第 12 章 交换机基本配置

交换机是局域网中最重要的设备，交换机是基于 MAC 来进行工作的。和路由器类似，交换机也有 IOS，IOS 的基本使用方法是一样的。本章将简单介绍交换机的一些基本配置，以及交换机独特的密码恢复、IOS 恢复步骤。关于 VLAN、Trunk 等将在后面章节介绍。

12.1 交换机简介

交换机是第二层的设备，可以隔离冲突域。交换机是基于收到的数据帧中的源 MAC 地址和目的 MAC 地址来进行工作。交换机的作用主要有这么两个：一个是维护 CAM（Context Address Memory）表，该表是 MAC 地址和交换机端口的映射表；另一个是根据 CAM 来进行数据帧的转发。交换机对帧的处理有三种：交换机收到帧后，查询 CAM 表，如果能查询到目的计算机所在的端口，并且目的计算机所在的端口不是交换机接收帧的源端口，交换机将把帧从这一端口转发出去（Forward）；如果该计算机所在的端口和交换机接收帧的源端口是同一端口，交换机将过滤掉该帧（Filter）；如果交换机不能查询到目的计算机所在的端口，交换机将把帧从源端口以外的其他所有端口上发送出去，这称为泛洪（Flood），当交换机接收到的是帧是广播帧或者多播帧，交换机也会泛洪帧。

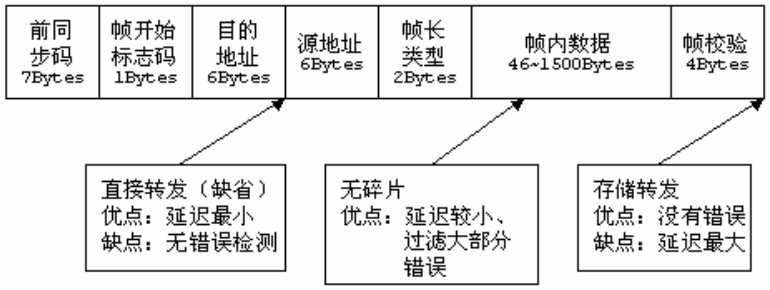

图 12-1 三种交换方式的比较

以太网交换机转发数据帧有三种交换方式，如图12-1：

（1） 存储转发（Store-and-Forward）

存储转发方式是先存储后转发的方式。它把从端口输入的数据帧先全部接收并存储起来；然后进行CRC（循环冗余码校验）检查，把错误帧丢弃；最后才取出数据帧目的地址，查找地址表后进行过滤和转发。存储转发方式延迟大；但是它可以对进入交换机的数据包进行高级别的错误检测。这种方式可以支持不同速度的端口间的转发。

（2） 直接转发（Cut-Through）

交换机在输入端口检测到一个数据帧时，检查该帧的帧头，只要获取了帧的目的地址，就开始转发帧。它的优点是：开始转发前不需要读取整个完整的帧，延迟非常小。它的缺点是：不能提供错误检测能力。

（3） 无碎片（Fragment-Free）

这是改进后的直接转发，是介于前两者之间的一种解决方法。无碎片方法在读取数据帧的长前64个字节后，就开始转发该帧。这种方式虽然也不提供数据校验，但是能够避免大多数的错误。它的数据处理速度比直接转发方式慢，但比存储转发方式快许多。

CISCO 交换机和路由器一样，本质上也是一台特殊的计算机，也有 CPU、RAM 等部件。也采用 IOS，所以交换机的很多基本配置（例如密码、主机名等）和路由器是类似的。

