作者：豆豆老师

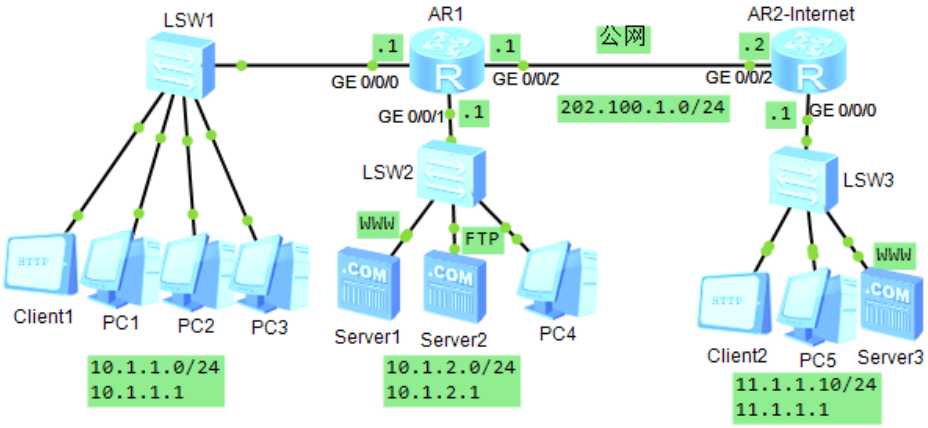
实验 15　配置基本 ACL 和高级 ACL

实验目的

- ✧ 掌握基本 ACL 的配置方法
- ✧ 掌握高级 ACL 的配置方法
- ✧ 掌握 ACL 在接口下的应用方法

实验步骤

1 使用 eNSP 搭建如下拓扑图



2 基本配置（接口 IP、设备主机名等）

3 在 AR1 和 AR2 上配置静态路由，实现全网互通

4 在 R1 上配置基本 ACL，实现如下需求：

- ✧ 10.1.1.0 网络内的主机在上班时间（9：00-17：00）不能访问公网
- ✧ 10.1.2.0 网络内只有 Server1（10.1.2.100）不能访问公网外

5 在 R1 上配置高级 ACL，实现如下需求：

- ✧ 10.1.1.0 网络内的主机只能通过 HTTP 访问公网
- ✧ 10.1.1.0 网络内的主机不能 ping 10.1.2.0 网络内的 FTP 服务器（Server2：10.1.2.200）

实验总结

作者：豆豆老师

实验配置详解

1 使用 eNSP 搭建拓扑图

2 基本配置（接口 IP、设备主机名等）

3 在 AR1 和 AR2 上配置静态路由，实现全网互通

[AR1]ip route-static 0.0.0.0 0.0.0.0 202.100.1.2

[AR2]ip route-static 0.0.0.0 0.0.0.0 202.100.1.1

测试：各个网络内的主机互 ping，保证全网互通

4 在 R1 上配置基本 ACL，实现如下需求：

- ✧ 10.1.1.0 网络内的主机在上班时间（9：00-17：00）不能访问公网
- ✧ 10.1.2.0 网络内只有 Server1（10.1.2.100）不能访问公网外

