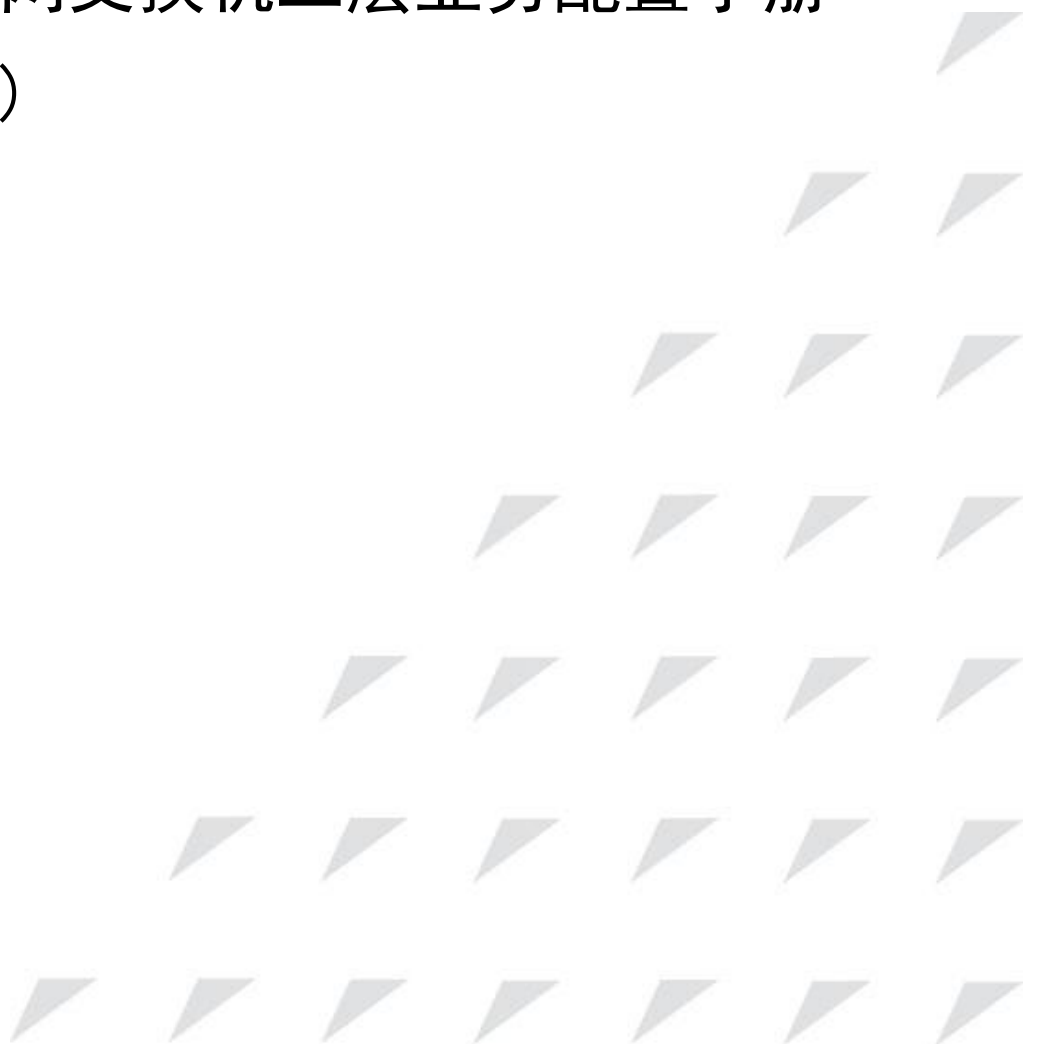


甲信三层以太网交换机二层业务配置手册  
配置指南 (CLI)  
(Rel\_01)



北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：[www.jiaxinnet.com.cn](http://www.jiaxinnet.com.cn)

技术支持邮箱：[jxhelp@bjjx.cc](mailto:jxhelp@bjjx.cc)

技术支持热线：400-179-1180

公司总部地址：北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码：100080

---


## 声 明

**Copyright ©2025**

北京甲信技术有限公司

版权所有，保留一切权利。

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

 是北京甲信技术有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保

## 目录

1 以太网	6
1.1 MAC 地址转发表	6
1.1.1 简介	6
1.1.2 配置准备	8
1.1.3 MAC 地址转发表的缺省配置	9
1.1.4 配置静态 MAC 地址	9
1.1.5 配置黑洞 MAC 地址	9
1.1.6 配置 MAC 地址学习	10
1.1.7 配置 MAC 地址学习数目限制	10
1.1.8 配置 MAC 老化时间	10
1.1.9 配置 MAC 地址漂移检测与保护	10
1.1.10 检查配置	11
1.1.11 维护	11
1.1.12 配置 MAC 地址转发表示例	12
组网需求	12
1.2 VLAN	13
1.2.1 简介	13
1.2.2 配置准备	15
1.2.3 VLAN 的缺省配置	16
1.2.4 配置 VLAN 属性	16
1.2.5 配置接口模式	16
1.2.6 配置基于 Access 接口的 VLAN	17
1.2.7 配置基于 Trunk 接口的 VLAN	17
1.2.8 配置基于 Hybrid 接口的 VLAN	18
1.2.9 配置基于 MAC 地址的 VLAN	19
1.2.10 配置基于 IP 子网的 VLAN	19
1.2.11 配置基于协议的 VLAN	20
1.2.12 查询 VLAN 统计信息	20
1.2.13 检查配置	20
1.2.14 配置 VLAN 示例	21

组网需求	21
1.3 Voice VLAN	23
1.3.1 简介	23
1.3.2 配置准备	24
1.3.3 Voice VLAN 的缺省配置	24
1.3.4 配置 OUI 地址	25
1.3.5 使能 Voice VLAN 功能	25
1.3.6 检查配置	26
1.3.7 配置端口加入 Voice VLAN 示例	26
1.3.8 配置 LLDP 实现 IP 话机接入 Voice VLAN 示例	27
组网需求	27
1.4 QinQ	29
1.4.1 简介	29
1.4.2 配置准备	30
1.4.3 QinQ 的缺省配置	30
1.4.4 配置基本 QinQ	31
1.4.5 配置灵活 QinQ	31
1.4.6 配置网络侧接口为 Trunk 模式	32
1.4.7 配置 TPID	32
1.4.8 检查配置	32
1.4.9 配置基本 QinQ 示例	33
1.4.10 配置灵活 QinQ 示例	34
组网需求	34
1.5 VLAN 转换	35
1.5.1 简介	35
1.5.2 配置准备	36
1.5.3 VLAN 转换的缺省配置	36
1.5.4 配置 VLAN 转换	37
1.5.5 检查配置	37
1.5.6 配置 VLAN 转换示例	38
组网需求	38

1.6 MRP/MVRP	39
1.6.1 简介	39
1.6.2 配置准备	42
1.6.3 缺省配置	42
1.6.4 配置 MVRP 基本功能	42
1.6.5 检查配置	43
1.6.6 配置 MVRP 应用示例	43
1.7 VTP	46
1.7.1 简介	46
1.7.2 配置准备	47
1.7.3 缺省配置	48
1.7.4 配置 VTP 基本功能	48
1.7.5 检查配置	48
1.7.6 配置 VTP 应用示例	49

# 1 以太网

---

本章介绍以太网特性的原理和配置过程，并提供相关的配置案例。

- MAC 地址转发表
- VLAN
- Voice VLAN
- QinQ
- VLAN 转换
- MRP/MVRP
- VTP

## 1.1 MAC 地址转发表

### 1.1.1 简介

以太网设备转发以太网报文是通过 MAC 地址转发规则实现的快速转发，每台设备都有一个 MAC 地址与每个接口的转发对应表，这就是 MAC 地址转发表。所有入接口报文都会依据 MAC 地址转发表进行转发，是以太网设备实现二层报文快速转发的基础。MAC 地址转发表存储在设备的缓存中，缓存容量决定设备能存储多少 MAC 地址。

MAC 地址转发表的表项中包含如下信息：

- 目的 MAC 地址
- 目的 MAC 地址所对应的接口号
- 接口所属的 VLAN ID
- 标志位 Flag

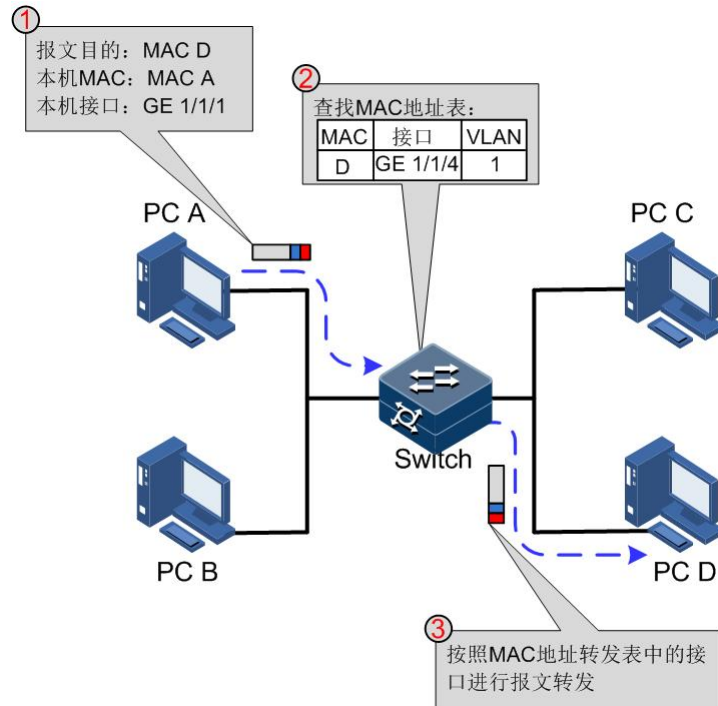
设备可基于设备、接口和 VLAN 来查看 MAC 地址表信息。

### MAC 地址转发方式

以太网设备在转发报文时，根据 MAC 地址表项信息，会采取以下转发方式：

- 单播方式：当 MAC 地址转发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接口发送；如不包含对应表项，则以广播方式向除接收接口外的所有接口转发。如下图所示。

图 1-1 MAC 地址表转发示意图



- 组播方式：当设备收到目的地址为组播 MAC 地址的报文时，组播以广播形式发送，如果开启了组播功能并设置了未知组播过滤，则发送到指定 Report 接口。如无指定 Report 接口，则报文丢弃不转发。
- 广播方式：当设备收到目的地址为全 F 的报文，或 MAC 地址转发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转发。

## MAC 地址表项的分类

MAC 地址转发表分为静态地址表和动态地址表两项。

- 静态 MAC 地址表项：也称为“永久地址”，由用户手工添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手工添加静态地址表项可以减少网络中的广播流量，能够提高接口的安全性，且系统复位后，表项不丢失。
- 动态 MAC 地址表项：交换机可以通过 MAC 地址学习机制学习动态 MAC 地址表项，该表项会按照用户配置的老化时间而老化掉。系统复位后，表项会清空。

## MAC 地址老化时间

以太网交换机的 MAC 地址转发表是有容量限制的。为了最大限度利用地址转发表资源，以太网交换机利用老化机制更新 MAC 地址转发表，即：系统在动态创建某条表项的同时，开启老化定时器，如果在老化时间内没有再次收到来自该表项中的 MAC 地址的报文，交换机就会把该 MAC 地址表项删除。

