

目 录

第 1 章 VLAN配置.....	1-1
1.1 VLAN配置.....	1-1
1.1.1 VLAN介绍	1-1
1.1.2 VLAN的配置任务序列	1-2
1.1.3 VLAN典型应用	1-4
1.1.4 Hybrid端口的典型应用	1-6
1.2 GVRP配置	1-8
1.2.1 GVRP介绍	1-8
1.2.2 GVRP配置任务序列	1-9
1.2.3 GVRP举例	1-10
1.2.4 GVRP排错帮助	1-12
1.3 Dot1q-tunnel配置	1-12
1.3.1 Dot1q-tunnel介绍	1-12
1.3.2 Dot1q-tunnel配置	1-13
1.3.3 Dot1q-tunnel典型应用	1-13
1.3.4 Dot1q-tunnel排错帮助	1-14
1.4 VLAN-translation配置	1-15
1.4.1 VLAN-translation介绍	1-15
1.4.2 VLAN-translation配置	1-15
1.4.3 VLAN-translation典型应用	1-16
1.4.4 VLAN-translation排错帮助	1-17
1.5 Super VLAN配置	1-17
1.5.1 Super VLAN简介	1-17
1.5.2 Super VLAN配置任务序列	1-19
1.5.3 Super VLAN典型应用	1-20
1.5.4 Super VLAN排错帮助	1-21
第 2 章 MAC地址表配置	2-1
2.1 MAC地址表介绍	2-1
2.1.1 MAC地址表的获取	2-1
2.1.2 转发或过滤	2-2
2.2 MAC地址表配置	2-3
2.3 典型配置举例	2-5
2.4 排错帮助	2-5

2.5 MAC Notification配置.....	2-6
2.5.1 MAC Notification介绍.....	2-6
2.5.2 MAC Notification配置.....	2-6
2.5.3 MAC Notification举例.....	2-7
2.5.4 MAC Notification排错帮助	2-8

第1章 VLAN配置

1.1 VLAN配置

1.1.1 VLAN介绍

VLAN（Virtual Local Area Network）即虚拟局域网，这项技术可以根据功能、应用或者管理的需要将局域网内部的设备逻辑地划分为一个个网段，从而形成一个个虚拟的工作组，并且不需要考虑设备的实际物理位置。IEEE 颁布了 IEEE802.1Q 协议以规定标准化 VLAN 的实现方案，交换机的 VLAN 功能即按照 802.1Q 的标准实现。

VLAN 技术的特点在于可以根据需要动态的将一个大的局域网划分成许多不同的广播域：

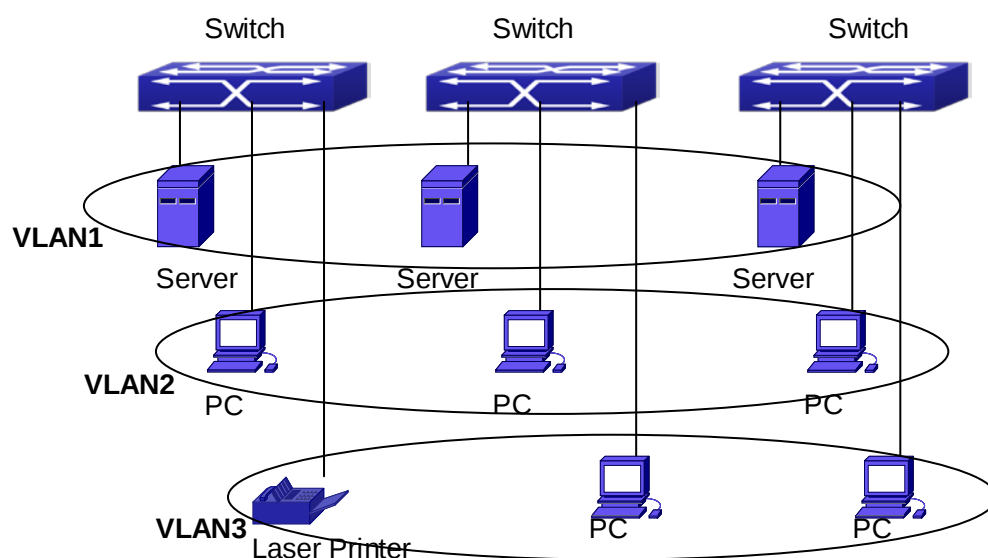


图 1-1 按照逻辑定义的 VLAN 网络

每个广播域即一个 VLAN，VLAN 和物理上的局域网有相同的属性，不同之处只在于 VLAN 是逻辑的而不是物理的划分，所以 VLAN 的划分不必根据实际的物理位置，而每个 VLAN 内部的广播、组播和单播流量都是与其它 VLAN 隔绝的。

基于 VLAN 的以上特性，VLAN 技术给我们带来以下的便利：

- ☞ 改善网络性能
- ☞ 节约网络资源

- ☞ 简化网络管理
- ☞ 降低网络成本
- ☞ 提高网络安全

交换机根据端口在转发报文时是否带tag 标签的不同处理方式，把以太网端口分为三种链路类型：Access、Hybrid和Trunk。

Access 类型的端口只能属于一个 VLAN，一般用于连接计算机的端口。

Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口。

Hybrid 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时：Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许 native VLAN 的报文发送时不打标签。

在交换机中，实现了 802.1Q 所定义的 VLAN 和 GVRP（GARP VLAN Registration Protocol），本章将对交换机 VLAN 和 GVRP 的使用和配置进行详细的说明。

1.1.2 VLAN的配置任务序列

1. 创建或删除 VLAN
2. 指定或删除 VLAN 名称
3. 为 VLAN 分配交换机端口
4. 设置交换机端口类型
5. 设置 Trunk 端口
6. 设置 Access 端口
7. 设置 Hybrid 端口配置
8. 打开或关闭全局的 VLAN 入口规则
9. 配置 Private VLAN
10. 设置 Private VLAN 的绑定操作
11. 指定内部 VLAN ID

1.创建或删除 VLAN

命令	解释
全局配置模式	
vlan WORD	创建/删除 VLAN 或进入 VLAN 模式。
no vlan WORD	

2.指定或删除 VLAN 名称

命令	解释
----	----

VLAN 配置模式	
name <vlan-name> no name	设置/删除 VLAN 名称。

3. 为 VLAN 分配交换机端口

命令	解释
VLAN 配置模式	
switchport interface <interface-list> no switchport interface <interface-list>	为 VLAN 分配交换机端口。

4. 设置交换机端口类型

命令	解释
端口配置模式	
switchport mode {trunk access hybrid}	设置当前端口为 Trunk, Access 端口或 Hybrid 端口。

5. 设置 Trunk 端口

命令	解释
端口配置模式	
switchport trunk allowed vlan {WORD all add WORD except WORD remove WORD} no switchport trunk allowed vlan	设置/删除 Trunk 端口允许通过的 VLAN。
switchport trunk native vlan <vlan-id> no switchport trunk native vlan	设置/删除 Trunk 端口的 PVID。

6. 设置 Access 端口

命令	解释
端口配置模式	
switchport access vlan <vlan-id> no switchport access vlan	将当前端口加入/退出到指定 VLAN。

7. 设置 Hybrid 端口

命令	解释
端口配置模式	

switchport hybrid allowed vlan {WORD all add WORD except WORD remove WORD} {tag untag} no switchport hybrid allowed vlan	设置/删除 Hybrid 端口允许以 tag 或 untag 方式通过的 VLAN。
switchport hybrid native vlan <vlan-id> no switchport hybrid native vlan	设置/删除端口的 PVID。

8. 打开或关闭 VLAN 的入口规则

命令	解释
端口配置模式	
vlan ingress enable no vlan ingress enable	打开及关闭 VLAN 的入口规则。

9. 配置 Private VLAN

命令	解释
VLAN 配置模式	
private-vlan {primary isolated community} no private-vlan	将当前 VLAN 设置为 Private VLAN。

