项目3

对企业各部门的网络 进行隔离及广播风暴控制

项目描述

公司网络经常因为有计算机中病毒而导致整个网络中有大量的广播数据存在,使得网络的正常使用受到一定的影响,为此公司决定为各个部门划分不同的 VLAN,减少广播风暴对整个网络的影响。

项目目标

- 理解 VLAN 的概念和作用;
- 理解 VLAN 的帧格式;
- 理解 VLAN 的端口类型;
- 掌握 VLAN 的创建方法;
- 掌握向 VLAN 中添加接口的方法;
- 掌握 VLAN 中 Trunk 端口的使用。

3.1 预备知识

在交换机的管理与配置中,VLAN 技术是一个必须要熟悉和掌握的技术。VLAN 技术 既是交换机配置与管理的重点,也是交换机管理与配置的难点。在交换机的管理与配置中, 关键是要理解 VLAN 的创建和端口类型的设置。

3.1.1 VLAN 概述

VLAN(Virtual Local Area Network,虚拟局域网)技术的出现主要是为了解决交换机 在进行局域网互连时无法限制广播的问题。VLAN 技术可以将一个局域网划分成多个逻 辑的而不是物理的网络,即 VLAN。VLAN 有着和普通物理网络同样的属性,除了没有物 理位置的限制,其他和普通局域网都相同。在同一个 VLAN 中的工作站,无论它们实际与 哪个交换机连接,它们之间的通信就好像在独立的交换机上一样,同一个 VLAN 中的广播 只有 VLAN 中的成员才能收到,而不会传输到其他的 VLAN 中去,这样可以很好地控制不 必要的广播风暴的产生。同时,若没有路由,不同 VLAN 之间不能相互通信,这样加强了企 业网络中不同部门之间的安全性。网络管理员可以通过配置 VLAN 之间的路由来全面管 理企业内部不同管理单元之间的信息互访。

3.1.2 VLAN 的作用

VLAN 的主要用途是缩小广播域,抑制广播风暴。在传统的共享介质的以太网和交换

式的以太网中,所有的用户在同一个广播域中,会引起网络性能的下降,浪费宝贵的带宽资源,而且广播对网络性能的影响随着广播域的增大而迅速增强。当网络中的用户达到一定的数量后,网络就会变得不可用,此时唯一的途径就是重新划分网络,把单一结构的大网划分成相互逻辑上独立的小网络。

每个 VLAN 是一个广播域,VLAN 内的主机间通信就和在一个局域网内一样,而 VLAN 间则不能直接互通,这样,广播报文被限制在一个 VLAN 内。VLAN 除了能将网络 划分为多个广播域,从而有效地控制广播风暴的发生,以及使网络的拓扑结构变得非常灵 活,还可以用于控制网络中不同部门、不同站点之间的互相访问,如图 3-1 所示。



3.1.3 VLAN 的划分

常用的 VLAN 的划分方法有以下 4 种。

1. 基于端口的划分

基于端口的 VLAN 划分就是根据以太网交换机的端口来划分。也就是说,交换机某些端口连接的主机在一个 VLAN 内,而另一些端口连接的主机在另一个 VLAN 中。VLAN 和端口连接的主机无关。这种划分方式的优点是定义 VLAN 的成员非常简单,只要指定交换机的端口即可,如果用户要更换 VLAN,只需要改变用户接入端口所处的 VLAN。基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法。基本上所有支持 VLAN 划分的交换机都支持基于端口的 VLAN 划分。

2. 基于 MAC 地址的划分

基于 MAC 地址的 VLAN 划分方法是根据连接在交换机上的主机的 MAC 地址来划分 的。也就是说,某个主机属于哪一个 VLAN 只和它的 MAC 地址有关。与它所连接的端口 和使用的 IP 地址无关。这种划分方式最大的优点是当用户改变接入端口时,不用重新配 置;缺点是初始的配置量很大,要知道每台主机的 MAC 地址并进行配置。

3. 基于协议的划分

基于协议的划分是指根据网络主机使用的网络协议来划分 VLAN。也就是说,主机属 于哪一个 VLAN 取决于主机所允许的网络协议(如 IP 和 IPX 协议),而与其他因素无关。 这种划分方式实际应用非常少,因为目前绝大多数是运行 IP 的主机,所以很难将 VLAN 划分的更小。

4. 基于子网的划分

基于子网的划分就是根据主机所用的 IP 地址所在的网络子网来划分。也就是说,IP 地址属于同一个子网的主机属于同一个 VLAN,而与主机的其他因素无关。这种划分方式 比较灵活,用户移动位置而不用重新配置主机或交换机,而且可以根据具体的应用来组织用 户。但也有不足的地方,如一个端口有可能存在多个 VLAN 用户,所以对广播报文起不到 抑制作用。用户也可以自己改变自己主机的 IP 地址所属的子网进入别的 VLAN,从而无 法控制用户的相互访问。

所以,从上面几种 VLAN 划分的方式来看,基于端口的 VLAN 划分是十分普遍的方法 之一,也是目前所有交换机都支持的一种 VLAN 划分方法。

3.1.4 VLAN 数据帧

为了保证不同厂商的设备能够顺序互通,IEEE 802.1q标准严格规定了统一的 VLAN 帧格式及其他重要参数。

IEEE 802.1q标准规定在原有的标准以太网帧格式中增加一个特殊的标准域——Tag 域,用于标识数据帧所属的 VLAN ID,其帧格式如图 3-2 所示。



图 3-2 以太网帧模式

Tag 域长度为4字节,其中各个标签的解释如下。

TPID:长度为2字节,协议标识字段,值为固定的0x8100,说明该帧具有 IEEE 802.1q 标签。

TCI:长度为2字节,控制信息字段,包括用户优先级、规范格式指示器和 VLAN ID。

Priority:长度为3个二进制位,用来指明帧的优先级,一共有8种优先级,主要用于当 交换机发生拥塞时,优先发送哪个数据包。

CFI:长度为1个二进制位,这一位主要用于总线型的以太网与FDDI、令牌环网交换数据时的帧格式。在以太网交换机中,规范格式指示器总被设置为0。

VLAN ID: 长度为 12 位,指明 VLAN 的 ID,每个支持 IEEE 802.1q 协议的主机发出 的数据包都会包含这个域,以指明自己属于哪一个 VLAN。该字段为 12 位,理论上支持

4096 个 VLAN 的识别。在这 4096 个 VLAN ID 中,0 被用于识别帧的优先级,4095 被预 留,所以最多有 4094 个,这也就是为什么在交换机上创建 VLAN 时 VLAN ID 范围是 1~ 4094 的原因。

3.1.5 VLAN 数据帧的传输

目前大部分主机不支持带有 Tag 域的以太网数据帧,即主机只接收和发送标准的以太 网数据帧,而会把带有 Tag 域的 VLAN 数据帧当作非法数据。所以支持 VLAN 的交换机 在与主机和交换机进行通信时,要区别对待,如图 3-3 所示。



