveAll 定时器才会生效。

4. GARP协议报文封装格式

图1-2 GARP 协议报文封装格式



如 图 1-2 所示，GARP协议报文采用IEEE 802.3 Ethernet封装格式，其中主要字段的说明如 表 1-1 所示。

表1-1 GARP 协议报文主要字段说明

字段	说明
GARP PDU	封装在GARP协议报文中的GARP PDU（Protocol Data Unit，协议数据单元）
Protocol ID	协议编号，GARP PDU的协议编号为0x0001
Message	属性消息，每个消息都由Attribute type和Attribute list两个字段构成
End mark	结束标志，取值为0x00
Attribute type	属性类型，由具体的GARP应用来定义。取值为0x01时表示VLAN ID，代表GVRP应用
Attribute list	属性列表，由多个属性构成
Attribute	属性，每个属性都由Attribute length、Attribute event和Attribute value这三个字段构成
Attribute length	属性长度（包括本字段在内），取值范围为2～255，单位为字节

字段	说明
Attribute event	属性所描述的事件，取值及含义如下： • 0x00：表示 LeaveAll 事件 • 0x01：表示 JoinEmpty 事件 • 0x02：表示 JoinIn 事件 • 0x03：表示 LeaveEmpty 事件 • 0x04：表示 LeaveIn 事件 • 0x05：表示 Empty 事件
Attribute value	属性取值。GVRP应用的属性取值为VLAN ID，但当Attribute event字段的取值为0x00时（即LeaveAll事件），本字段无效

GARP 协议报文以特定组播 MAC 地址为目的 MAC，如 GVRP 的目的 MAC 地址为 01-80-C2-00-00-21。当设备在收到 GARP 应用实体的报文后，会根据其目的 MAC 地址分发给不同的 GARP 应用进行处理。

1.1.2 GVRP实现

1. GVRP概述

GVRP 是 GARP 应用的一种，它基于 GARP 的工作机制来维护设备中的 VLAN 动态注册信息，并将该信息向其它设备传播：当设备启动了 GVRP 之后，就能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员及这些 VLAN 成员可通过哪个端口到达等；此外，设备还能够将本地的 VLAN 注册信息向其它设备传播，从而使同一局域网内所有设备的 VLAN 信息都达成一致。

GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

2. GVRP的注册模式

我们将通过手工创建的 VLAN 称为静态 VLAN，通过 GVRP 协议创建的 VLAN 称为动态 VLAN。GVRP 有三种注册模式，不同注册模式对静态 VLAN 和动态 VLAN 的处理方式也不同。

(1) Normal 模式

该模式下的端口允许进行动态 VLAN 的注册或注销，并允许发送动态和静态 VLAN 的声明。

(2) Fixed 模式

该模式下的端口禁止进行动态 VLAN 的注册或注销，且只允许发送静态 VLAN 的声明。也就是说，该模式下的 Trunk 端口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手工创建的那部分 VLAN。

(3) Forbidden 模式

该模式下的端口禁止进行动态 VLAN 的注册或注销，且只允许发送 VLAN 1 的声明。也就是说，该模式下的 Trunk 端口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN 1。

1.1.3 协议规范

与 GVRP 相关的协议规范有：

- IEEE 802.1Q：Virtual Bridged Local Area Networks

1.2 GVRP配置任务简介

表1-2 GVRP 配置任务简介

配置任务	说明	详细配置
配置GVRP功能	必选	1.3
配置GARP定时器	可选	1.4

说明

对于 GVRP 的相关配置来说:

- 二层以太网端口视图下或二层聚合接口视图下的配置只对当前接口有效；端口组视图下的配置对当前端口组中的所有端口有效。
- 聚合成员端口上的配置只有当该端口退出聚合组后才会生效。

1.3 配置GVRP功能

在使能端口的 GVRP 功能之前，必须先全局使能 GVRP 功能。此外，GVRP 功能只能配置在 Trunk 端口上，并且需要通过配置来保证所有动态注册的 VLAN 都能够从该端口通过。

表1-3 配置 GVRP 功能

操作		命令	说明
进入系统视图		**system-view**	-
全局使能GVRP功能		**gvrp**	必选 缺省情况下，全局的GVRP功能处于关闭状态
进入相应视图	进入以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型为Trunk类型		**port link-type trunk**	必选 缺省情况下，端口的链路类型为Access类型
允许所有VLAN都通过当前Trunk端口		**port trunk permit vlan all**	必选 缺省情况下，Trunk端口只允许VLAN 1通过
使能端口上的GVRP功能		**gvrp**	必选 缺省情况下，端口上的GVRP功能处于关闭状态
配置GVRP端口的注册模式		**gvrp registration** { **fixed** | **forbidden** | **normal** }	可选 缺省情况下，GVRP端口的注册模式为Normal模式

说明

- 有关 **port link-type trunk** 和 **port trunk permit vlan all** 命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。
- GVRP 功能与业务环回功能互斥，两者不可以同时应用。
- GVRP 功能只能与 STP、RSTP 或 MSTP CIST 配合使用，而无法与 PVST 配合使用。在与 MSTP CIST 配合使用时，CIST 上被 MSTP 阻塞的端口将不能收发 GVRP 协议报文。有关 STP、RSTP、MSTP CIST 和 PVST 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。
- 建议不要同时启用远程端口镜像功能和 GVRP 功能，否则 GVRP 可能将远程镜像 VLAN 注册到不希望的端口上，此时在镜像目的端口就会收到很多不必要的报文。有关端口镜像的详细介绍，请参见“网络管理和监控配置指导”中的“端口镜像”。
- 在二层聚合接口上启用了 GVRP 功能后，会同时在二层聚合接口和对应的所有选中成员端口上进行动态 VLAN 的注册或注销。

1.4 配置GARP定时器

在配置 GARP 定时器时：

- LeaveAll 定时器的配置将对所有端口都生效；
- Hold 定时器、Join 定时器和 Leave 定时器的配置只对所配置的端口生效。

表1-4 配置 GARP 定时器

操作		命令	说明
进入系统视图		**system-view**	-
配置LeaveAll定时器		**garp timer leaveall** *timer-value*	可选 缺省情况下，LeaveAll定时器的值为1000厘秒
进入相关视图	进入以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置Hold定时器		**garp timer hold** *timer-value*	可选 缺省情况下，Hold定时器的值为10厘秒
配置Join定时器		**garp timer join** *timer-value*	可选 缺省情况下，Join定时器的值为20厘秒
配置Leave定时器		**garp timer leave** *timer-value*	可选 缺省情况下，Leave定时器的值为60厘秒

如 表 1-5 所示，各GARP定时器的取值范围之间存在着相互制约的关系：

- 当配置某定时器时，如果配置值超出了该定时器当前有效的取值范围，则该配置无效。用户可以通过改变相关定时器的值来重新进行配置。
- 当用户欲恢复各定时器的值为缺省值时，须按照 Hold 定时器->Join 定时器->Leave 定时器->LeaveAll 定时器的顺序依次恢复。

表1-5 各 GARP 定时器取值范围间的制约关系

定时器	取值下限	取值上限
Hold定时器	10厘秒	小于等于Join定时器值的一半
Join定时器	大于等于Hold定时器值的两倍	小于Leave定时器值的一半
Leave定时器	大于Join定时器值的两倍	小于LeaveAll定时器的值
LeaveAll定时器	大于所有端口上Leave定时器的值	32765厘秒

说明

过小的 LeaveAll 定时器值可能会影响通过 GVRP 学习到的动态 VLAN 的稳定性，建议 LeaveAll 定时器的取值不要小于其缺省值（即 1000 厘秒）。

1.5 GVRP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 GARP 或 GVRP 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 GARP 的统计信息。

表1-6 GVRP 显示和维护

操作	命令
显示端口上GARP的统计信息	**display garp statistics** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口上各GARP定时器的取值	**display garp timer** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口上GVRP本地VLAN的信息	**display gvrp local-vlan interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口上指定VLAN内各GVRP状态机的信息	**display gvrp state interface** *interface-type interface-number* **vlan** *vlan-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Trunk端口上GVRP的统计信息	**display gvrp statistics** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GVRP的全局状态信息	**display gvrp status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口上当前的动态VLAN操作信息	**display gvrp vlan-operation interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除端口上GARP的统计信息	**reset garp statistics** [**interface** *interface-list*]

1.6 GVRP典型配置举例

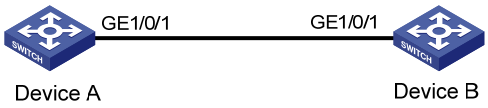
1.6.1 GVRP Normal注册模式配置举例

1. 组网需求

- Device A 和 Device B 分别通过各自的端口 GigabitEthernet1/0/1 相连。
- 通过启用 GVRP 功能，并配置 GVRP 的注册模式为 Normal 模式，来实现 Device A 和 Device B 之间所有动态和静态 VLAN 的注册和注销。

2. 组网图

图1-3 GVRP Normal 注册模式配置组网图



3. 配置步骤

(1) 配置 Device A

全局使能 GVRP 功能。

```
<DeviceA> system-view
[DeviceA] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能。

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 2。

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

(2) 配置 Device B

使能全局的 GVRP 功能。

```
<DeviceB> system-view
[DeviceB] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能。

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 3。

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

(3) 检验配置效果

通过使用 **display gvrp local-vlan** 命令可以查看端口上 GVRP 本地 VLAN 的信息，例如：

查看 Device A 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceA] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default),2-3
```

由此可见，VLAN 1 的信息、在本设备上创建 VLAN 2 的静态 VLAN 信息，以及在 Device B 上创建 VLAN 3 的动态 VLAN 信息都已通过 GVRP 协议进行了注册。

查看 Device B 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceB] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default),2-3
```

由此可见，VLAN 1 的信息、在本设备上创建 VLAN 3 的静态 VLAN 信息，以及在 Device A 上创建 VLAN 2 的动态 VLAN 信息都已通过 GVRP 协议进行了注册。

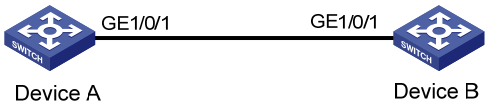
1.6.2 GVRP Fixed注册模式配置举例

1. 组网需求

- Device A 和 Device B 分别通过各自的端口 GigabitEthernet1/0/1 相连。
- 通过启用 GVRP 功能，并配置 GVRP 的注册模式为 Fixed 模式，来实现 Device A 和 Device B 之间所有静态 VLAN 的注册和注销。

2. 组网图

图1-4 GVRP Fixed 注册模式配置组网图



3. 配置步骤

(1) 配置 Device A

全局使能 GVRP 功能。

```
<DeviceA> system-view
[DeviceA] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能，并配置其注册模式为 Fixed 模式。

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] gvrp registration fixed
[DeviceA-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 2。

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

(2) 配置 Device B

使能全局的 GVRP 功能。

```
<DeviceB> system-view
[DeviceB] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能，并配置其注册模式为 Fixed 模式。

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] gvrp registration fixed
[DeviceB-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 3。

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

(3) 检验配置效果

通过使用 **display gvrp local-vlan** 命令可以查看端口上 GVRP 本地 VLAN 的信息，例如：

查看 Device A 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceA] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default), 2
```

由此可见，VLAN 1 的信息以及在本设备上创建 VLAN 2 的静态 VLAN 信息已通过 GVRP 协议进行了注册，而在 Device B 上创建 VLAN 3 的动态 VLAN 信息并未通过 GVRP 协议进行注册。

查看 Device B 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceB] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default), 3
```

由此可见，VLAN 1 的信息以及在本设备上创建 VLAN 3 的静态 VLAN 信息已通过 GVRP 协议进行了注册，而在 Device A 上创建 VLAN 2 的动态 VLAN 信息并未通过 GVRP 协议进行注册。

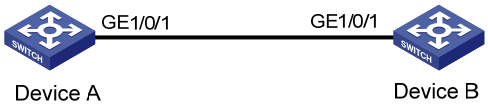
1.6.3 GVRP Forbidden注册模式配置举例

1. 组网需求

- Device A 和 Device B 分别通过各自的端口 GigabitEthernet1/0/1 相连。
- 通过启用 GVRP 功能，并配置 GVRP 的注册模式为 Forbidden 模式，来阻止 Device A 和 Device B 之间除 VLAN 1 以外所有 VLAN 的注册和注销。

2. 组网图

图1-5 GVRP Forbidden 注册模式配置组网图



3. 配置步骤

(1) 配置 Device A

全局使能 GVRP 功能。

```
<DeviceA> system-view
[DeviceA] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能，并配置其注册模式为 Forbidden 模式。

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] gvrp registration forbidden
[DeviceA-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 2。

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

(2) 配置 Device B

使能全局 GVRP。

```
<DeviceB> system-view
[DeviceB] gvrp
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

在端口 GigabitEthernet1/0/1 上使能 GVRP 功能，并配置其注册模式为 Forbidden 模式。

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] gvrp registration forbidden
[DeviceB-GigabitEthernet1/0/1] quit
```

配置静态 VLAN 3。

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

(3) 检验配置效果

通过使用 **display gvrp local-vlan** 命令可以查看端口上 GVRP 本地 VLAN 的信息，例如：

查看 Device A 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceA] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default)
```

由此可见，除 VLAN 1 的信息外，在本设备上创建 VLAN 2 的静态 VLAN 信息，以及在 Device B 上创建 VLAN 3 的动态 VLAN 信息都未通过 GVRP 协议进行注册。

查看 Device B 的端口 GigabitEthernet1/0/1 上 GVRP 本地 VLAN 的信息。

```
[DeviceB] display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default)
```

由此可见，除 VLAN 1 的信息外，在本设备上创建 VLAN 3 的静态 VLAN 信息，以及在 Device A 上创建 VLAN 2 的动态 VLAN 信息都未通过 GVRP 协议进行注册。

目 录

1 QinQ配置

1.1 QinQ简介

QinQ 是 802.1Q in 802.1Q 的简称，它是基于 IEEE 802.1Q 技术的一种二层隧道协议，通过将用户的私网报文封装上外层 VLAN Tag，使其携带两层 VLAN Tag 穿越运营商的骨干网络（又称公网），从而为用户提供了一种比较简单的二层 VPN 隧道技术，也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成为了可能。

1.1.1 QinQ的产生背景和优点

IEEE 802.1Q 定义的 VLAN ID 域只有 12 个比特，最多可以表示 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。

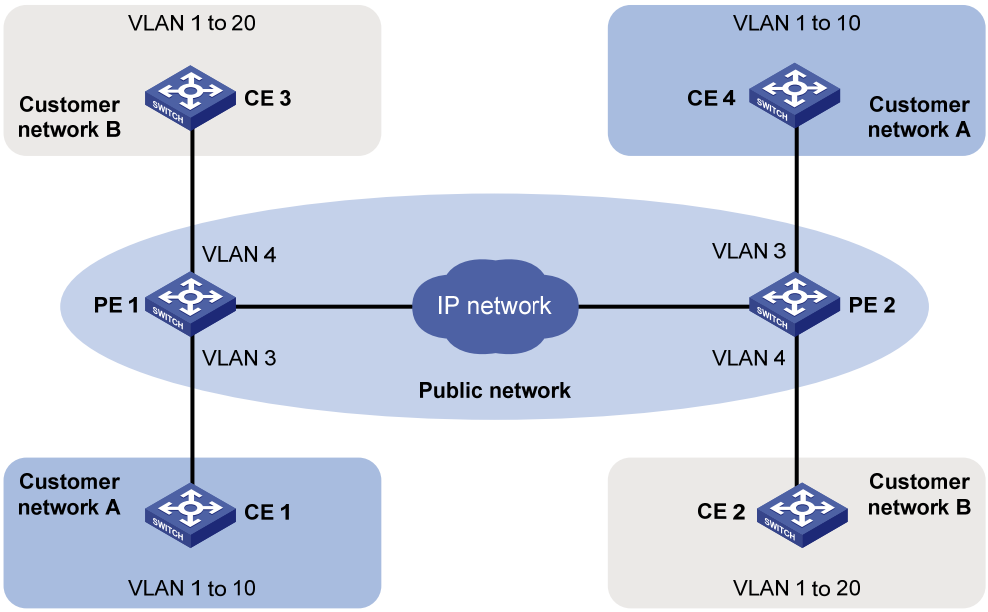
QinQ 使整个网络最多可提供 4094×4094 个 VLAN，从而满足了城域网对 VLAN 数量的需求。它具备以下优点：

- 缓解公网 VLAN ID 资源日益紧缺的问题。
- 用户可以规划自己的私网 VLAN ID，不会导致与公网 VLAN ID 冲突。
- 为小型城域网和企业网提供了一种简单、灵活的二层 VPN 解决方案。
- 当运营商升级网络时，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。

1.1.2 QinQ的实现原理

在公网的传输过程中，设备只根据外层 VLAN Tag 转发报文，并将报文的源 MAC 地址表项学习到外层 VLAN Tag 所在 VLAN 的 MAC 地址表中，而用户的私网 VLAN Tag 将被当作报文的数据部分进行传输。

图1-1 QinQ 典型应用组网图



如 图 1-1 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。当用户网络A和B中带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VLAN Tag。这样，来自不同用户网

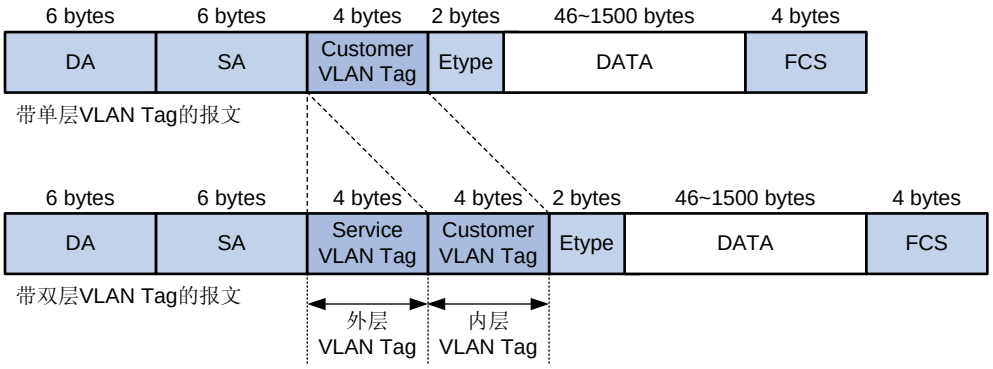
络的报文在运营商网络中传输时被完全分开，即使这些用户网络各自的VLAN范围存在重叠，在运营商网络中传输时也不会产生冲突。当报文穿过运营商网络，到达运营商网络另一侧PE设备后，报文会被剥离运营商网络为其添加的公网VLAN Tag，然后再传送给用户网络的CE设备。

1.1.3 QinQ的报文结构

如 图 1-2 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，依靠该 Tag 在私网中传送 QinQ 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，依靠该 Tag 在公网中传送 QinQ 报文，内层 VLAN Tag 在公网中被屏蔽。

图1-2 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）。

1.1.4 QinQ的实现方式

QinQ 的实现方式可分为以下两种：

1. 基本QinQ

基本 QinQ 是基于端口方式实现的。当端口上配置了基本 QinQ 功能后，不论从该端口收到报文是否带有 VLAN Tag，设备都会为该报文打上本端口缺省 VLAN 的 Tag：

- 如果收到的是带有 VLAN Tag 的报文，该报文就成为带双 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。

2. 灵活QinQ

灵活 QinQ 是基于端口与 VLAN 相结合的方式实现的，它对 QinQ 的功能进行了扩展，是对 QinQ 的一种更灵活的实现。灵活 QinQ 除了能实现所有基本 QinQ 的功能外，对于从同一个端口收到的报文，还可以根据 VLAN 的不同进行不同的操作，包括：

- 为具有不同内层 VLAN ID 的报文添加不同的外层 VLAN Tag。
- 根据报文内层 VLAN 的 802.1p 优先级标记外层 VLAN 的 802.1p 优先级。
- 在添加外层 VLAN Tag 的同时，还可修改内层的 VLAN ID。

