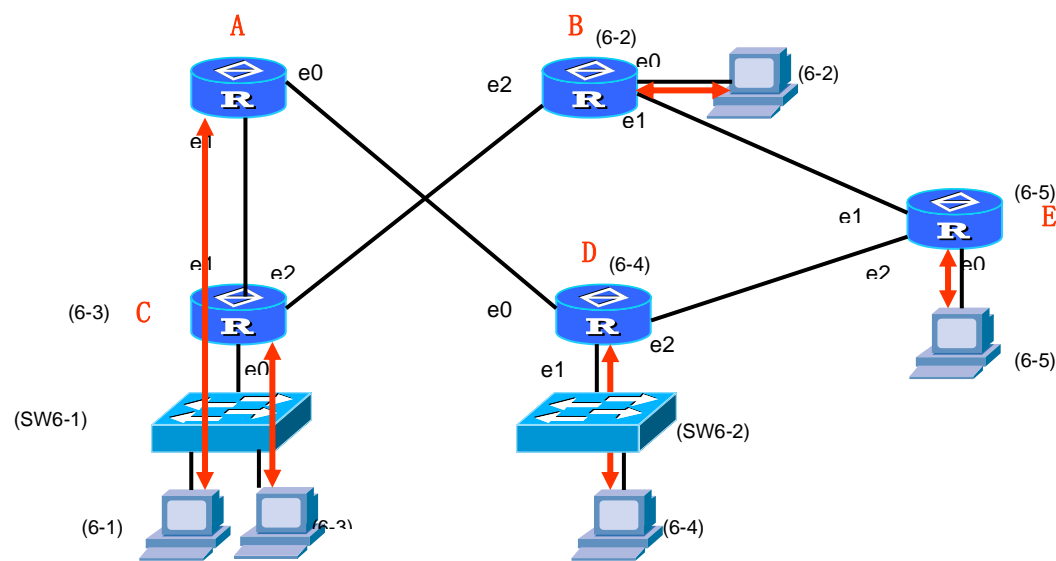


# 实验报告——基本访问控制列表实验

Hollow Man

## 一、实验小组拓扑



## 二、实验准备

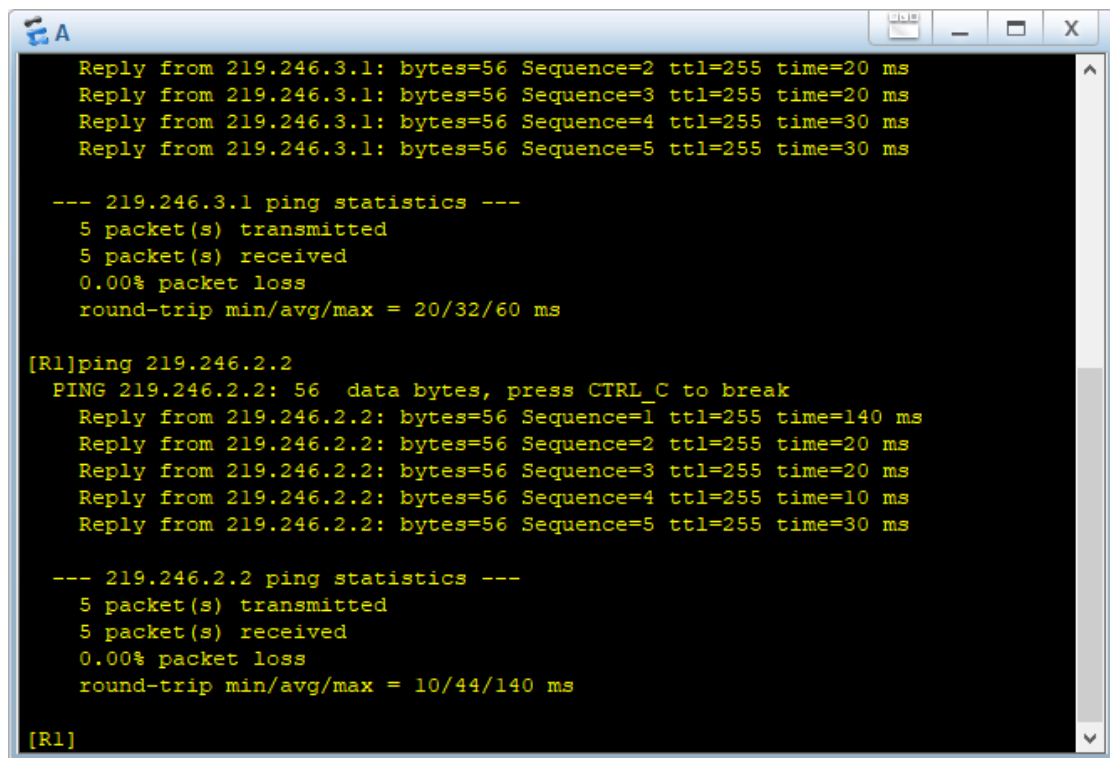
### 1、路由器网络地址方案设计

	E0	E1	E2
A	219.246.2.1/24	219.246.1.1/24	
B	219.246.9.1/24	219.246.8.2/24	219.246.4.2/24
C	219.246.3.1/24	219.246.1.2/24	219.246.4.1/24
D	219.246.2.2/24	219.246.5.1/24	219.246.6.1/24
E	219.246.7.1/24	219.246.8.1/24	219.246.6.2/24

