# 实验 3　VLAN 配 置

## 3.1　实验目标

(1) 掌握单交换机 VLAN 配置的方法。
(2) 掌握跨交换机 VLAN 配置的方法。
(3) 理解 trunk 的作用。

## 3.2　实验背景

假设有一位某公司新入职的网络管理员,员工对其投诉,称该公司网络中经常有大量的广播数据,挤占大量带宽,无法开展有效业务。经调研,该网络管理员发现该公司有管理、财务、销售等若干部门,每个部门有若干计算机,均接入同一交换机,并且网络上的所有用户都能监测到流经的业务,用户只要插入任一活动端口就可访问网段上的广播包。针对这个问题,应该如何提出一个有效的解决方案?

## 3.3　技术原理

### 3.3.1　VLAN 简介

虚拟局域网(virtual local area network,VLAN)是将局域网从逻辑上划分为一个个网段,从而实现虚拟工作组的一种交换技术。

使用交换机构成的一个物理局域网,整个网络属于同一个广播域,广播帧或多播帧(multicast frame)都将被广播到整个局域网中的每一台主机。在网络通信中,广播信息是普遍存在的,这些广播帧将占用大量的网络带宽,导致网络速度和通信效率的下降,并额外增加了网络主机为处理广播信息而产生的负荷。交换技术的发展,允许物理上分散的组织在逻辑上分成若干新的工作组,把一个大的广播域分割成多个小的广播域,这就是所谓的虚拟局域网技术(VLAN)。VLAN 之间的广播互不可达,VLAN 间互不影响,每个 VLAN 是一个独立的广播域。值得注意的是,VLAN 隔离了广播风暴,同时也隔离了各个不同的 VLAN 之间的通信,所以不同的 VLAN 之间的通信是需要有三层设备(如路由器、三层交换机)来完成的。

下面通过一个具体的案例分析在交换机上 VLAN 划分的作用。

在一台未设置任何 VLAN 的二层交换机上,任何广播帧都会被转发给除接收端口外的所有其他端口(flooding)。例如,如图 3.1 所示,计算机 A 发送广播信息后,会被转发给端口 2、3、4,并转发给与这些端口连接的主机 B、C、D。

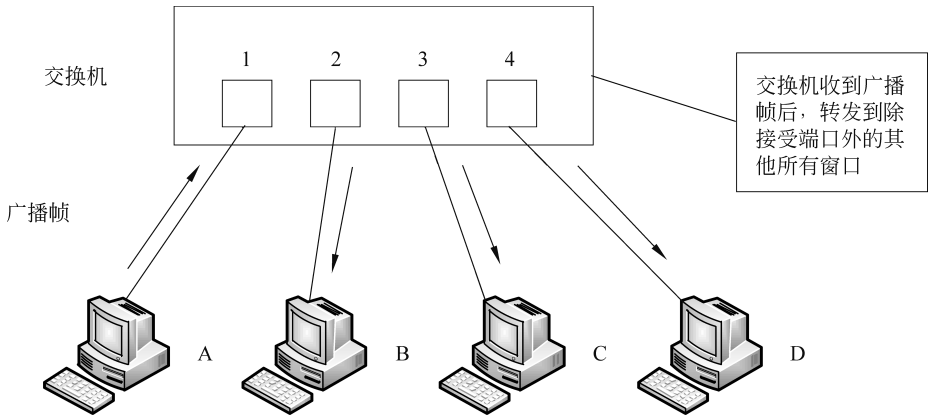



图 3.1　划分 VLAN 前

如果在交换机上生成两个 VLAN(10、20)，同时设置端口 1、2 属于 VLAN 10，端口 3、4 属于 VLAN 20(如图 3.2 所示)，若从 A 发出广播帧的话，交换机就只会把它转发给同属于一个 VLAN 的端口 2，不会转发给属于 VLAN 20 的端口。同样，C 发送广播信息时，只会被转发给属于 VLAN 20 的其他端口，不会被转发给属于 VLAN 10 的端口。