[AR1]time-range WORK 9:00 to 17:00 working-day

[AR1]acl 2000

[AR1-acl-basic-2000]rule deny source 10.1.1.0 0.0.0.255 time-range WORK

[AR1-acl-basic-2000]rule deny source 10.1.2.100 0.0.0.0

[AR1-acl-basic-2000]rule permit source 10.1.2.0 0.0.0.255

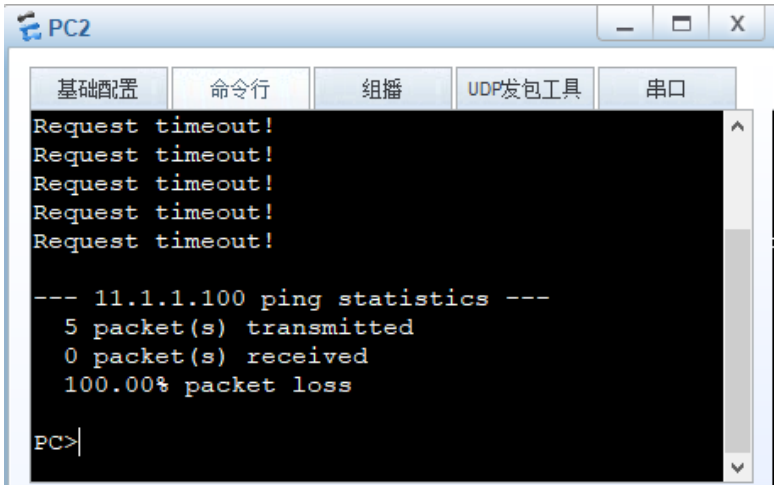
[AR1-acl-basic-2000]quit

[AR1]interface GigabitEthernet 0/0/2

[AR1-GigabitEthernet0/0/2]traffic-filter outbound acl 2000

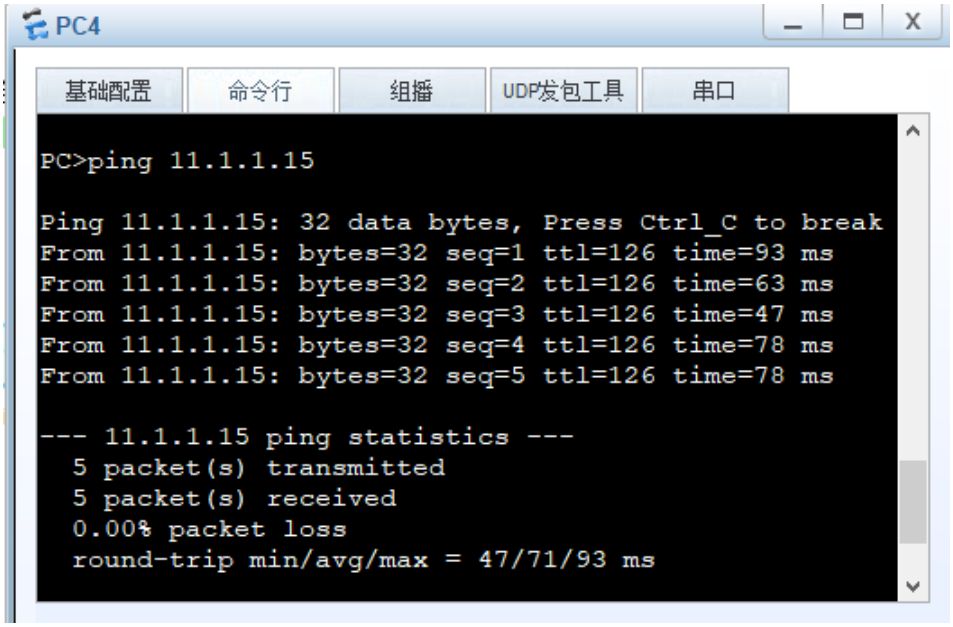
[AR1-GigabitEthernet0/0/2]quit

测试：10.1.1.0/24 和 10.1.2.0/24 网段内的主机访问 11.1.1.0/24



作者：豆豆老师





查看：

```
[AR1]display acl all
 Total quantity of nonempty ACL number is 1

Basic ACL 2000, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255 time-range WORK(Active) (15 matches)
 rule 10 deny source 10.1.2.100 0 (8 matches)
 rule 15 permit source 10.1.2.0 0.0.0.255 (15 matches)
```

作者：豆豆老师

继续测试:在路由器上修改时间为周末,然后测试 10.1.1.0 网络内的主机可否访问 11.1.1.0/24

<AR1>clock datetime 12:00 2020-03-28

```
[AR1]display acl all
 Total quantity of nonempty ACL number is 1

Basic ACL 2000, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255 time-range WORK(Inactive)
 rule 10 deny source 10.1.2.100 0
 rule 15 permit source 10.1.2.0 0.0.0.255
```

5 在 R1 上配置高级 ACL，实现如下需求：

- 10.1.1.0 网络内的主机只能通过 HTTP 访问公网
- 10.1.1.0 网络内的主机不能 ping 10.1.2.0 网络内的 FTP 服务器（Server2：10.1.2.200）

首先要在 AR1 上清除基本 ACL 配置，具体命令如下：

[AR1]interface GigabitEthernet 0/0/2

[AR1-GigabitEthernet0/0/2]undo traffic-filter outbound

[AR1-GigabitEthernet0/0/2]quit

[AR1]undo acl 2000

[AR1]acl 3000

[AR1-acl-adv-3000] rule deny icmp source 10.1.1.0 0.0.0.255 destination 10.1.2.200 0.0.0.0