## 2、PC 机设置方案

主机序号	IP 地址	网关
6-1	219.246.3.2/24	219.246.3.1/24
6-2	219.246.9.2/24	219.246.9.1/24
6-3	219.246.3.3/24	219.246.3.1/24
6-4	219.246.5.2/24	219.246.5.1/24
6-5	219.246.7.2/24	219.246.7.1/24

检测网络连通性（由于本次实验是基于第一次实验 rip1 路由实验，所以本次实验继续使用之前的 topo 文件，可以保证整个网络是联通的，多余的主机 ping 路由器等截图不再列出。）



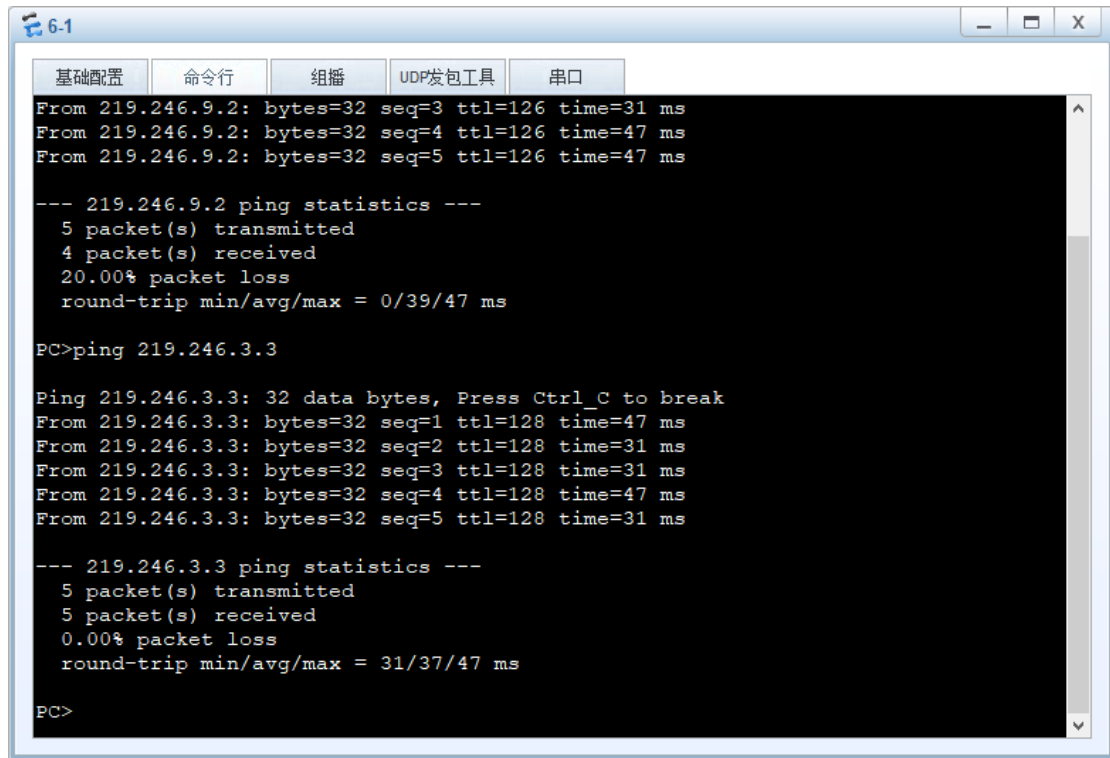
```
Reply from 219.246.3.1: bytes=56 Sequence=2 ttl=255 time=20 ms
Reply from 219.246.3.1: bytes=56 Sequence=3 ttl=255 time=20 ms
Reply from 219.246.3.1: bytes=56 Sequence=4 ttl=255 time=30 ms
Reply from 219.246.3.1: bytes=56 Sequence=5 ttl=255 time=30 ms

--- 219.246.3.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 20/32/60 ms

[R1]ping 219.246.2.2
PING 219.246.2.2: 56 data bytes, press CTRL_C to break
Reply from 219.246.2.2: bytes=56 Sequence=1 ttl=255 time=140 ms
Reply from 219.246.2.2: bytes=56 Sequence=2 ttl=255 time=20 ms
Reply from 219.246.2.2: bytes=56 Sequence=3 ttl=255 time=20 ms
Reply from 219.246.2.2: bytes=56 Sequence=4 ttl=255 time=10 ms
Reply from 219.246.2.2: bytes=56 Sequence=5 ttl=255 time=30 ms

--- 219.246.2.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 10/44/140 ms

[R1]
```



The screenshot shows a terminal window with a title bar '6-1' and tabs for '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The terminal output displays the results of a ping command from 219.246.9.2 to 219.246.3.3. The first set of results shows a 20.00% packet loss, while the second set shows 0.00% packet loss.

```
From 219.246.9.2: bytes=32 seq=3 ttl=126 time=31 ms
From 219.246.9.2: bytes=32 seq=4 ttl=126 time=47 ms
From 219.246.9.2: bytes=32 seq=5 ttl=126 time=47 ms

--- 219.246.9.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/39/47 ms

PC>ping 219.246.3.3

Ping 219.246.3.3: 32 data bytes, Press Ctrl_C to break
From 219.246.3.3: bytes=32 seq=1 ttl=128 time=47 ms
From 219.246.3.3: bytes=32 seq=2 ttl=128 time=31 ms
From 219.246.3.3: bytes=32 seq=3 ttl=128 time=31 ms
From 219.246.3.3: bytes=32 seq=4 ttl=128 time=47 ms
From 219.246.3.3: bytes=32 seq=5 ttl=128 time=31 ms

--- 219.246.3.3 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 31/37/47 ms

PC>
```