通过使用灵活 QinQ 技术，在能够隔离运营商网络和用户网络的同时，又能够提供丰富的业务特性和更加灵活的组网能力。

1.1.5 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

1.2 QinQ配置任务简介

表1-1 QinQ 配置任务简介

配置任务		说明	详细配置
配置基本QinQ功能	使能基本QinQ功能	必选	1.3.1
	配置VLAN透传功能	可选	1.3.2
配置灵活QinQ功能	配置外层VLAN Tag添加策略	三者至少选其一	1.4.1
	配置内、外层VLAN Tag中802.1p优先级的映射关系		1.4.2
	配置内层VLAN ID替换关系		1.4.3
配置VLAN Tag的TPID值		可选	1.5

说明

- QinQ 功能只需在运营商网络进行配置，用户网络不需进行配置。
- 对于 QinQ 的相关配置来说，以太网端口视图下的配置只对当前端口有效；二层聚合接口视图下的配置对当前接口及其对应聚合组中的所有成员端口都有效；端口组视图下的配置对当前端口组中的所有端口有效。
- 所有的 QinQ 相关配置都不能在镜像反射端口上进行配置。有关镜像反射端口的详细介绍，请参见“网络管理和监控配置指导”中的“端口镜像”。
- 开启基本 QinQ 的端口，需要配置允许端口的缺省 VLAN 通过，配置灵活 QinQ 功能的端口，需要配置允许 QinQ 外层 VLAN 通过。

1.3 配置基本QinQ功能

1.3.1 使能基本QinQ功能

使能了基本 QinQ 功能的端口将为其收到的报文添加新的 VLAN Tag，该 VLAN Tag 即该端口缺省 VLAN 的 Tag。

表1-2 使能基本 QinQ 功能

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
进入相应视图	进入二层以太网接口或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口的基本QinQ功能		**qinq enable**	必选 缺省情况下，端口的基本QinQ功能处于关闭状态

1.3.2 配置VLAN透传功能

端口上使能了基本QinQ功能后，从该端口收到的报文就会被打上本端口缺省VLAN的Tag。而VLAN透传功能则可使端口在收到带有指定 VLAN Tag 的报文后，不为其添加外层 VLAN Tag 而直接在运营商网络中传输。

表1-3 配置 VLAN 透传功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型		**port link-type** { **hybrid** | **trunk** }	-
配置端口允许透传VLAN和QinQ外层VLAN通过	当端口类型为Hybrid端口	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	二者必选其一
	当端口类型为Trunk端口	**port trunk permit vlan** { *vlan-id-list* | **all** }	
使能端口的基本QinQ功能		**qinq enable**	必选 缺省情况下，端口的基本QinQ功能处于关闭状态
配置端口的VLAN透传功能		**qinq transparent-vlan** *vlan-list*	必选 缺省情况下，端口没有配置VLAN透传功能

注意

- 配置 VLAN 透传功能时，还需在报文传输路径的所有设备上都配置允许透传的 VLAN 通过。
- 配置了端口对指定 VLAN 的报文进行透传后，请勿在该端口上对这些 VLAN 再进行 VLAN 映射的相关配置。有关 VLAN 映射的详细介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射”。

1.4 配置灵活QinQ功能

1.4.1 配置外层VLAN Tag添加策略

基本 QinQ 功能添加的外层 VLAN Tag 是端口缺省 VLAN 的 Tag，灵活的 QinQ 功能则可以为不同的内层 VLAN Tag 添加不同的外层 VLAN Tag。

用户可以通过以下两种方式来配置外层 VLAN Tag 的添加策略：

- 基于端口配置外层 VLAN Tag 的添加策略
- 基于 QoS 策略配置外层 VLAN Tag 的添加策略

两种方式的配置效果一致，如果在同一端口上同时使用两种方式配置了不同的外层 VLAN Tag 添加策略，则通过 QoS 策略方式的配置生效。

1. 基于端口配置外层VLAN Tag的添加策略

在开启端口的灵活 QinQ 功能前，需要先开启端口的基本 QinQ 功能。端口上同时配置了基本 QinQ 和灵活 QinQ 功能后，满足灵活 QinQ 配置的报文将按灵活 QinQ 处理，不满足灵活 QinQ 配置的报文将按基本 QinQ 处理。

表1-4 配置外层 VLAN Tag 的添加策略

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图或二层聚合端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口的基本QinQ功能		**qinq enable**	必选 缺省情况下，端口的基本QinQ功能处于关闭状态
进入QinQ视图，并配置端口添加的外层VLAN Tag		**qinq vid** *vlan-id*	必选 缺省情况下，端口添加的外层VLAN Tag是端口缺省VLAN的Tag
配置需添加外层VLAN Tag的内层VLAN Tag		**raw-vlan-id inbound** { **all** | *vlan-list* }	必选

注意

一个内层 VLAN Tag 只能对应一个外层 VLAN Tag。如果用户想改变报文的外层 VLAN Tag，需要先删除旧的外层 VLAN Tag 配置，然后再配置新的外层 VLAN Tag。

2. 基于QoS策略配置外层VLAN Tag的添加策略

本系列交换机的灵活 QinQ 功能也可以通过 QoS 策略的方式实现，通过配置匹配报文原有 VLAN Tag 的流分类和封装外层 VLAN Tag 的流行为，并将其在 QoS 策略中进行关联，然后应用到连接用户的端口，即可以实现根据报文内层 VLAN 封装外层 VLAN Tag 的功能。

表1-5 配置外层 VLAN Tag 的添加策略

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
创建类并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	必选 缺省情况下，类视图下各规则之间的关系为**and**，即逻辑与
配置匹配报文的规则，即指定报文的内层VLAN ID		**if-match customer-vlan-id** *vlan-id-list*	必选
退出至系统视图		**quit**	-
创建流行为并进入流行为视图		**traffic behavior** *behavior-name*	必选
定义流行为，即指定为报文封装的外层VLAN ID		**nest top-most vlan-id** *vlan-id*	必选
退出至系统视图		**quit**	-
创建QoS策略并进入QoS策略视图		**qos policy** *policy-name*	必选
将之前定义的流分类和指定的流行为进行绑定，组成QoS策略		**classifier** *classifier-name* **behavior** *behavior-name*	必选
退出至系统视图		**quit**	-
进入连接用户的以太网端口视图或端口组视图	进入以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
开启端口的基本QinQ功能		**qinq enable**	必选
在端口的入方向应用QoS策略		**qos apply policy** *policy-name* **inbound**	必选

说明

- 开启灵活 QinQ 前必须先配置端口的基本 QinQ 功能，灵活 QinQ 的优先级高于基本 QinQ，即当端口接收的报文不能匹配流分类规则的情况下，才根据基本 QinQ 的功能封装外层 VLAN Tag。
- 关于 QoS 策略的更多详细信息，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1.4.2 配置内、外层VLAN Tag中 802.1p优先级的映射关系

本系列交换机可以通过 QoS 策略来实现以下两种内、外层 VLAN Tag 的 802.1p 优先级映射功能：

- 根据内层 VLAN Tag 的 802.1p 优先级或内层 VLAN ID 来标记外层 VLAN Tag 中的 802.1p 优先级
- 将内层 VLAN Tag 的 802.1p 优先级复制到外层 VLAN Tag 中的 802.1p 优先级

表1-6 配置内外层 VLAN Tag 的 802.1p 优先级映射关系

操作	命令	说明
进入系统视图	**system-view**	-
创建类并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	必选 缺省情况下，类视图下各规则之间的关系为**and**，即逻辑与

操作		命令	说明
配置匹配报文的规则	配置内层VLAN ID作为匹配规则	**if-match customer-vlan-id** *vlan-id-list*	二者选其一
	配置内层VLAN Tag的802.1p优先级作为匹配规则	**if-match customer-dot1p** *8021p-list*	
退出至系统视图		**quit**	-
创建流行为并进入流行为视图		**traffic behavior** *behavior-name*	必选
定义流行为，即指定报文外层VLAN Tag的优先级	重标记外层VLAN Tag中的802.1p优先级	**remark dot1p** *8021p*	二者必选其一 用户可以根据需要选择不同的动作，实现内外层VLAN Tag的802.1p优先级的映射或复制功能
	将内层VLAN Tag的802.1p优先级复制到外层VLAN Tag中的802.1p优先级	**remark customer-dot1p-trust** **dot1p**	
退出至系统视图		**quit**	-
创建QoS策略并进入QoS策略视图		**qos policy** *policy-name*	必选
将之前定义的流分类和指定的流行为进行绑定，组成QoS策略		**classifier** *classifier-name* **behavior** *behavior-name*	必选
退出至系统视图		**quit**	-
进入连接用户网络的以太网端口视图或端口组视图	进入以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
开启端口的基本QinQ功能		**qinq enable**	必选
在端口的入方向应用QoS策略		**qos apply policy** *policy-name* **inbound**	必选

说明

- 在 S5500-HI 系列交换机上，如果没有使用上述两种方法重标记报文外层 VLAN Tag 的 802.1p 优先级，那么开启了 QinQ 或灵活 QinQ 的端口在信任报文的优先级的情况下，为报文封装外层 VLAN Tag 时，会将内层 VLAN Tag 的 802.1p 优先级复制到外层 VLAN Tag 的 802.1p 优先级，在不信任报文的优先级的情况下，会将接收报文的端口的端口优先级作为外层 VLAN Tag 的 802.1p 优先级（如果没有配置端口优先级，外层 VLAN Tag 的 802.1p 优先级为端口优先级缺省值 0）。
- 有关优先级信任模式的配置，请参见“ACL 和 QoS 配置指导”中的“优先级映射配置”。

1.4.3 配置内层VLAN ID替换关系

在设备连接用户网络的端口上应用基本 QinQ 功能或灵活 QinQ 配置外层 VLAN Tag 的添加策略可以为报文添加外层 VLAN Tag，但不能修改报文的内层 VLAN ID。如果需要修改报文的内层 VLAN ID，可以在设备连接运营商网络侧的端口上进行如下配置：

- 配置匹配报文内、外层 VLAN ID 的流分类；
- 配置修改报文内层 VLAN ID 的流行为；

- 将上述流分类和流行为在 QoS 策略中进行关联；
- 将 QoS 策略应用到设备连接运营商网络侧的端口的出方向上。

配置内层 VLAN ID 替换

操作		命令	说明
进入系统视图		**system-view**	-
创建类并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	必选 缺省情况下，类视图下各规则之间的关系为**and**，即逻辑与
配置匹配报文的规则，即指定报文的原始内层VLAN ID		**if-match customer-vlan-id** *vlan-id-list*	必选
配置匹配报文的规则，指定报文的外层VLAN ID		**if-match service-vlan-id** *vlan-id*	必选
退出至系统视图		**quit**	-
创建流行为并进入流行为视图		**traffic behavior** *behavior-name*	必选
定义流行为，即修改报文内层VLAN ID		**remark customer-vlan-id** *vlan-id*	必选
退出至系统视图		**quit**	-
创建QoS策略并进入QoS策略视图		**qos policy** *policy-name*	必选
将之前定义的流分类和指定的流行为进行绑定，组成QoS策略		**classifier** *classifier-name* **behavior** *behavior-name*	必选
退出至系统视图		**quit**	-
进入连接运营商网络的二层以太网端口视图或端口组视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入以太网端口后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
在端口的出方向应用QoS策略		**qos apply policy** *policy-name* **outbound**	必选

1.5 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携带有 VLAN Tag。使能 QinQ 或用户侧 QinQ 功能的端口（用户网络侧端口）根据全局配置的内层 VLAN Tag 的 TPID 值判断入报文是否携带 VLAN Tag，如果入报文的 TPID 值和全局配置的内层 VLAN Tag 的 TPID 值不同，设备认为报文没有携带 VLAN Tag。关于用户侧 QinQ 功能的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射配置”。

没有使能 QinQ 或用户侧 QinQ 功能的端口（运营商网络侧端口）根据端口配置的外层 VLAN Tag 的 TPID 值判断入报文是否携带 VLAN Tag。此外，由于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，配置了外层 VLAN Tag 的 TPID 值的端口会将出报文中外层 VLAN Tag 的 TPID 值修改为配置值，使发送到公网中的 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。

例如，PE 设备连接的用户网络侧设备设置报文的 TPID 值为 0x8200，PE 设备连接的运营商网络侧设备设置报文的 TPID 值为 0x9100，则 PE 设备应该在全局配置内层 VLAN Tag 的 TPID 值为 0x8200，在连接运营商网络侧端口配置外层 VLAN Tag 的 TPID 值 0x9100。

QinQ 端口为报文添加的外层 VLAN Tag 的 TPID 值是 0x8100。

1. 配置内层VLAN Tag的TPID值

内层 VLAN Tag 的 TPID 值应在 PE 设备上进行配置。

需要注意的是，配置内层 VLAN Tag 的 TPID 值仅用于判断入报文是否携带 VLAN Tag，不会对报文内层 VLAN Tag 的 TPID 值进行修改。

表1-7 配置内层 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值为0x8100

2. 配置外层VLAN Tag的TPID值

外层 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。

需要注意的是，设备不支持在同一端口上既配置外层 VLAN Tag 的 TPID 值，又使能 QinQ 功能或用户侧 QinQ 功能。

表1-8 配置外层 VLAN Tag 的 TPID 值

操作		命令	说明
进入系统视图		**system-view**	-
进入连接运营商网络的以太网端口视图、二层聚合端口视图或端口组视图	进入以太网端口视图或二层聚合端口组视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	
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

1.6 QinQ典型配置举例

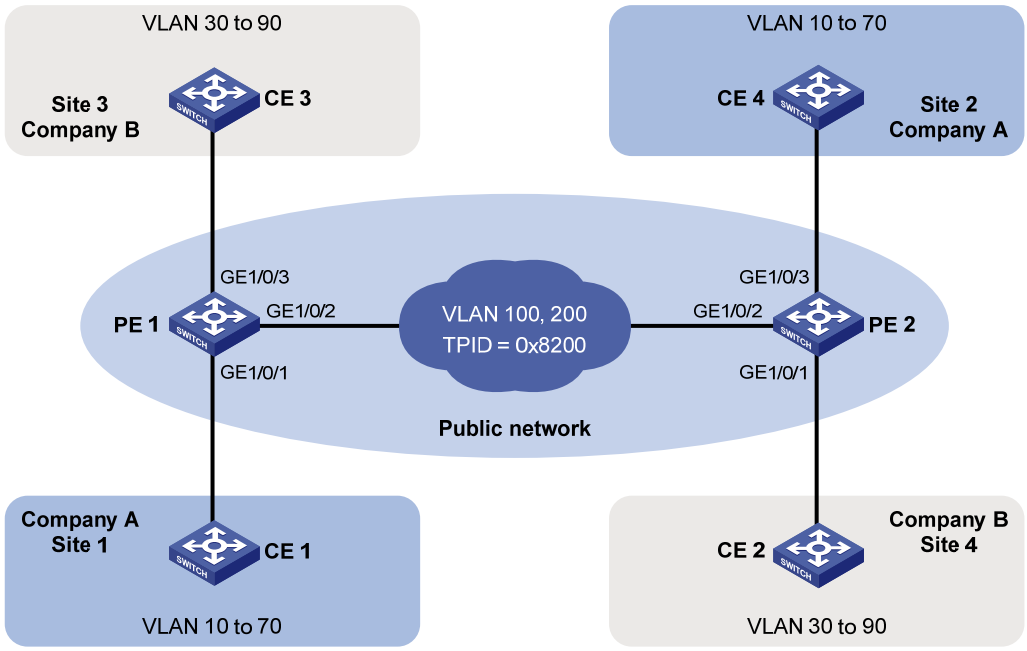
1.6.1 基本QinQ配置举例

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 基本 QinQ 配置组网图



3. 配置步骤

说明

用户必须通过配置保证运营商网络中的设备之间允许 QinQ 报文通过。

(1) 配置 PE 1

- 配置端口 GigabitEthernet1/0/1

配置端口为 Trunk 端口，且允许 VLAN 100 的报文通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100
```

配置端口的缺省 VLAN 为 VLAN 100。

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

使能端口的基本 QinQ 功能。

```
[PE1-GigabitEthernet1/0/1] qinq enable
[PE1-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

- 配置端口 GigabitEthernet1/0/3

配置端口为 Trunk 端口，且允许 VLAN 200 的报文通过。

```
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] port link-type trunk
[PE1-GigabitEthernet1/0/3] port trunk permit vlan 200
```

配置端口的缺省 VLAN 为 VLAN 200。

```
[PE1-GigabitEthernet1/0/3] port trunk pvid vlan 200
```

使能端口的基本 QinQ 功能。

```
[PE1-GigabitEthernet1/0/3] qinq enable
[PE1-GigabitEthernet1/0/3] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet1/0/1

配置端口为 Trunk 端口，且允许 VLAN 200 的报文通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 200
```

配置端口的缺省 VLAN 为 VLAN 200。

```
[PE2-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/1] qinq enable
[PE2-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] quit
```

- 配置端口 GigabitEthernet1/0/3

配置端口为 Trunk 端口，且允许 VLAN 100 的报文通过。

```
[PE2] interface gigabitethernet 1/0/3
[PE2-GigabitEthernet1/0/3] port link-type trunk
[PE2-GigabitEthernet1/0/3] port trunk permit vlan 100
```

配置端口的缺省 VLAN 为 VLAN 100。

```
[PE2-GigabitEthernet1/0/3] port trunk pvid vlan 100
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/3] qinq enable
[PE2-GigabitEthernet1/0/3] 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 200 的报文携带 VLAN Tag 通过。

1.6.2 VLAN透传配置举例

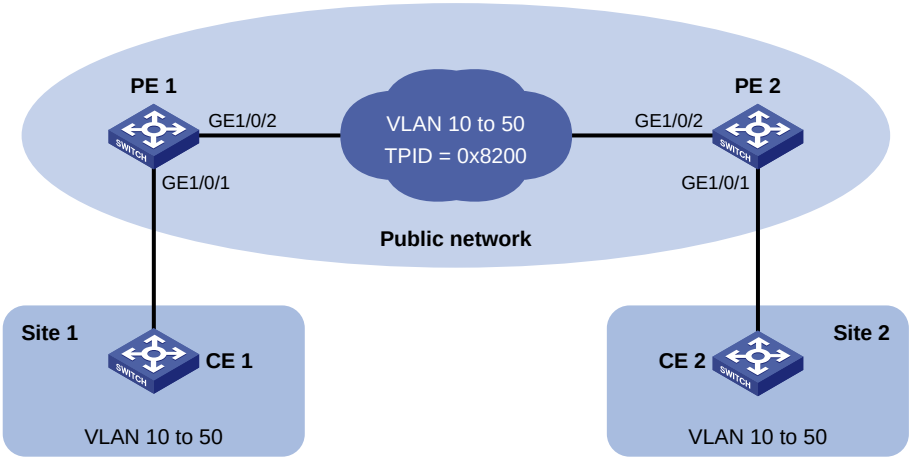
1. 组网需求

- 某公司的两个分支机构 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 10～50。

- 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，使这两个分支机构之间不利用运营商提供的 VLAN 就能实现互通。

2. 组网图

图1-4 VLAN 透传配置组网图



3. 配置步骤

说明

用户必须通过配置保证运营商网络中的设备之间允许 QinQ 报文通过。

(1) 配置 PE 1

- 配置端口 GigabitEthernet1/0/1

配置端口为 Trunk 端口，且允许 VLAN 10～50 的报文通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 10 to 50
```

使能端口的基本 QinQ 功能。

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

配置端口对 VLAN 10～50 的报文进行透传。

```
[PE1-GigabitEthernet1/0/1] qinq transparent-vlan 10 to 50
[PE1-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

配置端口为 Trunk 端口，且允许 VLAN 10～50 的报文通过。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 10 to 50
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet1/0/1

配置端口为 Trunk 端口，且允许 VLAN 10～50 的报文通过。

```
<PE2> system-view
```

```
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 10 to 50
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