图 3-3 VLAN 数据帧的传输

(1) 交换机从主机接收数据帧:由于主机处理的数据都是不带 VLAN 标签的,所 以这时交换机端口从主机上接收到的数据都是不带 VLAN 标签的,交换机会根据该端口 所属的默认 VLAN ID 给该数据帧打上相应的 VLAN 标签,然后发往交换机上其他的 端口。

(2) 交换机与交换机之间传输数据帧: 交换机与交换机之间传输的数据帧一般会被打 上 VLAN 标签。

(3)交换机发往主机的数据帧:由于主机不能处理带有 VLAN 标签的数据帧,因此当 交换机目的端口连接的是主机时,交换机在将数据帧发送给主机之前会先将数据帧中的 VLAN 标签删除,然后再发送数据帧。

注意:对于华为交换机默认 VLAN 被称为"Pvid Vlan",对于锐捷和思科交换机默认 VLAN 被称为"Native Vlan"。

3.1.6 VLAN 的端口类型

根据交换机处理数据帧的不同,交换机的端口可以分为三类: Access、Trunk 和 Hybrid。Access 类型的端口只能属于 1 个 VLAN,一般用于连接计算机的端口; Trunk 类 型的端口可以属于多个 VLAN,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 类型的端口可以属于多个 VLAN,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 的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签,而 Trunk 端口 只允许默认 VLAN 的报文发送时不打标签。

Access 端口只属于1个 VLAN,所以它的默认 VLAN 就是它所在的 VLAN,不用设

置; Hybrid 端口和 Trunk 端口属于多个 VLAN,所以需要设置默认 VLAN ID。默认情况下,Hybrid 端口和 Trunk 端口的默认 VLAN 为 VLAN 1。如果设置了端口的默认 VLAN ID,当端口接收到不带 VLAN Tag 的报文后,则将报文转发到属于默认 VLAN 的端口;当端口发送带有 VLAN Tag 的报文时,如果该报文的 VLAN ID 与端口默认的 VLAN ID 相同,则系统将去掉报文的 VLAN Tag,然后再发送该报文。

交换机各类 VLAN 端口对数据报文收发的处理如下。

Access 端口接收报文:收到一个报文,判断是否有 VLAN 信息标签。如果没有则打上端口的默认 VLAN ID 标签,并进行交换转发,如果有则直接丢弃(默认)。

Access 端口发送报文:将报文的 VLAN 信息标签剥离,直接发送出去。

Trunk 端口接收报文:收到一个报文,判断是否有 VLAN 信息标签。如果没有则打上端口的默认 VLAN ID 标签,并进行交换转发,如果有则判断该 Trunk 端口是否允许该 VLAN 的数据进入,如果可以则转发,否则丢弃。

Trunk 端口发送报文:比较端口的默认 VLAN ID 和将要发送报文的 VLAN 信息标签,如果两者相等则剥离 VLAN 信息标签,再发送,如果不相等则直接发送。

Hybrid 端口接收报文:收到一个报文,判断是否有 VLAN 信息标签。如果没有则打 上端口的默认 VLAN ID标签,并进行交换转发,如果有则判断该 Hybrid 端口是否允许该 VLAN 的数据进入,如果可以则转发,否则丢弃。

Hybrid 端口发送报文:判断该 VLAN 在本端口的属性(端口对哪些 VLAN 是 Untag, 对哪些 VLAN 是 Tag)。如果是 Untag 则剥离 VLAN 信息标签,再发送,如果是 Tag 则直接发送。

3.2 项目实施

任务一:给公司各个部门划分 VLAN

1. 任务描述

某公司有生产、销售、研发、人事、财务等多个部门,这些部门分别连接在两台交换机 (SW1和SW2)上,现要求给每个部门划分相应的VLAN,并分配相应的端口。生产部对应 的VLAN ID为100,销售部对应的VLAN ID为200,研发部对应的VLAN ID为300,人事 部对应的VLAN ID为400,财务部对应的VLAN ID为500,各个部门对应的端口分配如 表 3-1 所示。

部 门	交换机 1(SW1)端口号	交换机 2(SW2)端口号	VLAN ID
生产部	1,3,5,7,9	1~5	100
销售部	2,4,6,8,10	6~10	200
研发部	11~15	11~15	300
人事部	16,18~20	16	400
财务部	21~22	21~22	500

表 3-1 交换机端口分配表

2. 实验网络拓扑图

实验网络拓扑图如图 3-4 所示。



3. 设备配置(思科 Packet Tracer 模拟器)

1) 交换机 SW1 配置

Switch > enable

```
Switch # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # hostname SW1
SW1(config) # vlan 100
                                                   //创建 VLAN 100
                                                   //修改 VLAN 100 的名字为 shengchan
SW1(config-vlan) # name shengchan
SW1(config-vlan) # vlan 200
                                                   //创建 VLAN 200
SW1(config-vlan) # name xiaoshou
                                                   //修改 VLAN 200 的名字为 xiaoshou
SW1(config-vlan) # vlan 300
                                                   //创建 VLAN 300
SW1(config-vlan) # name yanfa
                                                   //修改 VLAN 300 的名字为 yanfa
SW1(config-vlan) # vlan 400
                                                   //创建 VLAN 400
SW1(config-vlan) # name renshi
                                                   //修改 VLAN 400 的名字为 renshi
SW1(config-vlan) # vlan 500
                                                   //创建 VLAN 500
SW1(config-vlan) # name caiwu
                                                   //修改 VLAN 500 的名字为 caiwu
SW1(config-vlan) # exit
SW1(config) #
SW1(config) # interface fastEthernet 0/1
                                                   //进入 F0/1 端口视图
                                                   //将 F0/1 端口加入 VLAN 100 中
SW1(config-if) # switchport access vlan 100
SW1(config-if) # exit
SW1(config) # interface range f0/3, f0/5, f0/7, f0/9
                                                   //同时进入 F0/3,5,7,9 端口
SW1(config-if-range) # switchport access vlan 100
                                                   //将 F0/3,5,7,9 端口一起加入 VLAN 100 中
SW1(config-if-range) # exit
SW1(config) # interface range f0/2, f0/4, f0/6, f0/8, f0/10
SW1(config-if-range) # switchport access vlan 200
                                                   //将 F0/2,4,6,8,10 端口一起加入 VLAN 200 中
```



SW1(config-if-range) # exit
SW1(config) # interface range f0/11-15
SW1(config-if-range) # switchport access vlan 300

SW1(config-if-range) # exit
SW1(config) # interface range f0/16,f0/18-20
SW1(config-if-range) # switchport access vlan 400

SW1(config-if-range) # exit
SW1(config) # interface range f0/21-22
SW1(config-if-range) # switchport access vlan 500

