央邦 IT 培训实验手册

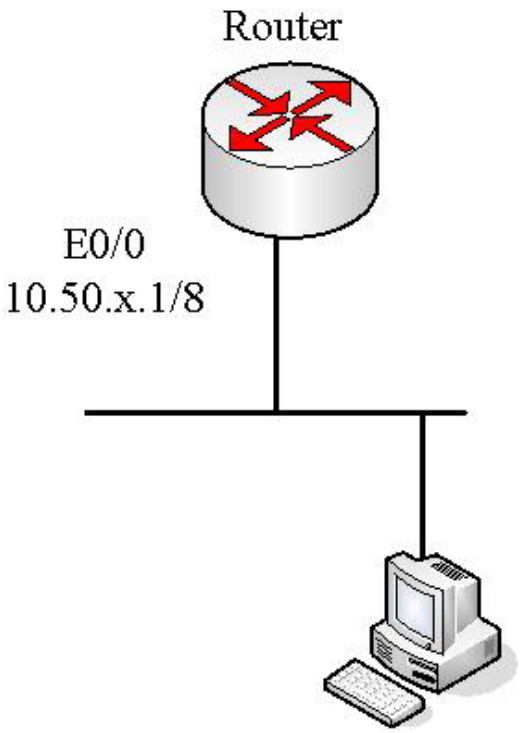
CCNA 部分

Lab 1 路由器的基本配置

实验要求

1. 掌握路由器的用户模式、特权模式、配置模式的切换。
2. 配置路由器的特权密码，明文密码为 ccna、密文密码为 cisco。
3. 配置路由器的 console 登录密码为 cisco、远程登录密码是 cisco。
4. 配置路由器 Ethernet 0/0 的接口 IP 为 10.50.x.1/8,并打开接口
5. 掌握常用的 show 命令
6. 使用 tftp 软件，将路由器上的 IOS 映像文件下载到本地计算机作备份。
7. 用本地计算机的 IOS 映像文件上传到路由器，掌握如果升级路由器 IOS。
8. 将 flash 中的 IOS 映像文件删除，在 ROMMON 模式下恢复路由器的 IOS。

实验拓扑



实验步骤

A 路由器配置模式的切换
1) 使用超级终端登录路由器
2) 进入特权模式 Router>enable
3) 进入全局配置模式 Router#config terminal
4) 进入 Ethernet 0 口的配置模式 Router(config)#interface Ethernet 0
5) 退出到全局配置模式 Router(config-if)#exit
6) 退出到特权模式 Router(config)#exit
7) 退出到用户模式 Router#disable

B .路由器的全局配置
1) 将路由器的名称命名为 cisco Router(config)#hostname cisco
2) 为路由器配置明文的特权密码（密码配置为 ccna）
cisco (config)#enable password ccna
3) 为路由器配置密文的特权密码（密码配置为 cisco）
cisco (config)#enable secret cisco
4) 比较明文密码和密文密码的优先关系(测试)
5) 为路由器开启 telnet，允许 5 人同时 telnet 路由器做管理，并配置 telnet 密码（密码配置为 cisco）
cisco (config)#line vty 0 4
cisco (config-line)#password cisco
cisco (config-line)#login
6) 为路由器的 console 控制台配置密码（密码配置为 cisco）
cisco(config)#line console 0
cisco (config-line)#password cisco
cisco (config-line)#login

C 路由器接口配置
1) 为路由器的 Ethernet 0/0 口配置 IP 地址（IP 地址为 10.50.1.x,子网掩码是 255.0.0.0，x 是你的路由器号）
cisco (config)#interface Ethernet 0/0
cisco (config-if)#ip address 10.50.1.x 255.0.0.0
2) 打开 Ethernet 0/0 口
cisco (config)#interface Ethernet 0/0
cisco (config-if)#no shutdown

D 查看路由器配置和运行状态
1) 查看路由器 Flash 的内容 cisco #show flash
2) 命令缓冲区存储的命令 cisco #show history
3) 查看路由器的当前运行的配置 cisco #show running-config
4) 查看路由器保存的配置 cisco #show startup-config
5) 查看路由器上所有端口的状态及信息 cisco #show interfaces

6) 查看路由器 Ethernet 0/0 的信息 cisco #show interfaces Ethernet 0/0
7) 查看路由器上所有端口的 IP 地址及端口状态的简要信息
cisco #show protocols
cisco #show ip interface brief
8) 查看路由器的 IOS 版本及配置寄存器的值 cisco #show version

