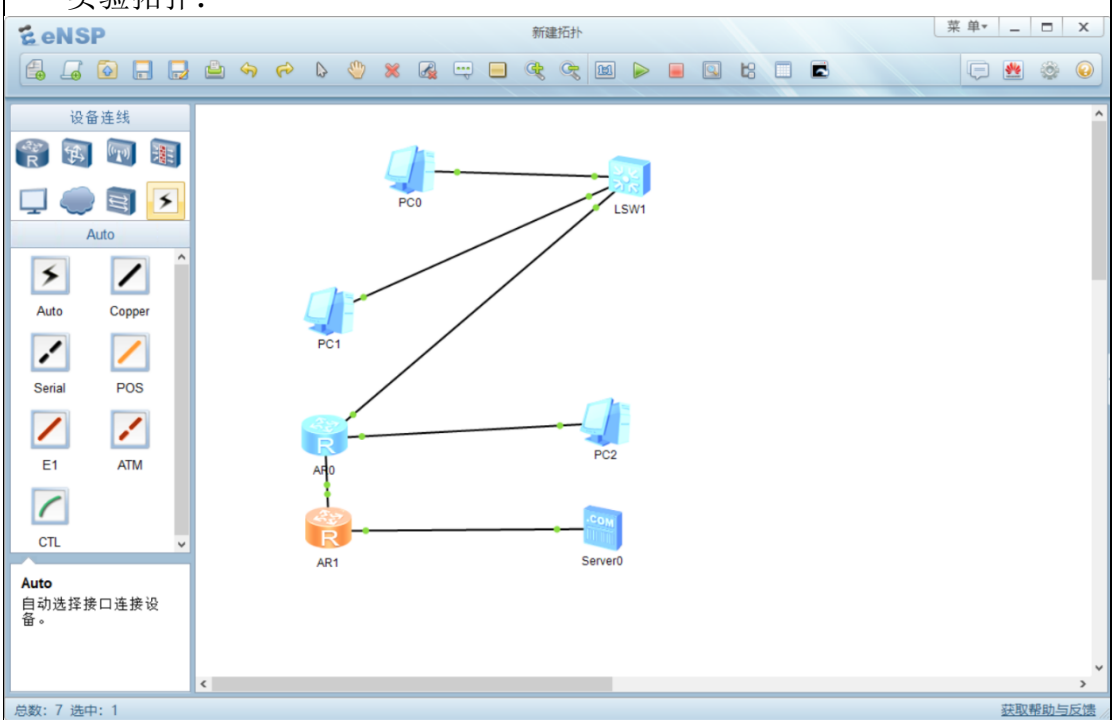


实验名称：ACL 网络访问控制	
实验台号：	实验时间：
实验小组：张楷	
<p>实验目的：</p> <ul style="list-style-type: none">•理解基本和扩展访问控制列表应用场景；•掌握标准访问控制列表的配置方法；•掌握扩展访问控制列表的配置方法；•掌握基于名称的访问列表的配置方法。	
<p>实验环境说明：装有 eNSP 的 PC</p> <p>实验拓扑：</p>  <p>图 1 实验拓扑</p>	

