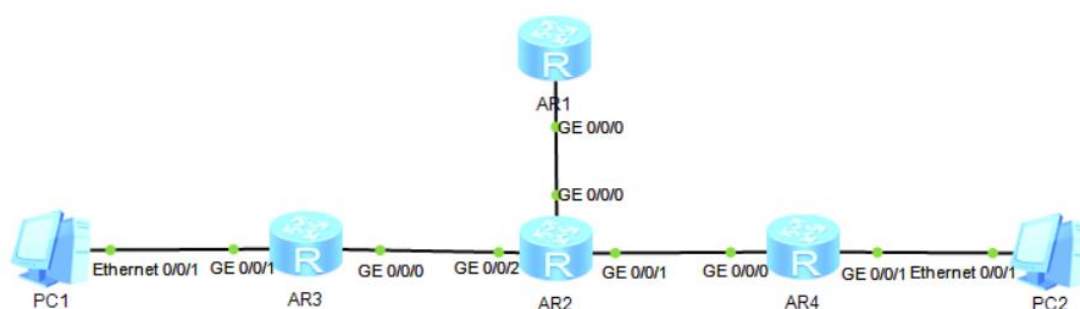


高级访问控制列表命令实验

Hollow Man

一、 实验网络拓扑



二、 实验网络 IP 划分

使用 RIP 1 协议进行路由配置，IP 划分见下表：

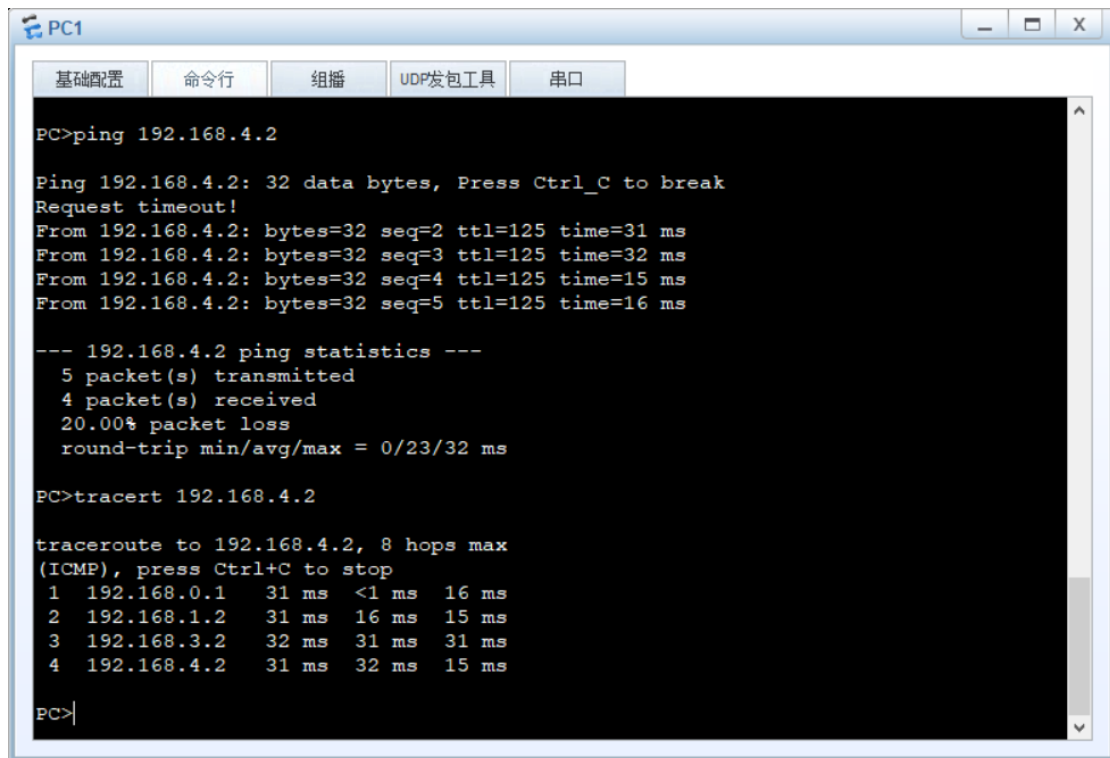
	GE 0/0/0	GE 0/0/1	GE 0/0/2
AR1	192.168.2.1/24		
AR2	192.168.2.2/24	192.168.3.1/24	192.168.1.2/24
AR3	192.168.1.1/24	192.168.0.1/24	
AR4	192.168.3.2/24	192.168.4.1/24	

