第 3 章　多层交换网络

随着光纤技术的发展，校园网、社区网、园区网、企事业单位网也蓬勃发展，它们都属于局域网范畴，统称为园区网，主要由交换机互连而成。其采用层次化设计方法，将一个复杂的网络分解为若干特定的层，从而简化网络设计的复杂度。园区网交换结构通常采用三层结构，包括核心层、汇聚层（分布层）、接入层。核心层由高端路由器或高端三层交换机组成，同时考虑多冗余和负载均衡，即由多台高端三层交换机组成。汇聚层将一幢、同类的几幢楼或几个逻辑单位所有信息点汇聚在一台或几台中高端三层交换机上，汇聚层上连核心层，下连一组接入层交换机。接入层交换机负责管理一个机房、一个楼面或一个部门的所有计算机。

核心层、汇聚层（分布层）、接入层的所有交换机相互的连接，包括交换机的选型、模块和接口的选择、线缆的选择和连接、协议的选择等，是多层交换网络中最主要的设计内容。根据不同单位的不同需求，就会产生丰富多样的网络结构。

本章介绍 Trunk 链路、聚合链路、VTP 协议、交换机端口安全，以使读者全面了解多层交换网络。

3.1　Trunk 链路

两台多 VLAN 的交换机如何实现相同 VLAN 间的通信？使用 Trunk 链路（也称为中继链路）。注意两台交换机都只有一个 VLAN，可以两端都定义为 Access 链路，且属于同一 VLAN，相互通信。

两台交换机相连时能否形成中继链路可以动态协商。有两种动态协商方式：Dynamic Desirable 和 Dynamic Auto。端口定义形式为：

```
Switch(config-if)#switchport mode dynamic desirable
```

或

```
Switch(config-if)#switchport mode dynamic auto
```

表 3-1 总结了两台交换机相连能否成功协商形成 Trunk 链路的情况。×表示链路不通，Access 表示只能左右是同一 VLAN 才能通信，Trunk 表示能形成 Trunk 链路。

表 3-1　Trunk 链路协商

交换机 1 的端口模式及链路形式	交换机 2 的端口模式及链路形式			
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	×
Access	Access	Access	×	Access

从表 3-1 中可以看出：

(1) 有一端的端口设置为 Access，无论对端是什么，均不能形成 Trunk 链路。

(2) 两端都是 Dynamic Auto 时，不能形成 Trunk 链路。

(3) 如果一端为 Trunk，而另一端为 Access，该链路不通。

为简单起见，两台交换机要么端口同时设置为 Trunk，要么同时设置为 Access，如图 3-1 所示。

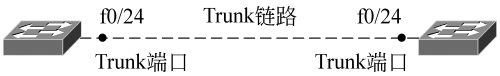


图 3-1　Trunk 链路

对 Trunk 链路，可以指定允许通过的 VLAN 列表，否则默认允许全部 VLAN 通过。但 Trunk 链路有一个 Native VLAN(本地 VLAN)，默认情况下 Native VLAN 是交换机中必有的 VLAN 1。但可以用命令来改变 Native VLAN，例如，下面命令为 Trunk 口指定的 Native VLAN 是 10：

```
Switch(config-if)#switchport trunk native vlan 10
```

定义 Native VLAN 并不影响 Trunk 链路允许所有 VLAN 通过，只是表示在 Trunk 链路上传输属于 Native VLAN 的数据帧时不添加标记。即当交换机在 Trunk 链路上收到未加标记的数据帧时，交换机认为该帧是属于 Native VLAN 的帧。

Trunk 链路可以接收与 Native VLAN 不一致的带标记的帧，即允许所有带有标记的帧通过。Trunk 链路也可以接收没有标记的帧，它把此帧归属于 Native VLAN。

通常不需要修改 Native VLAN。用 Switch(config-if)# **no switchport trunk native vlan** 命令恢复 Native VLAN 为 VLAN 1。

3.2　以太网链路聚合

以太网链路聚合(Etherchannel)通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。同时，这些捆绑在一起的链路相互提供动态冗余备份，其中任意一条链路断开，也不会影响其他链路的正常转发数据，从而可以有效地提高链路的可靠性。

端口链路聚合主要应用的场合如下：

- 交换机与交换机之间的连接：汇聚层交换机到核心层交换机或核心层交换机之间。
- 交换机与服务器之间的连接：集群服务器采用多网卡与交换机连接提供集中访问。
- 交换机与路由器之间的连接：交换机和路由器采用端口聚合解决广域网和局域网连接的瓶颈问题。
- 服务器和路由器之间的连接：集群服务器采用多网卡与路由器连接提供集中访问。

端口链路聚合的两端要求如下：

- 端口均为全双工模式。
- 端口速率相同。

- 端口的类型必须一样,比如同为以太网端口或同为光纤端口。
- 端口同为 Access 端口且属于同一个 VLAN 或同为 Trunk 端口。

如果端口为 Trunk 端口,则其 Allowed VLAN 和 Native VLAN 属性也应该相同。

有两种链路聚合协议:一种是思科独有的协议 PAgP(Port Aggregation Protocol,端口聚合协议),另一种是基于 IEEE 802.3ad 标准的链路聚合控制协议 LACP(Link Aggregate Control Protocol)。