实验过程、步骤（可另附页、使用网络拓扑图等辅助说明）及结果：

一、基本配置

- 1) 根据实验编制对各设备进行相应的配置。然后使用 ping 命令检测各直连链路的连通性。

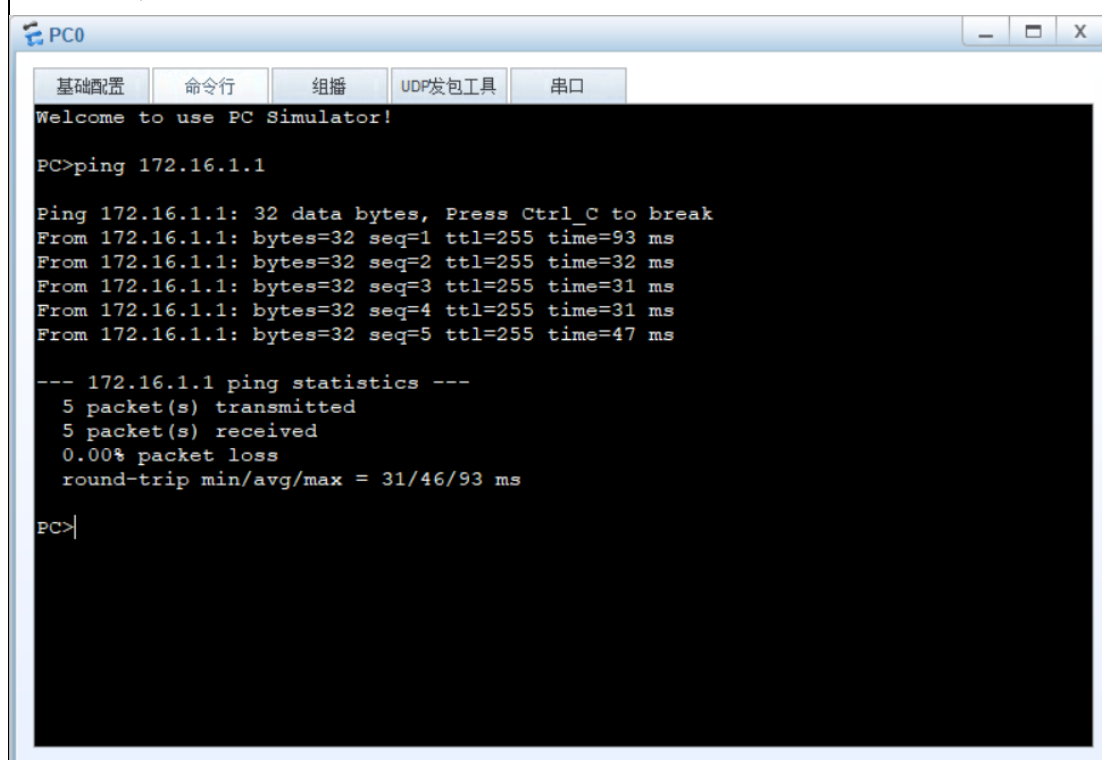