SW1(config-if-range) # exit
SW1(config) #

2) 交换机 SW2 配置

Switch > enable Switch # configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # hostname SW2 SW2(config) # vlan 100 SW2(config-vlan) # name shengchan SW2(config-vlan) # vlan 200 SW2(config-vlan) # name xiaoshou SW2(config-vlan) # vlan 300 SW2(config-vlan) # name yanfa SW2(config-vlan) # vlan 400 SW2(config-vlan) # name renshi SW2(config-vlan) # vlan 500 SW2(config-vlan) # name caiwu SW2(config-vlan) # exit SW2(config) # SW2(config) # interface range f0/1-5 SW2(config-if-range) # switchport access vlan 100 SW2(config-if-range) # exit SW2(config) # interface range f0/6-10 SW2(config-if-range) # switchport access vlan 200 SW2(config-if-range) # exit SW2(config) # interface range f0/11-15 SW2(config-if-range) # switchport access vlan 300 SW2(config-if-range) # exit SW2(config) # interface f0/16 SW2(config-if) # switchport access vlan 400 SW2(config-if) # exit SW2(config) # interface range f0/21-22 SW2(config-if-range) # switchport access vlan 500 SW2(config-if-range) # exit SW2(config) #

//同时进入 F0/11~F0/15 端口

//将 F0/11~F0/15 端口一起加入 VLAN 300 中

//同时进入 F0/16,18,19,20 端口

//将 F0/16, 18, 19, 20 端口一起加入 VLAN 400 中

//同时进入 F0/21,22 端口

//将 F0/21,22 端口一起加入 VLAN 500 中

```
    4. 思科相关命令介绍
    1) 创建 VLAN
    视图:全局配置视图/VLAN 配置视图。
    命令:
```

Switch(config) # vlan vlan-id
Switch(config) # no vlan vlan-id

参数:

vlan-id: VLAN 的编号,一般的范围是 1~4094。

说明:当输入的 vlan-id 号不存在时,该命令用来创建 vlan-id 号所对应的 VLAN;当输入的 vlan-id 号已经存在时,该命令则是进入 VLAN 配置视图的导航命令。no 选项可以用来删除 vlan-id 号对应的 VLAN。注意,VLAN 1 是默认存在的且不能被删除。

例如,创建 vlan-id 为 10 的 VLAN。

SW1(config) # vlan 10 SW1(config-vlan) #

2) 设置 VLAN 的名称

视图: VLAN 配置视图。

命令:

```
Switch(config-vlan) # name vlan-name
Switch(config-vlan) # no name
```

参数:

vlan-name: vlan 的名称。

说明:该命令用于给相应的 VLAN 设置名称,便于管理维护和识别。VLAN 默认的名称为 VLAN XXXX,其中,XXXX 是由 0 开头的 4 位 VLAN ID 号。例如,VLAN 10 的默认名称为 VLAN 0010。该命令可以通过 no 选项来恢复 VLAN 的默认名字。

例如,设置 VLAN 10 的名称为 keyan。

SW1(config) # vlan 10 SW1(config-vlan) # name keyan

3) 进入一组快速以太网端口视图

视图:全局配置视图。

命令:

Switch(config) # interface range fastEthernet { mod-num/port-num | , mod-num/port-num-port-num}

参数:

mod-num:模块号,范围由设备和扩展模块决定。

port-num:模块上的端口号。

说明:该命令可以同时进入一组以太网的端口视图,主要用于对多个端口同时配置相同参数的情况。根据多个端口的不同组成情况,命令后面的参数可以有以下几种表示方式。

54

• 端口组成为多个不连续的端口,如端口1,3,5组成一组时,命令描述如下。

interface range fastEthernet 0/1, fastEthernet 0/3, fastEthernet 0/5

也可以简写为:

inte range f0/1, f0/3, f0/5

 端口组成为多个连续的端口,如端口 11,12,13,14,15,16,17,18 组成一组时,命令 描述如下。

interface range fastEthernet 0/11-18

也可以简写为:

```
inte range f0/11-18
```

端口组成既有不连续的,也有连续的,如端口11,端口15,16,17组成一组时,命令描述如下。

interface range fastEthernet 0/11, fastEthernet 0/15-17

也可以简写为:

inte range f0/11, f0/15-17

```
4) 将端口添加到 VLAN 中
```

```
视图:接口配置视图。
```

命令:

Switch(config-if) # switchport access vlan vlan-id Switch(config-if) # no switchport access vlan

参数:

vlan-id: VLAN 的编号,一般的范围是 1~4094。

说明:该命令用来将接口添加到对应的 VLAN 中去,该命令需要在所添加的接口视图 下执行。例如,若要将交换机的端口 5 添加到 VLAN 10 中,就先要用 interface 命令进入端 口 5 的接口视图,然后在该视图下执行该命令。在执行该命令时,如果命令中所输入的 vlan-id 号不存在,则会自动创建该 VLAN,然后将端口添加进该 VLAN;如果命令中输入 的 vlan-id 号已经存在,则直接将端口添加进该 VLAN。华为的设备中要将端口添加到 VLAN 中时,可以用两种方式实现,第一种方式跟锐捷的相似,先进入端口视图,然后将端 口添加到 VLAN 中; 另外一种方式是在 VLAN 配置视图下,将需要添加的端口加进来。 具体命令见拓展知识部分华为命令。该命令的 no 选项可以使该端口从指定的 VLAN 中删 除,回到默认的 VLAN(VLAN 1)中。

例如,将端口10添加到VLAN 20中去。

```
SW1(config) # interface f0/10
SW1(config-if) # switchport access vlan 20
```

5) 查看 VLAN 配置信息 视图:系统视图。 命令:

Switch # show vlan [id vlan-id]

参数:

vlan-id: VLAN 的编号,一般的范围是 1~4094。

说明:该命令用来查看 VLAN 的配置信息。通过该命令可以了解 VLAN 的编号、名称、状态和 VLAN 中所包含的端口号。

例如:查看所有 VLAN 的配置信息。

SW1 # show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/17, Fa0/23, Fa0/24, Gig1/1 Gig1/2
100	shengchan	active	Fa0/1, Fa0/3, Fa0/5, Fa0/7 Fa0/9
200	xiaoshou	active	Fa0/2, Fa0/4, Fa0/6, Fa0/8 Fa0/10
300	yanfa	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15
400 500	renshi caiwu	active active	Fa0/16, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22

例如,查看 VLAN 100 的配置信息。

SW1 \ddagger show vlan id 100

VLAN	Name	Status	Ports
100	shengchan	active	Fa0/1, Fa0/3, Fa0/5, Fa0/7
			Fa0/9



5. 设备配置(华为 eNSP 模拟器)

