目　录

项目一　交换机配置基础

任务 1　交换机的初始化配置

【学习情境】

你是某公司的网络管理员，现在新买了一台二层交换机，需要安装在某个车间，要对其进行初始化配置，配置的内容包括：终端密码（控制台 Console 口）、虚拟终端密码（远程登录密码）、用户特权密码、管理地址以及默认网关。

【学习目的】

1. 能对交换机进行初始化配置的拓扑搭建与正确连线。
2. 能正确使用 PC 的超级终端，会配置交换机名称与控制台密码。
3. 会配置和验证交换机的远程登录密码。
4. 会配置和验证交换机的特权密码（加密和非加密两种方式）。
5. 会配置交换机的管理地址与默认网关。
6. 会配置 PC 的网卡地址与默认网关。
7. 会保存配置命令、配置文件和提交作业。

【相关设备】

二层交换机 1 台、PC1 台、交换机配置线 1 根、直连线 1 根。

【实验拓扑】

拓扑如图 1-1-1 所示。

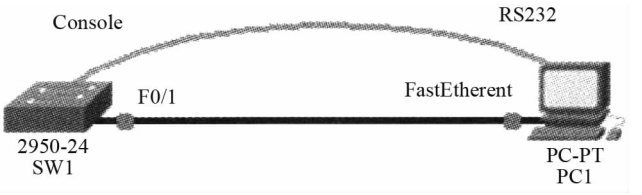

图 1-1-1　实验拓扑搭建示意图

【实验任务】

1. 先通过配置线进行网络拓扑搭建（图 1-1-2），指定相关端口（Console 和 RS232），并进行正确连线，对交换机和 PC 进行名称标注。

图 1-1-2　网络拓扑搭建示意图

2. 通过 PC 的超级终端（开始—程序—附件—通信—超级终端）进入交换机（图 1-1-3），配置交换机名为 SW2950。如果是模拟器，超级终端截图如图 1-1-4 所示。

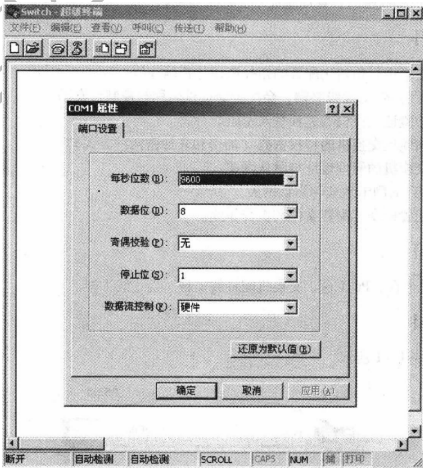

图 1-1-3　SW2950 交换机超级终端截图

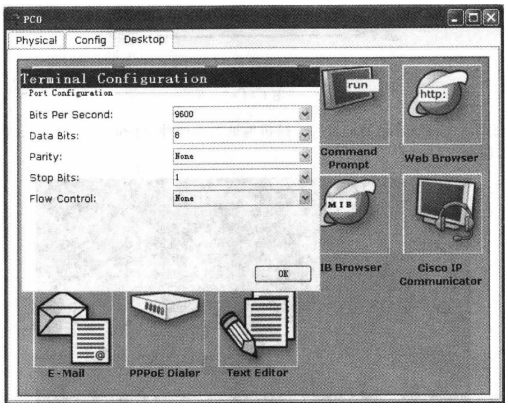

图 1-1-4　模拟器超级终端截图

3. 设置交换机的控制台密码为 123456。退出到用户模式，退出超级终端，重新进入，验证控制台密码的有效性（图 1-1-5）。

图 1-1-5　交换机超级终端登陆界面

4. 设置交换机的特权密码（非加密）为 swpassword，特权密码（加密）为 swsecret，注意当两种密码同时设置时，加密的密码有效，非加密的变为无效。退出到用户模式，再进入特权模式并验证特权密码的有效性（图 1-1-6）。

图 1-1-6　特权模式登陆界面

5. 配置交换机的管理 IP 为 192.168.0.10/24，配置交换机的默认网关为 192.168.0.254。

6. 设置交换机的远程登录密码为 abcdef。

7. 配置 PC1 的 IP 为 192.168.0.1/24，默认网关为 192.168.0.254。

8. 如图 1-1-7 所示，删除配置线，用直连线将交换机和 PC 连接，注意端口（F0/1 和网卡）的变化。

图 1-1-7　PC 与交换机直连线连接图

在 PC1 上测试自己的地址和交换机地址的连通性（ping 命令），一定要调通，如图

1-1-8所示。

```
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=16ms TTL=128
Reply from 192.168.0.1: bytes=32 time=15ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 7ms

PC>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:

Reply from 192.168.0.10: bytes=32 time=31ms TTL=255
Reply from 192.168.0.10: bytes=32 time=28ms TTL=255
Reply from 192.168.0.10: bytes=32 time=31ms TTL=255
Reply from 192.168.0.10: bytes=32 time=31ms TTL=255

Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 31ms, Average = 30ms

PC>
```

图 1-1-8　交换机连通图

再使用 telnet 命令远程登录交换机，测试远程登录密码，如图 1-1-9 所示。

```
PC>telnet 192.168.0.10
Trying 192.168.0.10 ...


User Access Verification

Password:
```

图 1-1-9　远程登陆交换机界面

9. 保存交换机的当前配置到启动配置中，确保重新启动配置不会丢失。

10. 最后把配置文件以及测试结果截图打包，以“学号姓名”为文件名，提交作业。

【实验命令】

1. 查看交换机的版本和当前配置

```
showversion
showrunning-config
```

2. 配置交换机的名称

```
Switch>
Switch>enable
Switch#configureterminal
Switch (config) #hostnameSW2950
SW2950 (config) #
```

3. 配置交换机的终端密码（控制台 Console 口密码）

```
SW2950>
SW2950>enable
SW2950#configureterminal
SW2950 (config) #lineconsole0
SW2950 (config-line) #password123456
SW2950 (config-line) #login
SW2950 (config-line) #exit
SW2950 (config) #
```

4. 设置用户特权密码

```
SW2950>
SW2950>enable
SW2950#configureterminal
SW2950 (config) #enablepasswordswpassword     （非加密）
SW2950 (config) #enablesecretswsecret     （加密）
```

5. 配置交换机的虚拟终端密码（远程登录密码，Vty 口密码。交换机为 15 级，路由器为 4 级）

```
SW2950>
```

```
SW2950＞enable
SW2950＃configureterminal
SW2950（config）＃linevty015
SW2950（configline）＃passwordabcdef
SW2950（config-line）＃login
SW2950（config-line）＃exit
SW2950（config）＃
```

6. 查看交换机的 MAC 地址表

```
SW2950＃showmac-address-table
```

7. 配置交换机的管理地址和默认网关

```
SW2950＞
SW2950＞enable
SW2950＃configureterminal
SW2950（config）＃interfaceVLAN1
SW2950（config-VLAN）＃ipaddress192.168.0.10255.255.255.0
SW2950（config-VLAN）＃noshutdown
SW2950（config-VLAN）＃exit
SW2950（config）＃ipdefault-gateway192.168.0.254
SW2950（config）＃
```

8. 保存当前配置文件

```
SW2950＃copyrunning-configstartup-config
SW2950＃writememory
```

【注意事项】

1. 确定自己设定的密码都正确，如果进不去，有可能你的输入法处于输入汉字状态，可以用＜Ctrl＋空格＞关闭输入法，再重试。

2. 在实验中出现问题的时候多使用命令 showrunning-config 来观看配置信息。

【配置结果】

```
SW2950＃showrunning-config：
```

```
Building configuration...
Current configuration:1046 bytes
version 12.1
no service password-encryption
hostname sw2950
enable secret 5 $1$mERr$SX1DdzJ6XG4NClAaR9JWv1
enable password swpassword
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface vlan1
ip address 192.168.0.10 255.255.255.0
ip default-gateway 192.168.0.254
line con 0
 password 123456
 login
line vty 0 4
 password abcdef
 login
line vty 0 15
password abcdef
 login
end
```

【技术原理】

1. 两大类主要的交换机的访问方式

（1）带外管理：通过带外对交换机进行管理（PC 与交换机直接相连）。

（2）带内管理：通过 Telnet 对交换机进行远程管理，通过 Web 对交换机进行远程管理，通过 SNMP 工作站对交换机进行远程管理。

2. 六种主要的交换机配置命令模式

（1）用户模式 Switch＞。

（2）特权模式 Switch＃。

（3）全局模式 Switch（config）＃。

（4）端口模式 Switch（config-if）＃。

（5）VLAN（虚拟局域网）配置模式 Switch（confg-vlan）＃。

（6）线路配置模式 Switch（config-line）＃。

3. 命令行的常用快捷键及其功能

（1）?：获取命令帮助；

（2）tab：将简写的命令补填完整；

（3）Ctrl＋P 或上方向键：调出最近（前一）使用过的命令；

（4）Ctrl＋N 或下方向键：调出更近用过的命令；

（5）Ctrl＋A：光标移动到命令行的开始位置；

（6）Ctrl＋E：光标移动到命令行的结束位置；

（7）Esc＋B：回移一个单词；

（8）Ctrl＋F：下移一个字符；

（9）Ctrl＋B：回移一个字符；

（10）Esc＋F：下移一个单词；

（11）Ctrl＋D：删除当前字符；

（12）Ctrl＋Shift＋6：终止一个进程。

4. 交换机的硬件结构（图 1-1-10）

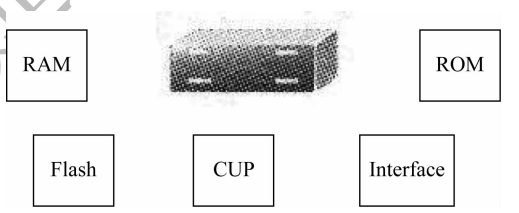

图 1-1-10　交换机的硬件结构

（1）Flash（闪存）：交换机操作系统（RCNOS）、配置文件（config. text）。

（2）RAM（随机存储器）：交换机当前运行的配置（running-config）。

（3）ROM（只读存储器）：MiniOS、BootStart。

5. 配置文件的管理

（1）保存配置：将当前运行的参数保存到 Flash 中，用于系统初始化时初始化参数。

```
Switch＃copyrunning-configstartup-config
```

```
Switch#writememory
Switch#write
```

（2）删除配置：永久性地删除 Flash 中不需要的文件。

使用命令 deleteflash：config.text

（3）删除 Vlan 数据库：永久性地删除 Flash 中 Vlan 数据库文件。

使用命令 deleteflash：vlan.dat

（4）查看配置文件内容。

```
Switch#moreflash：config.text
Switch#showconfigure
Switch#showrunning-config
```