2、PC 机设置方案

主机序号	IP 地址	网关
PC1	192.168.0.2/24	192.168.0.1/24
PC2	192.168.4.2/24	192.168.4.1/24

三、 实验内容

使用华为 eNSP 模拟器，配置好 IP 地址及 RIP 1 路由协议，然后用 ping 和 tracet 测试两台主机之间的链接：



The screenshot shows a terminal window titled 'PC1' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The '命令行' (Command Line) tab is active. The terminal displays the output of a ping and a traceroute command to the IP address 192.168.4.2.

```
PC>ping 192.168.4.2

Ping 192.168.4.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.4.2: bytes=32 seq=2 ttl=125 time=31 ms
From 192.168.4.2: bytes=32 seq=3 ttl=125 time=32 ms
From 192.168.4.2: bytes=32 seq=4 ttl=125 time=15 ms
From 192.168.4.2: bytes=32 seq=5 ttl=125 time=16 ms

--- 192.168.4.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/23/32 ms

PC>tracert 192.168.4.2

tracert to 192.168.4.2, 8 hops max
(ICMP), press Ctrl+C to stop
 1  192.168.0.1    31 ms  <1 ms  16 ms
 2  192.168.1.2    31 ms  16 ms  15 ms
 3  192.168.3.2    32 ms  31 ms  31 ms
 4  192.168.4.2    31 ms  32 ms  15 ms

PC>|
```

可见路由器配置成功。

然后配置 AR4 的 telnet 服务：

```
AR4
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]aaa
[Huawei-aaa]local-user admin password cipher 123
[Huawei-aaa]local-user admin service-type telnet
[Huawei-aaa]local-user admin privilege level 3
[Huawei-aaa]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode aaa
      ^
Error: Unrecognized command found at '^' position.
[Huawei-ui-vty0-4]auth?
      authentication-mode  Configure the authentication mode for a user terminal
                           interface
[Huawei-ui-vty0-4]auth aaa
[Huawei-ui-vty0-4]telnet server enable
Error: TELNET server has been enabled
[Huawei]telnet 192.168.4.1
      ^
Error: Unrecognized command found at '^' position.
[Huawei]
<Huawei>telnet 192.168.4.1
Press CTRL_] to quit telnet mode
Trying 192.168.4.1 ...
Connected to 192.168.4.1 ...

Login authentication

Username:admin
Password:
Error: Local authentication is rejected.

  Logged Fail!

Username:admin
Password:
#
```

在 AR3 上登陆 192.168.4.1 端口，显示登陆成功：

```
AR3
<Huawei>telnet 192.168.4.1
Press CTRL_] to quit telnet mode
Trying 192.168.4.1 ...
Connected to 192.168.4.1 ...

Login authentication

Username:admin
Password:
-----

User last login information:
-----
Access Type: Telnet
IP-Address  : 192.168.4.1
Time       : 2019-11-13 20:20:18-08:00
-----
<Huawei>
```

使用 WireShark 抓包，结果如下：

No.	Time	Source	Destination	Protocol	Length	Info
3	26.609000	192.168.1.2	255.255.255.255	RIPv1	106	Response
4	28.031000	192.168.1.1	192.168.4.1	TCP	60	49800 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
5	28.047000	192.168.4.1	192.168.1.1	TCP	60	23 → 49800 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
6	28.062000	192.168.1.1	192.168.4.1	TCP	60	49800 → 23 [ACK] Seq=1 Ack=1 Win=8192 Len=0
7	28.062000	192.168.1.1	192.168.4.1	TELNET	63	Telnet Data ...
8	28.078000	192.168.4.1	192.168.1.1	TELNET	63	Telnet Data ...
9	28.078000	192.168.4.1	192.168.1.1	TELNET	63	Telnet Data ...
10	28.078000	192.168.4.1	192.168.1.1	TELNET	60	Telnet Data ...
11	28.093000	192.168.4.1	192.168.1.1	TELNET	82	Telnet Data ...
12	28.093000	192.168.1.1	192.168.4.1	TELNET	66	Telnet Data ...
13	28.093000	192.168.1.1	192.168.4.1	TELNET	65	Telnet Data ...
14	28.093000	192.168.4.1	192.168.1.1	TELNET	65	Telnet Data ...
15	28.140000	192.168.4.1	192.168.1.1	TCP	60	23 → 49800 [ACK] Seq=64 Ack=33 Win=8169 Len=0
16	28.187000	192.168.1.1	192.168.4.1	TCP	60	49800 → 23 [ACK] Seq=33 Ack=64 Win=8192 Len=0
17	35.015000	192.168.1.1	255.255.255.255	RIPv1	66	Response
18	36.703000	192.168.4.1	192.168.1.1	TCP	60	[TCP Keep-Alive] 23 → 49800 [ACK] Seq=63 Ack=33 Win=8192 Len=0
19	36.718000	192.168.1.1	192.168.4.1	TCP	60	[TCP Keep-Alive ACK] 49800 → 23 [ACK] Seq=33 Ack=64 Win=8192 Len=0

