

## 实验三十七、扩展访问列表的配置

### 一、 实验目的

1. 掌握扩展访问列表的配置
2. 理解理解扩展访问列表丰富的过滤条件

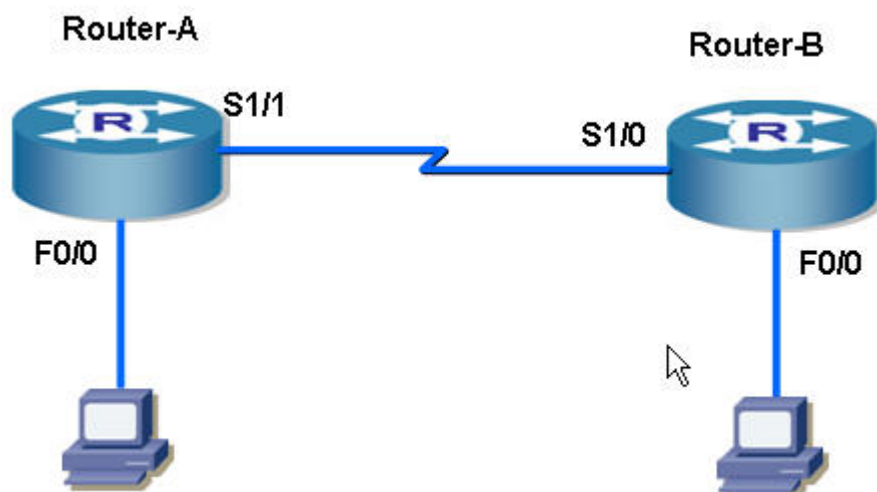
### 二、 应用环境

1. 可以针对目标 IP 地址进行控制
2. 针对某些服务进行控制
3. 可以针对某些协议进行控制

### 三、 实验设备

- |             |    |
|-------------|----|
| 1. DCR-1751 | 两台 |
| 2. PC 机     | 两台 |
| 3. CR-V35MT | 一条 |
| 4. CR-V35FC | 一条 |
| 5. 网线       | 两条 |

### 四、 实验拓扑



### 五、 实验要求

#### ROUTER-A

S1/1 (DCE)	192.168.1.1/24
F0/0	192.168.0.1/24

#### ROUTER-B

S1/0 (DTE)	192.168.1.2/24
F0/0	192.168.2.1/24

	PC-A	PC-B
IP	192.168.0.2/24	192.168.2.2/24
网关	192.168.0.1	192.168.2.1

实验目标: 禁止 192.168.0.0/24 Telnet 到 PC-B, 但能 Ping。

## 六、 实验步骤

第一步: 参照实验三和上表, 配置所有接口的地址, 并测试连通性

Router-A#**ping 192.168.1.2**

PING 192.168.1.2 (192.168.1.2): 56 data bytes

!!!!