3.2.1 PAgP

PAgP 是一个在检查 Channel 两端参数的一致性以及在出现增加链路或链路失效时重新适配的管理协议,具有如下的限制条件:

(1) PAgP 需要所有 Channel 中的端口处于同一个 VLAN 或都配置成为 Trunk 链路端口(因为动态 VLAN 可能会强制地将端口放到不同的 VLAN 中,所以动态 VLAN 不能和以太网通道在一个端口上并行操作)。

(2) PAgP 不能在不同速度或不同双工模式的端口之间配合操作,当一个 Channel 中某个端口的速度或双工模式改变时,PAgP 将改变该 Channel 中所有端口的速度和双工模式。

(3) 当对已有 Channel 中的某个端口的配置进行修改时(如改变 VLAN 或 Trunk 模式),该 Channel 中的所有端口均将做相同的修改。

(4) 思科最多允许 EtherChannel 绑定 8 个端口。如果是快速以太网,总带宽可达 1600Mb/s;如果是 G 比特以太网,总带宽可达 16Gb/s。不支持 10Mb/s 端口绑定。

(5) 不仅支持二层 EtherChannel,还支持三层 EtherChannel。

EtherChannel 将物理接口组指定至某个 Channel 组,命令为:

```
Switch(config-if-range)#channel-group [num] mode [on|off|auto| desirable]
```

其中,

- num:channel 组号,为 1～64。channel 组号只在本地有效,链路两端的组号可以不一样。
- on:PAgP 不进行操作,不管对方是怎样配置的,端口总处理 channeling 状态,如果对方的模式也为 on,正好形成一个 EtherChannel。建议不使用 on 模式。
- off:防止端口形成 EtherChannel。
- auto:默认模式,被动协商,将端口置于被动协商状态,在收到 PAgP 包之前不会有 PAgP 包发送。端口接收到 PAgP 包就形成 EtherChannel。
- desirable:主动协商,将端口置于一个主动协商状态,主动发送 PAgP 包,推荐使用此模式。
- non-silent(5000 的光 FE 和 GE 端口的默认状态):auto 或 desirable 模式的一个关键字。如果在端口上没有收到数据包,端口一直不会关联到 agport,不能传输数据。
- silent(4000、6000 的端口和 5000 的铜端口的默认状态):auto 或 desirable 模式的一个关键字。如果在 15s 内没收到数据包,端口将关联到一个 agport 并进行数据传输。silent 模式允许和一个不发送 PAgP 包的服务器进行 Channel 操作。

建议在链路的两端均使用 desirable 模式,并保留 silent/non-silent 关键字的默认设置,

在 6000 和 4000 上使用 silent，在 5000 的光口上使用 non-silent。

PAgP 两端模式协商的情况如表 3-2 所示。

表 3-2　PAgP 两端模式协商

一端模式	另一端模式		
	on	desirable	auto
on	√	×	×
desirable	×	√	√
auto	×	√	×

3.2.2　LACP

LACP 是一种基于 IEEE 802.3ad 标准，能够实现链路动态聚合与解聚合的协议。LACP 通过 LACPDU(Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元)与对端交互信息。

设置某端口的 LACP 协议后，该端口将通过发送 LACPDU 向对端通告自己的系统 LACP 协议优先级、系统 MAC、端口的 LACP 协议优先级、端口号和操作 Key。对端接收到 LACPDU 后，将其中的信息与其他端口所收到的信息进行比较，以选择能够聚合的端口，从而双方可以就端口加入或退出某个动态 LACP 聚合组达成一致。

操作 Key 是在链路聚合时根据端口的配置(即速率、双工模式、up/down 状态、基本配置等信息)自动生成的一个配置组合。对于动态 LACP 聚合组，同组成员有相同的操作 Key；对于手工聚合组和静态 LACP 聚合组，处于 Selected 状态的端口有相同的操作 Key。命令如下：

```
Switch(config-if-range)#channel-group 1 mode [on|off|active|Passive]
```

- on：强制端口不使用 LAGP 而形成 EtherChannel。
- off：防止端口形成 EtherChannel。
- passive：默认模式，被动协商，端口接收 LAGP，就形成 EtherChannel。相当于 PAgP 的 auto。
- active：主动端口利用 LAGP 形成 EtherChannel，为推荐模式。相当于 PAgP 的 desirable，能够收发协商消息。

LACP 两端模式协商的情况如表 3-3 所示。

表 3-3　LACP 两端模式协商

一端模式	另一端模式		
	on	active	passive
on	√	×	×
active	×	√	√
passive	×	√	×

3.2.3 聚合链路的配置步骤

1. 创建 EtherChannel

(1) 规划并选择要配置为 EtherChannel 的物理接口组,命令如下:

```
Switch(config)#interface range f0/1-2
```

(2) 配置物理接口组内端口为同一 VLAN 的 Access、Trunk 或路由端口,命令如下:

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 1
```

或

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

或

```
Switch(config-if-range)#no switchport
```

(3) 选择 EtherChannel 的协议类型:LACP 或 PAgP,在 PacketTracer 中默认的是 PAgP 协议,命令如下:

```
Switch(config-if-range)#channel-protocol [pagp| lacp]
```

(4) 将物理接口组指定至 EtherChannel 组,命令如下:

```
Switch(config-if-range)#channel-group {num} mode [on|off|auto| desirable]
```

(5) 进入聚合端口,命令如下:

```
Switch(config)#int port-channel {num}
```

(6) 配置聚合端口为 Access、Trunk 或路由口(及 IP 地址),命令如下:

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

或

```
Switch(config-if-range)#switchport mode access
```

或

```
Switch(config-if-range)#no switchport
```

2. 配置 EtherChannel 负载均衡

EtherChannel 具有负载均衡和线路备份的作用。

所谓负载均衡,就是指当交换机之间或交换机与服务器之间进行通信时,EtherChannel 的所有链路将同时参与数据的传输,从而使所有的传输任务都能在极短的时间完成,线路占用的时间更短,网络传输的效率更高。

所谓线路备份,是指当部分 EtherChannel 链路出现故障时,并不会导致连接的中断,其他链路将能够不受影响地正常工作,从而增强了网络的稳定性和安全性。

配置 EtherChannel 负载均衡的命令如下：

```
Switch(config)#port-channel load-balance [dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac]
```

注意：要在全局配置模式下配置负载均衡。默认情况下是 src-mac，是基于源 MAC 地址的负载均衡。常用 dst-ip，即基于目标 IP 地址的负载均衡。

3. 检验配置的命令

```
Switch#show etherchannel load-balance
Switch#show etherchannel summary
Switch#show etherchannel port-channel
Switch#show running-config
```

4. 从 EtherChannel 中移除端口

```
Switch(config)#interface interface-id     /* 指定要配置的物理端口 */
Switch(config-if)#no channel-group        /* 从 EtherChannel 中移除端口 */
Switch#show running-config                /* 检验配置中是否移除了端口 */
```

5. 删除 EtherChannel 端口

```
Switch(config)#no int port-channel [num]
Switch#show etherchannel summary          /* 检验配置(或查看当前的 EtherChannel) */
```

6. 将 EtherChannel 端口从 err-disable 状态恢复正常

EtherChannel 端口如果进入 err-disable 状态，有两种方法使其恢复正常：

(1) 手动恢复：先执行 shutdown 命令，再执行 no shutdown 命令。

(2) 自动恢复：此方法在 PacketTracer 中不能实现。

```
Switch(config)#int  port-channel  [num]
Switch(config-if)#errdisable recovery cause {all|arp-inspection|bpduguard|link-flap}
                                                          /* 指定原因 */
Switch(config-if)#errdisable recovery interval 30   /* 指定自动恢复时间间隔 */
```

3.2.4　聚合链路应用举例

1. 二层聚合链路的配置

把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接就称为聚合端口(aggregate port，AP)。它可以把多个端口的带宽叠加起来使用。

通过 AP 发送的帧将在 AP 的成员端口上进行流量均衡，当一个成员端口链路失效后，AP 会自动将这个成员端口上的流量转移到别的端口上。同样，一个 AP 可以为 Access 端口或 Trunk 端口，但 AP 各成员端口必须属于同一类型。

二层 Access 端口聚合成一个逻辑端口，要求两台交换机的对应端口及成员端口都属于同一个 VLAN(子网)。这就是交换机的级联，其目的是增加端口的总数(扩容)，通过聚合增加带宽并提供冗余。

思科二层 Access 端口聚合的命令行配置如下。

(1) Access端口聚合

```
Switch(config)#interface range f0/23 -24
Switch(config-if-range)#switchport mode access  /*23、24号端口都为Access端口*/
Switch(config-if-range)#channel-protocal lacp            /*或pagp*/
Switch(config-if-range)#channel-group 1 mode active
/*或desirable,将23、24号端口聚合一起为1号端口*/
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode access
/*将聚合1号端口设置为Access端口,仅属于VLAN 1*/
```

(2) Trunk端口聚合

思科二层Trunk端口聚合的命令行配置如下:

```
Switch(config)#interface range f0/23-24
Switch(config-if--range)#switchport mode trunk
/*23、24号端口都为Trunk端口*/
Switch(config-if-range)#channel-protocal pagp            /*或lacp*/
Switch(config-if-range)#channel-group 2 mode desirable   /*或active*/
Switch(config-if-range)#exit
Switch(config)#int port-channel 2
Switch(config-if)#switchport mode trunk
/*将聚合2号端口设置为Trunk端口,属于全体VLAN*/
```

注意:如果是三层交换机做Trunk端口聚合,必须增加一条封装协议:

```
Switch(config-if-range)#switchport trunk encapsulation dot1q
                                          /*Trunk封装协议IEEE 802.1q*/
```

(3) 将23号端口从2号聚合端口中拆除

```
Switch(config)#interface  f0/23
Switch(config-if)#no channel-group 2 mode active   /*将f0/23端口从聚合端口中拆除*/
```

(4) 删除一个聚合端口

```
Switch(config)#no int Port-channel 2
/*删除2号聚合端口*/
```

注意:删除聚合端口时,需先解除聚合。

2. 三层聚合链路的配置

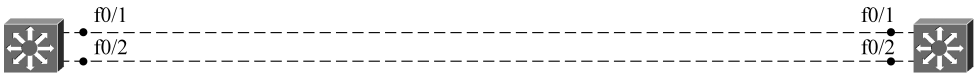
左右两端的三层交换机多个端口用交叉线互连,将两端的端口设定为三层路由端口,每个端口不设置IP地址,将这些端口聚合成一个三层聚合端口(L3 aggregate port),为其分配IP地址以建立路由。

在左边的三层交换机上创建三层聚合端口的命令如下:

```
Switch(config)#interface range f0/1-2
Switch(config-if-range)#no switchport          /*将1和2两个端口变成路由端口*/
Switch(config-if-range)#channel-group 3 mode desirable
```

```
/* 将 1 和 2 两个端口聚合成 3 号聚合端口 */
Switch(config-if-range)#no ip address              /* 1 和 2 两个端口均无 IP 地址 */
Switch(config-if-range)#exit
Switch(config)#interface port-channel 3            /* 对聚合端口 3 */
Switch(config-if)#no switchport                    /* 使聚合端口 3 成为路由端口 */
Switch(config-if)#ip address 192.168.1.253 255.255.255.0
/* 设置聚合端口 3 的 IP 地址 */
Switch(config-if)#exit                             /* 返回特权模式 */
Switch(config)#port-channel load-balance dst-ip    /* 配置针对目标 IP 的负载均衡 */
```

同理，按上述步骤在右边的三层交换机上也创建三层聚合端口，但其聚合端口的 IP 地址为 192.168.1.254，如图 3-2 所示。



port-channel load-balance dst-ip
interface range f0/1-2
no switchport
channel-group 3 mode desirable
no ip address
!
interface port-channel 3
no switchport
ip address 192.168.1.253 255.255.255.0

port-channel load-balance dst-ip
interface range f0/1-2
no switchport
channel-group 3 mode desirable
no ip address
!
interface port-channel 3
no switchport
ip address 192.168.1.254 255.255.255.0

图 3-2　三层交换机的三层聚合链路

检查端口配置信息：

```
Switch#show etherchannel summary              /* 显示链路汇总信息 */
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group     Port-channel      Protocol         Ports
------    +-------------    +------------    +------------
3         Po3(RU)           PAgP             f0/1(P) f0/2(P)

Switch#show etherchannel port-channel         /* 显示详细链路信息 */
Channel-group listing:
-----------------------
Group: 3
----------
Port-channels in the group:
```

```
----------------------------
Port-channel: Po3
------------
Age of the Port-channel=00d:00h:05m:14s
Logical slot/port=2/3    Number of ports=2
GC=0x00000000            HotStandBy port=null
Port state=Port-channel
Protocol=PAGP
Port Security=Disabled
Ports in the Port-channel:
Index     Load        Port        EC state              No of bits
------  +------    +------    +---------------     +------------
0         00          f0/2        Desirable-Sl          0
0         00          f0/1        Desirable-Sl          0
Time since last port bundled: 00d:00h:05m:13s f0/1

Switch#show running-config                  /* 显示信息略 */
Switch#show etherchannel load-balance       /* 显示信息略 */
Switch#ping 192.168.1.254                   /* 左端交换机 ping 右端,通 */
```

3.3 虚拟主干协议 VTP

3.3.1 VTP 基础

VTP(VLAN Trunk Protocol)即 VLAN 中继协议,也称为虚拟局域网干道协议。它是思科私有协议,工作在数据链路层。

要管理 VLAN 的增加、删除以及更名以保持所有交换机中 VLAN 的一致性,可以使用 VTP 协议。

VTP 提供了一种在交换机上管理 VLAN 的方法,该协议使用户可以在一个或者几个中央点(服务器)上创建、修改、删除 VLAN,通过 Trunk 链路把 VLAN 信息自动扩散到其他交换机。把一台交换机配置成 VTP 服务器,其余交换机配置成 VTP 客户端,这样它们可以自动学习到服务器上的 VLAN 信息,使大规模的网络管理简单、自动化。

VTP 被组织成域(VTP domain),相同域中的交换机能共享 VLAN 信息。域名由服务器定义,其他交换机跟从,命令如下:

```
Switch(config)#vtp domain 域名
```

根据交换机在 VTP 域中的作用不同,VTP 可以分为 3 种模式,命令如下:

```
Switch(config)#vtp mode {Server| Client | Transparent}
```

其中,Server 为服务器模式,Client 为客户端模式,Transparent 为透明模式。新出厂的交换机默认配置是 VLAN 1,VTP 模式为 Server。

- VTP Server 维护该 VTP 域中所有 VLAN 信息列表,能在本地删除、创建、修改

VLAN 信息，可以产生、发送、接收、处理、转发 VTP 消息。

- VTP Client 虽然也维护所有 VLAN 信息列表，但其 VLAN 的配置信息是从 VTP Server 学到的。VTP Client 不能在本地删除、创建、修改 VLAN 信息，但可以产生、发送 VTP 消息。
- VTP Transparent 相当于一个独立的交换机，它不参与 VTP 工作，不从 VTP Server 学习 VLAN 的配置信息，只拥有本设备上自己维护的 VLAN 信息。VTP Transparent 能在本地删除、创建、修改 VLAN 信息；只能转发 VTP 消息，不能发送自身的 VLAN 消息，修订号始终为 0。

VTP 通告是在交换机之间用来传递 VLAN 信息的数据包，称为 VTP 数据包。VTP 通告信息以多播帧的方式在 Trunk 链路上传输，信息中包括配置修订号，代表配置的新旧，只要交换机收到更高的信息，就覆盖以前的信息，所以配置版本号在 VTP 更新中起着非常重要的作用，每当服务器修改后，配置修订号都会自动加 1。

VTP 通告类型有 3 种：汇总通告、通告请求、子网通告。

(1) VTP 汇总通告：交换机每 5min 发送一次汇总通告，通告邻居目前的 VTP 域名和配置修订号。

(2) VTP 通告请求：在交换机重启后或 VTP 参数改变时发送通告请求。

(3) VTP 子网通告：在 VTP 服务器上删除、创建或修改了 VLAN 就发送子网通告。

当某些子网不需要传递 VTP 通告时，会采用 VTP 修剪(图 3-3)，命令如下：