设备配置如图 3-5 所示。 1) 交换机 SW1 配置

< Huawei > sys Enter system view, return user view with Ctrl + Z. [Huawei]sysname SW1 [SW1]vlan 100 //创建 VLAN 100 [SW1-vlan100]description shengchan //设置 VLAN 100 的说明 [SW1-vlan100]vlan 200 //创建 VLAN 200 [SW1-vlan200]description xiaoshou //设置 VLAN 200 的说明 [SW1-vlan200]vlan 300 [SW1-vlan300]description yanfa [SW1-vlan300]vlan 400 [SW1-vlan400]description renshi [SW1-vlan400]vlan 500

56



< Huawei > sys

Enter system view, return user view with Ctrl + Z. [Huawei]sysname SW2 //创建 VLAN 100 [SW2]vlan 100 [SW2-vlan100]description shengchan //设置 VLAN 100 的说明 [SW2-vlan100]vlan 200 //创建 VLAN 200 [SW2-vlan200]description xiaoshou //设置 VLAN 200 的说明 [SW2-vlan200]vlan 300 [SW2-vlan300]description yanfa [SW2-vlan300]vlan 400 [SW2-vlan400]description renshi [SW2-vlan400]vlan 500 [SW2-vlan500]description caiwu [SW2-vlan500]quit [SW2]port-group 1 [SW2-port-group-1]group-member g0/0/1 to g0/0/5 [SW2-port-group-1]port link-type access [SW2-port-group-1]port default vlan 100 [SW2-port-group-1]guit [SW2]port-group 2 [SW2-port-group-2]group-member g0/0/6 to g0/0/10 [SW2-port-group-2]port link-type access [SW2-port-group-2]port default vlan 200 [SW2-port-group-2]quit [SW2]port-group 3 [SW2-port-group-3]group-member g0/0/11 to g0/0/15 [SW2-port-group-3]port link-type access [SW2-port-group-3]port default vlan 300 [SW2-port-group-3]quit [SW2]interface q0/0/16 [SW2-GigabitEthernet0/0/16]port link-type access [SW2-GigabitEthernet0/0/16]port default vlan 400 [SW2-GigabitEthernet0/0/16]guit [SW2]port-group 5 [SW2-port-group-5]group-member g0/0/21 to g0/0/22 [SW2-port-group-5]port link-type access [SW2-port-group-5]port default vlan 500 [SW2-port-group-5]guit

6. 华为相关命令说明

1) 创建 VLAN
 视图:系统视图。
 命令:

[Huawei]**vlan** vlan-id

或者

[Huawei]vlan batch { vlan-id 1 [to vlan-id 2] } & <1-10>

参数:

vlan-id,*vlan-id*1,*vlan-id*2为 VLAN 的编号,整数形式,取值范围为 1~4094。华为 交换机可以使用参数 batch 批量创建 VLAN。

例如,创建连续的 VLAN 10,11,12,13,14,15。

[SW1]vlan batch 10 to 15

例如,创建不连续的 VLAN 100,200,300,400,500。

[SW1]vlan batch 100 200 300 400 500

2) 将端口划分到 VLAN

视图:接口视图。

指定端口类型的命令:

[Huawei-GigabitEthernet0/0/1]port link-type { access | hybrid | trunk }

指定 Access 端口的默认 VLAN 命令:

[Huawei-GigabitEthernet0/0/1] port default vlan vlan-id

华为交换机中要将一个端口加入的某个 VLAN 时,是先设置该端口 link-type 为 Access 类型(华为交换机端口默认是 Hybrid 类型),然后设置 default vlan 的方式来完成的。

例如,将端口 g0/0/1 加入到 VLAN 100 中去。

[SW1]interface g0/0/1 [SW1-GigabitEthernet0/0/1]port link-type access [SW1-GigabitEthernet0/0/1]port default vlan 100

3) 创建端口组
 视图:系统视图。
 创建端口组的命令:

[Huawei]port-group n

参数:

n为端口组编号,取值范围为1~32。

4) 端口组中添加成员

视图:端口组视图。

端口组添加成员端口命令:

[Huawei-port-group-1]group-member interface 1 to interface 2

参数:

interface1: 起始接口编号。

interface2:结束接口编号。

华为交换机要将一组端口同时加入到某个 VLAN 中时,是采用端口组的方式,先创建端口组,然后把相应的端口加入端口组,最后设置端口组的类型和 VLAN。

例如,将端口 g0/0/1 到 g/0/0/5 加入到 VLAN 100。

[SW1]port-group 1

//创建端口组,编号为1

[SW1-port-group-1]group-member g0/0/1 to g0/0/5//添加端口组成员[SW1-port-group-1]port link-type access//设置端口组类型为 Access[SW1-port-group-1]port default vlan 100//设置端口组默认 VLAN 为 100

例如,将端口g/0/1,g/0/3,g/0/5加入到 VLAN 100。

[SW1]port-group 1 [SW1-port-group-1]group-member g0/0/1 g/0/3 g0/0/5 [SW1-port-group-1]port link-type access [SW1-port-group-1]port default vlan 100

注意:当将一个端口从端口组中删除时,该端口上还是会保留端口组配置的链接类型和 VLAN 信息。

任务二:同一部门用户跨交换机的访问控制

1. 任务描述

公司在给各个部门划分 VLAN 后,分别连接在两台交换机(SW1 和 SW2,两交换机通 过 F0/24 端口连接)上的同一部门的用户无法进行通信了,现要求连接在两台交换机上的 研发、人事、财务三个部门的用户能各自相互访问,生产和销售两个部门隔离两个交换机之 间的用户访问。各部门的 VLAN 划分和端口分配如表 3-2 所示。

部 门	交换机 1(SW1)端口号	交换机 2(SW2)端口号	VLAN ID
生产部	1,3,5,7,9	1~5	100
销售部	2,4,6,8,10	6~10	200
研发部	11~15	11~15	300
人事部	16,18~20	16	400
财务部	21~22	21~22	500

表 3-2 各部门的 VLAN ID 和交换机端口分配表



2. 实验网络拓扑图

实验网络拓扑图如图 3-6 所示。

3. 设备配置(思科 PT 模拟器)

1) 交换机 SW1 配置

Switch > enable

Switch # configure terminal

Enter configuration commands, one per line. End with $\ensuremath{\texttt{CNTL}/\texttt{Z}}.$

Switch(config) # hostname SW1

- SW1(config) # vlan 100
- SW1(config-vlan) # name shengchan
- SW1(config-vlan) # vlan 200
- SW1(config-vlan) # name xiaoshou
- SW1(config-vlan) # vlan 300
- SW1(config-vlan) # name yanfa
- SW1(config-vlan) # vlan 400
- SW1(config-vlan) # name renshi
- SW1(config-vlan) # vlan 500





