

网络系统与安全实践

目录

实验一、交换机的基本配置（2 学时）	1
实验 1 交换机的基本配置	1
实验 2 备份交换机配置到 TFTP 服务器	4
实验 3 从 TFTP 服务器恢复交换机配置	7
实验二、路由器的基本配置（2 学时）	10
实验 1 路由器的基本配置	10
实验 2 备份路由器配置到 TFTP 服务器	14
实验 3 从 TFTP 服务器恢复路由器配置	17
实验三、虚拟局域网 VLAN（4 学时）	21
实验 1 交换机端口隔离	21
实验 2 跨交换机实现 VLAN	23
实验 3 通过三层交换机实现 VLAN 间路由（选做）	26
实验四、网络地址转换（4 学时）	31
实验 1 静态内部源地址转换 NAT	31
实验 2 动态内部源地址转换	34
实验 3 复用内部全局地址转换 NAPT（选做）	38
实验五、生成树配置（4 学时）	41
实验 1 生成树协议 STP	41
实验 2 快速生成树协议 RSTP（选做）	48
实验六、路由协议（6 学时）	55
实验 1 静态路由	55
实验 2 RIP V1 路由协议基本配置	61
实验 3 RIP V2 路由协议基本配置	67
实验 4 OSPF 单区域基本配置（选做）	73
实验七、IP 访问列表（2 学时）	77
实验 1 编号的标准 IP 访问列表	77
实验 2 编号的扩展 IP 访问列表	81
实验八、交换机安全（4 学时）	85
实验 1 设备口令及权限	85
实验 2 静态 MAC 地址的配置	88
实验 3 交换机端口安全性	91
实验 4 交换机端口限速	96
实验九、防火墙的初始配置（4 学时）	100

实验一、交换机的基本配置（2 学时）

实验 1 交换机的基本配置

一、实验性质

本实验为验证型实验，实验学时为 2 学时。

二、实验目的

掌握交换机的管理特性，学会配置交换机支持 Telnet 操作的相关语句。

三、预备知识

交换机的基本组成及工作原理

四、实验设备

S2126G 交换机（1 台），PC 机（1 台）

五、实验内容

1、背景描述

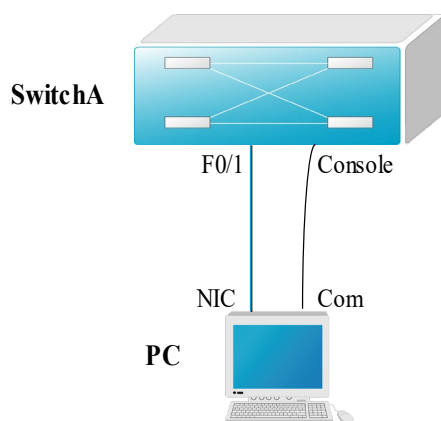
假设某学校的网络管理员第一次在设备机房对交换机进行了初次配置后，他希望以后在办公室或出差时也可以对设备进行远程管理，现要在交换机上做适当配置，使他可以实现这一愿望。

本实验以 S2126G 交换机为例，交换机命名为 SwitchA。一台 PC 机通过串口（Com）连接到交换机的控制（Console）端口，通过网卡（NIC）连接到交换机的 F0/1 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，配置交换机的管理 IP 地址和网络掩码分别为 192.168.0.138，255.255.255.0。

2、实现功能

使网络管理员可以通过 Telnet 对交换机进行远程管理。

3、拓扑结构



六、实验步骤

1、在交换机上配置管理 IP 地址

Red-Giant>enable ! 进入特权模式

Red-Giant # configure terminal ! 进入全局配置模式

Red-Giant (config)# hostname SwitchA ! 配置交换机名称为 “SwitchA”

SwitchA(config)# interface vlan 1 ! 进入交换机管理接口配置模式

SwitchA(config-if)# ip address 192.168.0.138 255.255.255.0 ! 配置交换机管理接口 IP 地址

SwitchA(config-if)# no shutdown ! 开启交换机管理接口

2、验证测试：验证交换机管理 IP 地址已经配置和开启

SwitchA#show ip interface ! 验证交换机管理 IP 地址已经配置，管理接口已开启

```
Interface          : Vlan1
Description        : Vlan 1
OperStatus         : up
ManagementStatus   : Enabled
Primary Internet address: 192.168.0.138/24
Broadcast address   : 255.255.255.255
PhysAddress        : 00d0.f8fe.1e48
```

或：

SwitchA#show interface vlan 1 ! 验证交换机管理 IP 地址已配置，管理接口已开启

```
Interface   : Vlan 1
Description :
AdminStatus : up
OperStatus  : up
Hardware    : -
Mtu         : 1500
LastChange  : 0d:0h:0m:0s
ARP Timeout : 3600 sec
PhysAddress : 00d0.f8fe.1e48
ManagementStatus:Enabled
Primary Internet address: 192.168.0.138/24
Broadcast address   : 255.255.255.255
```

3、配置交换机远程登录密码

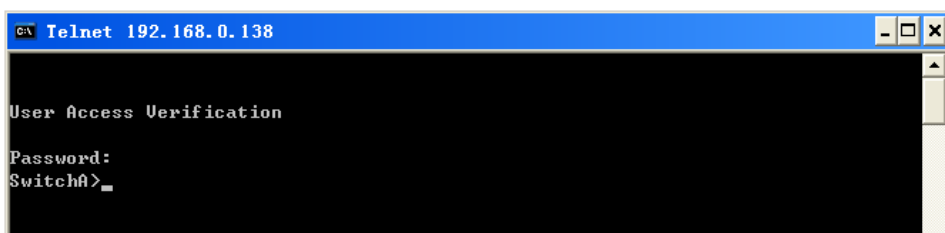
SwitchA(config)# enable secret level 1 0 star ! 设置交换机远程登录密码为“star”

Level 1 为普通用户级别，可选为 1~15，15 为最高权限级别；0 表示密码不加密

验证测试：

验证从 PC 机可以通过网线远程登录到交换机上

C:\>telnet 192.168.0.138 ! 从 PC 机登录到交换机上



4、配置交换机特权模式密码

SwitchA(config)# enable secret level 15 0 star ! 设置交换机特权模式密码为 “star”

验证测试：

验证从 PC 机通过网线远程登录到交换机上后可以进入特权模式

C:\>telnet 192.168.0.138 ! 从 PC 机登录到交换机上



5、保存在交换机上所做的配置

SwitchA# copy running-config startup-config ! 保存交换机配置

或： SwitchA# write memory

6、验证测试：验证交换机配置已保存

SwitchA# show configure ! 验证交换机配置已保存

Using 243 out of 4194304 bytes

!

version 1.0

!

hostname SwitchA

enable secret level 1 5 \$2,1u_;C3&-8U0<D4'.tj9=GQ+/7R:>H

enable secret level 15 5 \$2,1u_;C3&-8U0<D4'.tj9=GQ+/7R:>H

!

interface vlan 1

no shutdown

ip address 192.168.0.138 255.255.255.0

!

end

7、注意事项

交换机的管理接口缺省一般是关闭的（shutdown），因此在配置管理接口 interface vlan 1 的 IP 地址后须用命令 “no shutdown” 开启该接口。

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 2 备份交换机配置到 TFTP 服务器

一、实验性质

本实验为验证型实验，实验学时为 2 学时。

二、实验目的

能够将交换机配置文件备份到 TFTP 服务器。

三、预备知识

- 1、交换机的基本工作原理
- 2、TFTP 的基本工作原理

四、实验设备

S2126G 交换机（1 台），PC 机（1 台）

五、实验内容

1、背景描述

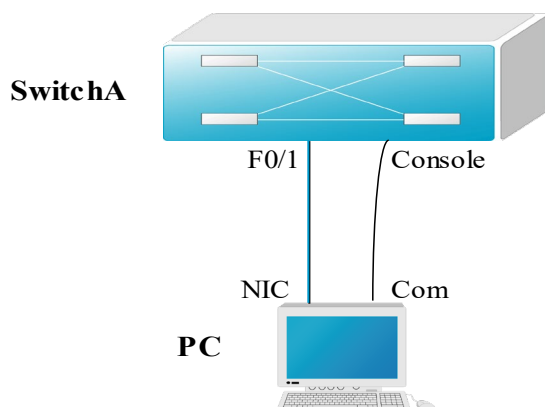
作为网络管理员，在交换机上做好配置后，需要将其配置文件做备份，以备将来需要时使用。

本实验以一台 S2126G 交换机为例，交换机名为 SwitchA。一台 PC 机通过串口（Com）连接到交换机的控制（Console）端口，通过网卡（NIC）连接到交换机的 fastethernet 0/1 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，PC 机上已安装和打开了 TFTP Server 程序，且在 PC 机已经准备好了新的交换机操作系统。

2、实现功能

保存交换机配置文件的备份。

3、拓扑结构



六、实验步骤

1、在交换机上配置管理接口 IP 地址。

SwitchA(config)# interface vlan 1 ! 进入交换机管理接口配置模式

SwitchA(config-if)# ip address 192.168.0.138 255.255.255.0 !配置交换机管理接口 IP 地址

SwitchA(config-if)# no shutdown ! 开启交换机管理接口

验证测试: 验证交换机管理 IP 地址已经配置和开启, TFTP 服务器与交换机有网络连通性

SwitchA#show ip interface ! 验证交换机管理 IP 地址已经配置, 管理接口已开启

```
Interface          : VLI
Description        : Vlan 1
OperStatus         : up
ManagementStatus   : Enabled
Primary Internet address: 192.168.0.138/24
Broadcast address   : 255.255.255.255
PhysAddress        : 00d0.f8fe.1e48
```

SwitchA#ping 192.168.0.137 ! 验证交换机与 TFTP 服务器具有网络连通性

```
Sending 5, 100-byte ICMP Echos to 192.168.0.137,
timeout is 2000 milliseconds.
```

!!!!

```
Success rate is 100 percent (5/5)
```

```
Minimum = 1ms Maximum = 2ms, Average = 1ms
```

2、备份交换机配置。

SwitchA#copy running-config startup-config ! 保存交换机的当前配置

SwitchA#copy startup-config tftp: ! 备份交换机的配置到 TFTP 服务器

Address of remote host []192.168.0.137 ! 按提示输入 TFTP 服务器 IP 地址

Destination filename [config.text]? ! 选择要保存的配置文件名称

!

```
%Success : Transmission success,file length 302
```

验证测试: 验证已保存配置文件

打开 TFTP 服务器上的配置文件 C:\config.text, 文件内容显示如下:

!

```
version 1.0
```

!

```
hostname SwitchA
```

```
enable secret level 1 5 $2)sv'~13Y*T7+.t4Z[V/,|7Q(\W&-/-
```

```
enable secret level 15 5 $2Nq&#Z13IOrJ%(84Mp]K*.tQxB^"/7
```

!

```
interface fastEthernet 0/5
```

```
switchport access vlan 10
```

!

```
interface vlan 1
```

```
no shutdown
```

```
ip address 192.168.0.138 255.255.255.0
```

!

```
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 3 从 TFTP 服务器恢复交换机配置(免做)

一、实验性质

本实验为验证型实验，实验学时为 2 学时。

二、实验目的

能够从 TFTP 服务器恢复交换机配置。

三、预备知识

- 1、交换机的基本工作原理
- 2、TFTP 的基本工作原理

四、实验设备

S2126G 交换机（1 台），PC 机（1 台）

五、实验内容

1、背景描述

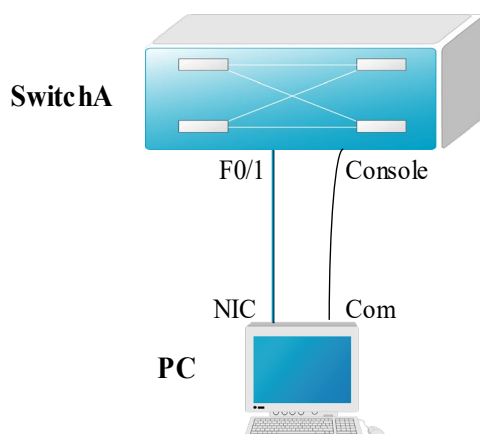
假设某台交换机的配置文件由于误操作或其它某种原因被破坏了，现在需要从 TFTP 服务器上的备份配置文件中恢复。

本实验以一台 S2126G 交换机为例，交换机名为 SwitchA。一台 PC 机通过串口（Com）连接到交换机的控制（Console）端口，通过网卡（NIC）连接到交换机的 fastethernet 0/1 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，PC 机上已安装和打开了 TFTP Server 程序，且在 PC 机已经准备好了新的交换机操作系统。

2、实现功能

使网络管理员可以将已有的配置恢复到交换机上。

3、拓扑结构



六、实验步骤

- 1、在交换机上配置管理接口 IP 地址。

SwitchA(config)# interface vlan 1 ! 进入交换机管理接口配置模式
SwitchA(config-if)# ip address 192.168.0.138 255.255.255.0 !配置交换机管理接口 IP
地址

SwitchA(config-if)# no shutdown ! 开启交换机管理接口

验证测试: 验证交换机管理 IP 地址已经配置和开启, TFTP 服务器与交换机有网络连
通性

SwitchA#show ip interface ! 验证交换机管理 IP 地址已经配置, 管理接口已开启

```

Interface          : Vlan1
Description        : Vlan 1
OperStatus         : up
ManagementStatus   : Enabled
Primary Internet address: 192.168.0.138/24
Broadcast address   : 255.255.255.255
PhysAddress        : 00d0.f8fe.1e48

```

SwitchA#ping 192.168.0.137 ! 验证交换机与 TFTP 服务器具有网络连通性

```

Sending 5, 100-byte ICMP Echos to 192.168.0.137,
timeout is 2000 milliseconds.
!!!!
Success rate is 100 percent (5/5)
Minimum = 1ms Maximum = 2ms, Average = 1ms

```

2、加载交换机配置。

SwitchA#copy tftp: startup-config ! 加载配置到交换机的初始配置文件中

```

Source filename []?config.text      ! 按提示输入源文件名
Address of remote host []192.168.0.137      ! 按提示输入 TFTP 服务器的 IP 地址
!
%Success : Transmission success,file length 302

```

验证测试: 验证交换机已经更改为新的配置

SwitchA#show configure ! 验证交换机的初始配置文件

```

Using 302 out of 4194304 bytes
!
version 1.0
!
hostname SwitchA
enable secret level 1 5 $2)sv'~13Y*T7+.t4Z[V/,|7Q(\W&-/-
enable secret level 15 5 $2Nq&#Z13IOrJ%(84Mp]K*.tQxB^[7
!
interface fastEthernet 0/5
    switchport access vlan 10
!
interface vlan 1
    no shutdown
    ip address 192.168.0.138 255.255.255.0
!

```

end

3、重启交换机，使新的配置生效。

SwitchA#reload ! 重启交换机

System configuration has been modified. Save? [yes/no]:n ! 选择 no

Proceed with reload? [confirm]

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验二、路由器的基本配置（2 学时）

实验 1 路由器的基本配置

一、实验性质

本实验为设计型实验，实验学时为 2 学时。

二、实验目的

掌握路由器的管理特性，学会配置路由器支持 Telnet 操作的相关语句。

三、预备知识

路由器的基本工作原理

四、实验设备

R2624 路由器（1 台），PC 机（1 台）

五、实验内容

1、背景描述

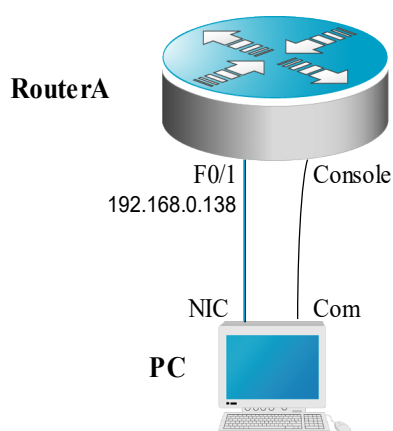
假设某学校的网络管理员第一次在设备机房对路由器进行了初次配置后，他希望以后在办公室或出差时也可以对设备进行远程管理，现要在路由器上做适当配置，使他可以实现这一愿望。

本实验以一台 R2624 路由器为例，路由器命名为 RouterA。一台 PC 机通过串口（Com）连接到路由器的控制（Console）端口，通过网卡（NIC）连接到路由器的 fastethernet0 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，配置路由器的 fastethernet0 端口的 IP 地址和网络掩码分别为 192.168.0.138，255.255.255.0。

2、实现功能

使网络管理员可以通过 Telnet 对路由器进行远程管理。

3、拓扑结构



六、实验步骤

1、在路由器上配置 fastethernet0 端口的 IP 地址。

Red-Giant>enable ! 进入特权模式

Red-Giant # configure terminal ! 进入全局配置模式

Red-Giant (config)# hostname RouterA ! 配置路由器名称为 “RouterA”

RouterA(config)# interface fastethernet0 ! 进入路由器接口配置模式

RouterA(config-if)# ip address 192.168.0.138 255.255.255.0 !配置路由器管理接口 IP 地址

RouterA(config-if)# no shutdown ! 开启路由器 fastethernet0 接口

验证测试: 验证路由器接口 fastethernet0 的 IP 地址已经配置和开启

RouterA#show ip interface fastethernet0 !验证接口 fastethernet0 的 IP 地址已经配置和开启

```
FastEthernet0 is up, line protocol is up
Internet address is 192.168.0.138/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP multicast fast switching is enabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Policy routing is disabled
```

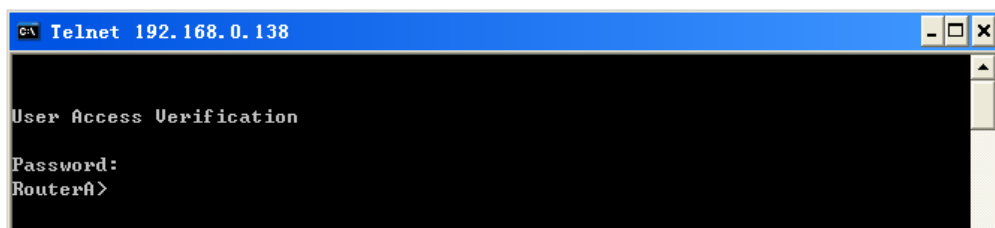
或:

RouterA#show ip interface brief ! 验证接口 fastethernet0 的 IP 地址已经配置和开启

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	192.168.0.138	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	unassigned	YES	unset	administratively down	down
Serial1	unassigned	YES	unset	administratively down	down

2、配置路由器远程登录密码。

```
RouterA(config)# line vty 0 4      ! 进入路由器线路配置模式
RouterA(config-line)# login        ! 配置远程登录
RouterA(config-line)# password star ! 设置路由器远程登录密码为“star”
RouterA(config-line)# end
验证测试: 验证从 PC 机可以通过网线远程登录到路由器上
C:\>telnet 192.168.0.138          ! 从 PC 机登录到路由器上
```



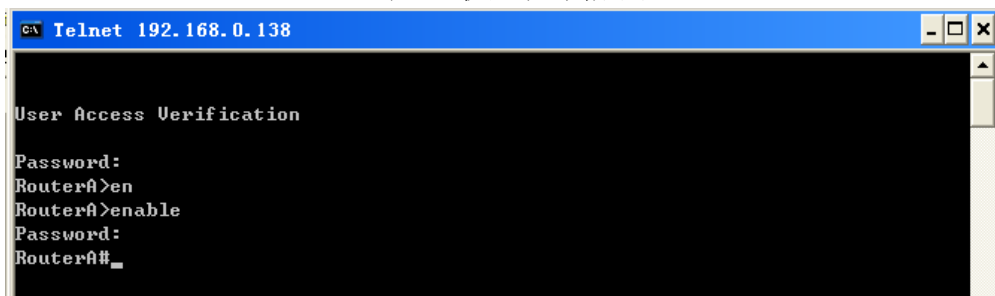
3、配置路由器特权模式密码。

```
RouterA(config)# enable secret star ! 设置路由器特权模式密码为“star”
或:
```

```
RouterA(config)# enable password star
```

验证测试: 验证从 PC 机通过网线远程登录到路由器上后可以进入特权模式

```
C:\>telnet 192.168.0.138          ! 从 PC 机登录到路由器上
```



4、保存在路由器上所做的配置。

```
RouterA# copy running-config startup-config ! 保存路由器配置
```

或:

```
RouterA# write memory
```

验证测试: 验证路由器配置已保存

```
RouterA#show startup-config        ! 验证路由器配置已保存
```

```
Using 593 out of 32768 bytes
```

!

