目 录

1 VLAN

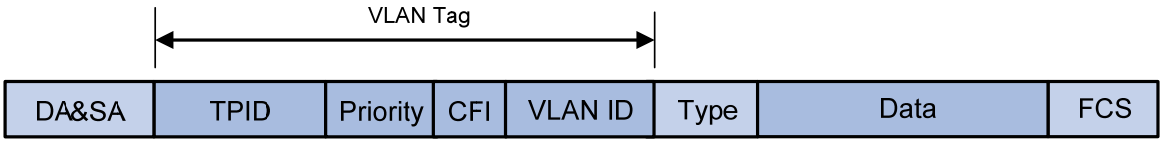
1.1 VLAN简介

VLAN（Virtual Local Area Network，虚拟局域网）技术把一个物理 LAN 划分成多个逻辑的 LAN——VLAN，处于同一 VLAN 的主机能直接互通，而处于不同 VLAN 的主机则不能直接互通，从而增强了局域网的安全性。划分 VLAN 后，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域，有效地限制了广播域的范围。通过 VLAN 可以将不同的主机划分到不同的工作组，同一工作组的主机可以位于不同的物理位置，网络构建和维护更方便灵活。

1.1.1 VLAN报文封装

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

图1-1 VLAN Tag 的组成字段



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

网络设备根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 信息，来对报文进行处理，利用 VLAN ID 来识别报文所属的 VLAN。

说明

以太网支持 Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式，本文以 Ethernet II 型封装为例。802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式添加 VLAN Tag 字段的方式请参见相关协议规范。

对于携带有多层 VLAN Tag 的报文，设备会根据其最外层 VLAN Tag 进行处理，而内层 VLAN Tag 会被视为报文的普通数据部分。

1.1.2 VLAN的划分

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 IP 子网的 VLAN
- 基于协议的 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。

1.1.3 基于端口的VLAN

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，该端口就可以转发该 VLAN 的报文。

1. 端口的链路类型

端口的链路类型分为三种，端口的链路类型决定了端口能否加入多个 VLAN。不同链路类型的端口在转发报文时对 VLAN Tag 的处理方式不同：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。在一些应用场景下，需要使用 Hybrid 端口的功能。比如在 1:2 VLAN 映射中，服务提供商网络的多个 VLAN 的报文在进入用户网络前，需要剥离外层 VLAN Tag，此时 Trunk 端口不能实现该功能，因为 Trunk 端口只能使该端口缺省 VLAN 的报文不带 VLAN Tag 通过。有关 1:2 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”。

2. 端口缺省VLAN

端口缺省 VLAN 简称为 PVID（Port VLAN ID）。当端口收到 Untagged 报文时，会认为该报文所属的 VLAN 为 PVID。

Access 端口的 PVID 就是它所在的 VLAN。

Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置端口 PVID。

3. 端口对报文的处理方式

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 1-1。

表1-1 不同链路类型端口收发报文的差异

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

1.1.4 基于MAC地址的VLAN

基于 MAC 的 VLAN 是根据报文的源 MAC 地址来划分 VLAN。设备维护的 MAC VLAN 表记录了 MAC 地址和 VLAN 的对应关系。这种划分方法的最大优点就是当用户物理位置发生变化，VLAN 不用重新配置。所以这种根据 MAC 地址的划分方法也称为基于用户的 VLAN。

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，开启基于 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 地址匹配 MAC VLAN 表项。首先进行模糊匹配，即查询 MAC VLAN 表中掩码不是全 F 的表项，将源 MAC 地址和掩码相与运算后与 MAC VLAN 表项中的 MAC 地址匹配，如果完全相同，则模糊匹配成功，给报文添加表项中对应的 VLAN Tag 并转发该报文；如果模糊匹配失败，则进行精确匹配，即查询表中掩码为全 F 的表项。如果报文中的源 MAC 地址与某 MAC VLAN 表项中的 MAC 地址完全相同，则精确匹配成功，给报文添加表项中对应的 VLAN Tag 并转发该报文；如果没有找到匹配的 MAC VLAN 表项，则继续按照其他原则（基于 IP 子网的 VLAN、基于协议的 VLAN、基于端口的 VLAN）确定报文所属的 VLAN，给报文添加对应的 VLAN Tag 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；否则丢弃该报文。

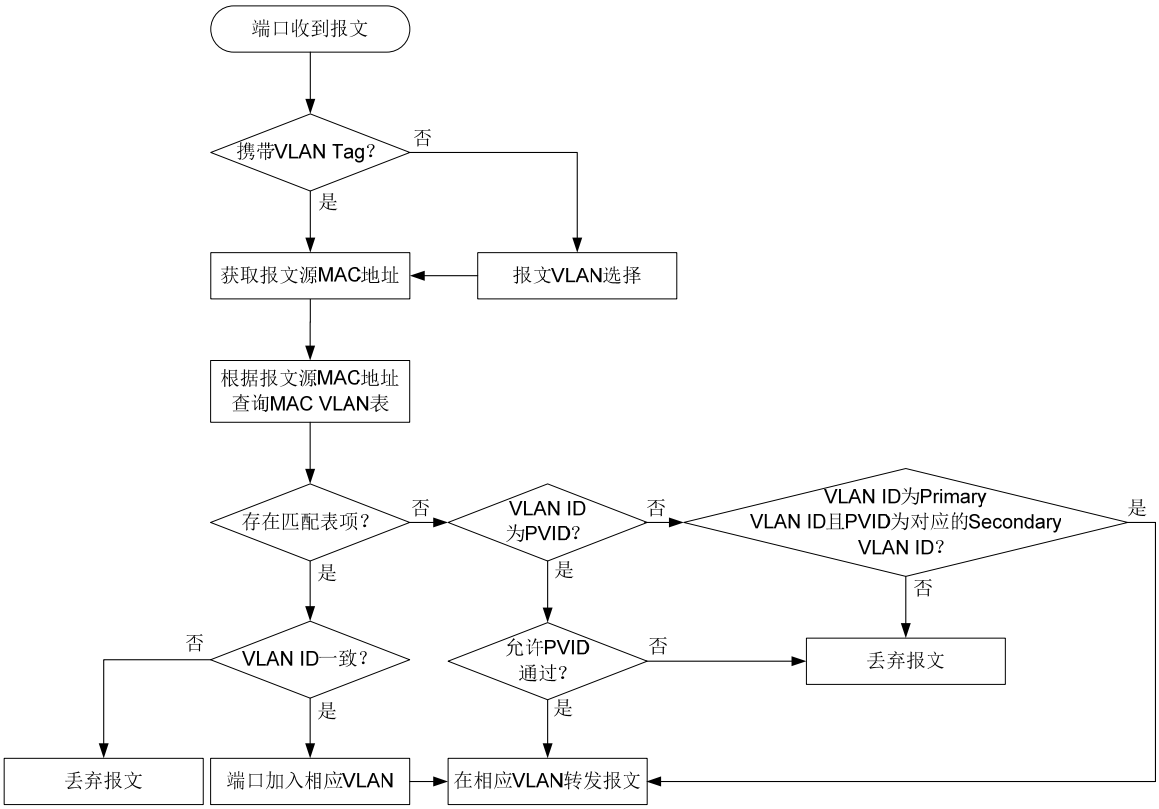
2. 动态触发端口加入静态MAC VLAN

手动配置静态 MAC VLAN 时，如果不能确定从哪些端口收到指定 VLAN 的报文，就不能把相应端口加入到 MAC VLAN。此时可以采用动态触发端口加入静态 MAC VLAN 的方式。在该方式下，配置 MAC VLAN 表项后，需要在端口上开启基于 MAC 的 VLAN 功能和 MAC VLAN 的动态触发功能，不需要手动把端口加入 MAC VLAN。

配置动态触发端口加入静态 MAC VLAN 后，端口在收到报文时，首先判断报文是否携带 VLAN Tag，若带 VLAN Tag，则直接获取报文源 MAC 地址；若不带 VLAN 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 VLAN Tag，并获取该 VLAN Tag），再获取报文源 MAC 地址，然后根据报文的源 MAC 地址和 VLAN 查询静态 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，再检查报文的 VLAN ID 是否与对应表项中的 VLAN ID 一致，若一致，通过该报文动态触发端口加入相应 VLAN，同时转发该报文；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PVID，判断是否报文VLAN ID为Primary VLAN ID且PVID为对应的Secondary VLAN ID，若是，则转发该报文；否则丢弃该报文。处理流程如 图 1-2 所示：

图1-2 动态触发端口加入静态 MAC VLAN 的处理



3. 动态MAC VLAN

动态 MAC VLAN 是由接入认证过程来动态决定接入用户报文所属的 VLAN。该功能需要和接入认证功能（比如端口接入控制方式为 MAC-based 的 802.1X）配合使用，以实现终端的安全、灵活接入。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 信息生成动态 MAC VLAN 表项（要求与已有的静态 MAC VLAN 表项不能冲突），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。

有关接入认证功能的详细介绍请参见“安全配置指导”中的“802.1X”和“MAC 地址认证”。

1.1.5 基于IP子网的VLAN

基于 IP 子网的 VLAN（简称子网 VLAN）是根据报文源 IP 地址及子网掩码来进行划分的。设备从端口收到 Untagged 报文后，会根据报文的源 IP 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 地址的报文划分到指定的 VLAN 中传送。

1.1.6 基于协议的VLAN

基于协议的 VLAN（简称协议 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）等，封装格式有 Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP 等。

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

1.1.7 不同VLAN间的三层互通

不同 VLAN 间的主机不能直接通信，通过在设备上创建并配置 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，此时该 VLAN 接口能对需要跨网段的报文进行三层转发。

1.1.8 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

1.2.1 配置限制和指导

VLAN 1 为系统缺省 VLAN，用户不能手工创建和删除。

动态学习到的 VLAN，以及被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

S5560X-EI 系列交换机支持的 VLAN 数量上限为 1024。

1.2.2 创建VLAN

(1) 进入系统视图。

system-view

(2) 创建 VLAN。请至少选择其中一项进行配置。

- 创建一个 VLAN，并进入 VLAN 视图。

  vlan *vlan-id*

- 批量创建 VLAN，然后进入 VLAN 视图。

  vlan { *vlan-id-list* | **all** }

  vlan *vlan-id*

缺省情况下，系统只有一个缺省 VLAN（VLAN 1）。

(3) （可选）指定 VLAN 的名称。

name *text*

缺省情况下，VLAN 的名称为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的名称为“VLAN 0100”。

(4) （可选）配置 VLAN 的描述信息。

description *text*

缺省情况下，VLAN 的描述信息为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的描述信息为“VLAN 0100”。

1.3 配置基于端口的VLAN

1.3.1 配置限制和指导

- 当执行 **undo vlan** 命令删除的 VLAN 是某个端口的 PVID 时，对 Access 端口，端口的 PVID 会恢复到 VLAN 1；对 Trunk 或 Hybrid 端口，端口的 PVID 配置不会改变，即它们可以使用已经不存在的 VLAN 作为端口 PVID。
- 建议本端设备端口的 PVID 和相连的对端设备端口的 PVID 保持一致。
- 建议保证端口的 PVID 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 PVID 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。