图 2PC0 和 R0 连通性测试

- 2) 在 AR1 和 AR0 上配置 OSPF 协议。

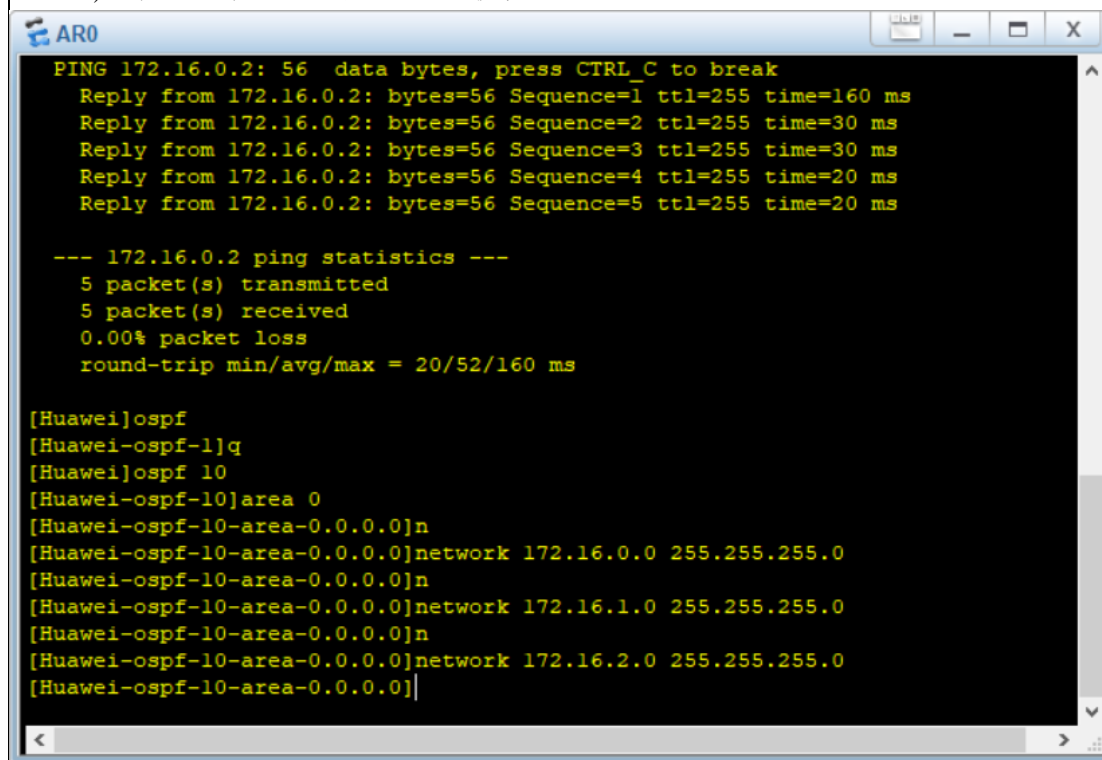
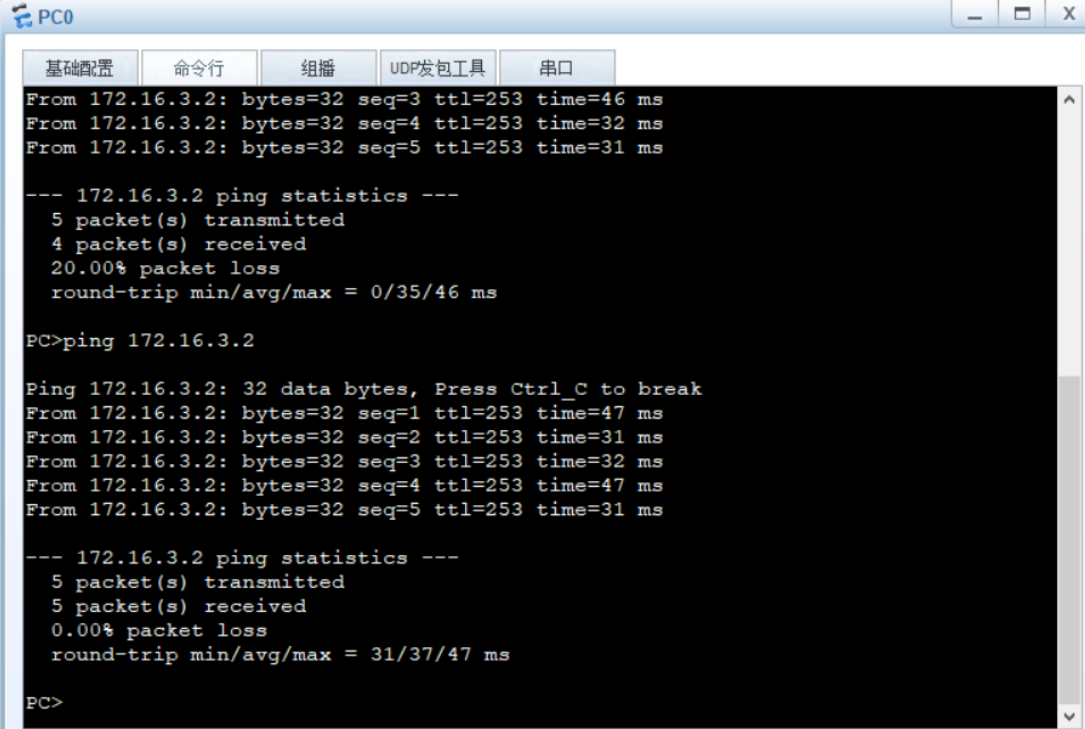