```
version 6.14(2)
```

```
hostname "RouterA"
```

```
enable secret 5 $1$J.MN$6eZyYdYsJMhhEUdtT3ZXG0
```

```
enable password star
```

```
ip subnet-zero
```

!

```
interface FastEthernet0
```

```
ip address 192.168.0.138 255.255.255.0
```

```
interface FastEthernet1
```

```
no ip address
```

```
shutdown
```

```
!  
interface FastEthernet2  
  no ip address  
  shutdown  
!  
interface FastEthernet3  
  no ip address  
  shutdown  
!  
interface Serial0  
  no ip address  
  shutdown  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
voice-port 0  
voice-port 1  
voice-port 2  
voice-port 3  
ip classless  
line con 0  
line 1 8  
line aux 0  
line vty 0 4  
  password star  
  login  
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 2 备份路由器配置到 TFTP 服务器

一、实验性质

本实验为验证型实验，实验学时为 2 学时。

二、实验目的

能够将路由器配置文件备份到 TFTP 服务器。

三、预备知识

- 1、路由器的基本工作原理
- 2、TFTP 的基本工作原理

四、实验设备

R2624 路由器（1 台），PC 机（1 台）

五、实验内容

1、背景描述

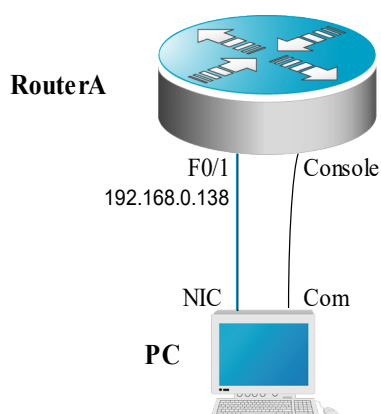
作为网络管理员，你在路由器上做好配置后，需要将其配置文件做备份，以备将来需要时。

本实验以一台 R2624 路由器为例，路由器命名为 RouterA。一台 PC 机通过串口（Com）连接到路由器的控制（Console）端口，通过网卡（NIC）连接到路由器的 fastethernet0 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，路由器的 fastethernet0 端口的 IP 地址和网络掩码分别为 192.168.0.138，255.255.255.0。

2、实现功能

保存路由器配置文件的备份。

3、拓扑结构



六、实验步骤

- 1、在路由器上配置 fastethernet0 端口的 IP 地址。

RouterA(config)# interface fastethernet0 ! 进入路由器接口配置模式
RouterA(config)# ip address 192.168.0.138 255.255.255.0 ! 配置路由器管理接口 IP 地址

RouterA(config)# no shutdown ! 开启路由器 fastethernet0 接口

验证测试: 验证路由器接口 fastethernet0 的 IP 地址已经配置和开启, PC 机与路由器有网络连通性

RouterA#show ip interface fastethernet0 ! 验证接口 fastethernet0 的 IP 地址已经配置和开启

```
FastEthernet0 is up, line protocol is up
Internet address is 192.168.0.138/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP multicast fast switching is enabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Policy routing is disabled
```

或

RouterA#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	192.168.0.138	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	unassigned	YES	unset	administratively down	down
Serial1	unassigned	YES	unset	administratively down	down

RouterA#ping 192.168.0.137 ! 验证路由器与 PC 机具有网络连通性

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 192.168.0.137, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

2、备份路由器配置。

```
RouterA#copy running-config startup-config      ! 保存交换机的当前配置
RouterA#copy startup-config tftp:               ! 备份交换机的配置到 TFTP 服务器
Address of remote host []192.168.0.137         ! 按提示输入 TFTP 服务器 IP 地址
Destination filename [config.text]?            ! 选择要保存的配置文件名称
!
%Success : Transmission success,file length 302
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 3 从 TFTP 服务器恢复路由器配置（免做）

一、实验性质

本实验为综合型实验，实验学时为 2 学时。

二、实验目的

能够从 TFTP 服务器恢复路由器配置。

三、预备知识

- 1、路由器的基本工作原理
- 2、TFTP 的基本工作原理

四、实验设备

R2624 路由器（1 台），PC 机（1 台）

五、实验内容

1、背景描述

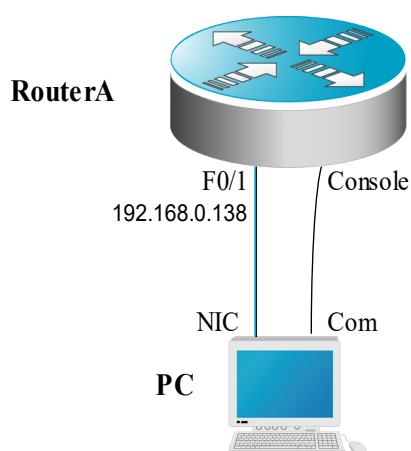
假设某台路由器的配置文件由于误操作或其它某种原因被破坏了，现在需要从 TFTP 服务器上的备份配置文件中恢复。

本实验以一台 R2624 路由器为例，路由器命名为 RouterA。一台 PC 机通过串口（Com）连接到路由器的控制（Console）端口，通过网卡（NIC）连接到路由器的 fastethernet0 端口。假设 PC 机的 IP 地址和网络掩码分别为 192.168.0.137，255.255.255.0，路由器的 fastethernet0 端口的 IP 地址和网络掩码分别为 192.168.0.138，255.255.255.0。

2、实现功能

使网络管理员可以将已有的路由器配置恢复到路由器上。

3、拓扑结构



六、实验步骤

1、在路由器上配置 fastethernet0 端口的 IP 地址。

RouterA(config)# interface fastethernet0 ! 进入路由器接口配置模式

RouterA(config)# ip address 192.168.0.138 255.255.255.0 ! 配置路由器管理接口 IP 地址

RouterA(config)# no shutdown ! 开启路由器 fastethernet0 接口

验证测试：验证路由器接口 fastethernet0 的 IP 地址已经配置和开启，PC 机与路由器有网络连通性

RouterA#show ip interface fastethernet0 ! 验证接口 fastethernet0 的 IP 地址已经配置和开启

```
FastEthernet0 is up, line protocol is up
Internet address is 192.168.0.138/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP multicast fast switching is enabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Policy routing is disabled
```

或

RouterA#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	192.168.0.138	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	unassigned	YES	unset	administratively down	down
Serial1	unassigned	YES	unset	administratively down	down

RouterA#ping 192.168.0.137 ! 验证路由器与 PC 机具有网络连通性

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 192.168.0.137, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

2、恢复路由器配置。

RouterA#copy tftp running-config ! 恢复配置到路由器的当前配置文件中

Address of remote host [255.255.255.255]? 192.168.0.137 ! 按提示输入 TFTP 服务器的

IP 地址

Name of configuration file [routera-config]? ! 选择输入配置文件名

Configure using routera-config from 192.168.0.137? [confirm]

Loading routera-config from 192.168.0.137 (via FastEthernet0): !

[OK - 608/32727 bytes]

RouterA#copy running-config startup-config ! 保存路由器的当前配置文件

或:

RouterA#copy tftp startup-config ! 恢复配置到路由器的初始配置文件中

Address of remote host [192.168.0.137]?

Name of configuration file [routera-config]?

Configure using routera-config from 192.168.0.137? [confirm]

Loading routera-config from 192.168.0.137 (via FastEthernet0): !

[OK - 608/32727 bytes]

[OK]

RouterA# copy startup-config running-config ! 将初始配置文件拷贝到路由器的当前配置文件中

验证测试：验证路由器已经更改为新的配置

RouterA#show running-config ! 验证路由器的当前配置文件为新的文件

或:

RouterA#show startup-config ! 验证路由器的初始配置文件为新的文件

hostname "RouterA"

enable secret 5 \$1\$J.MN\$6eZyYdYsJMhhEUdtT3ZXG0

enable password star

ip subnet-zero

interface FastEthernet0

ip address 192.168.0.138 255.255.255.0

interface FastEthernet1

ip address 192.168.1.138 255.255.255.0

interface FastEthernet2

no ip address

shutdown

!

interface FastEthernet3

no ip address

shutdown

!

interface Serial0

```
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
voice-port 0
voice-port 1
voice-port 2
voice-port 3
ip classless
line con 0
line 1 8
line aux 0
line vty 0 4
password star
login
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验三、虚拟局域网 VLAN （4 学时）

实验 1 交换机端口隔离

一、实验性质

本实验为设计型实验，实验学时为 2 学时。

二、实验目的

理解 Port Vlan 的配置。

三、预备知识

VLAN 的实现原理

四、实验设备

S2126G (1 台)，PC 机（2 台）

五、实验内容

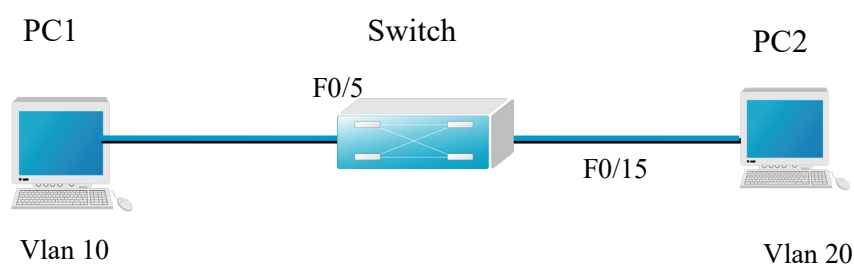
1、背景描述

假设此交换机是宽带小区域网中的一台楼道交换机，住户 PC1 连接在交换机的 0/5 口；住户 PC2 连接在交换机的 0/15 口。现要实现各家各户的端口隔离。

2、实现功能

通过划分 PORT VLAN 实现本交换端口隔离。

3、拓扑结构



六、实验步骤

1、在未划 VLAN 前两台 PC 互相 ping 可以通。

2、创建 VLAN。

Switch#configure terminal

！ 进入交换机全局配置模式。

Switch(config)# vlan 10

！ 创建 vlan 10。

Switch(config-vlan)# name test10

！ 将 Vlan 10 命名为 test10。

Switch(config)# vlan 20

！ 创建 vlan 20。

Switch(config-vlan)# name test20

！ 将 Vlan 20 命名为 test20。

验证测试

Switch#show vlan

VLAN Name	Status	Ports
1	active	Fa0/1 ,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	active	
20	active	

3、将接口分配到 VLAN。

Switch(config-if)# interface fastethernet 0/5 ! 进入 fastethernet 0/5 的接口配置模式。
Switch(config-if)# switch access vlan 10 ! 将 fastethernet 0/5 端口加入 vlan 10 中。
Switch(config-if)# interface fastethernet 0/15 ! 进入 fastethernet 0/15 的接口配置模式。
Switch(config-if)# switch access vlan 20 ! 将 fastethernet 0/15 端口加入 vlan 20 中。

4、两台 PC 互相 ping 不通。

验证测试

Switch#show vlan

VLAN Name	Status	Ports
1	active	Fa0/1 ,Fa0/2 ,Fa0/3 Fa0/4 ,Fa0/6 ,Fa0/7 Fa0/8 ,Fa0/9 ,Fa0/10 Fa0/11,Fa0/12,Fa0/13 Fa0/14,Fa0/16,Fa0/17 Fa0/18,Fa0/19,Fa0/20 Fa0/21,Fa0/22,Fa0/23 Fa0/24
10	active	Fa0/5
20	active	Fa0/15

5、注意事项

清空交换机原有 vlan 配置。

delete flash:config.text

delete flash:vlan.dat

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 2 跨交换机实现 VLAN

一、实验性质

本实验为综合型实验，实验学时为 2 学时。

二、实验目的

理解 VLAN 如何跨交换机实现。

三、预备知识

VLAN 的实现原理

四、实验设备

S2126G (2 台), PC 机 (3 台)

五、实验内容

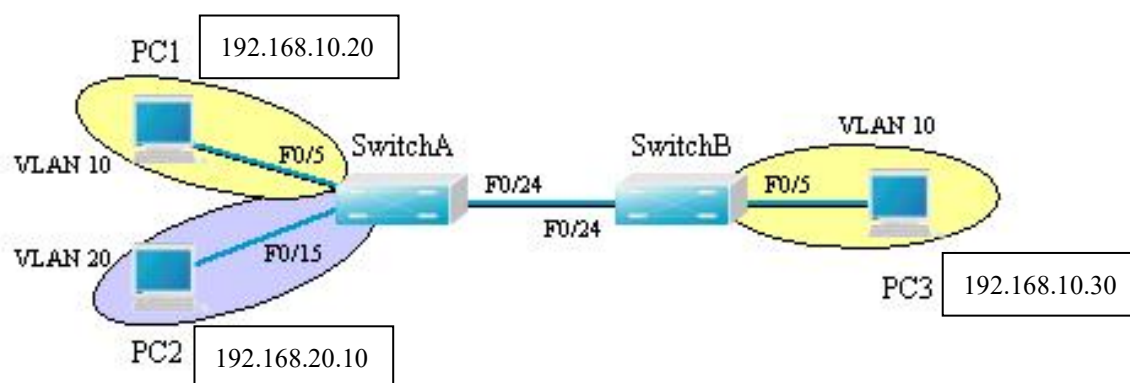
1、背景描述

假设某企业有 2 个主要部门：销售部和技术部，其中销售部门的个人计算机系统分散连接在 2 台交换机上，他们之间需要相互进行通信，但为了数据安全起见，销售部和技术部需要进行相互隔离，现要在交换机上做适当配置来实现这一目标。

2、实现功能

使在同一 VLAN 里的计算机系统能跨交换机进行相互通信，而在不同 VLAN 里的计算机系统不能进行相互通信。

3、拓扑结构



六、实验步骤

1、在交换机 SwitchA 上创建 Vlan 10，并将 0/5 端口划分到 Vlan 10 中。

SwitchA # configure terminal ! 进入全局配置模式。

SwitchA(config)# vlan 10 ! 创建 Vlan 10。

SwitchA(config-vlan)# name sales ! 将 Vlan 10 命名为 sales。

SwitchA(config-vlan)#exit

SwitchA(config)#interface fastethernet 0/5 ! 进入接口配置模式。
SwitchA(config-if)#switchport access vlan 10 ! 将 0/5 端口划分到 Vlan 10。
验证测试: 验证已创建了 Vlan 10, 并将 0/5 端口已划分到 Vlan 10 中。
SwitchA#show vlan id 10

VLAN Name	Status	Ports
10 sales	active	Fa0/5

2、在交换机 SwitchA 上创建 Vlan 20, 并将 0/15 端口划分到 Vlan 20 中。

SwitchA(config)# vlan 20 ! 创建 Vlan 20。
SwitchA(config-vlan)# name technical ! 将 Vlan 20 命名为 technical。
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/15 ! 进入接口配置模式。
SwitchA(config-if)#switchport access vlan 20 ! 将 0/15 端口划分到 Vlan 20。
验证测试: 验证已创建了 Vlan 20, 并将 0/15 端口已划分到 Vlan 20 中。
SwitchA#show vlan id 20

VLAN Name	Status	Ports
20 technical	active	Fa0/15

3、在交换机 SwitchA 上将与 SwitchB 相连的端口（假设为 0/24 端口）定义为 tag vlan 模式。

SwitchA(config)#interface fastethernet 0/24 ! 进入接口配置模式。
SwitchA(config-if)#switchport mode trunk ! 将 fastethernet 0/24 端口设为 tag vlan 模式。

验证测试: 验证 fastethernet 0/24 端口已被设置为 tag vlan 模式。

SwitchA#show interfaces fastEthernet 0/24 switchport

Interface	Switchport	Mode	Access	Native	Protected	VLAN lists
Fa0/24	Enabled	Trunk	1	1	Disabled	All

4、在交换机 SwitchB 上创建 Vlan 10, 并将 0/5 端口划分到 Vlan 10 中。

SwitchB # configure terminal ! 进入全局配置模式。
SwitchB(config)# vlan 10 ! 创建 Vlan 10。
SwitchB(config-vlan)# name sales ! 将 Vlan 10 命名为 sales。
SwitchB(config-vlan)#exit
SwitchB(config)#interface fastethernet 0/5 ! 进入接口配置模式。
SwitchB(config-if)#switchport access vlan 10 ! 将 0/5 端口划分到 Vlan 10。
验证测试: 验证已在 SwitchB 上创建了 Vlan 10, 并将 0/5 端口已划分到 Vlan 10 中。
SwitchB#show vlan id 10

VLAN Name	Status	Ports
10 sales	active	Fa0/5

5、在交换机 SwitchB 上将与 SwitchA 相连的端口（假设为 0/24 端口）定义为 tag vlan

模式。

SwitchB(config)#interface fastethernet 0/24 ! 进入接口配置模式。
SwitchB(config-if)#switchport mode trunk !将 fastethernet 0/24 端口设为 tag vlan 模式。

验证测试：验证 fastethernet 0/24 端口已被设置为 tag vlan 模式。

SwitchB#show interfaces fastEthernet 0/24 switchport

Interface	Switchport	Mode	Access	Native	Protected	VLAN lists

Fa0/24	Enabled	Trunk	1	1	Disabled	All

6、验证 PC1 与 PC3 能互相通信，但 PC2 与 PC3 不能互相通信。

C:\>ping 192.168.10.30 ! 在 PC1 的命令行方式下验证能 Ping 通 PC3 。

Pinging 192.168.10.30 with 32 bytes of data:

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.10.30:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.30 ! 在 PC2 的命令行方式下验证不能 Ping 通 PC3 。

Pinging 192.168.10.30 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.10.30:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

7、注意事项

两台交换机之间相连的端口应该设置为 tag vlan 模式。

七、考核方式

1、当场演示结果

2、提交配置文件

实验 3 通过三层交换机实现 VLAN 间路由（选做）

一、实验性质

本实验为综合型实验, 2 课时.