任务 2　交换机 VLAN 划分

【学习情境】

你是某公司的网络管理员，现在新买了一台二层交换机，需要安装在销售部门，其中 PC1 和 PC2 为同一个销售小组，PC3 是一个独立的销售小组，要求同小组的 PC 之间可以相互通信，不同小组的 PC 之间不能通信。要对其进行配置，配置的内容包括：终端密码（控制台 Console 口）、虚拟终端密码（远程登录密码）、用户特权密码、管理地址以及默认网关、VLAN 划分。

【学习目的】

1. 能对交换机进行拓扑搭建与正确连线。
2. 复习和巩固交换机多种管理密码的配置。
3. 了解交换机 VLAN 的原理、作用和多种方式。
4. 学会配置 VLAN 和验证 VLAN 的效果。

【相关设备】

二层交换机 1 台、PC4 台、交换机配置线 1 根、直连线 4 根。

【实验拓扑】

拓扑如图 1-2-1 所示。

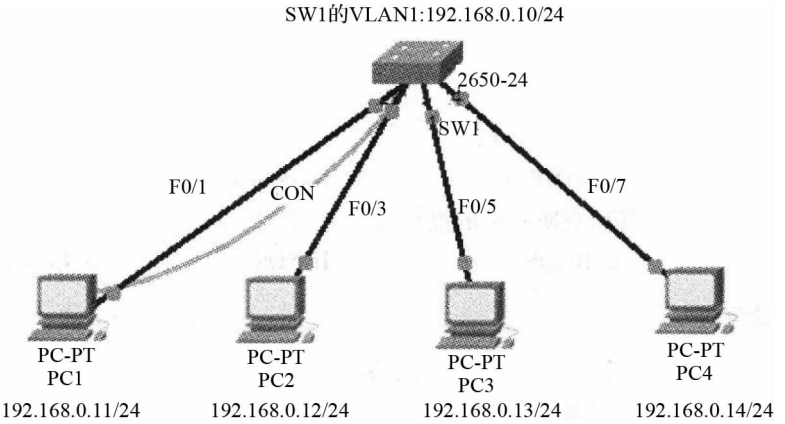

图 1-2-1　实验拓扑搭建示意图

【实验任务】

1. 进行网络拓扑搭建，将 4 台 PC 分别连在交换机的 F0/1、F0/3、F0/5、F0/7 口上，交换机 Console 口接到 PC1 的 RS232 口上。对交换机和 PC 进行名称标注、地址设置（包括子网掩码）。

2. 配置 PC 的 IP。PC1：192.168.0.11；PC2：192.168.0.12；PC3：192.168.0.13；PC4：192.168.0.14；子网掩码均为 255.255.255.0，网关均为 192.168.0.254。测试 4 台 PC 之间的互通情况（结果应该是全通）。

3. 配置交换机。名为 SW1，管理 IP 为 192.168.0.10/24，网关为 192.168.0.254。控制台密码为 network，远程登录密码为 rjxy，特权密码为 wjxvtc。测试交换机与 4 台 PC 之间的互通情况（结果应该是全通）。

4. 在交换机上创建 VLAN2 和 VLAN3，并按如下要求进行划分。VLAN2 包含 F0/1～F0/4 口（即包含 PC1、PC2），VLAN3 包含 F0/5 口（即包含 PC3），结果如图 1-2-2 所示。

```
SW1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    F0/6, F0/7, F0/8, F0/9
                                                 F0/10, F0/11, F0/12, F0/13
                                                 F0/14, F0/15, F0/16, F0/17
                                                 F0/18, F0/19, F0/20, F0/21
                                                 F0/22, F0/23, F0/24
2    VLAN0002                          active    F0/1, F0/2, F0/3, F0/4
3    VLAN0003                          active    F0/5
```

图 1-2-2　VLAN2 和 VLAN3 创建划分示意图

5. 测试交换机、4 台 PC 之间的互通情况，验证 VLAN 的功能（结果应该 PC1 与 PC2 互通，PC4 与交换机互通，其他都不通）。

6. 删除 VLAN3，注意要先把 F0/5 释放回 VLAN1 再删除。再测试 PC3 与其他设备的通信情况（应该是 PC3 可以与 PC4、交换机互通，与 PC1、PC2 不通）。

7. 最后把配置以及测试结果截图打包，以“学号姓名”为文件名，提交作业。

【实验命令】

1. 创建 VLAN

```
SW1#vlandatabase
SW1 (vlan) #vlan2
SW1 (vlan) #exit
SW1#
SW1 (config) #vlan2
SW1 (config-vlan) #exit
SW1 (config) #
```

2. 查看 VLAN

```
SW1#showvlan
```

3. 划分 port-vlan

```
SW1 (config) #interface  FastEthernet0/5
SW1 (config-if) #switchportaccessvlan3
SW1 (config) #interfacerangeFastEthernet0/1-4
SW1 (config-if-range) #switchportaccessvlan2
```

4. 删除 VLAN

```
SW1 (config) #interface FastEthernet0/5
SW1 (config-if) #switchportaccessvlan1
SW1 (config-if) #end
SW1#VLANdatabase
SW1 (VLAN) #novlan3
```

【注意事项】

1. 注意交换机的提示符状态，不同情况下做的命令和事情是不一样的。如下面的错误情况（本想创建完 VLAN3，再把 F0/5 口加入），请分析原因。

```
SW1#vlandatabase
SW1 (VLAN) #vlan3
SW1 (VLAN) #interface FastEtharnet0/5 此时发现命令错误
SW1 (config-if) #switchportaccessvlan3
```

2. 如果发现 PC1 已经不能对交换机进行远程登录了，那是因为 PC1 和交换机的 IP 不在

同一个 VLAN 中。可以把交换机的 Console 口配置线移至 PC4 的 RS232 口上进行远程登录。

【配置结果】

SW1 # showrunning-config：

```
Building configuration...
Current configuration:1154 bytes
version 12.1
no service password-encryption
hostname SW1
enable password wjxvtc
interface FastEthernet0/1
  switchport access vlan 2
switchport mode access
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
```

```
Building configuration...
Current configuration:1154 bytes
version 12.1
no service password-encryption
hostname SW1
enable password wjxvtc
interface FastEthernet0/1
  switchport access vlan 2
switchport mode access
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
interface FastEthernet0/3
  switchport access vlan 2
  switchport mode access
interface FastEthernet0/4
  switchport access vlan 2
  switchport mode access
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface vlan1
  ip address 192.168.0.10 255.255.255.0
line con 0
password network
  login
line vty 0 4
  password rjxy
  login
line vty 5 15
  password rjxy
  login
end
```

【技术原理】

1. VLAN（Virtual Local Area Network），翻译成中文是“虚拟局域网”

VLAN 是在一个物理网络上划分出来的逻辑网络。这个网络对应于 OSI 模型的第二层网络。VLAN 的划分不受网络端口的实际物理位置的限制。VLAN 有着和普通物理网络同样的属性。第二层的单播帧、广播帧和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。

广播域的概念：广播域，指的是广播帧（目标 MAC 地址全部为 1）所能传递到的范围，即能够直接通信的范围。严格地说，并不仅是广播帧，多播帧（MulticastFrame）和目标不明的单播帧（UnknownUnicastFrame）也能在同一个广播域中畅行无阻。

本来二层交换机只能构建单一的广播域，不过使用 VLAN 功能后，VLAN 通过限制广播帧转发的范围分割了广播域，这样就将网络分割成多个广播域。

2. 交换机的端口的两种模式

（1）访问链接（AccessLink）。

（2）汇聚链接（TrunkLink）。

设定访问链接的方法可以是事先固定的，也可以是根据所连的计算机而动态改变设定。前者称为“静态 VLAN”，后者则称为“动态 VLAN”。

3. VLAN 的种类

（1）静态 VLAN（基于端口的 VLAN）：将交换机的各端口固定指派给 VLAN（一个端口只属于一个 PortVLAN）。

（2）基于 MAC 地址的动态 VLAN：根据各端口所连计算机的 MAC 地址设定。

（3）基于子网的动态 VLAN：根据各端口所连计算机的 IP 地址设定。

（4）基于用户的动态 VLAN：根据端口所连计算机上的登录用户设定。

任务 3　跨交换机实现相同 VLAN 互通

【学习情境】

你是某公司的网络管理员，现在 PC1 和 PC3 都是财务部的电脑，是处于不同的楼层中的不同交换机上，但要实现它们的相互通信；PC2 是销售部的电脑，虽然和财务部的 PC1 处于同一台交换机上，但要限制它们不能通信，需要对同一广播域进行隔离。

【学习目的】

1. 掌握 TagVLAN 的功能和作用。

2. 掌握 IEEE802.1Q 的技术原理。

3. 理解 Trunk 连接与普通连接的区别和作用。

4. 会对跨交换机之间的 VLAN 实现互通。

【相关设备】

二层交换机 2 台、PC3 台、直连线 3 根、交叉线 1 根。

【实验拓扑】

拓扑如图 1-3-1 所示。

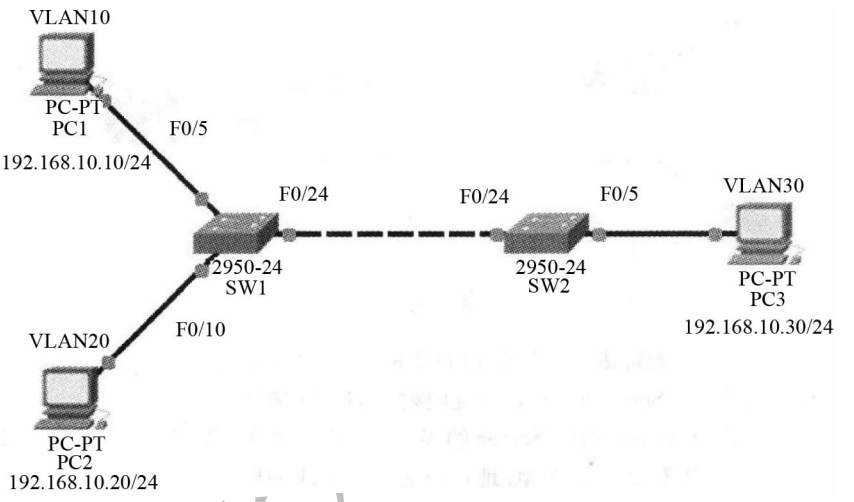

图 1-3-1　实验拓扑搭建示意图

【实验任务】

1. 进行网络拓扑搭建，将 PC1 连接在 SW1 的 F0/5 口上，将 PC2 连接在 SW1 的 F0/10 口上，将 PC3 连接在 SW2 的 F0/5 口上。SW1 与 SW2 之间通过 F0/24 日用交叉线相连。