10. 设置 Private VLAN 的绑定操作

命令	解释
VLAN 配置模式	
private-vlan association <secondary-vlan-list> no private-vlan association	设置/删除 Private VLAN 的绑定关系。

11. 指定内部 VLAN ID

命令	解释
全局配置模式	
vlan <2-4094> internal	指定内部 VLAN 的 ID 号。

1.1.3 VLAN典型应用

案例：

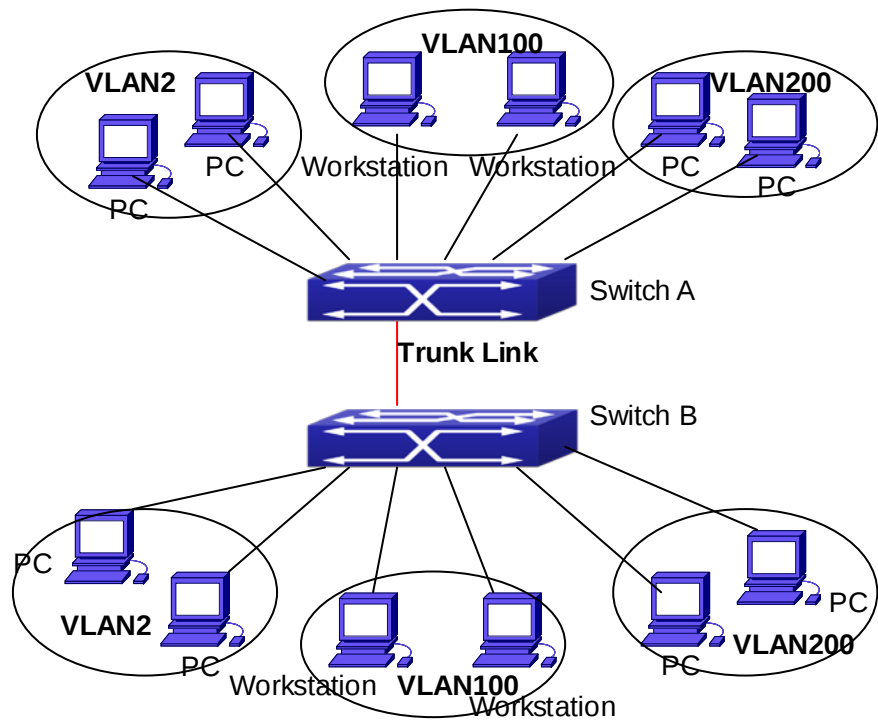


图 1-2 VLAN 典型应用拓扑图

由于局域网安全和应用的需要，需要将现有的整个局域网划分为 3 个 VLAN：VLAN2、VLAN100 和 VLAN200，并且要求这三个 VLAN 跨越两个地域 A 和 B，现在两处分别放置一台交换机，因此 VLAN 流量只要可以在交换机间传输，就可以满足跨地域的要求。

配置项目	配置说明
VLAN2	A 地、B 地交换机 2~4 端口
VLAN100	A 地、B 地交换机 5~7 端口
VLAN200	A 地、B 地交换机 8~10 端口
Trunk port	A 地、B 地交换机的 11 端口

将两台交换机的 Trunk port 相连，成为 Trunk link，用于承载跨交换机的 vlan 流量；将各种网络设备连接到交换机的各个 VLAN 的端口上，就归属到相应的 VLAN 之中。

在本例中，1 号和 12 号端口空闲，可以做为管理端口或其它用途。

配置步骤如下：

A 交换机：

Switch (config)#vlan 2

Switch (Config-Vlan2)#switchport interface ethernet 1/2-4

Switch (Config-Vlan2)#exit

```
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/5-7
Switch (Config-Vlan100)#exit
Switch (config)#vlan 200
Switch (Config-Vlan200)#switchport interface ethernet 1/8-10
Switch (Config-Vlan200)#exit
Switch (config)#interface ethernet 1/11
Switch (Config-If-Ethernet1/11)#switchport mode trunk
Switch (Config-If-Ethernet1/11)#exit
Switch (config)#
```

B 交换机:

```
Switch (config)#vlan 2
Switch (Config-Vlan2)#switchport interface ethernet 1/2-4
Switch (Config-Vlan2)#exit
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/5-7
Switch (Config-Vlan100)#exit
Switch (config)#vlan 200
Switch (Config-Vlan200)#switchport interface ethernet 1/8-10
Switch (Config-Vlan200)#exit
Switch (config)#interface ethernet 1/11
Switch (Config-If-Ethernet1/11)#switchport mode trunk
Switch (Config-If-Ethernet1/11)#exit
```

1.1.4 Hybrid端口的典型应用

案例:

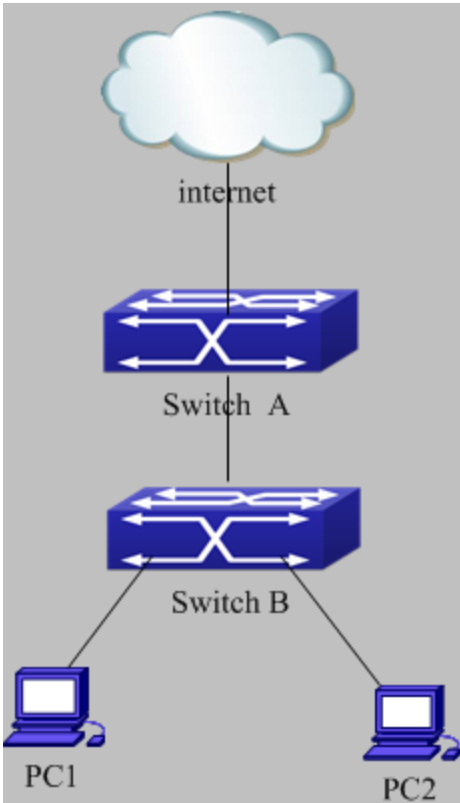


图 1-3 Hybrid 口的典型应用场景

PC1 与 Switch B 的 Ethernet 1/7 口相连，PC2 与 Switch B 的 Ethernet 1/9 口相连，Switch A 的 Ethernet 1/10 与 Switch B 的 Ethernet 1/10 相连。

出于安全的考虑，要求 PC1 和 PC2 之间不能互访，但是 PC1 和 PC2 可以通过网关 Switch A 访问其它的网络资源。这种情况下我们可以通过 Hybrid 端口来实现。

配置项如下：

端口	类型	PVID	允许通过的 VLAN
Switch A 的 1/10	Access	10	允许 VLAN 10 的报文以 untag 方式通过
Switch B 的 1/10	Hybrid	10	允许 VLAN 7,9,10 的报文以 untag 方式通过
Switch B 的 1/7	Hybrid	7	允许 VLAN 7,10 的报文以 untag 方式通过
Switch B 的 1/9	Hybrid	9	允许 VLAN 9,10 的报文以 untag 方式通过

配置步骤如下：

A 交换机：

```
Switch(config)#vlan 10
```

```
Switch(Config-Vlan10)#switchport interface ethernet 1/10
```

B 交换机:

```
Switch(config)#vlan 7;9;10
```

```
Switch(config)#interface ethernet 1/7
```

```
Switch(Config-If-Ethernet1/7)#switchport mode hybrid
```

```
Switch(Config-If-Ethernet1/7)#switchport hybrid native vlan 7
```

```
Switch(Config-If-Ethernet1/7)#switchport hybrid allowed vlan 7;10 untag
```

```
Switch(Config-If-Ethernet1/7)#exit
```

```
Switch(Config)#interface Ethernet 1/9
```

```
Switch(Config-If-Ethernet1/9)#switchport mode hybrid
```

```
Switch(Config-If-Ethernet1/9)#switchport hybrid native vlan 9
```

```
Switch(Config-If-Ethernet1/9)#switchport hybrid allowed vlan 9;10 untag
```

```
Switch(Config-If-Ethernet1/9)#exit
```

```
Switch(Config)#interface Ethernet 1/10
```

```
Switch(Config-If-Ethernet1/10)#switchport mode hybrid
```

```
Switch(Config-If-Ethernet1/10)#switchport hybrid native vlan 10
```

```
Switch(Config-If-Ethernet1/10)#switchport hybrid allowed vlan 7;9;10 untag
```

```
Switch(Config-If-Ethernet1/10)#exit
```

