实验　利用 IP 标准访问列表进行网络流量的控制

【实验名称】

利用 IP 标准访问列表进行网络流量的控制

【实验目的】

掌握路由器上编号的标准 IP 访问列表规则及配置

【背景描述】

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 3 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。

经理部的网段为 172.16.2.0，销售部门的网段为 172.16.1.0、财务部门的网段为 172.16.4.0。

【需求分析】

只允许网段 172.16.2.0 与 172.16.4.0 的主机进行通信，不允许 172.16.1.0 去访问 172.16.4.0 网段的主机。

【实验拓扑】

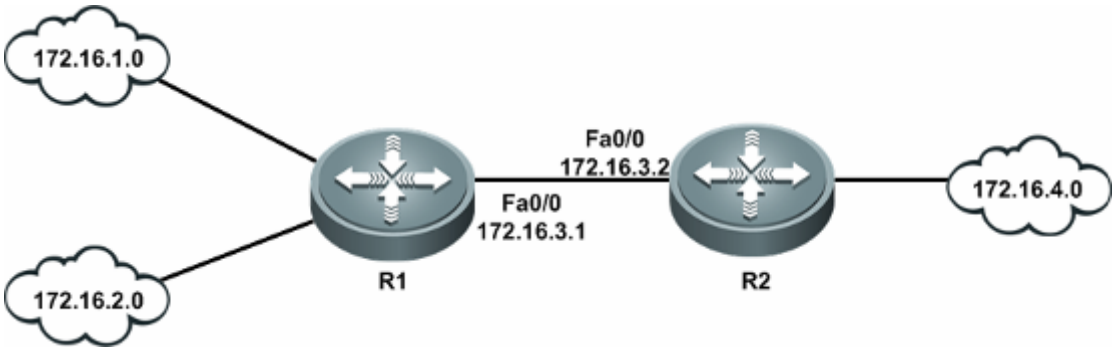

图 10-2 实验拓扑图

【预备知识】

路由器基本配置知识、访问控制列表知识

【实验设备】

路由器（两台）、V.35 线缆（1 条）、直连线或交叉线（3 条）

【实验原理】

IP ACL（IP 访问控制列表或 IP 访问列表）是实现对流经路由器或交换机的数据包根据一定的规则进行过滤，从而提高网络可管理性和安全性。

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表。

标准 IP 访问列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤。

扩展 IP 访问列表可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用。

入栈应用是指由外部经该接口进行路由器的数据包进行过滤。

出栈应用是指路由器从该接口向外转发数据时进行数据包的过滤。

IP ACL 的配置有两种方式：按照编号的访问列表，按照命名的访问列表。

标准 IP 访问列表编号范围是 1~99、1300~1999，扩展 IP 访问列表编号范围是 100~199、2000~2699。

【实验步骤】

第一步：路由器基本配置

```
R1(config)#
R1(config)# interface    loopback 0
R1 (config-if)#ip add 172.16.1.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)# interface    loopback 1
R1 (config-if)#ip add 172.16.2.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#interface FastEthernet0/0
R1 (config-if)#ip add 172.16.3.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#end

R2(config)# interface FastEthernet 0/0
R2 (config-if)#ip add 172.16.3.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config-if)#interface FastEthernet 0/1
R2 (config-if)#ip add 172.16.4.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#end
```

第二步：配置路由

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.2
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.1
```

第三步：配置标准 IP 访问控制列表

```
R2(config)#access-list 10 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 10 permit 172.16.2.0 0.0.0.255
R2(config)# interface FastEthernet 0/1
```

R2(config-if)#ip access-group 10 out

第三步：验证测试

在没有配置 ACL 时，可以使用原地址为 172.16.1.1，目标地址为 172.16.4.10（此为连接到 R2 接口 fa0/1 的一台主机），进行 ping 通信，如下所示。

R1#ping
Protocol [ip]:
Target IP address: 172.16.4.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:172.16.1.1
Time to Live [1, 64]:
Type of service [0, 31]:
Data Pattern [0xABCD]:0xabcd
Sending 5, 100-byte ICMP Echoes to 172.16.4.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

配置 ACL 后的测试，如下所示

R1#ping
Protocol [ip]:
Target IP address: 172.16.4.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:172.16.1.1
Time to Live [1, 64]:
Type of service [0, 31]:
Data Pattern [0xABCD]:0xabcd
Sending 5, 100-byte ICMP Echoes to 172.16.4.10, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5)

R1#ping
Protocol [ip]:
Target IP address: 172.16.4.10
Repeat count [5]:

Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:172.16.2.1
Time to Live [1, 64]:
Type of service [0, 31]:
Data Pattern [0xABCD]:0xabcd
Sending 5, 100-byte ICMP Echoes to 172.16.4.10, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ping（172.16.2.0 网段的主机不能 ping 通 172.16.4.0 网段的主机；172.16.1.0 网段的主机能 ping 通 172.16.4.0 网段的主机）。

R2#show access-lists

ip access-list standard 10
 10 deny 172.16.1.0 0.0.0.255
 20 permit 172.16.2.0 0.0.0.255
 35 packets filtered

R2#sh ip access-group interface fa0/1
ip access-group 10 out
Applied On interface FastEthernet 0/1

【注意事项】
1、注意在访问控制列表的网络掩码是反掩码。
2、标准控制列表要应用在尽量靠近目的地址的接口。

【参考配置】

R1#show running-config

Building configuration...
Current configuration : 590 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007 -ubu1server)
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.3.1 255.255.255.0
 duplex auto

```
 speed auto
!
interface FastEthernet 0/1
 duplex auto
 speed auto
!
interface Loopback 0
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback 1
 ip address 172.16.2.1 255.255.255.0
!
ip route    0.0.0.0 0.0.0.0    172.16.3.2
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R2#show running-config

```
Building configuration...
Current configuration : 627 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname R2
!
ip access-list standard 10
 10 deny 172.16.1.0 0.0.0.255
 20 permit 172.16.2.0 0.0.0.255
!
interface FastEthernet 0/0
 ip address 172.16.3.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/1
 ip access-group 10 out
 ip address 172.16.4.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
ip route    0.0.0.0 0.0.0.0    172.16.3.1
!
line con 0
line aux 0
line vty 0 4
  login
!
end
```