1.3.2 配置基于Access端口的VLAN

1. 简介

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

2. 在VLAN视图下配置基于Access端口的VLAN

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 向当前 VLAN 中添加一个或一组 Access 端口。

port *interface-list*

缺省情况下，系统将所有端口都加入到 VLAN 1。

3. 在接口视图下配置基于Access端口的VLAN

(1) 进入系统视图。

system-view

(2) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口的链路类型为 Access 类型。

port link-type access

缺省情况下，端口的链路类型为 Access。

(4) 将 Access 端口加入到指定 VLAN。

port access vlan *vlan-id*

缺省情况下，所有 Access 端口都属于 VLAN 1。

在将 Access 端口加入到指定 VLAN 之前，该 VLAN 必须已经存在。

1.3.3 配置基于Trunk端口的VLAN

1. 简介

Trunk 端口可以加入多个 VLAN。基于 Trunk 端口的 VLAN 只能在接口视图下配置。

2. 配置限制和指导

Trunk 端口不能直接切换为 Hybrid 端口，只能先将 Trunk 端口配置为 Access 端口，再配置为 Hybrid 端口。

配置端口 PVID 后，必须使用 **port trunk permit vlan** 命令配置允许 PVID 的报文通过，接口才能转发 PVID 的报文。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口的链路类型为 Trunk 类型。

port link-type trunk

缺省情况下，端口的链路类型为 Access 类型。

(4) 允许指定的 VLAN 通过当前 Trunk 端口。

port trunk permit vlan { *vlan-id-list* | **all** }

缺省情况下，Trunk 端口只允许 VLAN 1 的报文通过。

(5) （可选）配置 Trunk 端口的 PVID。

port trunk pvid vlan *vlan-id*

缺省情况下，Trunk 端口的 PVID 为 VLAN 1。

1.3.4 配置基于Hybrid端口的VLAN

1. 简介

Hybrid 端口可以加入多个 VLAN。基于 Hybrid 端口的 VLAN 只能在接口视图下配置。将 Hybrid 端口加入 VLAN 时，指定 VLAN 必须已经存在。

2. 配置限制和指导

Hybrid 端口不能直接切换为 Trunk 端口，只能先将 Hybrid 端口配置为 Access 端口，再配置为 Trunk 端口。

配置端口 PVID 后，必须使用 **port hybrid vlan** 命令配置允许 PVID 的报文通过，出接口才能转发 PVID 的报文。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，端口的链路类型为 Access 类型。

(4) 允许指定的 VLAN 通过当前 Hybrid 端口。

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

缺省情况下，Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

(5) （可选）配置 Hybrid 端口的 PVID。

port hybrid pvid vlan *vlan-id*

缺省情况下，Hybrid 端口的 PVID 为该端口在链路类型为 Access 时的所属 VLAN。

1.4 配置基于MAC的VLAN

1.4.1 配置限制和指导

- 基于 MAC 的 VLAN 只对 Hybrid 端口配置有效。
- Super VLAN 不能作为 MAC VLAN 表项中的 VLAN。
- 请不要在同一个二层以太网接口/二层聚合接口上同时配置基于 MAC 的 VLAN、以太网服务实例与 VSI 关联，或在作为 VXLAN 隧道源接口的二层以太网接口/二层聚合接口上配置基于 MAC 的 VLAN。否则可能导致这些功能不可用。关于 VXLAN 与 VSI 的详细介绍，请参见“VXLAN 配置指导”中的“VXLAN”。

1.4.2 手动配置静态MAC VLAN

(1) 进入系统视图。

system-view

(2) 配置 MAC VLAN 表项。

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]

(3) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(4) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，所有端口的链路类型均为 Access 类型。

(5) 允许基于 MAC 的 VLAN 通过当前 Hybrid 端口。

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

缺省情况下，Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

(6) 开启 MAC VLAN 功能。

mac-vlan enable

缺省情况下，MAC VLAN 功能处于关闭状态。

(7) （可选）配置接口优先根据 MAC 地址来匹配 VLAN。

vlan precedence mac-vlan

缺省情况下，对于基于 MAC 的 VLAN 和基于 IP 子网的 VLAN，优先根据 MAC 地址来匹配 VLAN。

1.4.3 配置动态触发端口加入静态MAC VLAN

1. 功能简介

当端口接收报文的源 MAC 地址精确匹配了 MAC VLAN 表项时，动态触发端口加入 MAC VLAN。源 MAC 地址匹配的 VLAN 必须是静态 VLAN（本地手工创建的 VLAN）。

端口自动加入 MAC VLAN 表项中相应的 VLAN 时，若端口此前未配置允许该 VLAN 通过，则端口自动以 Untagged 方式加入该 VLAN；若端口此前已配置允许该 VLAN 通过，则不改变原有配置。

当端口对 MAC VLAN 的中的报文进行转发时，根据 MAC VLAN 的优先级（MAC 地址对应 VLAN 的 802.1p 优先级）高低来决定报文传输的优先程度。

2. 配置限制和指导

- 如果用户在同一端口上同时配置了 1.4.2 手动配置静态MAC VLAN和 1.4.3 配置动态触发端口加入静态MAC VLAN，此时该端口选择使用后者的功能。
- 不建议 MAC VLAN 的动态触发功能和 802.1X/MAC 地址认证功能同时使用，否则会影响 802.1X/MAC 地址认证功能的正常工作。
- 不建议 MAC VLAN 的动态触发功能与 MAC 地址禁止学习功能或 MAC 地址数学习上限功能同时使用，否则部分流量可能被丢弃：
  - 同时配置 MAC VLAN 的动态触发功能与 MAC 地址禁止学习功能时，仅精确匹配了 MAC VLAN 的报文能够正常转发，未精确匹配的报文将被丢弃。
  - 同时配置 MAC VLAN 的动态触发功能与 MAC 地址数学习上限功能时，当接口学习到的 MAC 地址到达所配置的上限后，仅匹配 MAC 地址表中已学习到的表项的报文能够正常转发，其余报文将被丢弃。
- 配置 MSTP 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，不能完成动态触发端口加入静态 MAC VLAN，因此不建议本功能和多实例 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，不能完成动态触发端口加入静态 MAC VLAN，因此不建议本功能和 PVST 同时使用。
- 当端口配置了自动模式下的 Voice VLAN，又配置本功能时，两个功能可能会相互影响，导致其中某个功能不可用。当端口同时配置了本功能和自动模式下的 Voice VLAN，再取消其中任何一个功能的配置，会导致另一个功能不可用。因此不建议同一端口同时配置本功能和自动模式下的 Voice VLAN。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 MAC VLAN 表项。

mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**dot1q** *priority*]

(3) 进入二层以太网接口视图。

interface *interface-type interface-number*

(4) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，所有端口的链路类型均为 Access 类型。

(5) 开启 MAC VLAN 功能。

mac-vlan enable

缺省情况下，MAC VLAN 功能处于关闭状态。

(6) 开启 MAC VLAN 的动态触发功能。

mac-vlan trigger enable

缺省情况下，MAC VLAN 的动态触发功能处于关闭状态。

(7) （可选）配置接口优先根据 MAC 地址来匹配 VLAN。

vlan precedence mac-vlan

缺省情况下，对于基于 MAC 的 VLAN 和基于 IP 子网的 VLAN，优先根据 MAC 地址来匹配 VLAN。

(8) （可选）配置当报文源 MAC 地址与 MAC VLAN 表项的 MAC 地址未精确匹配时，禁止该报文在 PVID 内转发。

port pvid forbidden

缺省情况下，当报文源 MAC 地址与 MAC VLAN 表项的 MAC 地址未精确匹配时，允许该报文在 PVID 内转发。

1.4.4 配置动态MAC VLAN

(1) 进入系统视图。

system-view

(2) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，所有端口的链路类型均为 Access 类型。

(4) 允许基于 MAC 的 VLAN 通过当前 Hybrid 端口。

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

缺省情况下，Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

(5) 开启 MAC VLAN 功能。

mac-vlan enable

缺省情况下，MAC VLAN 功能处于关闭状态。

(6) 配置接入认证功能。请至少选择其中一项进行配置。

- 配置 802.1X。

  请参见“安全命令参考”中的“802.1X”。

- 配置 MAC 地址认证。

  请参见“安全命令参考”中的“MAC 地址认证”。

1.5 配置基于IP子网的VLAN

1. 配置限制和指导

基于 IP 子网的 VLAN 只对 Hybrid 端口配置有效，只对 Untagged 报文应用。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 VLAN 与指定的 IP 子网或 IP 地址关联。

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

缺省情况下，VLAN 未关联 IP 子网或 IP 地址。

VLAN 关联的 IP 网段或 IP 地址不允许是组播网段或组播地址。

(4) 退回系统视图。

quit

(5) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(6) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，所有端口的链路类型均为 Access 类型。

(7) 允许子网 VLAN 通过当前端口。

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

缺省情况下，Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

(8) 配置端口与子网 VLAN 关联。

port hybrid ip-subnet-vlan vlan *vlan-id*

缺省情况下，端口未关联子网 VLAN。

1.6 配置基于协议的VLAN

1. 功能简介

协议 VLAN 由协议模板定义。协议模板是用来匹配报文所属协议类型的标准，由“协议类型＋封装格式”组成。对于一个协议 VLAN 来说，其绑定的多个协议模板用协议索引（*protocol-index*）来区分；对于不同的协议 VLAN 来说，其绑定的协议模板用协议 *vlan-id* 和 *protocol-index* 来唯一标识。最后通过命令行将协议 VLAN 中的协议模板与端口绑定。

当端口收到 Untagged 报文时，如果该报文携带的协议类型和封装格式与某协议模板相匹配，则为其添加该协议模板绑定的协议 *vlan-id* 的 VLAN Tag，否则为其添加 PVID 的 VLAN Tag。

2. 配置限制和指导

配置协议 VLAN 时，需要注意的是，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，因此，不能将某个 VLAN 同时配置为协议 VLAN 和 Voice VLAN。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 VLAN 与指定的协议模板关联。

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* } }

缺省情况下，当前 VLAN 未关联协议模板。

(4) 退出 VLAN 视图。

quit

(5) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(6) 配置端口的链路类型为 Hybrid 类型。

port link-type hybrid

缺省情况下，所有端口的链路类型均为 Access 类型。

(7) 允许协议 VLAN 通过当前端口。

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

缺省情况下，Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

(8) 配置端口与协议 VLAN 关联。

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

缺省情况下，端口未关联协议 VLAN。

1.7 配置VLAN组

1. 功能简介

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

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

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建一个 VLAN 组，并进入 VLAN 组视图。

vlan-group *group-name*

(3) 在 VLAN 组内添加 VLAN 成员。

vlan-list *vlan-id-list*

缺省情况下，当前 VLAN 组中不存在 VLAN 列表。

可以多次在当前 VLAN 组内添加 VLAN 成员。

1.8 配置VLAN接口

1.8.1 配置限制和指导

配置 VLAN 接口基本属性时，需要注意的是不能对 Sub VLAN 及在 Primary VLAN interface 下配置了三层互通的 Secondary VLAN 创建对应的 VLAN 接口。有关 Sub VLAN 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“Super VLAN”；有关 Secondary VLAN 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“Private VLAN”。