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 20/28/30 ms

第二步: 参照实验七, 配置静态路由

Router-A#**sh ip route**

Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected

D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area

ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2

OE1 - OSPF external type 1, OE2 - OSPF external type 2

DHCP - DHCP type

VRF ID: 0

C 192.168.0.0/24 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Serial1/1

**S 192.168.2.0/24 [1,0] via 192.168.1.2**

Router-B#**sh ip route**

Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected

D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area

ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2

OE1 - OSPF external type 1, OE2 - OSPF external type 2

DHCP - DHCP type

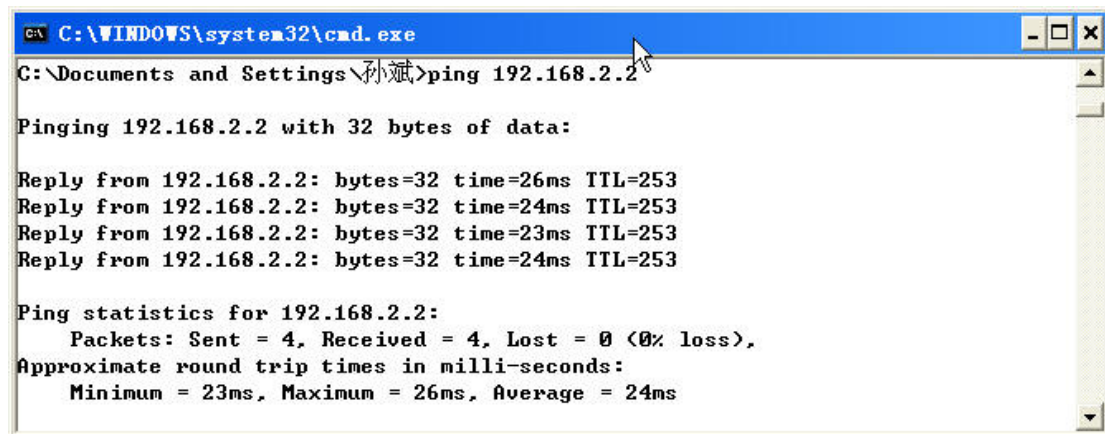
VRF ID: 0

**S 192.168.0.0/24 [1,0] via 192.168.1.1**

C 192.168.1.0/24 is directly connected, Serial1/0

C 192.168.2.0/24 is directly connected, FastEthernet0/0

第三步: PC-A 能与 PC-B 通讯



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\孙斌>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=26ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 26ms, Average = 24ms
```

第四步: 在 ROUTER-A 上设置访问列表

Router-A#conf

Router-A\_config#ip access-list extended 192 ! 定义扩展访问列表

Router-A\_config\_ext\_nacl#deny tcp 192.168.0.0 255.255.255.0 192.168.2.2 255.255.255.255 eq 23  
! 设置扩展访问列表, 拒绝 Telnet

Router-A\_config\_ext\_nacl#permit icmp any any ! 允许 Ping

Router-A\_config\_ext\_nacl#exit

Router-A\_config#int f0/0 ! 进入离源比较近的接口

Router-A\_config\_f0/0#ip access-group 192 in ! 绑定访问列表在 IN 的方向

第五步: 查看访问列表

Router-A#sh ip access-list

Extended IP access list 192

```
deny    tcp 192.168.0.0 255.255.255.0 192.168.2.2 255.255.255.0 eq telnet
permit icmp any any
```

第六步: 验证



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\孙斌>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=27ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253
Reply from 192.168.2.2: bytes=32 time=25ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 27ms, Average = 25ms

C:\Documents and Settings\孙斌>telnet 192.168.2.2
正在连接到192.168.2.2...不能打开到主机的连接, 在端口 23: 连接失败
C:\Documents and Settings\孙斌>
```

## 七、 注意事项和排错

1. 扩展访问列表通常放在离源比较近的地方
2. 扩展访问列表可以基于源、目标 IP、协议、端口号等条件过滤

3. 命令比较长, 可以通过? 的方式查看帮助
4. 注意隐含的 DENY

## 八、配置序列

Router-A#sh run

Building configuration...

Current configuration:

!

!version 1.3.2E

service timestamps log date

service timestamps debug date

no service password-encryption

!

hostname Router-A

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.0.1 255.255.255.0

no ip directed-broadcast

**ip access-group 192 in**

!

interface Serial1/0

no ip address

no ip directed-broadcast

physical-layer speed 64000

!

interface Serial1/1

ip address 192.168.1.1 255.255.255.0

no ip directed-broadcast

physical-layer speed 64000

!

interface Async0/0

no ip address

no ip directed-broadcast

!

!

!

ip route 192.168.2.0 255.255.255.0 192.168.1.2

!



```
!  
ip access-list extended 192  
  deny    tcp 192.168.0.0 255.255.255.0 192.168.2.2 255.255.255.0 eq telnet  
  permit icmp any any  
!  
!  
!
```

## 九、 共同思考

1. 为什么扩展访问列表通常放在源比较近的接口?
2. 访问列表中主机还有什么表示方法?
3. 为什么访问列表中至少要有一条允许?