2) 交换机 SW2 配置

Switch > enable

Switch # configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # hostname SW2 SW2(config) # vlan 100 SW2(config-vlan) # name shengchan SW2(config-vlan) # vlan 200 SW2(config-vlan) # name xiaoshou SW2(config-vlan) # vlan 300 SW2(config-vlan) # name yanfa SW2(config-vlan) # vlan 400 SW2(config-vlan) # name renshi SW2(config-vlan) # vlan 500 SW2(config-vlan) # name caiwu SW2(config-vlan) # exit SW2(config) # SW2(config) # interface range f0/1-5 SW2(config-if-range) # switchport access vlan 100 SW2(config-if-range) # exit SW2(config) # interface range f0/6-10 SW2(config-if-range) # switchport access vlan 200 SW2(config-if-range) # exit SW2(config) # interface range f0/11-15 SW2(config-if-range) # switchport access vlan 300 SW2(config-if-range) # exit SW2(config) # interface f0/16 SW2(config-if) # switchport access vlan 400 SW2(config-if) # exit SW2(config) # interface range f0/21-22 SW2(config-if-range) # switchport access vlan 500 SW2(config-if-range) # exit SW2(config) # //配置交换机之间的连接端口 SW2(config) # interface f0/24 SW2(config-if) # switchport mode trunk SW2(config-if) # switchport trunk allowed vlan remove 100 SW2(config-if) # switchport trunk allowed vlan remove 200 SW2(config-if) # exit

4. 思科相关命令介绍

参数.

设置 VLAN 端口的类型
 视图:接口视图。
 命令:
 Switch(config-if) # switchport mode { access | trunk | hybrid }
 Switch(config-if) # no switchport mode

access:设置端口为 Access 端口; trunk:设置端口为 Trunk 端口; hybrid:设置端口为 Hybrid 端口。

说明:该命令用来设置交换机接口在 VLAN 中的端口类型,交换机所有的端口默认都 是 Access 端口。Access 端口只能属于一个 VLAN,当需要端口属于多个 VLAN 时,需要 将端口设置成 Trunk 端口或 Hybrid 端口。

例如,将端口 F0/24 设置为 Trunk 端口

SW2(config) # interface f0/24 SW2(config-if) # switchport mode trunk

2) 设置 Trunk 端口的许可 VLAN 列表
 视图:接口视图。
 命令:

Switch(config-if) # switchport trunk {allowed vlan { all | [add | remove | except] vlan-list }
Switch(config-if) # no switchport trunk {allowed vlan }

参数:

allowed vlan vlan-list: 配置这个 Trunk 端口的许可 VLAN 列表。参数 vlan-list 可以 是一个 VLAN,也可以是一系列 VLAN,以小的 VLAN ID 开头,以大的 VLAN ID 结尾,中 间用"-"符号连接。如 10-20。段之间可以用","符号隔开,如 1-10,20-25,30,33。

all: 表示许可 VLAN 列表包含所有支持的 VLAN;

add: 表示将指定 VLAN 列表加入许可 VLAN 列表;

remove: 表示将指定 VLAN 列表从许可 VLAN 列表中删除;

except: 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表。

说明:在思科的交换机上,Trunk端口默认情况下是允许所有的 VLAN 的数据通过的。可以通过该命令来改变 Trunk端口允许通过的 VLAN 列表。该命令同样可以用 no 选项来恢复 Trunk端口的默认许可的 VLAN 列表。

例如,允许所有的 VLAN 通过 Trunk 端口。

SW2(config) # interface f0/24 SW2(config-if) # switchport mode trunk SW2(config-if) # switchport trunk allowed vlan all

例如,将 VLAN 10 和 VLAN 20 从 Trunk 端口的 VLAN 许可列表中删除。

SW2(config-if) # switchport trunk allowed vlan remove 10,20

例如,将 VLAN 30 加入到 Trunk 端口的 VLAN 许可列表中。

SW2(config-if) # switchport trunk allowed vlan add 30

3) 设置 Trunk 端口的默认 VLAN
 视图:接口视图。
 命令:

Switch(config-if) # switchport trunk native vlan vlan-id Switch(config-if) # no switchport trunk native vlan

参数:

native vlan vlan-id : 默认 VLAN ID。

说明:该命令是用来设置 Trunk 端口的默认 VLAN,每个端口都有一个默认 VLAN, 端口在接收不打 Tag 标签的数据帧时,都会当作默认 VLAN 的数据帧,在转发到其他接口 去时,会给数据帧打上默认 VLAN 的 Tag 标签。同样在 Trunk 端口发送带有默认 VLAN 的 Tag 标签的数据帧时,会把 Tag 标签去除。所有端口的默认 VLAN 都是 VLAN 1。 Access 类型的端口因为只能属于一个 VLAN,所有端口当前所属的 VLAN 即为默认 VLAN。而 Trunk 端口和 Hybrid 端口都可以同时属于多个 VLAN,所以可以通过相应的 命令来设置端口的默认 VLAN。

例如,设置 Trunk 端口的默认 VLAN 为 VLAN 20。

```
SW2(config) # interface f0/24
SW2(config-if) # switchport mode trunk
SW2(config-if) # switchport trunk native vlan 20
```

5. 设备配置(华为 eNSP 模拟器)

设备配置如图 3-7 所示。





1) 交换机 SW1 配置

< Huawei > sys Enter system view, return user view with Ctrl + Z. [Huawei]sysname SW1 [SW1]vlan 100 [SW1-vlan100]description shengchan [SW1-vlan100]vlan 200 [SW1-vlan200]description xiaoshou

64

[SW1-vlan200]vlan 300 [SW1-vlan300]description yanfa [SW1-vlan300]vlan 400 [SW1-vlan400]description renshi [SW1-vlan400]vlan 500 [SW1-vlan500]description caiwu [SW1-vlan500]quit [SW1]port-group 1 [SW1-port-group-1]group-member g0/0/1 g0/0/3 g0/0/5 g0/0/7 g0/0/9 [SW1-port-group-1]port link-type access [SW1-port-group-1]port default vlan 100 [SW1-port-group-1]quit [SW1]port-group 2 [SW1-port-group-2]group-member g0/0/2 g0/0/4 g0/0/6 g0/0/8 g0/0/10 [SW1-port-group-2]port link-type access [SW1-port-group-2]port default vlan 200 [SW1-port-group-2]quit [SW1]port-group 3 [SW1-port-group-3]group-member g0/0/11 to g0/0/15 [SW1-port-group-3]port link-type access [SW1-port-group-3]port default vlan 300 [SW1-port-group-3]quit [SW1]port-group 4 [SW1-port-group-4]group-member g0/0/16 g0/0/18 to g0/0/20[SW1-port-group-4]port link-type access [SW1-port-group-4]port default vlan 400 [SW1-port-group-4]quit [SW1]port-group 5 [SW1-port-group-5]group-member g0/0/21 to g0/0/22[SW1-port-group-5]port link-type access [SW1-port-group-5]port default vlan 500 [SW1-port-group-5]guit //配置交换机之间的连接端口 [SW1]interface g0/0/24 [SW1-GigabitEthernet0/0/24]port link-type trunk [SW1-GigabitEthernet0/0/24]port trunk allow-pass vlan 300 400 500