E 将路由器的 IOS 映像文件（bin 文件）备份到本地 pc
1) 配置路由器的 Ethernet 0/0 口的 IP 地址，并打开接口，使它能和您的 pc 互相通信：
Router#configure terminal
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 10.50.1.x 255.0.0.0
------x 是您的路由器号码
Router(config-if)#no shutdown
2) 在您的 pc 上开启 tftp 软件，并查看您的 pc 的 IP 地址，假设您 pc 的 ip 地址是 10.x.y.z
3) 在路由器的特权模式输入以下命令将 flash 中的 ios 映像文件传递到服务器上
Router#copy flash:c2600-j1s3-mz.123-26.bin tftp:
------flash 后的文件名可用 tab 键补全
Address or name of remote host []? 10.x.y.z
------输入您刚刚查到的自己的主机 IP 地址
Destination filename [c2600-j1s3-mz.123-26.bin]? ccna.bin
---指定放在 tftp 服务器上的文件名
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
复制完成后您会在 tftp 软件所在的目录下看到一个 ccna.bin 文件，它就是备份的 ios 文件

F 将路由器中的原有 IOS 映像文件替换成一个新的映像文件（ccna.bin）
1) 配置路由器的 Ethernet 0/0 口的 IP 地址，并打开接口，使它能和您的 pc 互相通信：
Router#configure terminal
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 10.50.1.x 255.0.0.0
-----x 是您的路由器号码
Router(config-if)#no shutdown
2) 在您的 pc 上开启 tftp 软件，并查看您的 pc 的 IP 地址，假设您 pc 的 ip 地址是 10.x.y.z
3) 在路由器的特权模式输入以下命令将 tftp 上的 ccna.bin 传递到 flash 中去，在这个过程中路由器会提示您清空 flash，按回车键确认清空就可以了
Router#copy tftp: flash:
Address or name of remote host []? 10.x.y.z
---------输入您的主机 IP 地址

Source filename []? ccna.bin
-------输入源文件的名称（tftp 服务器上的文件名）
Destination filename [ccna.bin]? ccna.bin
---输入目标文件名（在 flash 中存储的文件名）
Accessing tftp://10.255.199.199/ccna.bin...
Erase flash: before copying? [confirm]
---提示您要不要清空，按回车就可以了
Erasing the flash filesystem will remove all files! Continue? [confirm]
----再次确认，再按回车

在拷贝时会看到一串！！！！！,表示拷贝成功，在完成拷贝后一定要看到校验正确：
Verifying checksum... OK (0x3C0E)
这是才能重启路由器；
注意：在清空 flash 到完成拷贝这段时间内不能重启路由器

G 恢复 2600 系列路由器的 IOS 映像文件

做这个实验之前，我们需要将路由器的映像文件删除：
#erase flash:
1) 路由器启动是会在 flash 里边寻找 IOS 映像文件(bin 文件),但是如果 flash 里没有可用的 bin 文件，路由器就会进入 Rommon 模式：

```
device does not contain a valid magic number
boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:"

System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 65536 Kbytes of main memory

rommon 1 > 
```

在 Rommon 模式下面，我们可以对路由器的存储体以及部分硬件作简单配置

2) 在路由器的 Rommon 模式下指定路由器在从 tftp 服务器下载 bin 文件时的关键参数
Rommon1>IP_ADDRESS=10.50.1.X
-------------X 是您的路由器号码
rommon 2 > IP_SUBNET_MASK=255.0.0.0
rommon 3 > DEFAULT_GATEWAY=10.0.0.254
rommon 4 > TFTP_SERVER=10.255.199.199
--服务器地址是您的 pc 的网卡地址
rommon 5 > TFTP_FILE=ccna.bin

3.在自己的本地主机开启 tftp 软件，并保证自己的 tftp 软件的工作目录有 ccna.bin,而且 ccna.bin 文件是一个正确的 IOS
4.执行以下指令开始让路由器开始从 tftp 服务器下载 bin 文件：
rommon 6 > tftpdnld

```
           IP_ADDRESS: 10.50.1.100
      IP_SUBNET_MASK: 255.0.0.0
     DEFAULT_GATEWAY: 10.0.0.254
         TFTP_SERVER: 10.255.199.199
           TFTP_FILE: ccna.bin

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
```