### 三、实验内容

#### 基本访问控制列表实验：

实验 1：AR28-11 路由器的访问控制列表或者说防火墙的缺省过滤方式是允许通过还是禁止通过？

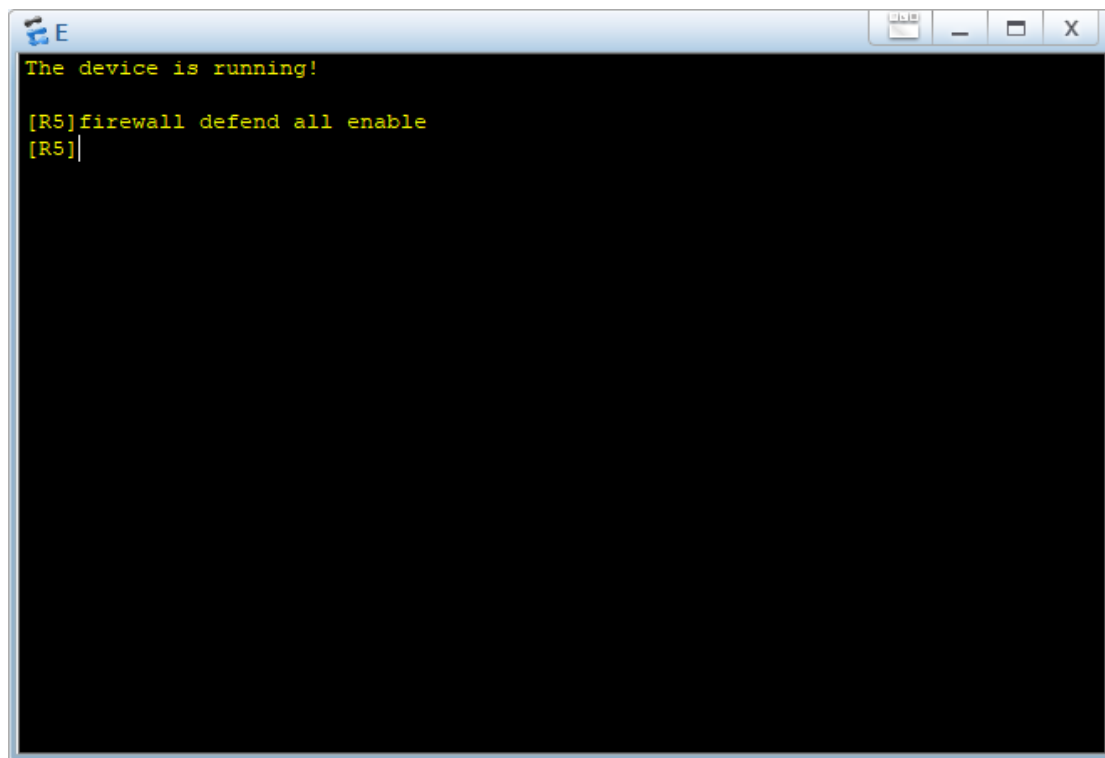
实验 2：禁止特定主机 PC3 访问 PC5 所在网络内的主机。

实验 3：禁止特定网络 219.246.3.0/24(即 PC3 所在的网络)内的主机访问 PC5 所在网络内的主机。

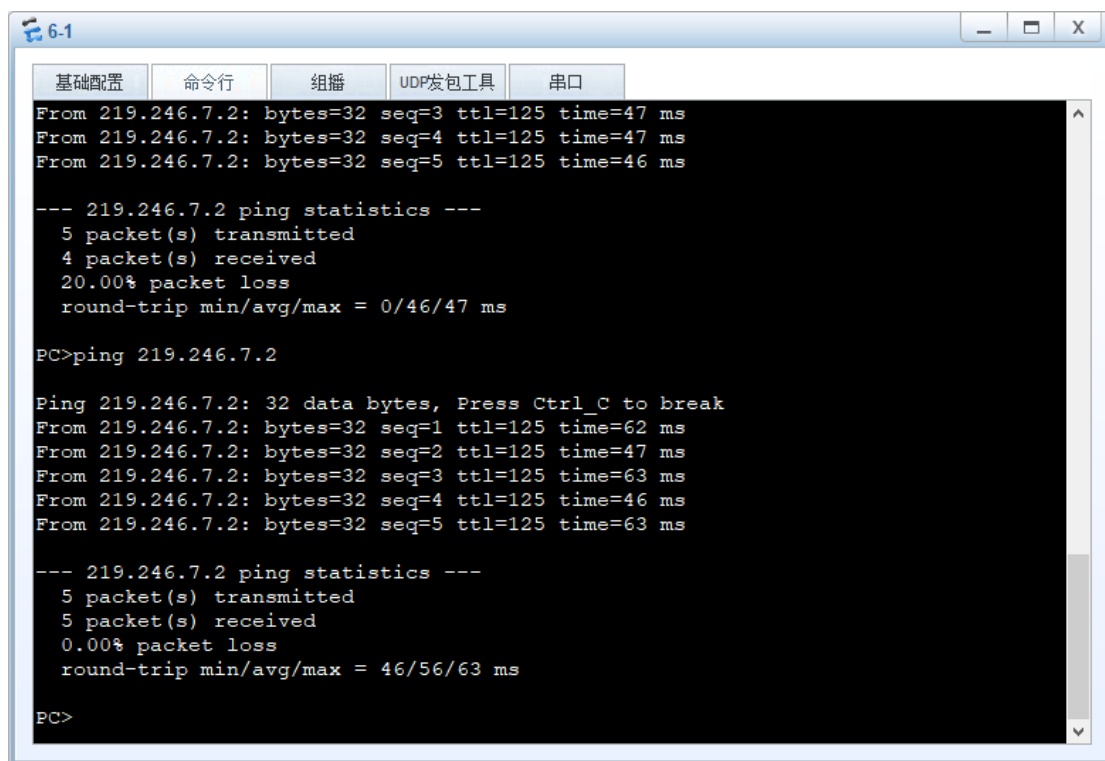
实验 1 步骤：

- 1) 启动路由器 E 的防火墙，不设置默认过滤方式。