二、实验目的

掌握如何通过三层交换机实现 VLAN 间路由。

三、预备知识

需要预先掌握三层交换机的原理和基本用法，以及 VLAN 的原理及基本应用知识。

四、实验设备

S2126G（1 台），S3550-24（1 台），双绞线若干条。

五、实验内容

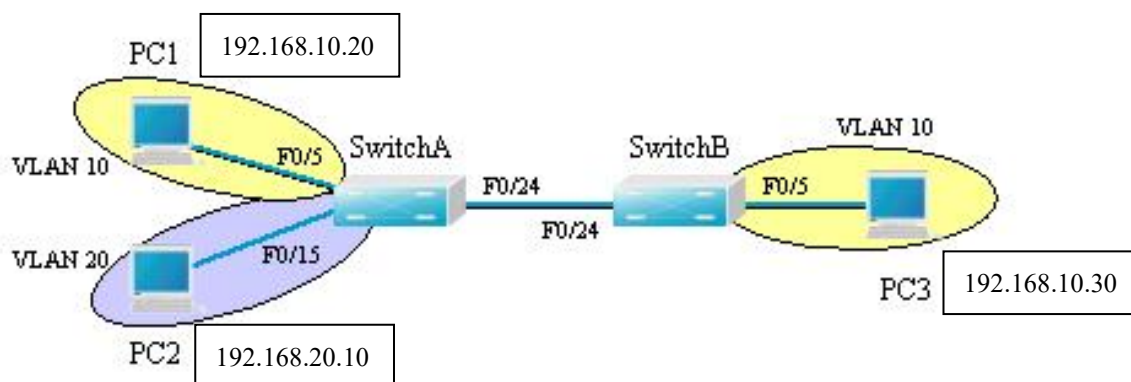
1、背景描述

假设某企业有 2 个主要部门：销售部和技术部，其中销售部门的个人计算机系统分散连接在 2 台交换机上，他们之间需要相互进行通信，销售部和技术部也需要进行相互通讯，现在在交换机上做适当配置来实现这一目标。

2、实现功能

使在同一 VLAN 里的计算机系统能跨交换机进行相互通信，而在不同 VLAN 里的计算机系统也能进行相互通信。

3、实验拓扑



六、实验步骤

1. 交换机 SwitchA 上创建 Vlan 10，并将 0/5 端口划分到 Vlan 10 中，输入如下代码：

SwitchA # configure terminal ! 进入全局配置模式。

SwitchA(config)# vlan 10 ! 创建 Vlan 10。

SwitchA(config-vlan)# name sales ! 将 Vlan 10 命名为 sales。

SwitchA(config-vlan)#exit

SwitchA(config)#interface fastethernet 0/5 ! 进入接口配置模式。

SwitchA(config-if)#switchport access vlan 10 ! 将 0/5 端口划分到 Vlan 10。

验证测试：验证已创建了 Vlan 10，并将 0/5 端口已划分到 Vlan 10 中。

显示结果：

SwitchA#show vlan id 10

VLAN Name	Status	Ports
10 sales	active	Fa0/5

2. 在交换机 SwitchA 上创建 Vlan 20，并将 0/15 端口划分到 Vlan 20 中，输入如下代码：

SwitchA(config)# vlan 20 ! 创建 Vlan 20。

SwitchA(config-vlan)# name technical ! 将 Vlan 20 命名为 technical。

SwitchA(config-vlan)#exit

SwitchA(config)#interface fastethernet 0/15 ! 进入接口配置模式。

SwitchA(config-if)#switchport access vlan 20 ! 将 0/15 端口划分到 Vlan 20。

验证测试：验证已创建了 Vlan 20，并将 0/15 端口已划分到 Vlan 20 中。

显示结果：

SwitchA#show vlan id 20

VLAN Name	Status	Ports
20 technical	active	Fa0/15

3. 在交换机 SwitchA 上将与 SwitchB 相连的端口（假设为 0/24 端口）定义为 tag vlan 模式，输入如下代码：

SwitchA(config)#interface fastethernet 0/24 ! 进入接口配置模式。

SwitchA(config-if)#switchport mode trunk ! 将 fastethernet 0/24 端口设为 tag vlan 模式。

验证测试：验证 fastethernet 0/24 端口已被设置为 tag vlan 模式。

显示结果：

SwitchA#show interfaces fastEthernet 0/24 switchport

Interface	Switchport Mode	Access	Native	Protected VLAN lists
Fa0/24	Enabled Trunk	1	1	Disabled All

4. 在交换机 SwitchB 上创建 Vlan 10，并将 0/5 端口划分到 Vlan 10 中，输入如下代码：

SwitchB # configure terminal ! 进入全局配置模式。

SwitchB(config)# vlan 10 ! 创建 Vlan 10。

SwitchB(config-vlan)# name sales ! 将 Vlan 10 命名为 sales。

SwitchB(config-vlan)#exit

SwitchB(config)#interface fastethernet 0/5 ! 进入接口配置模式。

SwitchB(config-if)#switchport access vlan 10 ! 将 0/5 端口划分到 Vlan 10。

验证测试：验证已在 SwitchB 上创建了 Vlan 10，并将 0/5 端口已划分到 Vlan 10 中。

显示结果：

SwitchB#show vlan id 10

VLAN Name	Status	Ports

10 sales	active	Fa0/5

5. 在交换机 SwitchB 上将与 SwitchA 相连的端口（假设为 0/24 端口）定义为 tag vlan 模式，输入如下代码：

SwitchB(config)#interface fastethernet 0/24 ! 进入接口配置模式。

SwitchB(config-if)#switchport mode trunk ! 将 fastethernet 0/24 端口设为 tag vlan 模式。

验证测试：验证 fastethernet 0/24 端口已被设置为 tag vlan 模式。

显示结果：

SwitchB#show interfaces fastEthernet 0/24 switchport

Interface	Switchport Mode	Access	Native	Protected	VLAN lists

Fa0/24	Enabled	Trunk	1	1	Disabled All

6. 验证 PC1 与 PC3 能互相通信，但 PC2 与 PC3 不能互相通信，输入如下代码：

C:\>ping 192.168.10.30 ! 在 PC1 的命令行方式下验证能 Ping 通 PC3 。

Pinging 192.168.10.30 with 32 bytes of data:

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Reply from 192.168.10.30: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.10.30:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.30 ! 在 PC2 的命令行方式下验证不能 Ping 通 PC3 。

Pinging 192.168.10.30 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.10.30:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

7. 设置三层交换机 VLAN 间通讯，输入如下代码：

```
SwitchA(config)# int vlan 10          ! 创建虚拟接口 vlan 10
SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0
! 配置虚拟接口 vlan 10 的地址为 192.168.10.254
SwitchA(config-if)#exit              ! 返回到全局配置模式
SwitchA(config)# int vlan 20         ! 创建虚拟接口 vlan 20
SwitchA(config-if)#ip address 192.168.20.254 255.255.255.0
! 配置虚拟接口 vlan 20 的地址为 192.168.20.254
```

8. 将 PC1 和 PC3 的默认网关设置为 192.168.10.254，将 PC2 的默认网关设置为 192.168.20.254。

测试结果

不同 VLAN 内的主机可以互相 PING 通。

注意事项

- 两台交换机之间相连的端口应该设置为 tag vlan 模式；
- 需要设置 PC 的网关。

参考配置

SwitchA#show running-config ! 显示交换机 SwitchA 的全部配置。

Building configuration...

Current configuration : 349 bytes

version 1.0

hostname SwitchA

interface FastEthernet 0/5

switchport access vlan 10

interface FastEthernet 0/15

switchport access vlan 20

interface FastEthernet 0/24

switchport mode trunk

interface Vlan 10

ip address 192.168.10.254 255.255.255.0

interface Vlan 20

ip address 192.168.20.254 255.255.255.0

end

SwitchB#show running-config ! 显示交换机 SwitchB 的全部配置。

Building configuration...

Current configuration : 284 bytes

version 1.0

hostname SwitchB

vlan 1

vlan 10

name sales

interface fastEthernet 0/5

```
switchport access vlan 10
interface fastEthernet 0/24
switchport mode trunk
end
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验四、网络地址转换 （4 学时）

实验 1 静态内部源地址转换 NAT

一、实验性质

本实验为综合型实验, 2 课时.

二、实验目的

掌握内网中一台服务器连接到 Internet 时的静态内部源地址转换 NAT 的配置和用法。

三、预备知识

需要预先掌握 Internet 中静态内部源地址转换的原理, 以及常用转换方法 NAT 的原理。

四、实验设备

R2624 或 R2620 (2 台), 双绞线若干条。

五、实验内容

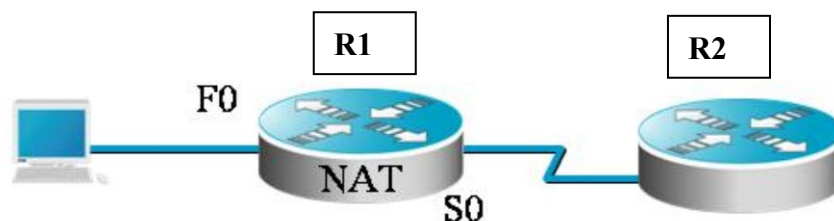
1、背景描述

某内部网络有 FTP 服务器可以为外部用户提供的服务, 服务器的 IP 地址必须采用静态地址转换, 以便外部用户可以使用这些服务。

2、实现功能

可以通过 NAT 将内部网络与外部 Internet 隔离开, 使外部用户根本不知道通过 NAT 设置的内部 IP 地址。

3、实验拓扑



六、实验步骤

1. 基本配置:

```
Red-Giant (config)#hostname R1
R1(config)#interface serial 0
R1(config-if)#ip address 192.1.1.1 255.255.255.0
```



```
R1(config-if)#clock rate 64000
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#end
```

```
R1(config)#interface fastEthernet 0
```

```
R1(config-if)#ip add 192.168.1.1 255.255.255.0
```

```
R1(config-if)#no sh
```

```
Red-Giant(config)#hostname R2
```

```
R2(config)#int serial 0
```

```
R2(config-if)#ip add 192.1.1.2 255.255.255.0
```

```
R2(config-if)#no sh
```

```
R2(config-if)#end
```

验证测试：R2#ping 192.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 192.1.1.1, timeout is 2 seconds:

!!!!

2. 配置静态 NAT 映射。

```
R1(config)#ip nat inside source static 192.168.1.2 192.1.1.3 ! 定义静态映射一一匹配
```

```
R1(config)#int fastEthernet 0
```

```
R1(config-if)#ip nat inside ! 定义内部接口
```

```
R1(config)#int serial 0
```

```
R1(config-if)#ip nat outside ! 定义外部接口
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0
```

验证测试：R1#sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	192.1.1.3	192.168.1.2	---	---

注意事项

- 不要把 inside 和 outside 应用的接口弄错；
- 要加上能使数据包向外转发的路由，比如默认路由；
- 尽量不要用广域网接口地址作为映射的全局地址。

参考配置

```
R1#sh run
```

```
Current configuration:
```

```
version 6.14(2)
```

```
hostname "R1"
```

```
ip subnet-zero
```

```
interface FastEthernet0
```

```
ip address 192.168.1.1 255.255.255.0
```

```
ip nat inside
```

```
interface FastEthernet1
```

```
no ip address
```

```
shutdown
interface FastEthernet2
  no ip address
  shutdown
interface FastEthernet3
  no ip address
  shutdown
interface Serial0
  ip address 192.1.1.1 255.255.255.0
  ip nat outside
  clock rate 64000
interface Serial1
  no ip address
  shutdown
!ip nat inside source static 192.168.1.2 192.1.1.3
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
line con 0
line aux 0
line vty 0 4
  login
end
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 2 动态内部源地址转换

一、实验性质

本实验为综合型实验, 2 课时.

二、实验目的

- 1: 掌握内网中多台主机连接到 Internet 网时, 通过分时复用进行多个内部全局地址转换技术。
- 2: 定义特定网段转发数据分时复用全局地址。

三、预备知识

掌握网络地址转换的基本原理、动态内部源地址转换的理论知识, 路由器的原理和基本用法, 及预先做过路由器/交换机的基本配置实验。

四、实验设备

R2624 (2 台)

五、实验内容

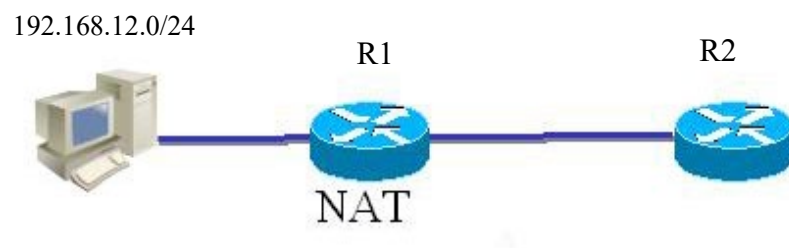
1、背景描述

某公司申请了 50 个公网 IP 地址为整个销售部门提供上网服务, 销售部门的网段是 192.168.1.0/24。合法地址不够每人分配一个, 但是销售部门平时有三分之一的人在外跑业务, 在公司内部的也不会一直需要网络服务, 根据此情况请你解决公司全局地址不够一一映射的情况。

2、实验功能

定义特定网段转发数据分时复用全局地址。

3、实验拓扑



- 1: 完成对路由器的基本配置。
- 2: 验证连通性。
- 3: 配置动态内部源地址转换。
- 4: 验证动态内部源地址转换的结果。

六、实验步骤

第 1 步：基本配置，输入如下代码：

```
Red-Giant>enable
Red-Giant#conf t
Red-Giant(config)#int s0
Red-Giant(config-if)#ip add 200.168.12.1 255.255.255.0
Red-Giant(config-if)#cl ra 64000
Red-Giant(config-if)#no sh
Red-Giant(config)#hos R1
R1(config)#int f0
R1(config-if)# ip add 192.168.12.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#end
R2(config)#int serial 0
R2(config-if)#ip add 200.168.12.100 255.255.255.0
R2(config-if)#no sh
R2(config-if)#end
```

第 2 步：验证测试：R2#ping 200.168.12.1。

显示结果：

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 200.168.12.1, timeout is 2 seconds:
!!!!
```

第 3 步：配置动态内部源地址转换，输入如下代码：

```
R1(config)#ip nat pool net200 200.168.12.2 200.168.12.50 netmask 255.255.255.0 ! 定义转
```

换地址池

```
R1(config)#access-list 1 permit 192.168.12.0 0.0.0.255 ! 定义可以转换地址的网段
```

R1(config)#ip nat inside source list 1 pool net200 ! 定义内部本地地址池调用转换地址池地址

```
R1(config)#interface s0
```

```
R1(config-if)#ip nat outside ! 定义外部接口
```

```
R1(config-if)#exit
```

```
R1(config)#interface f0
```

```
R1(config-if)#ip nat inside ! 定义内部接口
```

```
R1(config-if)#end
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0
```

第 4 步：验证测试：R1#sh ip nat translations。

显示结果：

Pro	Inside global	Inside local	Outside local	Outside global
---	200.168.12.2	192.168.12.2	---	---

注意事项

- 不要把 inside 和 outside 应用的接口弄错；
- 要加上能使数据包向外转发的路由，比如默认路由；
- 尽量不要用广域网接口地址作为映射的全局地址。

参考配置

```
sh run
```

```
Current configuration:
```

```
!
```

```
version 6.14(2)
```

```
!
```

```
hostname "R1"
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
interface FastEthernet0
```

```
ip address 192.168.12.1 255.255.255.0
```

```
ip nat inside
```

```
!
```

```
interface FastEthernet1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface FastEthernet2
```

```
no ip address
```

```

shutdown
!
interface FastEthernet3
  no ip address
  shutdown
!
interface Serial0
  ip address 200.168.12.1 255.255.255.0
  ip nat outside
  clock rate 64000
!
interface Serial1
  no ip address
  shutdown
!
ip nat pool net200 200.168.12.2 200.168.12.50 netmask 255.255.255.0
ip nat inside source list 1 pool net200
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
access-list 1 permit 192.168.12.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
  login
!
end

```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 3 复用内部全局地址转换 NAPT（选做）

一、实验性质

本实验为综合型实验，实验学时为 2 学时。

二、实验目的

掌握内网中所有主机连接到 Internet 网时，通过端口号区分的复用内部全局地址转换。

三、预备知识

掌握网络地址转换的基本原理，路由器的原理和基本用法，及预先做过路由器/交换机的基本配置实验。

四、实验设备

R2624 或 R2620 (2 台)

五、实验内容

1、背景描述

你是某公司的网络管理员，公司只向 ISP 申请了一个公网 IP 地址，希望全公司的主机都能访问外网，请你实现。

2、实现功能

允许内部所有主机在公网地址缺乏的情况下可以访问外部网络。

3、实验拓扑



六、实验步骤

1. 基本配置。

```
Red-Giant (config)#hostname R1
```

```

R1(config)#interface serial 0
R1(config-if)#ip address 192.1.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh

```

```

Red-Giant(config)#hostname R2
R2(config)#int serial 0
R2(config-if)#ip add 192.1.1.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#end

```

验证测试:

```

R2#ping 192.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.1.1.1, timeout is 2 seconds:
!!!!

```

2. 配置动态 NAT 映射。

```

R1(config)#ip nat pool to-internet 192.1.1.1 192.1.1.1 netmask 255.255.255.0
! 定义地址池

```

```

R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255 ! 定义允许转换的地址

```

```

R1(config)#ip nat inside source list 1 pool to-internet overload ! 为内部本地调用转换地址池

```

*动态 NAT 与动态 NAT 的命令差别在关键字 overload, 有则为动态 NAT, 无则为动态 NAT

```

R1(config)#int fastEthernet 0
R1(config-if)#ip nat inside ! 定义内部接口
R1(config)#int serial 0
R1(config-if)#ip nat outside ! 定义外部接口
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0

```

验证测试:

```

R1#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 192.1.1.1:3000      192.168.1.4      ---                ---

```

【注意事项】

- ✎ 不要把 inside 和 outside 应用的接口弄错;
- ✎ 要加上能使数据包向外转发的路由, 比如默认路由;
- ✎ 尽量不要用广域网接口地址作为映射的全局地址, 本例子中特定仅有一个公网地址, 实际工作中不推荐。

【参考配置】

Current configuration:

```
!  
hostname "R1"  
!  
ip subnet-zero  
!  
interface FastEthernet0  
  ip address 192.168.1.1 255.255.255.0  
  ip nat inside  
!  
interface FastEthernet1  
  no ip address  
  shutdown  
!  
interface FastEthernet2  
  no ip address  
  shutdown  
!  
interface FastEthernet3  
  no ip address  
  shutdown  
!  
interface Serial0  
  ip address 192.1.1.1 255.255.255.0  
  ip nat outside  
  clock rate 64000  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
ip nat pool to-internet 192.1.1.1 192.1.1.1 netmask 255.255.255.0 overload  
ip nat inside source list 1 pool to-internet  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0  
access-list 1 permit 192.168.1.0 0.0.0.255  
!  
line con 0  
line aux 0  
line vty 0 4
```

login

!

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验五、生成树配置 （4 学时）

实验 1 生成树协议 STP

一、实验性质

本实验为设计型实验，2 课时。

二、实验目的

进一步加深理解生成树协议 STP 原理，掌握配置方法。

三、预备知识

掌握生成树协议（STP）的原理。

生成树协议（Spanning Tree）定义在 IEEE 802.1D 中，是一种链路管理协议，它为网络提供路径冗余同时防止产生环路。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，最常见的一种是有意生成的冗余——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。

STP 允许网桥之间相互通信以发现网络物理环路。该协议定义了一种算法，网桥能够使用它创建无环路（loop-free）的逻辑拓扑结构。换句话说，STP 创建了一个由无环路树叶和树枝构成的树结构，其跨越了整个第二层网络。

四、实验设备

2 台 S2126G 交换机为例，2 台 pc，网线 4 根。

五、实验内容

1、背景描述

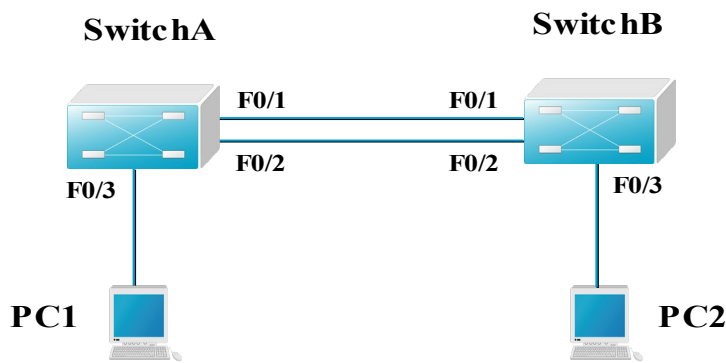
某学校为了开展计算机教学和网络办公，建立了一个计算机教室和一个校办公区，这两处的计算机网络通过两台交换机互连组成内部校园网，为了提高网络的可靠性，网络管理员用 2 条链路将交换机互连，现要在交换机上做适当配置，使网络避免环路。

本实验以 2 台 S2126G 交换机为例，2 台交换机分别命名为 SwitchA, SwitchB。PC1 与 PC2 在同一个网段，假设 IP 地址分别为 192.168.0.137，192.168.0.136，网络掩码为 255.255.255.0。

2、实现功能

使网络在有冗余链路的情况下避免环路的产生，避免广播风暴等。

3、拓扑结构



六、实验步骤

1.在每台交换机上开启生成树协议。例如对 SwitchA 做如下配置:

SwitchA#configure terminal ! 进入全局配置模式

SwitchA(config)#spanning-tree ! 开启生成树协议

SwitchA(config)#end

测试: 验证生成树协议已经开启

SwitchA#show spanning-tree ! 显示交换机生成树的状态

StpVersion : MSTP

SysStpStatus : Enabled

BaseNumPorts : 24

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops : 20

TxHoldCount : 3

PathCostMethod : Long

BPDUGuard : Disabled

BPDUFilter : Disabled

MST 0 vlans mapped : All

BridgeAddr : 00d0.f8ef.9e89

Priority : 32768

TimeSinceTopologyChange : 0d:0h:0m:8s

TopologyChanges : 0

DesignatedRoot : 800000D0F8EF9D09

RootCost : 200000

RootPort : Fa0/1

CistRegionRoot : 800000D0F8EF9E89

```

CistPathCost : 0
SwitchA#show spanning-tree interface fastthernet 0/1 ! 显示交换机接口 fastthernet 0/1 的状态
PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled

##### MST 0 vlans mapped : All
PortState : forwarding ! 显示接口 fastthernet 0/1 处于转发（forwarding）状态
PortPriority : 128
PortDesignatedRoot : 800000D0F8EF9D09
PortDesignatedCost : 0
PortDesignatedBridge : 800000D0F8EF9D09
PortDesignatedPort : 8001
PortForwardTransitions : 1
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : rootPort

```

2.设置生成树模式

SwitchA(config)#spanning-tree mode stp ! 设置生成树模式为 STP (802.1D)
 测试：验证生成树协模式为 802.1D