2) 交换机 SW2 配置

< Huawei > sys Enter system view, return user view with Ctrl + Z. [Huawei]sysname SW2 [SW2]vlan 100 [SW2-vlan100]description shengchan [SW2-vlan100]vlan 200 [SW2-vlan200]description xiaoshou [SW2-vlan200]vlan 300 [SW2-vlan300]description yanfa [SW2-vlan300]vlan 400 [SW2-vlan400]vlan 400

[SW2-vlan500]description caiwu [SW2-vlan500]guit [SW2]port-group 1 [SW2-port-group-1]group-member q0/0/1 to q0/0/5[SW2-port-group-1]port link-type access [SW2-port-group-1]port default vlan 100 [SW2-port-group-1]quit [SW2]port-group 2 [SW2-port-group-2]group-member g0/0/6 to g0/0/10 [SW2-port-group-2]port link-type access [SW2-port-group-2]port default vlan 200 [SW2-port-group-2]guit [SW2]port-group 3 [SW2-port-group-3]group-member g0/0/11 to g0/0/15 [SW2-port-group-3]port link-type access [SW2-port-group-3]port default vlan 300 [SW2-port-group-3]quit [SW2]interface g0/0/16 [SW2-GigabitEthernet0/0/16]port link-type access [SW2-GigabitEthernet0/0/16]port default vlan 400 [SW2-GigabitEthernet0/0/16]guit [SW2]port-group 5 [SW2-port-group-5]group-member g0/0/21 to g0/0/22 [SW2-port-group-5]port link-type access [SW2-port-group-5]port default vlan 500 [SW2-port-group-5]quit //配置交换机之间的连接端口 [SW2]interface g0/0/24 [SW2-GigabitEthernet0/0/24]port link-type trunk [SW2-GigabitEthernet0/0/24]port trunk allow-pass vlan 300 400 500

6. 华为相关命令说明

1)设置端口 Trunk 类型
 视图:接口视图。
 命令:

[SW1-GigabitEthernet0/0/1]port link-type trunk

 2) 设置 Trunk 端口放行的 VLAN 视图:接口视图。
 命令:

[SW2-GigabitEthernet0/0/24]port trunk allow-pass vlan [vlan-id / all]

说明:华为交换机上 Trunk 端口默认拒绝所有 VLAN 通过,思科 PT 模拟器上 Trunk 端口默认允许所有 VLAN 通过。所以华为的 Trunk 端口要通过命令设置放行的 VLAN。如果要从放行的 VLAN 列表中删除某个 VLAN,可以用 undo 来实现。

例如,Trunk 端口只放行 VLAN 100,VLAN 200。

[SW2-GigabitEthernet0/0/24]port trunk allow-pass vlan 100 200

例如,Trunk 端口放行所有 VLAN。

[SW2-GigabitEthernet0/0/24]port trunk allow-pass vlan all

例如,从当前放行的列表中删除 VLAN 10。

[SW2-GigabitEthernet0/0/24] undo port trunk allow-pass vlan 10

 3) 设置 Trunk 端口的默认 VLAN 视图:接口视图。
 命令:

[SW1-GigabitEthernet0/0/24]port trunk pvid vlan vlan-id

参数:

vlan-id 是默认的 VLAN 编号,默认所有端口的 VLAN 都是 1。 例如,设置 Trunk 端口的默认 VLAN 为 100。

[SW1-GigabitEthernet0/0/24]port trunk pvid vlan 100

3.3 拓展知识

PVLAN 即私有 VLAN(Private VLAN),它采用两层 VLAN 隔离技术,在一台交换机 上存在主 VLAN(Primary VLAN)和从 VLAN(Secondary VLAN),如图 3-8 所示。一个 Primary VLAN 和多个 Secondary VLAN 对应,且 Primary VLAN 包含所对应的所有 Secondary VLAN 中包含的端口和上行端口,这样对于交换机来说,只需识别下层交换机中 的 Primary VLAN,而不必关心 Primary VLAN 中包含的 Secondary VLAN,简化了配置, 节省了 VLAN 资源。PVLAN 中各成员虽然同处于一个子网中,但各自只能与自己的默认 网关通信,相互之间不能通信。因此,相当于在一个 VLAN 内部就实现了 VLAN 本身所具 有的隔离特性。开发这种 VLAN 的目的主要是为 ISP 解决客户 VLAN 数太多,超过交换 机所允许的最大 4096 个 VLAN 的限制。



PVLAN 的应用对于保证接入网络的数据通信的安全性是非常有效的。用户只需与自己的默认网关连接,一个 PVLAN 不需要多个 VLAN 和 IP 子网就提供了具备第二层数据通信安全性的连接。所有的用户接入 PVLAN 就实现了所有用户与默认网关的连接,而与 PVLAN 内的其他用户没有任何访问。PVLAN 功能可以保证同一个 VLAN 中的各个端口相互之间不能通信,但可以穿过 Trunk 端口。这样即使同一 VLAN 中的用户,相互之间也不会受到广播的影响。

3.3.1 PVLAN 中的端口类型

在 PVLAN 中,交换机端口有 3 种类型:隔离端口(Isolated Port)、公共端口 (Community Port)和混杂端口(Promiscuous Port)。在 PVLAN 中,Isolated Port 只能和 Promiscuous Port 通信,但彼此不能交流通信流; Community Port 不仅可以和 Promiscuous Port 通信,而且彼此也可以交换通信流; Promiscuous Port 与路由器或三层交换机接口相连,它收到的通信流可以发往 Isolated Port 和 Community Port。它们分别对应 不同的 VLAN 类型: Isolated Port 属于 Isolated PVLAN, Community Port 属于 Community PVLAN,而代表一个 Private VLAN 整体的是 Primary VLAN,前面两类 VLAN 需要和它绑定在一起,同时它还包括 Promiscuous Port。

(1) 混杂端口(Promiscuous Port): 一个混杂类型端口属于主 VLAN,可以与所有端口 通信,包括与主 VLAN 关联的从 VLAN 中的共有端口和隔离 VLAN 中的主机端口。

(2)隔离端口(Isolated Port):一个隔离端口是一个属于隔离 VLAN 中的主机端口(也就是只能与主机连接的端口)。这个端口与同一个 PVLAN 域中的其他端口完全二层隔离,除混杂端口外。但是,PVLAN 会阻止所有从混杂端口到达隔离端口的通信,从隔离端口接收到的通信仅可以转发到混杂端口上。

(3) 公共端口(Community Port): 一个公共端口是一个属于公共 VLAN 的主机端口。 公共端口可以与同一个公共 VLAN 中的其他端口通信。这些端口与所有其他公共 VLAN 上的端口,以及同一 PVLAN 中的其他隔离端口之间都是二层隔离的。