1.2 GVRP配置

1.2.1 GVRP介绍

GVRP 即 GARP VLAN 属性注册协议，它是 GARP（通用属性注册）协议的一个应用。GARP 协议主要用于建立一种属性传递扩散的机制，以保证协议实体能够注册和注销该属性。GARP 作为一个属性注册的载体，可以用来传播属性。而根据传播的属性的不同，可以分为很多应用协议，例如 GMRP 和 GVRP。所以说 GVRP 是通过 GARP 这一协议机制，把 VLAN 属性信息传播到整个二层网络的协议。

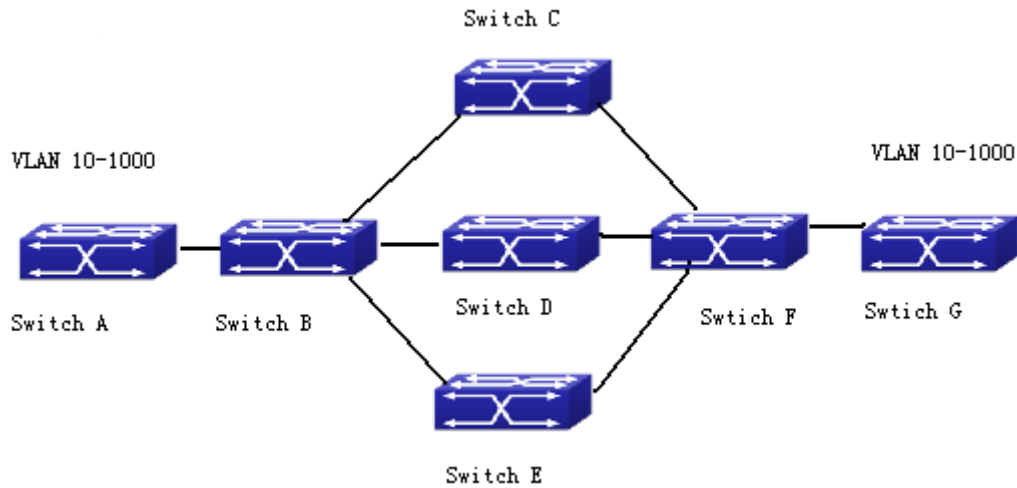


图 1-4 典型应用场景。

其中 A 和 G 是二层网络中没有直连的两个交换机，BCDEF 是二层网络连接 A 和 G 的中间的交换机，交换机 A 和 G 手工配置了 VLAN100-1000，BCDEF 没有此配置，在没有开启 GVRP 的情况下，A 和 G 的 VLAN100-1000 是不能相互通信的，因为中间交换机没有相关 VLAN，但是在所有交换机开启 GVRP 功能之后，通过 GVRP 的 VLAN 属性传播机制使得中间交换机 BCDEF 动态的注册了这些 VLAN，使得 A 和 G 的 VLAN100-1000 中每一个 VLAN 都可以相互通信，即可以看作是一个 VLAN。当 A 和 G 手动注销 VLAN100-1000 后，中间交换机 BCDEF 动态注册的这些 VLAN 也会随之注销。简单说来，通过 GVRP 协议，两个不相邻的交换机的相同 VLAN 可以互相通信，而不必去手动配置中间的每台路由器（这样的手动配置不但麻烦，并且很容易出错），从而达到在复杂的组网环境中简化 VLAN 配置的目的。

1.2.2 GVRP配置任务序列

GVRP 配置任务序列如下：

- 1. 配置 GARP 定时器参数
- 2. 配置端口类型
- 3. 开启 GVRP 功能

1. 配置 GARP 定时器参数

命令	解释
全局配置模式	
garp timer join <200-500> garp timer leave <500-1200> garp timer leaveall <5000-60000> no garp timer (join leave leaveAll)	配置 GARP 的 leaveall, join 和 leave 定时器。

2. 配置端口类型

命令	解释
端口配置模式	
gvrp no gvrp	开启/关闭端口上 GVRP 功能。

3. 开启 GVRP 功能

命令	解释
全局配置模式	
gvrp no gvrp	全局开启/关闭 GVRP 功能。

1.2.3 GVRP举例

GVRP 典型应用：

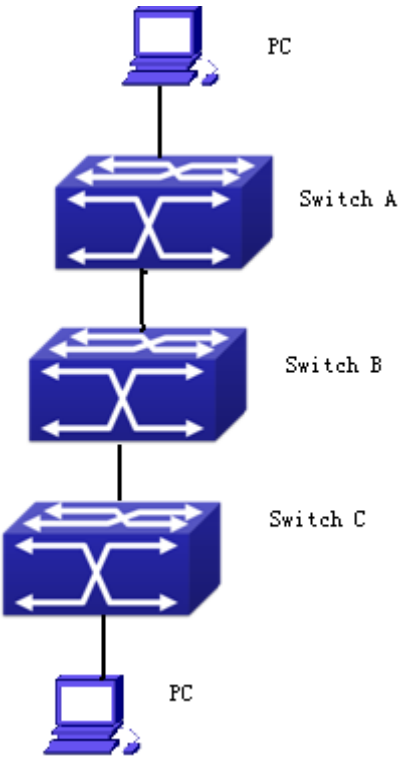


图 1-5 GVRP 典型应用拓扑图

为了实现交换机之间 VLAN 信息的动态注册和更新，需要在交换机上配置 GVRP 协议。在交换机 A、B 和 C 上配置 GVRP，使得交换机 B 学习到动态 VLAN100，这样，分别连接到交换机 A 和 C 的 VLAN100 上的两台工作站就可以通过没有配置静态 VLAN100 的交换机 B 互相通信。

配置项目	配置说明
VLAN100	交换机 A、C 的 2~6 端口
Trunk port	交换机 A、C 的 11 号端口，交换机 B 的 10、11 号端口
全局 GVRP	交换机 A、B、C
端口 GVRP	交换机 A、C 的 11 号端口，交换机 B 的 10、11 号端口

将两台工作站分别与交换机 A 和 B 的 VLAN100 的端口相连，将交换机 A 的 11 号端口与交换机 B 的 10 端口相连，交换机 B 的 11 号端口与交换机 C 的 11 号端口相连。

配置步骤如下：

Switch A:

```
Switch (config)#gvrp
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/2-6
Switch (Config-Vlan100)#exit
Switch (config)#interface ethernet 1/11
Switch (Config-If-Ethernet1/11)#switchport mode trunk
Switch (Config-If-Ethernet1/11)#gvrp
Switch (Config-If-Ethernet1/11)#exit
```

Switch B:

```
Switch(config)#gvrp
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/10)#gvrp
Switch(Config-If-Ethernet1/10)#exit
Switch (config)#interface ethernet 1/11
Switch (Config-If-Ethernet1/11)#switchport mode trunk
Switch (Config-If-Ethernet1/11)#gvrp
Switch (Config-If-Ethernet1/11)#exit
```

Switch C:

```
Switch (config)#gvrp
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/2-6
Switch (Config-Vlan100)#exit
Switch (config)#interface ethernet 1/11
Switch (Config-If-Ethernet1/11)#switchport mode trunk
```

```
Switch (Config-If-Ethernet1/11)#gvrp
Switch (Config-If-Ethernet1/11)#exit
```