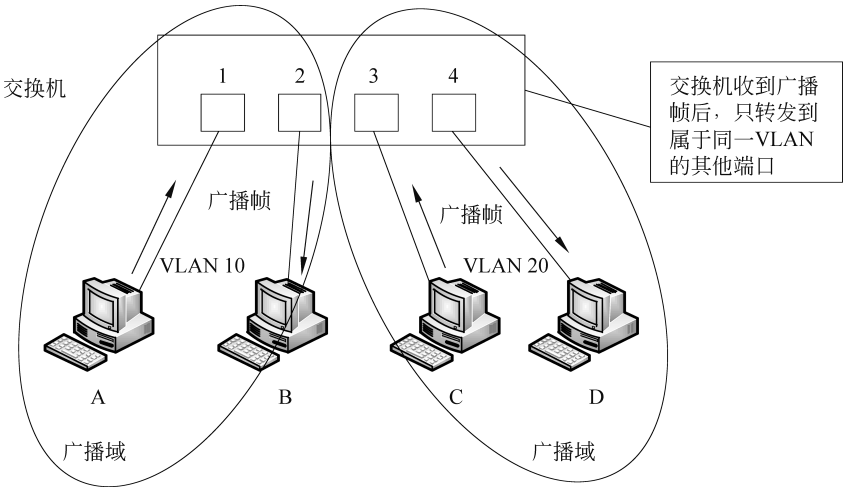



图 3.2　划分 VLAN 后

可见，VLAN 的本质是通过限制广播帧转发的范围来分割广播域的，用不同的广播域表示不同的 VLAN。不同的 VLAN 用不同的 VLAN ID 来区分。

通过以上分析可知，在交换机上划分不同的 VLAN 后，交换机端口必须能区分所接收的数据帧隶属于哪一个 VLAN，这就需要在普通的 MAC 帧上插入新的字段标签以区分不同的 VLAN，完成标签插入的代表协议有 IEEE 802.1q 和 ISL(inter switch link)。因为 ISL 是 Cisco 私有的协议，只能用于 Cisco 交换机的 VLAN 配置，所以下面仅分析 IEEE 802.1q 协议。

IEEE 802.1q 所附加的 VLAN 识别信息，位于以太网数据帧中“发送源 MAC 地址”与“类别域”(type field)之间(见图 3.3)。具体为 2 字节的 TPID(tag protocol identifier)和 2

字节的 TCI(tag control information),共计 4 字节。TPID 的值固定为 0x8100,它表示网络帧承载的 IEEE 802.1q 类型,交换机通过它来确定数据帧是否附加了基于 IEEE 802.1q 的 VLAN 信息。而关键的 VLAN ID,是 TCI 中的 12 位。由于总共有 12 位,因此最多可标识 4096 个 VLAN。这种基于 IEEE 802.1q 附加的 VLAN 信息,就像在传递物品时附加的标签。因此,它也被称作“标签型 VLAN”(tagging VLAN)。

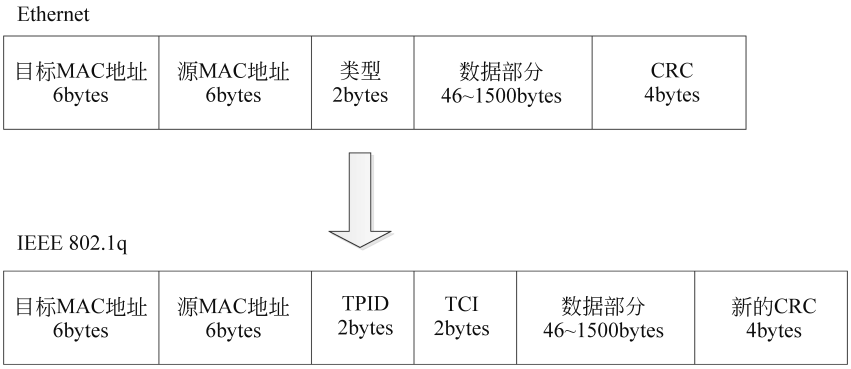



图 3.3　IEEE 802.1q 帧格式

因此,在引入 VLAN 技术后,以太网帧就可能有以下两种形式。

(1) 无标记帧(untagged 帧):原始的、未加入 4 字节 VLAN 标签的以太网帧。

(2) 有标记帧(tagged 帧):加入了 4 字节 VLAN 标签的帧,即图 3.3 中的 IEEE 802.1q 帧。

以太网链路包括接入链路(access link)和干道链路(trunk link)。接入链路用于连接交换机和用户(如用户主机、服务器等),只可以承载 1 个 VLAN 的数据帧。干道链路用于交换机间互连或连接交换机与路由器,可以承载多个不同 VLAN 的数据帧。在接入链路上传输的数据帧都是无标记帧,在干道链路上传输的数据帧都是有标记帧。