设备支持 MAC 地址自动老化，老化时间设置范围为 0 或 10s~1 000 000s，其中 0 表示永不老化。



MAC 地址的老化机制只对动态 MAC 地址表项生效。

## MAC 地址转发策略

MAC 地址转发表有 2 种转发策略：

- 当报文进入设备接口时，会在 MAC 地址表查找报文中的目的 MAC 地址所关联的接口，如果在 MAC 地址表中有目的 MAC，并且目的 MAC 对应的接口与报文进入设备的接口不同，则从目的 MAC 对应的接口转发报文，并将报文中的源 MAC 地址记录下来，与入报文的接口号、VLAN ID 相关联记录到 MAC 地址表中。当其它接口有去往该 MAC 地址时，可以通过 MAC 对应表将报文直接转发到对应的接口。
- 如果在 MAC 地址表中没有这个报文的目的 MAC，就会向除源接口外所有相同广播域的接口转发数据包，并记录该数据包中的源 MAC 地址到设备 MAC 地址表中。

## MAC 地址学习数目限制

MAC 地址学习数目限制功能主要是为了限制 MAC 地址条目数，避免了因 MAC 地址表过于庞大，可能延长查找转发表项的时间，导致以太网交换机的转发性能下降的情况，是一种管理 MAC 地址表的有效方法。

MAC 地址学习数目限制主要用于限制 MAC 地址转发表的大小，提高交换机芯片的转发速度。

### 1.1.2 配置准备

#### 场景

在以下情况，需要配置静态 MAC 地址转发表：

- 在公司内固定服务器、以及特定人员（经理、财务等）位置相对固定且较重要的主机上配置固定的静态 MAC 地址。以保证所有去往该 MAC 地址的数据流优先从静态 MAC 地址对应的接口进行转发。
- 对于固定静态 MAC 地址的接口，可以设置禁止 MAC 地址学习，防止其他主机通过该接口访问局域网数据。



同时，为避免 MAC 地址转发表中保存过多的 MAC 地址表项，而耗尽 MAC 地址表资源，需要配置 MAC 地址转发表的老化时间，以实现动态 MAC 地址的老化功能。

## 前提

无

### 1.1.3 MAC 地址转发表的缺省配置

设备上 MAC 地址转发表的缺省配置如下。

功能	缺省值
MAC 地址学习功能状态	使能
MAC 地址老化时间	300s
MAC 地址学习数目限制	无限制
MAC 地址漂移检测	使能
MAC 地址漂移保护	关闭

### 1.1.4 配置静态 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#mac-address static vlan <i>vlan-id</i> mac <i>mac-address</i> interface-type interface-number</code>	配置静态单播 MAC 地址



#### 说明

设备的 MAC 地址、组播地址、FFFF.FFFF.FFFF 及 0000.0000.0000 不能被配置为静态单播 MAC 地址。

### 1.1.5 配置黑洞 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#mac-address blackhole vlan <i>vlan-id</i> mac <i>mac-address</i></code>	配置黑洞 MAC 地址。

## 1.1.6 配置 MAC 地址学习

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入物理接口配置模式。
3	<code>JX(config-ge-1/0/1)#mac-learning { disable   enable }</code>	使能或禁止 MAC 地址学习功能

## 1.1.7 配置 MAC 地址学习数目限制

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入物理接口配置模式。
3	<code>JX(config-ge-1/0/1)#mac-limit limit-value</code>	配置接口下 MAC 地址学习数目限制阈值。

## 1.1.8 配置 MAC 老化时间

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#mac-address aging-time { 0   default   period }</code>	配置 MAC 地址老化时间。

## 1.1.9 配置 MAC 地址漂移检测与保护

请在需要的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#mac-address flapping detection { enable   disable }</code>	使能或关闭 MAC 地址漂移检测功能

步骤	配置	说明
3	<code>JX(config)#mac-address flapping detection exclude-vlan <i>vlan-list</i></code>	配置不检测 MAC 地址漂移的 VLAN
4	<code>JX(config)#mac-address flapping detection vlan <i>vlan-list</i> security-level { high   middle   low }</code>	配置检测 MAC 地址漂移的 VLAN 并配置触发 MAC 地址漂移保护的安全等级 安全等级越高，触发漂移保护需要的 MAC 地址漂移次数越少
5	<code>JX(config)#mac-address flapping error-down recovery-interval <i>period</i></code>	配置 MAC 地址漂移触发接口 error-down 的自动恢复的时间
6	<code>JX(config)#mac-address flapping quit-vlan recover-time <i>period</i></code>	配置 MAC 地址漂移触发接口 quit-vlan 的自动恢复的时间
7	<code>JX(config)#interface <i>interface-type</i> <i>interface-number</i></code>	进入物理接口配置模式。
8	<code>JX(config-ge-1/0/1)#mac-address flapping action { error-down   quit-vlan }</code>	配置接口下 MAC 地址漂移保护动作
9	<code>JX(config-ge-1/0/1)#mac-address flapping action priority <i>priority</i></code>	配置接口下 MAC 地址漂移保护动作的端口优先级 优先级数值越高，优先触发保护动作

### 1.1.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show mac-address</code>	查看 MAC 地址表项信息。
2	<code>JX#show mac-address vlan <i>vlan-id</i></code>	查看指定 VLAN 的 MAC 地址表项信息。
3	<code>JX#show mac-address interface <i>interface-type</i> <i>interface-number</i></code>	查看指定接口的 MAC 地址表项信息。
3	<code>JX#show mac-address { static   dynamic   blackhole } [ vlan <i>vlan-id</i> ]</code>	查看静态/动态/黑洞 MAC 地址表项信息。
4	<code>JX#show mac-address aging-time</code>	查看 MAC 地址老化时间。
5	<code>JX#show mac-address flapping record</code>	查看 MAC 地址漂移检测记录。
6	<code>JX#show mac-limit [ interface <i>interface-type</i> <i>interface-number</i> ]</code>	查看 MAC 地址学习数目限制的配置信息。

### 1.1.11 维护

用户可以通过以下命令维护 MAC 地址转发表特性。

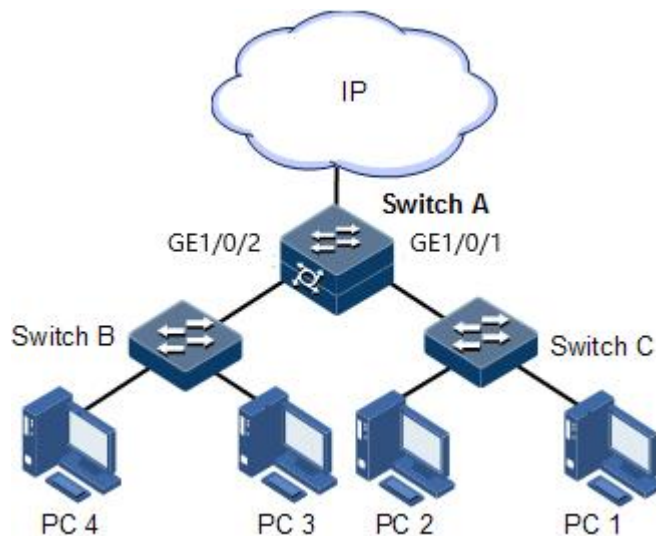
命令	描述
JX(config)#no mac-address [ vlan <i>vlan-id</i> ] [ mac <i>mac-address</i> ]	清除指定参数的 MAC 地址。
JX(config)#no mac-address <i>interface-type</i> <i>interface-number</i>	清除指定接口的 MAC 地址。
JX(config)#no mac-address { static   dynamic   blackhole } [ vlan <i>vlan-id</i> ] [ mac <i>mac-address</i> ]	清除指定参数的静态/动态/黑洞 MAC 地址
JX(config)#no mac-address { static   dynamic } [ <i>interface-type</i> <i>interface-number</i> ]	清除指定接口的静态/动态 MAC 地址
JX(config)#reset mac-address flapping record	清除 MAC 地址漂移记录

## 1.1.12 配置 MAC 地址转发表示例

### 组网需求

如下图所示，在 Switch A 上进行操作，在 GE 1/0/2 配置一条静态单播 MAC 地址 0001.0203.0405，所属 VLAN 为 VLAN 10；配置 MAC 地址老化时间为 500s。

图 1-2 MAC 应用组网示意图



### 配置步骤

步骤 1 创建 VLAN 10 并激活，将 GE 1/0/2 加入 VLAN 10。

```
JX#config
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
```

```
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
```

步骤 2 在 GE 1/0/2 配置一条静态单播 MAC 地址 0001.0203.0405, 所属 VLAN 10。

```
JX(config)#mac-address static vlan 10 mac 00:01:02:03:04:05 ge
1/0/2
```

步骤 3 配置 MAC 地址老化时间为 500s。

```
JX(config)#mac-address aging-time 500
```

## 检查结果

通过 **show mac-address** 命令查看 MAC 地址配置。

```
JX#show mac-address
```

MacAddress	VLAN/VSI/BD	Learned-From	Type	valid
0001:0203:0405	10/--/--	ge-1/0/2	static	yes
Total:1	Static:1	Dynamic:0	Blackhole:0	
Sticky:0	Security:0	Snooping:0		

## 1.2 VLAN

### 1.2.1 简介

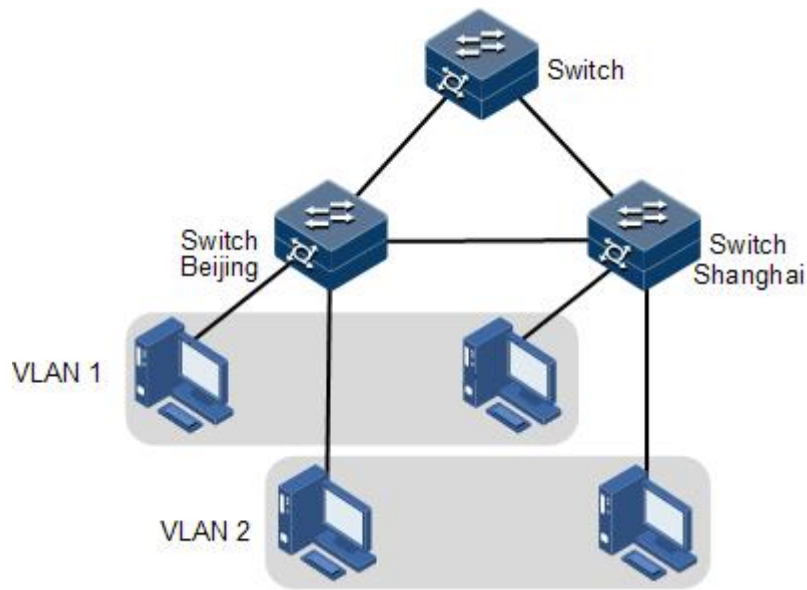
#### VLAN 概述

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议。它是一种通过将局域网内的设备逻辑地而不是物理地划分成不同的广播域, 从而实现多个互不影响的虚拟工作组的二层隔离技术。从功能上看, VLAN 和 LAN 有着相同的特性, 但两者的主要区别在于同一 VLAN 内的成员可以不受物理位置的限制进行相互访问。

#### VLAN 划分

VLAN 划分有多种方式, 例如基于接口、基于 MAC 地址、基于 IP 子网、基于协议划分等, 如下图所示。

图 1-3 VLAN 划分示意图



VLAN 技术允许将一个物理的 LAN 逻辑地划分成不同的广播域。通过划分 VLAN，将没有互通需求的主机进行隔离，在增强网络安全性、减少广播流量的同时也减少了广播风暴的发生。