配置端口对 VLAN 10～50 的报文进行透传。

```
[PE2-GigabitEthernet1/0/1] qinq transparent-vlan 10 to 50
[PE2-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

配置端口为 Trunk 端口，且允许 VLAN 10～50 的报文通过。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 10 to 50
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] 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 10～50 的报文携带 VLAN Tag 通过。

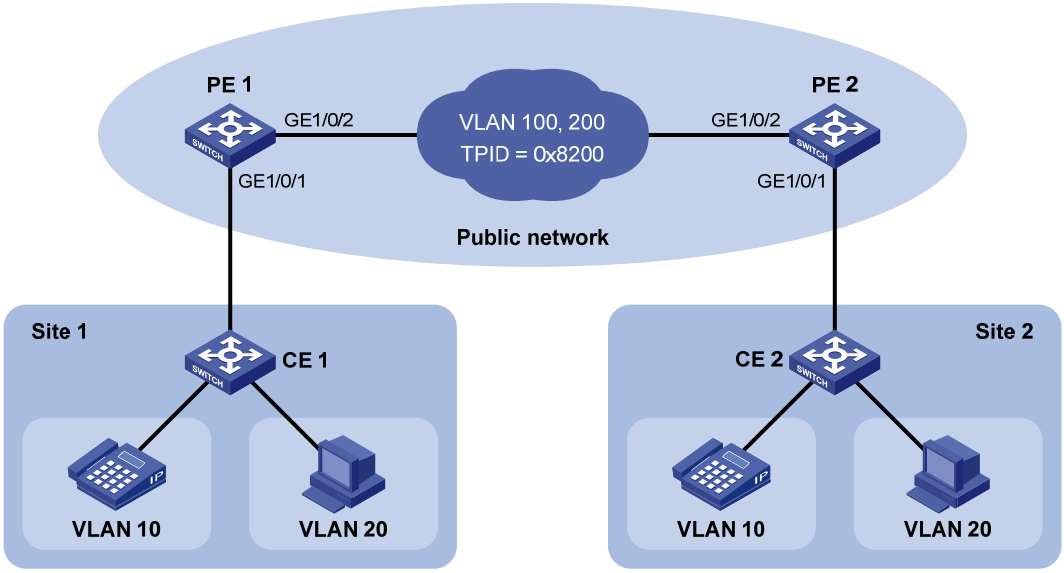
1.6.3 灵活QinQ配置举例一（基于端口配置外层VLAN Tag添加策略）

1. 组网需求

- 某公司的两个分支机构 Site 1 和 Site 2 通过运营商网络进行通信，该公司的语音和数据业务分别使用 VLAN 10 和 VLAN 20 加以区分。
- 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 和 VLAN 200 分别使这两个分支机构间的语音和数据业务实现互通。

2. 组网图

图1-5 灵活 QinQ 配置组网图



3. 配置步骤

说明

用户必须通过配置保证运营商网络中的设备之间允许 QinQ 报文通过。

(1) 配置 PE 1

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
 [PE1-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

使能端口的基本 QinQ 功能。

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

配置端口将来自 VLAN 10 的报文打上 VLAN ID 为 100 的外层 VLAN Tag。

```
[PE1-GigabitEthernet1/0/1] qinq vid 100
[PE1-GigabitEthernet1/0/1-vid-100] raw-vlan-id inbound 10
[PE1-GigabitEthernet1/0/1-vid-100] quit
```

配置端口将来自 VLAN 20 的报文打上 VLAN ID 为 200 的外层 VLAN Tag。

```
[PE1-GigabitEthernet1/0/1] qinq vid 200
[PE1-GigabitEthernet1/0/1-vid-200] raw-vlan-id inbound 20
[PE1-GigabitEthernet1/0/1-vid-200] quit
[PE1-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type hybrid
[PE2-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

配置端口将来自 VLAN 10 的报文打上 VLAN ID 为 100 的外层 VLAN Tag。

```
[PE2-GigabitEthernet1/0/1] qinq vid 100
[PE2-GigabitEthernet1/0/1-vid-100] raw-vlan-id inbound 10
[PE2-GigabitEthernet1/0/1-vid-100] quit
```

配置端口将来自 VLAN 20 的报文打上 VLAN ID 为 200 的外层 VLAN Tag。

```
[PE2-GigabitEthernet1/0/1] qinq vid 200
[PE2-GigabitEthernet1/0/1-vid-200] raw-vlan-id inbound 20
[PE2-GigabitEthernet1/0/1-vid-200] quit
```

```
[PE2-GigabitEthernet1/0/1] quit
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] 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 200 的报文携带 VLAN Tag 通过。

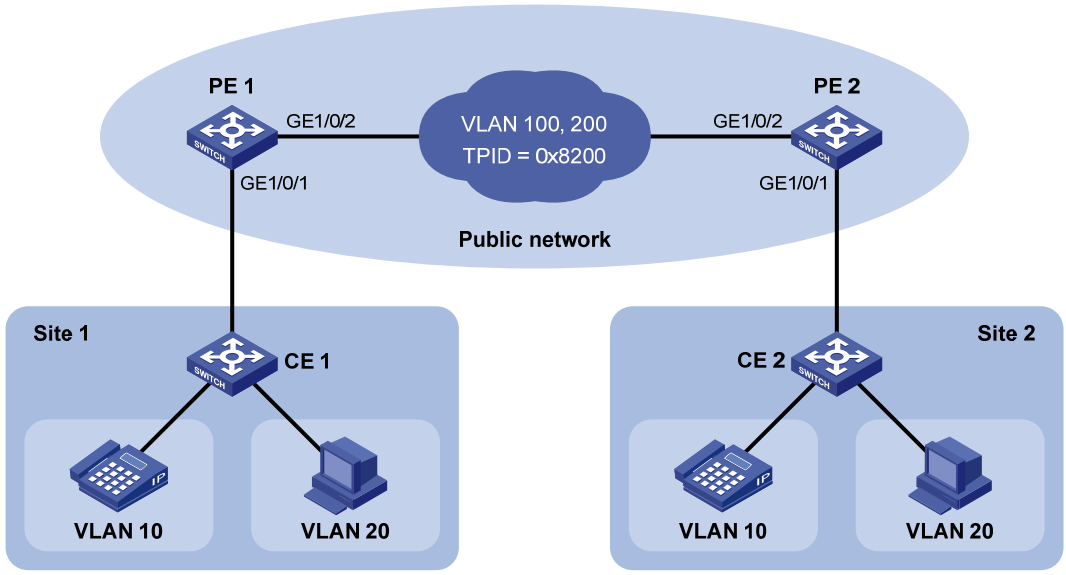
1.6.4 灵活QinQ配置举例二（基于QoS策略配置外层VLAN Tag添加策略）

1. 组网需求

- 某公司的两个分支机构 Site 1 和 Site 2 通过运营商网络进行通信，该公司的语音和数据业务分别使用 VLAN 10 和 VLAN 20 加以区分。
- 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 和 VLAN 200 分别使这两个分支机构间的语音和数据业务实现互通。

2. 组网图

图1-6 灵活 QinQ 配置组网图



3. 配置步骤

说明

用户必须通过配置保证运营商网络中的设备之间允许 QinQ 报文通过。

(1) 配置 PE 1

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[PE1-GigabitEthernet1/0/1] quit
```

创建流分类规则，将来自 Site 1 的 VLAN10 的报文定义为“A10”类。

```
[PE1] traffic classifier A10
[PE1-classifier-A10] if-match customer-vlan-id 10
[PE1-classifier-A10] quit
```

定义流行为，为报文封装 VLAN100 的外层 VLAN Tag，流行为命名为“P100”。

```
[PE1] traffic behavior P100
[PE1-behavior-P100] nest top-most vlan-id 100
[PE1-behavior-P100] quit
```

与以上配置类似，创建流分类“A20”匹配用户 VLAN ID 为 20 的报文，并创建流行为“P200”，为此类报文封装外层 VLAN200 的 Tag。

```
[PE1] traffic classifier A20
[PE1-classifier-A20] if-match customer-vlan-id 20
[PE1-classifier-A20] quit
[PE1] traffic behavior P200
[PE1-behavior-P200] nest top-most vlan-id 200
[PE1-behavior-P200] quit
```

创建 QoS 策略，将流分类“A10”和流行为“P100”进行关联，将流分类“A20”和流行为“P200”关联，策略命名为“qinq”。

```
[PE1] qos policy qinq
[PE1-qospolicy-qinq] classifier A10 behavior P100
[PE1-qospolicy-qinq] classifier A20 behavior P200
[PE1-qospolicy-qinq] quit
```

使能端口的基本 QinQ 功能。

```
[PE1] interface Gigabitethernet1/0/1
[PE1-GigabitEthernet1/0/1] qinq enable
```

在 GigabitEthernet1/0/1 端口的接收方向应用“qinq”规则。

```
[PE1-GigabitEthernet1/0/1] qos apply policy qinq inbound
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type hybrid
[PE2-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[PE2-GigabitEthernet1/0/1] quit
```

创建流分类规则，将来自 Site 2 的 VLAN10 的报文定义为“A10”类。

```
[PE2] traffic classifier A10
[PE2-classifier-A10] if-match customer-vlan-id 10
[PE2-classifier-A10] quit
```

定义流行为，为报文封装 VLAN100 的外层 VLAN Tag，流行为命名为“P100”。

```
[PE2] traffic behavior P100
[PE2-behavior-P100] nest top-most vlan-id 100
[PE2-behavior-P100] quit
```

与以上配置类似，创建流分类“A20”匹配用户 VLAN ID 为 20 的报文，并创建流行为“P200”，为此类报文封装外层 VLAN200 的 Tag。

```
[PE2] traffic classifier A20
[PE2-classifier-A20] if-match customer-vlan-id 20
[PE2-classifier-A20] quit
[PE2] traffic behavior P200
[PE2-behavior-P200] nest top-most vlan-id 200
[PE2-behavior-P200] quit
```

创建 QoS 策略，将流分类“A10”和流行为“P100”进行关联，将流分类“A20”和流行为“P200”关联，策略命名为“qinq”。

```
[PE2] qos policy qinq
[PE2-qospolicy-qinq] classifier A10 behavior P100
[PE2-qospolicy-qinq] classifier A20 behavior P200
[PE2-qospolicy-qinq] quit
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

在 GigabitEthernet1/0/1 端口的接收方向应用“qinq”规则。

```
[PE2-GigabitEthernet1/0/1] qos apply policy qinq inbound
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置端口添加的外层 Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] 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 200 的报文携带 VLAN Tag 通过。

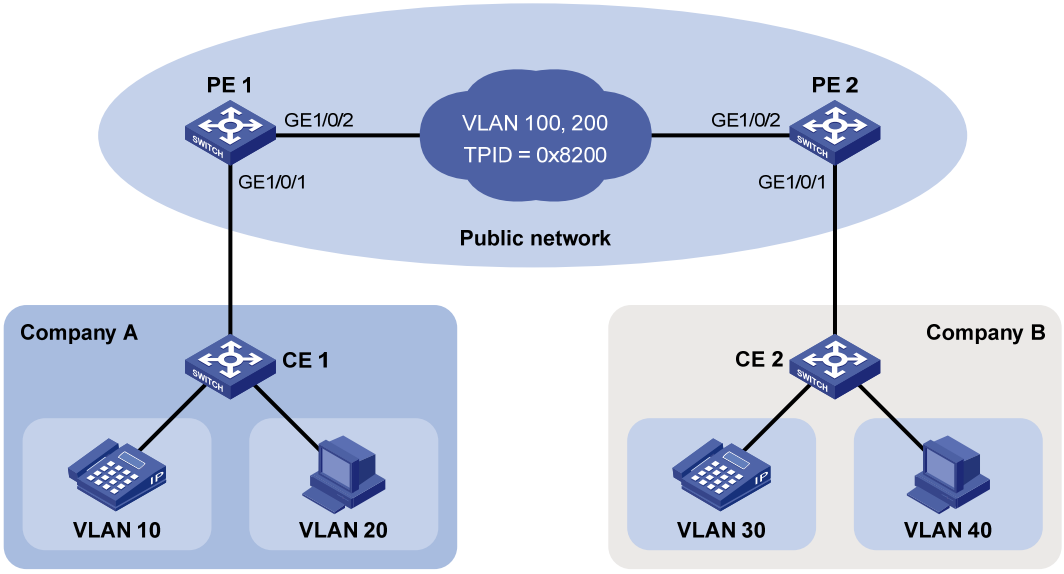
1.6.5 灵活QinQ配置举例三（替换内层VLAN Tag）

1. 组网需求

- 公司 A 的语音和数据业务分别使用 VLAN 10 和 VLAN 20 加以区分，而公司 B 的语音和数据业务则分别使用 VLAN 30 和 VLAN 40 加以区分。随着这两家公司的合并，需要在不改变现有 VLAN 划分的前提下将其网络进行整合。
- 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 和 VLAN 200 分别使这两家公司间的语音和数据业务实现互通。

2. 组网图

图1-7 灵活 QinQ 配置组网图二



3. 配置步骤

说明

用户必须通过配置保证运营商网络中的设备之间允许 QinQ 报文通过。

(1) 配置 PE 1

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[PE1-GigabitEthernet1/0/1] quit
```

创建流分类规则，将来自 VLAN10 的报文定义为“A10”类。

```
[PE1] traffic classifier A10
[PE1-classifier-A10] if-match customer-vlan-id 10
[PE1-classifier-A10] quit
```

定义流行为，为报文封装 VLAN100 的外层 VLAN Tag，流行为命名为“P100”。

```
[PE1] traffic behavior P100
[PE1-behavior-P100] nest top-most vlan-id 100
[PE1-behavior-P100] quit
```

与以上配置类似，创建流分类“A20”匹配用户 VLAN ID 为 20 的报文，并创建流行为“P200”，为此类报文封装外层 VLAN200 的 Tag

```
[PE1] traffic classifier A20
[PE1-classifier-A20] if-match customer-vlan-id 20
[PE1-classifier-A20] quit
[PE1] traffic behavior P200
[PE1-behavior-P200] nest top-most vlan-id 200
[PE1-behavior-P200] quit
```

创建 QoS 策略，将流分类“A10”和流行为“P100”进行关联，将流分类“A20”和流行为“P200”关联，策略命名为“qinq”。

```
[PE1] qos policy qinq
[PE1-qospolicy-qinq] classifier A10 behavior P100
[PE1-qospolicy-qinq] classifier A20 behavior P200
[PE1-qospolicy-qinq] quit
```

使能端口的基本 QinQ 功能。

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

在 GigabitEthernet1/0/1 端口的接收方向应用“qinq”规则。

```
[PE1-GigabitEthernet1/0/1] qos apply policy qinq inbound
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

创建流分类规则，将内层 VLAN ID 是 10，外层 VLAN ID 是 100 的报文定义为“A100”类。

```
[PE1] traffic classifier A100
[PE1-classifier-A100] if-match customer-vlan-id 10
[PE1-classifier-A100] if-match service-vlan-id 100
[PE1-classifier-A100] quit
```

定义流行为，修改报文的内层 VLAN ID 为 30，流行为命名为“T100”。

```
[PE1] traffic behavior T100
[PE1-behavior-T100] remark customer-vlan-id 30
[PE1-behavior-T100] quit
```

创建流分类规则，将内层 VLAN ID 是 20，外层 VLAN ID 是 200 的报文定义为“A200”类。

```
[PE1] traffic classifier A200
[PE1-classifier-A200] if-match customer-vlan-id 20
[PE1-classifier-A200] if-match service-vlan-id 200
[PE1-classifier-A200] quit
```

定义流行为，修改报文的内层 VLAN ID 为 40，流行为命名为“T200”。

```
[PE1] traffic behavior T200
[PE1-behavior-T200] remark customer-vlan-id 40
[PE1-behavior-T200] quit
```

创建 QoS 策略，将流分类“A100”和流行为“T100”进行关联，流分类“A200”和流行为“T200”进行关联，策略命名为“sqinq”。

```
[PE1] qos policy sqinq
[PE1-qospolicy- sqinq] classifier A100 behavior T100
[PE1-qospolicy- sqinq] classifier A200 behavior T200
[PE1-qospolicy- sqinq] quit
```

在 GigabitEthernet1/0/2 端口的发送方向应用“sqinq”规则。

```
[PE1-GigabitEthernet1/0/2] qos apply policy sqinq outbound
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 PE 2

- 配置端口 GigabitEthernet1/0/1

配置端口为 Hybrid 端口，且允许 VLAN 100 和 200 的报文不带 Tag 通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
```

```
[PE2-GigabitEthernet1/0/1] port link-type hybrid
[PE2-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[PE2-GigabitEthernet1/0/1] quit
```

创建流分类规则，将来自 VLAN30 的报文定义为“A30”类。

```
[PE2] traffic classifier A30
[PE2-classifier-A30] if-match customer-vlan-id 30
[PE2-classifier-A30] quit
```

定义流行为，为报文封装 VLAN100 的外层 VLAN Tag，流行为命名为“P100”。

```
[PE2] traffic behavior P100
[PE2-behavior-P100] nest top-most vlan-id 100
[PE2-behavior-P100] quit
```

与以上配置类似，创建流分类“A40”匹配用户 VLAN ID 为 40 的报文，并创建流行为“P200”，为此类报文封装外层 VLAN200 的 Tag。

```
[PE2] traffic classifier A40
[PE2-classifier-A40] if-match customer-vlan-id 40
[PE2-classifier-A40] quit
[PE2] traffic behavior P200
[PE2-behavior-P200] nest top-most vlan-id 200
[PE2-behavior-P200] quit
```

创建 QoS 策略，将流分类“A30”和流行为“P100”进行关联，将流分类“A40”和流行为“P200”关联，策略命名为“qinq”。

```
[PE2] qos policy qinq
[PE2-qospolicy-qinq] classifier A30 behavior P100
[PE2-qospolicy-qinq] classifier A40 behavior P200
[PE2-qospolicy-qinq] quit
```

使能端口的基本 QinQ 功能。

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

在 GigabitEthernet1/0/1 端口的接收方向应用“qinq”规则。

```
[PE2-GigabitEthernet1/0/1] qos apply policy qinq inbound
```

- 配置端口 GigabitEthernet1/0/2

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

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

创建流分类规则，将内层 VLAN ID 是 30，外层 VLAN ID 是 100 的报文定义为“A100”类。

```
[PE2] traffic classifier A100
[PE2-classifier-A100] if-match customer-vlan-id 30
[PE2-classifier-A100] if-match service-vlan-id 100
[PE2-classifier-A100] quit
```

定义流行为，修改报文的内层 VLAN ID 为 10，流行为命名为“T100”。

```
[PE2] traffic behavior T100
[PE2-behavior-T100] remark customer-vlan-id 10
[PE2-behavior-T100] quit
```

创建流分类规则，将内层 VLAN ID 是 40，外层 VLAN ID 是 200 的报文定义为“A200”类。

```
[PE2] traffic classifier A200
[PE2-classifier-A200] if-match customer-vlan-id 40
[PE2-classifier-A200] if-match service-vlan-id 200
[PE2-classifier-A200] quit
```

定义流行为，修改报文的内层 VLAN ID 为 20，流行为命名为“T200”。

```
[PE2] traffic behavior T200
```

```
[PE2-behavior-T200] remark customer-vlan-id 20
[PE2-behavior-T200] quit
```

创建 QoS 策略，将流分类“A100”和流行为“T100”进行关联，流分类“A200”和流行为“T200”进行关联，策略命名为“sqinq”。

```
[PE2] qos policy sqinq
[PE2-qospolicy- sqinq] classifier A100 behavior T100
[PE2-qospolicy- sqinq] classifier A200 behavior T200
[PE2-qospolicy- sqinq] quit
```