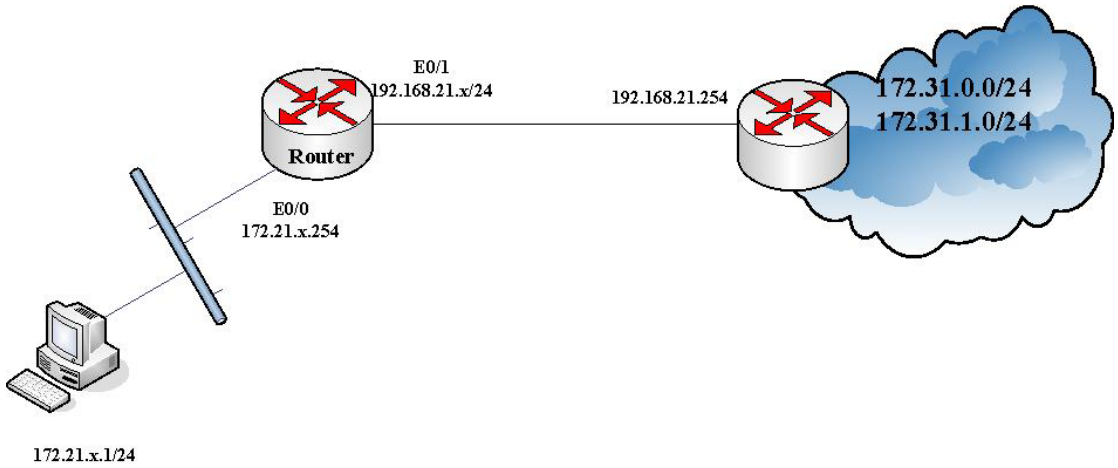
路由器会显示刚刚输入的参数，仔细校对参数，确定没有问题后输入 y，路由器开始擦除 flash，并开始下载新的 bin 文件（ccna.bin）

Lab 2 配置静态路由

实验要求

1) 配置 Router 的接口 IP 并打开接口，是路由器能 ping 同 192.168.21.254。
2) 配置路由器的静态路由，使路由器能正确转发到 172.31.0.0/24 到 172.31.1.0/24 的数据包。
3) 192.168.21.254 接入骨干网络，配置 路由器默认路由，使路由器能正确转发到骨干网络所有 IP 地址的数据包。

实验拓扑



实验步骤

1)配置接口和 IP 地址

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface ethernet 0/0
R1(config-if)#ip address 172.21.x.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ethernet 0/1
R1(config-if)#ip address 192.168.21.x 255.255.255.0
R1(config-if)#no shutdown
```

在 R1 上查看路由表：

```
R1#show ip route
C    172.21.x.0/24 is directly connected, Ethernet0/0
C    192.168.21.0/24 is directly connected, Ethernet0/1
```
发现路由表只有直连的网络，查看 R2 也是一样

2)配置静态路由
```
R1(config)#ip route 172.31.0.0/24 255.255.255.0 192.168.21.254
R1(config)#ip route 172.31.1.0/24 255.255.255.0 192.168.21.254
```

在 R1 上查看路由表：
```
R1#show ip route
C    172.21.x.0/24 is directly connected, Ethernet0/0
C    192.168.21.0/24 is directly connected, Ethernet0/1
S    172.31.0.0/24 [1/0] via 192.168.21.254
S    172.31.1.0/24 [1/0] via 192.168.21.254
```

192.168.21.254 接入骨干网络，配置路由器默认路由，使路由器能正确转发到骨干网络所有 IP 地址的数据包。
路由器上分别配置默认路由：

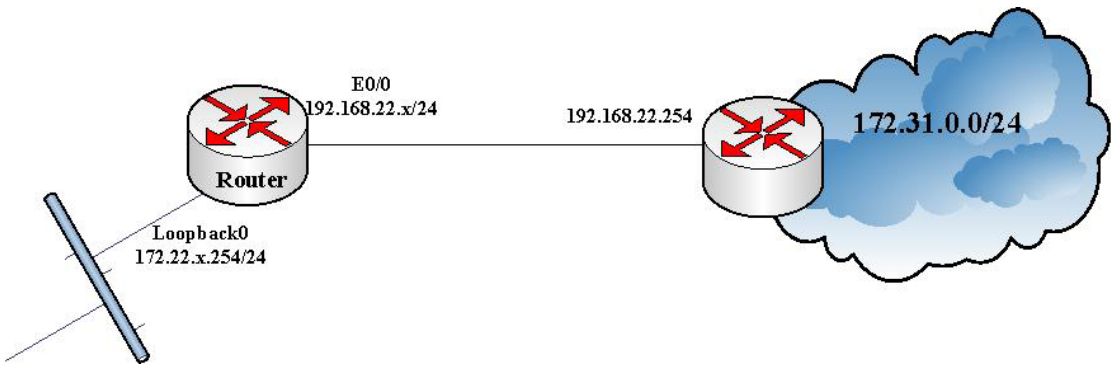
R1 的默认路由下一跳指向 192.168.21.254
```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.21.254
```

Lab 3 配置动态路由协议

实验要求

1) 配置路由器接口 IP 地址，实现直连链路的正常通信
2) 配置 RIP 路由协议实现网络互联
3) 将 RIP 路协议的工作版本更改为版本 2，并保证网络正常通信
4) 配置 EIGRP 路由协议，自治系统号为 100
5) 配置 OSPF 路由协议，将所有接口加入 area 0

实验拓扑



实验步骤

开始实验之前输入以下命令，避免实验是其他路由器干扰您的实验：
(config)#access-list 1 permit 192.168.22.254
(config)#access-list 1 permit 172.31.0.0 0.0.255.255
(config)#interface ethernet 0/0
(config-if)#ip access-group 1 in

实验中 X 以“1”为例
1) 配置接口和 IP 地址