```
Switch(config)#vtp pruning
```

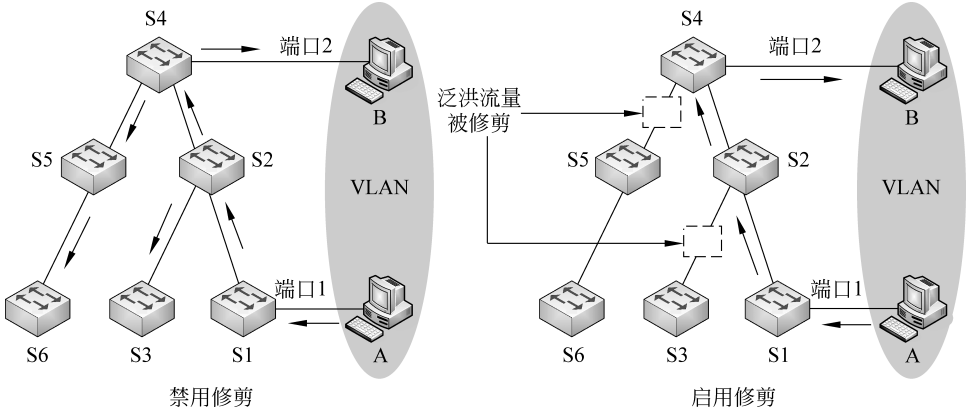


图 3-3　VTP 的修剪原理

3.3.2　VTP 的配置

1. 实验目的

(1) 理解 VTP 协议(域、模式、工作过程等)。

(2) 掌握 VTP 的配置方法。

2. 实验拓扑

实验拓扑如图 3-4 所示，有三台二层交换机，用交叉线互连，并定义为 Trunk 链路。

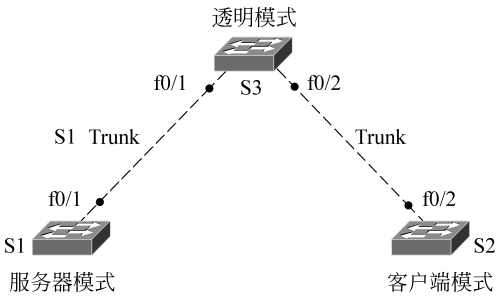


图 3-4　VTP 模式设计与配置实例

3. 实验配置步骤

(1) 在交换机 S1 上配置 VTP 服务器,并创建 3 个 VLAN,即 10、20、30:

```
/* 定义 Trunk 链路,VTP 必须在 Trunk 链路上发送数据包 */
S1(config)#int f0/1
S1(config-if)#switchport mode Trunk
/* 配置为 VTP 服务器 */
S1(config)#vtp mode Server
S1(config)#vtp domain sspu
S1(config)#vtp password 12345
/* 创建 3 个 VLAN */
S1(config)#VLAN 10
S1(config)#VLAN 20
S1(config)#VLAN 30
```

(2) 在交换机 S2 上配置 VTP 客户端

```
/* 定义 Trunk 链路 */
S2(config)#int f0/2
S2(config-if)#switchport mode Trunk
/* 配置为 VTP 客户端 */
S2(config)#vtp mode Client
S2(config)#vtp domain sspu
S2(config)#vtp password 12345
```

(3) 在交换机 S3 上配置 VTP 为 Transparent 模式

```
/* 定义两个 Trunk 链路 */
S3(config)#int range f0/1-2
S3(config-if-range)#switchport mode Trunk
/* 配置 VTP 为 Transparent 模式 */
S3(config)#vtp mode Transparent
S3(config)#vtp domain sspu
S3(config)#vtp password 12345
```

4. 检测结果及说明

(1) 在 S1(即 VTP 服务器)上查看 VLAN 信息:

```
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

(2) 在 S3(即 VTP Transparent 上)创建 VLAN 100,并查看 VLAN 信息:

```
S3#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
100  VLAN0100                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

可以看到,VTP 服务器中的 VLAN 10、20、30 均不存在,但自己创建的 VLAN 100 存在。

(3) 在 S2(即 VTP 客户端)上查看 VLAN 信息:

```
S2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, 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
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