12.2 实验 1:交换机基本配置

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1） 熟悉交换机的基本配置

2. 实验拓扑

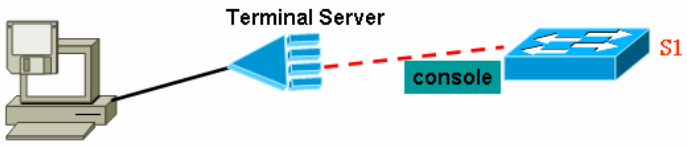

图 12-2 实验 1 拓扑图

3. 实验步骤

(1) 步骤 1：配置主机名

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
```

(2) 步骤 2：配置密码

```
S1(config)#enable secret cisco
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
```

(3) 步骤 3：接口基本配置

默认时交换机的以太网接口是开启的。对于交换机的以太网口可以配置其双工模式、速率等。

```
S1(config)#interface f0/1
switch(config-if)#duplex { full | half | auto }
```

//duplex 用来配置接口的双工模式，full——全双工、half——半双工、auto——自动检测双工的模式

```
switch(config-if)#speed { 10 | 100 | 1000 | auto }
```

//speed 命令用来配置交换机的接口速度，10——10M、100——100M、1000——1000M、auto——自动检测接口速度。

(4) 配置管理地址

交换机也允许被 telnet，这时需要在交换机上配置一个 IP 地址,这个地址是在 VLAN 接口上配置的。如下：

```
S1(config)#int vlan 1
S1(config-if)#ip address 172.16.0.1 255.255.0.0
S1(config-if)#no shutdown
S1(config)#ip default-gateway 172.16.0.254
```

//以上在 VLAN 1 接口上配置了管理地址，接在 VLAN 1 上的计算机可以直接进行 telnet 该地址。为了其他网段的计算机也可以 telnet 交换机，我们在交换机上配置了缺省网关。

(5)　保存配置

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

12.3 实验 2:交换机端口安全

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1）　理解交换机的 MAC 表

（2）　理解交换机的端口安全

（3）　配置交换机的端口安全特性

2. 实验拓扑

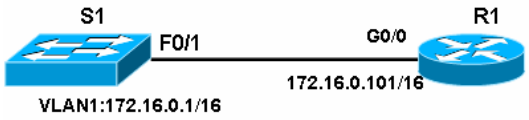

图 12-3　实验 2 拓扑图

3. 实验步骤

交换机端口安全特性，可以让我们配置交换机端口，使得非法的 MAC 地址的设备接入时，交换机自动关闭接口或者拒绝非法设备接入，也可以限制某个端口上最大的 MAC 地址数。我们这里限制 f0/1 接口只允许 R1 接入。

(1)　步骤 1：检查 R1 的 g0/0 接口的 MAC 地址

```
R1(config)#int g0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 172.16.0.101 255.255.0.0

R1#show int g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 0019.5535.b828 (bia 0019.5535.b828)
  //这里可以看到 g0/0 接口的 MAC 地址，记下它
  Internet address is 172.16.0.101/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
（此处省略）
```

(2)　步骤 2：配置交换机端口安全

```
S1(config)#int f0/1
S1(config-if)#shutdown
S1(config-if)#switch mode access
//以上命令把端口改为访问模式，即用来接入计算机，在下一章详细介绍该命令的含义。
S1(config-if)#switch port-securitiy
//以上命令是打开交换机的端口安全功能。
```

S1(config-if)#switch port-securitiy maximum 1
//以上命令只允许该端口下的 MAC 条目最大数量为 1，即只允许一个设备接入
S1(config-if)#switch port-securitiy violation { protect | shutdown | restrict }

- protect:当新的计算机接入时，如果该接口的 MAC 条目超过最大数量，则这个新的计算机将无法接入，而原有的计算机不受影响
- shutdown:当新的计算机接入时，如果该接口的 MAC 条目超过最大数量，则该接口将会被关闭，则这个新的计算机和原有的计算机都无法接入，需要管理员使用“no shutdown”命令重新打开。
- restrict:当新的计算机接入时，如果该接口的 MAC 条目超过最大数量，则这个新的计算机可以接入，然而交换机将向发送警告信息。

S1(config-if)#switchport port-security mac-address 0019.5535.b828
//允许 R1 路由器从 f0/1 接口接入
S1(config-if)#no shutdown

S1(config)#int vlan1
S1(config-if)#no shutdown
S1(config-if)#ip address 172.16.0.1 255.255.0.0
//以上配置交换机的管理地址
(3)　步骤 3：检查 MAC 地址表
S1#show mac-address-table

Mac Address Table

（此处省略）

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
1	0018.ba11.eb91	DYNAMIC	Fa0/15
1	**0019.5535.b828**	**STATIC**	**Fa0/1**

Total Mac Addresses for this criterion: 24
//R1 的 MAC 已经被登记在 f0/1 接口，并且表明是静态加入的
(4)　步骤 4：模拟非法接入
这时从 R1 ping 交换机的管理地址，可以 ping 通,如下：
R1#ping 172.16.0.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

在 R1 上修改 g0/0 的 MAC 地址为另一个地址，模拟是另外一台设备接入。如下：
R1(config)#int g0/0
R1(config-if)#mac-address 12.12.12
几秒钟后，则在 S1 上，出现：