交换机内部处理的数据帧一律都是有标记帧。从用户终端接收无标记帧后,交换机会为无标记帧添加 VLAN 标签,重新计算帧检验序列(FCS),然后通过干道链路发送帧;向用户终端发送帧前,交换机会去除 VLAN 标签,并通过接入链路向终端发送无标记帧。

总结划分 VLAN 的作用如下。

(1) 控制网络的广播,增加广播域的数量,减小广播域的范围。

(2) 增强网络的安全性。在缺少路由的情况下,VLAN 之间不能直接通信,从而起到了隔离作用,并提高了 VLAN 中用户的安全性。VLAN 间的通信可通过应用访问控制列表,来实现 VLAN 间的安全通信。

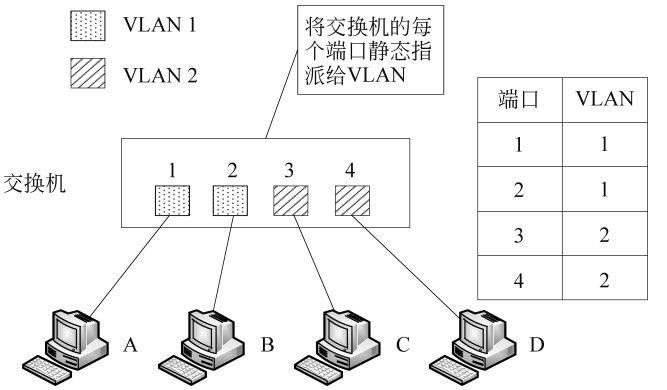
(3) 便于对网络进行管理和控制。

### 3.3.2　VLAN 划分方式

**1. 静态 VLAN——基于端口**

静态 VLAN 又被称为基于端口的 VLAN(port-based VLAN),就是明确指定交换机各端口属于哪个 VLAN。如图 3.4 所示,1、2 号端口指派给 VLAN 1,3、4 号端口指派给 VLAN 2,这样接入端口 1 和 2 的终端就属于同一个广播域,即同一个虚拟局域网,而接入

端口 3 和 4 的终端就属于另一个虚拟局域网。这种方式的优点是管理简单，缺点是由于需要一个个端口地指定，因此当网络中的计算机超过一定数量（比如数百台）后，设定操作就会变得复杂。并且，客户端每次变更所连端口，都必须同时更改该端口所属 VLAN 的设定，不适合需要频繁改变拓扑结构的网络。




| 端口 | VLAN |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |

图 3.4　基于端口的 VLAN

**2. 动态 VLAN**

动态 VLAN 是以终端设备来定义虚拟局域网，交换机端口因不同的接入终端改变所属的 VLAN。动态 VLAN 可以分为 3 类：基于 MAC 地址的 VLAN（MAC_based VLAN）、基于子网的 VLAN（subnet_based VLAN）、基于用户的 VLAN（user_based VLAN）。

（1）基于 MAC 地址的 VLAN，是通过查询并记录端口所连计算机上网卡的 MAC 地址来决定端口的所属的。假定有一个 MAC 地址 A 被交换机设定为属于 VLAN 10，那么不论这台 MAC 地址为 A 的计算机连在交换机哪个端口，该端口都会被划分到 VLAN 10 中去。这种基于 MAC 地址的 VLAN 缺点是在设定时必须调查所连接的所有计算机的 MAC 地址并加以记录。如果计算机变换了网卡，还需要更改设定。

（2）基于子网的 VLAN，是通过所连计算机的 IP 地址来决定端口所属 VLAN 的。即使计算机因为变换了网卡或是其他原因导致 MAC 地址改变，只要它的 IP 地址不变，就仍可以加入原先设定的 VLAN。

（3）基于用户的 VLAN，是根据交换机各端口所连的计算机上当前登录的用户的，来决定该端口属于哪个 VLAN。这里的用户识别信息，一般是计算机操作系统登录的用户，比如可以是 Windows 域中使用的用户名。这些用户名信息，属于 OSI 第四层以上的信息。