2. 配置 3 台 PC 的地址、子网掩码，默认网关都是 192.168.10.254。测试结果：PC1、PC2、PC3 都能互通，这是实验的基础，必须全通。

3. 在 SW1 和 SW2 上分别创建 VLAN10 和 VLAN20，并把 SW1 和 SW2 的 F0/5 口放入 VLAN10 中，把 SW1 上的 F0/10 口放入 VLAN20 中。测试结果：PC1、PC2、PC3 都不能互通。

4. 2 台交换机的连接口配置 Trunk 模式，形成干线，实现不同交换机之间的相同 VLAN 可以互通。测试结果：PC1 能与 PC3 互通，而 PC2 与 PC1、PC3 不通。

5. 再把 PC3 放到 VLAN20，观察互通的情况。测试结果：PC1 与 PC2、PC3 不通，而 PC2 与 PC3 互通。

6. 最后把配置以及 ping 的结果截图打包，以“学号姓名”为文件名，提交作业。

【实验命令】

1. 建立 VLAN 的另一种方式（全局模式下创建）

```
Switch>enable
Switch#configureterminal
SW1 (config) #vlan10
SW1 (config-vlan) #exit
SW1 (config) #vlan20
SW1 (config-vlan) #exit
SW1 (config) #
```

2. 2 台交换机的连接口配置 Trunk 模式

```
SW1 (config) #interfaceFastEthernet0/24
SW1 (config-if) #switchportmodetrunk
SW2 (config) #interfaceFastEthernet0/24
SW2 (config-if) #switchportmodetrunk
```

【注意事项】

1. 一般情况下，相同设备之间用交叉线连接，不同设备之间用直连线连接。如图 1-3-1 中的 SW1 与 SW2 之间通过 F0/24 口用交叉线相连。

2. 交换机配置 Trunk 模式时，两个相关的交换机互连端口都要进行配置，单方配置 Trunk 是没有作用的。

3. 有时为了更好地观察实验的效果，在 ping 命令中可以加 t 参数。如 PC1 对 PC3 进行 ping 的时候：ping192. 168. 10. 30-t（或 ping-t192. 168. 10. 30）。

【配置结果】

1. SW1#showvlan

```
VLAN    Name            Status    Ports
----    --------------- --------  -------------------------------
1       default         active    F0/1,F0/2,F0/3,F0/4
                                  F0/6,F0/7,F0/8,F0/9
                                  F0/11,F0/12,F0/13,F0/14
                                  F0/15,F0/16,F0/17,F0/18
                                  F0/19,F0/20,F0/21,F0/22
                                  F0/23,F0/24
10      VLAN0010        active    F0/5,F0/24
20      VLAN0020        active    F0/10,F0/24
```

2. SW1 # showrunning-config

```
Building configuration...
Current configuration:941 bytes
version 12.1
no service password-encryption
hostname Switch1
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
  switchport access vlan 10
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
switchport access vlan 20
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
```

```
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
  switchport mode trunk
interface Vlan1
  no ip address
  shutdown
line con 0
line vty 0 4
  login
line vty 5 15
  login
end
```

【技术原理】

1. 设置跨越多台交换机的 VLAN

前面学习的都是使用单台交换机设置 VLAN 时的情况。那么，如果需要设置跨越多台交换机的 VLAN 时又如何呢？在规划企业级网络时，很有可能会遇到隶属于同一部门的用户分散在同一座建筑物中的不同楼层的情况，这时可能就需要考虑如何跨越多台交换机设置 VLAN 的问题了。

为了避免这种低效率的连接方式，人们想办法让交换机间互联的网线集中到一根上，这时使用的就是汇聚链接（TrunkLink）的方法。

汇聚链接（TrunkLink）指的是能够转发多个不同 VLAN 通信的端口。汇聚链路上流通的数据帧都被附加了用于识别分属于哪个 VLAN 的特殊信息（TagVLAN），如图 1-3-2 所示。

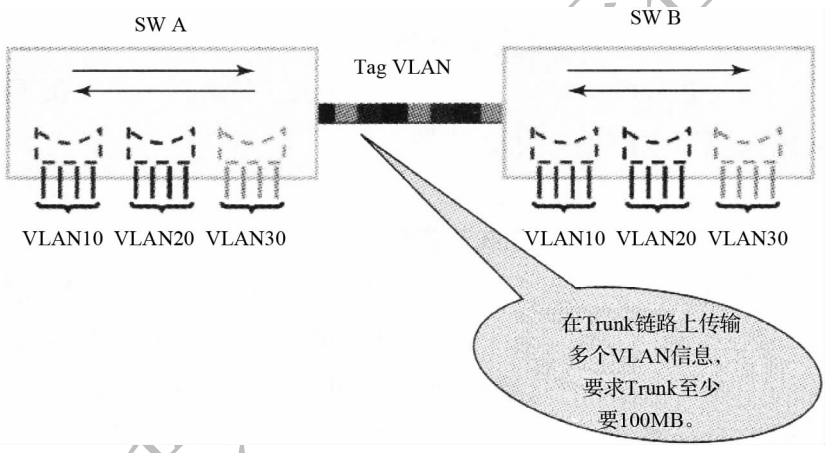

图 1-3-2　汇聚链接示意图

通过汇聚链路时附加的 VLAN 识别信息，就要支持标准的“IEEE802.1Q”协议。基于 IEEE802.IQ 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（TaggingVLAN）”。

（1）传输多个 VLAN 的信息。

（2）实现同一 VLAN 跨越不同的交换机。

2. IEEE802.10 数据帧

IEEE802.1Q，俗称“DotOneQ”，是经过 IEEE 认证的对数据帧附加 VLAN 识别信息的协议。

IEEE802.1Q 所附加的 VLAN 识别信息位于数据帧中“发送源 MAC 地址”与“类别域（Type23Field）”之间。具体内容为 2 字节的 TPID 和 2 字节的 TCI，共计 4 字节，如图 1-3-3 所示。

目的，源MAC地址	2字节标记协议标识 2字节标记控制信息	类型，数据	重新计算帧检测序列

图 1-3-3　数据帧中的内容

在数据帧中添加了 4 字节的内容，那么 CRC 值自然也会有所变化。这时数据帧上的 CRC 是插入 TPID、TCI 后，对包括它们在内的整个数据帧重新计算后所得的值。而当数据帧离开汇聚链路时，TPID 和 TCI 会被去除，这时还会进行一次 CRC 的重新计算。

（1）标记协议标识（TPID）：周定值 Ox8100，表示该帧载有 802.1Q 标记信息。

（2）标记控制信息（TCI）：

Priority：3 比特表示优先级。

Canonicalformatindicator：1 比特用于总线型以太网、FDDI、令牌环网。

VlanID：12 比特表示 VID，范围 1～4094。

任务 4　利用三层交换机路由功能实现不同 VLAN 互通

【学习情境】

一个公司或单位的局域网中，进行 VLAN 的划分是为了防止病毒的传播和相同部门的隔离，提高安全性，可是最终要都实现全部互通，以保证局域网内的互联功能，所以，不仅要实现相同 VLAN 的互通，也要实现不同 VLAN 的互通。

【学习目的】

1. 掌握在三层交换机上配置 SVI 口（交换虚拟接口）的方法。
2. 掌握三层交换机上直连路由的形成原理。
3. 了解路由的作用和掌握查看路由表的方法。

【相关设备】

三层交换机 1 台、二层交换机 2 台、PC2 台、直连线 2 根、交叉线 2 根。

【实验拓扑】

拓扑如图 1-4-1 所示。

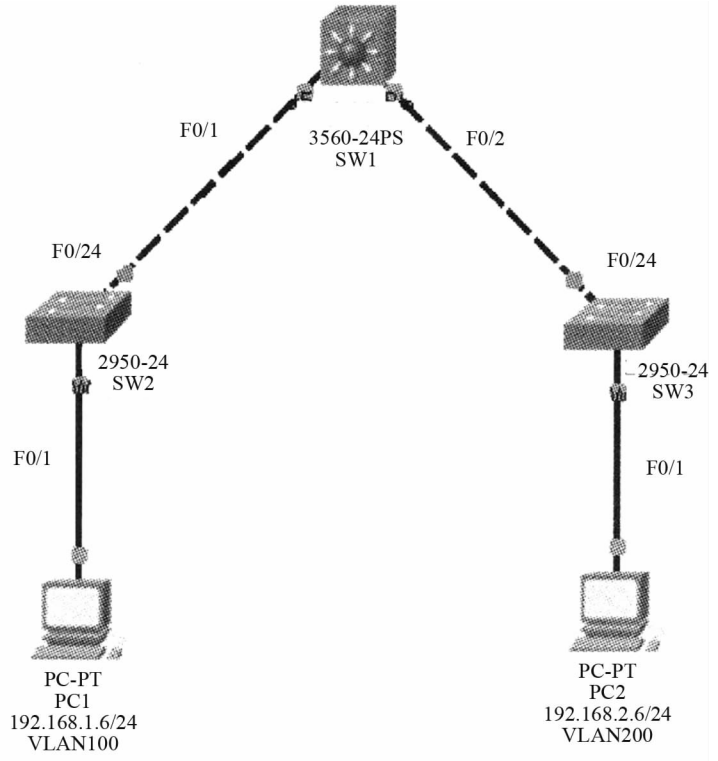

图 1-4-1　数据帧中的内容

【实验任务】

1. 如图 1-4-1 所示，搭建网络拓扑，PCI 的 IP 是 192.168.1.6/16，网关 192.168.1.254；PC2 的 IP 为 192.168.26/16，网关 192.168.2.254；子网掩码都是 255.255.0.0，测试 2 台 PC 的通信情况（互通）。

2. 设置交换机的提示符名分别为 SW1（三层）和 SW2、SW3。

3. 配置二层交换机，分别在 2 个二层交换机上创建 VLAN100 和 VLAN200，并将 PC1 移入 VLAN100，PC2 移入 VLAN100。测试 2 台 PC 的通信情况（不通）。

4. 在三层交换机 SW1 上设置 VLAN100 和 VLAN200，在交换机间启用 Trunk 链路，保证 VLAN 能够实现跨越交换机的通信。测试 2 台 PC 的通信情况（互通）。