图 3AR0 的 OSPF 协议设置

3) 检测 PC0 和服务器 Server0 之间的连通性，发现可连通。



```
PC0
基础配置 命令行 组播 UDP发包工具 串口
From 172.16.3.2: bytes=32 seq=3 ttl=253 time=46 ms
From 172.16.3.2: bytes=32 seq=4 ttl=253 time=32 ms
From 172.16.3.2: bytes=32 seq=5 ttl=253 time=31 ms

--- 172.16.3.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/35/46 ms

PC>ping 172.16.3.2

Ping 172.16.3.2: 32 data bytes, Press Ctrl_C to break
From 172.16.3.2: bytes=32 seq=1 ttl=253 time=47 ms
From 172.16.3.2: bytes=32 seq=2 ttl=253 time=31 ms
From 172.16.3.2: bytes=32 seq=3 ttl=253 time=32 ms
From 172.16.3.2: bytes=32 seq=4 ttl=253 time=47 ms
From 172.16.3.2: bytes=32 seq=5 ttl=253 time=31 ms

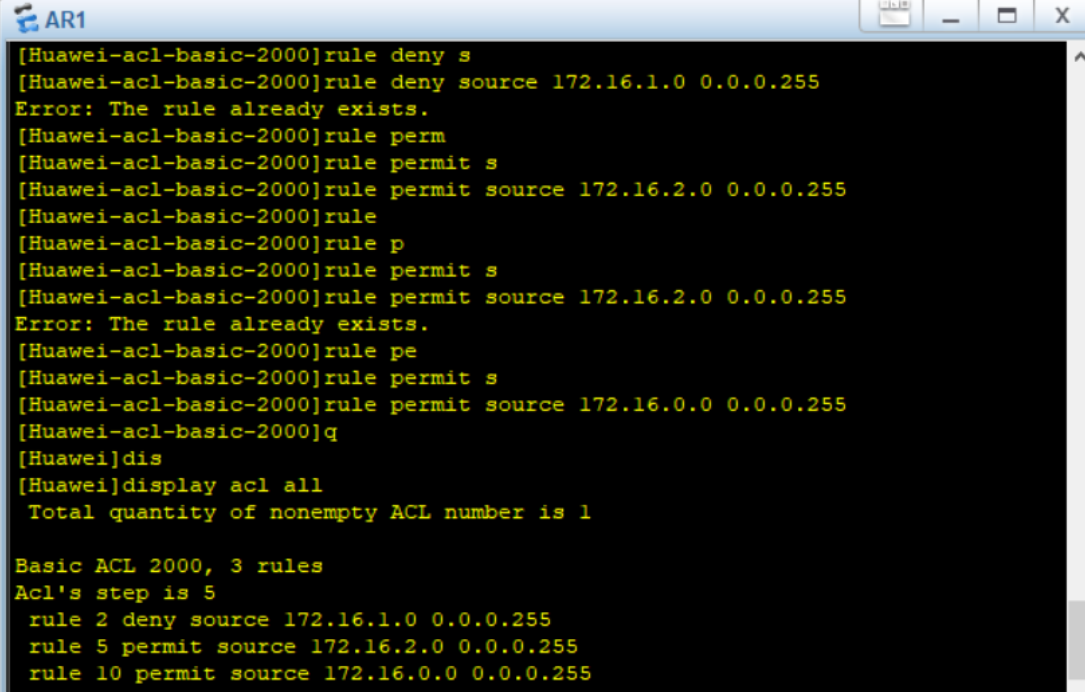
--- 172.16.3.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/37/47 ms

PC>
```

图 4 连通性检测

二、基本 ACL 配置

1) 在路由器 AR1 配置 ACL 允许 172.16.2.0/24 网段，禁止 172.16.1.0/24 主机访问 172.16.3.0/24 子网，并查看 AR1 的 ACL 配置。在端口 GigabitEthernet0/0/0 处使用 traffic-filter inbound acl 2000 命令，在该端口上调用。