3.3.2 PVLAN 中的 VLAN 类型

PVLAN 中有 3 种不同类型的 VLAN:主 VLAN(Primary VLAN)、隔离 VLAN (Isolated VLAN)和公共 VLAN(Community VLAN)。隔离 VLAN 和公共 VLAN 都属于 从 VLAN(Secondary VLAN)。

PVLAN 功能是将一个 VLAN 二层广播域划分为多个子域。一个子域包括一对 PVLAN:一个主 VLAN(Primary VLAN)和一个从 VLAN(Secondary VLAN)。一个 PVLAN 域中可以有多个 PVLAN 对,每个子域一对。PVLAN 域的所有子域中的 PVLAN 对共享相同的主 VLAN,但每个子域中的从 VLAN ID 是不同的。也就是说,一个 PVLAN 域仅有一个主 VLAN(Primary VLAN)。一个 PVLAN 域中的每个端口都是主 VLAN 的 成员。

(1) 主 VLAN: 主 VLAN 承载从混杂端口到隔离端口和共有主机端口的及其他混杂

端口的单向通信。

(2) 隔离 VLAN: 一个 PVLAN 域中仅有一个隔离 VLAN, 一个隔离 VLAN 是一个承载从主机到混杂端口和网关之间单向通信的从 VLAN。

(3)公共 VLAN: 一个公共 VLAN 是一个承载从公共端口到混杂端口、网关和其他在同一个公共 VLAN 中的主机端口之间单向通信的从 VLAN。

3.3.3 PVLAN 中使用的一些规则

- •一个 Primary VLAN 当中至少有一个 Secondary VLAN,没有上限。
- 一个 Primary VLAN 当中只能有一个 Isolated VLAN,可以有多个 Community VLAN。
- 不同 Primary VLAN 之间的任何端口都不能互相通信(这里"互相通信"是指二层连 通性)。
- Isolated 端口只能与混杂端口通信,除此之外不能与任何其他端口通信。
- Community 端口可以和混杂端口通信,也可以和同一 Community VLAN 当中的其他物理端口进行通信,除此之外不能和其他端口通信。

3.3.4 PVLAN 配置过程

1. 创建 Primary VLAN

配置: PVLAN 的步骤见表 3-3。

表 3-3 配置 PVLAN	的步骤
----------------	-----

步骤	命令	说 明
1	vlan vlan-id	进入要配置的 VLAN 配置模式
	private-vlan{community isolated primary}	配置 PVLAN 的类型
2	no private-vlan{community isolated primary}	清除 PVLAN 配置,这个命令的配置 要到退出 VLAN 配置模式后才生效
3	end	退出 VLAN 配置模式
4	<pre>show vlan private-vlan [type]</pre>	显示 PVLAN

例如,配置 VLAN 20 为主 VLAN。

S2328G(config) # vlan 20 S2328G(config-vlan) # private-vlan primary S2328G(config-vlan) # exit S2328G(config) # show vlan private-vlan

VLAN	Туре	Status	Routed	Ports	Associated VLANs
20	primary	inactive	Disabled		

S2328G(config) #

2. 创建 Secondary VLAN

例如,配置 VLAN 201 为公共 VLAN(Community VLAN), VLAN 202 为隔离 VLAN

(Isolated VLAN).

S2328G(config) # vlan 201 S2328G(config-vlan) # private-vlan community S2328G(config-vlan) # exit S2328G(config) # vlan 202 S2328G(config-vlan) # private-vlan isolated S2328G(config-vlan) # exit S2328G(config-vlan) # exit

VLAN	Туре	Status	Routed	Ports	Associated VLANs
20	primary	inactive	Disabled		
201	community	inactive	Disabled		No Association
202	isolated	inactive	Disabled		No Association

S2328G(config) #

3. 关联 Secondary VLAN 和 Primary VLAN

例如,关联 Secondary VLAN(VLAN 201,202)和 Primary VLAN(VLAN 20)。配置 步骤如表 3-4 所示。

步 骤	命令	说 明
1	vlan p-vlan-id	进入 Primary VLAN 配置模式
2	<pre>private-vlan association { svlist add svlist remove svlist }</pre>	关联 Secondary VLAN, svlist 为 Secondary VLAN 列表
	no private-vlan association	清除与所有 Secondary VLAN 的关联
3	end	退出 VLAN 配置模式
4	show vlan private-vlan [type]	显示 PVLAN

表 3-4 关联 Secondary VLAN 和 Primary VLAN 的步骤

S2328G(config) # vlan 20

S2328G(config-vlan) # private-vlan association 201,202 S2328G(config-vlan) # show vlan private-vlan

VLAN	Туре	Status	Routed	Ports	Associated VLANs
20	primary	inactive	Disabled		201 - 202
201	community	inactive	Disabled		20
202	isolated	inactive	Disabled		20

S2328G(config-vlan) #

4. 映射 Secondary VLAN 和 Primary VLAN 的三层接口

映射 Secondary VLAN 和 Primary VLAN 的三层接口配置步骤如表 3-5 所示。

步骤	命令	说 明
1	Interface vlan p-vid	进入 Primary VLAN 的接口模式
	private vlan mapping (sulist add sulist	映射 Secondary VLAN 到 Primary VLAN
2	private-vian mapping (sviist aud sviist	的三层口, <i>svlist</i> 为 Secondary VLAN
	remove sviist}	列表
	no private-vlan mapping	清除所有 Secondary VLAN 的映射
3	end	退出 VLAN 配置模式
4	show vlan private-vlan [type]	显示 PVLAN

表 3-5 映射 Secondary VLAN 和 Primary VLAN 的三层接口步骤

例如,配置 Secondary VLAN 的路由。

S2328G# configure terminal S2328G(config) # interface vlan 20 S2328G(config-if) # private-vlan mapping add 201,202 S2328G(config-if) # end S2328G#

5. 配置二层接口的 PVLAN 端口类型

配置二层接口的 PVLAN 的端口类型步骤如表 3-6、表 3-7 所示。

步骤	命令	说 明	
1	Interface interface	进入接口配置模式	
2	guitchport mode private ylan hest	指定二层接口为 PVLAN 的 host	
	switchport mode private-vian host	类型	
	noswitchport mode	清除二层接口的 PVLAN 端口类型	
		设置	
	switchport private-vlan host-association	关联二目接口 与 DVI A N	
3	p-vid s-vid	大联二压按口刁 FVLAN	
	no switchport private-vlan host-association	取消二层接口与 PVLAN 的关联	

表 3-6 配置二层接口作 PVLAN 的主机端口的步骤

例如,将F0/1指定为PVLAN的主机端口。

S2328G(config) # interface f0/1 S2328G(config-if) # switchport mode private-vlan host S2328G(config-if) # switchport private-vlan host-association 20 201 S2328G(config-if) # show vlan private-vlan