5. 如图 1-4-2 所示，改建网络拓扑，PC1 仍为 VIAN100，PC2 移入 VLAN200。测试 2 台 PC 的通信情况（不通）。

6. 配置三层交换机，为 SVI 口（交换虚拟接口）配置 IP 地址，VIAN100：192.168.1.254，VLAN200：192.168.2.254，子网掩码都是 255.255.255.0，实现直连路由功能。2 个 PC 的子网掩码也要改成 255.255.255.0，要与默认网关的子网掩码一致，路由才能起作用，最终实现 PC1 和 PC2 相互通信。

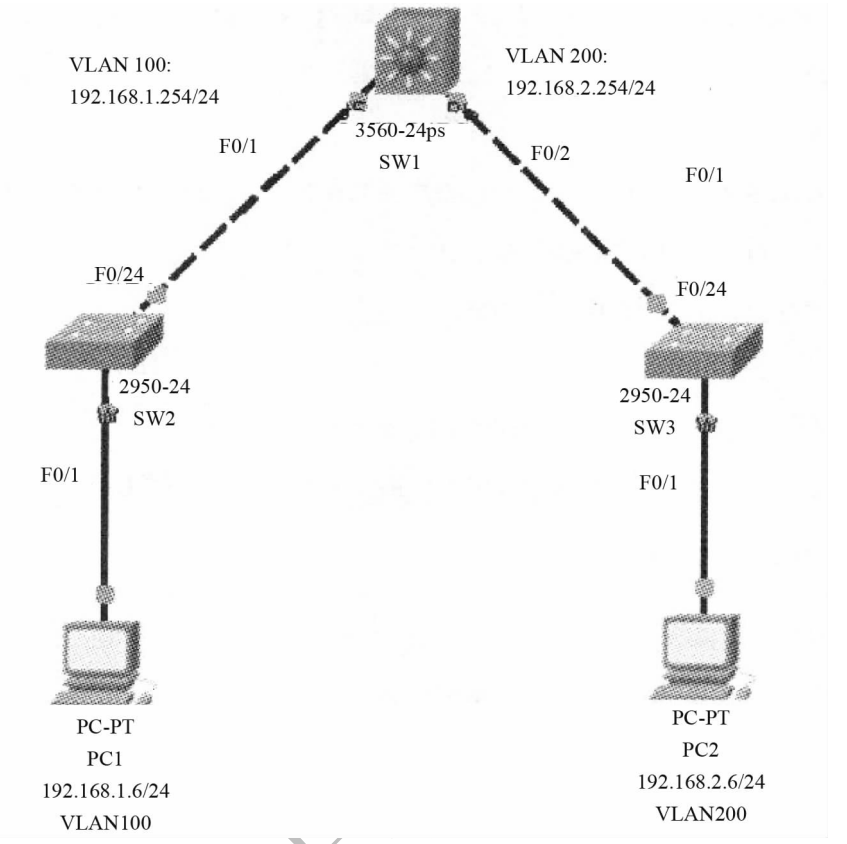

图 1-4-2　改建网络拓扑图

7. 最后把配置以及 ping 的结果截图打包，以“学号姓名”为文件名，提交作业。

【实验命令】

1. SVI 口（交换虚拟接口）配置 IP 地址

```
SW1 (config) #interfacevlan100
SW1 (config-VLAN) #ipaddress192.168.1.254255.255.255.0
SW1 (config-VLAN) #noshutdown
SW1 (config-VLAN) #exit
SW1 (config) #interface.vlan200
SW1 (config-VLAN) #ipaddress192.168.2.254255.255.255.0
SW1 (config-VLAN) #noshutdown
```

2. 查看路由表信息

```
SW1#showiproute
```

【配置结果】

1. SW1 # showiproute

```
Codes:C - connected,S - static,I - IGRP,R - RIP,M - mobile,B - BGP
      D - EIGRP,EX - EIGRP external,O - OSPF,IA - OSPF inter area
      N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1,E2 - OSPF external type 2,E - EGP
      i - IS - IS,L1 - IS - IS level - 1,L2 - IS - IS level - 2,ia - IS - IS in-
ter area
      * - candidate default,U - per - user static route,o - ODR
      P - periodic downloaded static route
Gateway of last resort is not set

C  192.168.1.0/24 is directly connected,Vlan100
C  192.168.2.0/24 is directly connected,Vlan200
```

2. SW1 # showrunning-config

```
Building configuration...
Current configuration:1147 bytes
version 12.2
no service password - encryption
hostname SW1
```

```
 ip ssh version 1
 port - channel load - balance src - mac
 interface FastEthernet0/1
   switchport mode trunk
 interface FastEthernet0/2
   switchport mode trunk
 interface FastEthernet0/3
 interface FastEthernet0/4
 interface FastEthernet0/5
 interface FastEthernet0/6
 interface FastEthernet0/7
 interface FastEthernet0/8
 interface FastEthernet0/9
 interface FastEthernet0/10
 interface FastEthernet0/11
 interface FastEthernet0/12
 interface FastEthernet0/13
 interface FastEthernet0/14
 interface FastEthernet0/15
 interface FastEthernet0/16
 interface FastEthernet0/17
 interface FastEthernet0/18
 interface FastEthernet0/19
 interface FastEthernet0/20
 interface FastEthernet0/21
 interface FastEthernet0/22
 interface FastEthernet0/23
 interface FastEthernet0/24
 interface GigabitEthernet0/1
 interface GigabitEthernet0/2
 interface Vlan1
   no ip address
   shutdown
interface Vlan100
ip address 192.168.1.254 255.255.255.0
interface Vlan200
  ip address 192.168.2.254 255.255.255.0
ip classless
```

```
line con 0
line vty 0 4
  login
end
```

【技术原理】

1. VLAN 间路由

VLAN 是广播域，而通常两个广播域之间由路由器连接，广播域之间来往的数据包都是由路由器中继的。因此，VLAN 间的通信也需要路由器提供中继服务，这被称作“VLAN 间路由”。VLAN 间路由，可以使用普通的路由器，也可以使用三层交换机。

为什么不同 VLAN 间不通过路由就无法通信。在 VLAN 内的通信，必须在数据帧头中指定通信目标的 MAC 地址。而为了获取 MAC 地址，TCP/IP 协议下使用的是 ARP。ARP 解析 MAC 地址的方法，则是通过广播。也就是说，如果广播报文无法到达，那么就无从解析 MAC 地址，亦无法直接通信。

计算机分属不同的 VLAN，也就意味着分属不同的广播域，自然收不到彼此的广播报文。因此，属于不同 VLAN 的计算机之间无法直接互相通信。为了能够在 VLAN 间通信，需要利用 OSI 参照模型中更高一层（网络层）的信息（IP 地址）来进行路由选择。

2. 开启三层交换机的路由功能，实现 VLAN 的划分、VLAN 内部的二层交换和 VLAN 间路由的功能

第一步：分别创建每个 VLAN 三层 SVI 端口，并分配 IP 地址：

```
Switch (config) #interfacevlan<vlan>
Switch (config-if) #ipaddress<address><netmask>
Switch (config-if) #noshutdown
```

第二步：将每个 VLAN 内主机的网关指定为本 VLAN 接口地址。

任务 5　生成树配置一（端口上开启 RSTP）

【学习情境】

你是某公司的网络管理员，为了提高网络的可靠性，在服务器和核心交换机等很多重要地方进行了 2 根或多根链路的连接，提供了冗余备份，可是现在还要做适当的配置，避免网络出现环路，防止广播风暴。

【学习目的】

1. 理解快速生成树协议的工作原理、广播风暴的形成和对网络的危害。

2. 掌握如何在交换机上配置快速生成树协议。

3. 学会识别快速生成树协议中的根交换机、非根交换机、根端口、指定端口、替换端口、备份端口等重要概念。

4. 掌握交换机优先级和端口优先级的设置。

【相关设备】

三层交换机 1 台、二层交换机 1 台、PC2 台、直连线 2 根、交叉线 2 根。

【实验拓扑】

拓扑如图 1-5-1 所示。

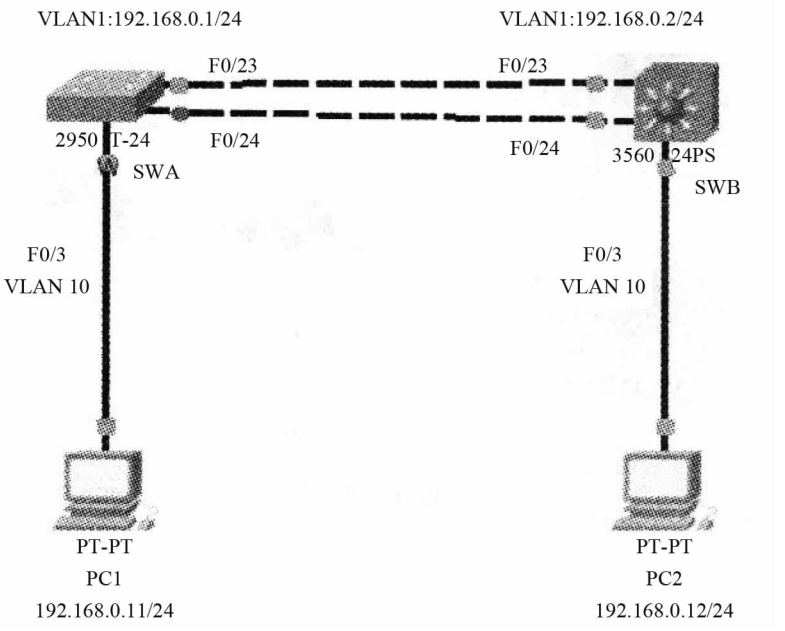

图 1-5-1　实验拓扑搭建示意图

【实验任务】

1. 进行网络拓扑的搭建，将 1 台二层交换机 2950（SWA）与 1 台三层交换机 3560（SWB）用两根交叉线连接 F0/23 和 F0/24 口，分别再连接 1 台 PC（都是 F0/3 口）。

2. 基本 IP 地址配置如图 1-5-1 所示。SWA 的 VLAN1 地址：192.168.0.1/24；SWB 的 VLAN1 地址：192.168.02/24；PC1 的地址：192.168.0.11/24；PC2 的地址：

192.168.0.12/24；4 台设备的默认网关都是 192.168.0.254。测试 4 台设备的互通性（应该是全通）。

3. 在 SWA 和 SWB 上分别建立 VLAN10，并把 F0/3 口都加入。再测试 4 台设备的互通性（应该是 SWA 和 SWB 互通，其他都不通，因为跨交换机之间的 Trunk 模式未设置）。

4. 分别设置 SWA 和 SWB 的 F0/23 口和 F0/24 口的模式为 Trunk。再测试 4 台设备的互通性（应该是 SWA 和 SWB 互通，PC1 和 PC2 互通，其他不通）。