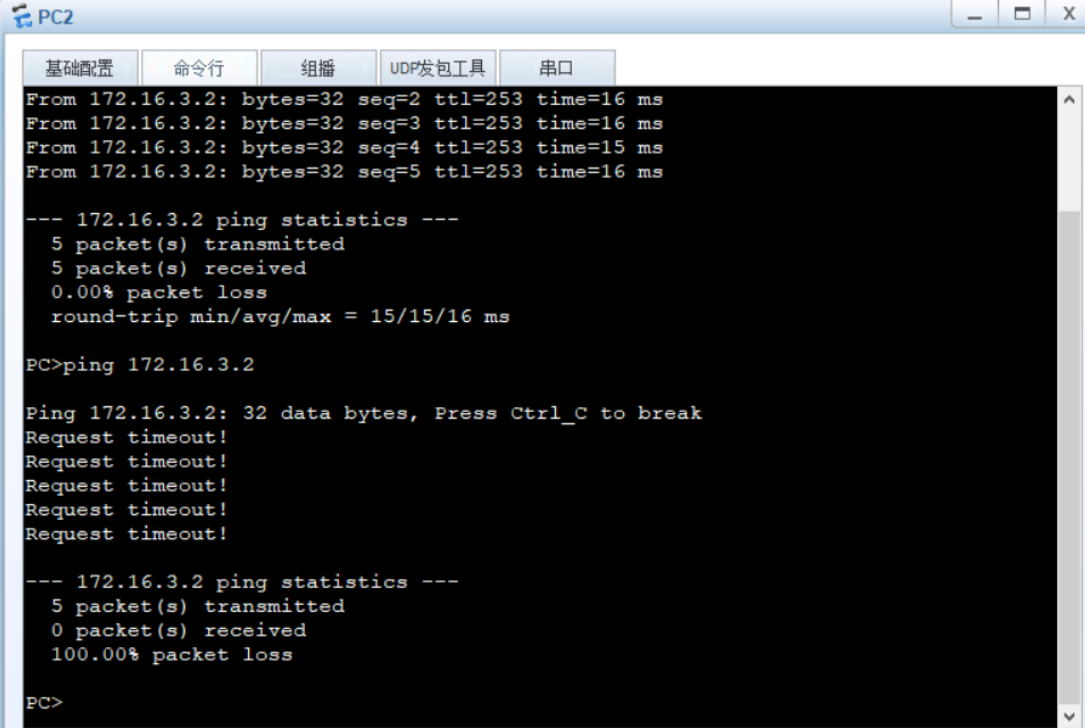


```
AR1
[Huawei-acl-basic-2000]rule deny s
[Huawei-acl-basic-2000]rule deny source 172.16.1.0 0.0.0.255
Error: The rule already exists.
[Huawei-acl-basic-2000]rule perm
[Huawei-acl-basic-2000]rule permit s
[Huawei-acl-basic-2000]rule permit source 172.16.2.0 0.0.0.255
[Huawei-acl-basic-2000]rule
[Huawei-acl-basic-2000]rule p
[Huawei-acl-basic-2000]rule permit s
[Huawei-acl-basic-2000]rule permit source 172.16.2.0 0.0.0.255
Error: The rule already exists.
[Huawei-acl-basic-2000]rule pe
[Huawei-acl-basic-2000]rule permit s
[Huawei-acl-basic-2000]rule permit source 172.16.0.0 0.0.0.255
[Huawei-acl-basic-2000]q
[Huawei]dis
[Huawei]display acl all
Total quantity of nonempty ACL number is 1

Basic ACL 2000, 3 rules
Acl's step is 5
rule 2 deny source 172.16.1.0 0.0.0.255
rule 5 permit source 172.16.2.0 0.0.0.255
rule 10 permit source 172.16.0.0 0.0.0.255
```