1.8.2 VLAN接口配置任务简介

VLAN 接口配置任务如下：

(1) 创建VLAN接口

(2) （可选）配置处理接口流量的slot

(3) （可选）恢复VLAN接口的缺省配置

1.8.3 配置准备

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。

1.8.4 创建VLAN接口

(1) 进入系统视图。

system-view

(2) 创建 VLAN 接口，并进入 VLAN 接口视图。

interface vlan-interface *interface-number*

(3) 配置 VLAN 接口的 IP 地址。

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

缺省情况下，未配置 VLAN 接口的 IP 地址。

(4) （可选）配置 VLAN 接口的描述信息。

description *text*

缺省情况下，VLAN 接口的描述信息为该 VLAN 接口的接口名，如“Vlan-interface1 Interface”。

(5) （可选）配置 VLAN 接口的 MTU 值。

mtu *size*

缺省情况下，VLAN 接口的 MTU 值为 1500 字节。

(6) （可选）配置 VLAN 接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbps）。

(7) 取消手工关闭 VLAN 接口。

undo shutdown

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。

1.8.5 配置处理接口流量的slot

1. 功能简介

当要求同一个 VLAN 接口的流量必须在同一个 slot 上进行处理时，可以在 VLAN 接口下配置处理接口流量的 slot。

2. 配置步骤

(1) 进入系统视图。

(2) **system-view**

(3) 进入 VLAN 接口视图。

interface vlan-interface *interface-number*

(4) 配置处理接口流量的 slot。

service slot *slot-number*

缺省情况下，未配置处理接口流量的 slot。

1.8.6 恢复VLAN接口的缺省配置

1. 配置限制和指导

注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

2. 配置步骤

(1) 进入系统视图。

(2) **system-view**

(3) 进入 VLAN 接口视图。

interface vlan-interface *interface-number*

(4) 恢复 VLAN 接口的缺省配置。

default

1.9 VLAN显示和维护

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

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

表1-2 VLAN 显示和维护

操作	命令
显示VLAN接口相关信息	**display interface vlan-interface** [*interface-number*] [**brief** [**description** | **down**]]
显示端口关联的子网VLAN的信息	**display ip-subnet-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
显示指定的或所有子网VLAN的信息	**display ip-subnet-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
显示设备上存在的Hybrid或Trunk端口	**display port** { **hybrid** | **trunk** }
显示端口关联的协议VLAN的信息	**display protocol-vlan interface** { interface-type interface-number1 [**to** interface-type interface-number2] | **all** }
显示指定的或所有协议VLAN的信息	**display protocol-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
显示VLAN相关信息	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

操作	命令
显示设备上所有已创建VLAN的概要信息	**display vlan brief**
显示创建的VLAN组及其VLAN成员列表	**display vlan-group** [*group-name*]
清除VLAN接口的统计信息	**reset counters interface vlan-interface** [*interface-number*]

1.10 VLAN典型配置举例

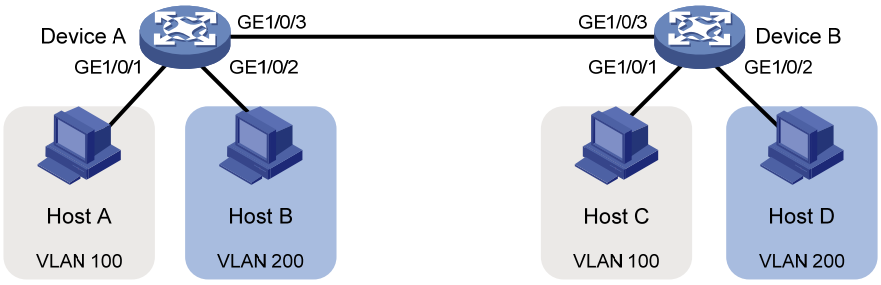
1.10.1 基于端口的VLAN配置举例

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。

2. 组网图

图1-3 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
```

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

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

4. 验证配置

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

(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
```

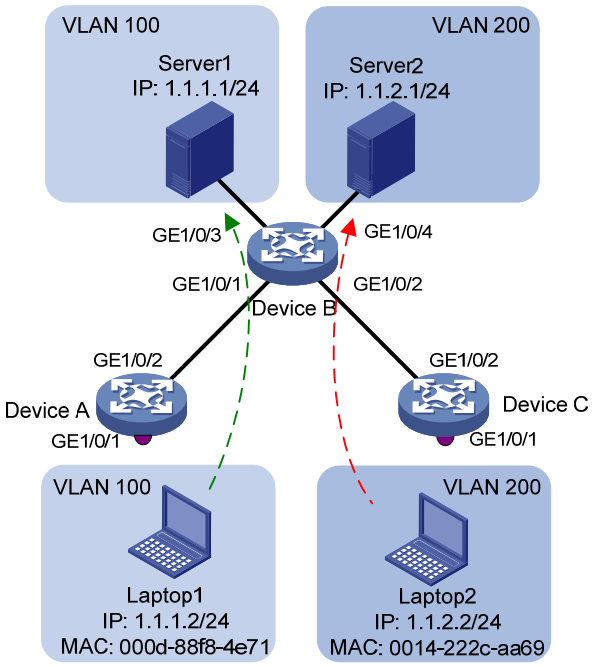
1.10.2 基于MAC的VLAN配置举例

1. 组网需求

- 如下图所示，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。

2. 组网图

图1-4 基于 MAC 的 VLAN 组网图



3. 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
[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 GigabitEthernet1/0/3 加入 VLAN 100，GigabitEthernet1/0/4 加入 VLAN 200。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/3
[DeviceB-vlan100] quit
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/4
[DeviceB-vlan200] quit
```

配置 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 端口为 Trunk 端口，均允许 VLAN 100 和 VLAN 200 的报文通过。

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

4. 验证配置

(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。以 Device A 为例：

```
[DeviceA] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC address      Mask             VLAN ID  Priority    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
```

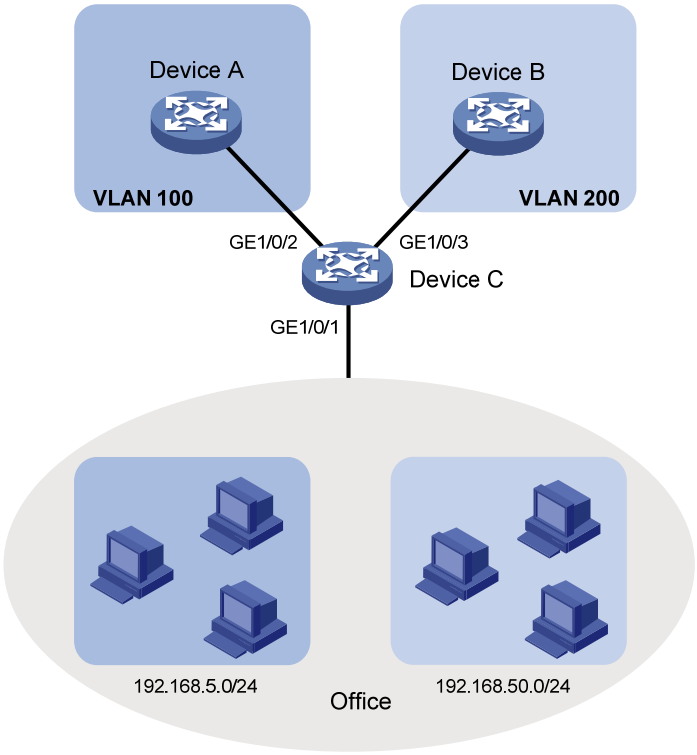
1.10.3 基于IP子网的VLAN配置举例

1. 组网需求

如下图所示，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，其中，来自网段 192.168.5.0/24 的报文在 VLAN 100 中传输，来自网段 192.168.50.0/24 的报文在 VLAN 200 中传输。

2. 组网图

图1-5 基于 IP 子网的 VLAN 组网图



3. 配置步骤

(1) 配置 Device C

配置子网 192.168.5.0/24 与 VLAN 100 关联。

```
<DeviceC> system-view
[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 GigabitEthernet1/0/2 为 Hybrid 端口，允许 VLAN 100 通过，并且在发送 VLAN 100 的报文时携带 VLAN Tag。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type hybrid
[DeviceC-GigabitEthernet1/0/2] port hybrid vlan 100 tagged
[DeviceC-GigabitEthernet1/0/2] quit
```

配置端口 GigabitEthernet1/0/3 为 Hybrid 端口，允许 VLAN 200 通过，并且在发送 VLAN 200 的报文时携带 VLAN Tag。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type hybrid
[DeviceC-GigabitEthernet1/0/3] port hybrid vlan 200 tagged
```

```
[DeviceC-GigabitEthernet1/0/3] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，允许 VLAN 100、200 通过，并且在发送 VLAN 100、200 的报文时不携带 VLAN Tag。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

配置端口 GigabitEthernet1/0/1 和基于 IP 子网的 VLAN 100、200 关联。

```
[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] quit
```

(2) 配置 Device A 和 Device B

配置 Device A 和 Device B 允许对应 VLAN 通过，配置过程略。

4. 验证配置

查看所有子网 VLAN 的信息。

```
[DeviceC] 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 GigabitEthernet1/0/1 关联的子网 VLAN 的信息。

```
[DeviceC] display ip-subnet-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  100       0               192.168.5.0      255.255.255.0     Active
  200       0               192.168.50.0     255.255.255.0     Active
```

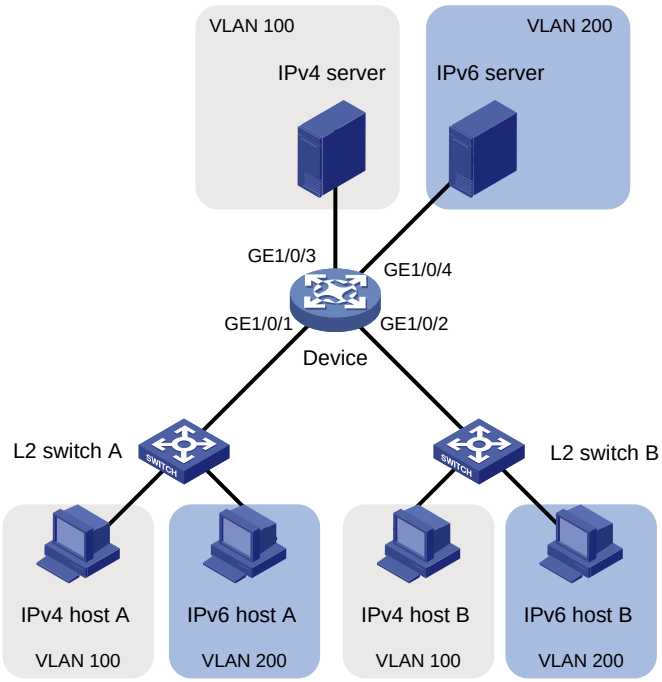
1.10.4 基于协议的VLAN配置举例

1. 组网需求

如下图所示，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部署了 IPv6 实验局，因此，有些主机运行 IPv6 网络协议。为了避免互相干扰，将 VLAN 100 与 IPv4 协议、ARP 协议关联，VLAN 200 与 IPv6 协议关联，通过协议 VLAN 将 IPv4 流量和 IPv6 流量二层互相隔离。