5. 在 PC1 上对 PC2 一直进行 Ping（命令 ping-t192.168.0.12），观察实验中的丢包和连接情况。此时断开主链路，如 F0/23 口（即数据转发口），观察丢掉多少个数据包 F0/24 才能从阻塞变为转发状态，PC2 可以重新 Ping 通。

6. 重新连接 F0/23，再次观察结果，如图 1-5-2 和图 1-5-3 所示。说明在默认的 STP 生成树中，冗余链路的延时比较长，影响网络速度和质量。查看和记录 2 台交换机的生成树信息（ShowSpanningTree），分析并判断 SWA 和 SWB 哪个是根交换机。找出 F0/23 口和 F0/24 口哪个是转发状态，哪个是根端口，哪个是替换端口，哪些是指定端口。

```
SWA#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000A.F373.7362
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F373.7362
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Desg LRN 19        128.23   P2p
F0/24            Desg LRN 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     000A.F373.7362
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

图 1-5-2　重新连接 F0/23 结果截图 a

```
SWB#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000A.F373.7362
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0030.F21B.1366
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Root FWD 19        128.23   P2p
F0/24            Altn BLK 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     000A.F373.7362
```

图 1-5-3　重新连接 F0/23 结果截图 b

7. 开启 SWA 和 SWB 的生成树协议，指定类型为 RSTP。再次断开 F0/23 口（即数据转发口），观察丢掉多少个数据包，F0/24 才能从阻塞变为转发状态，PC2 可以重新 Ping 通。重新连接 F0/23，再次观察结果，如图 1-5-4 和图 1-5-5 所示。说明在 RSTP 生成树中，冗余链路的延时比较短，加快了收敛速度，大大提高了网络速度和质量。再次查看和记录 2 台交换机的生成树信息（ShowSpanningTree），分析并判断 2 台交换机的状态与端口。

```
SWA#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0C45.33B8
             Cost        19
             Port        23(FastEthernet0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.F37E.8044
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Desg FWD 19        128.23   P2p
F0/24            Altn BLK 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     0000.0C45.33B8
```

图 1-5-4　RSTP 生成树中的观察结果截图 a

```
SWB#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0C45.33B8
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0000.0C45.33B8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Desg FWD 19        128.23   P2p
F0/24            Desg FWD 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     0000.0C45.33B8
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

图 1-5-5　RSTP 生成树中的观察结果截图 b

8. 更改交换机的优先级（可以改变根交换机的角色），并验证结果，如图 1-5-6 和

图 1-5-7所示。

```
SWA#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     0030.F21B.1366
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F373.7362
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Root FWD 19        128.23   P2p
F0/24            Altn BLK 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0030.F21B.1366
              Cost        19
```

图 1-5-6　更换交换机优先级结果截图 a

```
SWB#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     0030.F21B.1366
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4097  (priority 4096 sys-id-ext 1)
              Address     0030.F21B.1366
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
F0/23            Desg FWD 19        128.23   P2p
F0/24            Desg LSN 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0030.F21B.1366
```

图 1-5-7　更换交换机优先级结果截图 b

9. 更改端口的优先级（可以改变端口的角色，改变端口的状态），并验证结果。

10. 最后把配置以及 ping 的结果截图打包，以“学号姓名”为文件名，提交作业。

【实验命令】

1. 设置 SWA 的 F0/23 口和 F0/24 口的模式为 Trunk

```
SWA (config) #interfacerangefastEthernet0/23-24
SWA (config-if-range) #switchportmodetrunk
```

2. 开启 SWA 的生成树协议，指定类型为 RSTP

```
SWA (config) #spanning-treemoderapid-pvst
```

（锐捷设备中命令是：SWA（config）＃spanning-treemodeRSTP）

3. 查看 SWA 的生成树信息

SWA＃showspanning-tree

4. 更改 SWB 交换机的优先级（取值范围为 0～61440 的 4096 倍数，缺省优先级值为 32768）

SWB（config）＃spanning-treevlan1priority4096

SWB（config）＃spanning-treevlan10priority4096

（锐捷设备中命令是：SWB（config）＃spanning-treepriority4096）

5. 更改 SWA 的 F0/24 口的优先级(取值范围为 0～240 的 16 倍数，缺省优先级值为 128)

SWA（config）＃interfacefastEthernet0/ 24

SWA（config-if）＃spanning-treevlan1port-priority32

（锐捷设备中命令是：SWA（config-if）＃spanning-treeport-priority32）

【注意事项】

1. 出现时通时不通的不稳定情况，可以先保证配置，再把交换机重启。

SWA＃writememory

SWA＃reload，再输入 y

2. 二层交换机配置默认网关：SWA（config）＃ipdefault-gateway192.168.0.254；三层交换机配置默认网关：SWB（config）＃ipdefault-network192.168.0.254，注意两者配置命令的区别。

3. 在更改端口的优先级（可以改变端口的角色，改变端口的状态）并验证结果时，显示信息可能不正确，可以把 F0/23 与 F0/24 都断开，再重新连接，就显示正确了。

【配置结果】

1. SWA＃showrunning-config

```
Building configuration...
Current configuration:1023 bytes
version 12.1
no service password-encryption
hostname SWA
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
 switchport access vlan 10
```

```
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
  switchport mode trunk
interface FastEthernet0/24
  switchport mode trunk
  spanning-tree vlan 1,10 port-priority 16
interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip default-gateway 192.168.0.254
line con 0
line vty 0 4
  login
line vty 5 15
  login
end
```

2. SWB＃showrunning-conrig

```
Building configuration...
Current configuration:1197 bytes
version 12.2
no service password-encryption
```

```
hostname SWB
ip ssh version 1
port-channel load-balance src-mac
spanning-tree vlan 1,10 priority 4096
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
  switchport access vlan 10
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
  switchport mode trunk
interface FastEthernet0/24
  switchport mode trunk
spanning-tree vlan 1,10 port-priority 16
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
  ip address 192.168.0.2 255.255.255.0
ip classless
ip route 192.168.0.0 255.255.255.0 192.168.0.254
```

```
line con 0
line vty 0 4
  login
end
```

【技术原理】

1. 交换机网络中的冗余链路

在许多交换机或交换机设备组成的网络环境中，通常都使用一些备份连接，以提高网络的健全性、稳定性。备份连接也叫备份链路、冗余链路等。

使用冗余备份能够使网络具有健全性、稳定性和可靠性等好处，但是备份链路使网络存在环路，这是备份链路所面临的最为严重的问题之一。它会带来如下问题：

（1）广播风暴。

（2）同一帧的多份复制。

（3）不稳定的 MAC 地址表。

因此，在交换网络中必须有一个机制来阻止回路，于是有了生成树协议（SpanningTreeProtocol，STP）。

2. 生成树协议

生成树协议定义在 IEEE802.ID 中，是一种桥到桥的链路管理协议，它在防止产生自循环的基础上提供路径冗余。为使以太网更好地工作，两个工作站之间只能有一条活动路径。网络环路的发生有多种原因，最常见的一种是故意生成的冗余，万一一个链路或交换机失败，会有另一个链路或交换机替代。

所以，STP 的主要思想就是当网络中存在备份链路时，只允许主链路激活，如果主链路因故障而被断开，备用链路才会被打开。STP 的主要作用：避免回路，冗余备份。

3. 生成树协议的工作原理

生成树协议的国际标准是 IEEE802.1D，运行生成树算法的网桥/交换机在规定的间隔内通过网桥协议数据单元（BPDU）的组播帧与其他交换机交换配置信息，其工作的过程如下：

（1）通过比较网桥/交换机优先级选取根网桥/交换机（给定广播域内只有一个根网桥/交换机）。

（2）其余的非根网桥/交换机只有一个通向根网桥/交换机的端口，称为根端口。

（3）每个网段只有一个转发端口。

（4）根网桥/交换机所有的连接端口均为转发端口。

4. 生成树端口有四种状态

（1）阻塞：所有端口以阻塞状态启动以防止同路，由生成树确定哪个端口切换为转发状态，处于阻塞状态的端口不转发数据帧，但可接受 BPDU。

（2）侦听：能收 BPDU 报文，能发送 BPDU 报文，也不能学习 MAC 地址。

（3）学习：能接收发送 BPD 报文，也能学习 MAC 地址，但不能发送数据帧。

（4）转发：开始正常接收和发送数据帧。

一般从阻塞到侦听需要 20 秒，从侦听到学习需要 15 秒，从学习到转发需要 15 秒。生成树经过一段时间（默认值是 50 秒左右）稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。STPBPDU 仍然会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树就会重新计算，端口状态也会随之改变。

5. RSTP

为了解决 STP 收敛时间长这个缺陷，在 21 世纪之初，IEEE 推出了 802.1W 标准，作为对 802.1D 标准的补充。在 IEEE802.1W 标准里定义了快速生成树协议 RSTP（RapidSpanningTreeProtocol）。RSTP 在 STP 基础上做了三点重要改进，使得收敛速度比以前快得多（最快 1 秒以内）。

第一点改进：为根端口和指定端口设置了快速切换用的替换端口（AlternatePort）和备份端口（BackupPort）两种角色，在根端口/指定端口失效的情况下，替换端口/备份端口就会无时延地进入转发状态。

第二点改进：在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥是不会响应上游指定端口发出的握手请求的，只能等待两倍 ForwardDelay 时间进入转发状态。

第三点改进：直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（EdgePort）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，因此需要人工配置。

