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

某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，为此该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 的帧的格式
- 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 技术既是交换机管理与配置的重点，也是难点。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 技术可以把一个局域网划分成多个逻辑的而不是物理的网络，也就是 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，其他方面和普通局域网都相同。在同一个 VLAN 中的工作站，不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，这样就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 的主要用途就是缩小广播域，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。当网络中的用户多到一定的数量后，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逻辑上相互独立的小网络。

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外，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 所示为 VLAN 划分示意图。

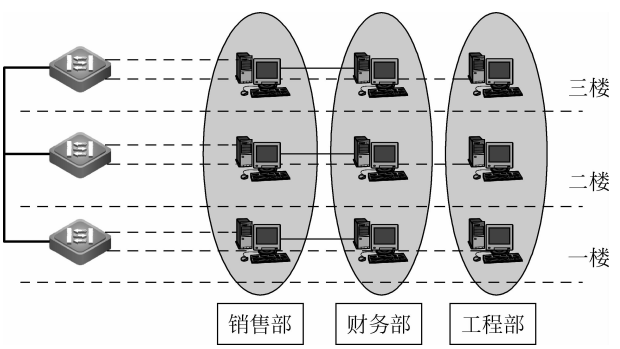

图 3-1　VLAN 划分示意图

3.1.3　VLAN 的划分

常用的 VLAN 划分方法有以下几种。

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 VLAN 划分的优点是定义 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，不用做重新配置。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 协议和 IPX 协议），而与其他因素无关。这种划分方式实际应用非常少，因为目前绝大多数都是运行 IP 协议的主机，所以很难将

VLAN 划分得更小。

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，而与主机其他的因素无关。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主机 IP 地址所属的网络子网进入别的 VLAN，从而无法控制用户的相互访问。

从上面几种 VLAN 划分的方式来看，基于端口的 VLAN 划分是最普遍的方法之一，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利互通，802.1q 标准严格规定了统一的 VLAN 帧格式以及其他重要参数。

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。

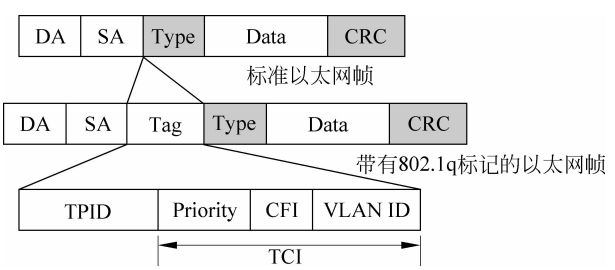

图 3-2　802.1q 标准规定的以太网帧格式

Tag 域长度为 4 个字节，其中各个标签的含义如下。

TPID：长度为两个字节，协议标识字段，值为固定的 0x8100，说明该帧具有 802.1q 标签。

TCI：长度为两个字节，控制信息字段，包括用户优先级、规范格式指示器和 VLAN ID。

Priority：长度为三个二进制位，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：长度为一个二进制位，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 802.1q 协议的主机发送出来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，所以最多只有 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

目前大部分主机都不支持带有 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。

VLAN 数据帧的传输过程如图 3-3 所示。

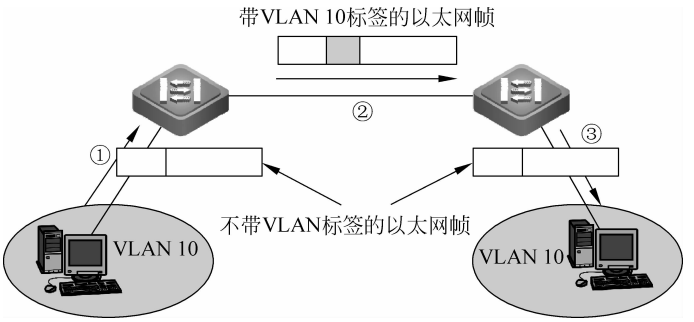

图 3-3　VLAN 数据帧的传输过程

(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都会被打上 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，所以当交换机目的端口连接的是主机时，交换机在把数据帧发送给主机之前会先把数据帧中的 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、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 端口只属于一个 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。

Acess 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 的标签，并进行交换转发，如果有则直接丢弃(默认)。

Acess 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 的标签，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 的标签，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，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 1：给公司各个部门划分 VLAN