```

SwitchA#show spanning-tree
StpVersion : STP
SysStpStatus : Enabled
BaseNumPorts : 24
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops : 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
BridgeAddr : 00d0.f8ef.9e89
Priority : 32768
TimeSinceTopologyChange : 0d:0h:7m:0s
TopologyChanges : 0

```

DesignatedRoot : 800000D0F8EF9D09
RootCost : 200000
RootPort : Fa0/1

3.设置交换机的优先级

SwitchA(config)#spanning-tree priority 4096 ! 设置交换机 SwitchA 的优先级为 4096, 数值最小的交换机为根交换机(也称根桥), 交换机 SwitchB 的优先级采用默认优先级(32768), 因此 SwitchA 将成为根交换机。

测试: 验证交换机 SwitchA 的优先级

SwitchA#show spanning-tree

StpVersion : STP
SysStpStatus : Enabled
BaseNumPorts : 24
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops : 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
BridgeAddr : 00d0.f8ef.9e89
Priority : 4096
TimeSinceTopologyChange : 0d:0h:0m:0s
TopologyChanges : 26
DesignatedRoot : 100000D0F8EF9E89
RootCost : 0
RootPort : 0

4.综合验证测试

A.验证交换机 SwitchB 的端口 F0/ 1 和 F0/ 2 的状态。

SwitchB#show spanning-tree interface fastEthernet 0/1 ! 显示 SwitchB 的端口 fasttthernet 0/1 的状态

PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding ! SwitchB 的端口 fasttthernet 0/ 1 处于转发 (forwarding) 状态
PortPriority : 128
PortDesignatedRoot : 200000D0F8EF9E89

SwitchB#show spanning-tree interface fastEthernet 0/2 ! 显示 SwitchB 的端口 fasttheternet 0/2 的状态

B. 验证网络拓扑发生变化时，ping 的丢包情况。

C:\>ping 192.168.0.136 -t ! 从主机 PC1 ping PC2 (用连续 ping), 然后拔掉 SwitchA 与 SwitchB 的端口 F0/1 之间的连线, 观察丢包情况。显示结果如下:

45

以上结果显示丢包数为 30 个。

C. 验证网络拓扑发生变化时，交换机 SwitchB 的端口 2 的状态变化，并观察生成树的收敛时间。

SwitchB#show spanning-tree interface fastEthernet 0/2 ! 显示 SwitchB 的端口 fastthnet 0/2 的状态

```
PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding      ! SwitchB 的端口 fastthnet 0/2 转变为转发（forwarding）状态，转换时间大约 32 秒
PortPriority : 128
PortDesignatedRoot : 200000D0F8EF9E89
PortDesignatedCost : 200000
PortDesignatedBridge : 800000D0F8EF9D09
PortDesignatedPort : 8002
PortForwardTransitions : 40
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : rootPort
```

SwitchB#show spanning-tree interface fastEthernet 0/2 ! 显示 SwitchB 的端口 fastthnet 0/2 的状态

```
2003-04-27 23:27:24 @5-LINKUPDOWN:Fa0/2 changed state to up
2003-04-27 23:27:53 @4-TOPOCHANGE:Topology is changed
```

```
PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : discarding      ! SwitchB 的端口 fastthnet 0/2 转变为阻塞（discarding）状态，转换时间大约 31 秒
PortPriority : 128
PortDesignatedRoot : 200000D0F8EF9E89
PortDesignatedCost : 200000
PortDesignatedBridge : 800000D0F8EF9D09
PortDesignatedPort : 8002
PortForwardTransitions : 40
PortAdminPathCost : 0
```

PortOperPathCost : 200000

PortRole : alternatePort

注意事项

锐捷交换机缺省是关闭 spanning-tree 的，因此，如果网络在物理上存在环路，则必须手工开启 spanning-tree。

参考配置

SwitchA#show run ! 交换机 SwitchA 的全部配置

Building configuration...

Current configuration : 122 bytes

!

version 1.0

!

hostname SwitchA

spanning-tree mode stp

spanning-tree

spanning-tree mst 0 priority 4096

end

SwitchB#show run ! 交换机 SwitchB 的全部配置

Building configuration...

Current configuration : 85 bytes

!

version 1.0

!

hostname SwitchB

spanning-tree mode stp

spanning-tree

end

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 2 快速生成树协议 RSTP（选做）

一、实验性质

本实验为设计型实验，2 课时。

二、实验目的

进一步加深理解快速生成树协议 RSTP 原理，掌握配置方法。

三、预备知识

掌握快速生成树协议（RSTP）的原理。

快速生成树协议是生成树协议的改进，在原有功能的基础上提高了网络保护的性能。传统生成树倒换时间为 42s，从发现链路断裂、数据中断到数据恢复至少需要三十多秒的时间，而快速生成树协议只需 6~8 秒的时间就可以将数据流切换到备份链路上。

预先需要做生成树协议 STP 的实验。

四、实验设备

2 台 S2126G 交换机为例，2 台 pc，网线 4 根。

五、实验内容

1、背景描述

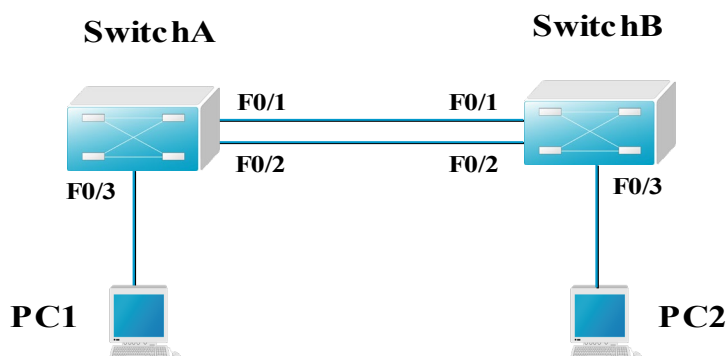
某学校为了开展计算机教学和网络办公，建立了一个计算机教室和一个校办公区，这两处的计算机网络通过两台交换机互连组成内部校园网，为了提高网络的可靠性，网络管理员用 2 条链路将交换机互连，现要在交换机上做适当配置，使网络避免环路。

本实验以 2 台 S2126G 交换机为例，2 台交换机分别命名为 SwitchA、SwitchB。PC1 与 PC2 在同一个网段，假设 IP 地址分别为 192.168.0.137，192.168.0.136，网络掩码为 255.255.255.0。

2、实现功能

使网络在有冗余链路的情况下避免环路的产生，避免广播风暴等。

3、拓扑结构



六、实验步骤

1.在每台交换机上开启生成树协议。例如对 SwitchA 做如下配置:

SwitchA#configure terminal ! 进入全局配置模式

SwitchA(config)#spanning-tree ! 开启生成树协议

SwitchA(config)#end

测试: 验证生成树协议已经开启

SwitchA#show spanning-tree ! 显示交换机生成树的状态

```
StpVersion : STP
SysStpStatus : Enabled
BaseNumPorts : 24
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops : 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
BridgeAddr : 00d0.f8ef.9e89
Priority : 4096
TimeSinceTopologyChange : 0d:0h:8m:55s
TopologyChanges : 0
DesignatedRoot : 100000D0F8EF9E89
RootCost : 0
RootPort : 0
```

SwitchA#show spanning-tree interface fastthernet 0/1 ! 显示交换机接口 fastthernet 0/1 的状态

```
PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding ! 接口 fastthernet 0/1 处于转发 (forwarding) 状态
PortPriority : 128
PortDesignatedRoot : 100000D0F8EF9E89
PortDesignatedCost : 0
PortDesignatedBridge : 100000D0F8EF9E89
```

PortDesignatedPort : 8001
PortForwardTransitions : 3
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : designatedPort

SwitchA#show spanning-tree interface fastthernet 0/2 ! 显示交换机接口 fastthernet 0/2 的状态

PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding ! 接口 fastthernet 0/2 处于转发（forwarding）状态
PortPriority : 128
PortDesignatedRoot : 100000D0F8EF9E89
PortDesignatedCost : 0
PortDesignatedBridge : 100000D0F8EF9E89
PortDesignatedPort : 8002
PortForwardTransitions : 3
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : designatedPort

2.设置生成树模式

SwitchA(config)#spanning-tree rstp ! 设置生成树模式为 802.1W

测试：验证生成树协模式为 802.1W

SwitchA#show spanning-tree

StpVersion : RSTP
SysStpStatus : Enabled
BaseNumPorts : 24
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops : 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
BridgeAddr : 00d0.f8ef.9e89

```
Priority : 4096
TimeSinceTopologyChange : 0d:0h:11m:39s
TopologyChanges : 0
DesignatedRoot : 100000D0F8EF9E89
RootCost : 0
RootPort : 0
```

3.设置交换机的优先级

SwitchA(config)#spanning-tree priority 8192 ! 设置交换机 SwithA 的优先级为 8192
测试：验证交换机 SwithA 的优先级

```
SwitchA#show spanning-tree
  StpVersion : RSTP
  SysStpStatus : Enabled
  BaseNumPorts : 24
  MaxAge : 20
  HelloTime : 2
  ForwardDelay : 15
  BridgeMaxAge : 20
  BridgeHelloTime : 2
  BridgeForwardDelay : 15
  MaxHops : 20
  TxHoldCount : 3
  PathCostMethod : Long
  BPDUGuard : Disabled
  BPDUFilter : Disabled
  BridgeAddr : 00d0.f8ef.9e89
  Priority : 8192
  TimeSinceTopologyChange : 0d:0h:13m:43s
  TopologyChanges : 0
  DesignatedRoot : 200000D0F8EF9E89
  RootCost : 0
  RootPort : 0
```

4.综合验证测试

A. 验证交换机 SwitchB 的端口 1 和 2 的状态。

SwitchB#show spanning-tree interface fastEthernet 0/1 ! 显示 SwitchB 的端口 fasttheternet 0/1 的状态

```
PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding ! SwitchB 的端口 fasttheternet 0/ 1 处于转发（forwarding）状态
```

PortPriority : 128
PortDesignatedRoot : 200000D0F8EF9E89
PortDesignatedCost : 0
PortDesignatedBridge : 200000D0F8EF9E89
PortDesignatedPort : 8001
PortForwardTransitions : 3
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : rootPort

SwitchB#show spanning-tree interface fastEthernet 0/2 ! 显示 SwitchB 的端口 fastthernet 0/2 的状态

PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : discarding ! SwitchB 的端口 fastthernet 0/2 处于阻塞（discarding）状态
PortPriority : 128
PortDesignatedRoot : 200000D0F8EF9E89
PortDesignatedCost : 200000
PortDesignatedBridge : 800000D0F8EF9D09
PortDesignatedPort : 8002
PortForwardTransitions : 3
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : designatedPort

B. 如果 SwitchA 与 SwitchB 的端口 F0/1 之间的链路 down 掉, 验证交换机 SwitchB 的端口 2 的状态, 并观察状态转换时间。

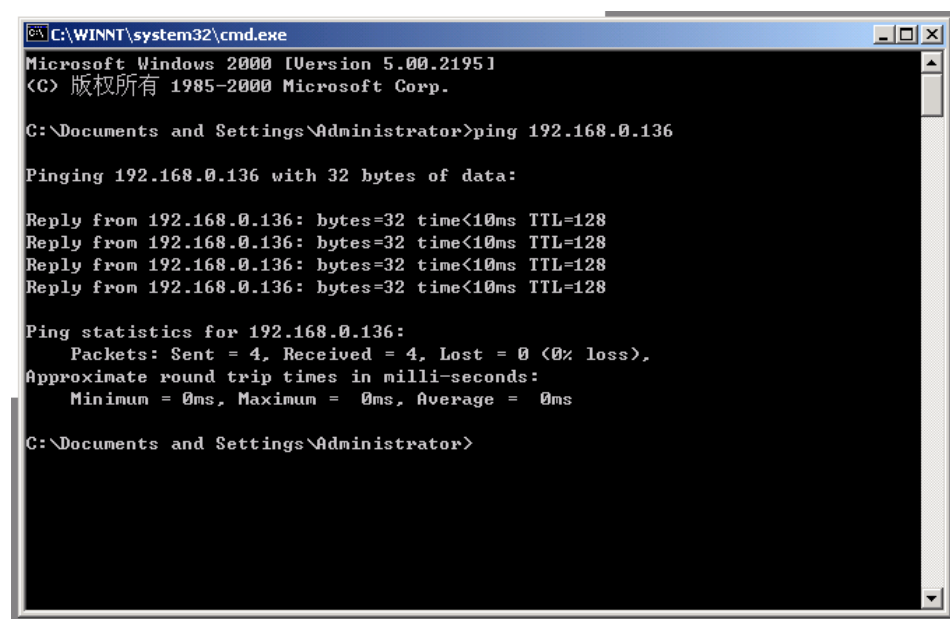
SwitchB#show spanning-tree interface fastEthernet 0/2 ! 显示 SwitchB 的端口 fastthernet 0/2 的状态

PortAdminPortfast : Disabled
PortOperPortfast : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard: Disabled
PortBPDUFilter: Disabled
PortState : forwarding ! SwitchB 的端口 fastthernet 0/2 从阻塞（discarding）状态转换到转发（forwarding）状态, 这说明生成树协议此时启用了原先处于阻塞状态的冗余链路。
! 状态转换时间大约 2 秒
PortPriority : 128

PortDesignatedRoot : 200000D0F8EF9E89
PortDesignatedCost : 200000
PortDesignatedBridge : 800000D0F8FE1E49
PortDesignatedPort : 8002
PortForwardTransitions : 8
PortAdminPathCost : 0
PortOperPathCost : 200000
PortRole : designatedPort

C. 如果 SwitchA 与 SwitchB 之间的一条链路 down 掉（如拔掉网线），验证交换机 PC1 与 PC2 仍能互相 ping 通，并观察 ping 的丢包情况。

以下为从 PC1 ping PC2 的结果（注：PC1 的 IP 地址为 192.168.0.137，PC2 的 IP 地址为 192.168.0.136）



```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.0.136

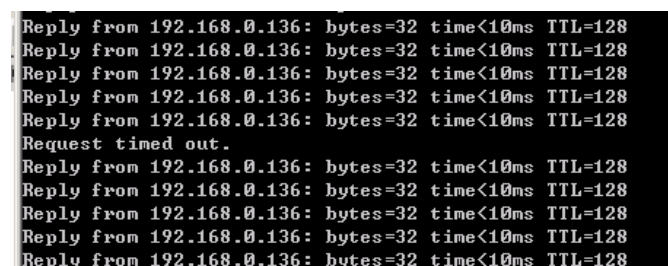
Pinging 192.168.0.136 with 32 bytes of data:

Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.0.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

C:\>ping 192.168.0.136 -t ! 从主机 PC1 ping PC2（用连续 ping），然后拔掉 SwitchA 与 SwitchB 的端口 F0/1 之间的连线，观察丢包情况。显示结果如下：



```
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Request timed out.
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
Reply from 192.168.0.136: bytes=32 time<10ms TTL=128
```

以上结果显示丢包数为 1 个。

注意事项

锐捷交换机缺省是关闭 spanning-tree 的，因此，如果网络在物理上存在环路，则必须手工开启 spanning-tree。

参考配置

SwitchA#show run ! 交换机 SwitchA 的全部配置

Building configuration...

Current configuration : 123 bytes

```
!  
version 1.0  
!  
hostname SwitchA  
spanning-tree mode rstp  
spanning-tree  
spanning-tree mst 0 priority 8192  
end
```

SwitchB#show run ! 交换机 SwitchB 的全部配置

```
Building configuration...  
Current configuration : 86 bytes  
!  
version 1.0  
!  
hostname SwitchB  
spanning-tree mode rstp  
spanning-tree  
end
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验六、路由协议 （6 学时）

实验 1 静态路由

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

通过静态路由方式实现网络的连通性，通过实验掌握路由表的基本结构，掌握基本的路由选路知识。

三、预备知识

路由的概念，路由表的结构，路由的基本原理。

预备实验：路由器的基本配置。

四、实验设备

R2624（2 台）、V35 DTE 线缆（1 根）、V35 DCE 线缆（1 根）。

五、实验内容

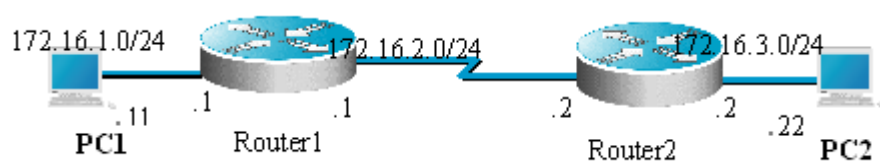
1、背景描述

假设校园网通过一台路由器连接到校园外的另一台路由器上，现要在路由器上做适当配置，实现校园网内部主机与校园网外部主机的相互通信。

2、实现功能

设置静态路由表,实现校园网内部主机与校园网外部主机的相互通信。

3、拓扑结构



六、实验步骤

在路由器 **Router1** 上配置接口的 IP 地址和串口上的时钟频率

Router1(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式

Router1(config-if)# ip address 172.16.1.1 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址

Router1(config)# no shutdown ! 开启路由器 fastethernet0 接口
!

Router1(config)# interface serial 0 ! 进入接口 S0 配置模式

Router1(config-if)# ip address 172.16.2.1 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址

Router1(config-if)#clock rate 64000 ! 配置 Router1 的时钟频率 (DCE)

Router1(config)# no shutdown ! 开启路由器 fastethernet0 接口

验证测试: 验证路由器接口的配置

Router1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.1.1	YES	manual	up	up
Serial0	172.16.2.1	YES	manual	down	down
Serial1	unassigned	YES	unset	administratively down	down

Router1#show interface serial 0

Serial0 is down, line protocol is down

Hardware is HDLC4530A

Internet address is 172.16.2.1/24

MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

Last input never, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0 (size/max/drops); Total output drops: 0

Queueing strategy: weighted fair

Output queue: 0/64/0 (size/threshold/drops)

Conversations 0/0 (active/max active)

Reserved Conversations 0/0 (allocated/max allocated)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 8 interface resets

0 output buffer failures, 0 output buffers swapped out

0 carrier transitions

DCD=down DSR=down DTR=down RTS=down CTS=down

在路由器 **Router1** 上配置静态路由

Router1(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2

或:

```
Router1(config)#ip route 172.16.3.0 255.255.255.0 serial 0
```

验证测试: 验证 Router1 上的静态路由配置

```
Router1#show ip route
```

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, FastEthernet0

C 172.16.2.0 is directly connected, Serial0

S 172.16.3.0/24 [1/0] via 172.16.2.2

在路由器 **Router2** 上配置接口的 IP 地址和串口上的时钟频率

```
Router2(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式
```

```
Router2(config-if)# ip address 172.16.3.2 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址
```

```
Router2(config)# no shutdown ! 开启路由器 fastethernet0 接口
```

!