任务 6　生成树配置二（VLAN 上开启 RSTP）

【学习情境】

公司的网络很多都是在 VLAN 的隔离之中，要实现冗余链路的备份，需要在 VLAN 上开启快速生成树。

【学习目的】

1. 掌握在 VLAN 上启用生成树的方法。
2. 掌握配置根网桥的方法。
3. 掌握生成树的多种测试技巧和方法。

【相关设备】

三层交换机 1 台、二层交换机 1 台、PC2 台、直连线 2 根、交叉线 2 根。

【实验拓扑】

拓扑如图 1-6-1 所示。

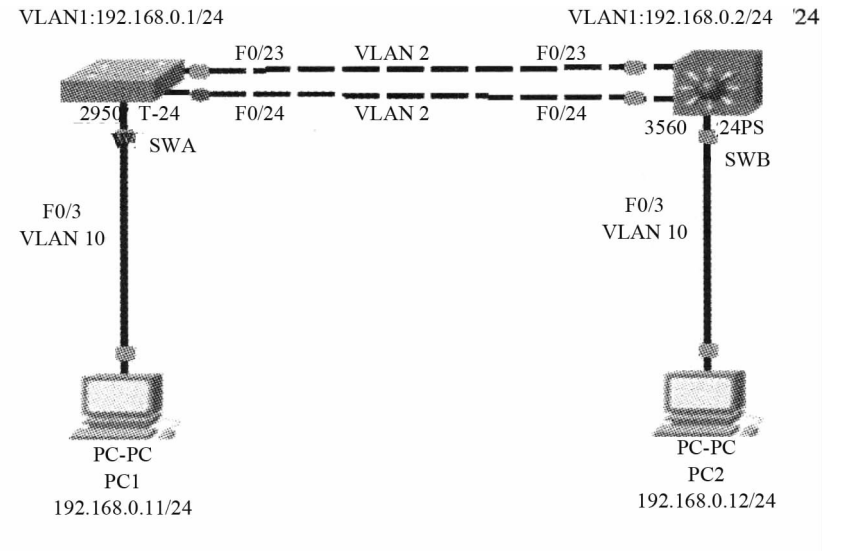

图 1-6-1　实验拓扑搭建示意图

【实验任务】

1. 1 台三层交换机 3560（SWA）与 1 台二层交换机 2950（SWB），用两根交叉线连接 F0/23 和 F0/24 口。分别再连接一台 PC（都是 F0/3 口）。

2. 基本 IP 地址配置如图 1-6-1 所示。SWA 的 VLANI 地址：192. 168. 0. 1/24，SWB 的 VLAN1 地址：192. 168. 0. 2/24，PC1 的地址：192. 168. 0. 11/24，PC2 的地址：192. 168. 0. 12/24，4 台设备的默认网关都是 192. 168. 0. 254。测试 4 台设备的互通性（应该是全通）。

3. 在 SWA 和 SWB 上分别建立 VLAN2 和 VLAN10，并把 F0/3 口都加入 VLAN10，把 F0/23 口和 F0/24 口加入 VLAN2。再测试 4 台设备的互通性（应该都不通，因为跨交换机之间的 Trunk 模式未设置）。

4. 分别设置 SWA 和 SWB 的 F0/23 口和 F0/24 口的模式为 Trunk。再测试 4 台设备的互通性（应该是 SWA 和 SWB 互通，PC1 和 PC2 互通，其他不通）。

5. 在 PC1 上对 PC2 一直进行 Ping（命令 ping-t192. 168. 0. 12），观察实验中的丢包和连接情况。此时断开 F0/23 口（即数据转发口），观察丢掉多少个数据包，F0/24 才能从

阻塞变为转发状态，PC2 可以重新 Ping 通。重新连接 F0/23，再次观察结果。说明在默认的 STP 生成树中，冗余链路的延时比较长。

6. 找出 SWA 和 SWB 哪个是根交换机。找出 F0/23 口和 F0/24 口哪个是转发状态，哪个是根端口，哪个是备份端口，哪些是指定端口。

7. 在 SWA 和 SWB 的 VLAN2 上启用生成树协议，指定类型为 RSTP。再次断开 F0/23 口（即数据转发口），观察丢掉多少个数据包，F0/24 才能从阻塞变为转发状态，PC2 可以重新 Ping 通。重新连接 F0/23，再次观察结果。说明在 RSTP 生成树中收敛速度比较快。

8. 手动设置根交换机的角色，用两种方法：（1）直接定义，设置 SWB 为根交换机，SWA 为备份根交换机；（2）更改 SWB 交换机优先级为 8192。

9. 改变根端口的角色，用两种方法：（1）修改 SWA 中的 F0/24 端口优先级为 64；（2）修改 SWA 中的 F0/24 端口成本为 19，F0/23 端口成本为 100（模拟器上不能实现）。

10. 在根交换机上修改 HELLO 时间为 1 秒；修改转发延迟时间为 10 秒；修改最大老化时间为 15 秒（模拟器上不能实现）。

11. 在二层交换机上配置快速端口和上行端口两种功能，以加快转发状态的收敛速度（模拟器上不能实现）。

【实验命令】

1. 在 VLAN 上启用生成树

```
spanning-treeVLAN2
```

2. 设置根网桥

（1）直接定义根交换机（如把 SWA 设置为根交换机）：

```
SWA（config）＃spanning-treeVLAN2rootprimary
```

（2）通过修改优先级定义根交换机（如把 SWA 设置为根交换机）：

```
SWA（config）＃spanning-treeVLAN2priority24768（4096 的倍数，值越小，优先级越高，默认为 32768）
```

3. 设置根端口

（1）可通过修改端口成本设置：

```
SWA（config）＃spanning-treeVLAN2cost＊＊＊（100m 为 19，10m 为 100，值越小，路径越优先）
```

（2）可修改端口优先级：

```
SWA（config-if）＃spanning-treeVLAN2port-priority＊＊＊（0-240，默认为 128）
```

4. 修改计时器（可选）

（1）修改 HELLO 时间：

spanning-treeVLAN2hello-time＊＊（1～10 秒，默认为 2 秒）

（2）修改转发延迟时间：

spanning-treeVLAN2forward-time＊＊＊（4～30 秒，默认为 15 秒）

（3）修改最大老化时间：

spanning-treeVLAN2max-age＊＊＊（6～40，默认为 20 秒）

5. 配置快速端口

spanning-treeportfast。这个是 PVST 的加快收敛速度三大特性之一，它的作用是，当你插入一个设备到一个没有启用的端口时，那么这个端口马上进入转发状态。

6. 配置上行端口

spanning-treeuplinkfast。这个是 PVST 的加快收敛速度三大特性之一，它的作用是本地端口快速切换为转发状态，一般给接八层交换机配置。注意：千万不要给核心或汇聚层配置。

7. 检查命令

（1）检查生成树：

showspanning-treesummary

（2）检查 HELLO 时间、转发延迟、最大老化时间：

showspanning-treeVLAN2

（3）检查根网桥：

showspannint-treeVLAN2detail

（4）检查端口：

showspanninn-treeinterfacef0/2detail

【技术原理】

1. 生成树协议的发展过程划分成三代

第一代生成树协议：STP/RSTP。

第二代生成树协议：PVST/PVST＋。

第三代生成树协议：MISTP/MSTP。

STP/RSTP 是基于端口的，PVST/PVST＋是基于 VLAN 的，而 MISTP/MSTP 就是基于实例的。所谓实例就是多个 VLAN 的一个集合，通过多个 VLAN 捆绑到一个实例中去的方法可以节省通信开销和资源占用率。

2. 形成一个生成树必须要决定的要素

（1）首先依据网桥 ID（由优先级和 MAC 地址两部分组成）确定根网桥（根交换机）。

（2）确定根端口，指定端口和备份端口（由路径成本，网桥 ID，端口优先级，端口 ID 来确定）。

3. 生成树协议端口的状态如图 1-6-2 所示

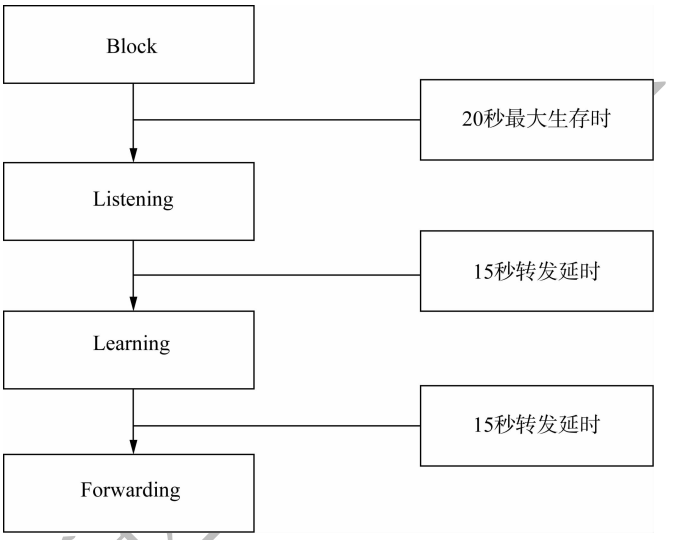

图 1-6-2　生成树协议端口的状态

生成树经过一段时间（默认值是 50 秒左右）稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。

4. 端口角色和端口状态

（1）Rootport：具有到根交换机的最短路径的端口。

（2）Designatedport：每个 LAN 通过该口连接到根交换机。

（3）Alternateport：根端口的替换口，一旦根端口失效，该口就立刻变为根端口。

（4）Backupport：Designatedport 的备份口，当一个交换机有两个端口都连接在一个 LAN 上，那么高优先级的端口为 Designatedport，低优先级的端口为 Backupport。

（5）Undesignatedport：当前不处于活动状态的口，即 OperStace 为 down 的端口都被分配了这个角色。

任务 7　端口聚合

【学习情境】

企业在某 2 台交换机之间可能数据量非常大，要加大两者之间的带宽，并实现链路的冗余备份，需要在相应的端口上进行 2 个或者多个端口的聚合。

【学习目的】

1. 理解端口聚合的工作原理。
2. 掌握如何在交换机上配置端口聚合。
3. 掌握端口聚合的多种方式、流量平衡和测试方法。

【相关设备】

三层交换机 2 台、PC2 台、直连线 2 根、交叉线 4 根。

【实验拓扑】

拓扑如图 1-7-1 所示。

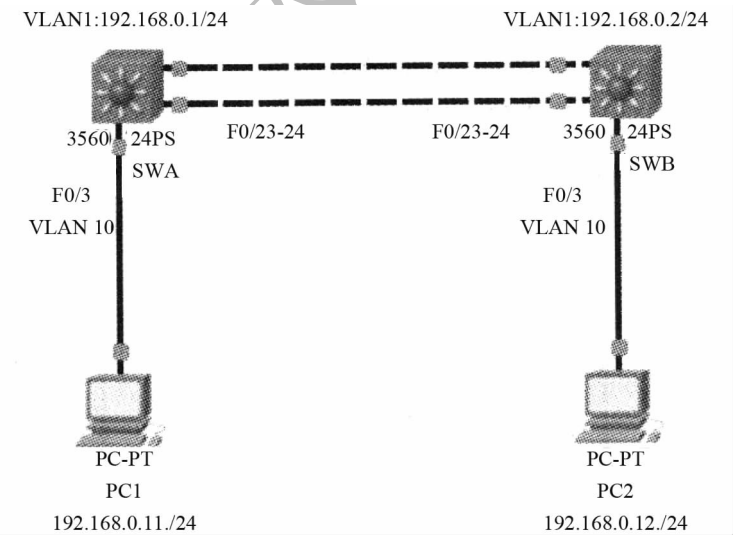

图 1-7-1　实验拓扑搭建示意图

【实验任务】

1. 2 台三层交换机用 2 根交叉线连接 F0/23 和 F0/24 口。分别再连接一台 PC（都是 F0/3 口）。

2. 基本 IP 地址配置如图 1-7-1 所示。SWA 的 VLAN1 地址：192.168.0.1/24；SWB 的 VLAN1 地址：192.168.0.2/24；PC1 的地址：192.168.0.11/24；PC2 的地址：192.168.0.12/24；4 台设备的默认网关都是 192.168.0.254。测试 4 台设备的互通性（应该是全通）。