设备符合 IEEE 802.1Q 标准的 VLAN，支持 4094 个并发 VLAN。

- 基于接口划分 VLAN

设备支持基于接口划分 VLAN。交换机设备的接口模式分为 Access 和 Trunk 两种，接口模式与报文转发处理方式比较请参考下表。

表 1-1 接口模式与报文转发

接口类型	入报文处理		出报文处理
	Untag 报文	带 Tag 报文	
Access	为报文打上 Access VLAN 的 Tag	<ul style="list-style-type: none"> <li>• 报文 VLAN ID=Access VLAN ID，接收该报文</li> <li>• 报文 VLAN ID≠Access VLAN ID，丢弃该报文</li> </ul>	<ul style="list-style-type: none"> <li>• 报文 VLAN ID=Access VLAN ID，去掉 Tag 发送该报文</li> <li>• 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文</li> </ul>
Trunk	为报文打上 Native VLAN 的 Tag	<ul style="list-style-type: none"> <li>• 接口允许通过的 VLAN ID 列表中包含报文 VLAN ID，接收该报文</li> <li>• 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文</li> </ul>	<ul style="list-style-type: none"> <li>• 报文 VLAN ID=Native VLAN ID，去掉 Tag 发送该报文</li> <li>• 报文 VLAN ID≠Native VLAN ID，且接口允许通过时，保持原有 Tag 发送该报文</li> </ul>

- 基于 MAC 地址划分 VLAN

基于 MAC 地址划分 VLAN 是指根据报文源 MAC 地址对 VLAN 进行划分。

- 当接口收到的报文为 Untag 报文时，根据报文的源 MAC 地址匹配 MAC VLAN 表项。如果报文中的源 MAC 地址与 MAC VLAN 表项中的 MAC 地址完全相同，则匹配成功，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，则继续匹配基于 IP 子网 VLAN、基于接口 VLAN。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。
- 基于 IP 子网划分 VLAN

基于 IP 子网划分 VLAN 是指根据报文源 IP 地址及子网掩码对 VLAN 进行划分。

- 设备从接口接收到 Untag 报文后，会根据报文的源 IP 地址及子网掩码确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。
- 基于协议划分 VLAN

基于协议划分 VLAN 是指根据数据帧所属的协议类型及封装格式对 VLAN 进行划分。

- 设备从接口接收到 Untag 报文后，会根据报文的协议域确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。
- 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

## 1.2.2 配置准备

### 场景

VLAN 最主要功能是划分逻辑网段，通常有 2 种典型应用模式。

- 一种是在小型局域网中，一台设备下划分多个 VLAN，用 VLAN 将所有连接到设备的主机逻辑的划分开，同一个 VLAN 内的主机之间可以相互通信，不同 VLAN 间的主机之间无法通信。例如财务部门与其他部门需要划分开，互相不能访问，通常连接主机的接口设置为 Access 模式。
- 另一种是在稍大型局域网或企业网中，有多台设备连接较多的主机，并且设备之间级联，转发数据报文时都携带 VLAN Tag，多台设备的相同 VLAN 的接口可以相互通信，不同 VLAN 的主机之间无法通信。主要用在公司人员及主机数量较多，并且同一个部门所在位置不同，但是要求部门内的主机可以互相访问，需要在多台设备上划分 VLAN。如果不同 VLAN 之间需要通信，则需要通过路由器等 3 层设备。设备之间级联的接口设置为 Trunk 模式。

当需要为 VLAN 配置 IP 地址时，可以为其关联一个三层接口，每一个三层接口将对应一个 IP 地址并关联一个 VLAN。

## 前提

无

### 1.2.3 VLAN 的缺省配置

设备上 VLAN 的缺省配置如下。

功能	缺省值
创建 VLAN	存在 VLAN 1
接口模式	Hybrid
PVID	1
Trunk 接口的 VLAN	VLAN 1
Access 接口的 VLAN	VLAN 1

### 1.2.4 配置 VLAN 属性

请在需要配置 VLAN 属性信息的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#vlan vlan-list</code>	创建 VLAN。 该命令也可用于批量创建 VLAN。
3	<code>JX(config)#vlan vlan-id</code>	进入 VLAN 配置模式。



#### 说明

- 用 `vlan vlan-id` 命令新创建的 VLAN 为活动状态。
- VLAN 的所有配置仅在该 VLAN 被激活后才会系统中生效。

### 1.2.5 配置接口模式

请在需要配置接口模式的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。



步骤	配置	说明
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#port link-type { access   default   dot1q-tunnel   hybrid   trunk }</code>	配置接口模式为 Access 或 Trunk 或 hybrid 或 dotq-tunnel。

## 1.2.6 配置基于 Access 接口的 VLAN

请在需要配置基于 Access 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以二层物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#port link-type access</code> <code>JX(config-ge-1/0/*)#port default vlan vlan-id</code>	配置接口模式为 Access，并将 Access 接口加入 VLAN。

### 说明

- 无论 Access 接口允许通过的 VLAN 列表如何配置，该接口都允许 Access VLAN 的数据包通过，且转发出去的数据包不携带相应 VLAN TAG 标记。
- 设置 Access VLAN 时，如果该 VLAN 没有创建并激活，将无法配置成功。
- 如果 Access VLAN 被用户手动删除或挂起，系统不会自动设置该接口 Access VLAN 为缺省 VLAN。
- 当配置接口 Access VLAN 为非缺省的 Access VLAN 时，缺省 Access VLAN 1 为 Access 出接口允许通过的 VLAN，通过配置删除 Access 出接口允许通过的 VLAN，可以将缺省 Access VLAN 1 从 Access 出接口允许通过 VLAN 列表中删除。
- 如果配置 Access VLAN 不是缺省 VLAN，且 Access 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。

## 1.2.7 配置基于 Trunk 接口的 VLAN

请在需要配置基于 Trunk 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#port link-type trunk</code>	配置接口模式为 Trunk。
4	<code>JX(config-ge-1/0/*)#port trunk pvid vlan-id</code>	配置接口 PVID。
5	<code>JX(config-ge-1/0/*)#port trunk allowed-pass vlan { all   vlan-list }</code>	配置 Trunk 接口允许通过的 VLAN。

### 说明

- 无论 Trunk 接口允许通过的 VLAN 列表列表如何配置，该接口都允许 VLAN 的数据包通过，且转发出去的数据包不携带相应 PVID 标记。
- 设置 Native VLAN 时，如果该 VLAN 没有创建并激活，系统不会自动创建并激活该 VLAN。
- 如果 Native VLAN 被用户手动删除或阻塞，系统不会自动设置该接口 Trunk Native VLAN 为缺省 VLAN。
- 接口允许 Trunk Allowed VLAN 报文出入。
- 如果配置 Native VLAN 不是缺省 VLAN，且 Trunk 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。
- Trunk 允许 VLAN 列表都只对静态 VLAN 生效，对集群 VLAN、GVRP 动态 VLAN 等不生效。

## 1.2.8 配置基于 Hybrid 接口的 VLAN

请在需要配置基于 Hybrid 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#port link-type hybrid</code>	配置接口模式为 hybrid。
4	<code>JX(config-ge-1/0/*)#port hybrid pvid vlan-id</code>	配置接口 PVID。
5	<code>JX(config-ge-1/0/*)#port hybrid vlan { all   vlan-list } { tagged   untagged }</code>	配置 hybrid 接口以 {tagged untagged} 方式允许通过的 VLAN。



## 说明

- Hybrid 端口根据配置的不同将有不同的工作方式，untagged 方式接口工作模式与 Access 模式端口相同，但可配置多个可通过 VLAN，tagged 方式接口工作模式与 trunk 模式端口相同。

## 1.2.9 配置基于 MAC 地址的 VLAN

请在需要配置基于 MAC 地址的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#mac-vlan mac-address vlan-id</code>	配置 MAC 地址与 VLAN 的关联
3	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式。
4	<code>JX(config-ge-1/0/*)#mac-vlan enable</code>	使能 MAC-VLAN 功能。



## 注意

- MAC 地址为组播 MAC 地址、全 0 或全 F 时，配置失败。
- 创建的 MAC 地址与 VLAN 关联与已经存在的关联冲突（例如同一个 MAC 地址关联到不同的 VLAN），则配置失败。

## 1.2.10 配置基于 IP 子网的 VLAN

请在需要配置基于 IP 子网的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#ip-subnet-vlan ip-address [ ip-mask ] vlan-id</code>	配置 VLAN 与 IP 子网地址的关联。
3	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式。
4	<code>JX(config-ge-1/0/*)#ip-subnet-vlan enable</code>	使能基于 IP 子网划分 VLAN 功能。



注意

- IP 地址或掩码无效时，配置失败。
- 创建的 IP 子网与 VLAN 关联与已经存在的关联冲突（例如同一个子网关联到不同的 VLAN 时），配置失败。

## 1.2.11 配置基于协议的 VLAN

请在需要配置基于协议划分 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	<code>JX#configure</code>	进入全局配置模式。
2	<code>JX(config)#protocol-vlan protocol-index { ethernet2   llc   snap protocol-id }</code>	配置协议 VLAN 与以太报文关联规则
3	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式。
4	<code>JX(config-ge-1/0/*)#protocol-vlan protocol-index vid vlan-id</code>	配置接口和协议 VLAN 的关联规则

## 1.2.12 查询 VLAN 统计信息

查询 VLAN 统计，请在设备上执行以下命令获取统计结果。

序号	检查项	说明
1	<code>JX(config-vlan-*)#statistics { enable   disable }</code>	使能 VLAN 统计功能。
2	<code>JX#show vlan [vlan-id] statistics</code>	查看 VLAN 统计信息。
3	<code>JX(config)#reset vlan [vlan-id] statistics</code>	清除 VLAN 统计信息。

## 1.2.13 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show vlan [ vlan-list   vlan-id ]</code>	查看 VLAN 配置。
2	<code>JX#show port vlan</code>	查看接口 VLAN 配置信息。
3	<code>JX#show mac-vlan [ id vlan vlan-id ]</code>	查看 MAC VLAN 配置信息
4	<code>JX#show ip-subnet-vlan [ vlan vlan-id ]</code>	查看 IP 子网 VLAN 的配置信息。

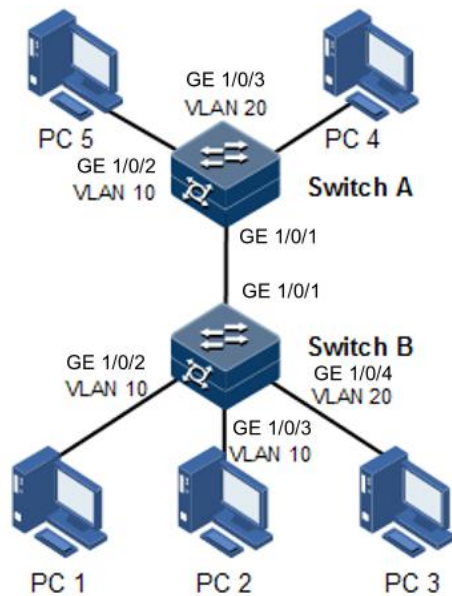
序号	检查项	说明
5	<code>JX#show protocol-vlan all</code>	查看全部协议 VLAN 配置信息。
6	<code>JX#show protocol-vlan interface</code>	查看接口的协议 VLAN 配置信息。

## 1.2.14 配置 VLAN 示例

### 组网需求

如图 2-4 所示，PC 1、PC 2、PC 5 属于 VLAN 10，PC3、PC4 属于 VLAN 20；两台设备相连的接口为 Trunk 模式，但不允许 VLAN 20 的报文通过，使 PC 3 和 PC 4 无法通信；在同一 Switch B 设备下的 PC 1 和 PC 2 的接口开启接口保护功能，使 PC 1 和 PC 2 无法通信，但 PC 1 和 PC 2 分别可以和 PC 5 通信。