```
Router2(config)# interface serial 0 ! 进入接口 S0 配置模式
```

```
Router2(config-if)# ip address 172.16.2.2 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址
```

```
Router2(config)# no shutdown ! 开启路由器 fastethernet0 接口
```

验证测试: 验证路由器接口的配置

```
Router2#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.3.2	YES	manual	up	up
Serial0	172.16.2.2	YES	manual	up	up
Serial1	unassigned	YES	unset	administratively down	down

```
Router2#show interface serial 0
```

Serial0 is up, line protocol is up

Hardware is HDLC4530A

Internet address is 172.16.2.2/24

MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

Last input never, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0 (size/max/drops); Total output drops: 0

Queueing strategy: weighted fair

Output queue: 0/64/0 (size/threshold/drops)

Conversations 0/0 (active/max active)

Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

在路由器 **Router2** 上配置静态路由

```
Router2(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

或:

```
Router2(config)#ip route 172.16.1.0 255.255.255.0 serial 0
```

验证测试: 验证 Router2 上的静态路由配置

```
Router2#show ip route
```

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.3.0 is directly connected, FastEthernet0

C 172.16.2.0 is directly connected, Serial0

S 172.16.1.0/24 [1/0] via 172.16.2.1

测试网络的互连互通性。

C:\>ping 172.16.3.22 ! 从 PC1 ping PC2

Pinging 172.16.3.22 with 32 bytes of data:

Reply from 172.16.3.22: bytes=32 time<10ms TTL=126

Reply from 172.16.3.22: bytes=32 time<10ms TTL=126

Reply from 172.16.3.22: bytes=32 time<10ms TTL=126

Reply from 172.16.3.22: bytes=32 time<10ms TTL=126

C:\>ping 172.16.1.11 ! 从 PC2 ping PC1

Pinging 172.16.1.11 with 32 bytes of data:

Reply from 172.16.1.11: bytes=32 time<10ms TTL=126

Reply from 172.16.1.11: bytes=32 time<10ms TTL=126

Reply from 172.16.1.11: bytes=32 time<10ms TTL=126

Reply from 172.16.1.11: bytes=32 time<10ms TTL=126

【注意事项】

如果两台路由器通过串口直接互连，则必须在其中一端设置时钟频率（DCE）。

【参考配置】

Router1#show running-config ! 显示路由器 Router1 的全部配置

Building configuration...

Current configuration:

```
version 6.14(2)
hostname "Router1"
ip subnet-zero
interface FastEthernet0
  ip address 172.16.1.1 255.255.255.0
interface Serial0
  ip address 172.16.2.1 255.255.255.0
  clock rate 64000
interface Serial1
  no ip address
  shutdown
!
voice-port 0
voice-port 1
voice-port 2
voice-port 3
ip classless
ip route 172.16.3.0 255.255.255.0 172.16.2.2
line con 0
line aux 0
line vty 0 4
  login
end
```

Router2#show running-config ! 显示路由器 Router2 的全部配置

Building configuration...

Current configuration:

```
version 6.14(2)
hostname "Router2"
ip subnet-zero
interface FastEthernet0
  ip address 172.16.3.2 255.255.255.0
interface Serial0
  ip address 172.16.2.2 255.255.255.0
interface Serial1
  no ip address
  shutdown
!
voice-port 0
voice-port 1
voice-port 2
```

```
voice-port 3
ip classless
ip route 172.16.1.0 255.255.255.0 172.16.2.1
line con 0
line aux 0
line vty 0 4
  login
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 2 RIP V1 路由协议基本配置

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

掌握在路由器上配置 RIP V1 路由协议的方法，通过实验掌握 RIP V1 路由协议的原理。

三、预备知识

掌握路由的基本概念、RIP V1 路由协议的原理等理论知识

预备试验：路由器的基本配置，静态路由

四、实验设备

R2624 路由器(2 台)、V35DCE (1 根)、V35DTE (1 根)。

五、实验内容

1、背景描述

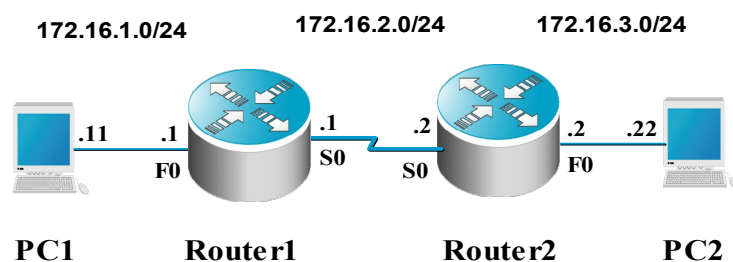
假设校园网通过一台路由器连接到校园外的另一台路由器上，现要在路由器上做适当配置，实现校园网内部主机与校园网外部主机的相互通信。

本实验以 2 台 R2624 路由器为例，路由器分别命名为 Router1 和 Router2，路由器之间通过串口采用 V35 DCE/DTE 电缆连接，DCE 端连接到 Router1（R2624）上。PC1 的 IP 地址和缺省网关分别为 172.16.1.11 和 172.16.1.1，PC2 的 IP 地址和缺省网关分别为 172.16.3.22 和 172.16.3.2，网络掩码都是 255.255.255.0。

2、实现功能

在 RIP V1 下，实现校园网内部主机与校园网外部主机的相互通信。

3、拓扑结构



六、实验步骤

1. 在路由器 Router1 上配置接口的 IP 地址和串口上的时钟频率。

Router1(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式

Router1(config-if)# ip address 172.16.1.1 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址

Router1(config-if)# no shutdown ! 开启路由器 fastethernet0 接口
!

Router1(config)# interface serial 0 ! 进入接口 S0 配置模式

Router1(config-if)# ip address 172.16.2.1 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址

Router1(config-if)# clock rate 64000 ! 配置 Router1 的时钟频率 (DCE)

Router1(config-if)# no shutdown ! 开启路由器 serial 0 接口

验证测试: 验证路由器接口的配置和状态

Router1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.1.1	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	172.16.2.1	YES	manual	down	down
Serial1	unassigned	YES	unset	administratively down	down

注: 串口 Serial0 的链路层状态是 down, 这是因为对端接口还没有配置。

2. 在路由器 Router1 上配置 RIP V1 路由协议。

Router1(config)# router rip ! 创建 RIP 路由进程

Router1(config-router)# network 172.16.0.0 ! 定义关联网络 (必须是直连的主类网络地址)

验证测试: 验证 Router1 上的 RIP V1 路由表

Router1#show ip route

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.1.0 is directly connected, FastEthernet0

C 172.16.2.0 is directly connected, Serial0

3. 在路由器 Router2 上配置接口的 IP 地址。

Router2(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式

Router2(config-if)# ip address 172.16.3.2 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址

Router2(config-if)# no shutdown ! 开启路由器 fastethernet0 接口
!

Router2(config)# interface serial 0 ! 进入接口 S0 配置模式

Router2(config-if)# ip address 172.16.2.2 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址

Router2(config-if)# no shutdown ! 开启路由器 serial 0 接口

验证测试：验证路由器接口的配置和状态

Router2#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.3.2	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	172.16.2.2	YES	manual	up	up
Serial1	unassigned	YES	unset	administratively down	down

在路由器 Router2 上配置 RIP V1 路由协议。

Router2(config)# router rip ! 创建 RIP 路由进程

Router2(config-router)#network 172.16.0.0 ! 定义关联网络（必须是直连的主类网络地址）

验证测试：验证 Router2 和 Router1 上的 RIP V1 路由表

Router2#show ip route

Codes: C - connected, S - static, R - RIP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:16, Serial0 ! Router2 通过 RIP 协议获得的路由

C 172.16.2.0 is directly connected, Serial0

C 172.16.3.0 is directly connected, FastEthernet0

Router1#sh ip route

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

C 172.16.1.0 is directly connected, FastEthernet0

C 172.16.2.0 is directly connected, Serial0

R 172.16.3.0 [120/1] via 172.16.2.2, 00:00:08, Serial0 ! Router1 通过 RIP 协议获得的路由

测试网络的连通性。

C:\>ping 172.16.3.22 ! 从 PC1 ping PC2


```
C:\WINDOWS\System32\cmd.exe

C:\>ping 172.16.3.22

Pinging 172.16.3.22 with 32 bytes of data:

Reply from 172.16.3.22: bytes=32 time=18ms TTL=126
Reply from 172.16.3.22: bytes=32 time=18ms TTL=126
Reply from 172.16.3.22: bytes=32 time=18ms TTL=126
Reply from 172.16.3.22: bytes=32 time=18ms TTL=126

Ping statistics for 172.16.3.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 18ms, Average = 18ms
```

C:\>ping 172.16.1.11 ! 从 PC2 ping PC1

```
C:\>ping 172.16.1.11

Pinging 172.16.1.11 with 32 bytes of data:

Reply from 172.16.1.11: bytes=32 time=18ms TTL=126
Reply from 172.16.1.11: bytes=32 time=18ms TTL=126
Reply from 172.16.1.11: bytes=32 time=18ms TTL=126
Reply from 172.16.1.11: bytes=32 time=18ms TTL=126

Ping statistics for 172.16.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 18ms, Average = 18ms
```

【注意事项】

在串口上配置时钟频率时，一定要在电缆 DCE 端的路由器上配置，否则链路不通；定义关联网络时，命令 network 后面必须是与该路由器直连的主类网络地址。

【参考配置】

Router1#show running-config ! 显示路由器 Router1 的全部配置

Building configuration...

Current configuration:

version 6.14(2)

hostname "Router1"

enable secret 5 \$1\$CT43\$gMntVy1ViUeKqRfmWanw/0

ip subnet-zero

interface FastEthernet0

ip address 172.16.1.1 255.255.255.0

interface FastEthernet1

no ip address

shutdown

!

interface FastEthernet2

no ip address

shutdown

!

interface FastEthernet3

no ip address

```

shutdown
!
interface Serial0
 ip address 172.16.2.1 255.255.255.0
 clock rate 64000
interface Serial1
 no ip address
 shutdown
!
voice-port 0
voice-port 1
voice-port 2
voice-port 3
router rip
 network 172.16.0.0
ip classless
line con 0
line 1 8
line aux 0
line vty 0 4
 password star
 login
end
Router2#show running-config    ! 显示路由器 Router2 的全部配置
Building configuration...
Current configuration:
hostname "Red-Giant"
enable secret 5 $1$TK6E$V8xIZJ40aN1LYoUd27U45/
ip subnet-zero
interface FastEthernet0
 ip address 172.16.3.2 255.255.255.0
interface FastEthernet1
 no ip address
 shutdown
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
interface Serial0

```

```
ip address 172.16.2.2 255.255.255.0
interface Serial1
no ip address
shutdown
!
router rip
network 172.16.0.0
ip classless
line con 0
line aux 0
line vty 0 4
password star
login
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 3 RIP V2 路由协议基本配置

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

掌握在路由器和三层交换机上配置 RIP V2，从而实现网络的互连互通，实现信息的共享和传递。通过实验掌握 RIP V2 路由协议的原理。

三、预备知识

掌握路由的基本概念、RIP V2 路由协议的原理等理论知识。

预备试验：RIP Version 1 路由协议基本配置。

四、实验设备

R2624（2 台）、V35DCE（1 根）、V35DTE（1 根）。

五、实验内容

1、背景描述

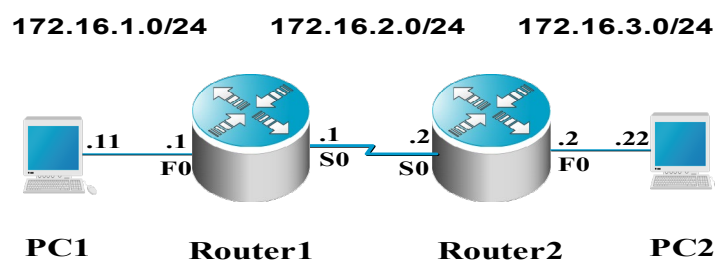
假设校园网通过一台路由器连接到校园外的另一台路由器上，现要在路由器上做适当配置，实现校园网内部主机与校园网外部主机的相互通信。

本实验以 2 台 R2624 路由器为例，路由器分别为 Router1 和 Router2，路由器之间通过串口采用 V35 DCE/DTE 电缆连接。将电缆的 DCE 端连接到 Router1 的串口 Serial 0 上，PC1 的 IP 地址和缺省网关分别为 172.16.1.11 和 172.16.1.1，PC2 的 IP 地址和缺省网关分别为 172.16.3.22 和 172.16.3.2，网络掩码都是 255.255.255.0。

2、实现功能

在 RIP V2 下，实现校园网内部主机与校园网外部主机的相互通信。

3、拓扑结构



六、实验步骤

1. 在路由器 **Router1** 上配置接口的 IP 地址和串口上的时钟频率，输入如下代码：

Router1(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式

Router1(config-if)# ip address 172.16.1.1 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址

Router1(config-if)# no shutdown ! 开启路由器 fastethernet0 接口

!

Router1(config)# interface serial 0 ! 进入接口 S0 配置模式

Router1(config-if)# ip address 172.16.2.1 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址

Router1(config-if)# clock rate 64000 ! 配置 Router1 的时钟频率（DCE）

Router1(config-if)# no shutdown ! 开启路由器 serial 0 接口

验证测试：验证路由器接口的配置

Router1#show ip interface brief

显示如下：

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.1.1	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	172.16.2.1	YES	manual	up	down
Serial1	unassigned	YES	unset	administratively down	down

2. 路由器 **Router1** 上配置 **RIP V2** 路由协议，输入如下代码：

Router1(config)# router rip ! 创建 RIP 路由进程

Router1(config-router)# version 2 ! 定义 RIP 版本

Router1(config-router)# network 172.16.0.0 ! 定义关联网络（必须是直连的主类网络地址）

验证测试：验证 Router1 上的 RIP V2 路由表

Router1#show ip route

显示如下：

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.1.0 is directly connected, FastEthernet0

C 172.16.2.0 is directly connected, Serial0

路由器 **Router2** 上配置接口的 IP 地址和串口上的时钟频率，输入如下代码：

Router2(config)# interface fastethernet 0 ! 进入接口 F0 的配置模式

Router2(config-if)# ip address 172.16.3.2 255.255.255.0 ! 配置路由器接口 F0 的 IP 地址

Router2(config-if)# no shutdown ! 开启路由器 fastethernet0 接口

!

Router2(config)# interface serial 0 ! 进入接口 S0 配置模式
 Router2(config-if)# ip address 172.16.2.2 255.255.255.0 ! 配置路由器接口 S0 的 IP 地址

Router2(config-if)# no shutdown ! 开启路由器 serial 0 接口

验证测试：验证路由器接口的配置

Router2#show ip interface brief

显示如下：

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.3.2	YES	manual	up	up
FastEthernet1	unassigned	YES	unset	administratively down	down
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	172.16.2.2	YES	SLARP	up	up
Serial1	unassigned	YES	unset	administratively down	down

3. 路由器 Router2 上配置 RIP V2 路由协议，输入如下代码：

Router2(config)# router rip ! 创建 RIP 路由进程

Router2(config-router)#version 2 ! 定义 RIP 版本

Router2(config-router)#network 172.16.0.0 ! 定义关联网络（必须是直连的主类网络地址）

验证测试：验证 Router2 上的 RIP V2 路由表

Router2#show ip route

显示如下：

Codes: C - connected, S - static, R - RIP

O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

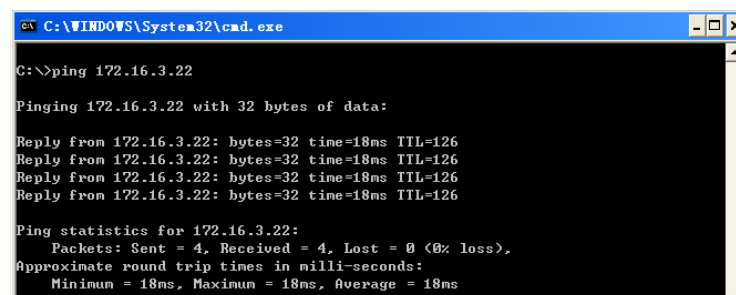
R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:04, Serial0

C 172.16.2.0 is directly connected, Serial0

C 172.16.3.0 is directly connected, FastEthernet0

试网络的连通性，输入如下代码：

C:\>ping 172.16.3.22 ! 从 PC1 ping PC2



显示网络连通

【注意事项】

当定义 RIP 版本后，路由器只接收该版本的路由信息；

也可以在接口上定义只接收或发送某一 RIP 版本或两个版本的路由信息；

缺省情况下，路由器接收两个 RIP 版本的路由信息，但只发送版本 1 的路由信息；在三层交换机上配置 RIP V2 与在路由器上配置一样。

【参考配置】

Router1#show running-config ! 显示路由器 Router1 的全部配置

Current configuration:

```
!  
version 6.14(2)  
!  
hostname "Router1"  
!  
enable secret 5 $1$ntvG$M9anDBfVvB7o33mc.TaZk0  
!  
ip subnet-zero  
!  
interface FastEthernet0  
 ip address 172.16.1.1 255.255.255.0  
!  
interface FastEthernet1  
 no ip address  
 shutdown  
!  
interface FastEthernet2  
 no ip address  
 shutdown  
!  
interface FastEthernet3  
 no ip address  
 shutdown  
!  
interface Serial0  
 ip address 172.16.2.1 255.255.255.0  
 clock rate 64000  
!  
interface Serial1  
 no ip address  
 shutdown  
!  
voice-port 0  
!  
voice-port 1  
!  
voice-port 2  
!  
voice-port 3
```

```

voice-port 0
!
voice-port 1
!
voice-port 2
!
voice-port 3
router rip
  version 2
  network 172.16.0.0
!
ip classless
!
line con 0
line 1 8
line aux 0
line vty 0 4
  password star
  login
!
end
Router2#show running-config    ! 显示路由器 Router2 的全部配置
Building configuration
Current configuration:
!
hostname "Router2"
!
enable secret 5 $1$Cqtw$OZvzRU/hDE6/1c5XnBINI/
!
ip subnet-zero
!
  interface FastEthernet0
    ip address 172.16.3.2 255.255.255.0
  !
  interface FastEthernet1
    no ip address
    shutdown
  !
  interface Serial0
    ip address 172.16.2.2 255.255.255.0
  !
  interface Serial1
    no ip address
    shutdown

```



```
!  
router rip  
  version 2  
  network 172.16.0.0  
!  
ip classless  
!  
line con 0  
line aux 0  
line vty 0 4  
  password star  
  login  
!  
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件



实验 4 OSPF 单区域基本配置（选做）

一、实验性质

本实验为设计型实验，2 课时

二、实验目的

OSPF 基本配置技术

三、预备知识

需要了解 IP 子网间的路由技术，理解什么是路由，路径选择的度量标准是什么，掌握路由算法的分类原则以及如何构建路由表，并重点掌握链路状态路由协议的工作原理。了解 RIP 和 OSPF 两个协议的区别。

典型的路由选择方式有两种：静态路由和动态路由。动态路由协议又分为外部网关协议和内部网关协议。内部网关协议是指在自治系统内部交换路由选择信息的路由协议，常用的因特网内部网关协议有 OSPF、RIP。

链路状态路由协议为路由计算而重新生成整个网络的准备拓扑，如 OSPF 等。链路状态路由选择比距离向量路由选择需要更强的处理能力，但它可以对路由选择过程提供更多的控制和对变化响应更快。路由选择可以基于避开拥塞区、线路的速度、线路的费用或各种优先级别。

OSPF(Open Shorted Path First,开放式最短路径优先)是一种链路状态路由协议。每一个 OSPF 路由器都维护一个相同的网络拓扑数据库，从这个数据库中，可以构造一个最短路径树来计算路由表。OSPF 的收敛速度比 RIP 要快，而且在更新路由信息时，产生的流量也较少。为了管理大规模的网络，OSPF 采用分层的连接结构，将自治系统分成不同的区域，以减少路由重计算的时间。

预先做过 RIP 路由协议相关实验。

四、实验设备

R2624 路由器（2 台）、V35DCE（1 根）、V35DTE（1 根）。

五、实验内容

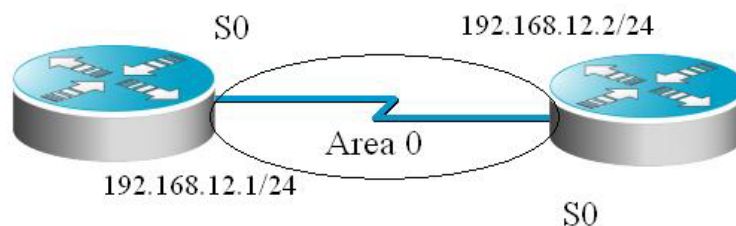
1、背景描述

为某企业设计一个网络骨干结构，选择使用 OSPF 路由协议来构建。

2、实现功能

构建 OSPF 骨干区域，为网络拓展打基础。

3、拓扑结构



六、实验步骤

1.基本配置，输入如下代码：

```
Red-Giant>en
Red-Giant#conf t
Red-Giant(config)#hostname R1 ! 更改路由器主机名
R1(config)#int s0
R1(config-if)#ip add 192.168.12.1 255.255.255.0 ! 为接口配置地址
R1(config-if)#clock rate 64000 ! 设置时钟速率 在 DTE 端不用设置
R1(config-if)#no sh
Red-Giant>en
Red-Giant#conf t
Red-Giant(config)#hostname R2
R2(config)#int s0
R2(config-if)#ip add 192.168.12.2 255.255.255.0
R2(config-if)#no sh
```

2.验证测试：R2#ping 192.168.12.1

显示如下：

Sending 5, 100-byte ICMP Echoes to 192.168.12.1, timeout is 2 seconds:

!!!!

启动 OSPF 路由协议，输入如下代码：

```
R1(config)#router ospf 1 !启动 ospf 进程
R1(config-router)#net 192.168.12.0 0.0.0.255 area 0 ! 声明网段属于区域 0
R1(config-router)#end
R2(config)#router ospf 1
R2(config-router)#net 192.168.12.0 0.0.0.255 area 0
R2(config-router)#end
```

3.验证测试：R1#sh ip os nei （以 R1 为例）

显示如下：

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.12.2	1	FULL/ -	00:00:37	192.168.12.2	Serial0

注意事项

在广域网口 DCE 端要配置时钟速率；

ospf 进程号要相同；

声明网段后，掩码用反掩码。

参考配置

R2#sh run （以 R2 为例）

Building configuration...