图 5AR1 的 ACL 配置

2) 检查 PC2 与服务器的连通, 发现连不通。



```
PC2
基础配置 命令行 组播 UDP发包工具 串口
From 172.16.3.2: bytes=32 seq=2 ttl=253 time=16 ms
From 172.16.3.2: bytes=32 seq=3 ttl=253 time=16 ms
From 172.16.3.2: bytes=32 seq=4 ttl=253 time=15 ms
From 172.16.3.2: bytes=32 seq=5 ttl=253 time=16 ms

--- 172.16.3.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 15/15/16 ms

PC>ping 172.16.3.2

Ping 172.16.3.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

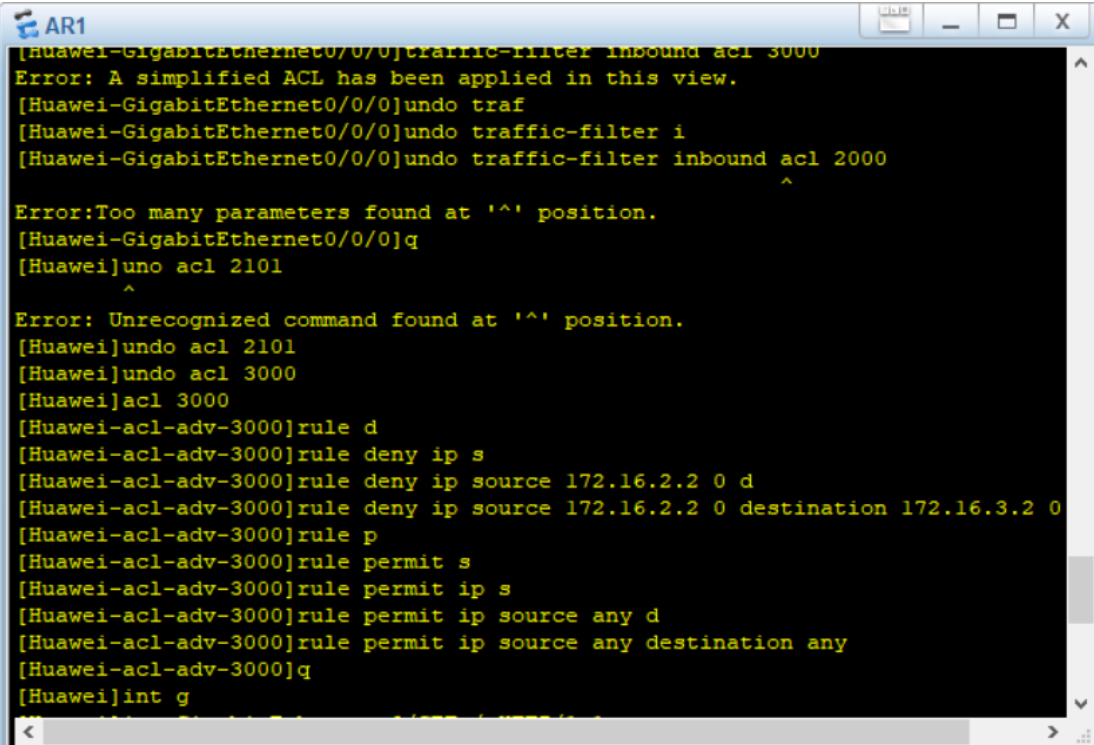
--- 172.16.3.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
```