- 2) 检验主机 6-1 和主机 6-5 能否访问。
- 3) 若能互相访问则说明缺省为允许，否则为禁止。

路由器 E 启动防火墙



主机 6-1 仍然可以通过路由器 E 访问主机 6-5



**结论：**防火墙的缺省过滤方式是允许通过。

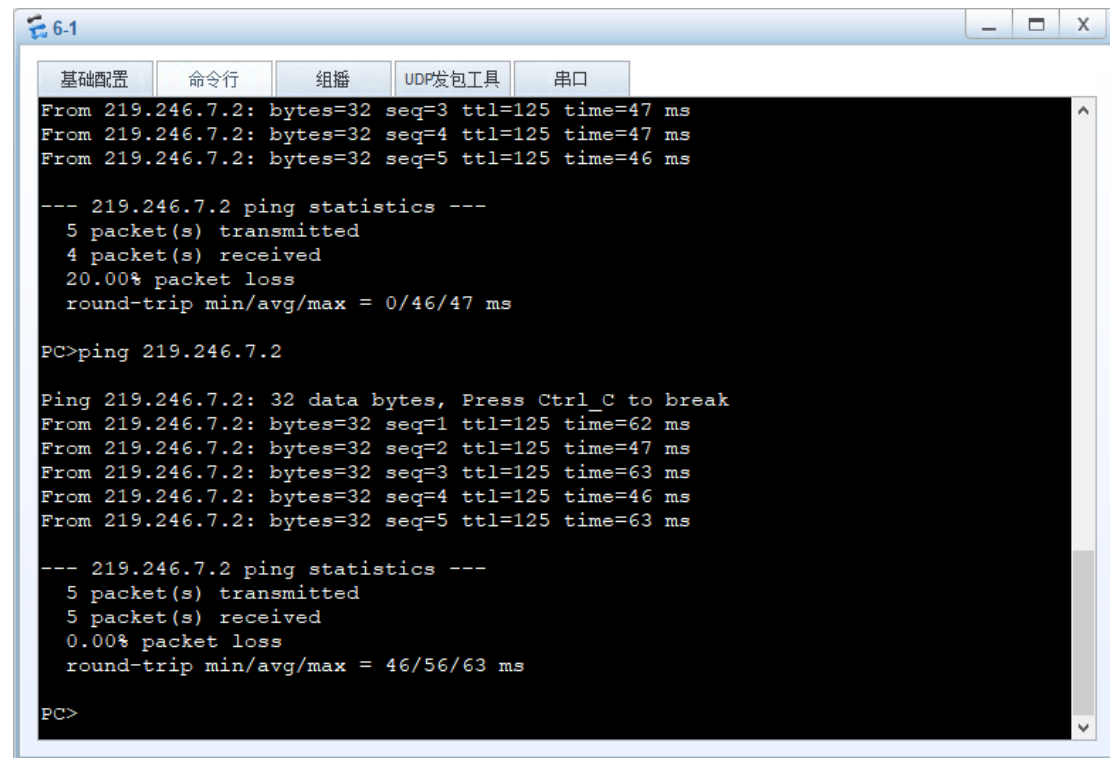
实验 2 步骤;

- 1) 设置访问控制列表之前查看其余主机能否访问主机 6-5
- 2) 设置正确的访问控制列表
- 3) 查看其余主机能否访问主机 6-5, 正确的实验结果应该是只有主机 6-3 无法访问主机 6-5