2. 组网图

图1-6 基于协议的 VLAN 组网图



3. 配置步骤

(1) 配置 Device

创建 VLAN 100，将端口 GigabitEthernet1/0/3 加入 VLAN 100。

```
<Device> system-view
[Device] vlan 100
[Device-vlan100] description protocol VLAN for IPv4
[Device-vlan100] port gigabitethernet 1/0/3
[Device-vlan100] quit
```

创建 VLAN 200，将端口 GigabitEthernet1/0/4 加入 VLAN 200。

```
[Device] vlan 200
[Device-vlan200] description protocol VLAN for IPv6
[Device-vlan200] port gigabitethernet 1/0/4
```

将 IPv6 协议报文划分到 VLAN 200 中传输。

```
[Device-vlan200] protocol-vlan 1 ipv6
[Device-vlan200] quit
```

将 IPv4 协议报文和采用 Ethernet II 封装格式的 ARP 协议报文（ARP 报文对应的封装格式为 Ethernet II）划分到 VLAN 100 中传输。

```
[Device] vlan 100
[Device-vlan100] protocol-vlan 1 ipv4
[Device-vlan100] protocol-vlan 2 mode ethernetii etype 0806
[Device-vlan100] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，允许 VLAN 100、200 通过，并且在发送 VLAN 100、200 的报文时不携带 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
```

配置端口 GigabitEthernet1/0/1 与 VLAN 100 的协议模板 1（即 IPv4 协议模板）、协议模板 2（即 ARP 协议模板）和 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 to 2
[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，允许 VLAN 100、200 通过，并且在发送 VLAN 100、200 的报文时不携带 VLAN Tag。

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

配置端口 GigabitEthernet1/0/2 与 VLAN 100 的协议模板 1（即 IPv4 协议模板）、协议模板 2（即 ARP 协议模板）和 VLAN 200 的协议模板 1（即 IPv6 协议模板）进行绑定。

```
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/2] quit
```

(2) L2 switch A 和 L2 switch B 采用缺省配置

(3) 配置 Host 和 Server

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。

4. 验证配置

(1) 通过 **ping** 命令查看

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/服务器与 VLAN 200 内的主机/服务器之间会 Ping 失败。

(2) 通过显示信息查看

查看所有协议 VLAN 的信息。

```
[Device] display protocol-vlan vlan all
 VLAN ID: 100
  Protocol index  Protocol type
  1               IPv4
  2               Ethernet II Etype 0x0806

 VLAN ID: 200
  Protocol index  Protocol type
  1               IPv6
```

查看所有端口关联的协议 VLAN 的信息。

```
[Device] display protocol-vlan interface all
 Interface: GigabitEthernet1/0/1
  VLAN ID  Protocol index  Protocol type            Status
  100      1              IPv4                     Active
  100      2              Ethernet II Etype 0x0806 Active
  200      1              IPv6                     Active
```

```
Interface: GigabitEthernet1/0/2
 VLAN ID  Protocol index  Protocol type             Status
 100      1               IPv4                      Active
 100      2               Ethernet II Etype 0x0806  Active
 200      1               IPv6                      Active
```

2 Super VLAN

2.1 Super VLAN简介

在交换局域网中，VLAN 技术以其对广播域的灵活控制、部署方便而得到了广泛的应用。但是在一般的交换设备中，通常是采用一个 VLAN 对应一个 VLAN 接口的方式来实现广播域之间的互通，这在某些情况下导致了对 IP 地址的较大浪费。

Super VLAN 可以对 VLAN 进行聚合，从而大幅缩减实际需要的 VLAN 接口数量，解决 IP 地址紧张的问题。其原理是一个 Super VLAN 和多个 Sub VLAN 关联，关联的 Sub VLAN 公用 Super VLAN 对应的 VLAN 接口（即 Super VLAN interface）的 IP 地址作为三层通信的网关地址，此时 Sub VLAN 间的三层通信以及 Sub VLAN 与外部的三层通信均借用 Super VLAN interface 来实现，从而节省了 IP 地址资源。

- Super VLAN：支持创建 VLAN 接口，并配置接口 IP 地址，不能加入物理接口。
- Sub VLAN：不支持创建 VLAN 接口，可以加入物理端口，不同 Sub VLAN 之间二层相互隔离。

为了实现 Sub VLAN 之间的三层互通，在创建好 Super VLAN 及其 Super VLAN interface 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 interface 上开启本地代理 ARP 功能，Super VLAN 利用本地代理 ARP，可以对 Sub VLAN 内用户发出的 ARP 请求和响应报文进行处理，从而实现 Sub VLAN 之间的三层互通。
- 对于 IPv6 网络环境，用户需要在 Super VLAN interface 上开启本地代理 ND 功能，Super VLAN 利用本地代理 ND，可以对 Sub VLAN 内用户发出的 NS 请求和 NA 响应报文进行处理，从而实现 Sub VLAN 之间的三层互通。

2.2 Super VLAN配置限制和指导

- MAC VLAN 表项中的 VLAN 不能配为 Super VLAN。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不建议被指定为某个端口的 Guest VLAN/Auth-Fail VLAN/Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN/Auth-Fail VLAN/Critical VLAN，则该 VLAN 不建议被指定为 Super VLAN。Guest VLAN/Auth-Fail VLAN/Critical VLAN 的相关内容请参见“安全配置指导”中的“802.1X”。
- 一个 VLAN 不能同时配置为 Super VLAN 和 Sub VLAN。
- 在 Super VLAN 下可以配置二层组播功能，但是由于 Super VLAN 中没有物理端口，该配置将不会生效。

2.3 Super VLAN配置任务简介

Super VLAN 配置任务如下：

(1) 创建Sub VLAN

(2) 配置Super VLAN

(3) 配置Super VLAN interface

2.4 创建Sub VLAN

(1) 进入系统视图。

system-view

(2) 创建 VLAN 用作 Sub VLAN。

vlan *vlan-id-list*

缺省情况下，系统只有一个缺省 VLAN（VLAN 1）。

2.5 配置Super VLAN

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 VLAN 的类型为 Super VLAN。

supervlan

缺省情况下，VLAN 类型不为 Super VLAN。

(4) 建立 Super VLAN 和 Sub VLAN 的映射关系。

subvlan *vlan-id-list*

建立 Super VLAN 和 Sub VLAN 的映射关系前，指定的 Sub VLAN 必须已经创建。

2.6 配置Super VLAN interface

1. 配置限制和指导

在 Super VLAN interface 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. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 VLAN 接口，并进入 VLAN 接口视图。

interface vlan-interface *interface-number*

interface-number 的值必须等于 Super VLAN ID。

(3) 配置 VLAN 接口的 IP 地址。

（IPv4 网络）

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

（IPv6 网络）

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

缺省情况下，没有配置 VLAN 接口的 IP 地址。

(4) 开启本地代理 ARP 功能或本地代理 ND 功能。

（IPv4 网络）

local-proxy-arp enable

缺省情况下，本地代理 ARP 功能处于关闭状态。

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“代理 ARP”。

（IPv6 网络）

local-proxy-nd enable

缺省情况下，本地代理 ND 功能处于关闭状态。

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”。

2.7 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2-1 Super VLAN 显示和维护

操作	命令
显示Super VLAN及其关联的Sub VLAN的信息	**display supervlan** [*supervlan-id*]

2.8 Super VLAN典型配置举例

2.8.1 Super VLAN基本组网配置举例

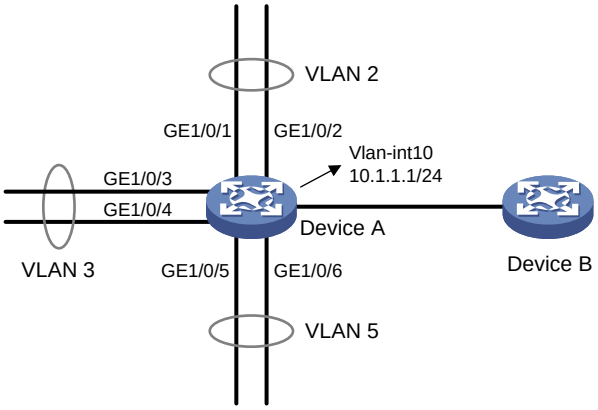
1. 组网需求

Device A 连接不同 VLAN 用户，其中，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。

为实现 Device A 连接的各 VLAN 用户（均在 10.1.1.0/24 网段）之间能够满足二层隔离和三层互通的同时，节省 IP 资源，创建 Super VLAN，其关联的 Sub VLAN 公用 Super VLAN interface 的 IP 地址 10.1.1.1/24 作为三层通信的网关地址。

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 10.1.1.1/24。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
```

开启设备的本地代理 ARP 功能。

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

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

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

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

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

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

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

配置 VLAN 10 为 Super VLAN，其关联的 Sub VLAN 为 VLAN 2、VLAN 3 和 VLAN 5。

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

4. 验证配置

查看 Super VLAN 的相关信息，验证以上配置是否生效。

```
<DeviceA> display supervlan
 Super VLAN ID: 10
 Sub-VLAN ID: 2-3 5

 VLAN ID: 10
 VLAN type: Static
 It is a super VLAN.
 Route interface: Configured
 Ipv4 address: 10.1.1.1
 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: 10.1.1.1
 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: 10.1.1.1
 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 unterface: Configured
 Ipv4 address: 10.1.1.1
 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 Private VLAN

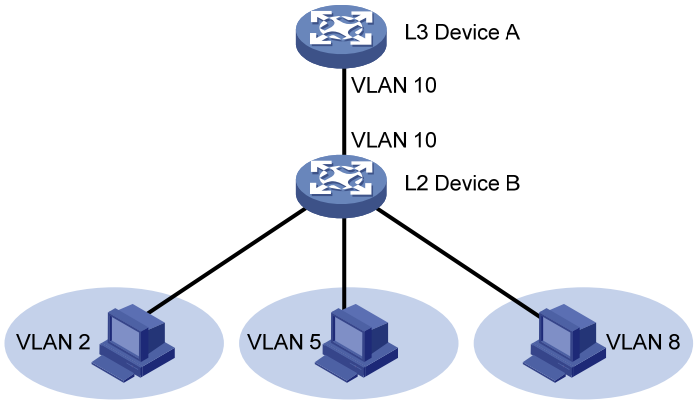
3.1 Private VLAN简介

在采用以太网接入的场景中，基于用户安全和管理计费等方面的考虑，一般会要求接入用户互相隔离。VLAN 是天然的隔离手段，于是很自然的想法是每个用户一个 VLAN。但是，根据 IEEE 802.1Q 规定，最多可以提供 4094 个 VLAN。如果每个用户一个 VLAN，4094 个 VLAN 远远不能满足需求。