在 GigabitEthernet1/0/2 端口的发送方向应用“sqinq”规则。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] qos apply policy sqinq outbound
```

配置端口添加的外层 VLAN Tag 的 TPID 值为 0x8200。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] 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 200 的报文携带 VLAN Tag 通过。

目 录

1 VLAN映射配置

1.1 VLAN映射简介

VLAN 映射（VLAN Mapping）功能可以修改报文携带的 VLAN Tag，提供下面 3 种映射关系：

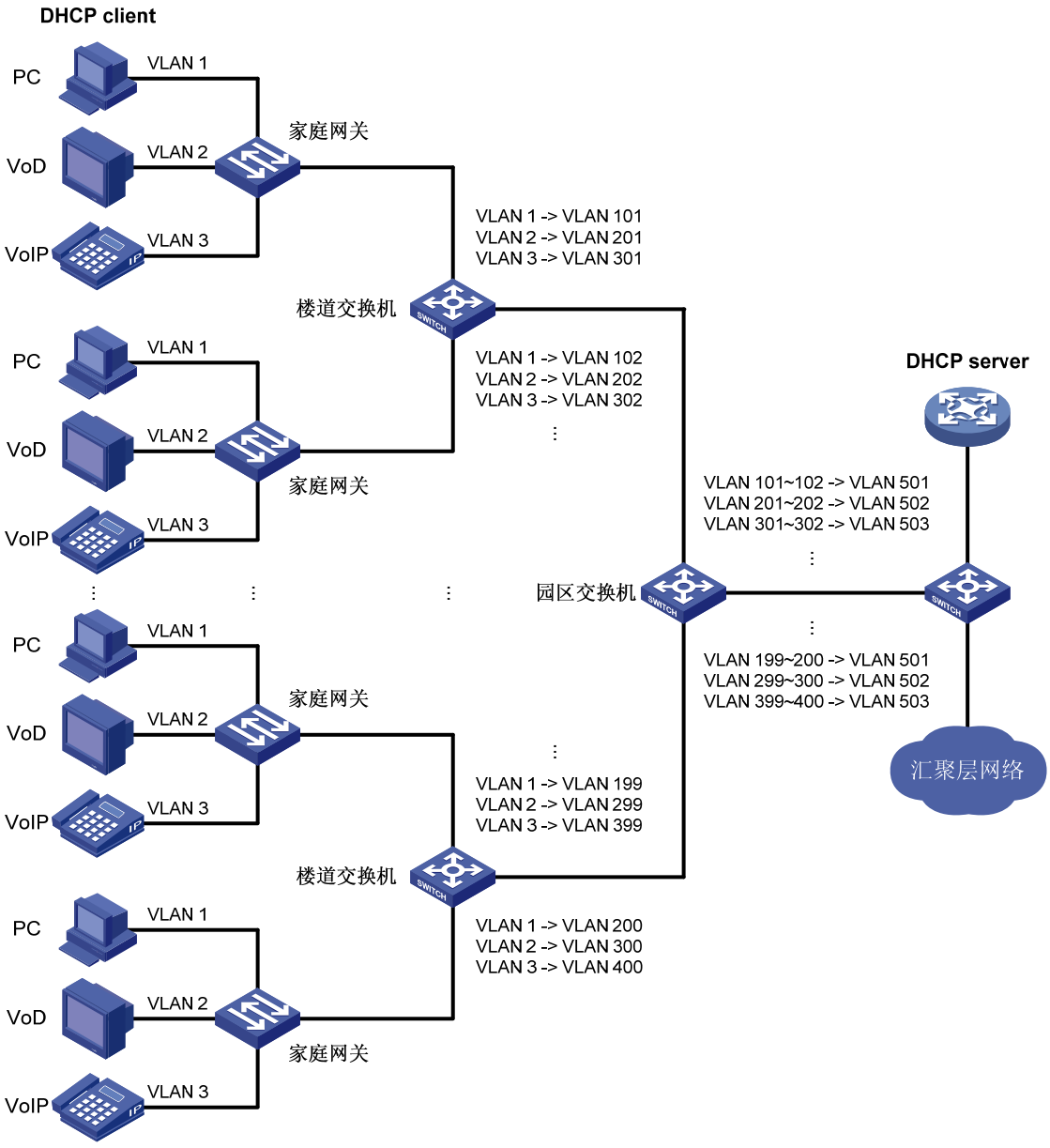
- 1:1 VLAN 映射：将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。
- N:1 VLAN 映射：将来自两个或多个 VLAN 的报文所携带的不同 VLAN Tag 替换为相同的 VLAN Tag。
- 2:2 VLAN 映射：将携带有两层 VLAN Tag 的报文的内、外层 VLAN Tag 都替换为新的 VLAN Tag。

下面将详细介绍这几种映射关系的应用以及工作原理。

1.1.1 1:1 和N:1 VLAN映射的应用

如 图 1-1 所示，是 1:1 和N:1 VLAN映射的应用环境，其中用不同的VLAN来承载各家庭用户不同类型的业务（包括PC、VoD和VoIP）。

图1-1 1:1 和 N:1 VLAN 映射应用示意图

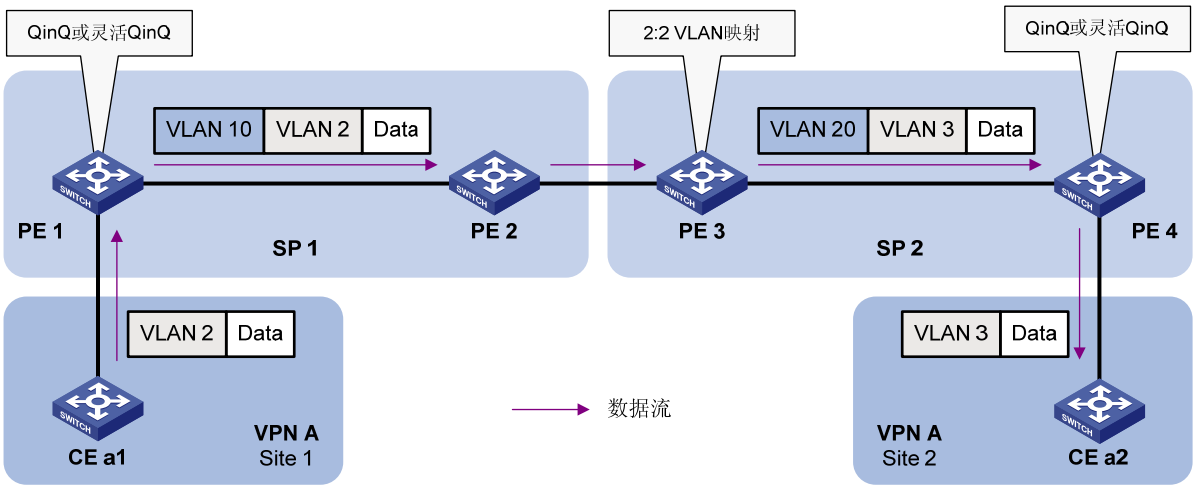


为了区分不同的用户，需要在楼道交换机处用不同的 VLAN 来承载不同用户的相同业务，即进行 1:1 VLAN 映射，这就要用到大量的 VLAN。但汇聚层网络接入设备可提供的 VLAN 数量有限，因此需要在园区交换机上来进行 VLAN 的汇聚，用一个 VLAN 来承载原本由多个 VLAN 承载的不同用户的相同业务，即进行 N:1 VLAN 映射。

1.1.2 2:2 VLAN映射的应用

如 图 1-2 所示，是 2:2 VLAN映射的应用环境，VPN A中处于不同地理位置（Site 1 和Site 2）的用户跨越了两个SP（Service Provider，服务提供商）——SP 1 和SP 2 的网络进行互通。

图1-2 2:2 VLAN 映射应用示意图



在 图 1-2 中，Site 1 和Site 2 中的用户所在的VLAN分别为VLAN 2 和VLAN 3，SP 1 和SP 2 分配给VPN A的VLAN分别为VLAN 10 和VLAN 20。当Site 1 中的报文进入SP 1 的网络后，SP1 通过QinQ或灵活QinQ功能，在报文外层封装上了VLAN 10 的VLAN Tag。这样，VPN用户就可以自由规划自己网络中的VLAN ID，而不用担心与SP的VLAN ID相冲突，同时也缓解了SP的网络中VLAN ID紧缺的问题。

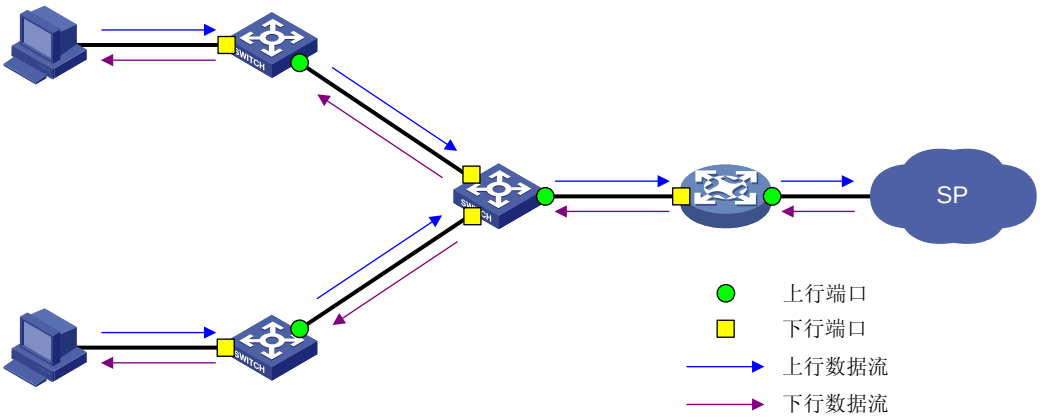
当上述报文继续由 SP 1 的网络进入 SP 2 的网络后，由于 SP 2 分配给 VPN A 的 VLAN 与 SP 1 不同，因此需将该报文的外层 VLAN Tag 替换为 VLAN 20 的 VLAN Tag，同时为了与 Site 2 中的用户互通，还需将其内层 VLAN Tag 替换为 VLAN 3 的 VLAN Tag。这种同时修改内、外两层 VLAN Tag 的过程就是 2:2 VLAN 映射。

说明

QinQ 和灵活 QinQ 的具体介绍及配置过程请参见“二层技术-以太网交换配置指导”中的“QinQ 配置”。

1.1.3 VLAN映射的基本概念

图1-3 VLAN 映射基本概念示意图



如 图 1-3 所示，为了更好的理解后面的配置过程，此处定义几个概念：

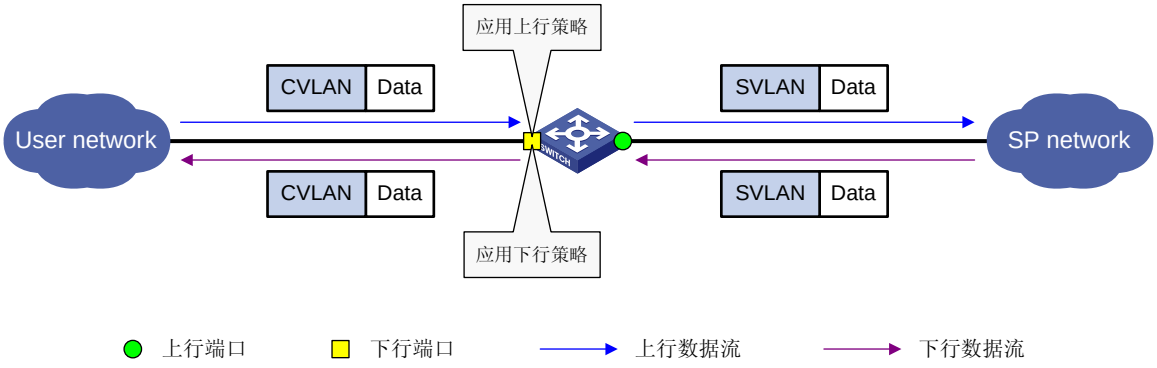
- 上行数据流：从用户网络发往汇聚层网络或 SP 网络的数据流，都称为上行数据流。

- 下行数据流：从汇聚层网络或 SP 网络发往用户网络的数据流，都称为下行数据流。
- 上行端口：发送上行数据流和接收下行数据流的端口称为上行端口。
- 下行端口：发送下行数据流和接收上行数据流的端口称为下行端口。
- 上行策略：负责上行数据流 VLAN 映射规则的 QoS 策略。
- 下行策略：负责下行数据流 VLAN 映射规则的 QoS 策略。

1.1.4 VLAN映射实现方式

1. 1:1 VLAN映射实现方式

图1-4 1:1 VLAN 映射实现方式示意图

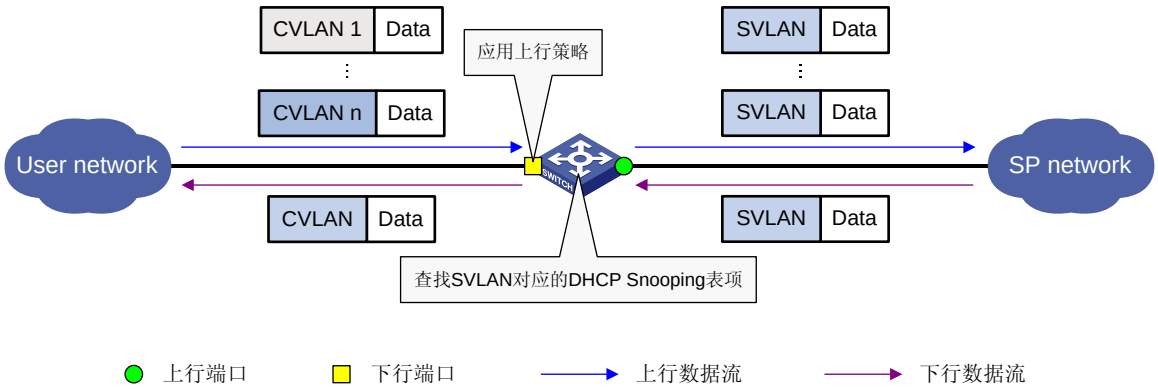


如 图 1-4 所示，1:1 VLAN映射的实现方式如下：

- 对于上行数据流，通过在下行端口上应用上行策略，将报文中 CVLAN 的 VLAN Tag 替换为 SVLAN 的 VLAN Tag。
- 对于下行数据流，通过在下行端口上应用下行策略，将报文中 SVLAN 的 VLAN Tag 替换为 CVLAN 的 VLAN Tag。

2. N:1 VLAN映射实现方式

图1-5 N:1 VLAN 映射实现方式示意图

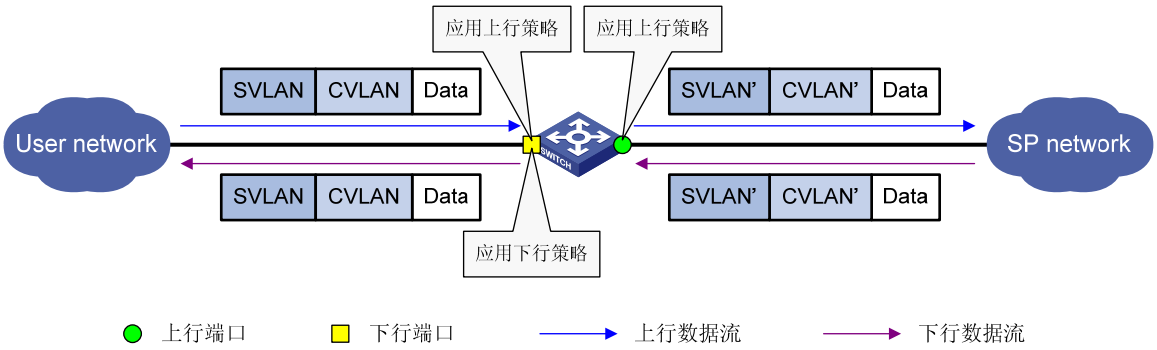


如 图 1-5 所示，N:1 VLAN映射的实现方式如下：

- 对于上行数据流，通过在下行端口上应用上行策略，将来自两个或多个 CVLAN 的报文所携带的不同 VLAN Tag 都替换为 SVLAN 的 VLAN Tag。
- 对于下行数据流，通过查找 SVLAN 对应的 DHCP Snooping 表项中 DHCP 客户端的 IP 地址、MAC 地址和 CVLAN 的绑定表项，将报文中 SVLAN 的 VLAN Tag 替换为 CVLAN 的 VLAN Tag。

3. 2:2 VLAN映射实现方式

图1-6 2:2 VLAN 映射实现方式示意图



如 图 1-6 所示，2:2 VLAN映射的实现方式如下：

- 对于上行数据流，通过在下行端口上应用上行策略，将报文的外层 VLAN Tag 替换为新的 VLAN Tag；通过在上行端口上应用上行策略，将报文的内层 VLAN Tag 替换为新的 VLAN Tag。
- 对于下行数据流，通过在下行端口上应用下行策略，将报文的内、外层 VLAN Tag 都替换为各自的原始 VLAN Tag。

说明

- 有关 DHCP Snooping 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。
- 有关 QoS 策略的详细介绍，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1.2 VLAN映射配置任务简介

用户需要根据网络规划，在不同的设备上进行不同的 VLAN 映射配置。

表1-1 VLAN 映射配置任务简介

配置任务	说明	详细配置
配置1:1 VLAN映射	在图1-1所示的组网中，需要在楼道交换机上进行此配置	1.3.1
配置N:1 VLAN映射	在图1-1所示的组网中，需要在园区交换机上进行此配置	1.3.2
配置2:2 VLAN映射	在图1-2所示的组网中，需要在SP 2网络的边缘设备PE 3上进行此配置	1.3.3

1.3 配置VLAN映射

1.3.1 配置 1:1 VLAN映射

在 图 1-1 所示的组网中，需要在楼道交换机上进行 1:1 VLAN映射的配置，以便将不同用户的不同业务用不同的VLAN进行隔离。

1. 配置任务简介

表1-2 1:1 VLAN 映射配置任务简介

配置任务	说明	详细配置
配置上行策略	必选	1.3.1 3.
配置下行策略	必选	1.3.1 4.
配置下行端口	必选	1.3.1 5.
配置上行端口	必选	1.3.1 6.

2. 配置准备

在配置 1:1 VLAN 映射之前，需完成以下任务：

- 创建好 CVLAN 和 SVLAN，并规划好 CVLAN 和 SVLAN 的映射关系。

3. 配置上行策略

通过配置上行策略，将不同用户的不同业务 VLAN（CVLAN）映射到不同的 VLAN（SVLAN）上。

表1-3 配置上行策略

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** *tcl-name* [**operator** { **and** | **or** }]	必选
定义匹配用户不同业务VLAN（CVLAN）的规则	**if-match customer-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的SVLAN	**remark service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选

4. 配置下行策略

通过配置下行策略，将 SVLAN 映射回原来的 CVLAN 上。

表1-4 配置下行策略

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** *tcl-name* [**operator** { **and** | **or** }]	必选
定义匹配SVLAN的规则	**if-match service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的CVLAN	**remark customer-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-

操作	命令	说明
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选

5. 配置下行端口

表1-5 配置下行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	
允许CVLAN和SVLAN通过当前端口	允许CVLAN和SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许CVLAN和SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	
使能端口的基本QinQ功能		**qinq enable**	必选 缺省情况下，端口的基本QinQ功能处于关闭状态
在端口的入方向上应用上行策略		**qos apply policy** *policy-name* **inbound**	必选
在端口的出方向上应用下行策略		**qos apply policy** *policy-name* **outbound**	必选

6. 配置上行端口

表1-6 配置上行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	

操作		命令	说明
允许SVLAN通过当前端口	允许SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	

1.3.2 配置N:1 VLAN映射

在 图 1-1 所示的组网中，需要在园区交换机上进行N:1 VLAN映射的配置，以便将不同用户的相同业务用同一个VLAN进行发送，从而节省VLAN资源。

1. 配置任务简介

表1-7 N:1 VLAN 映射配置任务简介

配置任务	说明	详细配置
使能DHCP Snooping功能	必选	1.3.2 3.
使能ARP Detection功能	必选	1.3.2 4.
配置上行策略	必选	1.3.2 5.
配置下行端口	必选	1.3.2 6.
配置上行端口	必选	1.3.2 7.

注意

如果用户想改变 VLAN 映射关系，必须先用 **reset dhcp-snooping** 命令（请参见“三层技术-IP 业务命令参考”中的“DHCP Snooping”）清除 DHCP Snooping 表项，然后再修改 QoS 策略中的 VLAN 映射关系。

2. 配置准备

在配置 N:1 VLAN 映射之前，需完成以下任务：

- 要求家庭用户中不同的业务终端都通过 DHCP 方式获取 IP 地址。有关通过 DHCP 方式获取 IP 地址的方法，请参见“三层技术-IP 业务配置指导”中的“DHCP 概述”。
- 创建好 CVLAN 和 SVLAN，并规划好 CVLAN 和 SVLAN 的映射关系。

3. 使能DHCP Snooping功能

表1-8 使能 DHCP Snooping 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能DHCP Snooping功能	**dhcp-snooping**	必选 缺省情况下，DHCP Snooping功能处于关闭状态

4. 使能ARP Detection功能

正常的 ARP 报文处理流程无法修改 ARP 报文所属的 VLAN，因此需要使用 ARP Detection 功能将 ARP 报文上送 CPU 进行处理，这样就可以对 ARP 报文进行 VLAN 映射。有关 ARP Detection 功能的详细介绍，请参见“安全配置指导”中的“ARP 攻击防御”。

请在所有 SVLAN 上都使能 ARP Detection 功能。

表1-9 使能 ARP Detection 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP Detection功能	**arp detection enable**	必选 缺省情况下，ARP Detection功能处于关闭状态

说明

建议在所有 CVLAN 上也都使能 ARP Detection 功能，以起到防攻击的作用。

5. 配置上行策略

通过配置上行策略，将不同用户的相同业务 VLAN（CVLAN）映射到同一个 VLAN（SVLAN）上。

表1-10 配置上行策略

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** *tcl-name* **operator or**	必选
定义匹配不同用户相同业务VLAN（CVLAN）的规则	**if-match customer-vlan-id** { *vlan-list* | *vlan-id1* **to** *vlan-id2* }	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的SVLAN	**remark service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为和绑定模式	**classifier** *tcl-name* **behavior** *behavior-name* **mode dot1q-tag-manipulation**	必选

6. 配置下行端口

表1-11 配置下行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	

操作		命令	说明
配置端口的链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	
允许CVLAN和SVLAN通过当前端口	允许CVLAN和SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许CVLAN和SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	
使能端口的用户侧QinQ功能		**qinq enable downlink**	必选 缺省情况下，端口的用户侧QinQ功能处于关闭状态
在端口的入方向上应用上行策略		**qos apply policy** *policy-name* **inbound**	必选

注意

在下行端口上应用 QoS 策略之前，需要先使能端口的用户侧 QinQ 功能；在下行端口上关闭用户侧 QinQ 功能之前，需要先解除 QoS 策略与该端口的绑定。

7. 配置上行端口

表1-12 配置上行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	
配置端口的链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	
允许SVLAN通过当前端口	允许SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	
配置端口为DHCP Snooping信任端口		**dhcp-snooping trust**	必选 缺省情况下，端口为DHCP Snooping非信任端口

操作	命令	说明
配置端口为ARP信任端口	**arp detection trust**	必选 缺省情况下，端口为ARP非信任端口
使能端口的网络侧QinQ功能	**qinq enable uplink**	必选 缺省情况下，端口的网络侧QinQ功能处于关闭状态

1.3.3 配置 2:2 VLAN映射

在 图 1-2 所示的组网中，需要在SP 2 网络的边缘设备PE 3 上进行 2:2 VLAN映射的配置，以便使得报文外层VLAN Tag为新SP网络分配给用户的VLAN，而内层的VLAN Tag可以和不同VLAN的同一VPN用户进行互通。

1. 配置任务简介

表1-13 2:2 VLAN 映射配置任务简介

配置任务	说明	详细配置
配置下行端口的上行策略	必选	1.3.3 2.
配置下行端口的下行策略	必选	1.3.3 3.
配置上行端口的上行策略	必选	1.3.3 4.
配置下行端口	必选	1.3.3 5.
配置上行端口	必选	1.3.3 6.

2. 配置下行端口的上行策略

通过配置下行端口的上行策略，来修改 SVLAN 的值。

表1-14 配置下行端口的上行策略

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** *tcl-name* [**operator and**]	必选
定义匹配CVLAN的规则	**if-match customer-vlan-id** *vlan-id*	必选
定义匹配SVLAN的规则	**if-match service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的SVLAN	**remark service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选

3. 配置下行端口的下行策略

通过配置下行端口的下行策略，来将 SVLAN 和 CVLAN 的值都修改为原来的值。

表1-15 配置下行端口的下行策略

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** *tcl-name* [**operator and**]	必选
定义匹配CVLAN的规则	**if-match customer-vlan-id** *vlan-id*	必选
定义匹配SVLAN的规则	**if-match service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的CVLAN	**remark customer-vlan-id** *vlan-id*	必选
配置重标记报文的SVLAN	**remark service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选

4. 配置上行端口的上行策略

通过配置上行端口的上行策略，来修改 CVLAN 的值。

表1-16 配置上行端口的上行策略

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** *tcl-name* [**operator and**]	必选
定义匹配CVLAN的规则	**if-match customer-vlan-id** *vlan-id*	必选
定义匹配SVLAN的规则	**if-match service-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置重标记报文的CVLAN	**remark customer-vlan-id** *vlan-id*	必选
退回系统视图	**quit**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选
为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选

5. 配置下行端口

表1-17 配置下行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	
允许SVLAN通过当前端口	允许SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	
在端口的入方向上应用上行策略		**qos apply policy** *policy-name* **inbound**	必选
在端口的出方向上应用下行策略		**qos apply policy** *policy-name* **outbound**	必选

6. 配置上行端口

表1-18 配置上行端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	-
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的链路类型	配置端口的链路类型为Trunk类型	**port link-type trunk**	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
	配置端口的链路类型为Hybrid类型	**port link-type hybrid**	
允许SVLAN通过当前端口	允许SVLAN通过当前Trunk端口	**port trunk permit vlan** { *vlan-list* | **all** }	二者必选其一 缺省情况下，Trunk端口只允许VLAN 1通过；Hybrid端口只允许VLAN 1的报文以Untagged方式通过
	允许SVLAN以Tagged方式通过当前Hybrid端口	**port hybrid vlan** *vlan-list* **tagged**	
在端口的出方向上应用上行策略		**qos apply policy** *policy-name* **outbound**	必选

1.4 VLAN映射典型配置举例

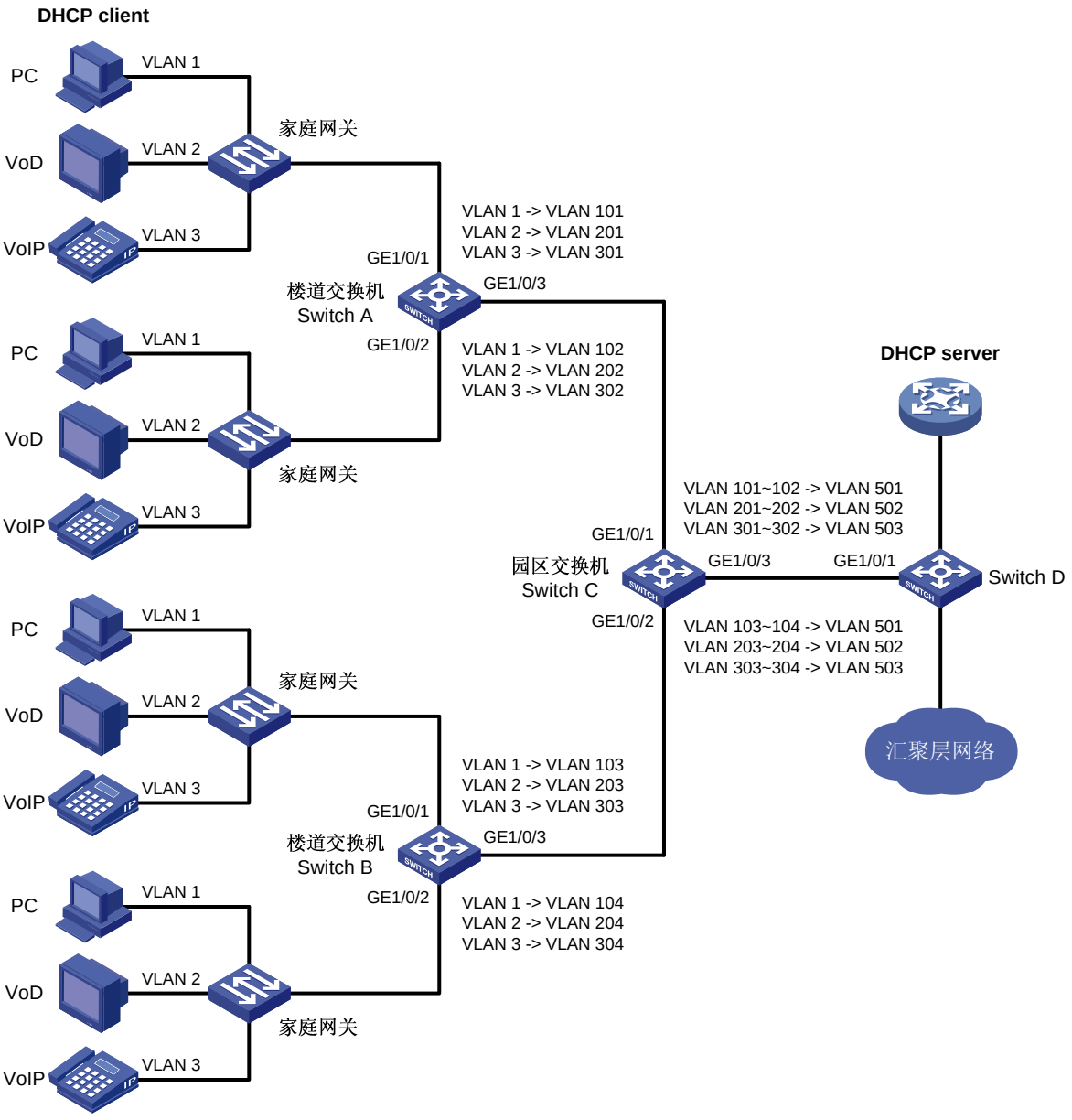
1.4.1 1:1 和N:1 VLAN映射配置举例

1. 组网需求

- 在某小区，服务提供商为每个家庭都提供了电脑上网（PC）、视频点播（VoD）和语音电话（VoIP）这三种数据服务，每个家庭都通过各自的家庭网关接入楼道交换机，并通过 DHCP 方式自动获取 IP 地址。
- 服务提供商希望实现以下网络规划：在家庭网关上，分别将 PC、VoD 和 VoIP 业务依次划分到 VLAN 1～3；在楼道交换机上，为了隔离不同家庭的同类业务，将每个家庭的每种业务都划分到不同的 VLAN；而在园区交换机上，为了节省 VLAN 资源，将所有家庭的同类业务都划分到相同的 VLAN，即分别将 PC、VoD 和 VoIP 业务依次划分到 VLAN 501～503。

2. 组网图

图1-7 1:1 和 N:1 VLAN 映射配置组网图



3. 配置步骤

(1) 配置 Switch A

创建 CVLAN 和 SVLAN。

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

配置上行策略 p1 和 p2：将不同用户的不同业务 CVLAN 映射到不同的 SVLAN 上。