该实验中, 禁止特定主机 PC3 访问 PC5 所在网络内的主机, 因此直接对路由器 E 端口设置访问控制即可。

该实验中, 选择了对 E 的 e0 端进行设置。

实验前其余主机能够 ping 通主机 6-5, 其余主机截图不再展示



```
6-1
基础配置 命令行 组播 UDP发包工具 串口
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=46 ms

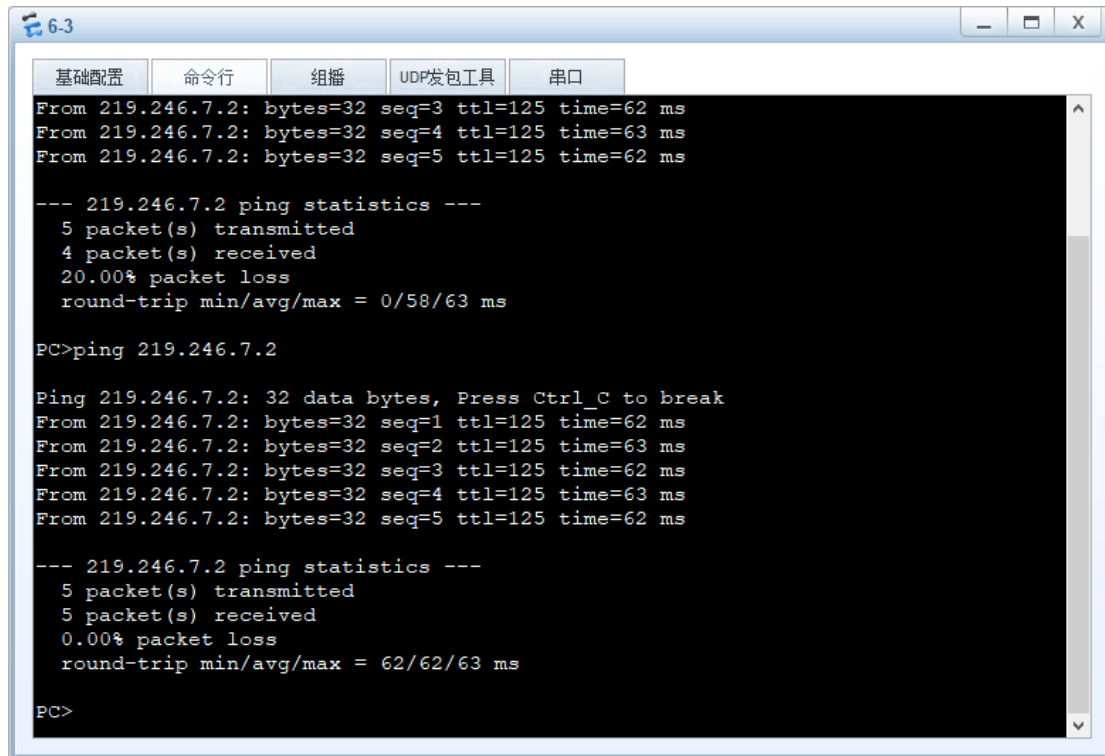
--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/46/47 ms

PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
From 219.246.7.2: bytes=32 seq=1 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=2 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=63 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=46 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=63 ms

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 46/56/63 ms

PC>
```



```
基础配置 命令行 组播 UDP发包工具 串口
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=63 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=62 ms

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/58/63 ms

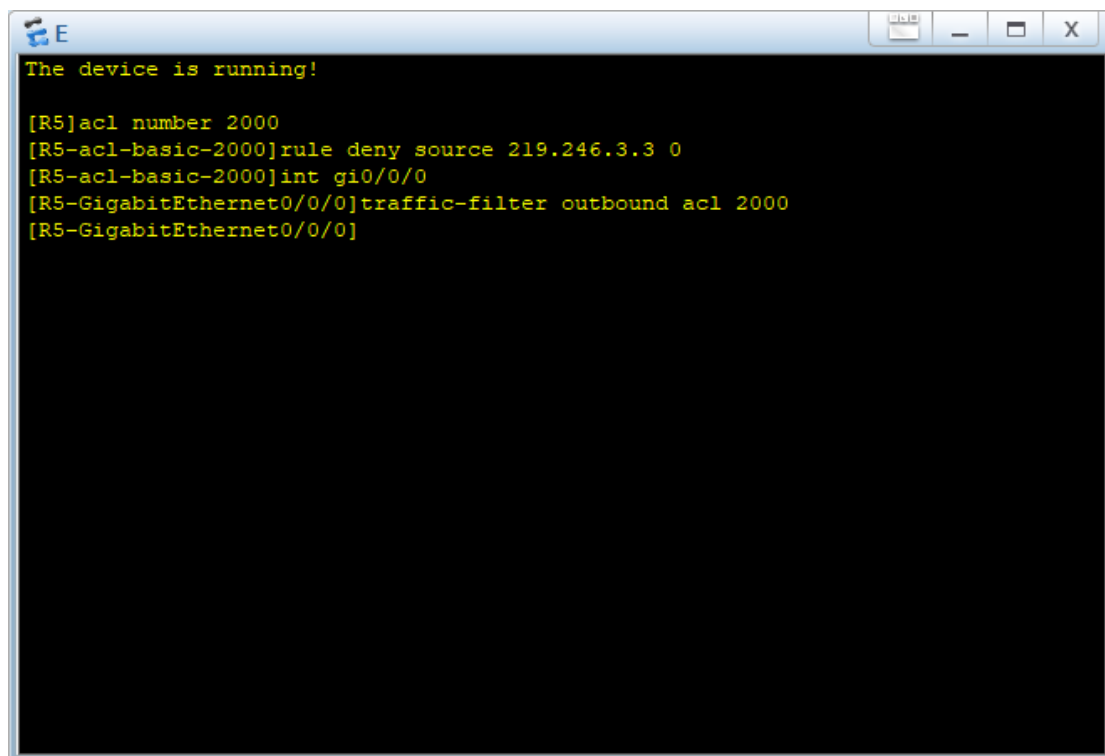
PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
From 219.246.7.2: bytes=32 seq=1 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=2 ttl=125 time=63 ms
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=63 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=62 ms

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 62/62/63 ms

PC>
```