```
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 192.168.22.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface loopback 0
```

```
Router(config-if)#ip address 172.22.1.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router#show ip route

     172.22.0.0/24 is subnetted, 1 subnets
C       172.22.1.0 is directly connected, Loopback0
C    192.168.22.0/24 is directly connected, Ethernet0/0
```

2) 配置 RIP 路由协议

```
Router(config)#router rip
Router(config-router)#network 172.22.0.0
Router(config-router)#network 192.168.22.0

Router#show ip route
     172.22.0.0/24 is subnetted, 1 subnets
C       172.22.1.0 is directly connected, Loopback0
     172.31.0.0/24 is subnetted, 1 subnets
R       172.31.0.0 [120/1] via 192.168.22.254, 00:00:20, Ethernet0/0
C    192.168.22.0/24 is directly connected, Ethernet0/0
```

3) 将两台路由器的 RIP 更改为版本 2

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary

Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 21 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface         Send  Recv  Triggered RIP  Key-chain
    Ethernet0/0       2     2
    Loopback0         2     2
  Automatic network summarization is not in effect
  Maximum path: 4
```

```
  Routing for Networks:
    172.22.0.0
    192.168.22.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.22.254       120      00:00:20
  Distance: (default is 120)
```

4) 配置 EIGRP 路由协议：

```
Router(config)#router eigrp 100
Router(config-router)#network 172.22.0.0
Router(config-router)#network 192.168.22.0
Router(config-router)#no auto-summary
Router(config-router)#exit
```

查看路由器是否建立正确的邻居关系：

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.22.254          Et0/0             14 00:06:16  148   888  0  5
```

查看 EIGRP 的拓扑表：

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(172.22.1.254)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
       r - reply Status, s - sia Status

P 192.168.22.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 172.31.0.0/24, 1 successors, FD is 409600
        via 192.168.22.254 (409600/128256), Ethernet0/0
P 172.22.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
```

查看路由器的路由表：

```
Router#show ip route
```

```
     172.22.0.0/24 is subnetted, 1 subnets
D       172.22.1.0 [90/409600] via 192.168.22.1, 00:10:46, Ethernet0/0
     172.31.0.0/24 is subnetted, 1 subnets
C       172.31.0.0 is directly connected, Loopback0
C    192.168.22.0/24 is directly connected, Ethernet0/0
```

5) 配置 ospf 路由协议

```
Router(config)#router ospf 1
Router(config-router)#network 172.22.1.0 0.0.0.255 area 1
Router(config-router)#network 192.168.22.0 0.0.0.255 area 0
```

查看 ospf 邻居状态

```
Router#show ip ospf neighbor

Neighbor ID     Pri     State           Dead Time   Address         Interface
192.168.22.254      1   FULL/DR         00:00:39    192.168.22.254  Ethernet0/0
```

------FULL 表示正确建立邻居关系，可以传递路由信息

查看路由器的路由表

```
R1#show ip route

C    192.168.22.0/24 is directly connected, Ethernet0/0
C    172.22.1.0/24 is directly connected, loopback0
O    172.31.0.0/24 [110/20] via 192.168.12.2, 00:01:40, Ethernet0/0
```

6)