1.2.4 GVRP排错帮助

Trunk 链路两端 Trunk 端口的 GARP 计数器设置必须相同，否则 GVRP 不能正常工作。交换机的 GVRP 功能不能和 RSTP 同时打开，如果要打开 GVRP 功能，请首先关闭端口的 RSTP 功能。

1.3 Dot1q-tunnel配置

1.3.1 Dot1q-tunnel介绍

Dot1q-tunnel 也称 QinQ (802.1Q-in-802.1Q)，是 802.1Q 的扩展，其核心思想是将用户私网 VLAN 标签（CVLAN tag）封装到公网 VLAN 标签（SPVLAN tag）上，报文带着两层 VLAN 标签穿越服务商的骨干网络，从而为用户提供一种较为简单的二层隧道。它简单而易于管理，仅仅通过静态配置即可实现，特别适用于小型的以三层交换机为骨干的企业网或小规模城域网。

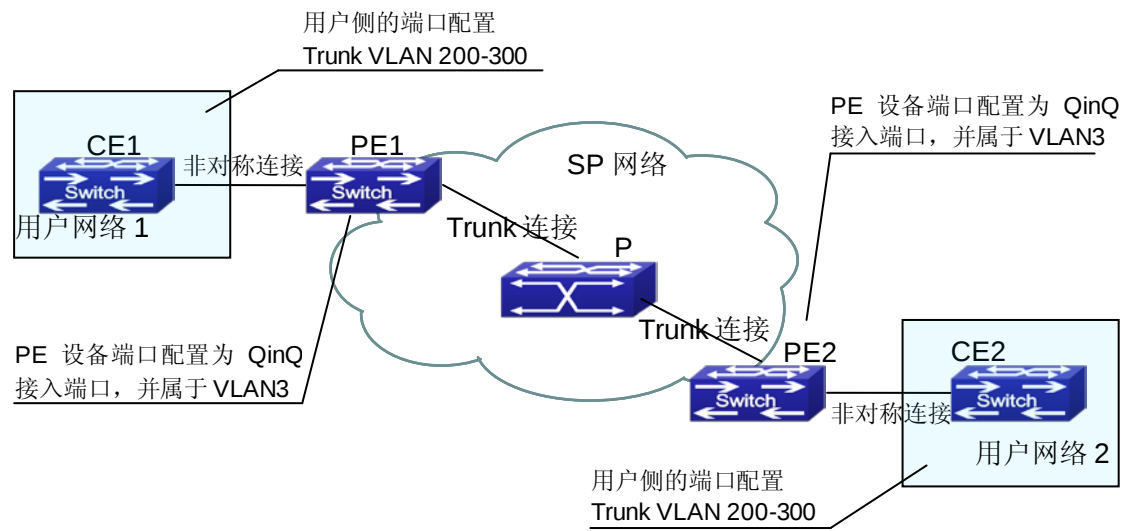


图 1-6 基于 Dot1q-tunnel 的互连模式

如上图所示，在用户端口上使能 dot1q-tunnel 功能，并为每个用户分配一个 SPVLAN 号（SPVID），此处为 3，不同的 PE 上应该为同一网络用户分配相同的 SPVID。当报文从 CE1 到达 PE1 时，带有用户内部网络的 VLAN tag 200~300，由于使能了 dot1q-tunnel 功能，PE1 上的用户端口将再次为报文加上另外一层 VLAN tag，其 ID 就是分配给该用户的 SPVID。此后该报文在服务提供商网络中传播时仅在 VLAN3 中进行且全程带有两层 VLAN

tag（内层为进入 PE1 时的 tag，外层为 SPVID），但用户网络的 VLAN 信息对运营商网络来说是透明的。当报文到达 PE2，从 PE2 上的客户端口转发给 CE2 之前，外层 VLAN tag 被剥去，CE2 收到的报文内容与 CE1 发送的报文完全相同。PE1 到 PE2 之间的运营商网络对于用户来说，其作用就是提供了一条可靠的二层链路。

Dot1q-tunnel 技术的产生使得服务提供商可以靠自己的一个 VLAN 来支持客户的多个 VLAN。服务提供商和客户可以独立设置自己的 VLAN。

可见，使用 dot1q-tunnel 功能具有如下特点：

- 通过简单的静态配置即可实现，免去了繁杂的配置，维护工作。
- 运营商只需为每个用户分配一个 **SPVID**，提升了可以同时支持的用户数目；而用户也具有选择和管理 **VLAN ID** 资源的最大自由度（从 **1~4096** 中任意选择）。
- 用户网络具有较高的独立性，在服务提供商升级网络时，用户网络不必更改原有的配置。

本节将对 switch 的 dot1q-tunnel 使用和配置进行详细说明。

1.3.2 Dot1q-tunnel配置

Dot1q-tunnel 的配置任务序列:

1. 设置端口的 dot1q-tunnel 功能
2. 设置端口的协议类型 (TPID)

1. 设置端口的 dot1q-tunnel 功能

命令	解释
端口配置模式	
dot1q-tunnel enable no dot1q-tunnel enable	进入/退出端口的 dot1q-tunnel 模式。

2. 设置端口的协议类型 (TPID)

命令	解释
端口配置模式	
dot1q-tunnel {0x8100 0x9100 0x9200 <1-65535>} tpid	在 trunk 端口上设置端口的协议类型。

1.3.3 Dot1q-tunnel典型应用

案例：

服务提供商边界交换机 PE1 与 PE2 用 VLAN3 来承载客户网络 CE1 与 CE2 的 VLAN200~300 的数据业务。PE1 的端口 1 连接 CE1，端口 10 连接公网，所连设备的 TPID

为 9100；PE2 的端口 1 连接 CE2，端口 10 连接公网。

配置项目	配置说明
VLAN3	PE1、PE2 的端口 1
dot1q-tunnel	PE1、PE2 的端口 1
tpid	9100

配置步骤如下：

PE1:

```
Switch(Config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/1)# exit
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/10)#exit
Switch(Config)#
```

PE2:

```
Switch(Config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/1)# exit
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/10)#exit
Switch(Config)#
```

1.3.4 Dot1q-tunnel排错帮助

- ☞ 在 Trunk 端口启用 dot1q-tunnel 功能会使数据包的标签层数据不可预知，也不是应用中所需要的，因而不推荐在 Trunk 端口启用 dot1q-tunnel 功能。
- ☞ 不能与 STP/MSTP 同时使用。
- ☞ 不能与 PVLAN 同时使用。

1.4 VLAN-translation配置

1.4.1 VLAN-translation介绍

VLAN translation 即 VLAN 翻译，它根据用户的需求将原有的 VLAN ID 转换为新的 VLAN ID，这样可以在不同的 VLAN 之间交换数据。VLAN translation 分为入口翻译与出口翻译，分别在入口或出口对 VLAN ID 进行转换。

本节将对 VLAN translation 的使用和配置进行详细的说明。

1.4.2 VLAN-translation配置

VLAN-translation 的配置任务序列：

1. 设置端口的 VLAN-translation 功能
2. 设置端口 VLAN-translation 的翻译关系
3. 设置端口 VLAN-translation 翻译关系查找失败是否丢包
4. 显示 VLAN-translation 相关配置

1. 设置端口的 VLAN-translation 功能

命令	解释
端口配置模式	
vlan-translation enable no vlan-translation enable	进入/退出端口的 VLAN-translation 模式。

2. 设置端口 VLAN-translation 的翻译关系

命令	解释
端口配置模式	
vlan-translation <old-vlan-id> to <new-vlan-id> {in out} no vlan-translation <old-vlan-id> {in out}	添加/删除 VLAN-translation 翻译关系。

3. 设置端口 VLAN-translation 翻译关系查找失败是否丢包

命令	解释
端口配置模式	
vlan-translation miss drop {in out both} no vlan-translation miss drop {in out both}	设置/取消 VLAN-translation 查找翻译关系失败时丢包。