随后在 AR2 路由器上进行高级访问控制列表的配置：

```

[Huawei]acl 3000
[Huawei-acl-adv-3000]rule 10 deny tcp 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.25
5 eq 23

Error:Too many parameters found at '^' position.
[Huawei-acl-adv-3000]rule 10 deny tcp source 192.168.4.0 0.0.0.255 destination 1
92.168.1.0 0.0.0.255 eq 23

Error: Wrong parameter found at '^' position.
[Huawei-acl-adv-3000]rule 10 deny tcp source 192.168.4.0 0.0.0.255 destinati
on 192.168.1.0 0.0.0.255 source-port eq 23
[Huawei-acl-adv-3000]rule 10 deny tcp source 192.168.4.0 0.0.0.255 destination 1
92.168.1.0 0.0.0.255 eq 23

Error:Too many parameters found at '^' position.
[Huawei-acl-adv-3000]
<Huawei>save
The current configuration will be written to the device.
Are you sure to continue? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
<Huawei>

```

可以看到，华为路由器在配置时必须显式地指定源地址和目标地址以及源端口和目标端口，否则会出错。

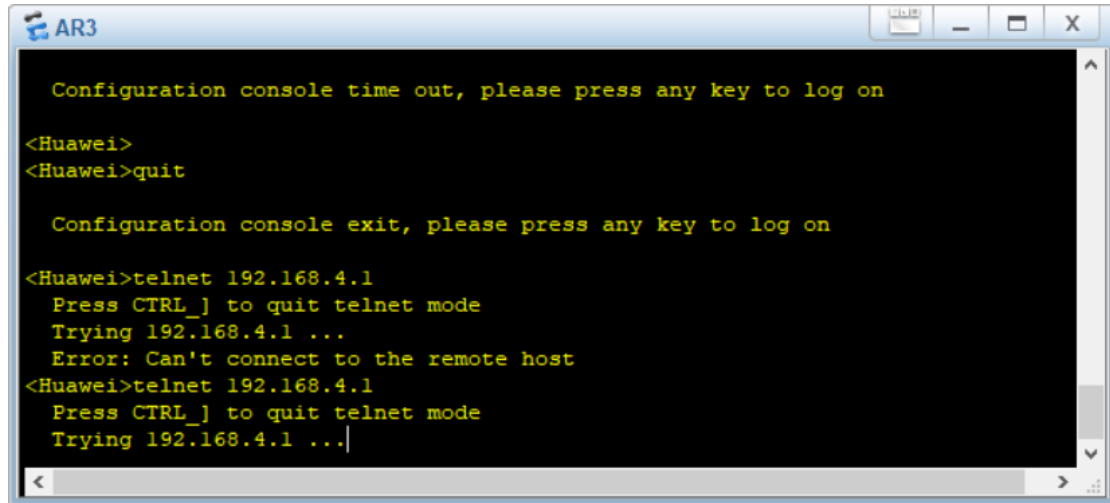
将此高级访问控制列表应用到 AR2 的 GE 0/0/1 端口：

```

Note: The configuration file will take effect after being activated
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]int gi0/0/1
[Huawei-GigabitEthernet0/0/1]traffic-filter ?
inbound Apply ACL to the inbound direction of the interface
outbound Apply ACL to the outbound direction of the interface
[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000
[Huawei-GigabitEthernet0/0/1]
<Huawei>save
The current configuration will be written to the device.
Are you sure to continue? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
<Huawei>

```

再次在 AR3 上登陆 192.168.4.1 端口，发现已经无法连接：



320 2129.062000	192.168.1.1	192.168.4.1	TCP	60 51023 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
321 2134.687000	192.168.1.1	192.168.4.1	TCP	60 [TCP Retransmission] 51023 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
322 2141.304000	192.168.1.1	192.168.4.1	TCP	60 [TCP Retransmission] 51023 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460

使用 Wireshark 抓包，可以看到此时 192.168.1.1 收不到来自 192.168.4.1 的返回数据。