```
01:09:39: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in
err-disable state
```

01:09:39: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0012.0012.0012 on port FastEthernet0/1.

01:09:40: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

//以上提示 f0/1 接口被关闭

S1#show int f0/1

FastEthernet0/1 is down, **line protocol is down (err-disabled)**

  Hardware is Fast Ethernet, address is 0018.ba11.f503 (bia 0018.ba11.f503)

  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

     reliability 255/255, txload 1/255, rxload 1/255

//以上表明 f0/1 接口因为错误而被关闭。非法设备移除后，在 f0/1 接口下，执行“**shutdown**”和“**no shutdown**”命令可以重新打开该接口。

4. 实验调试

S1#show port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	1	0	Shutdown

Total Addresses in System (excluding one mac per port)   : 0

Max Addresses limit in System (excluding one mac per port) : 6272

//以上可以查看端口安全的设置情况

12.4 实验 3:交换机的密码恢复

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1） 交换机的密码恢复步骤

2. 实验拓扑

如图 12-2。

3. 实验步骤

CISCO 交换机的密码恢复步骤和路由器的密码恢复方法差别较大，并且不同型号的交换机恢复方法也有所差异，以下是 Catalyst 3560（Catalyst 2950 也类似）交换机的密码恢复步骤。

（1） 拔掉交换机电源，按住交换机前面板的 Mode 键不放，接上电源，你会看到如下提示：

Base ethernet MAC Address: 00:18:ba:11:f5:00

Xmodem file system is available.

The password-recovery mechanism is enabled.

The system has been interrupted prior to initializing the

flash filesystem. The following commands will initialize
the flash filesystem, and finish loading the operating
system software:

flash_init
load_helper
boot

（2） 输入 **flash_init** 命令

```
Initializing Flash...
flashfs[0]: 3 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 6076928
flashfs[0]: Bytes available: 26437120
flashfs[0]: flashfs fsck took 12 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
Setting console baud rate to 9600...
```

（3） 输入 **load helper** 命令

（4） 输入 **dir flash:**

```
Directory of flash:/
2    -rwx  6073600   <date>              c3560-ipbasek9-mz.122-25.SEB4.bin
3    -rwx  1455      <date>              config.text
5    -rwx  24        <date>              private-config.text
26437120 bytes available (6076928 bytes used)
```

//config.text 就是交换机的启动配置文件，和路由器的 startup-config 类似

（5） 输入 **rename flash:config.text flash:config.old** 命令

//以上是把启动配置文件改名，这样交换机启动时就读不到 config.text 了，从而没有了密码。

（6） 输入 **boot** 命令引导系统，这时就不要再按住 mode 键了。

（7） 当出现如下提示时，输入 N：

Continue with the configuration dialog? [yes/no] : n

（8） 用 **enable** 命令进入 enable 状态，并将文件 config.old 改回 config.text，命令如下：

rename flash:config.old flash:config.text

（9） 将原配置装入内存，命令如下：

Switch# **copy flash:config.text system:running-config**

（10） 修改各个密码：