4. 显示 VLAN-translation 相关配置

命令	解释
特权用户配置模式	
show vlan-translation	显示 vlan-translation 相关配置。

1.4.3 VLAN-translation典型应用

案例：
服务提供商边界交换机 PE1 与 PE2 用 VLAN3 来承载客户网络 CE1 与 CE2 的 VLAN20 的数据业务。PE1 的端口 1/1 连接 CE1，端口 1/10 连接公网；PE2 的端口 1/1 连接 CE2，端口 1/10 连接公网（如下图）。

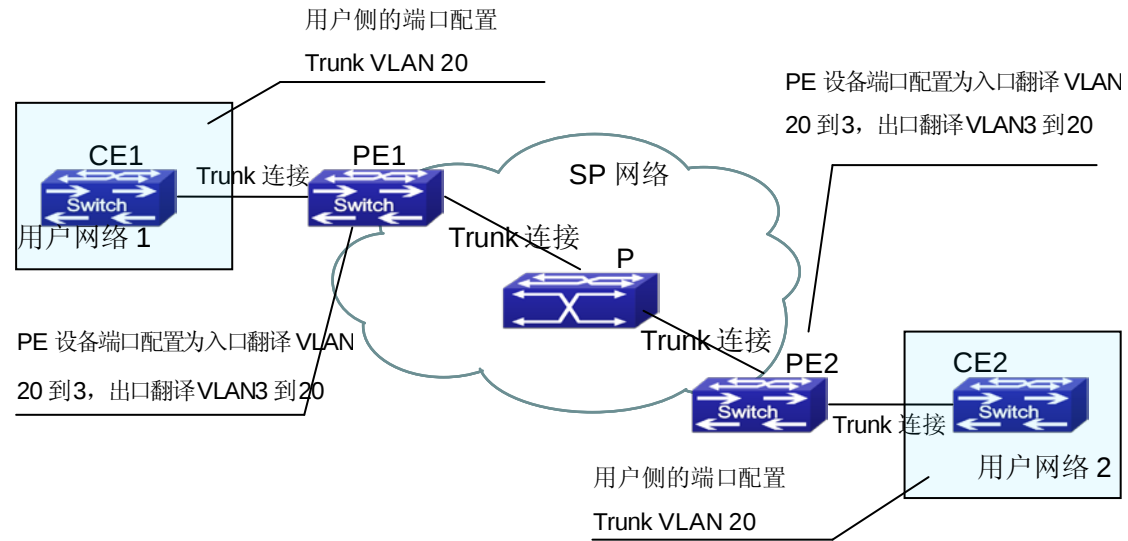


图 1-7 VLAN-translation 典型应用拓扑

配置项目	配置说明
VLAN-translation	PE1、PE2 的端口 1/1
Trunk port	PE1、PE2 的端口 1/1 与端口 1/10

配置步骤如下：

PE1、PE2:

```
switch(Config)#interface ethernet 1/1
switch(Config-Ethernet1/1)#switchport mode trunk
switch(Config-Ethernet1/1)# vlan-translation enable
switch(Config-Ethernet1/1)# vlan-translation 20 to 3 in
switch(Config-Ethernet1/1)# vlan-translation 3 to 20 out
```

```
switch(Config-Ethernet1/1)# exit
switch(Config)#interface ethernet 1/10
switch(Config-Ethernet1/10)#switchport mode trunk
switch(Config-Ethernet1/10)#exit
switch(Config)#
```

1.4.4 VLAN-translation排错帮助

不能与 Dot1q-tunnel 同时使用。

目前部分产品不支持对非 0x8100 的报文进行 vlan translation，所以不建议在 vlan-translation 端口配置 dot1q-tunnel tpid 为非 0x8100 的值。

灵活 QINQ、vlan translation 以及 QINQ 对报文处理的优先级关系如下：灵活 QINQ>vlan translation>QINQ。

如果入口翻译不匹配，部分产品可能会出现对入口 tag 报文在外层再打一层 tag 的行为，所以当确定入口报文不匹配入口翻译表项时请取消 vlan-translation enable。

1.5 Super VLAN配置

1.5.1 Super VLAN简介

Super VLAN 技术（也称 VLAN 聚合）引入 super VLAN 和 sub VLAN 的概念。一个 super VLAN 可以包含一个或多个保持着不同广播域的 sub VLAN。Sub VLAN 不再占用一个独立的子网网段。在同一个 super VLAN 中，无论主机属于哪一个 sub VLAN，它的 IP 地址都在 super VLAN 对应的子网网段内。

在 LanSwitch 网络中，VLAN 技术以其对广播域的灵活控制（可跨物理设备）、部署方便而得到了广泛的应用。但是在一般的三层交换机中，通常是采用一个 VLAN 对应一个三层接口的方式来实现广播域之间的互通的，这在某些情况下导致了对 IP 地址的较大浪费。我们来看下面这个例子，设备内 VLAN 划分如下图所示。

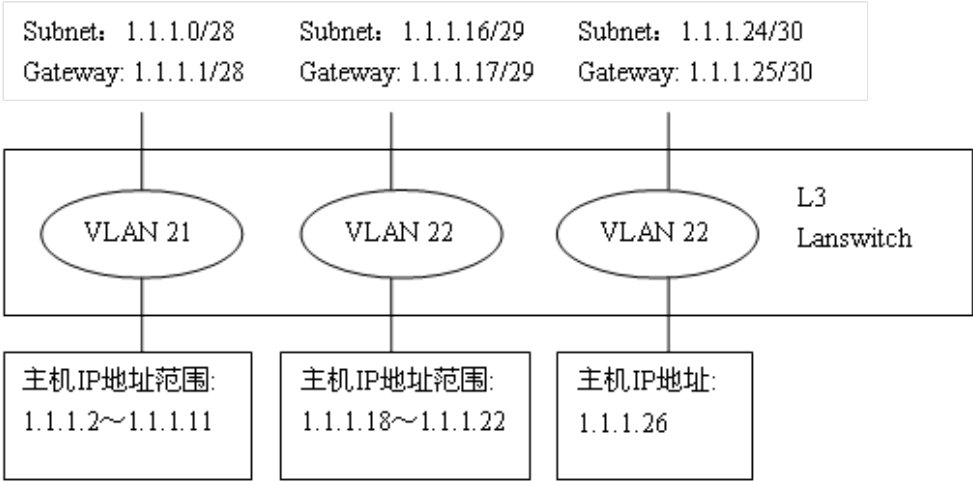


图 1-11 普通 VLAN 网络示意图

VLAN	IP Subnet	Gateway Address	Usable Hosts	Customer Hosts	Needed Hosts
21	1.1.1.0/28	1.1.1.1	14	13	10
22	1.1.1.16/29	1.1.1.17	6	5	5
23	1.1.1.24/30	1.1.1.25	2	1	1

表 1-1 普通 VLAN 主机地址划分示例

表 1-1 列出了地址的划分情况。VLAN 21 预计未来要有 10 个主机，给其分配一个掩码长 28 的子网——1.1.1.0/28。网段内子网号 1.1.1.0 和子网定向广播地址 1.1.1.15 不能用作主机地址，1.1.1.1 作为子网缺省网关地址也不可作为主机地址，剩下地址范围在 1.1.1.2～1.1.1.14 的主机地址可以被主机使用，这部分地址共有 13 个（ $2^{32-28}-3=13$ ）。这样，尽管 VLAN 21 只需要 10 个地址就可以满足需求了，但是按照子网划分却要分给它 13 个地址。

依此类推，VLAN 22 预计未来有 5 个主机地址需求，至少需要分配一个 29 位掩码的子网（1.1.1.16/29）才能满足要求。VLAN 23 只有 1 个主机，则占用子网 1.1.1.24/30。