研究一下，多种路由协议同时配置在路由器上，会不会发生冲突？什么时候会发生冲突？如果发生了冲突，几种路由协议的优先级排列是怎样的？

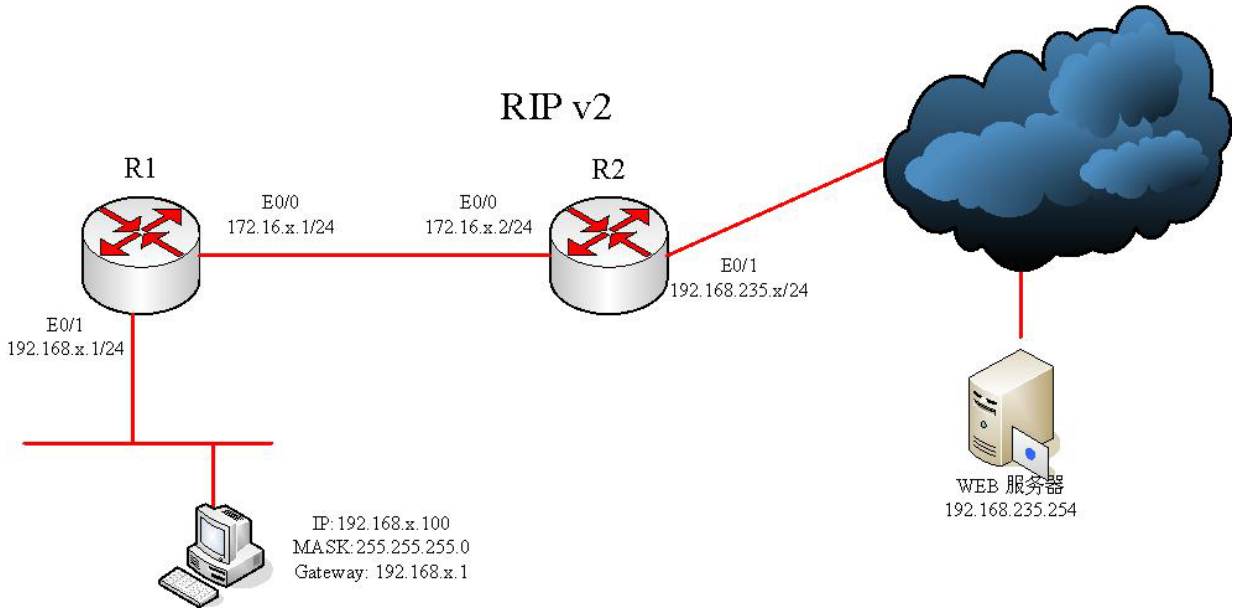
Lab 4 配置网络控制列表

实验要求

1) 在 R2 上配置基本访问控制列表，使 R2 拒绝转发那些所有来自 192.168.x.0/24 网段的数据包，其他数据包不作限制。
2) 在 R2 上配置基本访问控制列表，使 R2 只拒绝转发来自 192.168.x.1---63 的数据包，其他数据包不做限制。
3) 在 R2 上配置基本访问控制列表，使 R2 只接受来自 192.168.x.100 主机的 telnet 访问。
4) 在 R1 上配置扩展访问控制列表，使 R1 拒绝转发来自 192.168.x.0/24，到 192.168.235.0/24 的非 http 访问包，其他数据包不做限制。
5) 挑战实验：在 R2 上配置标准访问控制列表，使 R2 只接收来自 192.168.x.0 /24 的数据包（必须将访问控制列表绑定在 IN 方向上）

补充：
为了避免干扰 ，在 R2 上配置以下命令:
R2(config)#access-list 99 deny any
R2(config)#router rip
R2(config-router)#distribute-list 99 in ethernet 0/1
这些命令和本次学习内容没有任何关系

实验拓扑



实验步骤

在开始访问控制列表实验以前，需要先正确配置接口 IP，并打开接口；配置动态路由协议 RIPv2 来互联整个网络：

```
R1(config)#interface Ethernet 0/0
R1(config-if)#ip address 172.16.x.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Ethernet 0/1
R1(config-if)#ip address 192.168.x.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#router rip
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.x.0
R1(config-router)#version 2
R1(config-router)#no auto-summary
```

```
R2(config)#interface Ethernet 0/0
R2(config-if)#ip add 172.16.x.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Ethernet 0/1
R2(config-if)#ip address 192.168.235.x  255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router rip
R2(config-router)#network 172.16.0.0
R2(config-router)#network 192.168.235.0
R2(config-router)#version 2
R2(config-router)#no auto-summary
```

检查 R1 和 R2 的路由表，保证网络能互联

```
R1#show ip route
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.x.0 is directly connected, Ethernet0/0
C    192.168.x.0/24 is directly connected, Ethernet0/1
R    192.168.235.0/24 [120/1] via 172.16.200.2, 00:00:24, Ethernet0/0
```