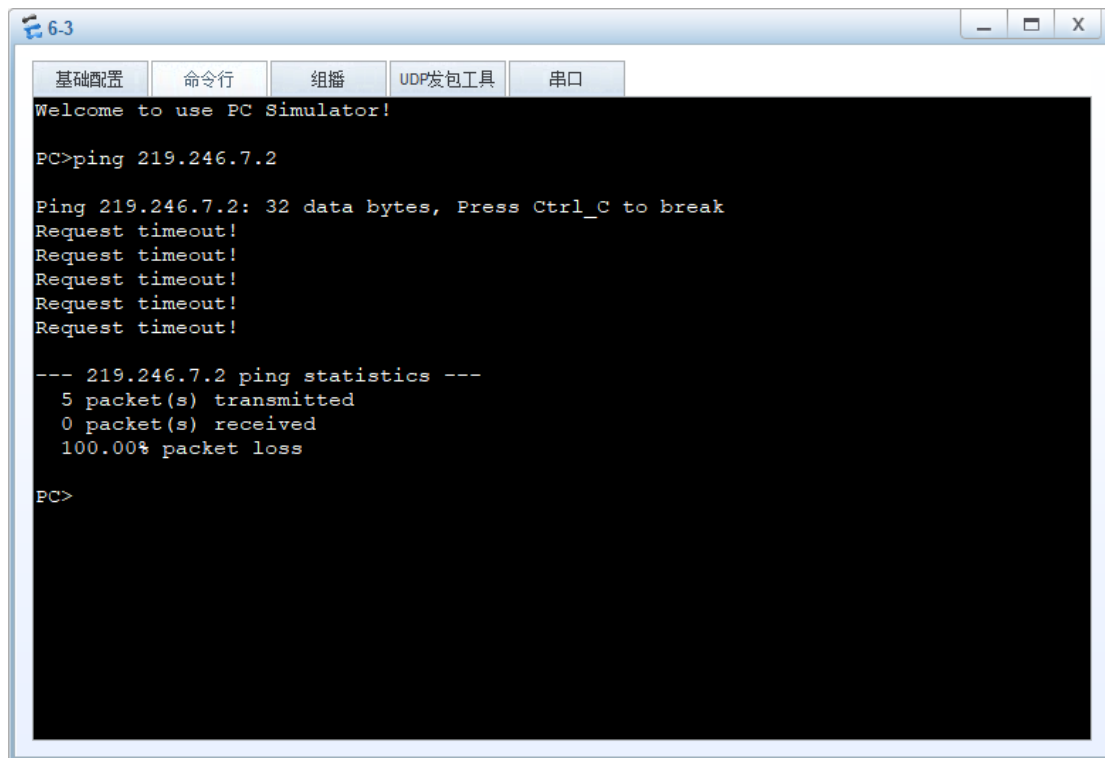
对路由器 E 的 e0 端口设置禁止发送主机 6-3 的数据包



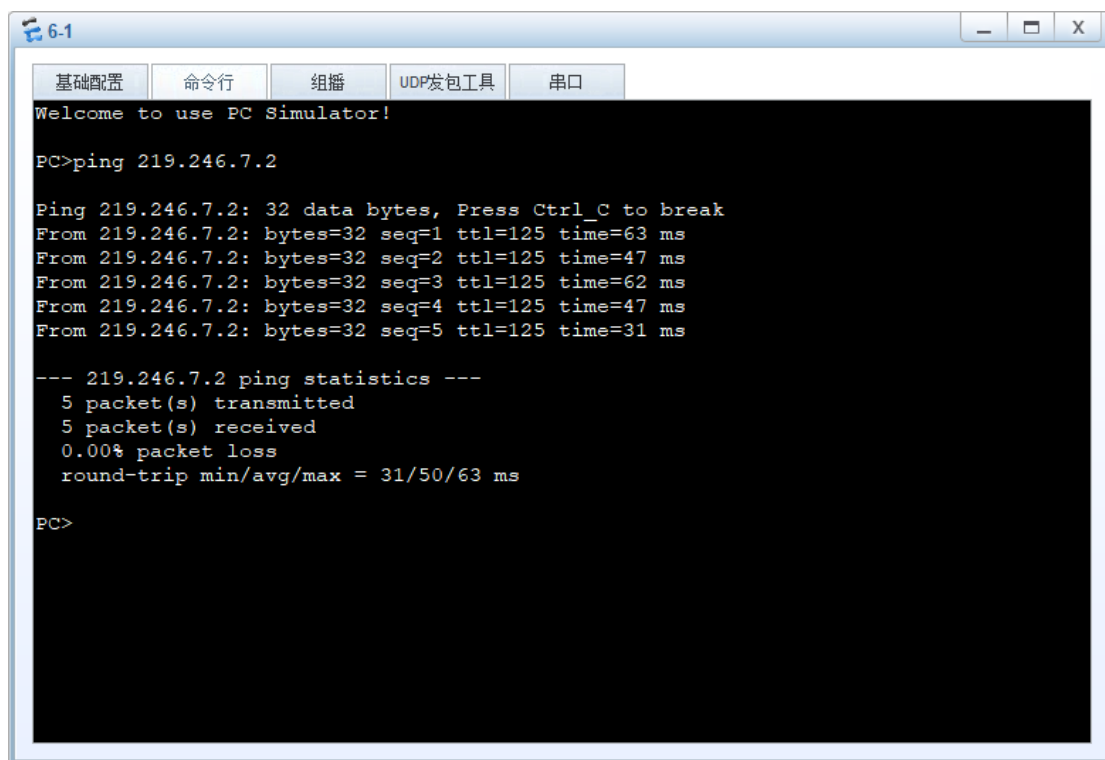
```
The device is running!

[R5]acl number 2000
[R5-acl-basic-2000]rule deny source 219.246.3.3 0
[R5-acl-basic-2000]int gi0/0/0
[R5-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
[R5-GigabitEthernet0/0/0]
```