这三个 VLAN 总共需要 $10+5+1=16$ 个地址，按照普通 VLAN 的编址方式，即使最优化的方案也需要占用 $2^{32-28}+2^{32-29}+2^{32-30}=28$ 个地址，地址浪费了将近一半。而且，如果 VLAN 21 后来并没有增长到 10 台主机，而只增长到了 3 台主机，本来分一个掩码长 29 的子网就够用了，但之前却分了一个子网掩码长 28 的子网给它，多出来的地址都因不能再被其他 VLAN 使用而被浪费掉了。

同时，这种划分也给后续的网络升级带来了很大不便。假设 VLAN23 所在的客户一段时间后需要增加 2 台主机，又不愿意改变已经分配的 IP 地址。在 1.1.1.24 后面的地址已经分配给了其他人的情况下，那没有办法，只能额外再给他分配一个的 29 位掩码的子网和一个新的 VLAN 给他。这样 VLAN23 的客户只有 3 台主机，却被迫分配了两个子网，不在同一个 VLAN，造成管理上的极大不便。

由此我们可以看出，被诸如子网号、子网定向广播地址、子网缺省网关地址消耗掉的 IP 地址数量是相当可观。同时，这种地址分配的固有约束也严重降低了编址的灵活性，使许多闲置地址被浪费。为了解决这一问题，Super VLAN 应运而生。

可见，Super VLAN 的好处是：减少子网号、子网缺省网关地址和子网定向广播地址的消耗，实现了不同广播域使用同一子网网段地址，增加编址的灵活性，减少了闲置地址浪费。

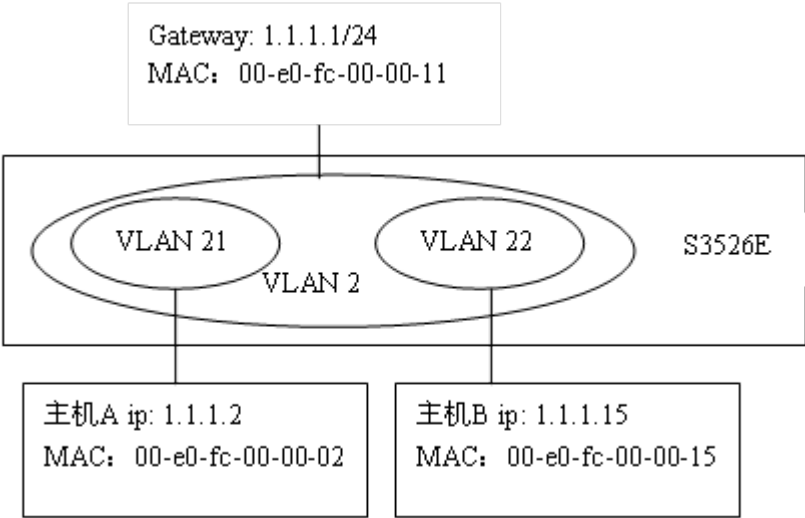


图 1-12 super vlan 功能示意图

- Super VLAN 不同于通常意义的 VLAN，Super VLAN 只是建立一个三层接口，不能包含任何端口，是一个三层的概念。
- Super VLAN 三层接口 UP：它所含 sub-VLAN 中存在 UP 状态的物理端口。

1.5.2 Super VLAN配置任务序列

1. 创建或删除 supervlan
2. 指定或删除 subvlan
3. 开启或关闭 subvlan 的 arp-proxy 功能
4. 指定或删除接口的 ip-addr-range
5. 指定或删除 subvlan 的 arp-check-range

1. 创建或删除 supervlan

命令	解释
VLAN 配置模式	
supervlan no supervlan	创建/删除 supervlan。

2. 指定或删除 subvlan

命令	解释
VLAN 配置模式	
subvlan WORD no subvlan {WORD all}	指定/删除 subvlan。

3. 开启或关闭 subvlan 的 arp-proxy 功能

命令	解释
----	----

接口配置模式	
arp-proxy subvlan {WORD all} no arp-proxy subvlan {WORD all}	开启/关闭 subvlan 的 arp-proxy 功能。

4. 指定或删除接口的 ip-addr-range

命令	解释
接口配置模式	
ip-addr-range <ipv4-addrss> to <ipv4-addrss> no ip-addr-range	指定/删除接口的地址范围。

5. 指定或删除 subvlan 的 arp-check-range

命令	解释
接口配置模式	
arp-check-range subvlan <vlan-id> <ipv4-addrss> to <ipv4-addrss> no -check-range subvlan <vlan-id>	指定/删除 subvlan 的地址范围。

1.5.3 Super VLAN典型应用

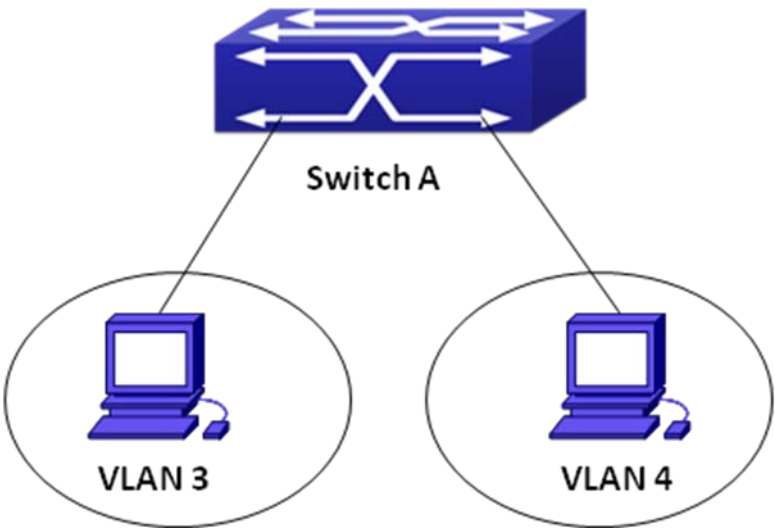


图 1-13 supervlan 典型应用拓扑图

由于局域网应用的需要，需要让两个 vlan 的终端配置为同一网段的地址，它们之间的二层流量要隔离，但是三层流量能正常转发。vlan3 用的地址范围为 1.1.1.1-10，vlan4 用的地址范围为 1.1.1.20-30，只有在这个地址范围内的终端的三层流量互通，而其他使用同网段地址的终端的三层流量不被转发。在交换机上设置 supervlan 可以实现这种需求。

配置项目	配置说明
------	------

VLAN2	Supervlan
VLAN3	A 交换机 1 端口
VLAN4	A 交换机 2 端口

配置步骤如下：

Switch A:

```
switch(Config)#vlan 2-4
switch(Config)#vlan 2
switch(Config-Vlan2)#supervlan
switch(Config-Vlan2)#subvlan 3;4
switch(Config-Vlan2)#exit
switch(Config)#interface vlan 2
switch(config-if-vlan2)#ip address 1.1.1.254 255.255.255.0
switch(config-if-vlan2)#arp-proxy subvlan all
switch(config-if-vlan2)#ip-addr-range subvlan 3 1.1.1.1 to 1.1.1.10
switch(config-if-vlan2)#ip-addr-range subvlan 4 1.1.1.20 to 1.1.1.30
switch(config-if-vlan2)#exit
```

1.5.4 Super VLAN排错帮助

- ☞ supervlan 功能与 VRRP、动态 VLAN、私有 VLAN、组播 VLAN 等功能互斥，不要同时使用。
- ☞ subvlan 的 arp-proxy 功能只对一个 subvlan 生效，配置 arp-proxy 的 VLAN 收到的流量可以向其他 VLAN 转发。当处于两个不同 subvlan 的设备互相发送流量通信时，请注意将两个 subvlan 的 arp-proxy 功能均开启。
- ☞ subvlan 上不能建立三层接口。
- ☞ 创建\删除 supervlan 时需要保证该 VLAN 没有三层接口，否则会报错。
- ☞ 当 supervlan 的接口上指定了接口的 IP 地址范围，未指定 subvlan 地址范围，则以接口上规定的地址范围为准；当接口和 subvlan 上都指定了 IP 地址范围时，按顺序先检查是否在 subvlan 地址范围内，然后再检查是否在接口地址范围内，通过上述两次检查后的数据包才可以进入后续处理环节。
- ☞ 设置 supervlan 或 subvlan 时必须是在存在的 VLAN 才可以设置。
- ☞ 将端口模式设置为 trunk 时，会自动将 supervlan 从 allow-vlan 中去除。