```
[SwitchA] traffic classifier c1
[SwitchA-classifier-c1] if-match customer-vlan-id 1
[SwitchA-classifier-c1] traffic classifier c2
[SwitchA-classifier-c2] if-match customer-vlan-id 2
[SwitchA-classifier-c2] traffic classifier c3
[SwitchA-classifier-c3] if-match customer-vlan-id 3
[SwitchA-classifier-c3] quit
[SwitchA] traffic behavior b1
[SwitchA-behavior-b1] remark service-vlan-id 101
[SwitchA-behavior-b1] traffic behavior b2
[SwitchA-behavior-b2] remark service-vlan-id 201
[SwitchA-behavior-b2] traffic behavior b3
[SwitchA-behavior-b3] remark service-vlan-id 301
[SwitchA-behavior-b3] traffic behavior b4
[SwitchA-behavior-b4] remark service-vlan-id 102
[SwitchA-behavior-b4] traffic behavior b5
[SwitchA-behavior-b5] remark service-vlan-id 202
[SwitchA-behavior-b5] traffic behavior b6
[SwitchA-behavior-b6] remark service-vlan-id 302
[SwitchA-behavior-b6] quit
[SwitchA] qos policy p1
[SwitchA-policy-p1] classifier c1 behavior b1
[SwitchA-policy-p1] classifier c2 behavior b2
[SwitchA-policy-p1] classifier c3 behavior b3
[SwitchA-policy-p1] quit
[SwitchA] qos policy p2
[SwitchA-policy-p2] classifier c1 behavior b4
[SwitchA-policy-p2] classifier c2 behavior b5
[SwitchA-policy-p2] classifier c3 behavior b6
[SwitchA-policy-p2] quit
```

配置下行策略 p11 和 p22：将 SVLAN 映射回原来的 CVLAN 上。

```
[SwitchA] traffic classifier c11
[SwitchA-classifier-c11] if-match service-vlan-id 101
[SwitchA-classifier-c11] traffic classifier c22
[SwitchA-classifier-c22] if-match service-vlan-id 201
[SwitchA-classifier-c22] traffic classifier c33
[SwitchA-classifier-c33] if-match service-vlan-id 301
[SwitchA-classifier-c33] traffic classifier c44
[SwitchA-classifier-c44] if-match service-vlan-id 102
[SwitchA-classifier-c44] traffic classifier c55
[SwitchA-classifier-c55] if-match service-vlan-id 202
[SwitchA-classifier-c55] traffic classifier c66
[SwitchA-classifier-c66] if-match service-vlan-id 302
```

```
[SwitchA-classifier-c66] quit
[SwitchA] traffic behavior b11
[SwitchA-behavior-b11] remark customer-vlan-id 1
[SwitchA-behavior-b11] traffic behavior b22
[SwitchA-behavior-b22] remark customer-vlan-id 2
[SwitchA-behavior-b22] traffic behavior b33
[SwitchA-behavior-b33] remark customer-vlan-id 3
[SwitchA-behavior-b33] quit
[SwitchA] qos policy p11
[SwitchA-policy-p11] classifier c11 behavior b11
[SwitchA-policy-p11] classifier c22 behavior b22
[SwitchA-policy-p11] classifier c33 behavior b33
[SwitchA-policy-p11] quit
[SwitchA] qos policy p22
[SwitchA-policy-p22] classifier c44 behavior b11
[SwitchA-policy-p22] classifier c55 behavior b22
[SwitchA-policy-p22] classifier c66 behavior b33
[SwitchA-policy-p22] quit
```

配置下行端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 CVLAN 和 SVLAN 通过，使能该端口的基本 QinQ 功能，在该端口的入方向上应用上行策略 p1，并在该端口的出方向上应用下行策略 p11。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
[SwitchA-GigabitEthernet1/0/1] qinq enable
[SwitchA-GigabitEthernet1/0/1] qos apply policy p1 inbound
[SwitchA-GigabitEthernet1/0/1] qos apply policy p11 outbound
[SwitchA-GigabitEthernet1/0/1] quit
```

配置下行端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 CVLAN 和 SVLAN 通过，使能该端口的基本 QinQ 功能，在该端口的入方向上应用上行策略 p2，并在该端口的出方向上应用下行策略 p22。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
[SwitchA-GigabitEthernet1/0/2] qinq enable
[SwitchA-GigabitEthernet1/0/2] qos apply policy p2 inbound
[SwitchA-GigabitEthernet1/0/2] qos apply policy p22 outbound
[SwitchA-GigabitEthernet1/0/2] quit
```

配置上行端口 GigabitEthernet1/0/3 为 Trunk 端口且允许 SVLAN 通过。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
```

说明

如果 PC（发送不带 VLAN Tag 的报文）直接连接在楼道交换机上，则需把楼道交换机连接 PC 的端口配置成 Access 端口或者 Trunk 端口：

- 当配置成 Access 端口时，要把端口加入到 SVLAN;
- 当配置成 Trunk 端口时，要把端口的缺省 VLAN 配置成 SVLAN。

(2) 配置 Switch B

Switch B 的配置与 Switch A 相似，配置过程略。

(3) 配置 Switch C

使能 DHCP Snooping 功能。

```
<SwitchC> system-view
[SwitchC] dhcp-snooping
```

创建 CVLAN 和 SVLAN，并在这些 VLAN 上分别使能 ARP Detection 功能。

```
[SwitchC] vlan 101
[SwitchC-vlan101] arp detection enable
[SwitchC-vlan101] vlan 201
[SwitchC-vlan201] arp detection enable
[SwitchC-vlan201] vlan 301
[SwitchC-vlan301] arp detection enable
[SwitchC-vlan301] vlan 102
[SwitchC-vlan102] arp detection enable
[SwitchC-vlan102] vlan 202
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
[SwitchC-vlan302] vlan 103
[SwitchC-vlan103] arp detection enable
[SwitchC-vlan103] vlan 203
[SwitchC-vlan203] arp detection enable
[SwitchC-vlan203] vlan 303
[SwitchC-vlan303] arp detection enable
[SwitchC-vlan303] vlan 104
[SwitchC-vlan104] arp detection enable
[SwitchC-vlan104] vlan 204
[SwitchC-vlan204] arp detection enable
[SwitchC-vlan204] vlan 304
[SwitchC-vlan304] arp detection enable
[SwitchC-vlan304] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

配置上行策略 p1 和 p2：将不同用户的相同业务 VLAN（CVLAN）映射到同一个 VLAN（SVLAN）上。

```
[SwitchC] traffic classifier c1
[SwitchC-classifier-c1] if-match customer-vlan-id 101 to 102
[SwitchC-classifier-c1] traffic classifier c2
[SwitchC-classifier-c2] if-match customer-vlan-id 201 to 202
[SwitchC-classifier-c2] traffic classifier c3
[SwitchC-classifier-c3] if-match customer-vlan-id 301 to 302
[SwitchC-classifier-c3] traffic classifier c4
[SwitchC-classifier-c4] if-match customer-vlan-id 103 to 104
[SwitchC-classifier-c4] traffic classifier c5
[SwitchC-classifier-c5] if-match customer-vlan-id 203 to 204
[SwitchC-classifier-c5] traffic classifier c6
[SwitchC-classifier-c6] if-match customer-vlan-id 303 to 304
[SwitchC-classifier-c6] quit
```

```
[SwitchC] traffic behavior b1
[SwitchC-behavior-b1] remark service-vlan-id 501
[SwitchC-behavior-b1] traffic behavior b2
[SwitchC-behavior-b2] remark service-vlan-id 502
[SwitchC-behavior-b2] traffic behavior b3
[SwitchC-behavior-b3] remark service-vlan-id 503
[SwitchC-behavior-b3] quit
[SwitchC] qos policy p1
[SwitchC-policy-p1] classifier c1 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c2 behavior b2 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c3 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p1] quit
[SwitchC] qos policy p2
[SwitchC-policy-p2] classifier c4 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p2] classifier c5 behavior b2 mode dot1q-tag-manipulation
[SwitchC-policy-p2] classifier c6 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p2] quit
```

配置下行端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 CVLAN 和 SVLAN 通过，使能该端口的用户侧 QinQ 功能，并在该端口的入方向上应用上行策略 p1。

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 101 201 301 102 202 302 501 502 503
[SwitchC-GigabitEthernet1/0/1] qinq enable downlink
[SwitchC-GigabitEthernet1/0/1] qos apply policy p1 inbound
[SwitchC-GigabitEthernet1/0/1] quit
```

配置下行端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 CVLAN 和 SVLAN 通过，使能该端口的用户侧 QinQ 功能，并在该端口的入方向上应用上行策略 p2。

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 103 203 303 104 204 304 501 502 503
[SwitchC-GigabitEthernet1/0/2] qinq enable downlink
[SwitchC-GigabitEthernet1/0/2] qos apply policy p2 inbound
[SwitchC-GigabitEthernet1/0/2] quit
```

配置上行端口 GigabitEthernet1/0/3 为 Trunk 端口且允许 SVLAN 通过，配置该端口为 DHCP Snooping 信任端口和 ARP 信任端口，并使能该端口的网络侧 QinQ 功能。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-GigabitEthernet1/0/3] port trunk permit vlan 501 502 503
[SwitchC-GigabitEthernet1/0/3] dhcp-snooping trust
[SwitchC-GigabitEthernet1/0/3] arp detection trust
[SwitchC-GigabitEthernet1/0/3] qinq enable uplink
```

(4) 配置 Switch D

使能 DHCP Snooping 功能。

```
<SwitchD> system-view
[SwitchD] dhcp-snooping
```

配置端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 SVLAN 通过。

```
<SwitchD> system-view
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 501 502 503
```