1. 任务描述

该公司有生产、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。

表 3-1 交换机端口分配表

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

2. 实验网络拓扑图

本实验网络拓扑图如图 3-4 所示。

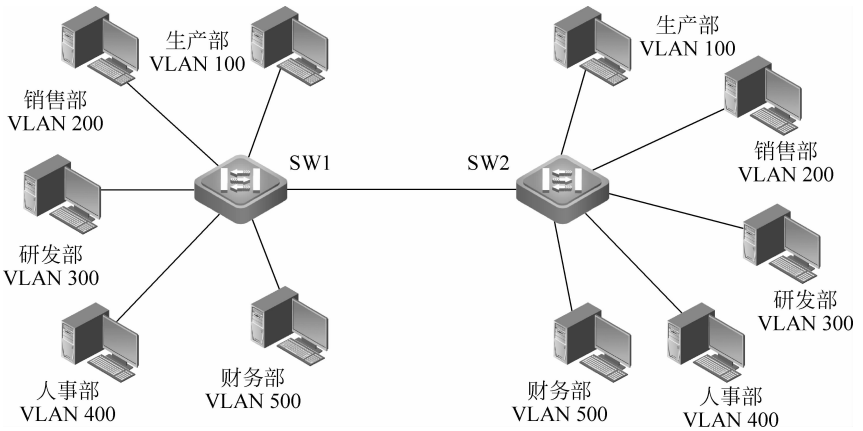

图 3-4　任务 1 实验网络拓扑图

3. 设备配置

交换机 SW1 配置如下：

```
S2328G>en
S2328G#config
Enter configuration commands, one per line. End with CNTL/Z.
S2328G(config)#hostname SW1
SW1(config)#vlan 100                              //创建 VLAN 100
SW1(config-vlan)#name shengchan                   //修改 VLAN 100 的名字为 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
SW1(config-if)#switchport access vlan 100         //将 F0/1 端口加入 VLAN 100 中
SW1(config-if)#exit
SW1(config)#interface range f0/3,0/5,0/7,0/9 //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 f0/2,0/4,0/6,0/8,0/10   //同时进入 F0/2,4,6,8,10 端口
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              //同时进入 F0/11 到 F0/15 端口
SW1(config-if-range)#switchport access vlan 300
                                                  //将 F0/11 到 F0/15 端口一起加入 VLAN 300 中
SW1(config-if-range)#exit
```

```
SW1(config)#interface range f0/16,0/18-20    //同时进入 F0/16,18,19,20 端口
SW1(config-if-range)#switchport access vlan 400
                                             //将 F0/16,18,19,20 端口一起加入 VLAN 400 中
SW1(config-if-range)#exit
SW1(config)#interface range f0/21-22         //同时进入 F0/21,22 端口
SW1(config-if-range)#switchport access vlan 500
                                             //将 F0/21,22 端口一起加入 VLAN 500 中
SW1(config-if-range)#exit
SW1(config)#
```

交换机 SW2 配置如下：

```
S2328G>en
S2328G#config
Enter configuration commands, one per line. End with CNTL/Z.
S2328G(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)#
```

4. 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：

vlan *vlan-id*

no vlan *vlan - id*

参数如下。

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 是默认存在的而且不能被删除。

例如：创建 vlan-id 为 10 的 VLAN。

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

2）设置 VLAN 的名字

视图：VLAN 配置视图。

命令：

name *vlan - name*
no name

参数如下。

vlan-name：vlan 的名字。

说明：

该命令是用来给相应的 VLAN 设置名字，便于管理维护和识别。VLAN 默认的名字为 VLANXXXX，其中 XXXX 是由 0 开头的 4 位 VLAN ID 号。例如，VLAN 10 的默认名字为 VLAN0010。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 的名字为 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：

interface range fastEthernet {*mod - num/port - num* | *, mod - num/ port - num - port - num* }

参数如下。

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。

- 端口组成为多个不连续的端口，如端口 1,3,5,11 组成一组时，命令描述如下：

```
interface range fastEthernet 0/1,0/3,0/5,0/11
```

也可以简写为：

```
inte range f0/1,0/3,0/5,0/11
```

- 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，又有连续的端口，如端口 11，端口 15,16,17 组成一组时，命令描述如下：

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

也可以简写为：

```
inte range f0/11,0/15 - 17
```

4）将端口添加到 VLAN 中

视图：接口配置视图。

命令：

switchport access vlan *vlan - id*
no switchport access vlan

参数如下。

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，要将交换机的端口 5 添加到 VLAN 10 中去，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，则会自动先创建该 VLAN，然后再将端口添加进该 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，可以有两种方式实现，第一种方式与锐捷的相似，先进入端口视图，然后将端口添加到 VLAN 中去。另外一种方式是在 VLAN 配置视图下，把所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 选项可以让该端口从指定的 VLAN 中删除，会到默认的 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：特权视图。

命令：

show vlan [**id** *vlan－id*]

参数如下。

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。

```
S2328G#show vlan
VLAN Name                              Status      Ports
-----  ------------------------------  ----------  ---------------------
  1 VLAN0001                           STATIC      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, Gi0/25
                                                   Gi0/26
  100 shengchan                        STATIC      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5
S2328G#
```

例如：查看 VLAN 100 的配置信息。

```
S2328G#show vlan id 100
VLAN Name                              Status      Ports
-----  ------------------------------  ----------  ---------------------
  100 shengchan                        STATIC      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5
S2328G#
```

任务 2：同一部门用户跨交换机的访问控制

1. 任务描述

该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。

表 3-2　各部门的 VLAN ID 和交换机端口分配表

部门	交换机 1(SW1)端口号	交换机 2(SW2)端口号	VLAN ID
生产部	1～5	1～5	100
销售部	6～10	6～10	200
研发部	11～15	11～15	300
人事部	16～20	16～20	400
财务部	21～22	21～22	500