Private VLAN 采用二层 VLAN 结构，它在同一台设备上配置 Primary VLAN 和 Secondary VLAN 两类 VLAN，既能够保证接入用户之间相互隔离，又能将接入的 VLAN ID 屏蔽掉，从而节省了 VLAN 资源。

- Primary VLAN：用于连接上行设备，一个 Primary VLAN 可以和多个 Secondary VLAN 相对应。上行连接的设备只需知道 Primary VLAN，而不必关心 Secondary VLAN，Primary VLAN 下面的 Secondary VLAN 对上行设备不可见。
- 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Primary 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 中的L3 Device A）的本地代理ARP/ND功能来实现三层报文的互通。

图3-1 Private VLAN 示意图



如 图 3-1 所示，L2 Device B上启动了Private VLAN功能。其中VLAN 10 是Primary 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L3 Device A不可见。

如果配置 Private VLAN 功能的设备为三层设备，Secondary VLAN 间及 Secondary VLAN 与外部需要进行三层互通，则可以通过在本地设备上创建 Secondary 对应的 VLAN 接口（即 Secondary VLAN interface），并在该 Secondary VLAN interface 上配置 IP 地址来实现；或者通过在本地设备上配置 Primary VLAN 下指定 Secondary VLAN 间三层互通，同时创建 Primary VLAN interface（但不能创建 Secondary VLAN interface），并在 Primary VLAN interface 上配置 IP 地址和本地代理 ARP/ND 功能来实现。

3.2 Private VLAN配置限制和指导

在完成 Private VLAN 的配置后，建议用户作如下确认：

- 对于工作模式为 promiscuous 的端口，确保该端口的 PVID 为 Primary VLAN，该端口以 Untagged 方式加入 Primary VLAN 和 Secondary VLAN；
- 对于工作模式为 trunk promiscuous/trunk secondary 的端口，确保该端口以 Tagged 方式加入 Primary VLAN 和 Secondary VLAN；
- 对于工作模式为 host 的端口，确保该端口的 PVID 为 Secondary VLAN，该端口以 Untagged 方式加入 Primary VLAN 和 Secondary VLAN。

系统缺省 VLAN（VLAN 1）不支持 Private VLAN 相关配置。

3.3 Private VLAN配置任务简介

Private VLAN 配置任务如下：

(1) 创建Primary VLAN

(2) 创建Secondary VLAN

(3) 配置Primary VLAN和Secondary VLAN间的映射关系

(4) 配置上行端口

(5) 配置下行端口

(6) （可选）配置Primary VLAN下指定Secondary VLAN间三层互通

3.4 创建Primary VLAN

(1) 进入系统视图。

system-view

(2) 创建 VLAN，并进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 VLAN 的类型为 Primary VLAN。

private-vlan primary

缺省情况下，VLAN 的类型不是 Primary VLAN。

3.5 创建Secondary VLAN

(1) 进入系统视图。

system-view

(2) 创建一个或多个 Secondary VLAN。

vlan { *vlan-id-list* | **all** }

3.6 配置Primary VLAN和Secondary VLAN间的映射关系

(1) 进入系统视图。

system-view

(2) 进入 Primary VLAN 视图。

vlan *vlan-id*

(3) 建立 Primary VLAN 和 Secondary VLAN 的映射关系。

private-vlan secondary *vlan-id-list*

缺省情况下，未建立 Primary VLAN 和 Secondary VLAN 的映射关系。

3.7 配置上行端口

1. 功能简介

当上行端口（如 图 3-1 中L2 Device B上与L3 Device A相连的端口）只对应一个Primary VLAN时，配置该端口工作在promiscuous模式，可以实现上行端口加入Primary VLAN及同步加入对应的Secondary VLAN的功能；当上行端口对应多个Primary VLAN时，配置该端口工作在trunk promiscuous模式，可以实现上行端口加入多个Primary VLAN及同步加入各自对应的Secondary VLAN的功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入上行端口视图。

interface *interface-type interface-number*

(3) 配置上行端口工作模式。请选择其中一项进行配置。

- 配置上行端口在指定 VLAN 中工作在 promiscuous 模式。

  port private-vlan *vlan-id* **promiscuous**

- 配置上行端口在指定 VLAN 中工作在 trunk promiscuous 模式。

  port private-vlan *vlan-id-list* **trunk promiscuous**

缺省情况下，端口在指定 VLAN 中不工作在 promiscuous/trunk promiscuous 模式。

3.8 配置下行端口

1. 功能简介

当下行端口（如 图 3-1 中L2 Device B上与用户相连的端口）只对应一个Secondary VLAN时，配置该端口工作在host模式，可以实现下行端口同步加入Secondary VLAN对应的Primary VLAN的功能；当下行端口对应多个Secondary VLAN时，配置该端口工作在trunk secondary模式，可以实现下行端口加入多个Secondary VLAN及同步加入各自对应的Primary VLAN的功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入下行端口视图。

interface *interface-type interface-number*

(3) 配置端口的链路类型。

port link-type { **access** | **hybrid** | **trunk** }

(4) 配置下行端口加入 Secondary VLAN。请选择其中一项进行配置。

- 将 Access 端口加入 Secondary VLAN。

  port access vlan *vlan-id*

- 将 Trunk 端口加入 Secondary VLAN。

  port trunk permit vlan { *vlan-id-list* | **all** }

- 将 Hybrid 端口加入 Secondary VLAN。

  port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

(5) 配置下行端口的工作模式。请选择其中一项进行配置。

- 配置下行端口在指定 VLAN 中工作在 trunk secondary 模式。

  port private-vlan *vlan-id-list* **trunk secondary**

- 配置下行端口工作在 host 模式。

  port private-vlan host

缺省情况下，端口不工作在 trunk secondary/host 模式。

(6) （可选）配置同一 Secondary VLAN 内各端口二层互通。

a. 退回系统视图。

quit

b. 进入 Secondary VLAN 视图。

vlan *vlan-id*

c. 请选择其中一项进行配置。

undo private-vlan isolated

private-vlan community

缺省情况下，同一 Secondary VLAN 内的端口能够二层互通。

3.9 配置Primary VLAN下指定Secondary VLAN间三层互通

(1) 进入系统视图。

system-view

(2) 进入 Primary VLAN interface 视图。

interface vlan-interface *interface-number*

(3) 配置当前 Primary VLAN 下指定的 Secondary VLAN 间三层互通。

private-vlan secondary *vlan-id-list*

缺省情况下，Secondary VLAN 之间三层不互通。

(4) 配置 Primary VLAN 接口的 IP 地址。

（IPv4 网络）

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

（IPv6 网络）

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

缺省情况下，没有配置 VLAN 接口的 IP 地址。

(5) 开启本地代理 ARP 功能或本地代理 ND 功能。

（IPv4 网络）

local-proxy-arp enable

缺省情况下，本地代理 ARP 功能处于关闭状态。

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“代理 ARP”。

（IPv6 网络）

local-proxy-nd enable

缺省情况下，本地代理 ND 功能处于关闭状态。

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”。

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

表3-1 Private VLAN 显示和维护

操作	命令
显示Primary VLAN和其包含的Secondary VLAN的信息	**display private-vlan** [*primary-vlan-id*]

3.11 Private VLAN典型配置举例

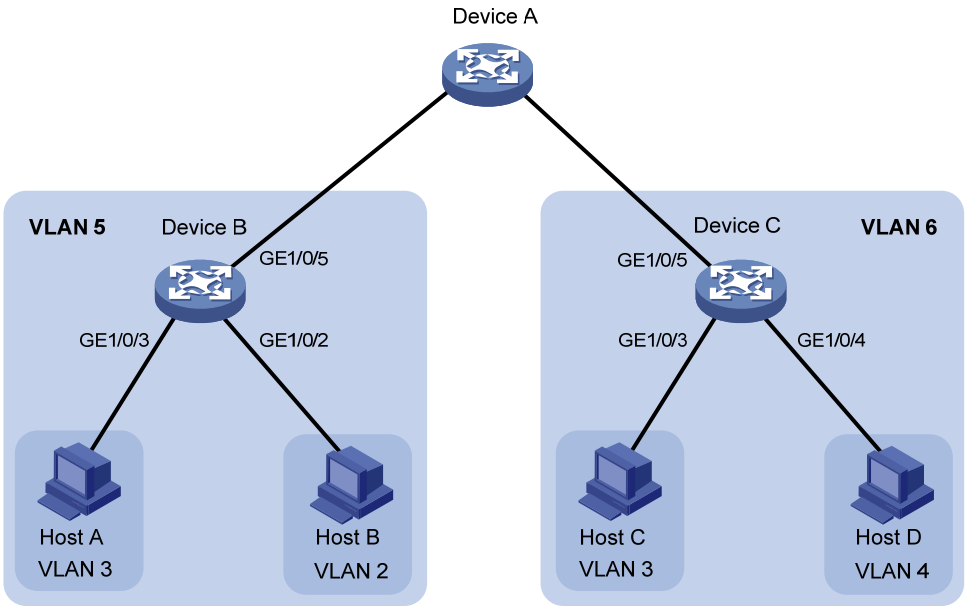
3.11.1 Private VLAN配置举例（promiscuous模式）

1. 组网需求

- Device B 上的 Primary VLAN 5 包含上行端口 GigabitEthernet1/0/5，并关联两个 Secondary VLAN（VLAN 2 和 VLAN 3），其中，VLAN 2 包含端口 GigabitEthernet1/0/2，VLAN 3 包含端口 GigabitEthernet1/0/3。
- Device C 上的 Primary VLAN 6 包含上行端口 GigabitEthernet1/0/5，并关联两个 Secondary VLAN（VLAN 3 和 VLAN 4），其中，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 Device C 只有一个 VLAN（VLAN 6）。

2. 组网图

图3-2 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 Primary VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
```

创建 Secondary VLAN 2、3。

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

配置 Primary VLAN 5 和 Secondary VLAN 2、3 的映射关系。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

配置上行端口 GigabitEthernet1/0/5 在 VLAN 5 中工作在 promiscuous 模式。

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

将下行端口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 分别添加到 VLAN 2、VLAN 3，并配置它们工作在 host 模式。

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

```
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

(2) 配置 Device C

配置 VLAN 6 为 Primary VLAN。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC–vlan6] private-vlan primary
[DeviceC–vlan6] quit
```

创建 Secondary VLAN 3、4。

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

配置 Primary VLAN 6 和 Secondary VLAN 3、4 的映射关系。