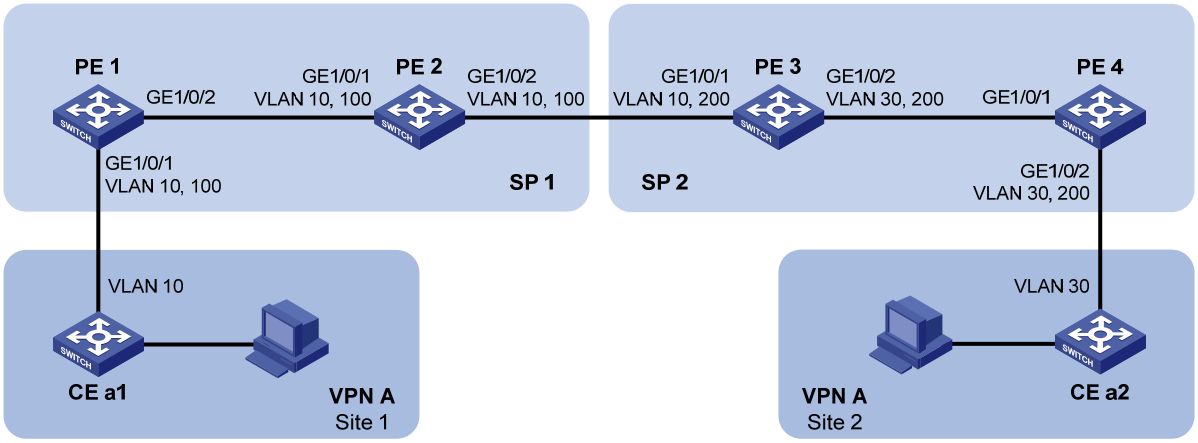
1.4.2 2:2 VLAN映射配置举例

1. 组网需求

- VPN A 中的站点 1 和站点 2 是某公司的两个分支机构，且分别利用 VLAN 10 和 VLAN 30 承载业务。由于分处不同地域，这两个分支机构采用了不同的服务提供商所提供的 VPN 接入服务，且 SP 1 和 SP 2 分别将 VLAN 100 和 VLAN 200 分配给这两个分支机构使用。
- 该公司希望其下属的这两个分支机构可以跨越 SP 1 和 SP 2 的网络实现互通。

2. 组网图

图1-8 2:2 VLAN 映射配置组网图



3. 配置步骤

(1) 配置 PE 1

配置 GigabitEthernet1/0/1 端口的 QinQ 功能，为 VLAN 10 报文添加 VLAN ID 为 100 的外层 VLAN Tag。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port access vlan 100
[PE1-GigabitEthernet1/0/1] qinq enable
[PE1-GigabitEthernet1/0/1] quit
```

配置上行端口 GigabitEthernet1/0/2 允许 VLAN 100 的报文通过。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
```

(2) 配置 PE 2

配置端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 VLAN 100 通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100
[PE2-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 100 通过。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100
```

(3) 配置 PE 3

配置下行端口的上行策略 downlink_in：即下行端口对入方向报文的匹配规则流行为。

```
<PE3> system-view
[PE3] traffic classifier downlink_in
[PE3-classifier-downlink_in] if-match customer-vlan-id 10
[PE3-classifier-downlink_in] if-match service-vlan-id 100
[PE3-classifier-downlink_in] quit
[PE3] traffic behavior downlink_in
[PE3-behavior-downlink_in] remark service-vlan-id 200
[PE3-behavior-downlink_in] quit
[PE3] qos policy downlink_in
[PE3-qospolicy-downlink_in] classifier downlink_in behavior downlink_in
[PE3-qospolicy-downlink_in] quit
```

配置下行端口的下行策略 downlink_out：即下行端口对出方向报文的匹配规则和流行为。

```
[PE3] traffic classifier downlink_out
[PE3-classifier-downlink_out] if-match customer-vlan-id 30
[PE3-classifier-downlink_out] if-match service-vlan-id 200
[PE3-classifier-downlink_out] quit
[PE3] traffic behavior downlink_out
[PE3-behavior-downlink_out] remark customer-vlan-id 10
[PE3-behavior-downlink_out] remark service-vlan-id 100
[PE3-behavior-downlink_out] quit
[PE3] qos policy downlink_out
[PE3-qospolicy-downlink_out] classifier downlink_out behavior downlink_out
[PE3-qospolicy-downlink_out] quit
```

配置上行端口的上行策略 uplink_out：即上行端口对出方向报文的匹配规则和流行为。

```
[PE3] traffic classifier uplink_out
[PE3-classifier-uplink_out] if-match customer-vlan-id 10
[PE3-classifier-uplink_out] if-match service-vlan-id 200
[PE3-classifier-uplink_out] quit
[PE3] traffic behavior uplink_out
[PE3-behavior-uplink_out] remark customer-vlan-id 30
[PE3-behavior-uplink_out] quit
[PE3] qos policy uplink_out
[PE3-qospolicy-uplink_out] classifier uplink_out behavior uplink_out
[PE3-qospolicy-uplink_out] quit
```

配置下行端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 VLAN 200 通过，在该端口的入方向上应用上行策略 downlink_in，并在该端口的出方向上应用下行策略 downlink_out。

```
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] port link-type trunk
[PE3-GigabitEthernet1/0/1] port trunk permit vlan 200
[PE3-GigabitEthernet1/0/1] qos apply policy downlink_in inbound
[PE3-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
[PE3-GigabitEthernet1/0/1] quit
```

配置上行端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 200 通过，并在该端口的出方向上应用下行策略 uplink_out。

```
[PE3] interface gigabitethernet 1/0/2
[PE3-GigabitEthernet1/0/2] port link-type trunk
[PE3-GigabitEthernet1/0/2] port trunk permit vlan 200
[PE3-GigabitEthernet1/0/2] qos apply policy uplink_out outbound
[PE3-GigabitEthernet1/0/2] quit
```

(4) 配置 PE 4

配置 GigabitEthernet1/0/2 的 QinQ 功能，为 VLAN 30 报文添加 VLAN ID 为 200 的外层 VLAN Tag。

```
<DeviceD> system-view
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port access vlan 200
[DeviceD-GigabitEthernet1/0/2] qinq enable
```

配置端口 GigabitEthernet1/0/1 允许 VLAN 200 的报文通过。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 200
```

目 录

1 LLDP配置

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。

说明

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”。

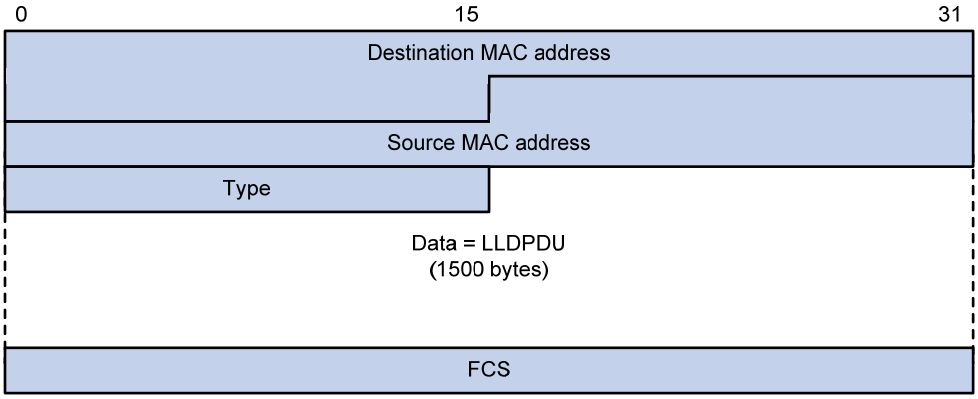
1.1.2 LLDP基本概念

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1-1 Ethernet II 格式封装的 LLDP 报文

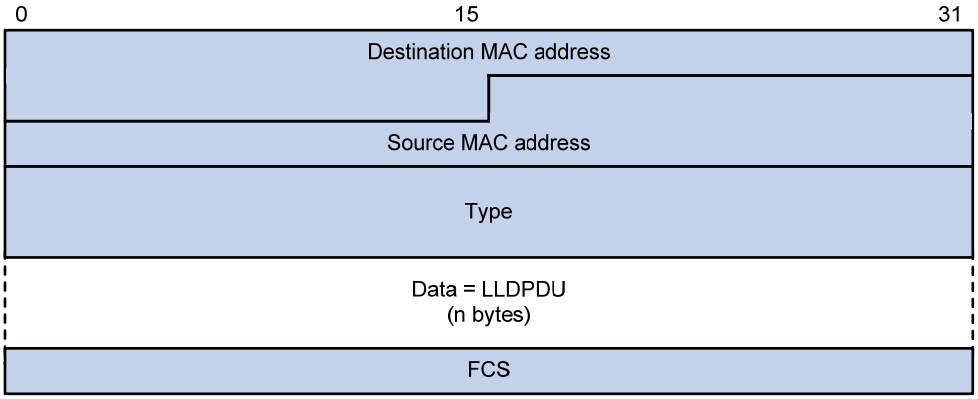


如 图 1-1 所示，是以Ethernet II格式封装的LLDP报文，其中各字段的含义如下：

- Destination MAC address：目的 MAC 地址，为固定的组播 MAC 地址 0x0180-C200-000E。
- 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1-2 SNAP 格式封装的 LLDP 报文



如 图 1-2 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，为固定的组播 MAC 地址 0x0180-C200-000E。
- 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。

2. 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1-3 LLDPDU 的封装格式

如 图 1-3 所示，深蓝色的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 28 种TLV。

3. 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（Media Endpoint Discovery，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

TLV 名称	说明	是否必须发布
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），一个LLDPDU中最多携带一个该类型TLV
Port And Protocol VLAN ID	端口的PPVID（Port and Protocol VLAN ID），一个LLDPDU中可携带多个互不重复的该类型TLV
VLAN Name	端口所属VLAN的名称，一个LLDPDU中可携带多个互不重复的该类型TLV
Protocol Identity	端口所支持的协议类型，一个LLDPDU中可携带多个互不重复的该类型TLV

说明

- 目前，H3C 设备不支持发送 Protocol Identity TLV，但可以接收该类型的 TLV。
- 三层以太网端口不支持 IEEE 802.1 组织定义 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（PSE（Power Sourcing Equipment，供电设备）或PD（Powered Device，受电设备））、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
Link Aggregation	端口是否支持链路聚合以及是否已使能链路聚合
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成本有效、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

4. 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

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

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，每发送一个 LLDP 报文后都需延迟一段时间后再继续发送下一个报文。

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 报文的发送周期缩短为 1 秒，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
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices

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LLDP工作模式	可选	1.3.2
	配置接口初始化延迟	可选	1.3.3
	配置轮询功能	可选	1.3.4
	配置允许发布的TLV类型	可选	1.3.5
	配置管理地址及其封装格式	可选	1.3.6
	调整LLDP相关参数	可选	1.3.7
	配置LLDP报文的封装格式	可选	1.3.8
配置LLDP兼容CDP功能		可选	1.4
配置LLDP Trap功能		可选	1.5

说明

对于 LLDP 的相关配置来说:

- 二层以太网端口视图下的配置只对当前端口有效;三层以太网端口视图下的配置只对当前接口有效；端口组视图下的配置对当前端口组中的所有端口有效。
- 三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

1.3 配置LLDP基本功能

1.3.1 使能LLDP功能

LLDP 功能必须在全局和接口上同时使能后才能生效。

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 enable**	必选 缺省情况下，LLDP功能处于全局使能状态
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
在接口上使能LLDP功能		**lldp enable**	可选 缺省情况下，LLDP功能在接口上处于使能状态

1.3.2 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1-7 配置 LLDP 工作模式

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置LLDP的工作模式		**lldp admin-status** { **disable** | **rx** | **tx** | **txrx** }	可选 缺省情况下，LLDP的工作模式为TxRx

1.3.3 配置接口初始化延迟

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1-8 配置接口初始化延迟

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置接口初始化的延迟时间	**lldp timer reinit-delay** *delay*	可选 缺省情况下，接口初始化的延迟时间为2秒

1.3.4 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它设备。

表1-9 配置轮询功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能轮询功能并配置轮询间隔		**lldp check-change-interval** *interval*	必选 缺省情况下，轮询功能处于关闭状态

1.3.5 配置允许发布的TLV类型

表1-10 配置允许发布的 TLV 类型

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置接口上允许发布的TLV类型（二层以太网端口视图和端口组视图）		**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }*&<1–10>* | **elin-address** *tel-number* } | **network-policy** | **power-over-ethernet** } }	可选 缺省情况下，二层以太网端口上允许发布除Location Identification TLV之外的所有类型的TLV
配置接口上允许发布的TLV类型（三层以太网端口视图）		**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } | **power-over-ethernet** } }	可选 缺省情况下，三层以太网端口上允许发布除IEEE 802.1组织定义的TLV、Network Policy TLV 和 Location Identification TLV之外所有类型的TLV

1.3.6 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，缺省为数字格式。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1-11 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**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
允许在LLDP报文中发布管理地址并配置所发布的管理地址		**lldp management-address-tlv** [*ip-address*]	可选 缺省情况下，允许在LLDP报文中发布管理地址：二层以太网端口发布的管理地址为该端口允许通过的、配置有IP地址的最小VLAN的主IP地址，但如果该端口允许通过的所有VLAN都未配置IP地址，则不发布管理地址；三层以太网端口发布的管理地址为该接口的IP地址，如果该接口未配置IP地址，则不发布管理地址
配置管理地址在TLV中的封装格式为字符串格式		**lldp management-address-format string**	可选 缺省情况下，管理地址在TLV中的封装格式为数字格式

1.3.7 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）），即取 65535 与（TTL 乘数×LLDP 报文的发送间隔）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1-12 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*	可选 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*	可选 缺省情况下，LLDP报文的发送间隔为30秒
配置LLDP报文的发送延迟	**lldp timer tx-delay** *delay*	可选 缺省情况下，LLDP报文的发送延迟为2秒
配置快速发送LLDP报文的个数	**lldp fast-count** *count*	可选 缺省情况下，快速发送LLDP报文的个数为3个

注意

- LLDP 报文的发送延迟应小于 TTL，否则将导致当前设备的信息在邻居设备上老化后仍无法收到当前设备发送的 LLDP 报文。
- 根据协议推荐，建议将 LLDP 报文的发送间隔配置为不小于其发送延迟的四倍。
- 如果所配置的 LLDP 报文的发送间隔小于其发送延迟，那么其实际发送间隔将以其发送延迟的取值为准。

1.3.8 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，且只有当收到以同种格式封装的 LLDP 报文时，设备才会对其进行处理。
- 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，且只有当收到以同种格式封装的 LLDP 报文时，设备才会对其进行处理。

LLDP 报文的缺省封装格式为 Ethernet II 格式。如果邻居设备以 SNAP 格式封装 LLDP 报文，用户可在本地设备上也将 LLDP 报文的封装格式改为 SNAP 格式，以保证与邻居设备的正常通信。

表1-13 配置 LLDP 报文的封装格式

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置LLDP报文的封装格式为SNAP格式		**lldp encapsulation snap**	必选 缺省情况下，LLDP报文的封装格式为Ethernet II格式

说明

LLDP CDP（Cisco Discovery Protocol，思科发现协议）报文的封装格式只能为 SNAP 格式，不能为 Ethernet II 格式。

1.4 配置LLDP兼容CDP功能

当设备与只支持 CDP（Cisco Discovery Protocol，思科发现协议）不支持 LLDP 的设备直连时，可以通过配置 LLDP 兼容 CDP 功能与直连设备交互信息。

配置LLDP兼容CDP功能后，当设备接收到邻居设备的CDP报文时，会向邻居设备发送CDP报文。设备向邻居设备发送的CDP报文中所包含的信息如 表 1-14 所示。

表1-14 CDP 报文信息描述表

字段	描述
Device ID	设备ID，为本设备的桥MAC地址

字段	描述
Addresses	端口IPv4地址 端口IPv4地址为该端口允许通过的、对应VLAN接口上配置有IPv4地址且处于up状态的最小VLAN的主IPv4地址，如果该端口允许通过的所有VLAN所对应的VLAN接口上都未配置IPv4地址或均处于down状态，则不发布端口IPv4地址
Port ID	端口ID
Capabilities	设备能力：Switch
Software Version	产品的软件版本
Platform	设备型号
Duplex	端口双工状态
MTU	最大传输单元
System Name	系统名称
Native VLAN	端口的PVID
Voice VLAN	通过**lldp voice-vlan**命令指定的VLAN或端口配置的Voice VLAN

如果需要查看 CDP 邻居设备发送给本设备的信息，请查看 **display lldp neighbor-information** 显示信息中 CDP neighbor-information 相关字段。

当设备与 Cisco 的 IP 电话直连时，IP 电话将会向设备发送 CDP 报文以请求在设备上所配 Voice VLAN 的 VLAN ID；如果在指定时间内没有收到设备发送的 Voice VLAN 的 VLAN ID，IP 电话将会把语音数据流以 untagged 方式发送，从而导致语音数据流与其它类型的数据流混在一起，无法进行区分。

通过在设备上配置 LLDP 兼容 CDP 功能，可以利用 LLDP 来接收、识别从 IP 电话接收的 CDP 报文，并向 IP 电话发送 CDP 报文，该 CDP 报文携带设备所配 Voice VLAN 的 TLV，使 IP 电话完成 Voice VLAN 的自动配置。语音数据流将被限制在配置的 Voice VLAN 内，与其它数据流区分开来。有关 Voice VLAN 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“Voice VLAN”。

1.4.2 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。
- 在设备与支持 CDP 的设备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。

1.4.3 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。

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**	-

操作		命令	说明
使能LLDP兼容CDP功能		**lldp compliance cdp**	必选 缺省情况下，LLDP兼容CDP功能处于关闭状态
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置LLDP兼容CDP功能的工作模式为TxRx		**lldp compliance admin-status cdp txrx**	必选 缺省情况下，LLDP兼容CDP功能的工作模式为Disable

注意

由于 CDP 报文所携 Time To Live TLV 中 TTL 的最大值为 255，而 TTL = Min（65535，（TTL 乘数 × LLDP 报文的发送间隔））， 因此为保证 LLDP 兼容 CDP 功能的正常运行，应确保 TTL 乘数与 LLDP 报文的发送间隔的乘积不大于 255。

1.5 配置LLDP Trap功能

使能 LLDP 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邻居、与原来邻居的通信链路发生故障等重要事件。

LLDP 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 功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能LLDP Trap功能		**lldp notification remote-change enable**	必选 缺省情况下，LLDP Trap功能处于关闭状态
退回系统视图		**quit**	-
配置LLDP Trap信息的发送间隔		**lldp timer notification-interval** *interval*	可选 缺省情况下，LLDP Trap信息的发送间隔为5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
显示待发送的LLDP信息	**display lldp local-information** [**global** | **interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示由邻居设备发来的LLDP信息	**display lldp neighbor-information** [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示LLDP的统计信息	**display lldp statistics** [**global** | **interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示LLDP的状态信息	**display lldp status** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示接口上可发送的可选TLV信息	**display lldp tlv-config** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.7 LLDP典型配置举例

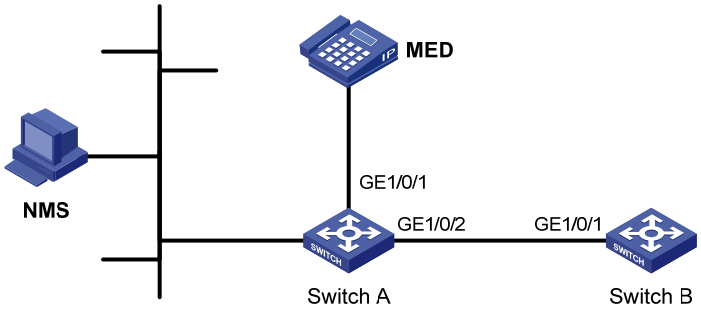
1.7.1 LLDP基本功能配置举例

1. 组网需求

- NMS（Network Management System，网络管理系统）通过以太网与 Switch A 相连，Switch A 通过接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别与 MED 设备和 Switch B 相连。
- 通过在 Switch A 和 Switch B 上配置 LLDP 功能，使 NMS 可以对 Switch A 与 MED 设备之间、以及 Switch A 与 Switch B 之间链路的通信情况进行判断。