图 1-4 VLAN 和接口保护组网示意图



### 配置步骤

步骤 1 在两台设备上分别创建 VLAN 10 和 VLAN 20 并激活。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 10,20
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#vlan 10,20
```

- 步骤 2 将 Switch B 的接口 GE 1/0/2 和 GE 1/0/3 以 Access 模式加入 VLAN 10，接口 GE 1/0/4 以 Access 模式加入 VLAN 20，接口 GE 1/0/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type access
SwitchB(config-ge-1/0/2)#port default vlan 10
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#port link-type access
SwitchB(config-ge-1/0/3)#port default vlan 10
SwitchB(config-ge-1/0/3)#exit
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#port link-type access
SwitchB(config-ge-1/0/4)#port default vlan 20
SwitchB(config-ge-1/0/4)#exit
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

- 步骤 3 将 Switch A 的接口 GE 1/0/2 以 Access 模式加入 VLAN 10，接口 GE 1/0/3 以 Trunk 模式加入 VLAN 20，接口 GE 1/0/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port access vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port mode trunk
SwitchA(config-ge-1/0/3)#port trunk pvid 20
SwitchA(config-ge-1/0/3)#port trunk allow-pass 20
SwitchA(config-ge-1/0/3)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allowed-pass vlan 10
```

## 检查结果

通过 **show vlan** 命令查看 VLAN 的配置信息是否正确。

以 Switch B 为例。

```
SwitchB#show vlan
```

```
      S: supervlan      P: pvlan      N: normal
```

```
Vlan Type      Ports('M': member , '-': not member)
```

```
-----
1      N/static  untagged: ge-1/0/1<->ge-1/0/16      M---MMMM
MMMMMMMMM
                                     ge-1/0/17<->ge-1/0/24      MMMMMMMM
```

```

                                10ge-1/0/25<->10ge-1/0/30      M-----
10   N/static   tagged:   ge-1/0/1<->ge-1/0/16      M-----
-----
                                untagged: ge-1/0/1<->ge-1/0/16      -MM-----
-----
20   N/static   untagged: ge-1/0/1<->ge-1/0/16      ---M-----
-----
-----
-----
Total: 3   Static: 3   Dynamic: 0

```

通过 **show interface interface-type interface-number config** 查看接口 VLAN 配置是否正确。

以 Switch B 为例。

```

SwitchB#show interface ge 1/0/2 config
!
interface ge 1/0/2
 port link-type access
 port default vlan 10

```

通过 PC 1 ping PC 5、PC 2 ping PC 5、PC 3 ping PC 4 是否能够 ping 通，查看 Trunk 接口允许通过 VLAN 是否正确。

- PC 1 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 2 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 3 ping PC 4，不能 ping 通，VLAN 20 无法通信

## 1.3 Voice VLAN

### 1.3.1 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。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 指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，可以为语音数据配置 QoS（Quality of Service，服务质量），提高语音流量的传输优先级，保证通话质量。

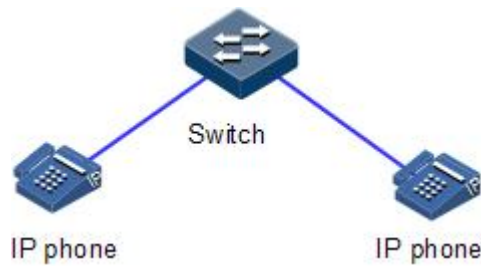
相对于使用其他语音流的方法，Voice VLAN 对语音流的管理具有以下一些优势：

- 配置简单：用户只需要在全局和端口下进行简单的配置，开启 Voice VLAN 功能，即可对语音数据进行分类处理。

- 便于维护: 用户可以在全局配置对语音数据的匹配规则 (Voice VLAN OUI 地址) 进行修改, 在新增 IP 语音设备的情况下, 各端口能够迅速根据更新的匹配规则识别语音流。
- 实现灵活: Voice VLAN 功能在全局提供了安全/普通两种模式, 端口上又可以分为自动/手动模式, 实现更为灵活, 用户可以根据自己需要进行组合, 最大限度满足用户的需求。

适用于 IP 电话单独接入交换机 (端口仅传输语音报文) 的组网方式 (如图 2 所示), 这种静态加入的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。

图 1-5 IP 电话单独接入交换机组网示意图



## 1.3.2 配置准备

### 场景

语音流量可通过专属 VLAN (Voice VLAN) 传输, 在一段时间内, 如果语音设备发生故障或语音设备退出网络, 连接语音设备的端口会自动从 Voice VLAN 中退出。

### 前提

已经创建 VLAN, 并且正确设备 VLAN 属性。

## 1.3.3 Voice VLAN 的缺省配置

设备上 Voice VLAN 的 OUI (Organizationally Unique Identifier, 全球统一标识符地址) 缺省配置如下。

OUI-Address	Mask address	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
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone



设备上 Voice VLAN 的其他缺省配置如下。

功能	缺省值
Voice VLAN 功能	禁止
Voice Vlan 工作模式为安全模式	禁止
Voice Vlan 工作模式为普通模式	使能
端口加入 Voice Vlan 的工作模式为自动模式	禁止
端口加入 Voice Vlan 的工作模式为手工模式	使能
Voice Vlan 报文的 Cos 和 DSCP 值	Voice VLAN 报文 COS 为 6, DSCP 为 46
Voice Vlan QoS 优先级信任	无
Voice Vlan 老化时间	5min

### 1.3.4 配置 OUI 地址

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#voice-vlan oui mac-address [ description word ]</code>	配置 Voice VLAN 的 OUI。

### 1.3.5 使能 Voice VLAN 功能

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入物理层接口配置模式。
3	<code>JX(config-ge-1/0/*)#voice-vlan vlan-id enable</code>	配置 Voice VLAN 功能使能。
4	<code>JX(config-ge-1/0/*)#voice-vlan mode { auto   manual }</code>	配置端口加入 Voice VLAN 的工作模式。
5	<code>JX(config)#voice-vlan aging-time time</code>	配置端口在自动模式下离开 Voice VLAN 的老化时间。

步骤	配置	说明
6	<pre>JX(config)#interface interface-type interface-number JX(config-ge-1/0/*)#voice-vlan security enable</pre>	配置 Voice Vlan 工作模式为安全模式。

### 1.3.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show voice-vlan oui</code>	查看当前设备上的 OUI 地址、OUI 地址掩码和描述信息。
2	<code>JX#show voice-vlan interface</code>	查看当前设备上 Voice VLAN 的接口状态。

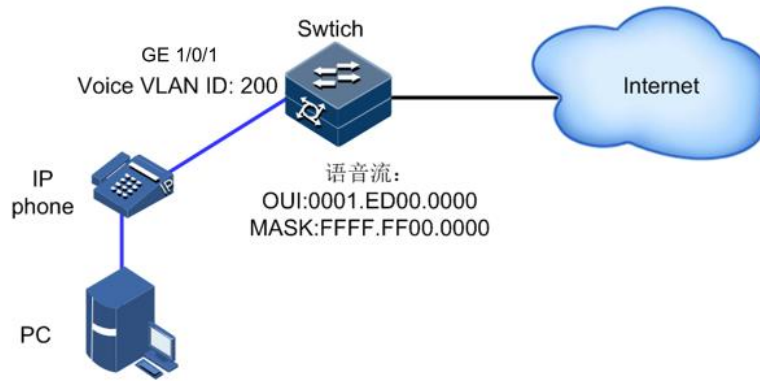
### 1.3.7 配置端口加入 Voice VLAN 示例

配置端口加入 Voice VLAN，工作于手动模式

#### 组网需求

Switch 的 GE 1/0/1 接口接入 IP 电话和 PC，要求 GE 1/0/1 端口同时转发并且隔离语音流和数据流。

可将端口配置为 Trunk 口，Native Vlan 转发数据流，Voice Vlan 转发语音流。PC 发出的是 Untagged 的报文，因此会在端口的 Native VLAN 内传输，将 Native Vlan 设置为 100，用来传输 PC 发出的数据流；IP 电话发出的也是 Untagged 报文，源 mac 配置为 Voice Vlan 的 OUI 地址，则报文通过 Voice Vlan 端口时会添加 Voice Vlan Tag，Voice Vlan 设置为 200，用来传输 IP 电话语音流。



## 配置步骤

步骤 1 在交换机上设置 IP Phone 的 MAC 地址（支持掩码）为 Voice Vlan OUI 地址，地址为 0001.ED00.0000，掩码是 FFFF.FF00.0000。设备默认支持的 OUI 参见 VoiceVLAN 缺省配置章节。

```
JX(config)#voice-vlan oui 00:01:ED:00:00:00/24
```

步骤 2 创建 VLAN100, VLAN200 并激活，设置 VLAN 200 为 Voice VLAN。

```
JX(config)#vlan 100,200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100,200
JX(config-ge-1/0/1)#voice-vlan 200 enable
```

## 检查配置

使用命令 **show voice-vlan interface** 查看设备当前的 Voice VLAN 接口状态

```
JX(config)#show voice-vlan interface
Support max interface      :64
Current enable interface   :1
Interface      VID      Mode      Security  RemainTime(s)
-----
ge-1/0/1      200      manual   disable   N/A
-----
```

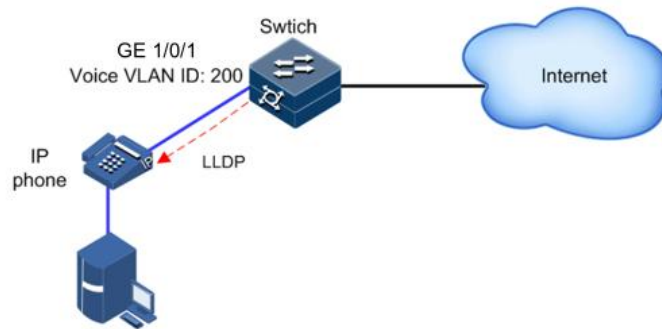
## 1.3.8 配置 LLDP 实现 IP 话机接入 Voice VLAN 示例

### 组网需求

当语音设备支持 LLDP 协议，如图所示，支持通过 LLDP 协议获取语音 VLAN。因此可通过在交换机上配置 LLDP 和 Voice VLAN 功能，实现 IP 话机接入。在交换机上通过配置 LLDP 协议向语音设备发布端口的 Voice VLAN；为保证通话质量，配置 Voice VLAN 功能提升语音报文的优先级。

Switch 的 GE 1/0/1 接口接入 IP 电话和 PC，要求 GE 1/0/1 端口同时转发并且隔离语音流和数据流。可将端口可配置为 Trunk 口，Native Vlan 转发数据流，Voice Vlan 转发语音流。PC 发出的是 Untagged 的报文，因此会在端口的 Native VLAN 内传输，将 Native Vlan 设置为 100，用来传输 PC 发出的数据流；Voice Vlan 设置为 200，用来传输 IP 电话语音流，IP

电话通过 LLDP 协议获取到 Voice VLAN，发出的是带 Voice VLAN Tag 的报文。



## 配置步骤

**步骤 1** 在交换机上设置 IP Phone 的 MAC 地址（支持掩码）为 Voice Vlan OUI 地址，地址为 0001.ED00.0000，掩码是 FFFF.FF00.0000。设备默认支持的 OUI 参见 VoiceVLAN 缺省配置章节。

```
JX(config)#voice-vlan oui 0001.ED00.0000/24
```