第2章 MAC地址表配置

2.1 MAC地址表介绍

MAC 地址表是标识目的 MAC 地址与交换机端口之间映射关系的表，其 MAC 地址分为静态 MAC 地址和动态 MAC 地址。静态 MAC 地址由用户配置，具有最高优先级（不能被动态 MAC 地址覆盖）且永久生效；动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址，与接收端口建立映射关系；然后根据目标 MAC 地址查询 MAC 地址表，如果命中相关表项，交换机将数据帧从相应端口转发；否则，交换机将数据帧在其所属广播域内广播。如果动态 MAC 地址长时间没有从转发数据帧中学习得到，交换机就将其从 MAC 地址表中删除。

对于 MAC 地址表的操作可分为两步：

1. MAC 地址的获取；
2. 根据 MAC 地址表转发或过滤。

2.1.1 MAC地址表的获取

MAC 地址表的获取可分为静态配置和动态学习。静态配置即由用户人为的建立 MAC 地址与端口的映射关系；动态学习即由交换机动态的发现 MAC 地址与端口的映射关系，并定期的更新 MAC 地址表。下面我们将重点介绍 MAC 地址表的动态学习过程。

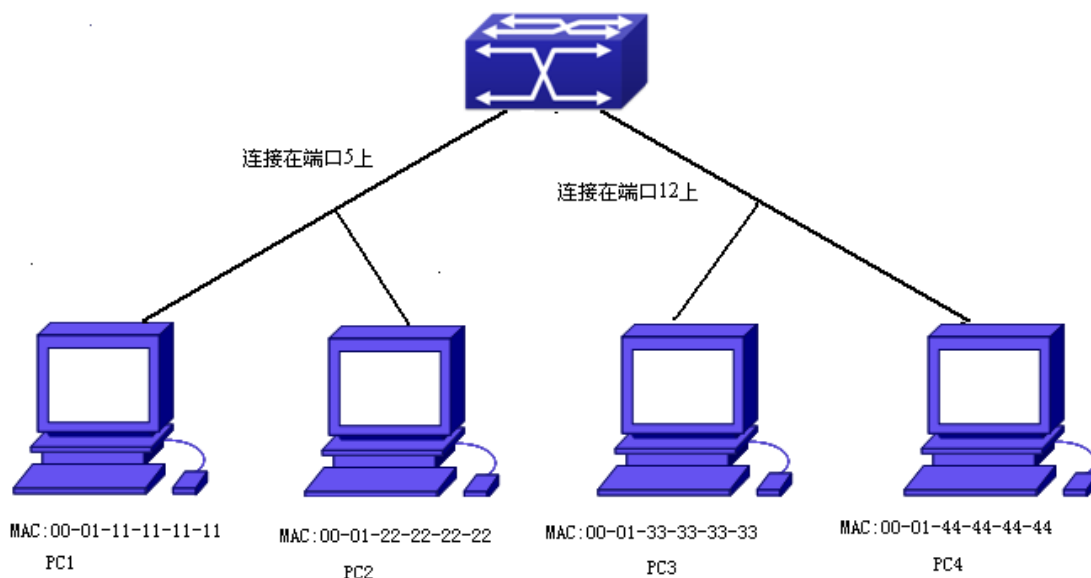


图 2-1 MAC地址表动态学习

上图的拓扑环境为：4 台主机连接在交换机上，其中主机 1、2 在同一个物理分段中（即相同的冲突域），该物理分段与交换机的端口 1/5 相连；主机 3、4 在同一个物理分段，该物理分段与交换机的端口 1/12 相连。

初始状态下MAC地址表中没有任何学习到的地址映射表项，以主机1和主机3的相互通信为例，MAC地址表的学习过程如下：

- 1. 当主机1向主机3传输信息时，交换机在端口1/5处收到该信息的源MAC地址00-01-11-11-11-11，交换机的MAC地址表中就会增加MAC地址00-01-11-11-11-11和端口1/5映射表项；
- 2. 同时交换机会检查到该信息的目标MAC地址00-01-33-33-33-33，此时交换机中只有MAC地址00-01-11-11-11-11和端口1/5的映射表项，没有00-01-33-33-33-33对应的端口映射，因此交换机只能将该信息广播给交换机的每个端口（假设交换机的所有端口都属于缺省VLAN）；
- 3. 位于端口1/12的主机3、4均收到主机1发出的信息，但主机4不会给主机1回应，因为目标MAC地址为00-01-33-33-33-33，只有主机3会给主机1回应。这时交换机的1/12号端口收到主机3的发出的信息，交换机的MAC地址表中就又增加了MAC地址00-01-33-33-33-33和端口1/12映射表项；
- 4. 目前MAC地址表的内容为MAC地址00-01-11-11-11-11动态对应着端口1/5，MAC地址00-01-33-33-33-33动态对应着端口1/12；
- 5. 经过一段时间的主机1和主机3的通信之后，交换机再也没有接收到从主机1和主机3发出的信息，300到2*300秒（即一到两倍的老化时间内）内交换机的MAC地址表将删除上面保存的MAC地址映射表项。这里的300秒是交换机缺省的MAC地址的老化时间，交换机提供老化时间的修改。

2.1.2 转发或过滤

交换机会根据MAC地址表对接收到的数据帧做出转发或过滤的决定。以上图为例，假设当前交换机 MAC地址表动态学习到了主机1和主机3的MAC地址，用户又手工配置了主机2和主机4与端口的映射关系。交换机的MAC地址表为：

MAC地址	端口号	获取方式
00-01-11-11-11-11	1/5	动态
00-01-22-22-22-22	1/5	静态
00-01-33-33-33-33	1/12	动态
00-01-44-44-44-44	1/12	静态

- 1. 根据MAC地址表转发的情况
如果主机1向主机3发送信息时，交换机根据MAC地址表，将从端口1/5接收到的数据从端口1/12发出。
- 2. 根据MAC地址表过滤的情况
如果主机1向主机2发送信息，交换机根据MAC地址表，检查到主机2和主机1在同一个物理分段中，交换机将对该信息进行过滤，即不发送帧信息。

另外交换机能转发三种类型的帧：

- ☞ 广播帧；
- ☞ 组播帧；
- ☞ 单播帧。

下面简单介绍交换机对三种帧的处理：

1. 广播帧：交换机能阻隔冲突域，但不能阻隔广播域，在没有设置VLAN的情况下连接在交换机的所有设备是处在同一个广播域中的，当交换机接收到广播帧时，它会向所有的端口转发该广播帧。当交换机设置了VLAN后，MAC地址表也会做相应的调整，会增加VLAN的信息，此时交换机接收到广播帧后，不会将该广播帧转发给交换机内的所有端口，而改变为只向属于同一个VLAN的所有端口转发。
2. 组播帧：对于未知组播，交换机会在同一个vlan内广播，如果交换机设置了IGMP Snooping功能或配置了静态组播组时，交换机只会向属于该组播组的端口转发该组播帧。
3. 单播帧：在没有设置VLAN的情况下，当交换机接收到的单播帧的目标MAC地址在MAC表中存在，交换机会直接将该单播帧转发到相应的端口；当接收到单播帧的目标MAC地址在MAC地址表中不存在时，交换机会对该单播帧进行广播。当交换机设置了VLAN，交换机只会同一VLAN内转发单播帧；当转发单播帧的目标MAC地址在MAC地址表中存在，但不属于同一VLAN，此时交换机只能将该单播帧在它属于的VLAN内进行广播。