```
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan secondary 3 to 4
[DeviceC-vlan6] quit
```

配置上行端口 GigabitEthernet1/0/5 在 VLAN 6 中工作在 promiscuous 模式。

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

将下行端口 GigabitEthernet1/0/3、GigabitEthernet1/0/4 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 private-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 private-vlan host
[DeviceC-GigabitEthernet1/0/4] quit
```

4. 验证配置

显示 Device B 上的 Private VLAN 配置情况（Device C 的显示结果类似，这里不再列出）。

```
[DeviceB] display private-vlan
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
    GigabitEthernet1/0/5
```

```
VLAN ID: 2
VLAN type: Static
Private 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
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports:    None
Untagged Ports:
   GigabitEthernet1/0/3
   GigabitEthernet1/0/5
```

可以看到，工作在 promiscuous 模式的端口 GigabitEthernet1/0/5 和工作在 host 模式的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 均以 Untagged 方式允许 VLAN 报文通过。

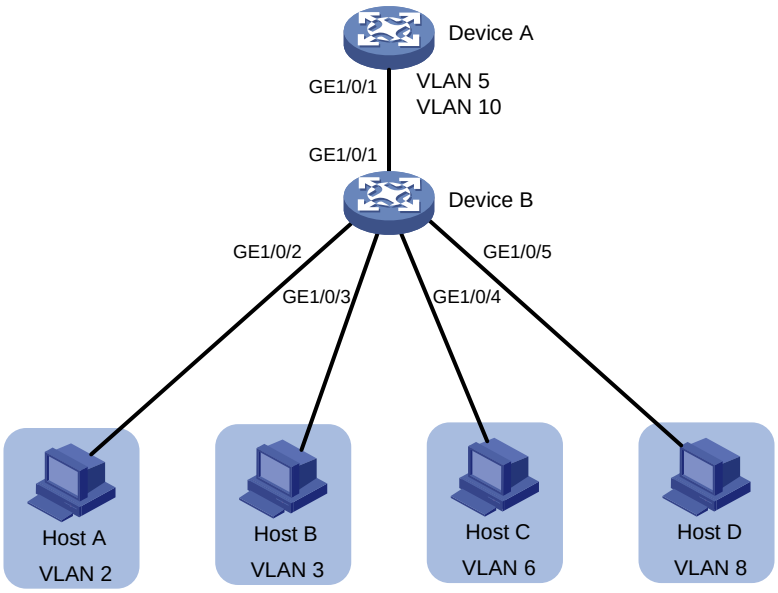
3.11.2 Private VLAN配置举例（trunk promiscuous模式）

1. 组网需求

- Device B 上的 VLAN 5 和 VLAN 10 为 Primary VLAN，其上行端口 GigabitEthernet1/0/1 需要允许 VLAN 5 和 VLAN 10 的报文携带 VLAN Tag 通过。
- Device B 的下行端口 GigabitEthernet1/0/2 允许 Secondary VLAN 2 通过，GigabitEthernet1/0/3 允许 Secondary VLAN 3 通过，Secondary VLAN 2、3 映射到 Primary VLAN 5。
- Device B 的下行端口 GigabitEthernet1/0/4 允许 Secondary VLAN 6 通过，GigabitEthernet1/0/5 允许 Secondary VLAN 8 通过，Secondary VLAN 6、8 映射到 Primary VLAN 10。
- 从 Device A 看，下接的 Device B 只有 VLAN 5 和 VLAN 10。

2. 组网图

图3-3 组网图



3. 配置步骤

(1) 配置 Device B

配置 VLAN 5 和 VLAN 10 为 Primary VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

创建 Secondary VLAN 2、3、6、8。

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
[DeviceB-vlan8] quit
```

配置 Primary VLAN 5 和 Secondary VLAN 2、3 的映射关系。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

配置 Primary VLAN 10 和 Secondary VLAN 6、8 的映射关系。

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 6 8
[DeviceB-vlan10] quit
```

配置上行端口 GigabitEthernet1/0/1 在 VLAN 5 和 VLAN 10 中工作在 trunk promiscuous 模式。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

将下行端口 GigabitEthernet1/0/2 加入 VLAN 2，GigabitEthernet1/0/3 加入 VLAN 3，并配置它们工作在 host 模式。

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

将下行端口 GigabitEthernet1/0/4 加入 VLAN 6，GigabitEthernet1/0/5 加入 VLAN 8，并配置它们工作在 host 模式。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 6
[DeviceB-GigabitEthernet1/0/4] port private-vlan host
[DeviceB-GigabitEthernet1/0/4] quit
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port access vlan 8
[DeviceB-GigabitEthernet1/0/5] port private-vlan host
[DeviceB-GigabitEthernet1/0/5] quit
```

(2) 配置 Device A

创建 VLAN 5 和 VLAN 10。

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并允许 VLAN 5 和 VLAN 10 携带 Tag 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

4. 验证配置

显示 Device B 上的 Primary VLAN 5 配置情况（Primary VLAN 10 的显示结果类似，这里不再列出）。

```
[DeviceB] display private-vlan 5
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
```

```
 Name: VLAN 0005
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:
    GigabitEthernet1/0/3
```

可以看到，工作在 trunk promiscuous 模式的端口 GigabitEthernet1/0/1 以 Tagged 方式允许 VLAN 报文通过，工作在 host 模式的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 以 Untagged 方式允许 VLAN 报文通过。

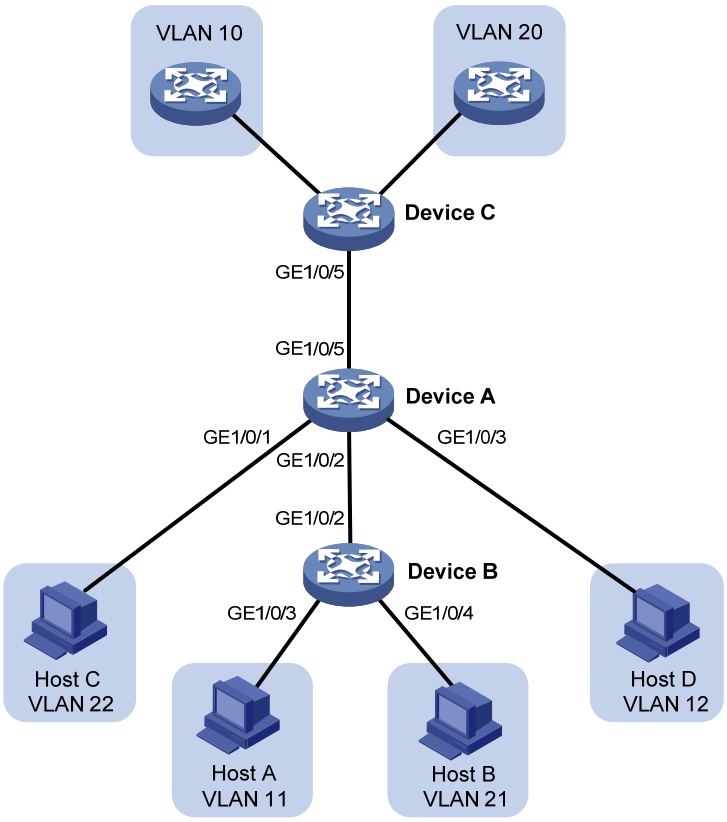
3.11.3 Private VLAN配置举例（trunk promiscuous & trunk secondary模式）

1. 组网需求

- Device A 上的 VLAN 10 和 VLAN 20 为 Primary VLAN，上行端口 GigabitEthernet1/0/5 需要允许 VLAN 10 和 VLAN 20 的报文携带 VLAN Tag 通过。
- Device A 上的 VLAN 11、12、21、22 为 Secondary VLAN，下行端口 GigabitEthernet1/0/2 允许 Secondary VLAN 11、21 的报文携带 VLAN Tag 通过，下行端口 GigabitEthernet1/0/1 允许 Secondary VLAN 22 通过，下行端口 GigabitEthernet1/0/3 允许 Secondary VLAN 12 通过。
- Secondary VLAN 11、12 映射到 Primary VLAN 10；Secondary VLAN 21、22 映射到 Primary VLAN 20。

2. 组网图

图3-4 组网图



3. 配置步骤

(1) 配置 Device A

配置 VLAN 10 和 VLAN 20 为 Primary VLAN。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan primary
[DeviceA-vlan20] quit
```

创建 Secondary VLAN 11、12、21、22。

```
[DeviceA] vlan 11 to 12
[DeviceA] vlan 21 to 22
```

配置 Primary VLAN 10 和 Secondary VLAN 11、12 的映射关系。

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 11 12
[DeviceA-vlan10] quit
```

配置 Primary VLAN 20 和 Secondary VLAN 21、22 的映射关系。

```
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan secondary 21 22
```

```
[DeviceA-vlan20] quit
```

配置上行端口 GigabitEthernet1/0/5 在 VLAN 10 和 VLAN 20 中工作在 trunk promiscuous 模式。

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
[DeviceA-GigabitEthernet1/0/5] quit
```

将下行端口 GigabitEthernet1/0/1 加入 VLAN 22，并配置其工作在 host 模式。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-GigabitEthernet1/0/1] quit
```

将下行端口 GigabitEthernet1/0/3 加入 VLAN 12，并配置其工作在 host 模式。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

配置下行端口 GigabitEthernet1/0/2 在 VLAN 11 和 VLAN 21 中工作在 trunk secondary 模式。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建 VLAN 11 和 VLAN 21。

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

配置端口 GigabitEthernet1/0/2 为 Hybrid 端口，并允许 VLAN 11 和 VLAN 21 携带 Tag 通过。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-GigabitEthernet1/0/2] quit
```

将端口 GigabitEthernet1/0/3 加入 VLAN 11。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 11
[DeviceB-GigabitEthernet1/0/3] quit
```

将端口 GigabitEthernet1/0/4 加入 VLAN 21。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 21
[DeviceB-GigabitEthernet1/0/4] quit
```

(3) 配置 Device C

创建 VLAN 10 和 VLAN 20。

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

```
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
```

配置端口 GigabitEthernet1/0/5 为 Hybrid 端口，并允许 VLAN 10 和 VLAN 20 携带 Tag 通过。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-GigabitEthernet1/0/5] quit
```

4. 验证配置

显示 Device A 上 Primary VLAN 10 的配置情况（Primary VLAN 20 的显示结果类似，这里不再列出）。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 11-12

 VLAN ID: 10
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/3

 VLAN ID: 11
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0011
 Name: VLAN 0011
 Tagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/5
 Untagged ports: None

 VLAN ID: 12
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0012
 Name: VLAN 0012
 Tagged ports:
```

```
    GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/3
```

可以看到，工作在 trunk promiscuous 模式的端口 GigabitEthernet1/0/5 和工作在 trunk secondary 模式的端口 GigabitEthernet1/0/2 以 Tagged 方式允许 VLAN 报文通过，工作在 host 模式的端口 GigabitEthernet1/0/3 以 Untagged 方式允许 VLAN 报文通过。