**步骤 2** 创建 VLAN100，VLAN200 并激活，设置 VLAN 200 为 Voice VLAN。

```
JX(config)#vlan 100,200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100
JX(config-ge-1/0/1)#voice-vlan 200 enable
JX(config-ge-1/0/1)#exit
```

**步骤 3** 全局和接口使能 LLDP 功能，向 IP 话机发布端口的 Voice VLAN。

```
JX(config)#lldp start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#lldp admin-status rx-tx
```

## 检查配置

使用命令 **show voice-vlan interface** 查看设备的 Voice VLAN 接口状态

```
JX(config)#show voice-vlan interface
Support max interface      :64
Current enable interface   :1
Interface      VID      Mode      Security  RemainTime(s)
-----
ge-1/0/1      200      auto     enable    N/A
-----
```

## 1.4 QinQ

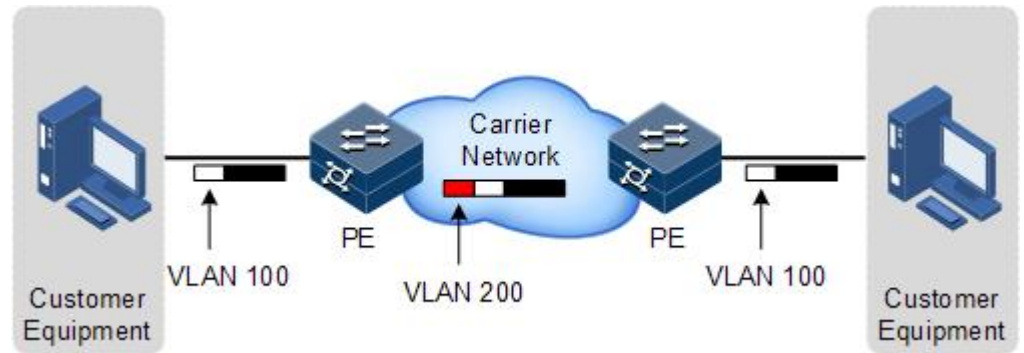
### 1.4.1 简介

QinQ（也称 Stacked VLAN 或 Double VLAN）技术是对 802.1Q 的扩展，是 IEEE 在 802.1ad 标准中定义的。

#### 基本 QinQ

基本 QinQ 是一种简单的二层 VPN 隧道技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商的骨干网络（公网）。在公网中，报文只根据外层 VLAN Tag（即公网 VLAN Tag）进行传输，用户的私网 VLAN Tag 则当作报文中的数据部分来进行传输。

图 1-6 基本 QinQ 典型组网示意图



基本 QinQ 典型组网应用如上图所示，设备作为运营商 PE (Provider Edge)。

报文从用户设备中传送到 PE 设备，此时报文携带标签的 VLAN ID 为 100。经过 PE 设备用户侧接口时打上外层标签 VLAN 200，经由 PE 设备的网络侧接口进入运营商网络。

带外层标签 VLAN 200 的报文经过运营商传送到另一端 PE 设备，另一端的 PE 把外层签 VLAN 200 剥去，然后发送到用户设备。报文此时又恢复到只携带一层标签 VLAN 100。

通过该技术可以缓解日益紧缺的公网 VLAN ID 资源，使得用户可以规划自己的私网 VLAN ID，不会导致和公网 VLAN ID 冲突。

#### 灵活 QinQ

灵活 QinQ 是基本 QinQ 的一种增强应用，可以根据一些特性对用户数据进行流分类，然后对不同的类别封装不同的外层 VLAN 标签，它基于接口与 VLAN 结合的方式来实现。除了能实现所有基本 QinQ 的功能外，灵活 QinQ 还能够对同一个接口收到的报文根据不同的 VLAN Tag 做不同的动作，为报文的内层 VLAN ID 添加不同的外层 VLAN ID。通过配置内外层 Tag 映射规则，还可以为具有不同内层 Tag 的报文按映射规则封装不同的外层 Tag。

灵活 QinQ 功能可以使运营商的网络构架更为灵活，在连接接入层设备的接口上可以根据 VLAN Tag 对不同的终端用户进行分类，为各类用户封装不同的外层 Tag，并可以在公网中按外层 Tag 配置 QoS 策略，灵活配置数据的传输优先级，使各类用户获得相应的服务。

## 1.4.2 配置准备

### 场景

对设备进行基本 QinQ 配置还是灵活 QinQ 配置，需要根据不同的业务需求进行选择。

- 基本 QinQ

通过基本 QinQ 技术应用，用户可以添加外层 VLAN Tag 自由规划自己的私网 VLAN ID，使得运营商网络两端的用户设备之间的数据可以通过运营商网络进行透明传输，而不会导致和服务提供商网络中 VLAN ID 冲突。

- 灵活 QinQ

与基本 QinQ 不同，外层 VLAN Tag 是可以根据业务不同进行选择的。用户网络中有多种业务，并设定不同的私网 VLAN ID，针对语音、视频、或数据业务等在运营商网络中通过加不同的外层 VLAN Tag 区分出来，针对不同业务转发的同时实现不同的分流，实现内外层的 VLAN 映射。

### 前提

在配置 QinQ 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。



- 基本 QinQ 和 1:1VLAN 转换命令行可同时配置，VLAN 转换在基本 QinQ 使能前后功能正常。
- 灵活 QinQ 和 1:1 VLAN 转换命令行可同时配置：同时配置时，灵活 QinQ 和 VLAN 转换功能正常；开启/关闭基本 QinQ，灵活 QinQ 和 VLAN 转换功能正常；取消其中一个配置命令，不影响其他配置正常使用。
- 基本 QinQ、灵活 QinQ 和 2:2VLAN 转换互斥：同时配置灵活 QinQ 和 1:1VLAN 转换时，匹配 VLAN 不能相同，转换后的 VLAN 不能相同。

## 1.4.3 QinQ 的缺省配置

设备上 QinQ 的缺省配置如下。

功能	缺省值
外层 VLAN Tag 的 TPID 值	0x8100

功能	缺省值
基本 QinQ 功能状态	禁用
灵活 QinQ 功能状态	禁用

### 1.4.4 配置基本 QinQ

请在需要的设备的用户侧接口上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/1)#port link-type dot1q-tunnel</code>	使能接口基本 QinQ 功能。
4	<code>JX(config-ge-1/0/1)#port default vlan vlan-id</code>	配置使能接口的基本 QinQ 功能，添加双层 TAG，指定 CVLAN，SVLAN 使用 PVID。
5	<code>JX(config-ge-1/0/1)#tpid tpid</code>	配置接口的 VLAN Tag 的 TPID，用于识别用户内层 VLAN 或者 QinQ 使能时识别用户外层 VLAN， tpid: TPID 值，十六进制数，整数形式，取值范围是 0x8100、0x88a8 或 0x9100
6	<code>JX(config-ge-1/0/1)#inner tpid tpid</code>	配置接口的内层 VLAN Tag 的 TPID，用于识别用户内层 VLAN 或者 QinQ 使能时识别用户外层 VLAN， tpid: TPID 值，十六进制数，整数形式，取值范围是 0x8100、0x88a8 或 0x9100



#### 说明

- 当接口开启基本 QINQ 时，所有报文均当做 Untagged 报文处理，若同时配置 Untagged 报文丢弃，那么 Tagged 的报文也会同时丢弃。

### 1.4.5 配置灵活 QinQ

请在需要的设备用户侧接口上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#vlan-stacking vlan vlan-id stack-vlan vlan-id [remark-8021p cos-id]</code>	配置灵活 qinq 功能。

## 1.4.6 配置网络侧接口为 Trunk 模式

请在需要配置基本 QinQ 或灵活 QinQ 的设备网络侧接口上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/*)#switchport mode trunk</code>	配置接口 Trunk 模式，可允许双 Tag 报文通过。

## 1.4.7 配置 TPID

请在需要设备的网络侧接口进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	<code>JX(config-ge-1/0/1)#tpid tpid</code>	配置接口的外层 VLAN Tag 的 TPID。

## 1.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show vlan-stacking config</code>	查看接口基本 QinQ 配置信息。



序号	检查项	说明
2	JX#show vlan-stacking interface	查看接口的 QinQ 配置信息。
3	JX#show vlan-stacking resource	查看 QinQ 的资源信息

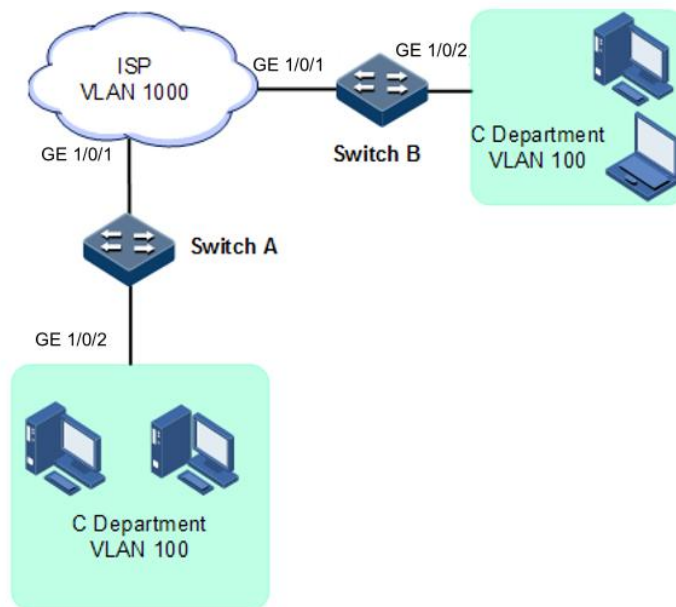
## 1.4.9 配置基本 QinQ 示例

### 组网需求

如下图所示，Switch A 和 Switch B 分别连接了 C 部门的 2 个不同地点的网络。C 部门为 VLAN100，要通过运营商 VLAN1000 网络进行通信。运营商的 TPID 为 9100。

通过在 Switch A 和 Switch B 配置基本 QinQ 功能来实现部门内部通过运营商网络的正常通信。

图 1-7 基本 QinQ 应用组网示意图



### 配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100 和 VLAN 1000 并激活。

```
JX#config
JX(config)#vlan 100,1000
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100
```

```
JX(config-ge-1/0/1)#tpid 0x9100
JX(config-ge-1/0/1)#exit
```