## 十、 课后练习

请配置禁止访问 PC-A 的 HTTP 服务

## 十一、 相关命令详解

### 1. deny

在 IP 访问列表配置模式中可使用此命令配置禁止规则, 要从 IP 访问列表中删除 deny 规则, 在命令前加 no 前缀。

```
deny source [source-mask] [log]
```

```
no deny source [source-mask] [log]
```

```
deny protocol source source-mask destination destination-mask [precedence  
precedence] [tos tos] [log]
```

```
no deny protocol source source-mask destination destination-mask [precedence  
precedence] [tos tos] [log]
```

对于互联网控制报文协议(ICMP), 也可以使用以下句法:

```
deny icmp source source-mask destination destination-mask [icmp-type] [precedence  
precedence] [tos tos] [log]
```

对于 Internet 组管理协议(IGMP), 可以使用以下句法:

```
deny igmp source source-mask destination destination-mask [igmp-type] [precedence  
precedence] [tos tos] [log]
```

对于 TCP, 可以使用以下句法:

```
deny tcp source source-mask [operator port] destination destination-mask [operator  
port ] [established] [precedence precedence] [tos tos] [log]
```

对于数据报协议(UDP), 可以使用以下句法:

```
deny udp source source-mask [operator port] destination destination-mask [operator
```

*port*] [*precedence precedence*] [*tos tos*] [*log*]

**参数:**

<i>protocol</i>	协议名字或 IP 协议号。它可以是关键字 icmp、igmp、igrp、ip、ospf、tcp 或 udp，也可以是表 IP 协议号的一个整数。为了匹配任何 Internet 协议(包括 ICMP、TCP 和 UDP)使用关键字 ip。某些协议允许进一步限定，如下描述。
<i>source</i>	源网络或主机号。有两种方法指定源：32 位二进制数，用四个点隔开的十进制数表示。使用关键字 any 作为 0.0.0.0 0.0.0.0 的源和源掩码缩写。
<i>source-mask</i>	源地址网络掩码。使用关键字 any 作为 0.0.0.0 0.0.0.0 的源和源掩码缩写。
<i>destination</i>	目标网络或主机号。有两种方法指定： 使用四个点隔开的十进制数表示的 32 位二进制数。 使用关键字 any 作为 0.0.0.0 0.0.0.0 的目标和目标掩码的缩写。
<i>destination-mask</i>	目标地址网络掩码。使用关键字 any 作为 0.0.0.0 0.0.0.0 的目标地址和目标地址掩码缩写。
<i>precedence</i> <i>precedence</i>	(可选)包可以由优先级过滤，用 0 到 7 的数字指定。
<i>tos tos</i>	(可选) 数据包可以使用服务层过滤。使用数字 0—15 指定。
<i>icmp-type</i>	(可选)ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255。
<i>igmp-type</i>	(可选)IGMP 包可由 IGMP 报文类型或报文名过滤。类型是 0 到 15 的数字。
<i>operator</i>	(可选)比较源或目标端口。操作包括 lt(小于)， gt(大于)， eq(等于)， neq(不等于)。如果操作符放在 <i>source</i> 和 <i>source-mask</i> 之后，那么它必须匹配这个源端口。如果操作符放在 <i>destination</i> 和 <i>destination-mask</i> 之后，那么它必须匹配目标端口。
<i>port</i>	(可选)TCP 或 UDP 端口的十进制数字或名称。端口号是一个 0 到 65535 的数字。TCP 端口名列在“使用方针”部



分。当过滤 TCP 时,可以只使用 TCP 端口名称。UDP 端口名称也列在“使用说明”部分。当过滤 TCP 时,只可使用 TCP 端口名。当过滤 UDP 时,只可使用 UDP 端口名。

**established** (可选)只对 TCP 协议,表示一个已建立的连接。如果 TCP 数据报 ACK 或 RST 位设置时,出现匹配。非匹配的情况是初始化 TCP 数据报,以形成一个连接。

**log** (可选)可以进行日志记录。

**命令模式: IP 访问列表配置态**

**使用说明:** 可以使用访问表控制包在接口上的传输,控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。分段 IP 包,而不是初始段,立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容,不必匹配 TCP 源端口、服务值的类型或包的优先权。

**注意:** 在初始建立一个访问表后,任何后续的添加内容(可能由终端键入)放置在列表的尾部。

以下显示用于替换端口号的 TCP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个? 替代端口号的方式来寻找。

bgp  
ftp  
ftp-data  
login  
pop2  
pop3  
smtp  
telnet  
www

以下显示用于替换端口号的 UDP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个? 替代端口号的方式来寻找。

domain  
snmp  
syslog  
tftp

### 示例:

下面示例禁止 192.168.5.0 这个网段:

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

**注意:** IP 访问表由一个隐含的 deny 规则结束。

### 相关命令:

```
ip access-group
ip access-list
permit
show ip access-list
```

## 2. ip access-group

为了控制访问一个接口,使用 ip access-group 接口配置命令。为了删除这个指定的访问组,使用 no 格式命令。

```
ip access-group {access-list-name} {in | out}
no ip access-group {access-list-name} {in | out}
```

### 参数:

<i>access-list-name</i>	访问表名。这是一个最长为 20 个字符的字符串。
in	在进接口时使用访问列表。
out	在出接口时使用访问列表。

### 命令模式: 接口配置态

**使用说明:** 访问列表既可用在出接口也可用在入接口。对于标准的入口访问列表,在接收到包之后,对照访问列表检查包的源地址。对于扩展的访问列表,该路由器也检查目标地址。如果访问表允许该地址,那么软件继续处理该包。如果访问表不允许该地址,该软件放弃包并返回一个 ICMP 主机不可到达报文。

对于标准的出口访问表,在接收和路由一个包到控制接口以后,软件对照访问列表检查包的源地址。对于扩展的访问表,路由器还检查接收端地址。如果访问表允许该软件就传送这个包。如果访问列表不允许该地址,软件放弃这个包并返回一个 ICMP 主机不可达报文。

如果指定的访问列表不存在,所有的包允许通过。

### 示例:

下例在以太网接口 0 的包出口上应用列表 filter:

```
interface ethernet 0
ip access-group filter out
```

### 相关命令:

```
ip access-list
```



show ip access-list

### 3. ip access-list

使用此命令后, 进入的 IP 访问列表配置模式。在这状态下可以增加和删除访问规则。命令 exit 返回配置状态。

使用 no 前缀, 删除 IP 访问列表。

ip access-list {standard | extended} *name*

no ip access-list {standard | extended} *name*

**参数:**

standard            指定为标准访问列表

extended           指定为扩展访问列表

name                访问表名。这是一个最长 20 的字符串。

**缺省:** 没有 IP 访问列表被定义。

**命令模式:** 全局配置态

**使用说明:** 使用此命令将进入 IP 访问列表配置模式, 在 IP 访问列表配置模式中, 可以用 deny 或 permit 命令来配置访问规则。

**示例:**

以下的例子配置一个标准访问列表

ip access-list standard filter

deny 192.168.1.0 255.255.255.0

permit any

**相关命令:**

deny

ip access-group

permit

show ip access-list

### 4. permit

在 IP 访问列表配置模式中可使用此命令配置允许规则, 要从 IP 访问列表中删除 permit 规则, 在命令前加 no 前缀。

permit *source* [*source-mask*] [*log*]

no permit *source* [*source-mask*] [*log*]

permit *protocol source source-mask destination destination-mask* [*precedence precedence*] [*tos tos*] [*log*]

no permit *protocol source source-mask destination destination-mask* [*precedence precedence*] [*tos tos*] [*log*]

对于互联网控制报文协议(ICMP), 也可以使用以下句法:

```
permit icmp source source-mask destination destination-mask [icmp-type] [precedence precedence] [tos tos] [log]
```

对于 Internet 组管理协议(IGMP), 可以使用以下句法:

```
permit igmp source source-mask destination destination-mask [igmp-type] [precedence precedence] [tos tos] [log]
```

对于 TCP, 可以使用以下句法:

```
permit tcp source source-mask [operator port] destination destination-mask [operator port] [established] [precedence precedence] [tos tos] [log]
```

对于数据报协议(UDP), 可以使用以下句法:

```
permit udp source source-mask [operator port [port]] destination destination-mask [operator port] [precedence precedence] [tos tos] [log]
```