可以看到,VTP 服务器中的 VLAN 10、20、30 都存在,但 S3(VTP Transparent)上创建的 VLAN 100 不存在。

在 S2 上试图创建 VLAN 200,被告知不允许:

```
S2(config)#vlan 200
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

以上实验结果验证了 VTP 协议的工作过程。

3.4 交换机的端口安全性

交换机端口的安全功能是指针对接入层交换机的端口进行安全属性的配置,从而控制用户的安全接入。

3.4.1 端口安全概述

交换机端口安全主要有两类:一类是限制交换机端口的最大连接数,另一类是针对交换机端口进行 MAC 地址、IP 地址的绑定。

限制交换机端口的最大连接数可以控制交换机端口下连的主机数,以防止用户进行恶意的 ARP 欺骗。

交换机端口可针对 MAC 地址、IP 地址、IP+MAC 地址进行灵活的绑定,从而实现对用户的严格控制,保证用户的安全接入,防止常见的内网中的网络攻击,如 ARP 欺骗、IP 地址和 MAC 地址欺骗、IP 地址攻击等。

1. 常见的攻击

在局域网内部,常常受到一些攻击,主要有以下几种形式:

(1) MAC 攻击。每秒发送成千上万个随机源 MAC 的报文,在交换机内部,大量广播包向所有端口转发,使 MAC 地址表空间很快就被不存在的源 MAC 地址占满,以致没有空间学习合法的 MAC 地址。

(2) ARP 的攻击。攻击者不断向对方计算机发送有欺诈性质的 ARP 数据包,数据包内含有与当前设备重复的 MAC 地址,使对方在回应报文时,由于简单的地址重复错误而导致不能进行正常的网络通信。一般情况下,受到 ARP 攻击的计算机会出现两种现象:

- 不断弹出"本机的×××段硬件地址与网络中的×××段地址冲突"的对话框。
- 计算机不能正常上网,出现网络中断的现象。

由于这种攻击是利用 ARP 请求报文进行"欺骗"的,防火墙会误认为这是正常的请求数据包,不予拦截,所以普通的防火墙很难抵御这种攻击。

(3) IP 地址和 MAC 地址欺骗:攻击者用网络盗用别人的 IP 地址和 MAC 地址,进行网络攻击。

端口安全的目的就是防止局域网的内部攻击对用户、网络设备所造成的破坏。

2. 端口安全功能

所谓端口安全,是指通过限制允许访问交换机上某个端口的 MAC 地址以及 IP 地址(可选)来实现对该端口输入的严格控制。当为安全端口(打开了端口安全功能的端口)配置了安全地址后,除了源地址为这些安全地址的报文之外,该端口将不转发其他任何报文。同时,可以将 MAC 地址和 IP 地址绑定起来作为安全地址,也可以通过限制端口上能包含的最大安全地址个数(如最大个数为 1),使连接这个端口的工作站(其地址为配置的安全地址)独享该端口的全部带宽。

交换机端口安全的基本功能如下:

(1) 限制交换机端口的最大连接数。

(2) 绑定端口的安全地址。例如,在端口上同时绑定 IP 和 MAC 地址,也可以防御

ARP 欺骗;在端口上绑定 MAC 地址,并限定安全地址数为 1,可以防恶意的 DHCP 请求。

```
Switch(config)#int f0/1
Switch(config-if)#switchport port-security  /* 打开该接口的端口安全功能 */
Switch(config-if)#switchport port-security maximum 1
/* 设置接口上安全地址的最大个数为 1,范围是 1~128,默认值为 128 */
Switch(config-if)#no switchport port-security maximum
/* 恢复接口安全地址的最大个数为默认值 */
Switch(config-if)#switchport port-security mac-address <mac-address>
[ip-address <ip-address>]
/* 手工配置接口上的安全地址(MAC 地址及 IP 地址) */
Switch(config-if)#no switchport port-security mac-address <mac-address>
/* 删除安全地址绑定 */
```

3. 安全违例的处理方式

在实际应用中,在配置了端口安全功能后,如果违反了端口安全,则将产生一个安全违例。对安全违例有 3 种处理方式:

(1) protect:当安全地址个数满后,安全端口将丢弃未知地址(不是该端口的安全地址中的任何一个)的数据包,这也是默认配置。

(2) restrict:当违反端口安全时,将发送一个 Trap 通知。

(3) shutdown:当违反端口安全时,将关闭端口并发送一个 Trap 通知。

有关安全违例的设置命令如下:

```
Switch(config-if)# switchport port-security violation {protect | restrict |
shutdown}
/* 设置处理违例的方式: protect 仅丢弃,restrict 丢弃且报警,shutdown 关机 */
Switch(config-if)#no switchport port-security violation
/* 将违例处理方式恢复为默认值 */
```

4. 配置端口的一些限制

配置端口安全时有如下一些限制:

(1) 安全端口不能是聚合端口,只能在 Access 链路端口上配置。

(2) 安全端口不能是 SPAN(Switched Port Analyzer,交换机端口分析器)的目标端口。

(3) 交换机最大连接数限制默认的处理方式是 protect。

(4) 端口安全和 IEEE 802.1x 认证端口是互不兼容的,不能同时启用。

(5) 安全地址有优先级,从低到高的顺序如下:

- 单 MAC 地址。
- 单 IP 地址/MAC 地址+IP 地址(后设置的地址生效)。

(6) 单个端口上的最大安全地址个数为 128 个。

(7) 在同一个端口上不能同时应用绑定 IP 的安全地址和安全 ACL,这两种功能是互斥的。

(8) 支持绑定 IP 地址的数量是有限制的。

5. 配置安全地址的老化时间

可以为一个接口上的所有安全地址配置老化时间。要设置系统 MAC 地址的老化时间,需要设置安全地址的最大个数,以便让交换机自动增加和删除接口上的安全地址。命令格式如下:

```
Switch(config-if)#switchport port-security aging {static | time<time>}
```

选项 static 表明老化时间将同时应用于手工配置的安全地址和自动学习的安全地址;若无 static,则老化时间只用于自动学习的安全地址。time 后指定这个端口上安全地址的老化时间,范围为 0～1440,单位为分,默认时间为 0。如果时间为 0,则表示关闭老化功能。老化时间是按绝对方式计时的,即当一个地址成为一个端口的安全地址后,经过指定的时间,这个地址将被自动删除。例如:

```
Switch(config)#interface f0/1
Switch(config-if)#switchport port-security aging static
Switch(config-if)#switchport port-security aging time 8
/*设置了 f0/1 接口安全地址的老化时间为 8min,且应用于手工配置的安全地址和自动学习的安全地址*/
Switch(config-if)#no switchport port-security aging time
/*关闭老化功能*/
Switch(config-if)#no switchport port-security aging static
/*老化时间仅用于自动学习的安全地址*/
```

6. 验证端口的安全性

(1) 显示接口的端口安全配置信息:

```
Switch#show port-security interface [interface-id]
```

(2) 显示安全地址信息:

```
Switch#show port-security address
```

(3) 显示某一接口的安全地址信息:

```
Switch#show port-security address [interface-id]
```

(4) 显示所有安全接口的统计信息:

```
Switch#show port-security
```

(5) 检查 MAC 地址表:

```
Switch#show mac-address-table
```

3.4.2 端口安全应用举例

1. 实验目的

(1) 理解交换机的端口安全性。

(2) 理解 MAC 地址表。

(3) 理解安全违例处理措施。

(4) 了解模拟非法接入及测试的方法。

2. 实验拓扑

实验拓扑如图 3-5 所示。

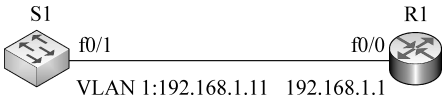


图 3-5　端口安全应用实验拓扑

3. 实验配置步骤

(1) 交换机的端口安全配置：

```
/*先关闭交换机的此端口*/
S1(config)#int f0/1
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
/*f0/1端口安全配置,0060.2FD3.7401是所连路由器的端口f0/0的MAC地址*/
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security max 1
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#switchport port-security mac-address 0060.2FD3.7401
/*实验中根据路由器的端口MAC地址而改变*/
/*再开启此端口*/
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
/*配置管理VLAN*/
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shutdown
```

(2) 路由器的配置：

```
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

4. 检测结果及说明

(1) 在路由器上 ping 交换机：

```
R1#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max=31/31/32 ms
```

(2) 在交换机上显示 MAC 地址表：

```
S1#show mac-address-table
        Mac Address Table
-------------------------------------
Vlan    Mac Address     Type        Ports
----    -----------  ---------  -----
1       0060.2fd3.7401  STATIC      Fa0/1
```

(3) 在交换机上显示端口的安全配置：

```
S1#show port-security int f0/1
Port Security: Enabled
Port Status: Secure-up
Violation Mode: Shutdown
Aging Time: 0 mins
Aging Type: Absolute
SecureStatic Address Aging: Disabled
Maximum MAC Addresses: 1
Total MAC Addresses: 1
Configured MAC Addresses: 1
Sticky MAC Addresses: 0
Last Source Address: Vlan: 0060.2FD3.7401: 1
Security Violation Count: 0
/*前面的行显示配置的参数,最后一行表明目前没有安全违例*/
```

(4) 在路由器上模拟对交换机端口的非法接入。

在路由器上修改 f0/0 端口的 MAC 地址为另一个地址：0018.0018.0018，模拟另一台设备接入到交换机的 f0/1 端口。

```
R1(config)#int f0/0
R1outer(config-if)#mac-address 0018.0018.0018
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
to down
```

在交换机上出现以下结果：

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
```

表明其 f0/1 端口已关闭。

(5) 在交换机上验证违例处理情况：

```
S1#show mac-address-table
  Mac Address Table
-------------------------------------------
Vlan    Mac Address     Type        Ports
----    -----------  ---------  -----
```

```
S1#show port-security int f0/1
Port Security: Enabled
Port Status: Secure-shutdown
Violation Mode: Shutdown
Aging Time: 0 mins
Aging Type: Absolute
SecureStatic Address Aging: Disabled
Maximum MAC Addresses: 1
Total MAC Addresses: 1
Configured MAC Addresses: 1
Sticky MAC Addresses: 0
Last Source Address: Vlan: 0018.0018.0018: 1
Security Violation Count: 1
/*最后一行表明已有一次安全违例*/
```

(6) 恢复交换机和路由器到正常情况：