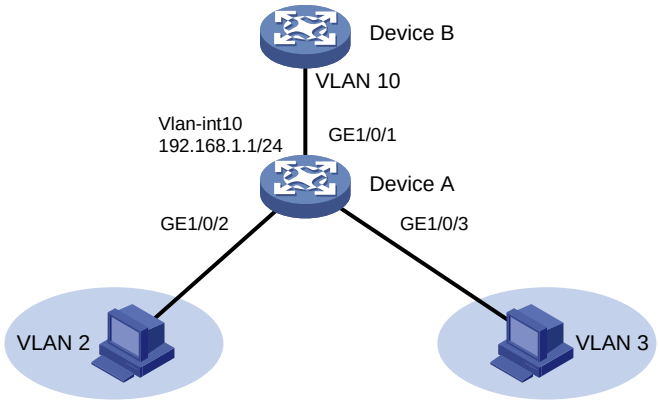
3.11.4 Secondary VLAN间三层互通配置举例

1. 组网需求

- Device A 上的 VLAN 10 为 Primary VLAN，包含上行端口 GigabitEthernet1/0/1 并关联两个 Secondary VLAN（VLAN 2 和 VLAN 3），VLAN 2 包含端口 GigabitEthernet1/0/2，VLAN 3 包含端口 GigabitEthernet1/0/3。VLAN 接口 10 的 IP 地址为 192.168.1.1/24。
- 实现各 Secondary VLAN 间二层隔离和三层互通。

2. 组网图

图3-5 组网图



3. 配置步骤

配置 VLAN 10 为 Primary VLAN。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
```

创建 Secondary VLAN 2、3。

```
[DeviceA] vlan 2 to 3
```

配置 Primary VLAN 10 和 Secondary VLAN 2、3 的映射关系。

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 2 3
[DeviceA-vlan10] quit
```

配置上行端口 GigabitEthernet1/0/1 在 VLAN 10 中工作在 promiscuous 模式。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceA-GigabitEthernet1/0/1] quit
```

将下行端口 GigabitEthernet1/0/2 加入 VLAN 2，并配置其工作在 host 模式。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 2
[DeviceA-GigabitEthernet1/0/2] port private-vlan host
[DeviceA-GigabitEthernet1/0/2] quit
```

将下行端口 GigabitEthernet1/0/3 加入 VLAN 3，并配置其工作在 host 模式。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 3
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

配置 Primary VLAN 10 下 Secondary VLAN 2、3 之间三层互通。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] private-vlan secondary 2 3
```

配置 VLAN 接口 10 的 IP 地址为 192.168.1.1/24。

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
```

开启本地代理 ARP 功能。

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

4. 验证配置

查看 Private VLAN 10 的相关信息，验证以上配置是否生效。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 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
Private VLAN type: Secondary
Route interface: Configured
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1
   GigabitEthernet1/0/3
```

可以看到，Secondary VLAN 2 和 Secondary VLAN 3 的 Route interface 字段都显示为 Configured，说明 Secondary VLAN 2 与 Secondary VLAN 3 间已配置三层互通。

4 Voice VLAN

4.1 Voice VLAN简介

Voice VLAN 是为用户的语音数据流专门划分的 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。

4.1.1 Voice VLAN工作过程

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 地址，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。

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。

4.1.2 设备识别IP电话

1. OUI地址

设备可以根据端口接收的报文的源 MAC 地址来判断该数据流是否为语音数据流。源 MAC 地址符合系统配置的语音设备 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。

用户可以预先配置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。

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	000f-e200-0000	H3C Aolynk phone
5	0060-b900-0000	Philips/NEC phone
6	00d0-1e00-0000	Pingtel phone
7	00e0-7500-0000	Polycom phone
8	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* 参数相与运算后的结果。

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。

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，网络管理员的配置工作量较大。如果 IP 电话支持 LLDP（Link Layer Discovery Protocol，链路层发现协议）功能，可以配置 LLDP 自动识别 IP 电话功能。

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 的其他功能，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。

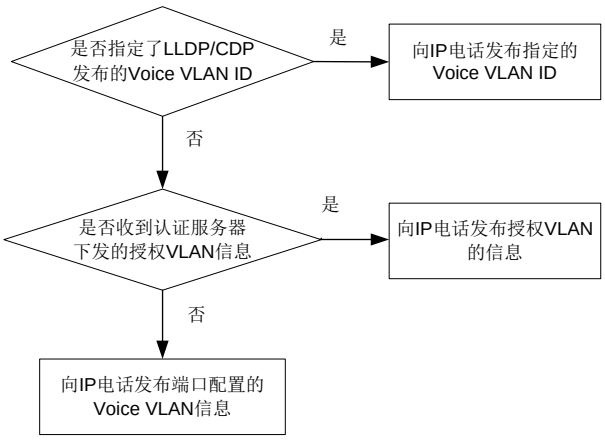
有关 LLDP 的详细信息，请参见“二层技术-以太网交换配置指导”中的“LLDP”。

4.1.3 设备将Voice VLAN信息通告给IP电话

设备可以通过三种方式将 Voice VLAN 信息通告给 IP 电话，这三种方式的优先顺序如下图所示。

- 通过命令行指定 LLDP 或 CDP（Cisco Discovery Protocol，思科发现协议）发布的 Voice VLAN ID。
- 当 IP 电话配合接入认证功能使用时，将认证服务器下发的授权 VLAN 信息通告给 IP 电话。
- 直接将端口配置的 Voice VLAN 信息通告给 IP 电话。

图4-1 设备向 IP 电话发布 Voice VLAN 信息的过程

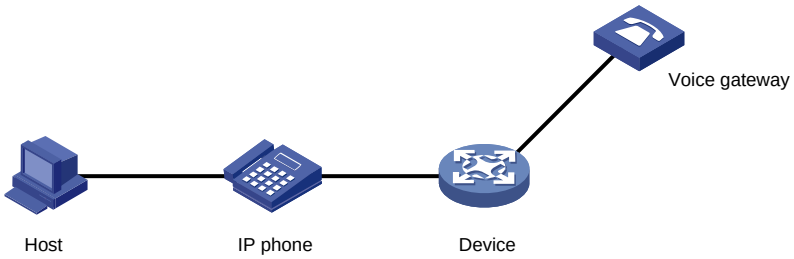


4.1.4 IP电话的接入方式

1. 主机和IP电话串联接入

如下图所示，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，需要配置端口允许 Voice VLAN 和 PVID 通过。

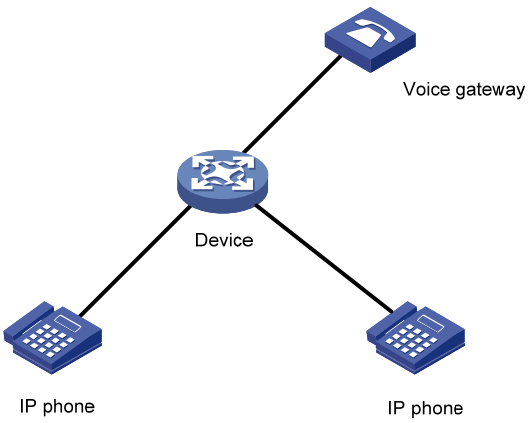
图4-2 主机与 IP 电话串联接入组网图



2. IP电话单独接入

如下图所示，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 PVID 为 Voice VLAN，并配置端口允许 PVID 通过。

图4-3 IP 电话单独接入组网图



4.1.5 端口加入Voice VLAN的方式

根据端口加入 Voice VLAN 的不同方式，可以将 Voice VLAN 的工作模式分为自动模式和手动模式。

1. 自动模式

自动模式适用于主机和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。

自动模式下，系统利用 IP 电话上电时发出的协议报文，识别报文的源 MAC 地址，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。用户可以在设备上配置 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 IP 电话重新启动，为保证已经建立的语音连接能够正常工作，系统会在 IP 电话重新启动完成后，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，需要手工将连接 IP 电话的端口加入 Voice VLAN 中。再通过识别报文的源 MAC 地址，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 的过程由网络管理员手动实现。

4.1.6 端口加入Voice VLAN的方式和IP电话的配合

由于IP电话类型较多，因此需要用户保证端口的链路类型与IP电话匹配，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。

如果用户的 IP 电话发出的是 Tagged 语音流，且接入端口上开启了 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、PVID 和 802.1X 的 Guest VLAN/Auth-Fail VLAN/Critical VLAN 分配不同的 VLAN ID。

如果用户的IP 电话发出的是Untagged 语音流，为实现 Voice VLAN 功能，只能将 PVID 配置为 Voice VLAN，此时将不能实现 802.1X 认证功能。

1. 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	PVID不能为Voice VLAN
	Hybrid		
手工模式	Access	不支持	-
	Trunk	支持	PVID不能为Voice VLAN，需要配置端口允许Voice VLAN的报文通过
	Hybrid	支持	PVID不能为Voice VLAN，需要配置端口允许Voice VLAN的报文携带Tag通过

2. 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	端口加入Voice VLAN
	Trunk	支持	PVID必须为Voice VLAN，且接入端口允许PVID通过
	Hybrid	支持	PVID必须为Voice VLAN，且允许PVID的报文不带VLAN Tag通过

4.1.7 Voice VLAN的安全模式和普通模式

开启了 Voice VLAN 功能的端口会对接收到的报文进行过滤，根据过滤机制的不同，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 PVID 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 地址匹配检查，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。

提示

只有匹配了 OUI 地址的报文才能被修改优先级。比如在普通模式下，报文在 Voice VLAN 中转发，但如果该报文未匹配 OUI 地址，则该报文不会被修改优先级。

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，否则业务数据会被丢弃。

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	当报文的源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	

Voice VLAN 工作模式	报文类型	处理方式
	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

4.2 Voice VLAN配置任务简介

Voice VLAN 配置任务如下：

(1) 配置语音报文的QoS优先级

(2) 配置端口Voice VLAN功能

请选择以下一项任务进行配置：

- 配置自动模式下的Voice VLAN
- 配置手动模式下的Voice VLAN

(3) （可选）配置通过LLDP自动发现IP电话功能

(4) （可选）配置通过LLDP/CDP通告Voice VLAN信息

请选择以下一项任务进行配置：

- 配置通过LLDP通告Voice VLAN信息
- 配置通过CDP通告Voice VLAN信息

4.3 配置语音报文的QoS优先级

1. 功能简介

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。

2. 配置限制和指导

缺省情况下，端口不信任报文携带的 802.1p 优先级。配置端口信任 Voice VLAN 内语音报文的优先级时，还需通过 **qos trust dot1p** 命令配置端口信任报文的 802.1p 优先级。配置方法请参见“ACL 和 QoS 配置指导”中的“QoS/优先级映射”。

在同一端口多次执行本配置，最后一次执行的配置生效。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入二层以太网接口视图。

interface *interface-type interface-number*

(3) 配置语音报文的 QoS 优先级。请选择其中一项进行配置。

- 配置端口信任 Voice VLAN 内语音报文的优先级。

  voice-vlan qos trust

- 配置端口将 Voice VLAN 内语音报文的 CoS 和 DSCP 值修改为指定值。

  voice-vlan qos *cos-value dscp-value*

缺省情况下，端口将 Voice VLAN 内语音报文的 CoS 值修改为 6，DSCP 值修改为 46。

4.4 配置端口Voice VLAN功能

4.4.1 配置自动模式下的Voice VLAN

1. 配置限制和指导

- 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，因此，不能将某个 VLAN 同时配置为 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。
- 当端口配置了动态触发端口加入静态 MAC VLAN，又配置本功能时，两个功能可能会相互影响，导致其中某个功能不可用。当端口同时配置了本功能和动态触发端口加入静态 MAC VLAN，再取消其中任何一个功能的配置，会导致另一个功能不可用。因此不建议同一端口同时配置本功能和动态触发端口加入静态 MAC VLAN。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）配置 Voice VLAN 的老化时间。

voice-vlan aging *minutes*

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。

(3) （可选）开启 Voice VLAN 的安全模式。

voice-vlan security enable

缺省情况下，Voice VLAN 工作在安全模式。

(4) （可选）配置 Voice VLAN 识别的 OUI 地址。

voice-vlan mac-address *oui* **mask** *oui-mask* [**description** *text*]

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”。

(5) 进入二层以太网接口视图。

interface *interface-type interface-number*

(6) 配置端口的链路类型。请选择其中一项进行配置。

- 配置端口的链路类型为 Trunk。

  port link-type trunk

- 配置端口的链路类型为 Hybird。

  port link-type hybrid

(7) 配置端口的 Voice VLAN 工作模式为自动模式。

voice-vlan mode auto

缺省情况下，端口的 Voice VLAN 工作模式为自动模式。

(8) 开启端口的 Voice VLAN 功能。

voice-vlan *vlan-id* **enable**

缺省情况下，端口的 Voice VLAN 功能处于关闭状态。

开启端口的 Voice VLAN 功能之前，须确保对应的 VLAN 已存在。

4.4.2 配置手动模式下的Voice VLAN

1. 配置限制和指导

- 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开启 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”。
- 当端口开启了 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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）开启 Voice VLAN 的安全模式。

voice-vlan security enable

缺省情况下，Voice VLAN 工作在安全模式。

(3) （可选）配置 Voice VLAN 中可识别的 OUI 地址。

voice-vlan mac-address *oui* **mask** *oui-mask* **[description** *text* **]**

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”。

(4) 进入二层以太网接口视图。

interface *interface-type interface-number*

(5) 配置端口的 Voice VLAN 工作模式为手动模式。

undo voice-vlan mode auto

缺省情况下，端口的 Voice VLAN 工作模式为自动模式。

(6) 将手动模式端口加入 Voice VLAN。请选择其中一项进行配置。

- 将 Access 端口加入 Voice VLAN。

  请参见“1.3.2 配置基于Access端口的VLAN”。

将 Access 端口加入 Voice VLAN 后，Voice VLAN 会自动成为 PVID。

- 将 Trunk 端口加入 Voice VLAN。

  请参见“1.3.3 配置基于Trunk端口的VLAN”。

- 将 Hybrid 端口加入 Voice VLAN。

  请参见“1.3.4 配置基于Hybrid端口的VLAN”。

(7) （可选）配置 PVID 为 Voice VLAN。请选择其中一项进行配置。

- 将 Trunk 端口 PVID 配置为 Voice VLAN。

  请参见“1.3.3 配置基于Trunk端口的VLAN”。

- 将 Hybrid 端口 PVID 配置为 Voice VLAN。

  请参见“1.3.4 配置基于Hybrid端口的VLAN”。

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 PVID 配置为 Voice VLAN。

(8) 开启端口的 Voice VLAN 功能。

voice-vlan *vlan-id* **enable**

缺省情况下，端口的 Voice VLAN 功能处于关闭状态。

开启端口的 Voice VLAN 功能之前，须先创建对应的 VLAN。

4.5 配置通过LLDP自动发现IP电话功能

1. 配置限制和指导

- 在配置本功能前，需要在全局和接入端口均开启 LLDP 功能。
- 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。
- 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。
- 设备开启通过 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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启通过 LLDP 自动发现 IP 电话功能。

voice-vlan track lldp

缺省情况下，通过 LLDP 自动发现 IP 电话功能处于关闭状态。

4.6 配置通过LLDP/CDP通告Voice VLAN信息

4.6.1 配置通过LLDP通告Voice VLAN信息

1. 功能简介

对于支持 LLDP 的 IP 电话，可以通过 LLDP-MED 中的 Network Policy TLV 将 Voice VLAN 信息通告给 IP 电话。

2. 配置准备

在配置本功能前，需要在全局和接入端口开启 LLDP 功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层以太网接口视图。

interface *interface-type interface-number*

(3) 配置端口上发布的 Voice VLAN ID。

lldp tlv-enable med-tlv network-policy *vlan-id*

缺省情况下，未配置端口上发布的 Voice VLAN ID。

(4) （可选）查看通告的 Voice VLAN 信息。

display lldp local-information

4.6.2 配置通过CDP通告Voice VLAN信息

1. 功能简介

如果 IP 电话只支持 CDP，不支持 LLDP，当设备与这类 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他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 电话发送的 CDP 报文，并向 IP 电话发送 CDP 报文，该 CDP 报文携带设备配置的 Voice VLAN 信息，使 IP 电话完成 Voice VLAN 的自动配置。之后 IP 电话的语音数据流将被限制在配置的 Voice VLAN 内，与其他数据流区分开来。

设备发送给 IP 电话的 CDP 报文中不包含优先级信息。

2. 配置准备

在配置本功能前，需要在全局和接入端口开启 LLDP 功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 LLDP 兼容 CDP 功能。

lldp compliance cdp

缺省情况下，LLDP 兼容 CDP 功能处于关闭状态。

(3) 进入二层以太网接口视图。

interface *interface-type interface-number*

(4) 配置 LLDP 兼容 CDP 功能的工作模式为 TxRx。

lldp compliance admin-status cdp txrx

缺省情况下，LLDP 兼容 CDP 功能的工作模式为 Disable。

(5) 配置 CDP 报文携带的 Voice VLAN ID。

cdp voice-vlan *vlan-id*

缺省情况下，未配置 CDP 报文携带的 Voice VLAN ID。

4.7 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4-5 Voice VLAN 显示和维护

操作	命令
显示Voice VLAN的状态	**display voice-vlan state**
显示系统当前支持的OUI地址	**display voice-vlan mac-address**

4.8 Voice VLAN典型配置举例

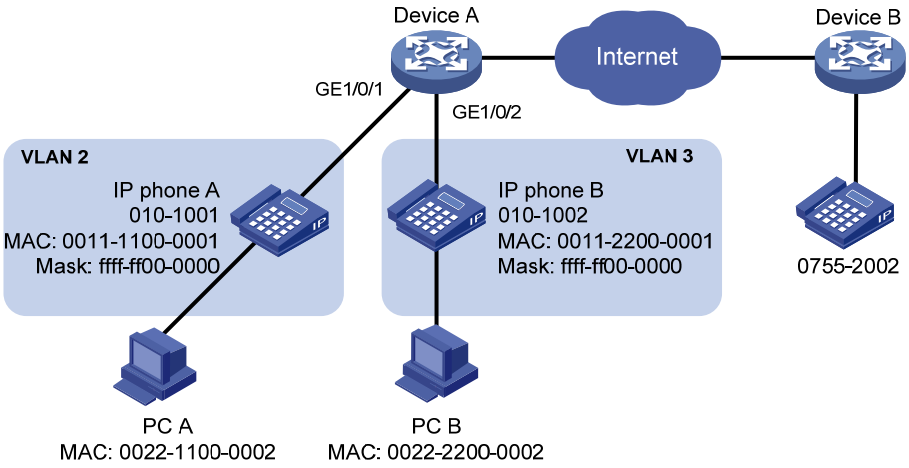
4.8.1 自动模式下Voice VLAN的配置举例

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。
- Device A 的端口 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4-4 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
```