图 6 连通性测试

三、扩展 ACL 配置。

扩展 ACL 配置, 禁止主机 PC0 访问服务器。

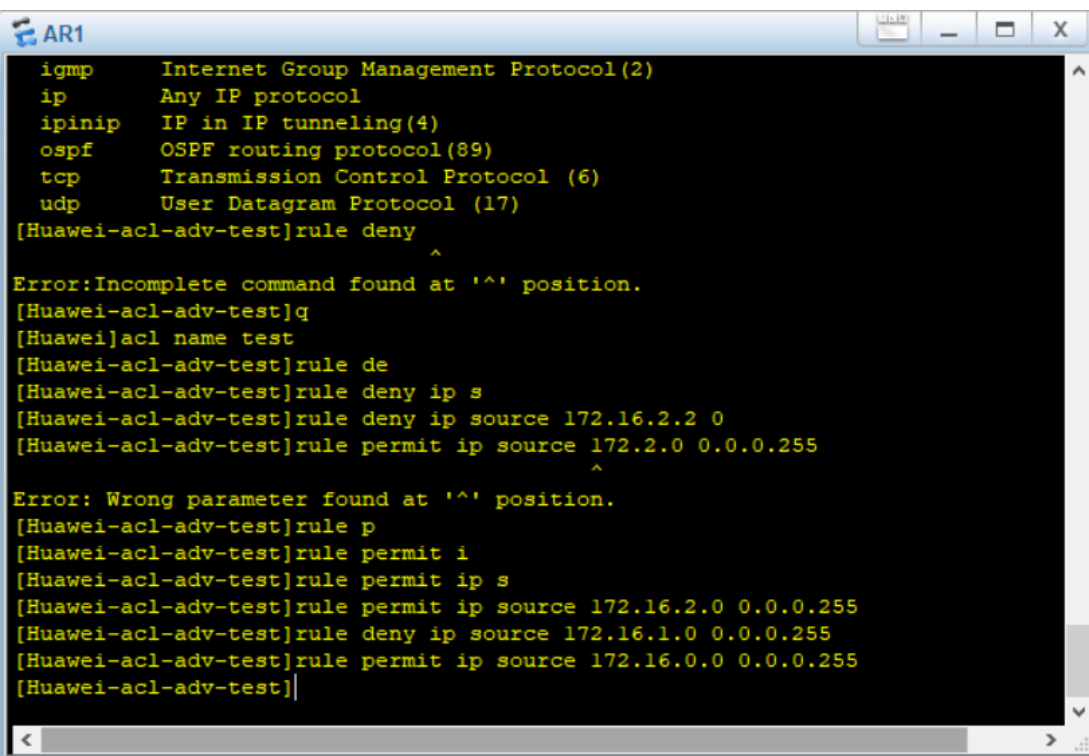


```
AR1
[Huawei-GigabitEthernet0/0/0]traffic-filter inbound acl 3000
Error: A simplified ACL has been applied in this view.
[Huawei-GigabitEthernet0/0/0]undo traf
[Huawei-GigabitEthernet0/0/0]undo traffic-filter i
[Huawei-GigabitEthernet0/0/0]undo traffic-filter inbound acl 2000
Error:Too many parameters found at '^' position.
[Huawei-GigabitEthernet0/0/0]q
[Huawei]uno acl 2101
Error: Unrecognized command found at '^' position.
[Huawei]undo acl 2101
[Huawei]undo acl 3000
[Huawei]acl 3000
[Huawei-acl-adv-3000]rule d
[Huawei-acl-adv-3000]rule deny ip s
[Huawei-acl-adv-3000]rule deny ip source 172.16.2.2 0 d
[Huawei-acl-adv-3000]rule deny ip source 172.16.2.2 0 destination 172.16.3.2 0
[Huawei-acl-adv-3000]rule p
[Huawei-acl-adv-3000]rule permit s
[Huawei-acl-adv-3000]rule permit ip s
[Huawei-acl-adv-3000]rule permit ip source any d
[Huawei-acl-adv-3000]rule permit ip source any destination any
[Huawei-acl-adv-3000]q
[Huawei]int g
```

图 7 扩展 ACL 配置

四、基于名称的访问控制列表的使用方法。

- 1) 设置名称为 test 的 ACL。



```
AR1
igmp      Internet Group Management Protocol(2)
ip        Any IP protocol
ipinip    IP in IP tunneling(4)
ospf      OSPF routing protocol(89)
tcp       Transmission Control Protocol (6)
udp       User Datagram Protocol (17)
[Huawei-acl-adv-test]rule deny
^
Error:Incomplete command found at '^' position.
[Huawei-acl-adv-test]q
[Huawei]acl name test
[Huawei-acl-adv-test]rule de
[Huawei-acl-adv-test]rule deny ip s
[Huawei-acl-adv-test]rule deny ip source 172.16.2.2 0
[Huawei-acl-adv-test]rule permit ip source 172.2.0 0.0.0.255
^
Error: Wrong parameter found at '^' position.
[Huawei-acl-adv-test]rule p
[Huawei-acl-adv-test]rule permit i
[Huawei-acl-adv-test]rule permit ip s
[Huawei-acl-adv-test]rule permit ip source 172.16.2.0 0.0.0.255
[Huawei-acl-adv-test]rule deny ip source 172.16.1.0 0.0.0.255
[Huawei-acl-adv-test]rule permit ip source 172.16.0.0 0.0.0.255
[Huawei-acl-adv-test]|
```

图 8 名称为 test 的 ACL

实验总结（遇到的问题及解决办法、体会）：
明白了 ACL 的用法，很有收获

器材、工具领用及归还负责人： 张楷

实验记录人：（签名）张楷

实验执笔人：（签名）张楷

报告协助人：（签名）张楷

小组成员签名：（签名）张楷

验收人：

成绩评定：