步骤 2 使能接口的基本 QinQ 功能。

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type dot1q-tunnel
JX(config-ge-1/0/2)#port default vlan 1000
JX(config-ge-1/0/2)#exit
```

## 检查结果

通过 **show dot1q-tunnel** 命令查看 QinQ 配置信息。

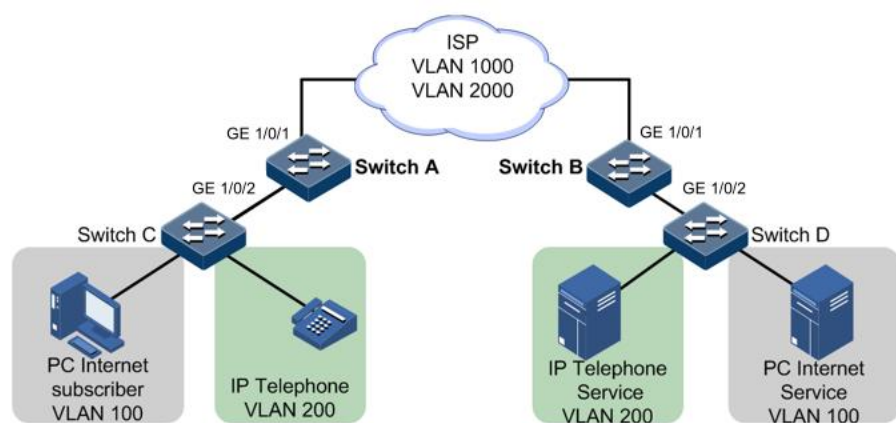
```
JX#show interface ge 1/0/2 config
!
interface ge 1/0/2
port link-type dot1q-tunnel
port default vlan 1000
```

## 1.4.10 配置灵活 QinQ 示例

### 组网需求

如下图所示，运营商网络区分普通 PC 上网业务和 IP 电话业务，故将 PC 上网业务分配 VLAN 1000，IP 电话业务分配的 VLAN 是 2000。在 Switch A 和 Switch B 上设置灵活 QinQ，将分配给 PC 上网业务的 VLAN 100 添加外层 Tag VLAN 1000，将分配给 IP 电话业务的 VLAN 200 添加外层 Tag VLAN 2000，使用户和服务器间通过运营商的网络能够正常通信。运营商的 TPID 为 9100。

图 1-8 灵活 QinQ 应用组网示意图



### 配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100, 200, 1000, 2000 并激活, TPID 为 9100。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vlan 100,200,1000,2000
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 1000,2000
SwitchA(config-ge-1/0/1)#tpid 0x9100
SwitchA(config-ge-1/0/1)#exit
```

步骤 2 使能接口 GE 1/0/2 的灵活 QinQ 功能。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan
100,200,1000,2000
SwitchA(config-ge-1/0/2)#vlan-stacking enable
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 100 stack-vlan 1000
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 200 stack-vlan 2000
SwitchA(config-ge-1/0/2)#exit
```

## 检查结果

通过 **show vlan-stacking interface** 命令查看灵活 QinQ 配置信息。

以 Switch A 为例。

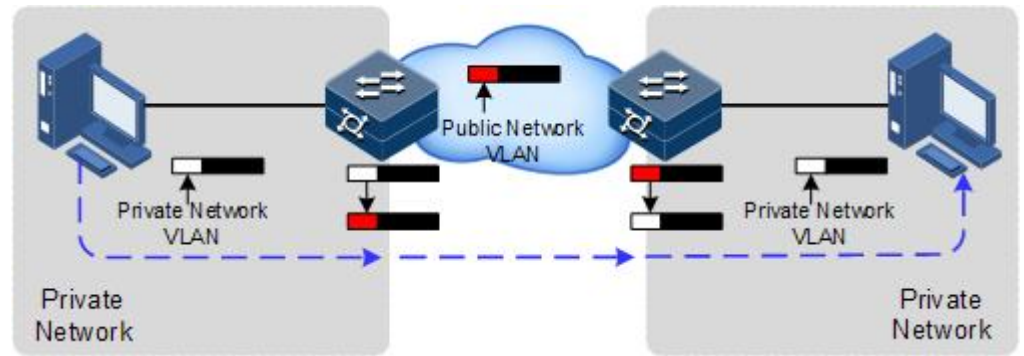
```
SwitchA#show vlan-stacking interface
Interface          MatchVlan(outer/8021p)
StackVlan(inner/outer/8021p)
-----
-----
ge-1/0/2           100/-                -/1000/-
ge-1/0/2           200/-                -/2000/-
```

## 1.5 VLAN 转换

### 1.5.1 简介

VLAN 转换主要功能是将以太网业务报文中的私网 VLAN Tag 替换为运营商的 VLAN Tag, 使其按照运营商的 VLAN 转发规则进行传输。在报文从运营商网络转发到对端用户私网时, 再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag, 使报文正确到达目的地。VLAN 转换原理如下图所示。

图 1-9 VLAN 转换原理组网示意图



交换机收到带有用户私网报文的 VLAN Tag 后，根据配置的 VLAN 转换规则对用户私网报文的 VLAN Tag 进行匹配，如果匹配成功，则按照 VLAN 转换规则将私网 VLAN Tag 进行替换。设备支持 1:1 的 VLAN 转换，即将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。

与 QinQ 功能不同的是，VLAN 转换功能不需要对报文进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输。

## 1.5.2 配置准备

### 场景

与 QinQ 区别的是，VLAN 转换只是变更 VLAN 标签，不额外进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输，不会增加原报文的帧长度。VLAN 转换可以用在如下场景：

- 用户业务转换为一个运营商的 VLAN ID。
- 多种用户业务转换为一个运营商的 VLAN ID。

### 前提

在配置 VLAN 转换之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。

## 1.5.3 VLAN 转换的缺省配置

设备上 VLAN 转换的缺省配置如下。

功能	缺省值
VLAN 转换功能状态	禁止

## 1.5.4 配置 VLAN 转换

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#interface interface-type interface-number</code>	进入二层物理接口配置模式。
3	<code>JX(config-ge-1/0/*)#vlan-mapping enable</code>	使能 VLAN 转换功能
4	<code>JX(config-ge-1/0/*)#vlan-mapping vlan vlan-id map-vlan vlan-id [remark-8021p cos-id]</code>	配置单层 1:1 VLAN 转换规则。
5	<code>JX(config-ge-1/0/*)#vlan-mapping vlan vlan-id 8021p cos-id map-vlan vlan-id [remark-8021p cos-id]</code>	配置单层 1:1 VLAN 匹配 cos 转换规则。
6	<code>JX(config-ge-1/0/*)#vlan-mapping vlan vlan-id inner-vlan vlan-id map-vlan vlan-id map-inner-vlan vlan-id [remark-8021p cos-id]</code>	配置内外层 2:2 VLAN 转换规则。
7	<code>JX(config-ge-1/0/*)#vlan-mapping vlan vlan-id inner-vlan vlan-id map-vlan vlan-id [remark-8021p cos-id]</code>	配置内外层 2:1 VLAN 转换规则。
8	<code>JX(config-ge-1/0/*)#vlan-mapping 8021p 802.1p priority map-vlan vlan-id [remark-8021p cos-id]</code>	配置匹配 cos 转换规则。



### 说明

- 基本 QinQ 和 1:1 VLAN 转换命令行可同时配置，VLAN 转换在基本 QinQ 使能前后功能正常。
- 灵活 QinQ 和 1:1 VLAN 转换命令行可同时配置：同时配置时，灵活 QinQ 和 VLAN 转换功能正常；开启/关闭基本 QinQ，灵活 QinQ 和 VLAN 转换功能正常；取消其中一个配置命令，不影响其他配置正常使用。
- 基本 QinQ、灵活 QinQ 和 2:2 VLAN 转换互斥：同时配置灵活 QinQ 和 1:1 VLAN 转换时，匹配 VLAN 不能相同，转换后的 VLAN 不能相同。

## 1.5.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show vlan-mapping interface</code>	查看接口的 VLAN 转换规则配置信息。

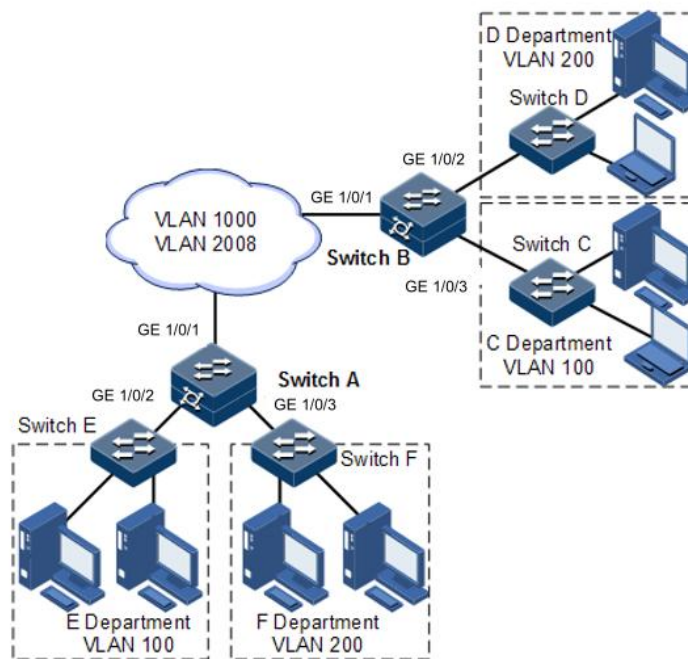
## 1.5.6 配置 VLAN 转换示例

### 组网需求

如下图所示，Switch A 的 GE1/0/2 和 GE1/0/3 分别连接使用 VLAN 100 的 E 部门和使用 VLAN 200 的 F 部门，Switch B 的 GE 1/0/2 和 GE 1/0/3 分别连接使用 VLAN 100 的 C 部门和使用 VLAN 200 的 D 部门。在运营商网络中为 E 部门和 C 部门分配 VLAN 1000 来传输，为 F 部门和 D 部门分配使用 VLAN 2008 来传输。

通过在 Switch A 和 Switch B 配置 1:1 的 VLAN 转换功能来实现 PC 用户和终端用户与其服务器之间的正常通信。

图 1-10 VLAN 转换应用组网示意图



### 配置步骤

Switch A 和 Switch B 配置相同，在这里只描述 Switch A 的配置信息。

步骤 1 创建 VLAN 并激活。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vlan 100,200,1000,2008
```

步骤 2 配置接口 GE 1/0/1 为 Trunk 模式，允许 VLAN 1000 和 VLAN 2008 通过。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 1000,2008
SwitchA(config-ge-1/0/1)#exit
```

- 步骤 3 配置接口 GE 1/0/2 为 Trunk 模式，允许 VLAN 100 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/0/2)#vlan-mapping vlan 100 map-vlan 1000
SwitchA(config-ge-1/0/2)#exit
```

- 步骤 4 配置接口 GE 1/0/3 为 Trunk 模式，允许 VLAN 200 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port link-type trunk
SwitchA(config-ge-1/0/3)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/0/3)#vlan-mapping vlan 200 map-vlan 2008
```

## 检查结果

通过 `show vlan-mapping both interface` 命令查看 1:1 VLAN 转换配置。