Current configuration:

!

version 6.14(2)

!

hostname "R2"

!

ip subnet-zero

!

interface FastEthernet0

no ip address

shutdown

!

interface FastEthernet1

no ip address

shutdown

!

interface FastEthernet2

no ip address

shutdown

!

interface FastEthernet3

no ip address

shutdown

!

interface Serial0

ip address 192.168.12.2 255.255.255.0

!

interface Serial1

no ip address

shutdown

!

router ospf 1

network 192.168.12.0 0.0.0.255 area 0

!

ip classless

!

line con 0

```
line aux 0  
line vty 0 4  
login
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验七、IP 访问列表 （2 学时）

实验 1 编号的标准 IP 访问列表

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

掌握编号的标准 IP 访问列表规则及配置。实现网段间互相访问的安全控制。

三、预备知识

掌握访问控制列表 ACL 的基本概念、三层交换机和路由器的工作原理等理论知识。

预备试验：路由器的基本配置。

四、实验设备

R2624 或 R2620 路由器（1 台）。

注：本实验也可以用三层交换机，但要把相应的端口设置为路由模式，输入“no switchport”命令。

五、实验内容

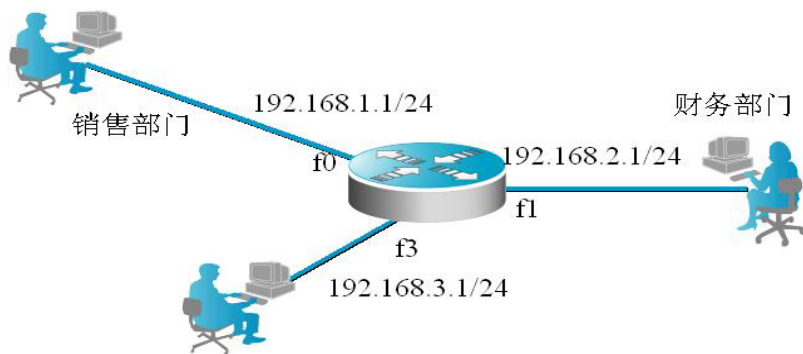
1、背景描述

假设你是一个公司的网络管理员，公司的经理部、财务部门和销售部门分属不同的三个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部门进行访问，但经理部可以对财务部门进行访问

2、实现功能

实现对部门的访问控制。

3、拓扑结构



六、实验步骤

1. 基本配置。

```

Red-Giant>
Red-Giant>enable
Red-Giant#configure terminal
Red-Giant(config)#hostname R1
R1(config)# interface fastEthernet 0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)# interface fastEthernet 1
R1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#interface fastEthernet 3
R1(config-if)#ip add 192.168.3.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#end
测试命令：show ip interface brief ! 观察接口状态
R1#sh ip int brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	192.168.1.1	YES	manual	up	up
FastEthernet1	192.168.2.1	YES	manual	up	up
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	192.168.3.1	YES	manual	up	up
Serial0	unassigned	YES	unset	administratively down	down
Serial1	unassigned	YES	unset	administratively down	down

2. 配置标准 IP 访问控制列表。

R1(config)#access-list 1 deny 192.168.1.0 0.0.0.255 ! 拒绝来自 192.168.1.0 网段的流量通过。

R1(config)#access-list 1 permit 192.168.3.0 0.0.0.255 ! 允许来自 192.168.3.0 网段的流量通过。

验证测试：

```
show access-lists 1
```

```
R1#sh access-lists 1
```

```
Standard IP access list 1
```

```
deny 192.168.1.0, wildcard bits 0.0.0.255
```

```
permit 192.168.3.0, wildcard bits 0.0.0.
```

3. 把访问控制列表在接口下应用。

```
R1(config)# interface fastEthernet 1
```

```
R1(config-if)#ip access-group 1 out ! 在接口下访问控制列表出栈流量调用
```

验证测试：

```
show ip access-lists 1
```

ping (192.168.1.0 网段的主机不能 ping 通 192.168.2.0 网段的主机；192.168.3.0 网段的主机能 ping 通 192.168.2.0 网段的主机)。

【注意事项】

注意在访问控制列表的网络掩码是反掩码；

标准控制列表要应用在尽量靠近目的地址的接口；

注意标准访问控制列表的编号是从 1-99。

【参考配置】

```
sh run
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
hostname "R1"
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
interface FastEthernet0
```

```
ip address 192.168.1.1 255.255.255.0
```

```
!
```

```
interface FastEthernet1
```

```
ip address 192.168.2.1 255.255.255.0
```

```
ip access-group 1 out
```

```
!
```

```
interface FastEthernet2
```

```
no ip address
```

```
shutdown
```

```
interface FastEthernet3
```

```
ip address 192.168.3.1 255.255.255.0
```

```
!
```

```
interface Serial0
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface Serial1
```



```
no ip address
shutdown
!
ip classless
access-list 1 deny    192.168.1.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
    login
!
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验 2 编号的扩展 IP 访问列表

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

掌握编号的扩展 IP 访问列表规则及配置。

三、预备知识

掌握访问控制列表 ACL 的基本概念、三层交换机和路由器的工作原理等理论知识。

预备试验：路由器的基本配置。

四、实验设备

R2624 或 R2620 路由器（1 台）。

五、实验内容

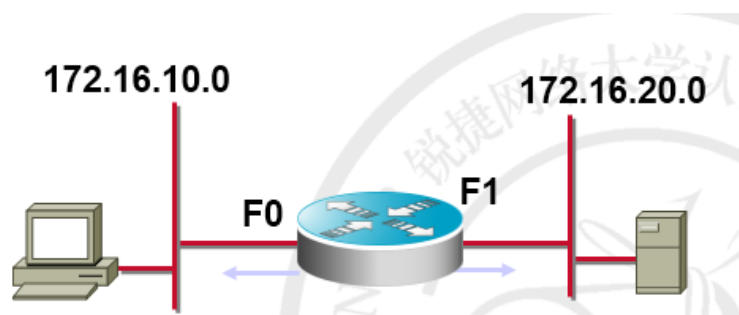
1、背景描述

你是学校的网络管理员，学校规定每年新入学的学生所在的网段不能通过学校的 FTP 服务器上网，学校规定新生所在网段是 172.16.10.0/24, 学校服务器所在网段是 172.16.20.0/24。

2、实现功能

实现对网络服务访问的安全控制。

3、实验拓扑



六、实验步骤

1. 基本配置。

```
Red-Giant#configure terminal
```

```
Red-Giant(config)#interface fastEthernet 0
```

```

Red-Giant(config-if)#ip address 172.16.10.1 255.255.255.0
Red-Giant(config-if)#no sh
Red-Giant(config-if)#exi
Red-Giant(config)#interface fastEthernet 1
Red-Giant(config-if)#ip add 172.16.20.1 255.255.255.0
Red-Giant(config-if)#no sh
Red-Giant(config-if)#end

```

验证测试

Red-Giant#sh ip interface brief ! 观察接口状态

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	172.16.10.1	YES	manual	up	up
FastEthernet1	172.16.20.1	YES	manual	up	up
FastEthernet2	unassigned	YES	unset	administratively down	down
FastEthernet3	unassigned	YES	unset	administratively down	down
Serial0	unassigned	YES	unset	administratively down	down
Serial1	unassigned	YES	unset	administratively down	down

2. 配置扩展 IP 访问控制列表。

```

Red-Giant(config)# access-list 101 deny tcp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255 eq ftp

```

! 禁止规定网段对服务器进行 www 访问

```

Red-Giant(config)# access-list 101 permit ip any any ! 允许其他流量通过

```

验证测试

```

Red-Giant#show access-lists 101

```

Extended IP access list 101

```

deny tcp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255 eq ftp
permit ip any any

```

3. 把访问控制列表在接口下应用。

```

Red-Giant(config)#interface fastEthernet 0

```

```

Red-Giant(config-if)#ip access-group 101 in ! 访问控制列表在接口下 in 方向应用

```

```

Red-Giant(config-if)#end

```

验证测试

```

show ip interface f 0

```

```

FastEthernet0 is up, line protocol is up
Internet address is 172.16.10.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 101

```

【注意事项】

- 访问控制列表要在接口下应用。

⚡ 要注意 deny 某个网段后要 permit 其他网段。

【参考配置】

```
Red-Giant#sh run
Building configuration...

Current configuration:
!
version 6.14(2)
!
hostname "Red-Giant"
!
ip subnet-zero
!
interface FastEthernet0
 ip address 172.16.10.1 255.255.255.0
 ip access-group 101 in
!
interface FastEthernet1
 ip address 172.16.20.1 255.255.255.0
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
ip classless
access-list 101 deny    tcp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255 eq www
access-list 101 permit ip any any
!
line con 0
```

line aux 0

line vty 0 4

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验八、交换机安全（4 学时）

实验 1 设备口令及权限

一、实验性质

本实验为综合设计型实验, 2 课时.

二、实验目的

- 1: 掌握如何设置交换机的口令及权限。
- 2: 通过设置不同的用户级别和权限来实现网络管理的灵活性和安全性。

三、预备知识

需要预先掌握交换机的工作原理、网络管理安全性定义的理论知识, 及了解 `configure` 全局配置模式、`exec` 特权模式、`interface` 接口配置模式的定义及各模式的命令语句。

应预先做过交换机的基本配置实验。

四、实验设备

S2126G (1 台)

五、实验内容

1、背景描述

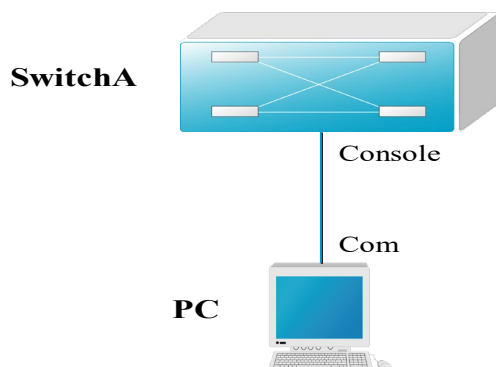
某公司有一名专职网络管理员, 由于网络管理任务较重, 因此他向公司经理请求在公司内给他找一名非专职的网络管理助手, 协助进行一些管理工作, 从网络管理的安全性方面考虑, 他决定授予该助手一定的操作权限 (比如在交换机上执行 `configure` 命令), 但不是全部权限, 现在需要在交换机上做适当的配置。

本实验以一台 S2126G 交换机为例, 交换机名为 SwitchA。

2、实验功能

通过设置不同的用户级别和权限来实现网络管理的灵活性和安全性。

3、实验拓扑



- 1: 在交换机上配置用户级别和口令。
- 2: 验证用户级别和口令。
- 3: 给配置的用户级别进行命令授权。
- 4: 验证命令授权。

六、实验步骤

第 1 步：在交换机上配置用户级别和口令，输入如下代码：

```
SwitchA#enable secret level 10 0 star
```

设置用户级别 10 及其口令（star），0 表示加密类型为明文输入形式

第 2 步：验证验证用户级别和口令。

测试：显示结果：

```
SwitchA>show privilege
```

Current privilege level is 1

```
SwitchA>enable 10
```

```
SwitchA#show privilege
```

Current privilege level is 10

```
SwitchA#disable
```

第 3 步：给配置的用户级别进行命令授权，输入如下代码：

```
Switch(config)#privilege exec level 10 configure
```

第 4 步：验证验证命令授权。

测试：显示结果：

```
SwitchA# configure
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SwitchA(config)#
```

注意事项

用户级别范围是 0—15 级，级别 0 是权限最低的级别，只能执行 `disable`、`enable`、`exit`、`help` 和 `logout` 命令，第 1 级是缺省的用户级别，第 15 级缺省是拥有全部的权限的特权级别。

可以将一些较高级别的命令的权限授予一些较低的级别，就像创建一个 `guest` 用户一样，该用户只有少量的可执行的命令。

可以授权的命令模式包括：`configure` 全局配置模式、`exec` 特权模式、`interface` 接口配置模式。

重设 `configure` 命令的缺省权限用 `Switch (config) # privilege exec reset configure`;

即使加密类型为明文输入形式，在保存时仍自动转换为密文保存。

参考配置

```
SwitchA#show running-config
Building configuration...
Current configuration : 297 bytes
!
version 1.0
!
hostname SwitchA
privilege exec level 10 configure
enable secret level 1 5 $2u_;C,t38U0<D+S4tj9=G1XQ7R:>H.Y
enable secret level 10 5 $2n'.tj93jo+/7R:4kE,1u_;Ql&-8U0<
enable secret level 15 5 $2fjo+/73cgkE,1u4dhl&-8UQein'.tj
!
interface vlan 1
 no shutdown
!
end
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 2 静态 MAC 地址的配置

一、实验性质

本实验为综合型实验, 2 课时.

二、实验目的

- 1: 掌握如何通过手工方式静态添加 MAC 地址到交换机。
- 2: 通过在交换机上手工配置静态 MAC 地址来减少网络广播流量。

三、预备知识

了解交换网络中交换机的工作原理。了解静态 MAC 地址与动态 MAC 地址的定义与应用。
了解网络广播流量的控制方法及原理。应预先做过交换机的基本配置试验。

四、实验设备

S2126G (1 台)

五、实验内容

1、背景描述

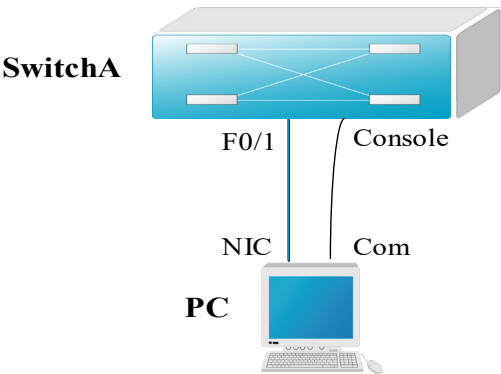
在交换网络中, 交换机可以通过动态方式学习 MAC 地址, 也可以通过静态方式配置 MAC 地址与端口的映射。某公司一名专职网络管理员, 在管理网络时, 考虑到某些主机的配置和位置比较固定, 他决定配置静态 MAC 地址, 这样可以减少一些因动态 MAC 地址老化而导致的网络广播流量, 以提高网络效率和稳定性。

本实验以一台 S2126G 交换机为例, 交换机名为 SwitchA。一台 PC 机通过串口 (Com) 连接到交换机的控制 (Console) 端口, 通过网卡 (NIC) 连接到交换机的 fastethernet 0/1 端口。

2、实验功能

通过在交换机上手工配置静态 MAC 地址来减少网络广播流量。

3、实验拓扑



- 1: 配置静态 MAC 表项所对应的 VLAN 及相应端口。
- 2: 验证交换机 VLAN 和端口配置。
- 3: 配置静态 MAC 地址。
- 4: 验证交换机已经配置的静态 MAC 地址。

六、实验步骤

第 1 步：配置静态 MAC 表项所对应的 VLAN 及相应端口，输入如下代码：

```
SwitchA(config)# vlan 10
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport access vlan 10
```

第 2 步：验证交换机 VLAN 和端口配置。

测试：显示结果：

```
SwitchA#show vlan
```

VLAN Name	Status	Ports
1	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	Fa0/1

第 3 步：配置静态 MAC 地址，输入如下代码：

```
SwitchA(config)#mac-address-table static 00e0.9823.9526 vlan 10 interface fastethernet 0/1
```

! 配置静态 MAC 地址 00-E0-98-23-95-26

第 4 步：验证交换机配置的静态 MAC 地址。

测试：显示结果：

```
SwitchA#show mac-address-table static
```

Vlan	MAC Address	Type	Interface
10	00e0.9823.9526	STATIC	Fa0/1

注意事项

如果交换机所连接的计算机网卡或计算机发生改变，则必须在交换机上对配置的静态 MAC 地址做相应的改变；

如果网络中的计算机很多，则采用静态 MAC 地址配置方法带来的管理工作量较大，一般较少用。

参考配置

```
SwitchA#show running-config
```

```
Building configuration...
```

```
Current configuration : 299 bytes
```

```
!
```

```
version 1.0
```

```
!
```

```
hostname SwitchA
```

```
enable secret level 1 5 $2yglowN3aeh`@IO4dfimLMpQbcknAxB
```

```
enable secret level 15 5 $2bcknAx3zyglowN4aeh`@IOQdfimLMp
```

```
!
```

```
interface fastEthernet 0/1
```

```
switchport access vlan 10
```

```
!
```

```
mac-address-table static 00e0.9823.9526 vlan 10 interface fastEthernet 0/1
```

```
end
```

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 3 交换机端口安全性

一、实验性质

本实验为综合型实验, 2 课时。

二、实验目的

- 1: 理解什么是交换机的端口安全性, 如何配置端口安全性。
- 2: 通过在交换机上设置端口安全性来实现对网络访问的控制。

三、预备知识

了解交换机和操作系统的相关知识;需要预先掌握交换机的工作原理、网络管理安全性定义的理论知识。应预先做过交换机的基本配置实验。

四、实验设备

S2126G (1 台)。

五、实验内容

1、背景描述

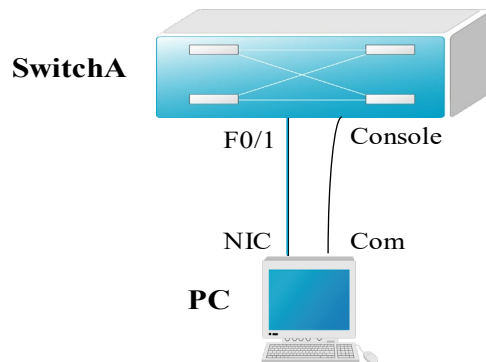
从网络管理的安全性考虑, 某企业网络管理员想对交换机上端口的访问权限做些限制, 通过限制允许访问交换机某个端口的 MAC 地址以及 IP 地址 (可选) 来实现严格控制对该端口的输入。现在要通过在交换机上做适当配置来实现这一目标。

本实验以一台 S2126G 交换机为例, 交换机名为 SwitchA。一台 PC 机通过串口 (Com) 连接到交换机的控制 (Console) 端口, 通过网卡 (NIC) 连接到交换机的 fastethernet 0/1 端口。假设该 PC 机的 IP 地址为 192.168.0.137, 网络掩码为 255.255.255.0, MAC 地址为 00-E0-98-23-95-26, 为了验证实验的效果, 另准备一台 PC 机, 其 IP 地址设为 192.168.0.150, 网络掩码为 255.255.255.0。

2、实验功能

通过在交换机上设置端口安全性来实现对网络访问的控制。

3、实验拓扑



- 1: 在交换机上配置管理接口 IP 地址。
- 2: 验证交换机管理 IP 地址是否配置和开启，PC 机与交换机是否有网络连通性。
- 3: 开启交换机上 fastethernet 0/1 接口的端口安全功能。
- 4: 验证是否开启 fastethernet 0/1 接口的端口安全功能。
- 5: 配置安全端口上的安全地址。
- 6: 验证是否配置了安全地址。
- 7: 验证这台 PC 机是否可以通过 fastethernet 0/1 端口访问交换机，而其它计算机不能通过 fastethernet 0/1 端口访问该交换机。

六、实验步骤

第 1 步：在交换机上配置管理接口 IP 地址，输入如下代码：

```
SwitchA(config)# interface vlan 1    ! 进入交换机管理接口配置模式
SwitchA(config-if)# ip address 192.168.0.138 255.255.255.0  ! 配置交换机管理接口 IP 地址
SwitchA(config-if)# no shutdown      ! 开启交换机管理接口
```

第 2 步：验证交换机管理 IP 地址是否配置和开启，PC 机与交换机是否有网络连通性。

测试：显示结果：

```
SwitchA#show ip interface ! 验证交换机管理 IP 地址已经配置，管理接口已开启
Interface                : VL1
Description               : Vlan 1
OperStatus                : up
ManagementStatus          : Enabled
Primary Internet address: 192.168.0.138/24
Broadcast address         : 255.255.255.255
PhysAddress               : 00d0.f8ef.9d08
SwitchA#ping 192.168.0.137 ! 验证交换机与 PC 机具有网络连通性
Sending 5, 100-byte ICMP Echos to 192.168.0.137,
```

```
timeout is 2000 milliseconds.
!!!!
Success rate is 100 percent (5/5)
Minimum = 1ms Maximum = 3ms, Average = 1ms
```

第 3 步：开启交换机上 **fastethernet 0/1** 接口的端口安全功能，输入如下代码：

```
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)#switchport mode access      ! 配置 fastethernet 0/1 接口为 access 模式
SwitchA(config-if)#switchport port-security    ! 在 fastethernet 0/1 接口上打开端口安全功能。
```

