第10章 IP访问列表

10.1 利用IP标准访问列表进行网络流量的控制

【实验名称】

编号的标准IP访问列表。

【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。

PC1代表经理部的主机，PC2代表销售部门的主机、PC3代表财务部门的主机。

【技术原理】

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。

【实现功能】

实现网段间互相访问的安全控制。

【实验设备】

R1762路由器（两台）、V.35线缆（1条）、直连线或交叉线（3条）

【实验拓扑】

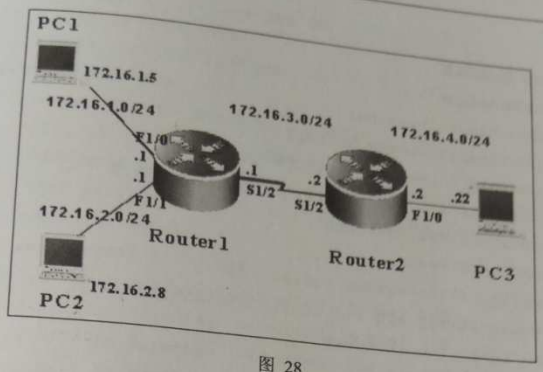

图 28

【实验步骤】

步骤1. 基本配置。

☼ Router1 基本配置

```
Red-Giant>enable
Red-Giant#configure terminal
Red-Giant(config)#hostname Router1
Router1(config)# interface fastEthernet 1/0
Router1(config-if)#ip add 172.16.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)# interface fastEthernet 1/1
Router1(config-if)#ip add 172.16.2.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#interface serial 1/2
Router1(config-if)#ip add 172.16.3.1 255.255.255.0
Router1(config-if)#clock rate 64000
Router1(config-if)#no shutdown
Router1(config-if)#end
```

测试命令：show ip interface brief。

```
Router1#show ip int brief                          !观察接口状态
Interface                  IP-Address(Pri)    OK?    Status
serial 1/2                 172.16.3.1/24      YES    UP
serial 1/3                  no address        YES    DOWN
FastEthernet 1/0           172.16.1.1/24      YES    UP
FastEthernet 1/1           172.16.2.1/24      YES    UP
```

```
Null 0                 no address          YES      UP
```

☼ Router2基本配置

```
Red-Giant>enable
Red-Giant#configure terminal
Red-Giant(config)#hostname Router2
Router2(config)# interface fastEthernet 1/0
Router2(config-if)#ip add 172.16.4.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config-if)#interface serial 1/2
Router2(config-if)#ip add 172.16.3.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#end
```

测试命令：show ip interface brief。

```
Router2#show ip int brief                                    !观察接口状态
Interface              IP-Address(Pri)    OK?    Status
serial 1/2             172.16.3.2/24      YES    UP
serial 1/3             no address         YES    DOWN
FastEthernet 1/0       172.16.4.1/24      YES    UP
FastEthernet 1/1       no address         YES    DOWN
Null 0                 no address         YES    UP
```

☼ 配置静态路由

```
Router1(config)#ip route 172.16.4.0 255.255.255.0 serial 1/2
Router2(config)#ip route 172.16.1.0 255.255.255.0 serial 1/2
Router2(config)#ip route 172.16.2.0 255.255.255.0 serial 1/2
```

测试命令：show ip route。

```
Router1#show ip route                                        !查看路由表信息
Codes:  C - connected, S - static,  R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default
Gateway of last resort is no set
C    172.16.1.0/24 is directly connected, FastEthernet 1/0
C    172.16.1.1/32 is local host.
C    172.16.2.0/24 is directly connected, FastEthernet 1/1
C    172.16.2.1/32 is local host.
```

```
C    172.16.3.0/24 is directly connected, serial 1/2
C    172.16.3.1/32 is local host.
S    172.16.4.0/24 is directly connected, serial 1/2
Router2#show ip route
Codes:  C - connected, S - static,  R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default
Gateway of last resort is no set
S    172.16.1.0/24 is directly connected, serial 1/2
S    172.16.2.0/24 is directly connected, serial 1/2
C    172.16.3.0/24 is directly connected, serial 1/2
C    172.16.3.2/32 is local host.
C    172.16.4.0/24 is directly connected, FastEthernet 1/0
C    172.16.4.1/32 is local host.
```

步骤2. 配置标准IP访问控制列表。

```
Router2(config)#access-list 1 deny 172.16.2.0 0.0.0.255
  ! 拒绝来自172.16.2.0网段的流量通过
Router2(config)#access-list 1 permit 172.16.1.0 0.0.0.255
  ! 允许来自172.16.1.0网段的流量通过
```

验证测试：

```
Router2#show access-lists 1
Standard IP access list 1 includes 2 items:
   deny   172.16.2.0, wildcard bits 0.0.0.255
  permit 172.16.1.0, wildcard bits 0.0.0.255
```

步骤3. 把访问控制列表在接口下应用。

```
Router2(config)# interface fastEthernet 1/0
Router2(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：

```
Router2#show ip interface fastEthernet 1/0
FastEthernet 1/0
 IP interface state is: UP
 IP interface type is: BROADCAST
 IP interface MTU is: 1500
 IP address is:
  172.16.4.1/24 (primary)
```

```
  IP address negotiate is: OFF
  Forward direct-boardcast is: ON
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Route horizontal-split is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
  Outgoing access list is 1.                    !查看访问列表在接口上的应用
  Inbound access list is not set.
```

步骤**4.** 验证测试。

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）。

【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】

```
Router1#show running-config
Building configuration...                       !查看路由器 1 的全部配置
Current configuration : 544 bytes
!
version 8.32(building 53)
hostname Router1
!
!
interface serial 1/2
ip address 172.16.3.1 255.255.255.0
clock rate 64000
!
interface serial 1/3
clock rate 64000
!
interface FastEthernet 1/0
ip address
```