VLAN	Туре	Status	Routed	Ports	Associated VLANs
20	primary	inactive	Enabled		201-202
201	community	inactive	Disabled F	a0/1	20
202	isolated	inactive	Disabled		20

S2328G(config-if) #

对企业各部门的网络进行隔离及广播风暴控制

项 目

3

步骤	命令	说 明	
1	Interface interface	进入接口配置模式	
	switchport mode private-vlan promiscuous	指定二层接口为 PVLAN 的 Promiscuous 类型	
Z	no switchport mode	清除二层接口的 PVLAN 端口类型 设置	
3	<pre>switchport private-vlan mapping p-vid {svlist add svlist remove svlist}</pre>	PVLAN 混杂端口选择所在 VLAN 及 混杂的 Secondary VLAN 列表	
	no switchport private-vlan mapping	取消混杂所有的 Secondary VLAN	

表 3-7 配置二层接口作 PVLAN 的混杂端口的步骤

例如,将 F0/3 指定为 PVLAN 的混杂端口。

S2328G(config) # interface f0/3 S2328G(config-if) # switchport mode private-vlan promiscuous S2328G(config-if) # switchport private-vlan mapping 20 201



3.4 项目实训

企业网络由4台交换机(一楼 SW1、二楼 SW2、三楼 SW3 和网络中心交换机 SW4)连接,因网络中经常有用户的 PC 感染病毒而向网络中发送广播形成广播风暴,导致企业整个网络的正常使用受到影响。现要求在交换机上使用 VLAN 来进行不同部门之间的隔离,减少广播风暴对整个网络的影响,如图 3-9、图 3-10 所示。



72



基本要求:

(1) 正确选择设备并使用线缆连接;

(2) 正确给各个 PC 配置相关 IP 地址及子网掩码等参数;

(3) 在 SW1 上配置相关 VLAN,并将交换机相应的端口添加到 VLAN 中,用相关显示 命令查看配置结果;

(4) 在 SW2 上配置相关 VLAN,并将交换机相应的端口添加到 VLAN 中,用相关显示 命令查看配置结果;

(5) 在 SW3 上配置相关 VLAN,并将交换机相应的端口添加到 VLAN 中,用相关显示 命令查看配置结果;

(6) 在 SW4 上进行相关配置,使得不同交换机上的相同部门的 PC(如销售部 PC1 和销售部 PC3)可以相互访问。

拓展要求:

配置如图 3-11 所示的网络拓扑图中的两个交换机,使得两个不同 VLAN 中的 PC 能相互访问(提示: 思科 PT 模拟器中要关闭生成树协议)。



图 3-11 网络拓扑图

项目3的考核表如表3-8所示。

项

目 3

序 号	项目考核知识点	参考分值	评 价
1	设备连接	2	
2	配置 PC 的 IP 地址及子网掩码等参数	6	
3	交换机上创建 VLAN 及划分相应端口	6	
4	交换机上 Trunk 端口的设置	4	
5	拓展要求	2	
	合计	20	

表 3-8 项目 3 考核表

3.5 3 颞

1. 选择题

- (1)下面哪一句话是错误的?())
 - A. VLAN 是不受物理区域和交换机限制的逻辑网络, 它构成一个广播域
 - B. VLAN 能解决局域网内由广播过多所带来的宽带利用率下降、安全性低等问题
 - C. VLAN 的主要作用是缩小广播域,控制广播风暴
 - D. 所有主机和交换机都能识别带有 VLAN 标签的数据帧
- (2) 一个 Access 端口可以属于多少个 VLAN? ()
 - A. 仅一个 VLAN
 - C. 最多 4096 个 VLAN

- B. 最多 4094 个 VLAN
- D. 根据管理员设置的结果而定
- (3)下面各类端口对报文处理正确的是()。
 - A. Access 端口可以接收和发生多个 VLAN 的报文
 - B. Trunk 端口可以接收和发生多个 VLAN 的报文
 - C. Hybrid 端口只可以接收和发送一个 VLAN 的报文
 - D. Trunk 端口可以接收和发送多个不打 VLAN 标签的报文
- (4) 当需要 VLAN 跨交换机时,交换机与交换机之间连接的端口应该设置为哪类端
- 口?()

А.	Access 端口	В.	Trunk 端口
----	-----------	----	----------

C. Hybrid 端口

- D. Console \square
- (5) IEEE 802.1g 协议是如何给以太网帧打上 VLAN 标签的?()
 - A. 在以太网帧的前面插入 4 字节的 Tag
 - B. 在以太网帧的后面插入 4 字节的 Tag
 - C. 在以太网帧的源地址和长度/类型字段之间插入4字节的 Tag
 - D. 在以太网帧的外部加上 802.1q 封装信息
- (6) 对交换机的 Access 端口和 Trunk 端口描述正确的是() _
 - A. Access 端口只能属于一个 VLAN, 而 Trunk 端口可以属于多个 VLAN
 - B. Access 端口只能发送不带 Tag 的帧,而 Trunk 端口只能发送带有 Tag 的帧
 - C. Access 端口只能接收不带 Tag 的帧,而 Trunk 端口只能接收带有 Tag 的帧
 - D. Access 端口的默认 VLAN 只能是 VLAN 1,而 Trunk 端口可以有多个默认 VLAN

(7) 下面删除 VLAN 的命令哪一条是正确的? () A. Switch # no vlan 10 B. Switch(config) # no vlan 1 C. Switch(config) # no vlan 10 D. Switch(config) # del vlan 10 (8) 在思科交换机上配置 Trunk 接口时,如果要从允许 VLAN 列表中删除 VLAN 10, 该用下面哪条命令?() A. Switch(config-if) # switchport trunk allowed remove 10 B. Switch(config-if) # switchport trunk vlan remove 10 C. Switch(config-if) # swtichport trunk vlan allowed remove 10 D. Switch(config-if) # swtichport trunk allowed vlan remove 10 (9) 当要使一个 VLAN 跨越两台交换机时,需要下面哪个条件支持?() A. 用三层交换机连接两台交换机 B. 将两台交换机的连接口设置成 Trunk C. 用路由器连接两台交换机 D. 在两台交换机上面配置相同的 VLAN (10) 在 PVLAN 中,哪类端口可以与所有类型的端口通信? () A. 公共端口 B. 隔离端口 C. 混杂端口 D. 私有端口 2. 简答题 (1) 简述 VLAN 的概念。VLAN 的作用是什么? (2) VLAN 有哪些划分方法? (3) 简述 Access 端口如何收发报文。

(4) 在一台锐捷交换机上配置一个 VLAN 10,并将端口 1~10 添加到 VLAN 10 中,将 端口 24 设置成 Trunk 端口,该如何配置?