2. 组网图

图1-4 LLDP 基本功能配置组网图



3. 配置步骤

(1) 配置 Switch A

全局使能 LLDP 功能。

```
<SwitchA> system-view
[SwitchA] lldp enable
```

在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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。

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

(2) 配置 Switch B

全局使能 LLDP 功能。

```
<SwitchB> system-view
[SwitchB] lldp enable
```

在接口 GigabitEthernet1/0/1 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。

```
[SwitchB] interface GigabitEthernet1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

(3) 检验配置效果

显示 Switch A 上所有接口的 LLDP 状态信息。

```
[SwitchA] display lldp status
Global status of LLDP: Enable
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
Hold multiplier                : 4
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3

Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

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

Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

Number of neighbors:             1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 3
```

由此可见，Switch A 的接口 GigabitEthernet1/0/1 上连接了一个 MED 邻居设备，GigabitEthernet1/0/2 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 Switch A 和 Switch B 间的链路断掉后，再显示 Switch A 上所有接口的 LLDP 状态信息。

```
[SwitchA] 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
Hold multiplier                : 4
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3

Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

Number of neighbors:             1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 5

Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

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

由此可见，Switch A 的接口 GigabitEthernet1/0/2 上已经没有任何邻居设备了。

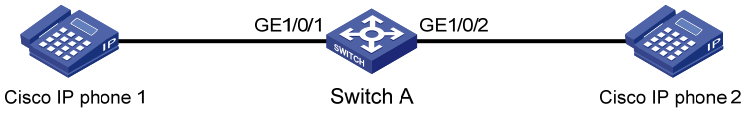
1.7.2 LLDP兼容CDP功能配置举例

1. 组网需求

- Switch A 通过接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别与两部 Cisco 的 IP 电话相连，这两部 IP 电话发送的是 Tagged 语音数据；
- 在 Switch A 上配置 VLAN ID 为 2 的 Voice VLAN，通过在 Switch A 上配置 LLDP 兼容 CDP 功能使 IP 电话完成 Voice VLAN 的自动配置，以使语音数据流被限制在 Voice VLAN 内，与其它数据流区分开来。

2. 组网图

图1-5 LLDP 兼容 CDP 功能配置组网图



3. 配置步骤

(1) 在 Switch A 上配置 Voice VLAN

创建 VLAN 2。

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

分别将接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为 Trunk 端口，并使能 Voice VLAN 功能。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/2] quit
```

(2) 在 Switch A 上配置 LLDP 兼容 CDP 功能

全局使能 LLDP 功能以及 LLDP 兼容 CDP 功能。

```
[SwitchA] lldp enable
[SwitchA] lldp compliance cdp
```

在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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），配置 LLDP 工作模式为 TxRx，并配置 LLDP 兼容 CDP 功能的工作模式为 TxRx。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

(3) 检验配置效果

显示 Switch A 上的邻居信息。

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  CDP neighbor index : 1
  Chassis ID         : SEP00141CBCDBFE
  Port ID            : Port 1
  Sofrware version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
```

```
  Duplex             : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  CDP neighbor index : 2
  Chassis ID         : SEP00141CBCDBFF
  Port ID            : Port 1
  Sofrware version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex             : Full
```

由此可见，Switch A 已发现了分别连接在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上的 IP 电话，并获取到了相关的设备信息。

目 录

1 业务环回组配置

1.1 业务环回组简介

为了增加业务重定向的吞吐能力，可以将一台设备上的多个以太网端口绑定在一起，使其在逻辑上呈现为一条链路，从而实现增加链路带宽、进行负载分担的目的，这些端口就构成了业务环回组。业务环回组中应当包含至少一个以太网端口，这样的端口就称为业务环回组的成员端口，也叫业务环回端口。

譬如，将一台设备的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 添加到同一个业务环回组中之后，这三个端口在逻辑上将呈现为一条链路，该链路的带宽等于这三个端口带宽的总和，从而达到了增加带宽的目的；同时，这三个端口之间还能够对业务流量进行负载分担。

1.1.1 业务环回组支持的业务类型

业务环回组只能应用于特定的业务类型，其支持的业务类型包括以下几种：

- Tunnel：用于支持单播隧道业务。
- Multicast tunnel：用于支持组播隧道业务。

1.1.2 业务环回组对成员端口的要求

要成为业务环回组的成员端口，必须满足下列条件：

- 端口必须支持该业务环回组的业务类型。
- 允许端口上有 QoS 和 ACL 的配置，但不允许有下列配置：速率、双工模式等物理配置以及 MSTP、LLDP、NDP、隔离组的上行口或下行口、802.1X、MAC 地址认证、端口安全模式以及 IP Source Guard 功能。
- 端口的链路类型必须为 Access 类型。
- 端口尚未加入任何聚合组或业务环回组。

1.1.3 业务环回组成员端口的状态

1. 成员端口状态的分类

业务环回组中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用户业务流量的环回，处于此状态的成员端口简称为“选中端口”。
- 非选中（Unselected）状态：此状态下的成员端口不能参与用户业务流量的环回，处于此状态的成员端口简称为“非选中端口”。

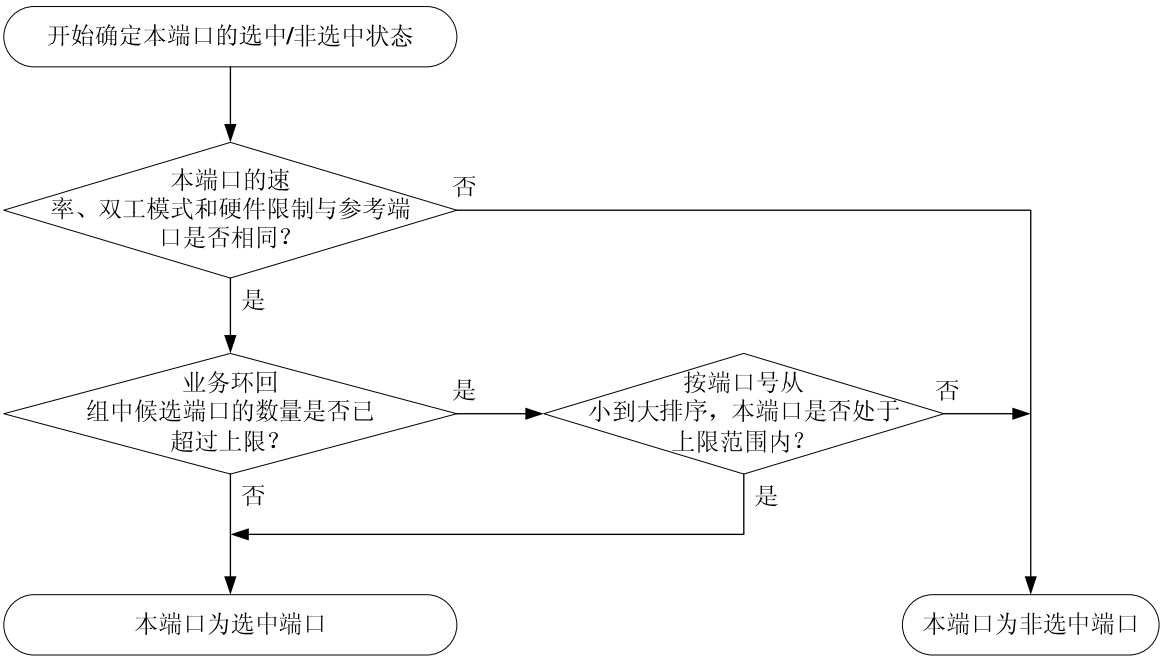
2. 成员端口状态的确定

系统按照以下方法来确定业务环回组中成员端口的状态：

(1) 选择双工模式为全双工的且速率最高的成员端口作为参考端口，如果速率相同，则选择端口号最小的成员端口作为参考端口。

(2) 按照 图 1-1 所示的流程来确定成员端口的状态。

图1-1 业务环回组中成员端口状态的确定流程



说明

当有新的端口加入业务环回组时，该组中所有成员端口的状态都将按照上述方法重新确定。

1.2 配置业务环回组

表1-1 配置业务环回组

操作	命令	说明
进入系统视图	**system-view**	-
创建业务环回组，并指定其业务类型	**service-loopback group** *number* **type** { **multicast-tunnel** | **tunnel** } *	必选 本系列交换机中S5500-28SC-HI和S5500-52SC-HI不支持**multicast-tunnel**参数
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
将端口加入业务环回组	**port service-loopback group** *number*	必选 缺省情况下，端口不属于任何业务环回组 在不同端口上执行本命令，可以将多个端口加入到业务环回组中

注意

- 业务环回组只有在被其他特性引用后才能处理业务。业务环回组一旦创建即可被引用，且一个业务环回组可以同时被多个特性引用。
- 每种业务类型的业务环回组在全局只能有一个。用户可以在业务环回组创建后更改其业务类型，但以下情况除外：将业务类型修改为已存在的业务类型；业务环回组已被其他特性引用；业务环回组中的成员端口存在与修改后的业务类型相冲突的属性。
- 建议不要删除已被其他特性引用的业务环回组，以免影响其他特性的正常使用。

1.3 业务环回组显示与维护

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业务环回组的运行情况，通过查看显示信息验证配置的效果。

表1-2 业务环回组显示与维护

操作	命令
显示业务环回组的信息	**display service-loopback group** [*number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.4 业务环回组典型配置举例

1. 组网需求

Device A 上的所有以太网端口都支持 Tunnel 业务类型，通过配置将端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 加入到业务环回组中以实现对 Tunnel 业务类型增加带宽并进行负载分担的目的。

2. 配置步骤

创建业务环回组 1，并指定其业务类型为 Tunnel 类型。

```
<DeviceA> system-view
[DeviceA] service-loopback group 1 type tunnel
```

分别在端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 上关闭 MSTP、NDP 和 LLDP 功能，并将其加入业务环回组 1。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] undo ndp enable
[DeviceA-GigabitEthernet1/0/1] undo lldp enable
[DeviceA-GigabitEthernet1/0/1] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] undo ndp enable
```

```
[DeviceA-GigabitEthernet1/0/2] undo lldp enable
[DeviceA-GigabitEthernet1/0/2] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] undo ndp enable
[DeviceA-GigabitEthernet1/0/3] undo lldp enable
[DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