第 4 步：验证是否开启 **fastethernet 0/1** 接口的端口安全功能。

测试：显示结果：

```
SwitchA#show port-security interface fastethernet 0/1
Interface : Fa0/1
Port Security : Enabled
Port status : up
Violation mode : Protect
Maximum MAC Addresses : 128
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Secure static address aging : Disabled
```

第 5 步：配置安全端口上的安全地址（可选），输入如下代码：

```
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport port-security mac-address 00e0.9823.9526 ip-address
192.168.0.137
! 手工配置接口上的安全地址
```

第 6 步：验证是否配置了安全地址。

测试：显示结果：

```
SwitchA#show port-security address
lan    Mac Address      IP Address      Type           Port           Remaining Age(mins)
-----
1      00e0.9823.9526  192.168.0.137  Configured     Fa0/1
```

第 7 步：验证这台 PC 机是否可以通过 **fastethernet 0/1** 端口访问交换机，而其它计算机不能通过 **fastethernet 0/1** 端口访问该交换机，输入如下代码：

```
C:\>ping 192.168.0.138      ! 验证这台 PC 机可以通过 fastethernet 0/1 端口访问交换机
```

```
C:\WINDOWS\System32\cmd.exe

C:\>ping 192.168.0.138

Pinging 192.168.0.138 with 32 bytes of data:

Reply from 192.168.0.138: bytes=32 time<1ms TTL=64
Reply from 192.168.0.138: bytes=32 time<1ms TTL=64
Reply from 192.168.0.138: bytes=32 time<1ms TTL=64
Reply from 192.168.0.138: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

第 8 步：现在拔下网线，将另一台计算机连接到交换机的 fastethernet 0/1 端口上，输入如下代码：

C:\>ping 192.168.0.138 ! 验证这台 PC 机不能通过 fastethernet 0/1 端口访问交换机

```
E:\WINNT\system32\cmd.exe

E:\>ping 192.168.0.138

Pinging 192.168.0.138 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.138:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

注意事项

安全地址设置是可选的；

如果交换机端口所连接的计算机网卡或 IP 地址发生改变，则必须在交换机上做相应的改变。

参考配置

```
SwitchA#show running-config
Building configuration...

Current configuration : 381 bytes
!
version 1.0
!
hostname SwitchA
enable secret level 1 5 $2dfimLM3{bcknAx4zyglowNQaeh`@IO
enable secret level 15 5 $2lowNq&3h`@IOrJ4imLMp]KQknAxB^"
!
interface fastEthernet 0/1
    switchport port-security
    switchport port-security mac-address 00e0.9823.9526 ip-address 192.168.0.137
!
interface vlan 1
    no shutdown
    ip address 192.168.0.138 255.255.255.0
!
```

end

七、考核方式

1. 当场演示结果
2. 提交报告(附有配置文件)

实验 4 交换机端口限速

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

掌握如何实现交换网络 QOS，实现端口限速。通过在交换机上设置端口速率限制来优化网络性能，提高网络效率。

三、预备知识

掌握交换的基本概念、交换机的工作原理等理论知识。

预备试验：交换机的基本配置。

四、实验设备

S2126G（1 台）。

五、实验内容

1、背景描述

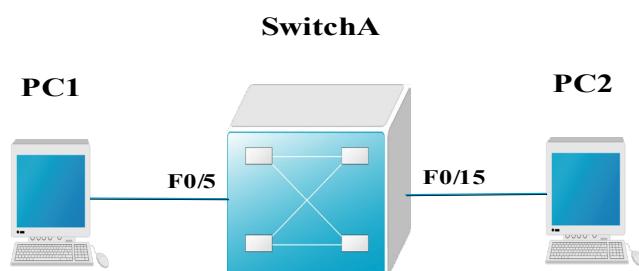
某企业网络管理员最近收到很多员工的投诉，他们抱怨网络变得很慢，不论是收发邮件还是上网查资料都很慢，影响了工作效率。对此，网络管理员进行了调查，发现有一台交换机的某些端口的数据流量很大，严重影响了网络性能，于是决定对这几个交换机端口进行速率限制，从而改进网络性能。

本实验以一台 S2126G 交换机为例，交换机命名为 SwitchA。假设 PC1 通过网线连接到交换机的 0/5 端口，IP 地址和网络掩码分别为 192.168.0.5，255.255.255.0，PC2 通过网线连接到交换机的 0/15 端口，IP 地址和网络掩码分别为 192.168.0.15，255.255.255.0。另外，PC1 通过串口（Com）连接到交换机的控制（Console）端口。

2、实现功能

通过限制交换机端口速率，改进网络性能。

3、拓扑结构



六、实验步骤

1. 在没有配置端口限速时测量传输速率。

在没有配置端口限速时，从 PC1 向 PC2 传输一个较大的文件（比如 60.5MB），将计算结果记录如下：

	传输数据大小(MB)	传输数据时间(秒)	平均传输速率(Mbps)
无限制情况	60.5MB	28	17.29

2. 用访问控制列表（ACL）定义需要限速的数据流，输入如下代码：

SwitchA(config)#ip access-list standard qoslimit1 ! 定义访问控制列表名称为 qoslimit1

SwitchA(config-std-ipacl)#permit host 192.168.0.5 ! 定义需要限速的数据流

SwitchA(config-std-ipacl)#end

验证测试：! 验证 ACL 配置正确。

显示结果：

SwitchA#show access-lists

Standard IP access list: qoslimit1

permit host 192.168.0.5

3. 设置带宽限制和突发数据量

SwitchA(config)#class-map classmap1 ! 设置分类映射图 classmap1

SwitchA(config-cmap)#match access-group qoslimit1

! 定义匹配条件为：匹配访问控制列表“qoslimit1”

SwitchA(config-cmap)#exit

SwitchA(config)#policy-map policymap1 ! 设置策略映射图

SwitchA(config-pmap)#class classmap1 ! 匹配分类映射图

SwitchA(config-pmap)#police 1000000 65536 exceed-action drop

! 设置带宽限制为 1Mbps，突发数据量为 64k/sec，超过限制则丢弃数据包

! 其中 1000000bps=1Mbps, 65536 bits=64k bits

exit

验证测试：验证分类映射图和分类映射图的配置。

显示结果：

SwitchA#show class-map ! 验证分类映射图的正确性

Class Map Name: classmap1

Match access-group name: qoslimit1

SwitchA#show policy-map ! 验证分类映射图的正确性

Policy Map Name: policymap1

Class Map Name: classmap1

Rate bps limit(bps): 1000000

Burst byte limit(byte): 65536

Exceed-action: drop

将带宽限制策略应用到相应的端口上，输入如下代码：

SwitchA(config)# interface fastethernet 0/5

SwitchA(config-if)#mls qos trust cos ! 启用 QoS，设置接口的 QoS 信任模式为 cos

SwitchA(config-if)#service-policy input policymap1 ! 应用带宽限制策略 policymap1

验证测试：验证端口 fastethernet 0/1 设置的正确性。

显示结果：

SwitchA#show mls qos interface fastethernet 0/1 ! 验证端口 QoS 策略的正确性

Interface: Fa0/5

Attached policy-map: policymap1

Trust state: cos

Default COS: 0

验证带宽限制策略的效果。

在配置了带宽限制策略的情况下，从 PC1 向 PC2 传一个较大的文件（比如 60.5MB），计算传输时间和平均传输速率。

将上述结果与没有配置带宽限制策略的计算结果进行比较。

	传输数据大小 (MB)	传输数据时间 (秒)	平均传输速率 (Mbps)
无限制情况	60.5MB	28	17.286
限制带宽为 1Mbps	60.5MB	608	0.796

以上结果显示说明：

当没有配置限速时，实际速度为 17.286Mbps（网卡和交换机端口是 10/100M），

当配置限速 1Mbps 时，实际速度为 0.796Mbps，限速效果很明显。

【注意事项】

限速配置的第一步是定义需要限速的流，这项是通过 QoS 的 ACL 列表来完成的。对于不在 QoS ACL 列表中的流，交换机依旧转发，只是限速功能无效。

所有的限速，只对端口的 input 有效，即进入交换机端口的流有效。目前无法做到对单一端口的 input/output 双向控制。若需对 output 方向控制，可以在另一端的交换机端口对 input 方向控制。

限速配置可以基于 IP、MAC、TCP 及 7 层应用流，配置方法与前相同。

【参考配置】

SwitchA#show running-config

Building configuration...

Current configuration : 476 bytes

version 1.0

hostname S2126G

enable secret level 1 5 \$2tj9=G13/7R:>H.41u_ ;C,tQ8U0<D+S

enable secret level 15 5 \$2\$Paein32F}bfjo43Q8cgkEQ4m`dhl&

ip access-list standard qoslimit1

permit host 192.168.0.5

class-map classmap1

match access-group qoslimit1

policy-map policymap1

class classmap1

police 1000000 65536

interface fastEthernet 0/5

mls qos trust cos

service-policy input policymap1

interface vlan 1

```
no shutdown  
end
```

七、考核方式

- 1、当场演示结果
- 2、提交配置文件

实验九、防火墙的初始配置（4 学时）

一、实验性质

本实验为设计型实验，实验学时为 4 学时。

二、实验目的

通过对防火墙进行初始配置，使管理人员以后可以通过 Web 方式对防火墙进行远程配置和管理。通过实验掌握防火墙的工作原理和配置方法。

三、预备知识

掌握防火墙的基本概念、防火墙的工作原理等理论知识。

四、实验设备

RG-WALL150 防火墙（1 台）。

五、实验内容

1、背景描述

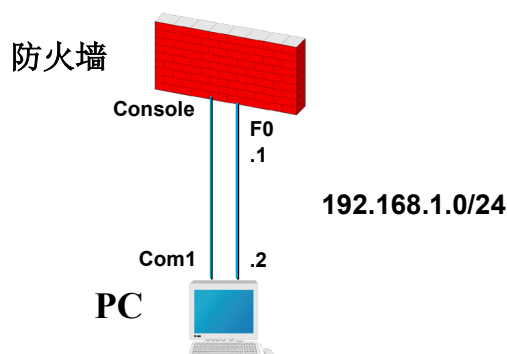
作为公司的网络管理员，希望在机房对防火墙进行初始配置后，以后可以通过 Web 方式对防火墙进行远程配置和管理，因此需要对其进行初始的基本设置。

本实验中 PC 通过串口 Com1 用控制线连接到防火墙的控制口（Console），通过一根交叉网线连接到防火墙的以太网口 F0，并事先在 PC 机上安装了 Java 程序（j2re-1_4_0-win-i，或更高版本）。

2、实现功能

使网络管理员可以通过 Web 方式对防火墙进行远程配置和管理。

3、拓扑结构



六、实验步骤

1. 登录防火墙，显示如下：

```
*****
** RG-OS V1.0    http://www.red-giant.com.cn **
*****
```

RG-Wall-150 login: root

Password: rg-wall123

以上是系统登入的默认 ID 和口令值

/>si

RG-WALL 缺省登入的提示或者重新设置时提示的内容如下。



在此按任意键进入缺省设置阶段。

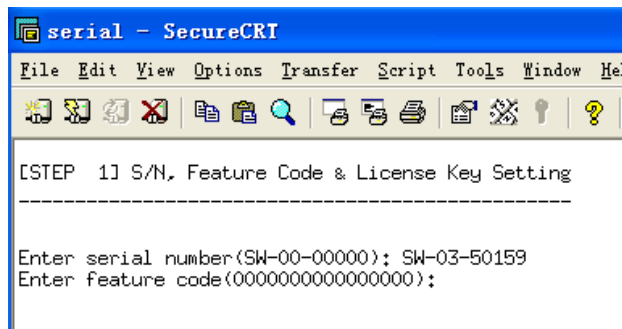
输入序列号、feature code 以及授权号。RG-WALL 的第一步系统将提示输入序列号、feature code 以及授权号。



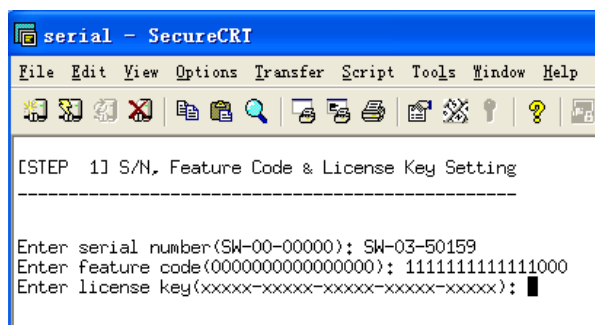
上图中，系统要求输入序列号。请按照“产品使用授权书”上提供的信息输入序列号，区分大小写。序列号的格式以 SW-xx-xxxxx 以及 SK-xx-xxxxx 输入。

SW-03-91004 ↵

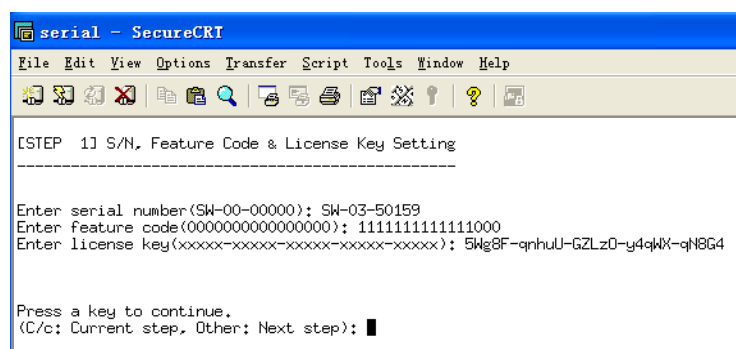
输入完序列号再输入 feature code。feature code 是设置 RG-WALL 可使用功能的编码，是根据与本公司签订合同提供的 16 位编码。



输入完 feature code 出现如下授权号输入提示。



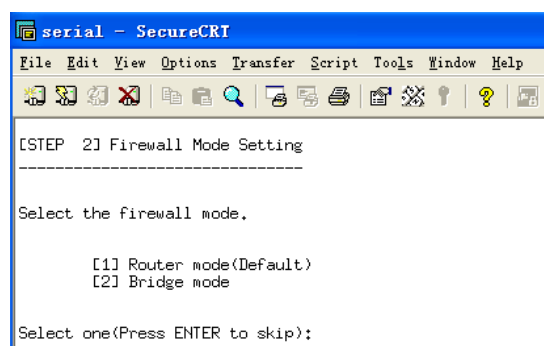
授权号与序列号和 feature code 相同，是本公司赋予的编号。授权号输入错误时也同样不能继续安装。产品授权号输入正确后，将出现如下图画面，进入下一步设置阶段。



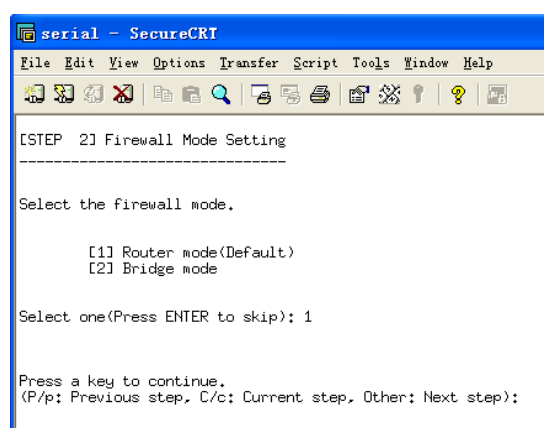
请按任意键继续。

2. 确定路由模式或网桥模式。

下一阶段将决定 RG-WALL 在安装网络中要起的作用，如图所示。



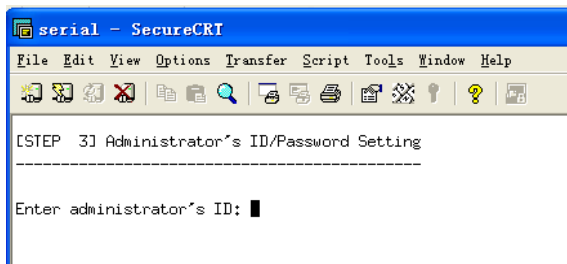
敲入 ENTER 将选择缺省的路由模式，并且这一阶段的选择决定以后的设置工作。本章将说明路由模式下的设置的方法。下图是选择路由模式以后出现的画面，在此选择路由模式后进入下一个安装阶段。



在最后的输入提示中敲入 P/p 时将取消当前设置和之前阶段的设置，进入前一个设置阶段。敲入 C/c 时将取消当前设置的内容，重新开始当前设置作业。即，现阶段里如果想重新选择系统模式，可以敲入 C/c 开始重新设置。输入任意键时将应用当前设置内容并进入下一个设置阶段。这些设置阶段的取消以及移动的方法在其他安装步骤中也相同，所以将省略以后的说明。

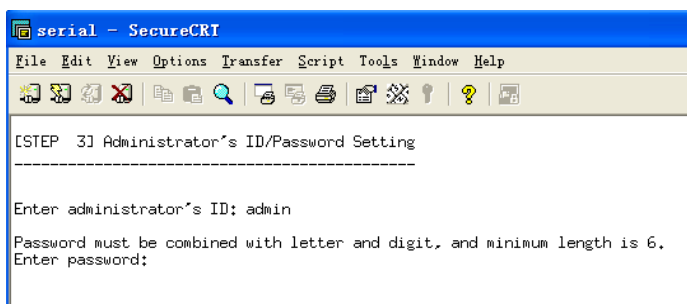
3. 输入管理员 ID 和密码。

完成防火墙模式设置以后出现如下管理员输入画面。



输入要启用的管理员 ID 和密码。这里的主管理员表示带有停止/启动系统、授权其他管理员权限的主要系统负责人员。

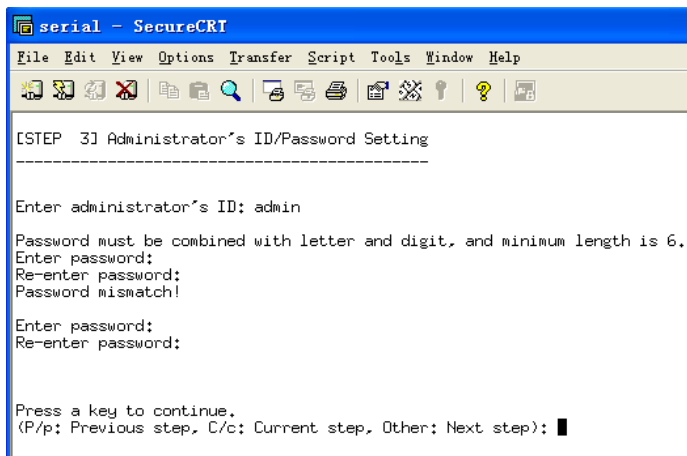
admin ↵



本手册中 admin 作为管理员帐号。输入完管理员帐号出现密码输入行，管理员密码必须是英文和数字的混合格式并且必须大于 6 个字，输入以下密码，注意通过管理员 GUI 输入同样的密码登入超过 20 次以上时系统会要求修改密码。

admin123 ↵

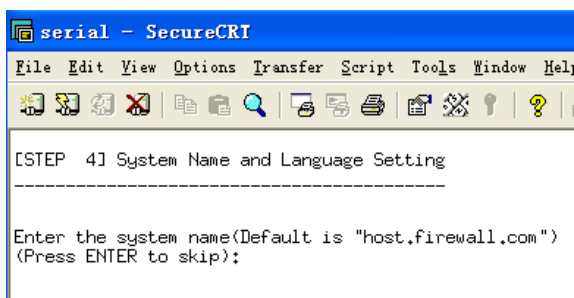
输入密码以后为了确认密码是否匹配，出现如下重复输入密码的提示。两次密码输入完全匹配时才可以进行下一步操作，设置管理员时出现的提示说明如下。