配置 Voice VLAN 的老化时间为 30 分钟。

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

由于端口 GigabitEthernet1/0/1 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，配置 Voice VLAN 工作在安全模式，即 Voice VLAN 只用于传输语音报文。（可选，缺省情况下，Voice VLAN 工作在安全模式）

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

配置允许 OUI 地址为 0011-1100-0000 和 0011-2200-0000 的报文通过 Voice VLAN，即当报文源 MAC 地址前缀为 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
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 类型端口。

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

将端口 GigabitEthernet1/0/1 上 Voice VLAN 的工作模式配置为自动模式。（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
```

开启端口 Voice VLAN 功能。

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

在端口 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
[DeviceA-GigabitEthernet1/0/2] quit
```

4. 验证配置

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 mac-address
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
000f-e200-0000  ffff-ff00-0000  H3C Aolynk 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
 Current voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Auto        6           46
 GE1/0/2                     3           Auto        6           46
```

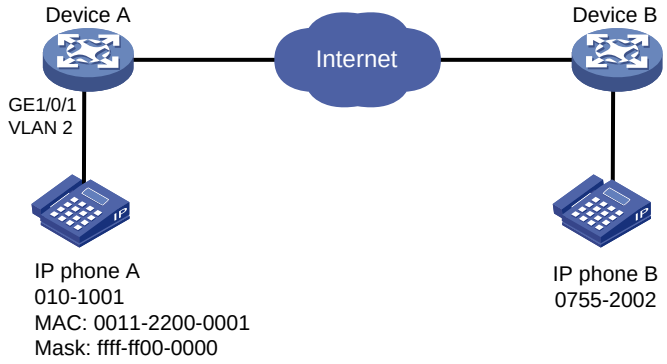
4.8.2 手动模式下Voice VLAN的配置举例

1. 组网需求

- IP Phone A 接入 Device A 的 Hybrid 类型端口 GigabitEthernet1/0/1。IP Phone A 发出的报文为 Untagged 报文。
- Device A 上 VLAN 2 为 Voice VLAN。
- 手工将 Device A 的端口 GigabitEthernet1/0/1 工作加入 Voice VLAN，其 PVID 为 VLAN 2，添加 OUI 地址 0011-2200-0000，使该端口专用于传输语音报文。

2. 组网图

图4-5 配置手动模式下 Voice VLAN 组网图



3. 配置步骤

配置 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，缺省情况下，Voice VLAN 工作在安全模式）

```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

配置允许 OUI 地址为 0011-2200-0000 的报文通过 Voice VLAN，即报文源 MAC 地址前缀为 0011-2200-0000 时，Device A 会把它当成语音报文来处理。

```
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description test
```

创建 VLAN 2。

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

配置端口 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
```

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

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

配置 Voice VLAN 是端口 GigabitEthernet1/0/1 的 PVID，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
```

开启端口 GigabitEthernet1/0/1 的 Voice VLAN 功能。

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

4. 验证配置

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 mac-address
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
```

```
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000  ffff-ff00-0000  test
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
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Manual      6           46
```