创建 Tunnel 逻辑接口 1，并在该接口上引用业务环回组 1。

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] service-loopback-group 1
```

目 录

1 MVRP

1.1 MVRP简介

MRP（Multiple Registration Protocol，多属性注册协议）作为一个属性注册协议的载体，可以用来传播属性消息。MVRP（Multiple VLAN Registration Protocol，多 VLAN 注册协议）是 MRP 的一种应用，用于在设备间发布并学习 VLAN 配置信息。当设备启动了 MVRP 之后，设备将本地的 VLAN 配置信息向其它设备传播，同时还能够接收来自其它设备的 VLAN 配置信息，并动态更新本地的 VLAN 配置信息（包括当前的 VLAN 成员及这些 VLAN 成员可通过哪个端口到达等），从而使所有设备的 VLAN 信息都达成一致，极大减轻了网络管理员的 VLAN 配置工作。在网络拓扑发生变化后，MVRP 还能根据新的拓扑重新发布及学习 VLAN，做到 VLAN 配置信息实时与网络拓扑同步更新。

MRP 和 MVRP 分别是 GARP（Generic Attribute Registration Protocol，通用属性注册协议）及 GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）的升级版本，用于替代 GARP 和 GVRP 协议。相比 GVRP，MVRP 有如下优点：

- GVRP 不支持 MSTI（Multiple Spanning Tree Instance，多生成树实例），而 MVRP 支持在 MSTI 的基础上运行，从而为不同 VLAN 的冗余链路计算及负载分担实现提供了便利。
- MVRP 可以有效减少在传递同样多 VLAN 信息量时的报文数量，从而提高了属性声明效率。

有关 GVRP 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“GVRP”。有关 MSTI 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

1.1.1 MRP简介

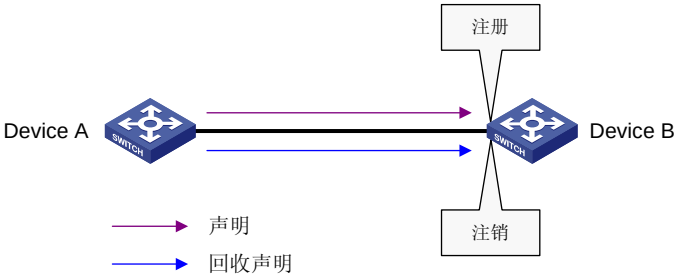
MRP 支持在基于 MSTI 的基础上，协助同一局域网内各成员之间声明、传播和注册某种信息（如 VLAN）。

1. MRP实现机制

设备上每一个参与协议的端口都可以视为一个应用实体，当 MRP 应用（如 MVRP）在端口上启动之后，该端口就可视为一个 MRP 应用实体（以下简称 MRP 实体，同样的，MVRP 应用实体简称 MVRP 实体）。

如 图 1-1 所示，MRP实体通过发送两种协议报文（声明或回收声明），来通知其它MRP实体来注册或注销自己的属性信息，并根据其它MRP实体发来的声明或回收声明来注册或注销对方的属性信息。通过MRP机制，一个MRP实体上的配置信息会迅速传遍整个局域网。

图1-1 MRP 实现机制示意图



对于 MVRP，实现 VLAN 属性注册和注销的方式如下：

- 当端口收到一个 VLAN 属性的声明时，该端口将注册该声明中所包含的 VLAN 属性（即将该端口加入到该 VLAN 中）。

- 当端口收到一个 VLAN 属性的回收声明时，该端口将注销该声明中所包含的 VLAN 属性（即将该端口退出该 VLAN）。

说明

图 1-1 可以看作是MVRP协议在某个MSTI上的实现机制，属于比较简单的一种情况，在实际应用的复杂组网情况下，可能存在多个MSTI，而VLAN的注册和注销只会在各自的MSTI上进行。

---

2. MRP消息

MRP 实体之间通过传递各种 MRP 消息来完成信息交换。MRP 消息主要包括 Join 消息、New 消息、Leave 消息和 LeaveAll 消息，它们通过互相配合来确保信息的注册或注销。其中，Join 消息和 New 消息属于声明协议报文，Leave 消息和 LeaveAll 消息属于回收声明协议报文。

(1) Join 消息

- 当一个 MRP 实体配置了某些属性，需要其它 MRP 实体来注册自己的属性信息时，它会对外发送 Join 消息。
- 当一个 MRP 实体收到来自其它实体的 Join 消息时，它会向除发送该 Join 消息的实体外的其它实体发送 Join 消息。

Join 消息又分为 JoinEmpty 和 JoinIn 两种，二者的区别如下：

- JoinEmpty：用于声明一个本身没有注册的属性。比如设备上存在某静态 VLAN，即使之后又通过 MRP 消息学习到该 VLAN，也不会改变该 VLAN 在本设备上的属性，所以该 VLAN 不能算作注册属性，这时对应的 Join 消息就为 JoinEmpty 消息。
- JoinIn：用于声明一个本身已经注册的属性。比如设备通过 MRP 消息学习到某 VLAN，并在本设备上动态创建该 VLAN，这时对应的 Join 消息就为 JoinIn 消息。

(2) New 消息

New 消息的作用和 Join 消息比较类似，都是为了实现属性的注册。

- 当 MSTP（Multiple Spanning Tree Protocol，多生成树协议）拓扑变化时，MRP 实体需要对外发送 New 消息声明拓扑变化。
- 当一个 MRP 实体收到来自其它实体的 New 消息时，它会向除发送该 New 消息的实体外的其它实体发送 New 消息。

(3) Leave 消息

- 当一个 MRP 实体注销了某些属性，需要其它实体进行同步注销时，它会对外发送 Leave 消息。
- 当一个 MRP 实体收到来自其它实体的 Leave 消息时，它会向除发送该 Leave 消息的实体外的其它实体发送 Leave 消息。

(4) LeaveAll 消息

- 每个 MRP 实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，MRP 实体就会向对端实体发送 LeaveAll 消息，使本实体和对端实体分别注销并重新注册所有的属性信息，从而周期性地清除网络中的垃圾属性。
- 当一个 MRP 实体收到来自对端实体的 LeaveAll 消息时，它会根据自身属性状态决定是否发送 Join 消息要求对端实体重新注册某属性信息。

3. MRP定时器

MRP 定义了四种定时器，用于控制各种 MRP 消息的发送。

(1) Periodic 定时器

每个 MRP 实体启动时都会启动各自的 Periodic 定时器，来控制 MRP 消息的发送。该定时器超时前，MRP 应用实体收集需要发送的 MRP 消息，在该定时器超时时，将所有待发送的 MRP 消息

封装成尽可能少的报文发送出去，这样减少了报文发送数量，同时可以定期发送报文。随后再重新启动 Periodic 定时器，开始新一轮的循环。


说明

Periodic 定时器允许用户通过命令行开启或关闭。如果关闭 Periodic 定时器，则不再周期发送 MRP 消息，仅在 LeaveAll 定时器超时或者收到对端的 LeaveAll 消息的情况下会发送 MRP 消息。

(2) Join 定时器

Join 定时器用来控制 Join 消息的发送。为了保证消息能够可靠地发送到其它实体，MRP 实体在发出 Join 消息后将等待一个 Join 定时器的时间间隔。如果在该定时器超时前收到了其它实体发来的 JoinIn 消息，且该 JoinIn 消息携带的属性信息与发出的 Join 消息携带的属性信息一致，便不再重发该 Join 消息。在该定时器超时后，当 Periodic 定时器也超时，它将重发一次该 Join 消息；否则不发送该 Join 消息。

(3) Leave 定时器

Leave 定时器用来控制属性的注销。当 MRP 实体需要其它实体注销自己的某属性信息时会发送 Leave 消息，收到该消息的实体将启动 Leave 定时器。如果启动 Leave 定时器的实体直到该定时器超时还未收到该属性信息的 Join 消息，该属性信息才会被注销。当实体发送和收到 LeaveAll 消息时，也会启动 Leave 定时器，在 Leave 定时器超时后，如果未收到某些原有属性信息的 Join 消息，这些属性信息会被注销。

(4) LeaveAll 定时器

每个 MRP 实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，该 MRP 实体就会向对端实体发送 LeaveAll 消息，随后再重新启动 LeaveAll 定时器，开始新一轮的循环，对端实体在收到 LeaveAll 消息后也重新启动 LeaveAll 定时器。


说明

LeaveAll 定时器具有抑制机制，即当某个 MRP 实体的 LeaveAll 定时器超时后，会向对端实体发送 LeaveAll 消息，对端实体在收到 LeaveAll 消息时，重启本实体的 LeaveAll 定时器，不再发送 LeaveAll 消息，从而有效抑制网络中的 LeaveAll 消息数。为了防止每次都是同一实体的 LeaveAll 定时器先超时，每次 LeaveAll 定时器重启时，LeaveAll 定时器的值都将在一定范围内随机变动。

1.1.2 MVRP注册模式

MVRP 传播的 VLAN 配置信息既包括本地手工配置的静态信息，也包括来自其它设备的动态信息。我们将本地手工创建的 VLAN 称为静态 VLAN，通过 MVRP 协议学习到的 VLAN 称为动态 VLAN。MVRP 有三种注册模式，不同注册模式对静态 VLAN 和动态 VLAN 的处理方式也不同。

(1) Normal 模式

该模式下的 MVRP 实体允许进行动态 VLAN 的注册或注销，并允许发送动态和静态 VLAN 的声明。

(2) Fixed 模式

该模式下的 MVRP 实体禁止动态 VLAN 的注销，但允许发送动态和静态 VLAN 的声明，收到的 MVRP 报文会被忽略丢弃。也就是说，该模式下的实体，学习到的动态 VLAN 是不会被注销的，同时也不会学习到新的动态 VLAN。

(3) Forbidden 模式

该模式下的 MVRP 实体禁止进行动态 VLAN 的注册，但允许发送动态和静态 VLAN 的声明，收到的 MVRP 报文会被忽略丢弃。也就是说，该模式下的实体，不允许进行动态 VLAN 的注册，一旦在配置该模式前学习到的动态 VLAN 被注销后，不会重新进行学习。

1.1.3 协议规范

与 MVRP 相关的协议规范有：

- IEEE 802.1ak：IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks – Amendment 07：Multiple Registration Protocol

1.2 MVRP配置任务简介

表1-1 MVRP 配置任务简介

配置任务	说明	详细配置
使能 MVRP 功能	必选	1.3.2
配置 MVRP 注册模式	可选	1.3.3
配置 MRP 定时器	可选	1.3.4
配置兼容 GVRP 功能	可选	1.3.5

说明

如果二层以太网接口加入了聚合组，则加入聚合组之前和加入聚合组之后在该接口上进行的 MVRP 相关配置不会生效；该接口退出聚合组后，MVRP 的配置才会生效。

1.3 配置MVRP功能

1.3.1 配置准备

- 由于 MVRP 需要基于 MSTI 运行，因此在配置 MVRP 时，需要保证当前网络内所有 MSTI 都生效，即网络中设备都需要至少存在一个 MSTI 对应的 VLAN 以保证 MSTI 能够生效。
- MVRP 功能只能在 Trunk 端口上配置，因此需要配置要运行 MVRP 功能的端口链路类型为 Trunk 类型。

1.3.2 使能MVRP功能

注意

- MVRP 功能只能与 STP、RSTP 或 MSTP 配合使用，而无法与其它二层网络拓扑协议（如 PVST、RRPP 和 Smart Link）配合使用。MVRP 报文的收发不受 STP/RSTP/MSTP 阻塞端口影响。有关 STP、RSTP、MSTP 和 PVST 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”；有关 RRPP 的详细介绍，请参见“可靠性配置指导”中的“RRPP”；有关 Smart Link 的详细介绍，请参见“可靠性配置指导”中的 “Smart Link”。
- 建议不要同时启用远程端口镜像功能和 MVRP 功能，否则 MVRP 可能将远程镜像 VLAN 注册到错误的端口上，导致镜像目的端口会收到很多不必要的报文。有关远程端口镜像的详细介绍，请参见“网络管理和监控配置指导”中的“镜像”。
- 在二层聚合接口上启用了 MVRP 功能后，会同时在二层聚合接口和对应的所有选中成员端口上进行动态 VLAN 的注册或注销。

表1-2 使能 MVRP 功能

操作		命令	说明
进入系统视图		**system-view**	-
全局使能 MVRP 功能		**mvrp global enable**	必选 缺省情况下，全局的 MVRP 功能处于关闭状态 要在端口上使能 MVRP 功能，必须先全局使能 MVRP 功能
进入相应视图	进入二层以太网接口或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置允许指定的 VLAN 通过当前 Trunk 端口		**port trunk permit vlan {** *vlan-list* **| all }**	必选 缺省情况下，Trunk 端口只允许 VLAN 1 通过 需要保证所有注册的 VLAN 都能够从该端口通过
在端口上使能 MVRP 功能		**mvrp enable**	必选 缺省情况下，端口上的 MVRP 功能处于关闭状态

说明

有关 **port link-type trunk** 和 **port trunk permit vlan** 命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

1.3.3 配置MVRP注册模式

表1-3 配置 MVRP 注册模式

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网接口或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置当前端口的MVRP注册模式		**mvrp registration** { **fixed** | **forbidden** | **normal** }	可选 缺省情况下，当前端口的 MVRP 端口注册模式为 Normal 模式

1.3.4 配置MRP定时器

注意

MRP 定时器值的改变将在当前端口所有运行的 MRP 应用（如 MVRP）上生效。MRP 定时器的配置值建议全网配置一致，否则在配置不一致的情况下会出现 VLAN 频繁注册/注销的情况。

说明

设备的每个端口上都独立维护自己的 Periodic 定时器、Join 定时器和 LeaveAll 定时器，而每个端口的每个属性上维护着一个 Leave 定时器。

表1-4 配置 MRP 定时器

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网接口或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置 LeaveAll 定时器		**mrp timer leaveall** *timer-value*	可选 缺省情况下，LeaveAll 定时器的值为 1000 厘秒
配置 Join 定时器		**mrp timer join** *timer-value*	可选 缺省情况下，Join 定时器的值为 20 厘秒
配置 Leave 定时器		**mrp timer leave** *timer-value*	可选 缺省情况下，Leave 定时器的值为 60 厘秒
配置 Periodic 定时器		**mrp timer periodic** *timer-value*	可选 缺省情况下，Periodic 定时器的值为 100 厘秒

如 表 1-5 所示，Join定时器、Leave定时器和LeaveAll定时器的取值范围之间存在着相互制约的关系：

- 当配置某定时器时，如果配置值超出了该定时器当前有效的取值范围，则该配置不成功。用户可以通过改变相关定时器的值来重新进行配置。
- 当用户欲恢复各定时器的值为缺省值时，须按照 Join 定时器->Leave 定时器->LeaveAll 定时器的顺序依次恢复。

表1-5 Join 定时器、Leave 定时器和 LeaveAll 定时器取值范围间的制约关系

定时器	取值下限	取值上限
Join 定时器	20 厘秒	小于 Leave 定时器值的一半
Leave 定时器	大于 Join 定时器值的两倍	小于 LeaveAll 定时器的值
LeaveAll 定时器	大于所有端口上 Leave 定时器的值	32760 厘秒

说明

Periodic 定时器的值可以在任何时刻恢复为缺省值。

1.3.5 配置兼容GVRP功能

注意

- 在配置兼容 GVRP 功能后，MVRP 功能只能与 STP 或 RSTP 配合使用，而不能与 MSTP 配合使用，否则可能会造成网络工作的不正常。
- 在配置兼容 GVRP 功能后，建议关闭 Periodic 定时器，否则当系统繁忙时，容易造成 VLAN 状态的频繁改变。

MVRP 允许兼容 GVRP。当对端设备支持 GVRP 功能时，可以通过配置兼容 GVRP 功能，允许本端设备同时接收发送 MVRP 和 GVRP 报文。

表1-6 配置兼容 GVRP 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置 MVRP 工作在兼容 GVRP 的模式	**mvrp gvrp-compliance enable**	必选 缺省情况下，MVRP 不兼容 GVRP 模式

1.4 MVRP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 MVRP 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 MVRP 的统计信息。

表1-7 MVRP 显示和维护

操作	命令
显示指定端口及 VLAN 的 MVRP 接口状态信息	**display mvrp state interface** *interface-type interface-number* **vlan** *vlan-id* [| { **begin** | **exclude** | **include** } *regular-expression*]
显示 MVRP 的运行状态信息	**display mvrp running-status** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]
显示 MVRP 的统计信息	**display mvrp statistics** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]
显示端口当前对动态 VLAN 的操作信息	**display mvrp vlan-operation interface** *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]
清除端口的 MVRP 统计信息	**reset mvrp statistics** [**interface** *interface-list*]

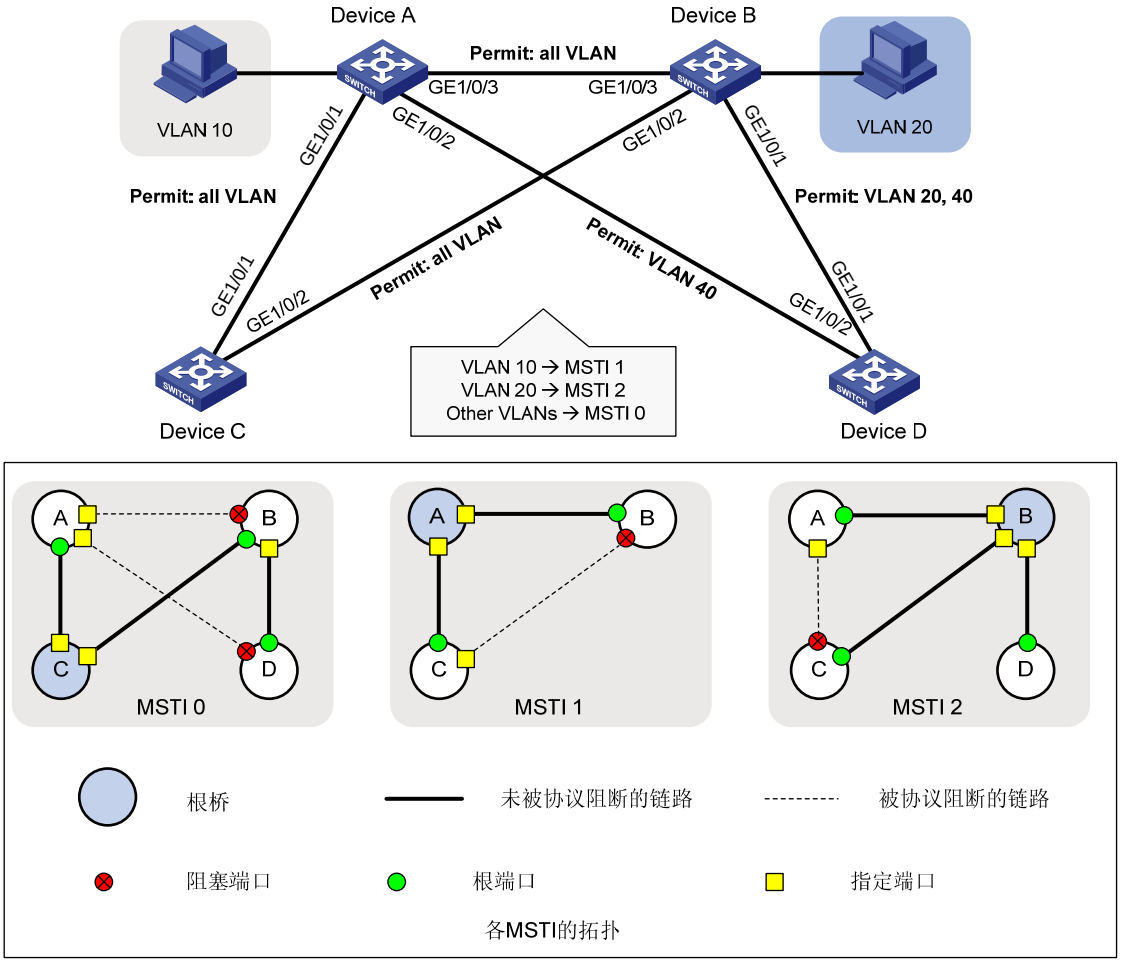
1.5 MVRP典型配置举例

1. 组网需求

- 如 图 1-2 所示，Device A、Device B、Device C和Device D分别相连。
- 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 20 沿 MSTI 2 转发，其它 VLAN 沿 MSTI 0 转发。
- 通过启用 MVRP 功能，并配置 MVRP 的注册模式为 Normal 模式，来实现 Device A、Device B、Device C 和 Device D 之间的所有动态和静态 VLAN 的注册和注销，从而保持各 MSTI 中 VLAN 配置的一致。
- 在网络稳定后，配置 Device B 上与 Device A 相连端口的 MVRP 注册模式为 Fixed 模式，使 Device B 学习到的的动态 VLAN 不被注销。

2. 组网图

图1-2 MVRP 配置组网图



3. 配置步骤

(1) 配置 Device A

进入 MST 域视图。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
```

配置 MST 域的域名、VLAN 映射关系和修订级别。

```
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 20
[DeviceA-mst-region] revision-level 0
```

手工激活 MST 域的配置。

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

定义 Device A 为 MSTI 1 的根桥。

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

全局使能生成树协议。

```
[DeviceA] stp enable
```

全局使能 MVRP 功能。

```
[DeviceA] mvrp global enable
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 口，并允许所有 VLAN 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/1 上使能 MVRP。
```
[DeviceA-GigabitEthernet1/0/1] mvrp enable
[DeviceA-GigabitEthernet1/0/1] quit
```
将端口 GigabitEthernet1/0/2 配置为 Trunk 口，并允许 VLAN 40 通过。
```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 40
```
在端口 GigabitEthernet1/0/2 上使能 MVRP。
```
[DeviceA-GigabitEthernet1/0/2] mvrp enable
[DeviceA-GigabitEthernet1/0/2] quit
```
将端口 GigabitEthernet1/0/3 配置为 Trunk 口，并允许所有 VLAN 通过。
```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/3 上使能 MVRP。
```
[DeviceA-GigabitEthernet1/0/3] mvrp enable
[DeviceA-GigabitEthernet1/0/3] quit
```
创建 VLAN 10。
```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```
(2)　配置 Device B

进入 MST 域视图。
```
<DeviceB> system-view
[DeviceB] stp region-configuration
```
配置 MST 域的域名、VLAN 映射关系和修订级别。
```
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] revision-level 0
```
手工激活 MST 域的配置。
```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```
定义 Device B 为 MSTI 2 的根桥。
```
[DeviceB] stp instance 2 root primary
```
全局使能生成树协议。
```
[DeviceB] stp enable
```
开启全局 MVRP 功能。
```
[DeviceB] mvrp global enable
```
将端口 GigabitEthernet1/0/1 配置为 Trunk 口，并允许 VLAN 20、VLAN 40 通过。
```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```
在端口 GigabitEthernet1/0/1 上使能 MVRP。
```
[DeviceB-GigabitEthernet1/0/1] mvrp enable
[DeviceB-GigabitEthernet1/0/1] quit
```
将端口 GigabitEthernet1/0/2 配置为 Trunk 口，并允许所有 VLAN 通过。
```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/2 上使能 MVRP。
```
[DeviceB-GigabitEthernet1/0/2] mvrp enable
[DeviceB-GigabitEthernet1/0/2] quit
```
将端口 GigabitEthernet1/0/3 配置为 Trunk 口，并允许所有 VLAN 通过。
```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/3 上使能 MVRP。
```
[DeviceB-GigabitEthernet1/0/3] mvrp enable
[DeviceB-GigabitEthernet1/0/3] quit
```
创建 VLAN 20。
```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```
(3) 配置 Device C

进入 MST 域视图。
```
<DeviceC> system-view
[DeviceC] stp region-configuration
```
配置 MST 域的域名、VLAN 映射关系和修订级别。
```
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 2 vlan 20
[DeviceC-mst-region] revision-level 0
```
手工激活 MST 域的配置。
```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```
定义 Device C 为 MSTI 0 的根桥。
```
[DeviceC] stp instance 0 root primary
```
全局使能生成树协议。
```
[DeviceC] stp enable
```
全局使能 MVRP 功能。
```
[DeviceC] mvrp global enable
```
将端口 GigabitEthernet1/0/1 配置为 Trunk 口，并允许所有 VLAN 通过。
```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/1 上使能 MVRP。
```
[DeviceC-GigabitEthernet1/0/1] mvrp enable
[DeviceC-GigabitEthernet1/0/1] quit
```
将端口 GigabitEthernet1/0/2 配置为 Trunk 口，并允许所有 VLAN 通过。
```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan all
```
在端口 GigabitEthernet1/0/2 上使能 MVRP。
```
[DeviceC-GigabitEthernet1/0/2] mvrp enable
[DeviceC-GigabitEthernet1/0/2] quit
```
(4) 配置 Device D

进入 MST 域视图。

```
<DeviceD> system-view
[DeviceD] stp region-configuration
```
配置 MST 域的域名、VLAN 映射关系和修订级别。
```
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 2 vlan 20
[DeviceD-mst-region] revision-level 0
```
手工激活 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 enable
```
全局使能 MVRP 功能。
```
[DeviceD] mvrp global enable
```
将端口 GigabitEthernet1/0/1 配置为 Trunk 口，并允许 VLAN 20，40 通过。
```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```
在端口 GigabitEthernet1/0/1 上使能 MVRP。
```
[DeviceD-GigabitEthernet1/0/1] mvrp enable
[DeviceD-GigabitEthernet1/0/1] quit
```
将端口 GigabitEthernet1/0/2 配置为 Trunk 口，并允许 VLAN 40 通过。
```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 40
```
在端口 GigabitEthernet1/0/2 上使能 MVRP。
```
[DeviceD-GigabitEthernet1/0/2] mvrp enable
[DeviceD-GigabitEthernet1/0/2] quit
```
4. 验证配置

(1) 验证 Normal 注册模式配置

通过使用 **display mvrp running-status** 命令可以查看 MVRP 本地 VLAN 的信息，验证配置是否生效。

查看 Device A 上的本地 VLAN 信息。
```
[DeviceA] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/2]----
 Config  Status                     : Enabled
```

```
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/3]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default), 20,
```

由此可见，在端口 GigabitEthernet1/0/1 和端口 GigabitEthernet1/0/2 上通过 MVRP 学习到的 VLAN 信息只有 VLAN 1。在端口 GigabitEthernet1/0/3 上通过 MVRP 学习到的 VLAN 信息包括 VLAN 1，以及在 Device B 上创建 VLAN 20 的动态 VLAN 信息。

查看 Device B 上的本地 VLAN 信息。

```
[DeviceB] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/2]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default), 10,

 ----[GigabitEthernet1/0/3]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
```

```
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default), 10,
```

由此可见，在端口 GigabitEthernet1/0/1 上通过 MVRP 学习到的 VLAN 信息只有 VLAN 1。在端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上通过 MVRP 学习到的 VLAN 信息包括 VLAN 1，以及在 Device A 上创建 VLAN 10 的动态 VLAN 信息。

查看 Device C 上的本地 VLAN 信息。

```
[DeviceC] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default), 10, 20,

 ----[GigabitEthernet1/0/2]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
 Periodic Timer                      : 100 (centiseconds)
 LeaveAll Timer                      : 1000 (centiseconds)
 Registration Type                   : Normal
 Local VLANs :
  1(default), 20,
```

由此可见，在端口 GigabitEthernet1/0/1 上通过 MVRP 学习到的 VLAN 信息包括 VLAN 1，以及在 Device A 上创建 VLAN 10 和在 Device B 上创建 VLAN 20 的动态 VLAN 信息。在端口 GigabitEthernet1/0/2 上通过 MVRP 学习到的 VLAN 信息包括 VLAN 1，以及在 Device B 上创建 VLAN 20 的动态 VLAN 信息。

查看 Device D 上的本地 VLAN 信息。

```
[DeviceD] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                      : Enabled
 Running Status                      : Enabled
 Join Timer                          : 20 (centiseconds)
 Leave Timer                         : 60 (centiseconds)
```

```
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default), 20,

 ----[GigabitEthernet1/0/2]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default),
```

由此可见，在端口 GigabitEthernet1/0/1 上通过 MVRP 学习到的 VLAN 信息包括 VLAN 1，以及在 Device B 上创建 VLAN 20 的动态 VLAN 信息。在端口 GigabitEthernet1/0/2 上通过 MVRP 学习到的 VLAN 信息只有 VLAN 1。

(2) 更改注册模式并验证

配置 Device B 上端口 GigabitEthernet1/0/3 的 MVRP 注册模式为 Fixed 模式，使其在 MSTI 1 中学习到的的动态 VLAN 不被注销。

配置端口 GigabitEthernet1/0/3 的 MVRP 注册模式为 Fixed 模式。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] mvrp registration fixed
[DeviceB-GigabitEthernet1/0/3] quit
```

查看 Device B 的端口 GigabitEthernet1/0/1 上 MVRP 本地 VLAN 的信息。

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/3]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Fixed
 Local VLANs :
  1(default), 10,
```

由此可见，此时端口 GigabitEthernet1/0/3 上的 VLAN 信息与没有配置 Fixed 模式时的 VLAN 信息相同。

在 Device A 上删除 VLAN 10。

```
[DeviceA] undo vlan 10
```

查看 Device B 的端口 GigabitEthernet1/0/3 上 MVRP 本地 VLAN 的信息。

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False
```

```
----[GigabitEthernet1/0/3]----
Config  Status                      : Enabled
Running Status                      : Enabled
Join Timer                          : 20 (centiseconds)
Leave Timer                         : 60 (centiseconds)
Periodic Timer                      : 100 (centiseconds)
LeaveAll Timer                      : 1000 (centiseconds)
Registration Type                   : Fixed
Local VLANs :
 1(default), 10,
```

由此可见，端口 GigabitEthernet1/0/3 配置 Fixed 模式后，该端口学习的动态 VLAN 信息不会发生变化。