2.2 MAC地址表配置

Mac 地址表的配置任务序列如下：

1. 配置 mac 地址老化时间，
2. 配置静态 mac 地址转发/过滤表项
3. 删除动态地址表项
4. 配置 MAC 软学习
5. 配置 hash 冲突表

1. 配置 MAC 地址老化时间

命令	解释
全局配置模式	
mac-address-table aging-time <0 aging-time> no mac-address-table aging-time	配置 mac 地址老化时间。

2. 配置静态 mac 地址转发/过滤表项

命令	解释
全局配置模式	

<pre> mac-address-table {static static-multicast blackhole} address <mac-addr> vlan <vlan-id> [interface [ethernet portchannel] <interface-name>] [source destination both] no mac-address-table {static static-multicast blackhole dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet portchannel] <interface-name>] </pre>	配置静态 mac 地址转发表项，配置静态组播 MAC 地址表项，配置地址过滤表项。
---	---

3. 删除动态地址表项

命令	解释
特权用户配置模式	
<pre> clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet portchannel] <interface-name>] </pre>	删除动态地址表项。

4. 配置 MAC 软学习

命令	解释
全局配置模式	
<pre> mac-address-learning cpu-control no mac-address-learning cpu-control </pre>	使能软件控制 mac 地址学习;no 命令恢复为硬件自动学习 mac 地址。

5. 配置 hash 冲突表

命令	解释
全局配置模式	
show collision-mac-address-table	打印 hash 冲突 mac 表。
特权用户配置模式	
clear collision-mac-address-table	清空 hash 冲突表。

2.3 典型配置举例

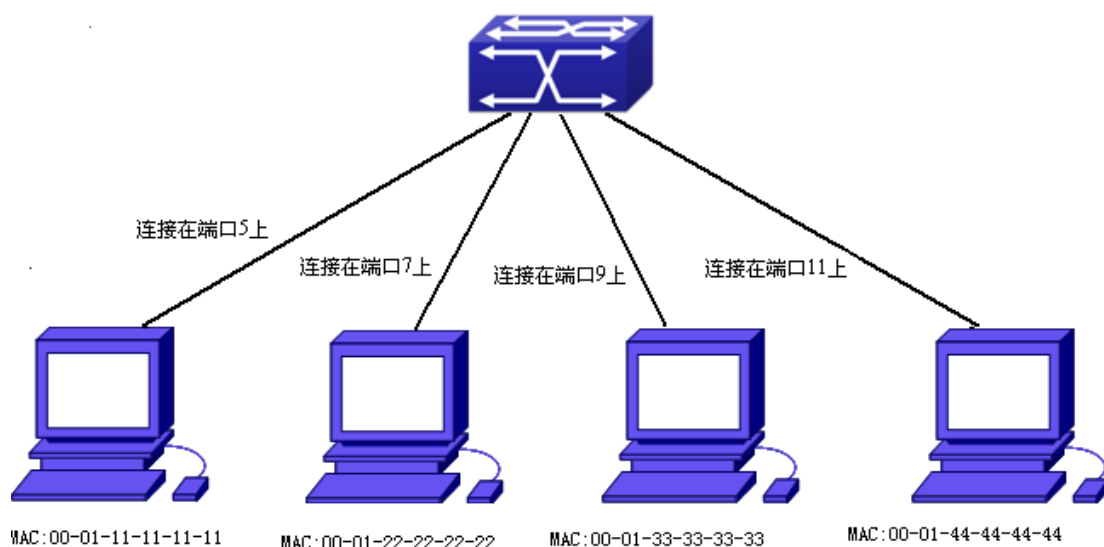


图 2-2 MAC 地址表典型配置举例

案例：

如上图所示四台主机分别连接在交换机的 1/5、1/7、1/9、1/11 端口，这四台主机都属于缺省 VLAN1。根据实际网络的需要，动态学习功能是打开的；主机 1（连接在端口 1/5）保存有机密资料，任何与它不在一个物理分段的主机不能访问它；主机 2（连接在端口 1/7）和主机 3（连接在端口 1/9）分别与端口 1/7 和端口 1/9 建立静态映射关系。

配置步骤如下：

1. 设置主机 1 的 MAC 地址 00-01-11-11-11-11 为过滤地址；

```
Switch(config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1
```

2. 主机 2 和主机 3 分别与端口 1/7 和端口 1/9 建立静态映射关系。

```
Switch(config)#mac-address-table static address 00-01-22-22-22-22 vlan 1 interface ethernet 1/7
```

```
Switch(config)#mac-address-table static address 00-01-33-33-33-33 vlan 1 interface ethernet 1/9
```

2.4 排错帮助

输入 `show mac-address-table` 命令时，发现某端口没有学习到该端口连接的设备的 MAC。可能的原因：

- ☞ 用于连接的以太网线损坏，更换以太网线；
- ☞ 交换机启动 **SpanningTree**，且端口处于 **discarding** 状态；或者端口刚连接上设备，**Spanning Tree** 还在计算中，等 **Spanning Tree** 计算完毕，端口就可以学习 MAC 地址

了；

☞ 若不是上述的问题时，请查看是否是端口损坏，若是请找技术支持解决。

2.5 MAC Notification配置

2.5.1 MAC Notification介绍

Mac notification 功能主要在于通知，mac 地址的新增或删除，就是当有 device 的加入或 device 移除时，通过 snmp 的 trap 功能通知网管发生的变化。

2.5.2 MAC Notification配置

Mac notification 配置任务序列如下：

1. 配置全局 snmp mac notification 功能
2. 配置全局 mac notification 功能
3. 配置全局发送 mac notification 通知的时间间隔
4. 配置 history table 的大小
5. 配置端口支持 mac notification 的 trap 类型
6. mac notification 配置情况和报文数据
7. 清除 mac notification trap 的计数值

1. 配置全局 snmp mac notification 功能

命令	解释
全局配置模式	
snmp-server enable traps mac-notification no snmp-server enable traps mac-notification	配置或取消 snmp 全局 mac notification 功能

2. 配置全局 mac notification 功能

命令	解释
全局配置模式	
mac-address-table notification no mac-address-table notification	配置或取消全局 mac notification 功能

3. 配置全局发送 mac notification 通知的时间间隔

命令	解释
全局配置模式	

mac-address-table notification interval <0-86400> no mac-address-table notification interval	配置 mac notification 的时间间隔或者恢复默认时间间隔
---	-------------------------------------

4. 配置 history table 的大小

命令	解释
全局配置模式	
mac-address-table notification history-size <0-500> no mac-address-table notification history-size	配置 history table 的大小或者恢复该 table 大小为默认值

5. 配置端口支持 mac notification 的 trap 类型

命令	解释
端口配置模式	
mac-notification {added both removed} no mac-notification	配置或取消端口支持 mac notification 的 trap 类型

6. 显示 mac notification 配置情况和报文数据

命令	解释
特权模式	
show mac-notification summary	显示 MAC 通知的配置情况和通知报文数据

7. 清除 mac notification trap 的计数值

命令	解释
特权模式	
clear mac-notification statistics	清除 mac notification trap 的计数值

2.5.3 MAC Notification 举例

管理站（NMS）的 IP 地址是 1.1.1.5；交换机（Agent）的 IP 地址是 1.1.1.9。

管理站要接收来自交换机的 Trap 消息(注:管理站可能设置了对 Trap 的团体字符串的验证,那么此例假设管理站的 Trap 验证团体字符串为 usertrap)。

配置步骤如下:

Switch(config)#snmp-server enable

```
Switch(config)#snmp-server enable traps mac-notification  
Switch(config)# mac-address-table notification  
Switch(config)# mac-address-table notification interval 5  
Switch(config)# mac-address-table notification history-size 100  
Switch(Config-If-Ethernet1/4)#mac-notification both
```

2.5.4 MAC Notification排错帮助

通过 show 和 snmp 部分的 debug 命令可以查看 trap 发送是否成功。