本实验主要学习基于端口的 VLAN 划分方法和步骤。

### 3.3.3　VLAN 设置命令格式

（1）在单台交换机上配置 VLAN 的基本步骤和主要命令如下。

① 创建 VLAN：

```
Switch (config)#vlan vlan-id
Switch (config)#name vlan-name
```

② 将端口加入 VLAN：

```
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan vlan-id
```

③ 检查的命令：

```
Switch#show vlan
```

(2) 跨交换机配置 VLAN 的基本步骤和主要命令如下。

① 在各交换机配置 VLAN；

② 将端口加入 VLAN；

③ 将交换机互联端口配置成 trunk 模式，建立 trunk 干线；

④ 检查。

其中配置 trunk 的基本步骤和主要命令如下。

① 进入接口配置命令模式；

② 选择封装类型（IEEE 802.1q 或 ISL），默认为 IEEE 802.1q：

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

③ 配置一个接口成为 trunk：

```
Switch(config-if)#switchport mode trunk
```

④ 配置 trunk 允许通过的 VLAN(默认允许全部)：

```
Switch(config-if)#switchport trunk allowed vlan all
```

⑤ 在接口下用 no shutdown 命令激活 trunk 进程：

```
Switch(config-if)#no shutdown
```

## 3.4　单交换机 VLAN 配置实验

### 3.4.1　实验准备

(1) 根据图 3.5 的拓扑图 1 所示完成网络电缆连接。

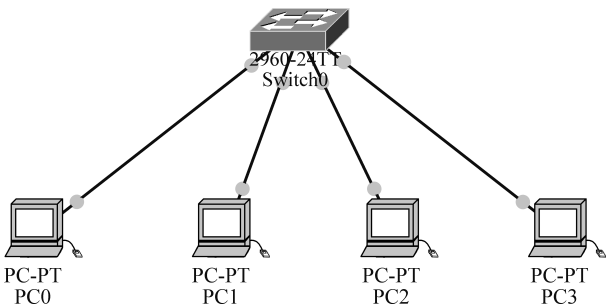



图 3.5　拓扑图 1

(2) 按表 3.1 完成终端设备的 IP 地址配置。以 PC0 为例,其 IP 地址配置如图 3.6 所示。

**表 3.1　接口地址分配表 1**

| 设备名称 | 接口 | IP 地址 | 子网掩码 | 默认网关 | 交换机端口 | VLAN |
|---|---|---|---|---|---|---|
| PC0 | 网卡 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | Fa0/1 | 10 |
| PC1 | 网卡 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | Fa0/2 | 10 |
| PC2 | 网卡 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 | Fa0/3 | 20 |
| PC3 | 网卡 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | Fa0/4 | 20 |

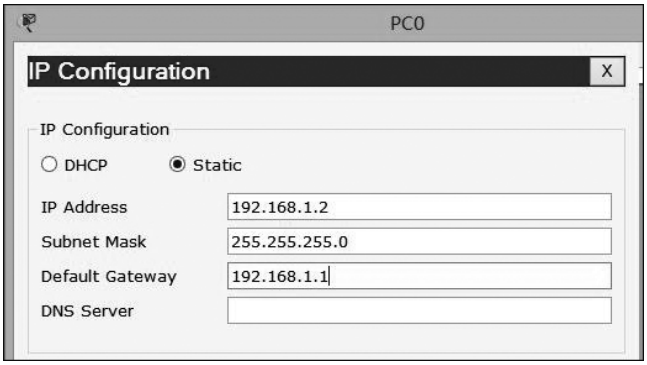



图 3.6　PC0 的 IP 地址配置

## 3.4.2　实验过程

**步骤 1**

(1) 配置交换机主机名为 S1,命令如下:

```
switch(config)#hostname s1
```

(2) 禁用 DNS 查找,命令如下:

```
s1(config)#no ip domain-lookup
```

**步骤 2**

(1) 在没有进行 VLAN 配置的情况下,使用 show vlan 命令查看 VLAN 情况,部分内容如图 3.7 所示。

从图 3.7 可知,在默认情况下,交换机已经创建了 VLAN 1,并且所有端口都属于 VLAN 1,所以默认情况下交换机的所有端口处于同一个广播域,也就是同一个局域网段。