```
S1#conf t
S1(config)#enable secret cisco
S1(config)#exit
```

（11） 将配置写入 nvram

```
S1#copy running-config start-config
```

12.5 实验 4：交换机的 IOS 恢复

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1） 交换机的 IOS 恢复

2. 实验拓扑

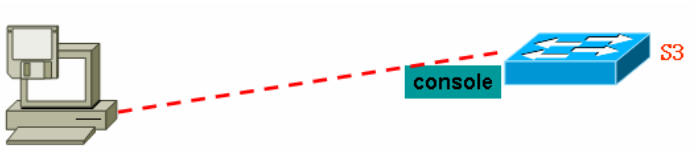

图 12-4 实验 4 拓扑图

3. 实验步骤

交换机如果已经正常开机，则 IOS 可以从 TFTP 服务器上恢复，具体步骤请参见路由器的 IOS 恢复步骤。然而如果交换机无法正常开机，IOS 的恢复要使用 XModem 方式，该方式是通过 concole 口从计算机下载 IOS，速度为 9600bps，因此速度很慢。步骤如下：

(1) 把计算机的串口和交换机的 console 口连接好，用超级终端软件连接上交换机

(2) 交换机开机后，执行以下命令：

switch: **flash_init**

switch: **load_helper**

(3) 输入拷贝指令：

switch:**copy xmodem: flash:c2950-i6q412-mz.121-22.EA5a.bin**

该命令的含义是通过 xmodem 方式拷贝文件，保存在 FLASH，文件名为 c2950-i6q412-mz.121-22.EA5a.bin。出现如下提示：

Begin the Xmodem or Xmodem-1K transfer now...

CCCC

在超级终端窗口中，选择【传送】→【传送文件】菜单，打开图 12-5 窗口，选择 IOS 文件，协议为“Xmodem”。点击“发送”按钮开始发送文件。由于速度很慢，请耐心等待，通信速率为 9600bps。

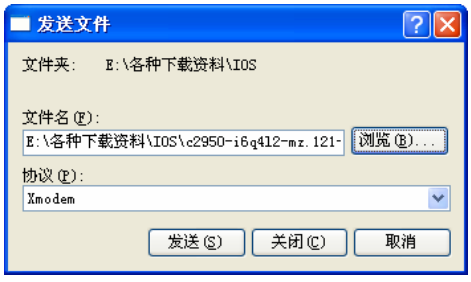

图 12-5 选择 IOS 文件

(4) 传送完毕后执行以下命令：

switch:**boot**

启动系统。

12.6 本章小结

本章简要介绍了交换机的基本配置，交换机的许多配置和路由器很类似。然而交换机的密码恢复和 IOS 恢复方法却和路由器有较大差别。为了减少非法设备的接入，可以在交换机上配置端口安全特性。表 12-1 是本章出现的命令。

表 12-1 本章命令汇总

命令	作用
duplex { full | half | auto }	配置以太口的双工属性
speed { 10 | 100 | 1000 | auto }	配置以太口的速率
ip default-gateway 172.16.0.254	配置缺省网关
switch mode access	把端口改为访问模式
switch port-securitiy	打开交换机的端口安全功能
switch port-securitiy maximum 1	允许该端口下的 MAC 条目最大数量为 1
switch port-securitiy violation { protect | shutdown | restrict }	配置交换机端口安全
switchport port-security mac-address 0019.5535.b828	允许 MAC 为 0019.5535.b828 的设备接入本接口
show mac-address-table	显示 MAC 地址表
mac-address 12.12.12	改变接口的 MAC 地址
rename flash:config.text flash:config.old	把 flash 中的文件改名
copy xmodem: flash:c2950-i6q4l2-mz.121-22.EA5a.bin	通过 Xmodem 模式把文件拷贝到 flash 中
boot	重启交换机