#### 参数:

<i>protocol</i>	协议名字或 IP 协议号。它可以是关键字 icmp、igmp、igrp、ip、ospf、tcp 或 udp, 也可以是表 IP 协议号的一个整数。为了匹配任何 Internet 协议(包括 ICMP、TCP 和 UDP)使用关键字 ip。某些协议允许进一步限定, 如下描述。
<i>source</i>	源网络或主机号。有两种方法指定源: 32 位二进制数, 用四个点隔开的十进制数表示。使用关键字 any 作为 0.0.0.0 0.0.0.0 的源和源掩码缩写。
<i>source-mask</i>	源地址网络掩码。使用关键字 any 作为 0.0.0.0 0.0.0.0 的源和源掩码缩写。
<i>destination</i>	目标网络或主机号。有两种方法指定: 使用四个点隔开的十进制数表示的 32 位二进制数。使用关键字 any 作为 0.0.0.0 0.0.0.0 的目标和目标掩码的缩写。
<i>destination-mask</i>	目标地址网络掩码。使用关键字 any 作为 0.0.0.0 0.0.0.0 的目标地址和目标地址掩码缩写。
<i>precedence</i> <i>precedence</i>	(可选)包可以由优先级过滤, 用 0 到 7 的数字指定。
<i>tos tos</i>	(可选) 数据包可以使用服务层过滤。使用数字 0—15 指定。
<i>icmp-type</i>	(可选)ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255。

<i>igmp-type</i>	(可选)IGMP 包可由 IGMP 报文类型或报文名过滤。类型是 0 到 15 的数字。
<i>operator</i>	(可选)比较源或目标端口。操作包括 lt(小于), gt(大于), eq(等于), neq(不等于)。如果操作符放在 source 和 source-mask 之后, 那么它必须匹配这个源端口。如果操作符放在 destination 和 destination-mask 之后, 那么它必须匹配目标端口。
<i>port</i>	(可选)TCP 或 UDP 端口的十进制数字或名称。端口号是一个 0 到 65535 的数字。TCP 端口名列在“使用方针”部分。当过滤 TCP 时, 可以只使用 TCP 端口名称。UDP 端口名称也列在“使用说明”部分。当过滤 TCP 时, 只可使用 TCP 端口名。当过滤 UDP 时, 只可使用 UDP 端口名。
<i>established</i>	(可选)只对 TCP 协议, 表示一个已建立的连接。如果 TCP 数据报 ACK 或 RST 位设置时, 出现匹配。非匹配的情况是初始化 TCP 数据报, 以形成一个连接。
<i>log</i>	(可选)可以进行日志记录。

**命令模式:** IP 访问列表配置态

**使用说明:** 可以使用访问表控制包在接口上的传输, 控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。

分段 IP 包, 而不是初始段, 立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容, 不必匹配 TCP 源端口、服务值的类型或包的优先权。

**注意:** 在初始建立一个访问表后, 任何后续的添加内容(可能由终端键入)放置在列表的尾部。

以下显示用于替换端口号的 TCP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个? 替代端口号的方式来寻找。

bgp  
ftp  
ftp-data  
login  
pop2  
pop3  
smtp

telnet

www

以下显示用于替换端口号的 UDP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个? 替代端口号的方式来寻找。

domain

snmp

syslog

tftp

示例:

下面示例允许 192.168.5.0 这个网段:

```
ip access-list standard filter
```

```
permit 192.168.5.0 255.255.255.0
```

注意: IP 访问表由一个隐含的 deny 规则结束。

相关命令:

```
deny
```

```
ip access-group
```

```
ip access-list
```

```
show ip access-list
```

## 5. show ip access-list

要显示当前的 IP 访问列表内容, 使用 show ip access-list 命令。

```
show ip access-list[access-list-name]
```

参数:

*access-list-name* 访问表名。这是一个最长 20 的字符串。

缺省: 显示所有标准的和扩展的 IP 访问列表。

命令模式: 管理态

使用说明: show ip access-list 命令允许你指定一个特定的访问列表。

示例:

以下是不指定名时 show ip access-list 命令的示例输出:

```
Router# show ip access-list
```

```
ip access-list standard aaa
```

```
permit 192.2.2.1
```

```
permit 192.3.3.0 255.255.255.0
```

```
ip access-list extended bbb
```

```
permit tcp any any eq www
```

permit ip any any

以下是指定访问表名时, show ip access-list 命令的示例输出:

ip access-list extended bbb

permit tcp any any eq www

permit ip any any