```
SwitchA#show vlan-mapping interface
Interface          MatchVlan(vlan/8021p)
MapVlan(vlan/8021p)
-----
ge-1/0/2           inner: -              inner: -/-
                   outer: 100/-          outer: 1000/-
ge-1/0/3           inner: -              inner: -/-
                   outer: 200/-          outer: 2008/-
-----
-----
```

## 1.6 MRP/MVRP

### 1.6.1 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，可以用来传递属性信息。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。通过 MVRP，局域网中的设备可以自动同步 VLAN 信息，极大地减少了网络管理员的 VLAN 配置工作。

### MRP 消息

MRP 消息主要包括 Join 消息、New 消息、Leave 消息和 LeaveAll 消息

- **Join 消息：** 当一个 MRP 实体配置了某些属性，需要对端实体来注册自己的属性信息时，它会向对端实体发送 Join 消息。当一个 MRP 实体收到来自对端实体的 Join 消息时，它会注册该 Join 消息中的属性，并向本设备的其他实体传播该 Join 消息，其他实体收到传播的 Join 消息后，向其对端实体发送 Join 消息。

- **New 消息：**New 消息的作用和 Join 消息比较类似，都是用于对属性的声明。不同的是，New 消息主要用于 MSTP (Multiple Spanning Tree Protocol, 多生成树协议) 拓扑变化的情况。
- **Leave 消息：**当一个 MRP 实体注销了某些属性，需要对端实体进行同步注销时，它会向对端实体发送 Leave 消息。当一个 MRP 实体收到来自对端实体的 Leave 消息时，它会注销该 Leave 消息中的属性，并向本设备的其他实体传播该 Leave 消息，其他实体收到传播的 Leave 消息后，根据该 Leave 消息中的属性在本设备上的状态，决定是否向其对端实体发送该 Leave 消息（比如该 Leave 消息中的属性为某 VLAN，若该 VLAN 为动态 VLAN，且本设备上无实体注册该 VLAN，则在设备上删除该 VLAN，并向对端实体发送该 Leave 消息；若该 VLAN 为静态 VLAN，则不向对端实体发送该 Leave 消息）。
- **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。当一个 MRP 实体收发 LeaveAll 消息时，它会启动 Leave 定时器，同时根据自身的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。该实体在 Leave 定时器超时前，重新注册收到的来自对端实体的 Join 消息中的属性；在 Leave 定时器超时后，注销所有未重新注册的属性信息，从而周期性地清除网络中的垃圾属性。

Leave 消息、LeaveAll 消息通过与 Join 消息配合，确保属性的注销或重新注册。通过消息交互，所有待注册的属性信息可以传播到同一局域网内使能 GARP 功能的所有设备上。

## MRP 定时器

MRP 消息发送的时间间隔通过定时器来实现，MRP 定义了四种定时器，用于控制 MRP 消息的发送周期。

- **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 消息的周期发送。该定时器超时前，实体收集需要发送的 MRP 消息，在该定时器超时后，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。随后再重新启动 Periodic 定时器，开始新一轮的循环。
- **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对端实体，MRP 实体在发送 Join 消息时，将启动 Join 定时器。如果在该定时器超时前收到了来自对端实体的 JoinIn 消息，且该 JoinIn 消息中的属性与发出的 Join 消息中的属性一致，便不再重发该 Join 消息，否则在该定时器超时后，当 Periodic 定时器也超时，它将重发一次该 Join 消息。
- **Leave 定时器：**用来控制属性的注销。当 MRP 实体收到来自对端实体的 Leave 消息（或收发 LeaveAll 消息）时，将启动 Leave 定时器。如果在该定时器超时前，收到来自对端实体的 Join 消息，且该 Join 消息中的属性与收到的 Leave 消息中的属性一致（或与收发的 LeaveAll 消息中的某些属性一致），则这些属性不会在本实体被注销，其他属性则会在该定时器超时后被注销。
- **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。



## MVRP

MVRP (Multiple VLAN Registration Protocol, 多 VLAN 注册协议) 是 MRP 的一种应用, 它基于 MRP 的工作机制, 维护交换机中的 VLAN 动态注册信息, 并传播该信息到其它交换机。

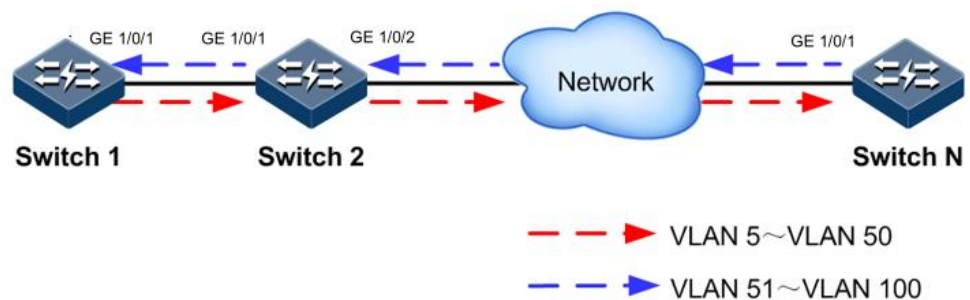
所有支持 MVRP 特性的交换机能够接收来自其它交换机的 VLAN 注册信息, 并动态更新本地的 VLAN 注册信息。而且所有支持 MVRP 特性的交换机能够将本地的 VLAN 注册信息向其它交换机传播, 以便使同一交换网内所有支持 MVRP 特性的设备 VLAN 信息达成一致。MVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息, 也包括来自其它交换机的动态注册信息。

MVRP 有三种注册模式:

- 正常模式 (Normal): 允许动态注册、注销 VLAN, 传播动态、静态 VLAN 信息。
- 固定模式 (Fixed): 禁止动态注册、注销 VLAN, 只传播静态 VLAN 信息, 不传播动态 VLAN 信息, 只允许静态 VLAN 通过, 即只对其他 MVRP 成员传播静态 VLAN 信息。
- 禁止模式 (Forbidden): 禁止动态注册、注销 VLAN, 禁止静态 VLAN 在接口上的创建, 同时删除接口上除 VLAN 1 外的所有 VLAN, 只允许缺省 VLAN (即 VLAN 1) 通过, 只对其他 MVRP 成员传播缺省 VLAN 的信息。

存在多台设备的网络中, 如图 2-11 所示, 如果想在每台设备上配置 VLAN 信息, 并允许指定 VLAN 的报文通过是比较繁琐的。采用 MVRP 来动态注册和传播指定 VLAN, 可以帮助网管人员提高工作效率, 提高准确性。

图 1-11 MVRP 原理示意图



在图 2-11 中, Switch 1 的 GE 1/0/1, Switch 2 的 GE 1/0/1 和 GE 1/0/2, Switch N 的 GE 1/0/1 均为 Trunk 接口。在 Switch 1 中创建 VLAN 5~VLAN 50, 则会按照红色连接线方向在接收接口上动态注册该 VLAN, 直到传播到 Switch N 交换机。在 Switch N 上创建 VLAN 51~VLAN 100, 则沿蓝色连接线注册该 VLAN 信息, 使每个交换机可以完全处理 VLAN 5~VLAN 100 的报文。

## 1.6.2 配置准备

### 场景

利用 MVRP 机制，一个 MVRP 成员上的配置信息会迅速传播到整个局域网中所有使能 MVRP 功能的设备上。

通过 MVRP 功能配置的 Join 定时器、Leave 定时器和 LeaveAll 定时器的值，将应用于所有在同一网络内运行的 MVRP 应用。

### 前提

无

## 1.6.3 缺省配置

### MVRP 缺省配置

设备上 MVRP 的缺省配置如下

功能	缺省值
全局 MVRP 功能状态	禁止
接口 MVRP 功能状态	禁止
MVRP 注册模式	Normal

## 1.6.4 配置 MVRP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	<code>JX#config</code>	进入全局配置模式。
2	<code>JX(config)#mvrp start</code>	使能全局 MVRP 功能。
3	<code>JX(config)#interface interface-type interface-number</code>	进入物理接口配置模式。
4	<code>JX(config-ge-1/0/1)#port link-type trunk</code>	配置接口为 Trunk 模式。
5	<code>JX(config-ge-1/0/1)#mvrp registration { fixed   forbidden   normal }</code>	配置 MVRP 注册模式。
6	<code>JX(config-ge-1/0/1)#mvrp enable</code>	使能接口 MVRP 功能。



- 接口必须先配置为 Trunk 模式才能使能接口 MVRP 功能。
- 不建议用户在聚合组成员接口上使能 MVRP 功能。

## 1.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	<code>JX#show mvrp config</code>	查看 MVRP 的配置信息。
2	<code>JX#show mvrp</code>	查看 MVRP 的接口状态信息。
3	<code>JX#show mvrp interface interface-type interface-number vlan vlan-id</code>	查看 MVRP 的定时器信息。

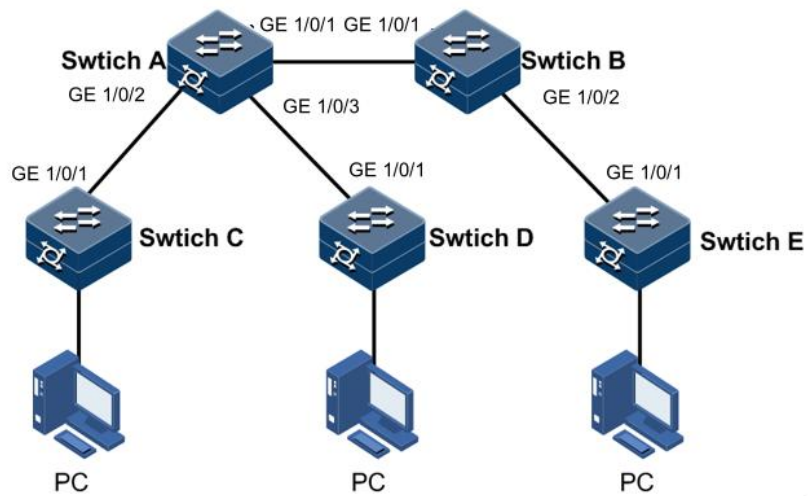
## 1.6.6 配置 MVRP 应用示例

### 组网需求

为了在交换机之间动态注册和更新 VLAN 信息，如图 2-12 所示，需要在各交换机上配置 MVRP 功能，来实现各交换机设备之间 VLAN 信息的动态注册和注销。具体要求如下：

- 在 Switch A 和 Switch C 中配置静态 VLAN 5~VLAN 10。
- Switch D 中配置静态 VLAN 15~VLAN 20。
- Switch E 中配置静态 VLAN 25~VLAN 30。
- 将所有与其他交换机相连的接口设置为 Trunk 模式，然后使能接口的 MVRP 功能。
- 配置各接口 MVRP 的 Join 定时器、Leave 定时器和 LeaveAll 定时器分别为 3000、15000 和 20000。

图 1-12 MVRP 应用组网示意图



## 配置步骤

步骤 1 创建 VLAN 并使能全局 MVRP 功能。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vlan 5-10
SwitchA(config)#mvrp start
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#mvrp start
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#config
SwitchC(config)#vlan 5-10
SwitchC(config)#mvrp start
```

配置 Switch D。

```
JX#hostname SwitchD
SwitchD#config
SwitchD(config)#vlan 15-20
SwitchD(config)#mvrp start
```

配置 Switch E。

```
JX#hostname SwitchE
SwitchE#config
SwitchE(config)#vlan 25-30
SwitchE(config)#mvrp start
```

步骤 2 分别配置 Switch A 的 GE 1/0/1、GE 1/0/2、GE 1/0/3 接口，Switch B 的 GE 1/0/1、GE 1/0/2，Switch C 的 GE 1/0/1，Switch D 的 GE 1/0/1 接口为

Trunk 模式，并使能接口的 MVRP 功能。以配置 Switch A 的 GE 1/0/1 接口为例，其余接口配置步骤相同。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/1)#mvrp enable
SwitchA(config-ge-1/0/1)#exit
```

- 步骤 3 分别配置 Switch A 的 GE 1/0/1、GE 1/0/2、GE 1/0/3 接口、Switch B 的 GE 1/0/1、GE 1/0/2，Switch C 的 GE 1/0/1，Switch D 的 GE 1/0/1 接口的 GARP 定时器时间。以配置 Switch A 为例，其余接口配置步骤相同。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#mvrp timer join 3000
SwitchA(config-ge-1/0/1)#mvrp timer leave 15000
SwitchA(config-ge-1/0/1)#mvrp timer leave-all 20000
```

## 检查结果

通过 **show mvrp config** 命令查看设备上接口的 MVRP 配置信息，以 Switch A 为例。

```
SwitchA#show mvrp config

Version                : MVRP_V13.10.00.00

Compliance-GVRP       : disable

Interface      JoinTime(ms)  LeaveTime(ms)
LeaveAllTime(ms) PeriodicTime(ms) Mode      State
-----
-----
GE 1/0/1      3000          15000        20000      --
normal enable
```