3. 在 SWA 和 SWB 上分别建立 VLAN10，并把 F0/3 口都加入。再测试 4 台设备的互通性（应该是 SWA 和 SWB 互通，其他都不通，因为跨交换机之间的 Trunk 模式未设置）。

4. 在 SWA 和 SWB 上分别创建聚合端口 1，设置模式为 Trunk. 并把 F0/23 口和 F0/24口加入。再测试 4 台设备的互通性（应该是 SWA 和 SWB 互通，PCI 和 PC2 互通，其他不通）。查看聚合端口的情况，如图 1-7-2 所示。

```
SWA#show etherchannel summary
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
------+-------------+-----------+-----------------------------------------------

1      Po1             PAgP    F0/23(P) F0/24(P)
SWA#show run
SWA#show running-config
Building configuration...
```

图 1-7-2　Trunk 模式下聚合端口情况截图

5. 设置聚合端口的负载平衡为 dst-mac 方式。

6. 在 SWA 和 SWB 上分别创建聚合端口 2，并把 F0/21 口和 F0/22 口加入，设置模式为 Trunk。分析聚合端口的情况，如图 1-7-3 所示。

7. 2 台三层交换机再用 2 根交叉线连接 F0/21 和 F0/22 口。再次查看聚合端口的情况和生成树情况，如图 1-7-4、图 1-7-5 所示。

8. 最后把配置以及 ping 的结果截图打包，以“学号姓名”为文件名，提交作业。

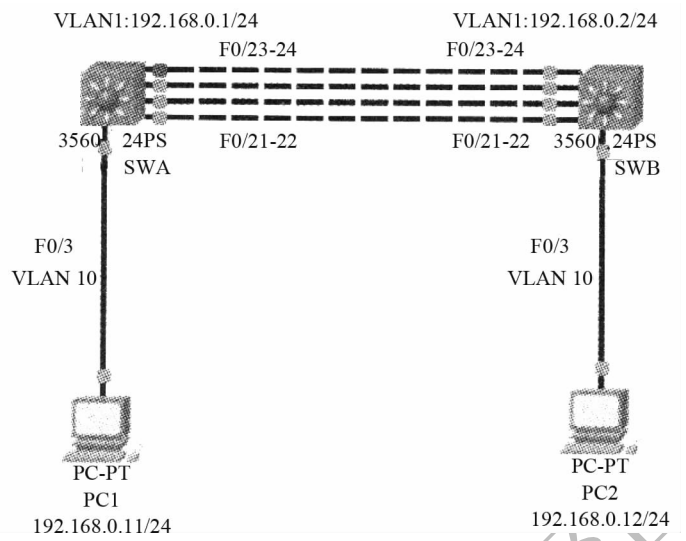

图 1-7-3　聚合端口情况拓扑示意图

```
SWA#show etherchannel summary
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: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1           PAgP   Fa0/23(P) Fa0/24(P)
2      Po2           PAgP   Fa0/21(P) Fa0/22(P)
SWA#
SWA#
SWA#
```

图 1-7-4　聚合端口情况截图

```
SWA#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0002.1684.A74E
              Cost        19
              Port        27(Port-channel 1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0030.A32D.8341
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root LSN 19        128.27   Shr
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Po2              Altn BLK 19        128.28   Shr
```

图 1-7-5　生成树情况截图

【实验命令】

1. 思科端口聚合配置（只是增加带宽，不会起到备份作用）

（1）创建聚合端口，并设置为 Trunk 模式：

```
SWA（config）＃interfaceport-channel1
SWA（config-if）＃switchportmodetrunk
SWA（config-if）＃exit
```

（2）以手动方式把端口加入聚合端口中：

```
SWA（config）＃interfacerangeFastEthernet0/23-24
SWA（config-if）＃channel-group1modeon
SWA（config-if）＃exit
```

（3）设置聚合端口的负载平衡：

```
SWA（config）＃port-channelload-balancedst-mac
```

（4）查看聚合端口：

```
SWA＃showetherchannelsummary
```

2. 锐捷端口聚合配置：（既增加带宽，又起到备用作用）最多支持 8 个物理端口聚合，最多支持 6 组

（l）创建聚合端口，并设置为 Trunk 模式：

```
SWA（config）＃interfaceaggregateport1
SWA（config-if）＃switchportmodetrunk
SWA（config-if）＃exit
```

（2）以手动方式把端口加入聚合端口中：

```
SWA（config）＃interfacerangeFastEthernet0/23-24
SWA（config-if-range）＃port-group1
SWA（config-if-range）＃exit
```

（3）设置聚合端口的负载平衡：

```
SWA（config）＃aggregateportload-balancedst-mac
```

（4）查看聚合端口：

```
SWA#showaggregateport1summary
```

【注意事项】

1. 如果两个交换机之间的连线指灯不正确，或出现时通时不通的不稳定情况，可以先保证配置，把两个交换机的连线拔掉再重新连接。

2. 创建聚合时要观察两个交换机可创建的最大聚合数，用 SWA（config）#interface port-channel? 命令进行查看，以保证所建的聚合名称一致。

【配置结果】

SWA#showrunning-config：

```
Building configuration...
Current configuration:1271 bytes
version 12.2
no service password-encryption
hostname SWA
ip ssh version 1
port-channel load-balance dst-mac
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
  switchport access vlan 10
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
  channel-group 2 mode on
interface FastEthernet0/22
  channel-group 2 mode on
interface FastEthernet0/23
channel-group 1 mode on
interface FastEthernet0/24
  channel-group 1 mode on
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Port-channel 1
  switchport mode trunk
interface Port-channel 2
switchport mode trunk
interface Vlan1
ip address 192.168.0.1 255.255.255.0
line con 0
```

```
line vty 0 4
 login
end
```

【技术原理】

1. 端口聚合

将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，形成一个拥有较大宽带的端口，形成一条干路，可以实现均衡负载，并提供冗余链路。

802.3AD 标准定义了如何将两个以上的以太网链路组合起来为高带宽网络连接实现负载共享、负载平衡以及提供更好的弹性。

802.3AD 的主要优点：链路聚合技术［也称端口聚合（AP)］帮助用户减少带宽瓶颈的压力。链路聚合标准在点到点链路上提供了固有的、自动的冗余性。

配置 Aggregateport 的注意事项：

（1）组端口的速度必须一致；

（2）组端口必须属于同一个 VLAN；

（3）组端口使用的传输介质相同；

（4）组端口必须属于同一层次，并与 AP 也要在同一层次。

2. 端口的聚合有两种方式：一种是手动的方式；一种是自动协商的方式

（1）手动方式：

这种方式很简单，设置端口成员链路两端的模式为“on”。命令格式为：channel-group＜number 组号＞modeon。

（2）自动方式：

自动方式有两种协议：PAgP（PortAggregationProtocol）和 LACP（LinkAggregationControlProtocol)。

PAgP：Cisco 设备的端口聚合协议，有 Auto 和 Desirable 两种模式。Auto 模式在协商中只收不发，Desirable 模式的端口收发协商的数据包。

LACP：标准的端口聚合协议 802.3AD，有 Active 和 Passive 两种模式。Active 相当于 PAgP 的 Auto，而 Passive 相当于 PAgP 的 Desirable。

3. 配置 port-channel 的流量平衡说明

port-channelload-balance｛dst-mac | src-mac | ip｝

设置 AP 的流量平衡，选择使用的算法：

dst-mac：根据输入报文的目的 MAC 地址进行流量分配。在 AP 各链路中，目的 MAC 地址相同的报文被送到相同的接口，目的 MAC 不同的报文分配到不同的接口。

src-mac：根据输入报文的源 MAC 地址进行流量分配。在 AP 各链路中，来自不同地址的报文分配到不同的接口，来自相同地址的报文使用相同的接口。

ip：根据源 IP 与目的 IP 进行流量分配。不同的源 IP-目的 IP 对的流量通过不同的端口转发，同一源 IP-目的 IP 对通过相同的链路转发，其他的源 IP-目的 IP 对通过其他的链路转发。

任务 8　交换机端口安全

【学习情境】

假设你是某公司的网络管理员，公司要求对网络进行严格控制，为了防止公司内部用户的 IP 地址冲突、网络攻击和破坏行为。要对每位员工的 IP 地址进行固定，并进行 MAC 和 IP 地址的绑定，防止其他主机的随意连接。

【学习目的】

1. 掌握交换安全功能的开启与配置方法。
2. 掌握控制用户进行安全接入的技巧。

【相关设备】

二层交换机 1 台、PC3 台、直连线 3 根、交叉线 1 根。

【实验拓扑】

拓扑如图 1-8-1 所示。

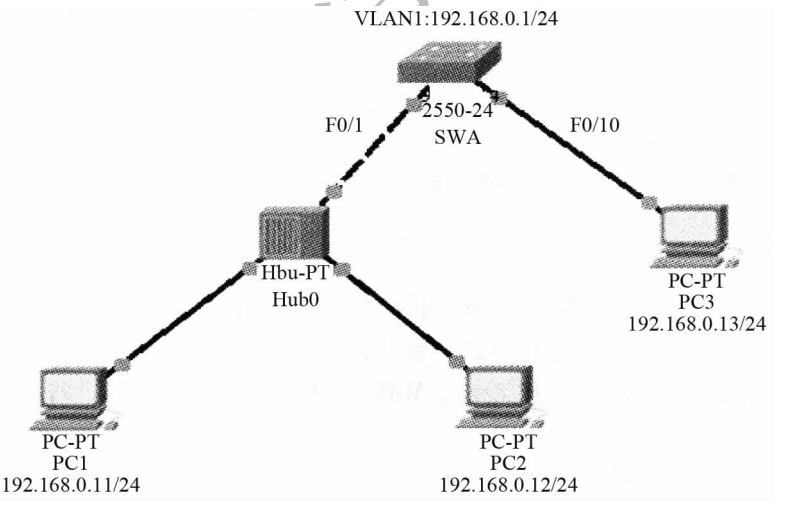

图 1-8-1　实验拓扑搭建示意图

【实验任务】

1. 1 台二层交换机 SWA 用 1 根交叉线（F0/1 口）连接 1 台 Hub，Hub 再连接 PC1、PC2；SWA 用 1 根直连线连接 PC3（F0/10 口）。