设置完成后主机 6-3 访问失败



主机 6-3 访问失败的同时，利用主机 6-1 ping 主机 6-5，成功

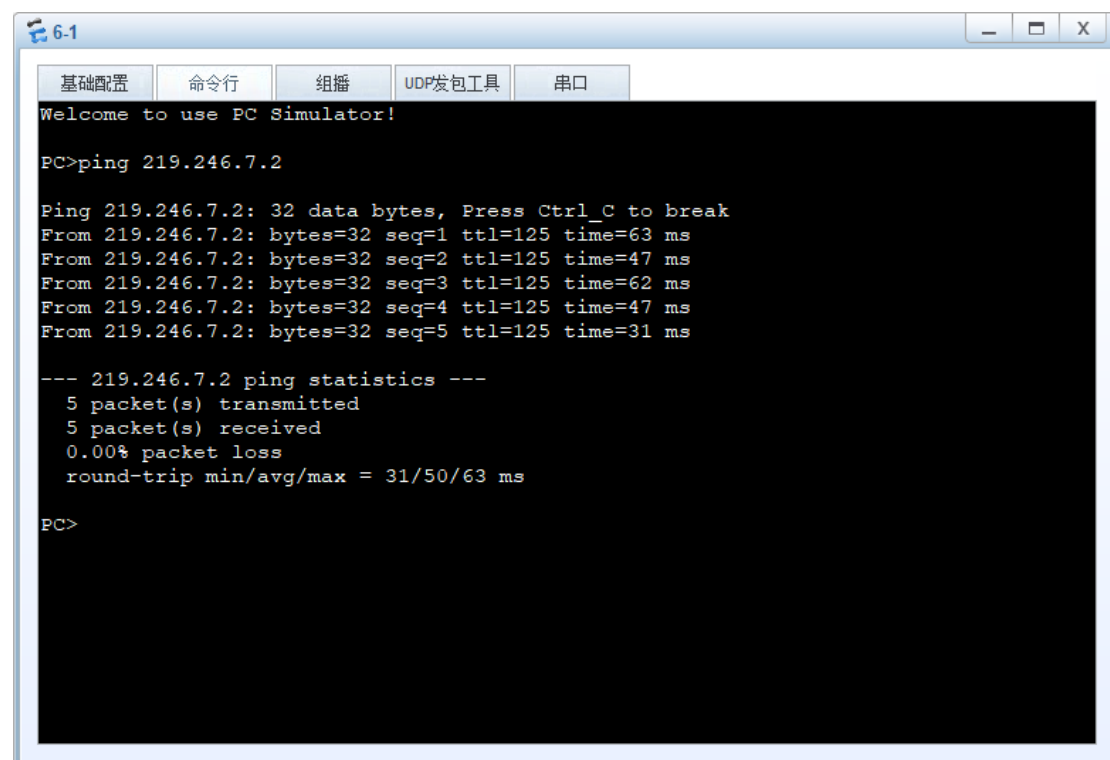


### 实验 3:

上一个实验中要求只屏蔽主机 6-3 的访问，因此源地址为主机 6-3 的 IP 地址，反子网掩码为 0.0.0.0。

在该实验中，根据本拓扑结构，主机 6-3 所在的网络是 219.246.3.0/24，因此需要的操作是计算出相应的反子网掩码，并且将该条规则添加进访问控制列表。具体操作如下：