通过 **show vlan** 命令查看设备上的 VLAN 信息，以 Switch A 为例。

```
SwitchA#show vlan

NOTE:

      S: supervlan      P: pvlan      N: normal

Vlan Type      Ports('M': member , '-' : not member)
-----
-----
1    N/static  untagged: ge-1/0/1<->ge-1/0/16
MMMMMMMMMMMMMMMMMMMM

                                ge-1/0/17<->ge-1/0/32
MMMMMMMMMMMMMMMMMMMM

                                ge-1/0/33<->ge-1/0/48
MMMMMMMMMMMMMMMMMMMM
```

```

                                10ge-1/0/49<->10ge-1/0/54      MMMMMM
2      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
3      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
4      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
5      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
6      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
7      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
8      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
9      N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
10     N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----
20     N/mvrrp      tagged:  ge-1/0/1<->ge-1/0/16
M-----

-----
-----

Total: 11   Static: 1   Dynamic: 10

```

## 1.7 VTP

### 1.7.1 简介

VTP 协议（VLAN TRUNK PROTOCOL）减少了在交换网络中的配置工作。当在 vtp server 上配置新的 vlan 时，这些 vlan 配置会通过交换机在同域中散播。这就减少了在各台交换机上都必须配置相同 vlan 的操作。

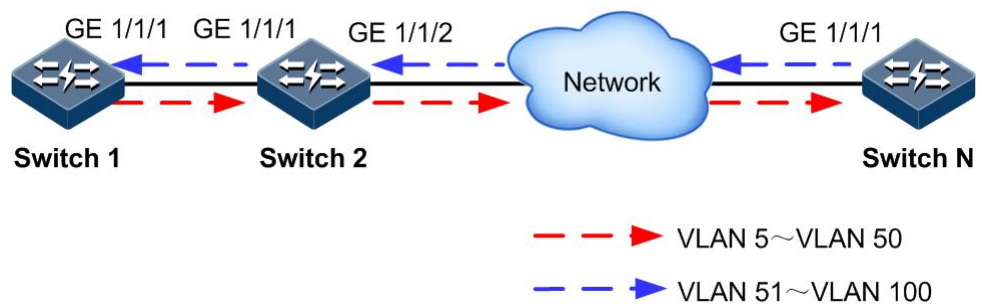
#### 相关概念

- **VTP 域：**也称为 VLAN 管理域，由一个以上共享 VTP 域名的相互连接的交换机组成。要使用 VTP，就必须为每台交换机指定 VTP 域名。VTP 信息只能在 VTP 域内保持。Vlan 信息只在相同域中进行同步。
- **服务器(server)模式：**该模式提供 VTP 消息：包括 VLAN ID 和名字信息，学习相同域名的 VTP 消息，转发相同域名的 VTP 消息，可以添加、删除和更改 VLAN。设置成功后进行 vlan 的配置，包括添加、

删除和更改 VLAN。配置成功后，server 会发出汇总通告，通知该 VTP 域内的交换机 vlan 信息更改情况。然后发送一个或多个子集通告。添加、删除、修改某个 VLAN，改变 VLAN 的名称都会触发子集通告。如果有多个 VLAN，为了通告所有的信息，可能需要发送多个子集通告。Server 模式重启后，会自动发汇总通告和子集通告，用于 vtp 域内信息的同步。

- 客户机(client)模式：该模式请求 VTP 消息，学习相同域名的 VTP 消息，转发相同域名的 VTP 消息，可以配置静态 vlan，但配置的静态 vlan 不会通告出去，配置静态 vlan 也不会修改配置修订号。将 client 上的静态 vlan 删除后，client 的配置修订号会重置为 0，同时向 server 发送请求通告，用于同步 vlan 信息。将一台交换机配置成 client 模式时，该交换机会向 server 发送通告请求，之后收到汇总通告和子集通告，将自身配置和 vtp 域内配置统一。
- 透明传输(transparent)模式：该模式中的交换机不参与 VTP。当交换机处于透明模式时，它不通告其 VLAN 配置信息。而且，它的 VLAN 数据库更新与收到的通告也不保持同步。但它可以创建和删除本地的 VLAN。不过，这些 VLAN 的变更不会传播到其他任何交换机上。该模式转发 VTP 包。当 VTP 从 client 以及 server 切换到 transparent 模式时，配置修订号会置 0。透明模式的交换机在转发 VTP 消息之前要检查 VTP 消息中的域名和版本，只有两者合本机相同才转发。
- 修订号：VTP 通告信息中带有配置修订号，配置修订号的大小代表着 VLAN 配置信息的新旧程度。高版本号代表更新的 VLAN 配置信息。只要客户机接收到一个有更高配置修订号的更新，它都用该 VTP 更新中的 vlan 信息覆盖当前的 vlan 信息。每当服务器上修改了 VLAN 的配置(修改包括创建、删除 VLAN、更改 VLAN 的名称)，其配置修订版本号就会增加，然后用新的版本号向域中通告。

VTP 原理示意图



在 Switch 1 中创建 VLAN 5~VLAN 50，则会按照红色连接线方向在接收接口上动态注册该 VLAN，直到传播到 Switch N 交换机。

## 1.7.2 配置准备

### 场景

利用第 2 层中继帧，在一组交换机之间进行 VLAN 通信。VTP 从一个中心控制点开始，维护整个企业网上 VLAN 信息，确认配置的一致性。

## 前提

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 将接口加入 VLAN。
- 如果接口配置有环协议，请确保接口没有被环协议阻塞

## 1.7.3 缺省配置

### VTP 缺省配置

设备上 MVRP 的缺省配置如下

功能	缺省值
全局 VTP 功能状态	禁止
VTP 域默认模式	Server
VTP 版本	1

## 1.7.4 配置 VTP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX# <b>configure</b>	进入全局配置模式。
2	JX(config)# <b>vtp domain name</b>	创建 VTP 域。
3	JX(config)# <b>password password</b>	配置 VTP 域密码
4	JX(config-vtp-domain-test)# <b>mode client</b>	设置 VTP 域的模式为客户机模式 client。
5	JX(config-ge-1/0/*)# <b>join vtp domain name</b>	接口加入 vtp 域。

## 1.7.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX# <b>show vtp domain</b>	查看 VTP 的域配置信息。
2	JX# <b>show vtp interface</b>	查看 VTP 的接口状态信息。



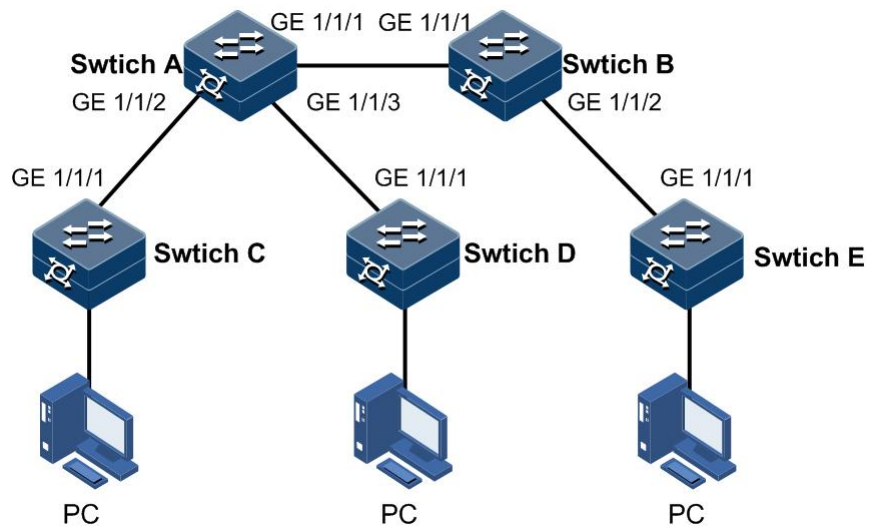
## 1.7.6 配置 VTP 应用示例

### 组网需求

为了在交换机之间动态注册和更新 VLAN 信息，如图 2-12 所示，需要在各交换机上配置 VTP 功能，来实现各交换机设备之间 VLAN 信息的动态注册和注销。具体要求如下：

- Switch A 作为 vtp 的 server 工作，配置静态 VLAN 5~VLAN 100。
- 其他 switch 作为 vtp 的 client，接收并创建 VLAN 5~VLAN 100。

图 1-13 VTP 应用组网示意图



### 配置步骤

步骤 1 创建 VTP 域并配置各自的工作模式。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vtp domain A
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#vtp domain A
SwitchB(config-vtp-domain-A)#mode client
```

其他交换机同 Switch B。

步骤 2 分别配置 Switch A 的 GE 1/0/1、GE 1/0/2、GE 1/0/3 接口，Switch B 的 GE 1/0/1、GE 1/0/2，Switch C 的 GE 1/0/1，Switch D 的 GE 1/0/1 接口加入 vtp 域。以配置 Switch A 的 GE 1/0/1 接口为例，其余接口配置步骤相同。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#join vtp domain A
SwitchA(config-ge-1/0/1)#port hybrid vlan 5-100 tagged
SwitchA(config-ge-1/0/1)#exit
```

步骤 3 在 Switch A 上创建 vlan 5-100

```
SwitchA(config)#vlan 5-100
```

## 检查结果

通过 **show vtp domain** 命令查看设备上的 VTP 域配置信息，以 Switch B 为例。

```
SwitchB#show vtp domain
Domain: 1
  Name:                A
  Version:              1
  Pruning:              Disable
  Password:             --
  Mode:                 client
  Configure Revision Num 2
  Vlan:                 1,5-100
```

通过 **show vtp interface** 命令查看设备上的 VTP 接口配置信息，以 Switch B 为例。

```
SwitchB#show vtp interface
  Interface      State      Domain      vlanList
-----
  ge-1/0/1       enable    A           2-4094
  ge-1/0/2       enable    A           2-4094
```

通过 **show vlan** 命令查看接口加入 vlan 的情况

```
SwitchB(config)#show vlan
NOTE:
   S: supervlan       P: pvlan           N: normal

  Vlan Type      Ports('M': member , '-' : not member)
-----
   1   N/static  untagged: ge-1/0/1<->ge-1/0/16
MMMMMMMM MMMMMMMM
                                  ge-1/0/17<->ge-1/0/32
MMMMMMMM MMMMMMMM
                                  ge-1/0/33<->ge-1/0/48
MMMMMMMM MMMMMMMM
                                  10ge-1/0/49<->10ge-1/0/54
5     N/vtp      tagged: ge-1/0/1<->ge-1/0/16  MMMMMMM
MM-----
```

```
6    N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
7    N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
8    N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
9    N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
10   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
11   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
12   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
13   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
14   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
15   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
16   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
17   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
18   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
19   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
20   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
21   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
22   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
23   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
24   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
25   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
26   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
27   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
28   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
29   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
30   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
31   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
32   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
33   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
34   N/vtp    tagged: ge-1/0/1<->ge-1/0/16
MM-----
```

```
35 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
36 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
37 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
38 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
39 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
40 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
41 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
42 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
43 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
44 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
45 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
46 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
47 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
48 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
49 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
50 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
51 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
52 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
53 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
54 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
55 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
56 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
57 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
58 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
59 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
60 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
61 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
62 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
63 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
```

```
64 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
65 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
66 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
67 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
68 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
69 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
70 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
71 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
72 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
73 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
74 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
75 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
76 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
77 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
78 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
79 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
80 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
81 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
82 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
83 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
84 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
85 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
86 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
87 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
88 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
89 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
90 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
91 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
92 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
```

```
93 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
94 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
95 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
96 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
97 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
98 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
99 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
100 N/vtp tagged: ge-1/0/1<->ge-1/0/16
MM-----
```

-----

```
Total: 97 Static: 1 Dynamic: 9
```