(2) 在全局配置模式下使用 **vlan** vlan-id 命令将 VLAN 10 和 VLAN 20 添加到交换机 S1。并分别命名为 management 和 guest,命令如下:

```
s1(config)#vlan 10
//创建 VLAN,其 vlan-id 值为 10,并进入 VLAN 配置模式,no vlan 10 命令删除 vlan 10
s1(config-vlan)#name management  //将 VLAN 10 命名为 management
```

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

图 3.7　使用 show vlan 命令查看 VLAN 情况

```
s1(config-vlan)#exit
s1(config)#vlan 20
s1(config-vlan)#name guest
s1(config-vlan)#exit
```

(3) 在特权用户配置模式下使用 show vlan 命令检验在 S1 上创建的 VLAN，如图 3.8 所示。

```
s1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   management                        active
20   guest                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

图 3.8　在特权模式下使用 show vlan 命令

观察 show vlan 的结果，出现 default、management 和 guest 3 个 VLAN，其 ID 分别为 1、10 和 20，其中 default 的端口为交换机的所有端口，而 management 和 gues 目前没有端口。

请思考，这个现象说明了什么问题？

(4) 在端口配置命令模式下将交换机端口分配给 VLAN，命令如下：

```
s1(config)#interface range f0/1 - 2
//进入端口配置，使用 range 参数实现了多端口的配置
s1(config-if-range)#switchport mode access
```

```
//设置端口工作模式为 access,access 是交换机端口默认工作模式
s1(config-if-range)#switchport access vlan 10
//把 f0/1 - 2 端口加入 VLAN 10,no witchport access vlan 10 可以从 VLAN 10 删除端口
s1(config-if-range)#exit
s1(config)#interface range f0/3 - 4
s1(config-if-range)#switchport mode access
s1(config-if-range)#switchport access vlan 20
```

(5) 在特权用户配置模式下用 show vlan 命令检验在 S1 上已添加的端口。

问：哪些端口已经分配给 VLAN 10 ？

**步骤 3**

配置管理 VLAN。管理 VLAN 是配置用于访问交换机管理功能的 VLAN，默认将 VLAN 1 作为管理 VLAN。通过为管理 VLAN 分配 IP 地址和子网掩码，交换机可通过 HTTP、telnet、SSH 或 SNMP 进行管理。因为 Cisco 交换机的出厂配置将 VLAN 1 作为默认 VLAN，所以将 VLAN 1 用作管理 VLAN 不安全。在本实验中，将管理 VLAN 配置为 VLAN 99。IP 地址为 192.168.3.1，掩码为 255.255.255.0，命令如下：

```
s1(config)#interface vlan 99
//将 VLAN 99 看作一个接口进行配置
s1(config-if)#ip address 192.168.3.1 255.255.255.0
//配置 IP 地址和掩码,以后对该交换机可以采用本地址进行远程访问
s1(config-if)#no shutdown
//激活接口
```

**步骤 4**

(1) 打开 PC0 的命令行窗口，执行 ping 192.168.1.3 命令，观察结果。

(2) 打开 PC0 的命令行窗口，执行 ping 192.168.2.3 命令，观察结果。

根据观察到的现象，可以得到什么结论？

**步骤 5**