实验前主机 6-1 可访问主机 6-5 所在网络



The screenshot shows a window titled "6-1" with tabs for "基础配置", "命令行", "组播", "UDP发包工具", and "串口". The "命令行" tab is active, displaying a terminal session. The user enters the command "ping 219.246.7.2". The output shows five successful ping attempts with varying round-trip times (63ms, 47ms, 62ms, 47ms, 31ms). The statistics section indicates 5 packets transmitted, 5 received, and 0.00% packet loss.

```
Welcome to use PC Simulator!

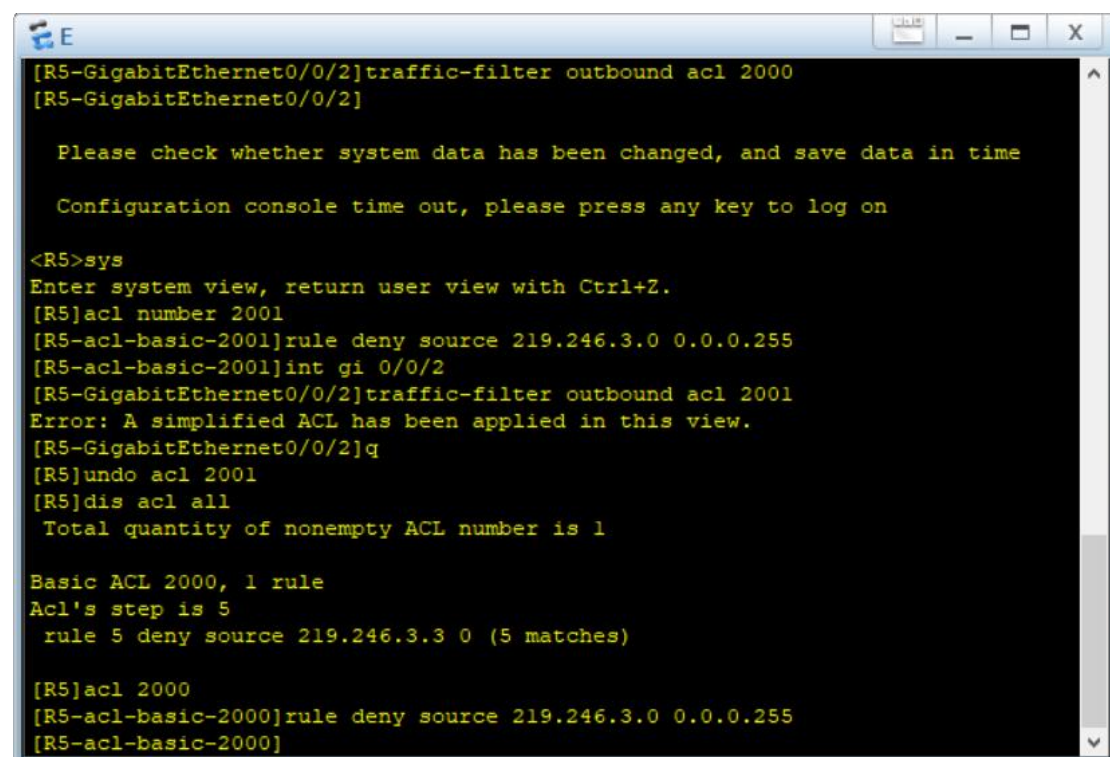
PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
From 219.246.7.2: bytes=32 seq=1 ttl=125 time=63 ms
From 219.246.7.2: bytes=32 seq=2 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=31 ms

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/50/63 ms

PC>
```

添加访问规则



The screenshot shows a network device configuration window titled "E". The user is in the configuration mode of the GigabitEthernet0/0/2 interface. They attempt to apply an outbound traffic filter with ACL 2001, but receive an error: "Error: A simplified ACL has been applied in this view." They then undo the ACL configuration and display the current ACL configuration, showing that ACL 2000 is already applied with one rule denying traffic from 219.246.3.0/24.

```
[R5-GigabitEthernet0/0/2]traffic-filter outbound acl 2000
[R5-GigabitEthernet0/0/2]

Please check whether system data has been changed, and save data in time

Configuration console time out, please press any key to log on

<R5>sys
Enter system view, return user view with Ctrl+Z.
[R5]acl number 2001
[R5-acl-basic-2001]rule deny source 219.246.3.0 0.0.0.255
[R5-acl-basic-2001]int gi 0/0/2
[R5-GigabitEthernet0/0/2]traffic-filter outbound acl 2001
Error: A simplified ACL has been applied in this view.
[R5-GigabitEthernet0/0/2]q
[R5]undo acl 2001
[R5]dis acl all
Total quantity of nonempty ACL number is 1

Basic ACL 2000, 1 rule
Acl's step is 5
rule 5 deny source 219.246.3.3 0 (5 matches)

[R5]acl 2000
[R5-acl-basic-2000]rule deny source 219.246.3.0 0.0.0.255
[R5-acl-basic-2000]
```

主机 6-3 所在网络无法访问



```
基础配置 命令行 组播 UDP发包工具 串口
From 219.246.7.2: bytes=32 seq=2 ttl=125 time=31 ms
From 219.246.7.2: bytes=32 seq=3 ttl=125 time=62 ms
From 219.246.7.2: bytes=32 seq=4 ttl=125 time=47 ms
From 219.246.7.2: bytes=32 seq=5 ttl=125 time=63 ms

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/50/63 ms

PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>|
```

## 四、实验总结

实验结果：

在老师的指导与小组成员的讨论下，我们完成了对于基本访问控制列表的使用操作。知道了华为路由器的防火墙的缺省过滤方式是允许通过。也完成了使主机 PC3 不能访问 PC5 所在网络内的主机以及 PC3 所在网络内的主机不能访问 PC5 所在网络内的主机的 ACL 的设计。

心得体会：通过本次实验，我们对于访问控制列表有了基本的了解，知道了它是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以通过，哪些数据包需要拒绝。另外，制作 ACL 时如果要限制本地计算机访问外部网络就用 OUT，如果是限制外部网络访问本地计算机就用 IN。

通过本实验，我们发现基本访问控制列表的实际应用有：

- 1) 阻止某个主机访问某个网段；
- 2) 阻止某个网段访问另一个网段。