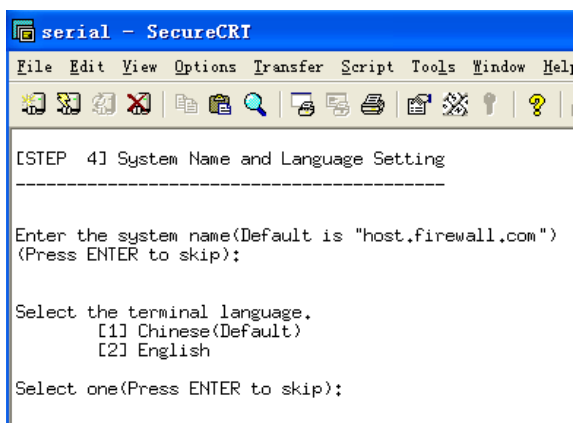
4. 设置系统名称以及语言。

下面输入系统名称，例如：

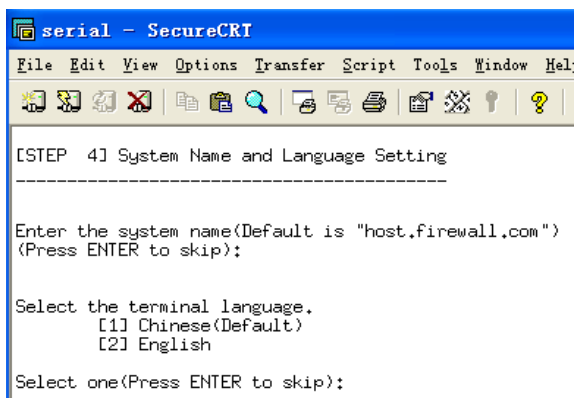
Host.firewall.com ↵



下一阶段选择 CLI Terminal 识别的语言。



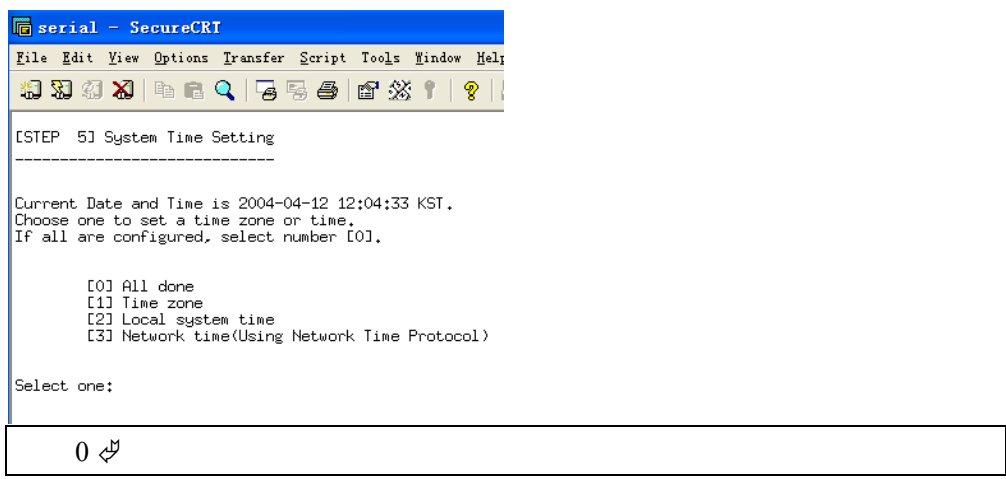
这里缺省值是中文。



本手册中敲入 ENTER 键选择中文进入下一个阶段。

5. 设置时间。

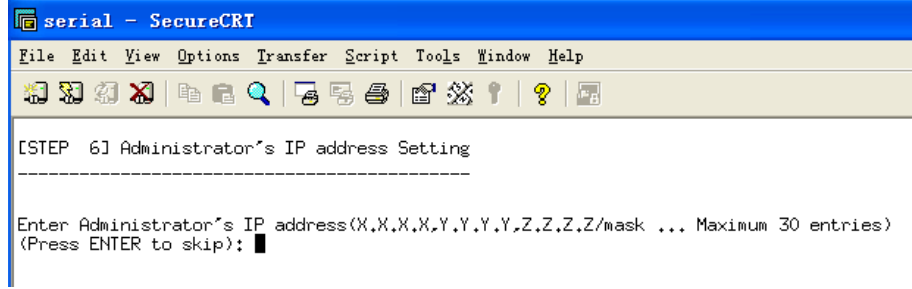
下一阶段是设置系统时间。所有的日志和报表以及计划任务的作业都会根据这里设置的时间来形成，因此必须正确输入当前时刻。



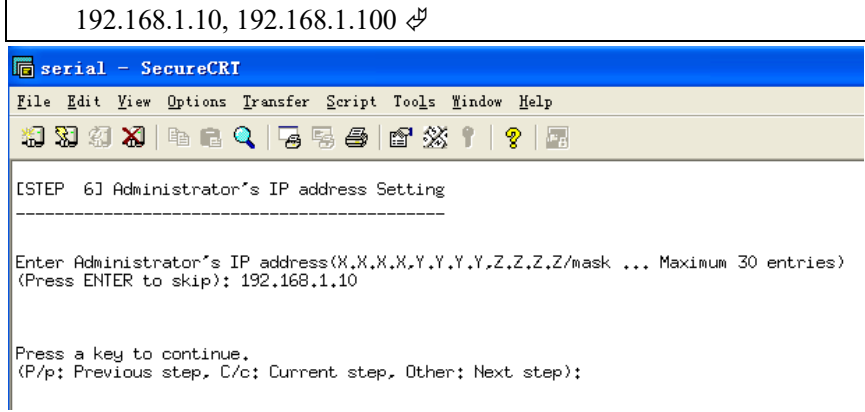
上图是设置时间的画面，显示当前设置的时刻和时区以及时间设置相关的菜单。选择 0 确认设置以后进入下一个阶段。

指定管理员 PC 的 IP 地址。

如前提到的 RG-WALL 提供的服务中包括了允许向特定管理员 IP 地址提供 SSHTTP、red-giantguid 服务。想利用 RG-WALL 的 GUI 以及 CLI 必须注册管理员 PC 的 IP 地址。设置时间以后进入管理员 IP 地址输入的提示行。



管理员 PC 的 IP 地址可以最多输入 10 个并且每个 IP 地址之间用 “,” 和 “ ”（空格）隔开，例如：

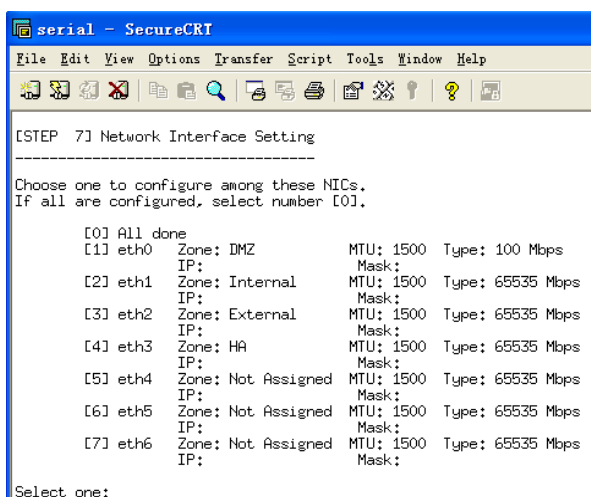


输入完管理员 IP 地址进入下一阶段。

网络接口构成。

为使 RG-WALL 的网络连接正常必须按照计划书的方案分配各接口地址。下面是显示当前接口设置以及选择接口的画面。各接口的区域分配可以修改，但是必须设置 Internal 和 External 并且启用 HA 时也必须设置 HA Link。

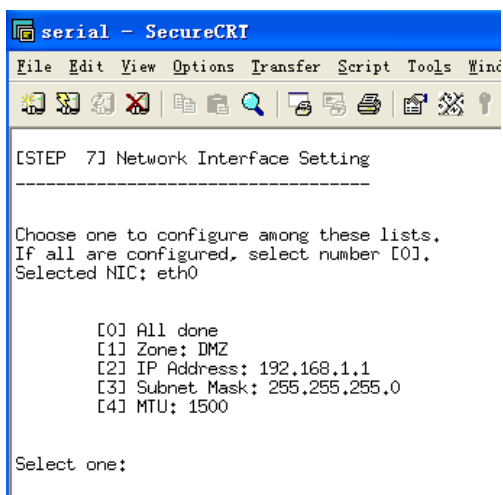
正确设置所有接口以后选择 0 后进入下一阶段。



0 ↵

输入要修改接口号开始改变设置。

选择接口以后出现如下设置各接口内容的画面，选择其内容项以后输入正确的值。



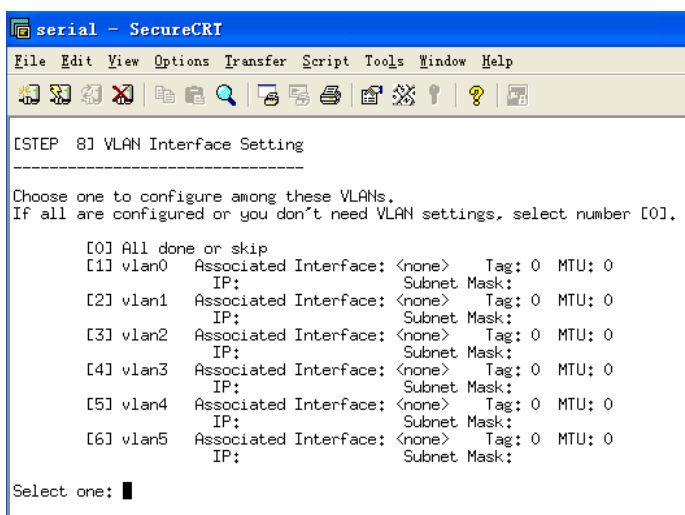
0 ↵

VLAN 构成。

如果要构成 VLAN 并通过 802.1q 方式访问时必须设置各 VLAN 的 IP 地址以及子网掩码和 MTU 信息。RG-WALL 共提供 6 个 VLAN 接口。设置完 VLAN 以后选择[0]进行下一个设置阶段。

0 ↵

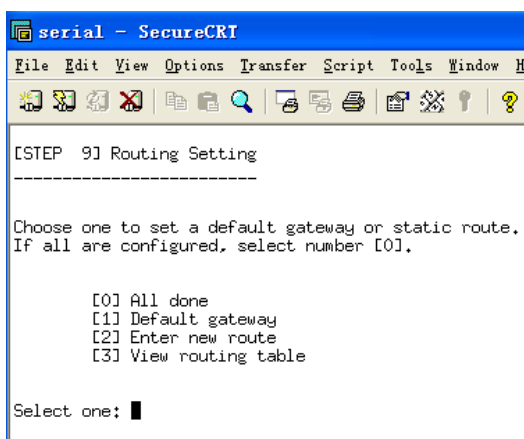
这一设置画面只在路由模式下出现。



输入 VLAN 设置的接口号开始设置 VLAN。

Static Route。

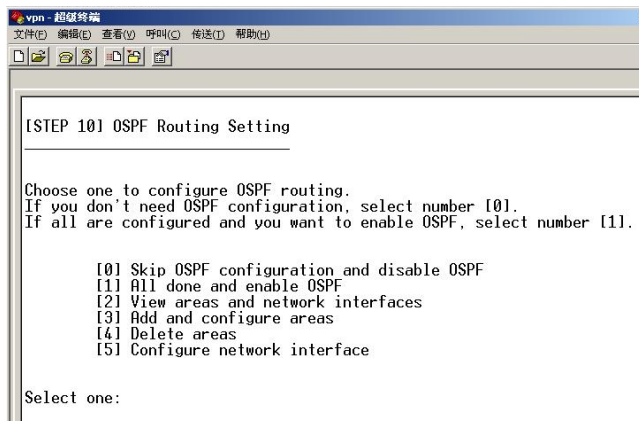
如果计划在路由模式下启用 OSPF 可以跳过这一阶段进入下一个 OSPF 设置阶段，或者以后通过 Web 方式设置。



RG-WALL 这里需要设置 RG-WALL 外部网的默认路径（Default Gateway）。

设置 OSPF。

路由模式下才可以设置该项。如果没有必要启用 OSPF 可以选择 0 跳过该设置。完成所有 OSPF 构成以后应用时选择 1 即可。



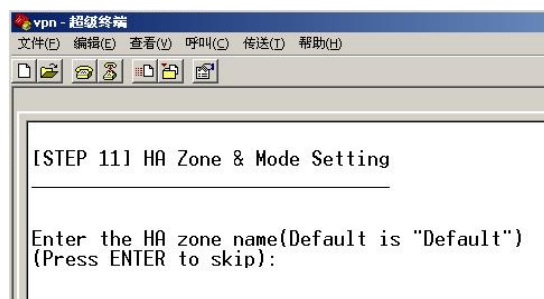
构成 OSPF 首先需要设置 Area。当前 Area 以及接口的 OSPF 信息可以通过选择菜单 2

来确认。

2 ↵

设置 HA Zone。

架设路由模式下高可用结构时首先要确定是否启用虚 IP 地址、配置什么样的虚 IP 以及是否使用 4 层交换机来实现高层同步模式，下图说明 HA 构成的画面。

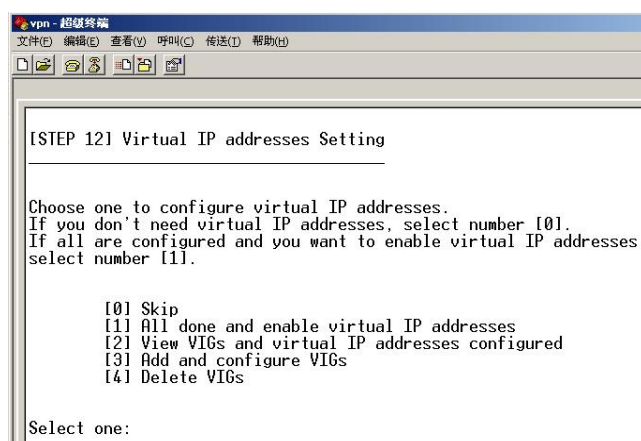


在此输入组成 HA Zone 的 RG-WALL 组名，缺省值为 Default。

↵

设置虚 IP 地址。

下图是设置虚 IP 地址的阶段。

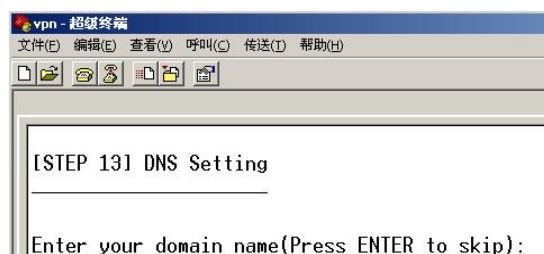


首先要构成 VIG（Virtual Interface Group）。选择 2 可以确认当前的 VIG 以及各接口的虚 IP 地址信息。

2 ↵

设置 DNS。

下面是 DNS 设置内容，在此输入域名，输入完按 ENTER 键进入下一阶段。

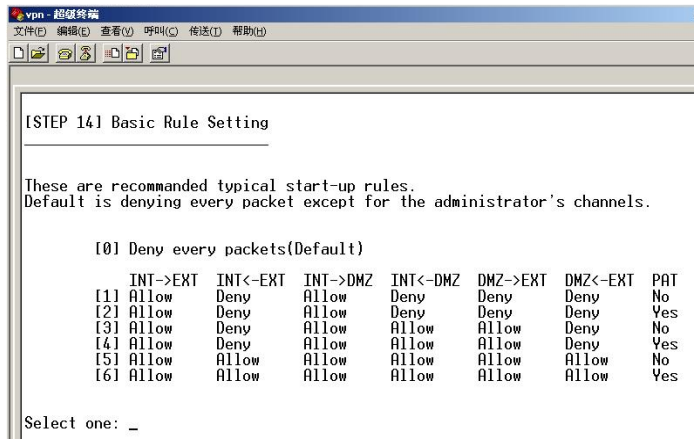


↵

选择基本规则。

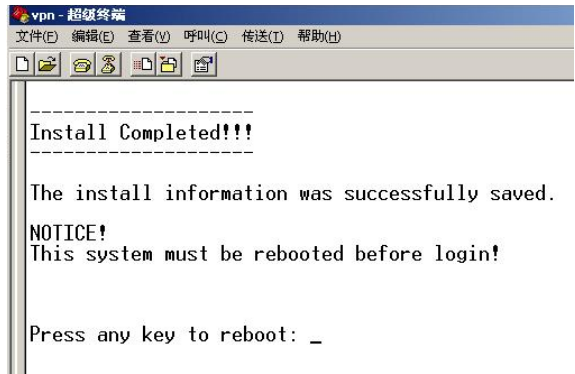
最后一个阶段是设置初始规则阶段。在这个阶段选择需要的基本规则即可，基本设置完

毕后通过 GUI 进一步设置。

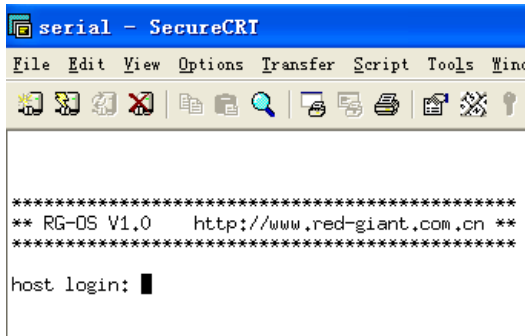


应用系统设置。

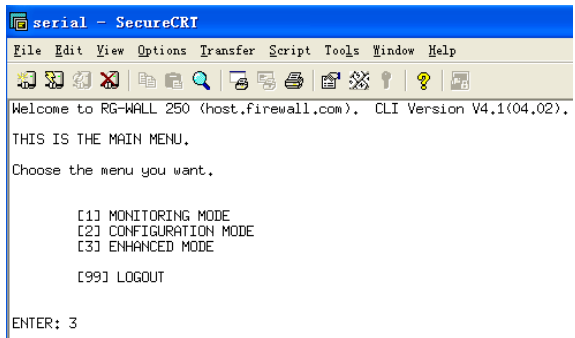
基本安装设置已经完成，出现如下安装完毕的画面。



按任意键重新启动系统的同时应用当前设置。重新启动后出现登入画面，登入操作系统，如下图所示。



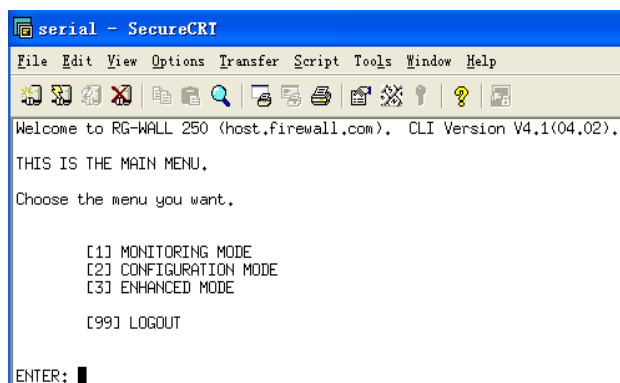
这时会出现 RG-WALL 的登入提示符。登入 RG-WALL 系统以后出现如下 CLI 基本菜单，如图所示。



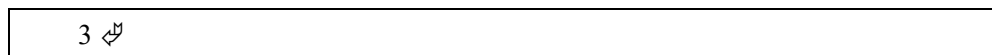
继续通过 CLI 进行作业可以选择 2 或者 3，CLI 的详细说明请参考管理员手册。

reinstall。

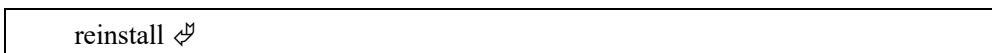
RG-WALL 的重新安装提供了路由模式设置和网桥模式设置中的所有设置项。



在上图 CLI 主菜单中选择 3 进入 CLI 的 ENHANCED MODE 以后可以重新设置 RG-WALL。

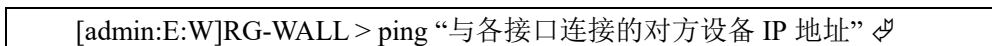


下面是 CLI ENHANCED MODE 显示画面。在 CLI 命令提示符上输入 reinstall 重新设置系统。



确认安装是否正常。

PING 测试，进入 RG-WALL CLI 模式并输入以下命令。



邻接网络设备的 PING 测试成功以后可以再测试 PING 管理员 PC、DMZ 的主要服务器以及外网常用的 IP 地址。

GUI 安装。

RG-WALL 的 GUI 通过 JAVA 技术实现，因此兼具客户端软件管理方式和 WEB 浏览器管理方式的优点，支持多种语言，与管理工作站的操作系统无关。

为了运行 JAVA 类程序，管理员工作站需要具备 SUN 公司的免费软件 Java Runtime Environment (JRE)。这一插件可以通过 RG-WALL 的 WEB 管理界面安装。

在管理员工作站上启动 Web 浏览器后，地址栏中输入 RG-WALL Internal 接口的 IP 地址，则出现如下图所示的初始界面。



RG-WALL WEB 初始画面如图所示。



RG-WALL Desktop 画面

【注意事项】

在初始配置中，关键是要设置管理员 ID、密码和 IP 地址，并设置至少一个接口的 IP 地址，其余配置可以在以后进入 Web 配置界面后设置。

【参考配置】

（无）

七、考核方式

- 1、当场演示结果
- 2、提交配置文件