```
S1(config)#int f0/1
S1(config-if)#shutdown
S1(config-if)#no shutdown
R1(config)#int f0/0
R1(config-if)#no mac-address
R1(config-if)#^Z
R1#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max=31/31/32 ms
```

如果没出现上面的信息，则可多次执行 ping 命令。

(7) 在交换机上验证效果(略)。

3.5　多层交换结构

多层交换网络都是通过交换机的端口相互连接，本节主要介绍交换机各种类型的端口和作用效果。

3.5.1　交换机、路由器之间的互连

二层交换机与三层交换机(或路由器)之间的连接方式主要采用 Access 端口(二层交换机属于同一 VLAN)、Trunk 端口(二层交换机属于多个 VLAN)和二层聚合端口(为增加带宽)。

三层交换机与三层交换机之间的连接方式主要采用 Access 端口(两台交换机属于同一 VLAN，相当于二层)、Trunk 端口(两台交换机属于不同的 VLAN，但要进行二层数据交

换)、路由端口(两台三层交换机连接不同网络,相互隔离广播)、二层聚合端口和三层聚合端口(为增加带宽)。

三层交换机与路由器之间的连接方式主要采用 Access 端口、Trunk 端口和路由端口。

交换机、路由器之间的互连拓扑结构示例如图 3-6～图 3-12 所示。

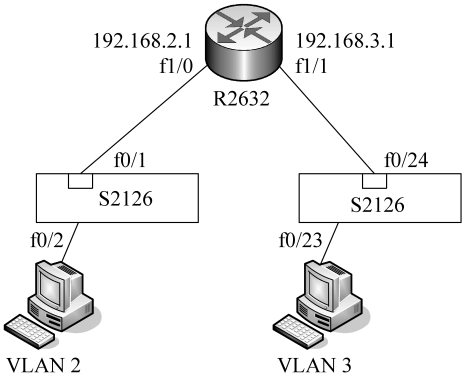


图 3-6　二层 Access 端口连接示例

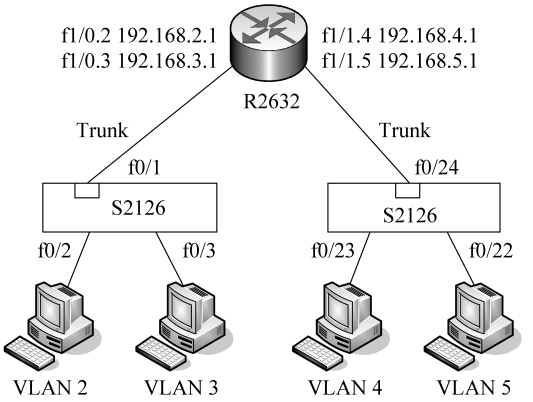


图 3-7　二层 Trunk 端口连接和单臂路由示例

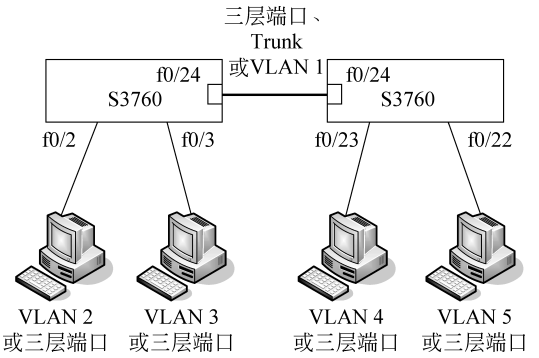


图 3-8　三层交换机之间的 3 种连接方式示例

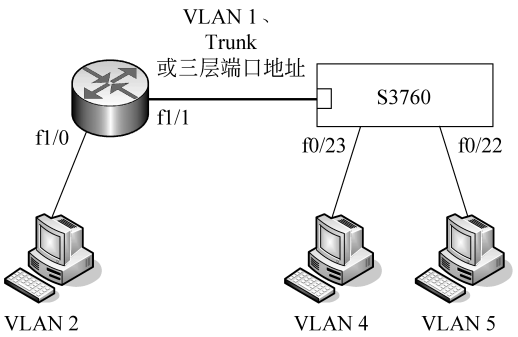


图 3-9　路由器与三层交换机之间的 3 种连接方式示例

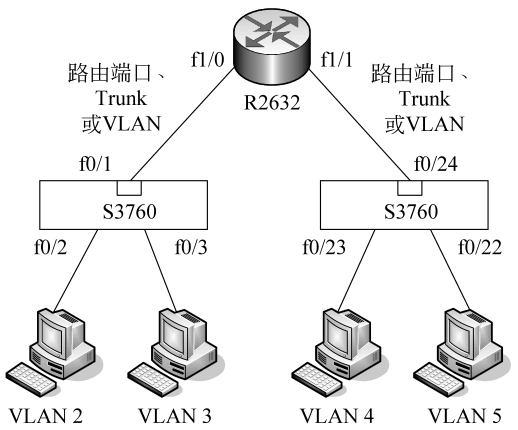


图 3-10　三层交换机与路由器之间的连接示例

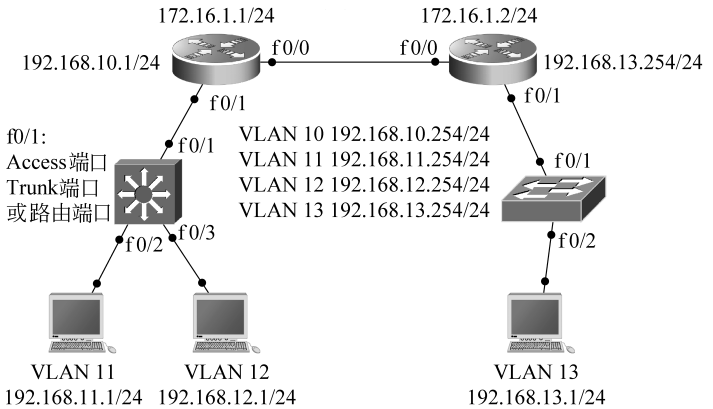


图 3-11　路由器与交换机之间的连接示例