配置PC，是PC能ping通web服务器，同时可以访问web服务器的http服务

1) 在 R2 上配置基本访问控制列表，使 R2 拒绝转发那些所有来自 192.168.x.0/24 网段的数据包，其他数据包不作限制。

```
R2(config)#access-list 1 deny 192.168.x.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#interface Ethernet 0/1
R2(config-if)#ip access-group 1 out
```

(或者可以配置在 E 0/0 口的 In 方向上)

2) 在 R2 上配置基本访问控制列表，使 R2 之拒绝转发来自 192.168.x.1---63 的数据包，其他数据包不做限制。

```
R2(config)#access-list 2 deny 192.168.x.0 0.0.0.63
R2(config)#access-list 2 permit any
R2(config)#interface Ethernet 0/1
R2(config-if)#ip access-group 2 out
```

(或者可以配置在 E 0/0 口的 In 方向)

在前两个实验我们似乎在R2 的E0/1 口的Out方向绑定了两个访问控制列表（1 和 2），尝试通过查看路由器的配置文件我们发现，路由器的一个接口的某个方向上只能绑定一个访问控制列表。

3) 在 R2 上配置基本访问控制列表，使 R2 只接受来自 192.168.x.100 主机的 telnet 访问。

```
R2(config)#access-list 10 permit 192.168.x.100 0.0.0.0
R2(config)#line vty 0 15
R2(config-line)#access-class 10 in
R2(config-line)#no login    -------开启 telnet 访问，允许远程主机 telnet 本路由器
```

使用 pc 验证：发现只有 IP 为 192.168.x.100 的 pc 可以 telnet 到 R2 上，其他都不可以。

4)在 R1 上配置扩展访问控制列表，使 R1 拒绝转发来自 192.168.x.0/24，到 192.168.235.0/24 的 http 访问包以外的数据包，其他网络之间的访问任何访问不受影响。

为了前面的实验配置的访问控制列表对这个实验的干扰，我们需要将前面实验配置过的访问控制列表删除

```
R2(config)#no access-list 1
R2(config)#no access-list 2
R2(config)#interface ethernet 0/1
R2(config-if)#no ip access-group 2 out
```

```
R1(config)#access-list 120 permit tcp 192.168.x.0 0.0.0.255 192.168.235.0 0.0.0.255
eq www
R1(config)#access-list 120 deny   ip 192.168.x.0 0.0.0.255 192.168.235.0 0.0.0.255
```

```
R1(config)#access-list 120 permit ip any any
R1(config)#interface Ethernet 0/0
R1(config-if)#ip access-group 120 out
```

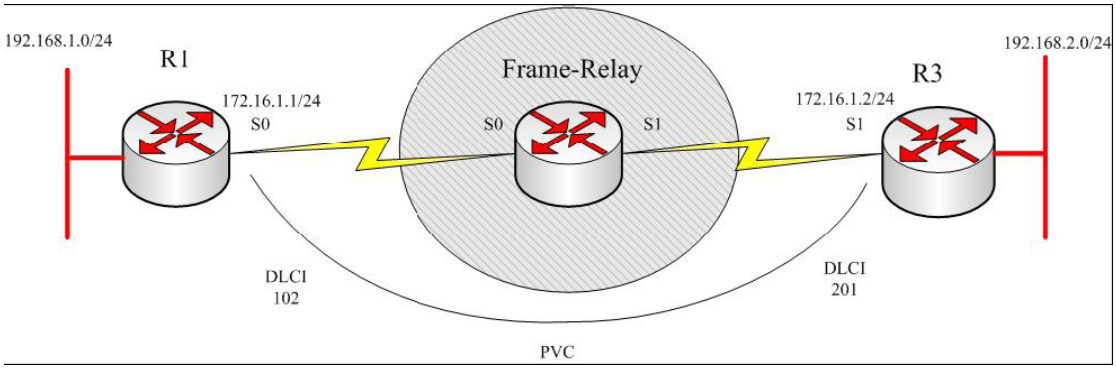
配置完成后我们可以通过 pc 测试，正确的结果是：pc 可以访问到 web 服务器的网站，但是不能 ping 通 web 服务器。