2. 基本 IP 地址配置如图 1-8-1 所示。SWA 的 VLAN1 地址：192.168.0.1/24；PCI 的地址：192.168.0.11/24；PC2 的地址：192.168.0.12/24；PC3 的地址：192.168.0.13/24；4 台设备的默认网关都是 192.168.0.254。测试 4 台设备的互通性（应该是全通）。

3. 对 F0/1-F0/10 口开启交换机端口的安全功能。配置最大连接数为 2，配置安全违例的处理方式为 shutdown。查看交换机端口的安全配置。

4. 查看 PC1 的 MAC 地址信息，把这个 MAC 绑定到 F0/1 口上，查看端口的地址绑定情况。

5. 测试绑定的效果，PC1 可以 ping 通交换机，PC2 不可以 Ping 通交换机。说明：本试验在模拟器中没效果，在真实设备中才能测试出效果。

【实验命令】

1. 对 F0/1-F0/10 口开启交换机端口的安全功能

```
SWA（config-if-range）＃switchportport-security
```

2. 配置最大连接数为 1

```
SWA（config-if-range）＃switchportport-securitymaximum2
```

3. 配置安全违例的处理方式为 shutdown

```
SWA（config-if-range）＃switchportport-securityviolationshutdown
```

4. 查看交换机 F0/1 口的安全配置

```
SWA＃showport-securityinterfacefastEthernet0/1
```

5. 对 F0/1 口进行端口的 MAC 绑定

```
SWA（config-if）＃switchportportsecurity ac-address00D0.BA83.2D93
```

6. 查看端口安全与地址绑定

```
SWA＃showport-security
SWA＃showport-securityaddress
```

【注意事项】

1. 交换机端口安全功能只能在 Access 接口中进行配置。

2. 交换机最大连接数范围是 1～128，默认是 128。

3. 在锐捷设备中，可以针对 IP 地址，MAC 地址、IP＋MAC 地址进行 3 种绑定方式。命令如下：

（1）对 F0/1 口进行端口的 MAC 绑定：

SWA（config-if）＃switchportport-securitymac-address00D0.BA83.2D93

（2）对 F0/1 口进行端口的 IP 绑定：

SWA（config-if）＃switchportport-securityip-address192.168.0.11

（3）对 F0/1 口进行端口的 IP＋MAC 绑定：

SWA（config-if）＃switchportport-securitymac-address00D0.BA83.2D93ip-address192.168.0.11

4. 在锐捷设备中，默认的违例处理方式是 protect。当端口因为违例而被关闭后，可以使用命令 errdisablerecovery 来将接口从错误状态中恢复过来，注意此命令是在全局模式下运行。

5. 在锐捷设备中，最好在三层交换机上做此实验，因为二层设备有 bug，对地址绑定部分的实验经常会出错。

【配置结果】

SWA＃showrunning-config：

```
Building configuration...
Current configuration:1321 bytes
version 12.1
no service password-encryption
hostname SWA
interface FastEthernet0/1
  switchport port-security maximum 2
  switchport port-security mac-address 00D0.BA83.2D93
interface FastEthernet0/2
  switchport port-security maximum 2
interface FastEthernet0/3
  switchport port-security maximum 2
interface FastEthernet0/4
  switchport port-security maximum 2
interface FastEthernet0/5
  switchport port-security maximum 2
interface FastEthernet0/6
  switchport port-security maximum 2
interface FastEthernet0/7
  switchport port-security maximum 2
interface FastEthernet0/8
  switchport port-security maximum 2
interface FastEthernet0/9
  switchport port-security maximum 2
interface FastEthernet0/10
  switchport port-security maximum 2
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
```

```
interface FastEthernet0/23
interface FastEthernet0/24
interface Vlan1
  ip address 192.168.0.1 255.255.255.0
ip default-gateway 192.168.0.254
line con 0
line vty 0 4
  login
line vty 5 15
  login
end
```

【技术原理】

1. MAC 地址与端口绑定和根据 MAC 地址允许流量的配置

（1）MAC 地址与端口绑定。

当发现主机的 MAC 地址与交换机上指定的 MAC 地址不同时，交换机相应的端口将 Down 掉。当给端口指定 MAC 地址时，端口模式必须为 Access 或者 Trunk 状态。

3550（config-if）＃switchportmodeaccess//指定端口模式。

3550（config-if）＃switchportport-securitymac-address00-90-F5-10-79-C1//配置 MAC 地址。

3550（config-if）＃switchportport-securitymaximum1//限制此端口允许通过的 MAC 地址数为 1。

3550（config-if）＃switchportport-securityviolationshutdown//当发现与上述配置不符时，端口 down 掉。

（2）通过 MAC 地址来限制端口流量。

此配置允许一 Trunk 口最多通过 100 个 MAC 地址，超过 100 时，来自新的主机的数据帧将丢失。

3550（config-if）＃switchporttrunkencapsulationdot1q

3550（config-if）＃switchportmodetrunk//配置端口模式为 Trunk。

3550（config-if）＃switchportport-securitymaximum100//允许此端口通过的最大 MAC 地址数目为 100。

3550（config-if）＃switchportport-securityviolationprotect//当主机 MAC 地址数目超过 100 时，交换机继续工作，但来自新的主机的数据帧将丢失。

2. 根据 MAC 地址来拒绝流量

上面的配置根据 MAC 地址来允许流量，下面的配置则是根据 MAC 地址来拒绝流量。此配置在 Catalyst 交换机中只能对单播流量进行过滤，对于多播流量则无效。

3550（config）＃mac-address-tablestatic00-90-F5-10-79-C1vlan2drop//在相应的Vlan丢弃流量。

3550（config）＃mac-address-tablestatic00-90-F5-10-79-C1vlan2intf0/1//在相应的接口丢弃流量。

3. 理解端口安全

当你给一个端口配置了最大安全MAC地址数量，安全地址是以以下方式包括在一个地址表中的：

（1）你可以配置所有的MAC地址使用switchportport-securitymac-address＜mac地址＞这个接口命令。

（2）你也可以允许动态配置安全MAC地址，使用已连接的设备的MAC地址。

（3）你可以配置一个地址的数目且允许保持动态配置。

注意：如果这个端口shutdown了，所有的动态学的MAC地址都会被移除。一旦达到配置的最大的MAC地址的数量，地址就会被存在一个地址表中。设置最大MAC地址数量为1，并且配置连接到设备的地址，确保这个设备独占这个端口的带宽。

4. 端口安全规则

当以下情况发生时就是一个安全违规：

（1）最大安全数目MAC地址表外的一个MAC地址试图访问这个端口。

（2）一个MAC地址被配置为其他的接口的安全MAC地址的站点试图访问这个端口。

5. 配置接口的三种违规模式

你可以配置接口的三种违规模式，这三种模式基于违规发生后的动作：

（1）protect：当MAC地址的数量达到这个端口所最大允许的数量，带有未知的源地址的包就会被丢弃，直到删除了足够数量的MAC地址，降到端口允许的最大数值以内才不会被丢弃。

（2）restrict：一个限制数据合并引起“安全违规”计数器的增加的端口安全违规动作。

（3）shutdown：一个导致接口马上shutdown，并且发送SNMP陷阱的端口安全违规动作。

当一个安全端口处在error-disable状态，你要恢复正常必须得敲入全局下的errdisablerecoverycausepsecure-violatinn命令，或者你可以手动shut再noshut端口。这个是端口安全违规的默认动作。

6. 默认的端口安全配置

（1）port-security默认设置：关闭的。

（2）最大安全MAC地址数目默认设置：1。

（3）违规模式默认配置：shutdown，这端口在达到最大安全 MAC 地址数量时会 shutdown，并发 SNMP 陷阱。

7. 配置端口安全的向导

（1）安全端口不能在动态的 Access 口或者 Trunk 口上做，换言之，敲 port-secure 之前先配置该端口的模式为 access。

（2）安全端口不能是一个被保护的口。

（3）安全端口不能是 SPAN 的目的地址。

（4）安全端口不能属于 CEC 或 FEC 的组。

（5）安全端口不能属于 802.1X 端口。如果你在安全端口试图开启 802.1X，就会有报错信息，而且 802.1X 也关了。如果你试图改变，开启了 802.1X 的端口为安全端口，错误信息就会出现，但安全性设置不会改变。

8. 802.1X 的相关概念和配置

802.1X 身份验证协议最初使用于无线网络，后来才在普通交换机和路由器等网络设备上使用。它可基于端口来对用户身份进行认证，即当用户的数据流量企图通过配置过 802.1X 协议的端口时，必须进行身份的验证，合法则允许其访问网络。这样做的好处就是可以对内网的用户进行认证，并且简化配置，在一定的程度上可以取代 Windows 的 AD。

配置 802.1X 身份验证协议，首先得全局启用 AAA 认证，这个和在网络边界上使用 AAA 认证没有太多的区别，只不过认证的协议是 802.1X；其次则需要在相应的接口上启用 802.1X 身份验证。（建议在所有的端口上启用 802.1X 身份验证，并且使用 radius 服务器来管理用户名和密码）

9. 配置 AAA 认证所使用的为本地的用户名和密码

```
3550（config）＃aaanew-model  //启用 AAA 认证。
3550（config）＃aaaauthenticationdot1xdefaultlocal//全局启用 802.1X 协议认证，并使用本地用户名与密码。
3550（config）＃intrangef0/1-24
3550（config-if-range）＃dot1xport-controlauto//在所有的接口上启用 802.ix 身份验证。
```

10. 交换机端口安全总结

通过 MAC 地址来控制网络的流量既可以通过上面的配置来实现，也可以通过访问控制列表来实现。

虽然通过 MAC 地址绑定在一定程度上可保证内网安全，但效果并不是很好，建议使用 802.1X 身份验证协议。在可控性、可管理性上 802.1X 都是不错的选择。

练习题

1. 交换机的管理有几种方式？

2. 重启锐捷交换机的命令是什么？

3. 查看交换机保存在 Flash 中的配置信息，使用什么命令？

4. 如果管理员需要对接入层交换机进行远程管理，可以在交换机的哪一个接口上配置管理地址？

5. 工程师将一台百兆交换机配置为生成树的根，并将 cost 计算方法设置为短整型。配置完成后，通过 ShowSpanningTree 查看生成树信息，会看到接口的根路径成本值是多少？

6. 生成树协议的 BPDU 的默认 HelloTime 是多少？