```
s1#write      //保存配置
```

## 3.5 跨交换机 VLAN 配置实验

在 VLAN 配置中，使用 switchport mode 命令来指定交换机端口(switchport)的工作模式，其工作模式主要有 access port 和 trunk port 两种(默认为 access)。如果一个 switch port 是 access 模式，则该接口只能为一个 VLAN 的成员，这种接口又称为 port VLAN；如果一个 switch port 是 trunk 模式，则该接口可以是多个 VLAN 的成员，这种配置被称为 tag VLAN。

为使跨越多台交换机的同一个 VLAN 的成员能够相互通信，交换机之间互联用的端口必须被设置为 trunk 模式，交换机之间可以传输多个 VLAN 的信息的那条线缆被称为干线(trunk)，干线又称主干。

### 3.5.1　实验准备

**步骤 1**

根据图 3.9 所示的拓扑图 2 完成网络电缆连接。

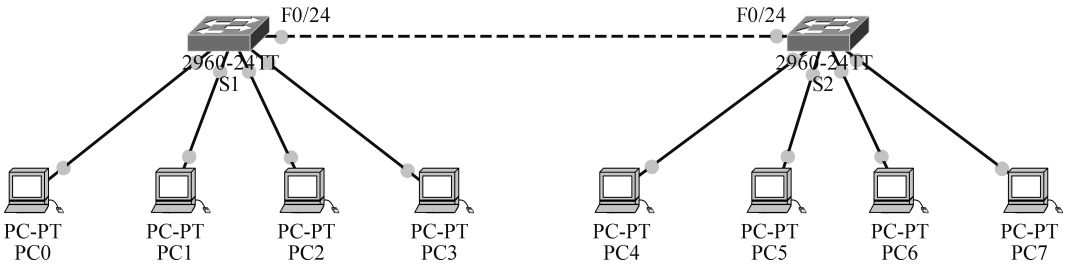



图 3.9　拓扑图 2

**步骤 2**

按表 3.2 完成终端设备的 IP 地址配置。

**表 3.2　接口地址分配表 2**

| 设备名称 | 交换机 | IP 地址 | 子网掩码 | 默认网关 | 交换机端口 | VLAN |
|---|---|---|---|---|---|---|
| PC0 | S1 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | F0/1 | 10 |
| PC1 | S1 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | F0/2 | 10 |
| PC2 | S1 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 | F0/3 | 20 |
| PC3 | S1 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | F0/4 | 20 |
| PC4 | S2 | 192.168.1.4 | 255.255.255.0 | 192.168.1.1 | F0/1 | 10 |
| PC5 | S2 | 192.168.1.5 | 255.255.255.0 | 192.168.1.1 | F0/2 | 10 |
| PC6 | S2 | 192.168.2.4 | 255.255.255.0 | 192.168.2.1 | F0/3 | 20 |
| PC7 | S2 | 192.168.2.5 | 255.255.255.0 | 192.168.2.1 | F0/4 | 20 |

### 3.5.2　实验过程

**步骤 1**

(1) 配置交换机主机名分别为 S1 和 S2。

(2) 在交换机 S1 完成 VLAN 10 和 VLAN 20 的配置，并将端口 F0/1、F0/2 移入 VLAN 10，将端口 F0/3、F0/4 移入 VLAN 20。

(3) 在交换机 S2 完成 VLAN 10 和 VLAN 20 的配置，并将端口 F0/1、F0/2 移入 VLAN 10，将端口 F0/3、F0/4 移入 VLAN 20。

**步骤 2**

(1) 配置交换机 S1，进入 F0/24 端口，设置该端口的工作模式为 trunk，并允许所有 VLAN 帧通过该端口，命令如下：

```
s1(config)#interface f0/24
```

```
S2(config)#shutdown
S2(config)#switchport trunk encapsulation dot1q
//使用 IEEE 802.1q 的帧格式封装端口所接收的数据帧

s1(config-if)#switchport mode trunk
//设置该交换机端口为 trunk 模式,trunk 链路在交换机之间起到了 VLAN 管道的作用,可以通过
//多个 VLAN 数据
s1(config-if)#switchport trunk allowed vlan 10,20
//设置 Trunk 端口允许通过的 VLAN,若用参数 all 则表示允许通过所有 VLAN
S1(config-if)#no shutdown
s1(config-if)#exit
s1#write
```

(2) 配置交换机 S2,进入 F0/24 端口,设置该端口的工作模式为 trunk,并允许所有 VLAN 帧通过该端口,命令如下:

```
S2(config)#interface f0/24
S2(config)#shutdown
S2(config)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan all
S2(config-if)#no shutdown
S2(config-if)#exit
S2#write
```

(3) 在交换机 S1 或者 S2 特权用户配置模式下输入 show interfaces trunk,请分析输出结果。

**步骤 3**

(1) 在终端 PC0 中打开命令行窗口输入命令 ping 192.168.1.4,观察其结果。

(2) 在终端 PC0 中打开命令行窗口输入命令 ping 192.168.2.4,观察其结果。

(3) 分析以上(1)、(2)步的操作,可以得到什么结论?