Lab 5 配置帧中继

实验要求

配置帧中继是两个远程站点可以通过帧中继交换网络实现通信

实验拓扑



实验步骤

1) 将R2配置成帧中继交换机

```
Router(config)#host Frame-Relay
Frame-Relay(config)#frame-relay switching
Frame-Relay(config)#interface serial 0
Frame-Relay(config-if)#encapsulation frame-relay        将封装格式定义为帧中继
Frame-Relay(config-if)#frame-relay lmi-type cisco       将LMI类型定义为Cisco
Frame-Relay(config-if)#frame-relay intf-type dce        将接口类型定义为DCE
Frame-Relay(config-if)#clock rate 64000                 定义时钟
Frame-Relay(config-if)#frame-relay route 102 interface serial 1 201
Frame-Relay(config-if)#no shutdown
Frame-Relay(config-if)#exit
Frame-Relay(config)#interface serial 1
Frame-Relay(config-if)#encapsulation frame-relay
Frame-Relay(config-if)#frame-relay lmi-type cisco
Frame-Relay(config-if)#frame-relay intf-type dce
Frame-Relay(config-if)#clock rate 64000
Frame-Relay(config-if)#frame-relay route 201 interface serial 0 102
Frame-Relay(config-if)#no shutdown
```

Frame-Relay(config-if)#exit
2) 配置R1和R3为帧中继客户端路由器
R1上：
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay lmi-type cisco 定义lmi类型为cisco
Router(config-if)#ip address 172.16.1.1 255.255.255.0 配置接口IP
Router(config-if)#frame-relay map ip 172.16.1.2 102 定义DLCI和IP的映射
Router(config-if)#no shutdown

在R3上：
Router(config)#interface serial 1
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay lmi-type cisco
Router(config-if)#ip address 172.16.1.2 255.255.255.0
Router(config-if)#frame-relay map ip 172.16.1.1 201
Router(config-if)#no shutdown

3) 在R1和R3上使用loopback接口模拟两个内网网段，再使用静态路由并通过帧中继的PVC使这两个网段能互相访问。
在R1上：
Router(config)#interface loopback 0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2
在R3上：
Router(config)#interface loopback 0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

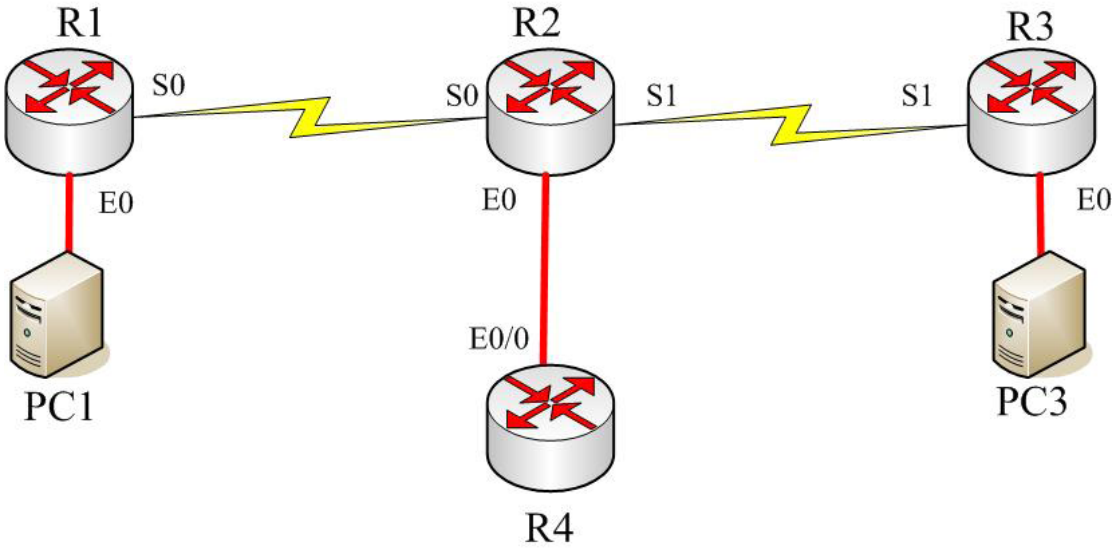
Lab 6 配置网络地址转换

实验要求

两人为一组，把R1和R3作为网络边界，把主机作为内网客户端，通过配置网络地址转换（NAT）和默认路由实现内网和公网的通信。

提示：R1和R3路由器是企业边界路由器，他们不能通过动态路由协议学习到公网的路由信息，R2和R4是公网路由器，他们不需要也不能看到内网的路由信息。

实验拓扑



R1、**R2**和**R3**是**2500**系列路由器，**R4**是**2600**系列路由器。

IP地址分配：

R1：

S 0: 12.0.0.1 255.0.0.0

E 0: 192.168.1x.1 255.255.255.0

R2:

S 0: 12.0.0.2 255.0.0.0

S 1: 23.0.0.2 255.0.0.0

E 0: 24.x.0.2 255.255.0.0

R3:

S1: 23.0.0.3 255.0.0.0

E0: 192.168.2 x.1 255.255.255.0

R4:

E0/0: 24.x.0.4 255.255.0.0

Loopback0 ： 100.0.0.1 255.0.0.0

实验步骤

实验之前建议将路由器配置清空,步骤如下：
R3#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm] 回车
R3#reload
System configuration has been modified. Save? [yes/no]: no 这里一定要选“no”
任务**1.** 配置网络地址转换（NAT）和默认路由实现内网和公网的通信。
首先按照图中要求配置接口IP地址，将R1和R3作为两个连接私有网络和公网的路由器，将R2和R4看作公网的路由器。R1和R3不需要启用任何动态路由协议。R2和R4是公网路由器，他们要使用动态路由协议实现公网的互联。
1. 配置个台路由器的接口IP地址。
2. 在R2和R4上配置动态路由协议，实现公网互联。两台路由器都能看到所有公网的路由信息。
3. 配置PC1和PC3的IP地址，它们作为两个私有网络的客户端。具体IP设置如下：
PC1：IP地址192.168.1x.2
子网掩码：255.255.255.0
网关：192.168.1x.1
PC3：IP地址192.168.2x.2
子网掩码：255.255.255.0
网关：192.168.3x.1
4. 在R1和R3上配置默认路由，使它们能正确转发到公网的数据包。
R1(config)#ip route 0.0.0.0 0.0.0.0 12.0.0.2
R3(config)#ip route 0.0.0.0 0.0.0.0 23.0.0.2
5. 使用PC1和PC3测试ping公网上R4上100.0.0.1。发现ping不通，也就是说，这是私有网络的主机还不能正常访问公网。
6. 在R4上使用R4#debug ip icmp命令 ，打开icmp数据包的监控。再次在PC1上ping 100.0.0.1，观察R4上的日志信息，发现R4试图将ping的回应包发到192.168.1x.2上去，显然R4的路由表中是不可能有这些私网的路由信息的。所以，PC1发出到公网的访问虽然能正确到达目的地，但是目的地发出的回应无法正确回到PC1上。
7. 在R1和R3上配置网络地址转换，以下是三种方式的配置：
（1）静态NAT
R1(config)#ip nat inside source static 192.168.1x.2 12.0.0.3 (要写没有用过的公网地址)
R1(config)#interface s0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#interface e0
R1(config-if)#ip nat inside
尝试使用PC1ping100.0.0.1，发现能通，在R4上观察日志，发现，这是R4的发出

的ping回应是去12.0.0.3的，实际上，R4将ping回应数据包发到R1上，R1再将这个数据包发回PC1，对R4来说，它看到的是12.0.0.3这个IP地址在ping它。

```
R3(config)#ip nat inside source static 192.168.2x.2 23.0.0.4
R3(config)#interface s1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#interface e0
R3(config-if)#ip nat inside
```

配置完成后做测试。

（2）动态NAT

```
R1(config)#no ip nat inside source static 192.168.1x.2 12.0.0.3 去掉原来的静态NAT转换规则
R1(config)#access-list 1 permit 192.168.1x.0 0.0.0.255
R1(config)#ip nat pool abc 12.0.0.3 12.0.0.100 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool abc
R1(config)#interface s0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#interface e0
R1(config-if)#ip nat inside
R1(config-if)#exit
```

```
R3(config)#no ip nat inside source static 192.168.2x.2 23.0.0.4去掉原来的静态NAT转换规则
R3(config)#access-list 1 permit 192.168.2x.0 0.0.0.255
R3(config)#ip nat pool abc 23.0.0.4 23.0.0.100 netmask 255.0.0.0
R3(config)#ip nat inside source list 1 pool abc
R3(config)#interface s1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#int e0
R3(config-if)#ip nat inside
```

(3)PAT

```
R1#clear ip nat translation *
R1#conf t
R1(config)#no ip nat pool abc 12.0.0.3 12.0.0.100 netmask 255.0.0.0 去掉原来的动态nat地址池
R1(config)#no ip nat inside source list 1 pool abc 去掉原来的动态NAT转换规则
R1(config)# access-list 1 permit 192.168.1x.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface serial 0 overload
```

```
R1(config)#interface s0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#interface e0
R1(config-if)#ip nat inside
R1(config-if)#exit
R3#clear ip nat translation *
R3#conf t
R3(config)# no ip nat pool abc 23.0.0.4 23.0.0.100 netmask 255.0.0.0
R3(config)#no ip nat inside source list 1 pool abc
R3(config)#access-list 1 permit 192.168.2x.0 0.0.0.255
R3(config)#ip nat inside source list 1 interface serial 1 overload
R3(config)#interface s1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#interface e0
R3(config-if)#ip nat inside
```