[AR1-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.1.2.0 0.0.0.255

[AR1-acl-adv-3000] rule permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www

[AR1-acl-adv-3000] rule deny ip

[AR1-acl-adv-3000] quit

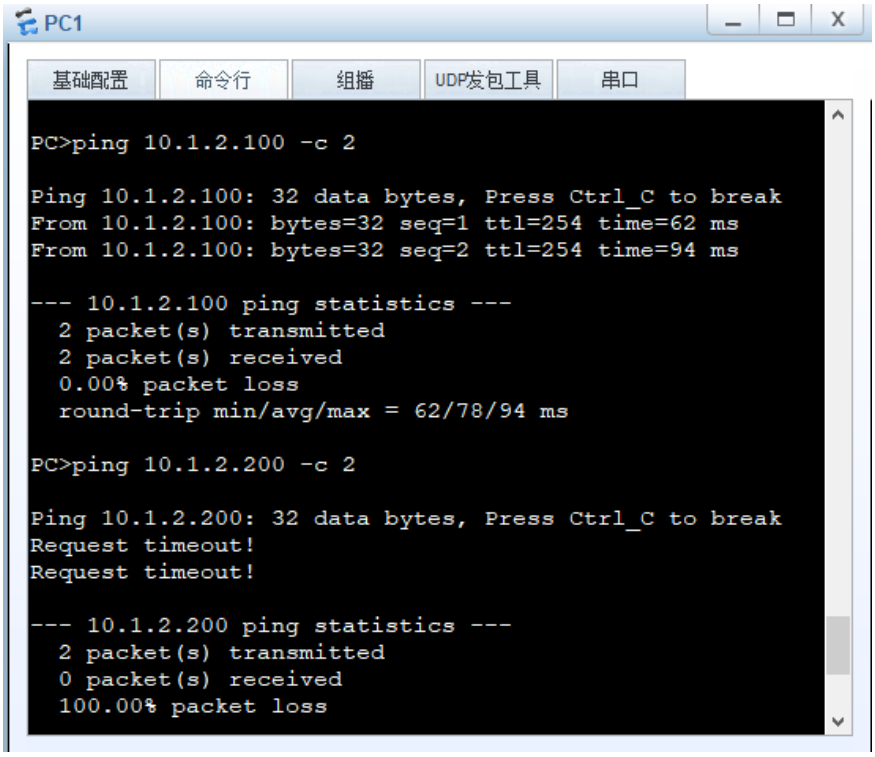
[AR1]interface GigabitEthernet 0/0/0

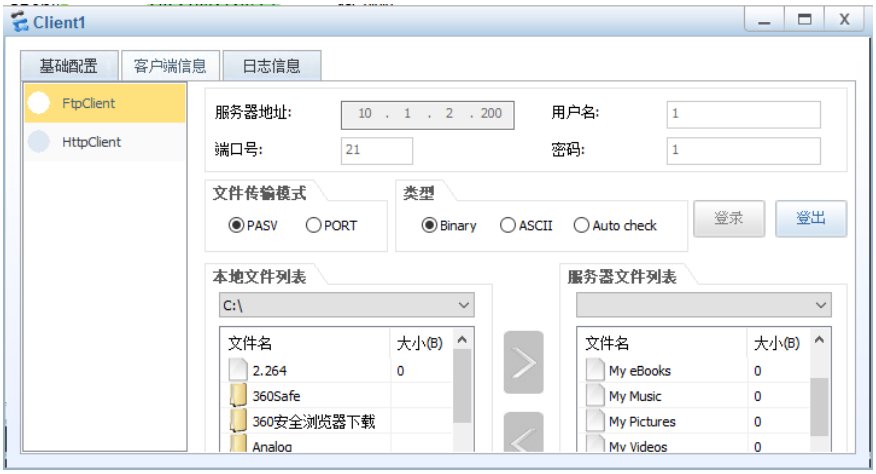
[AR1-GigabitEthernet0/0/0]traffic-filter inbound acl 3000

[AR1-GigabitEthernet0/0/0]quit

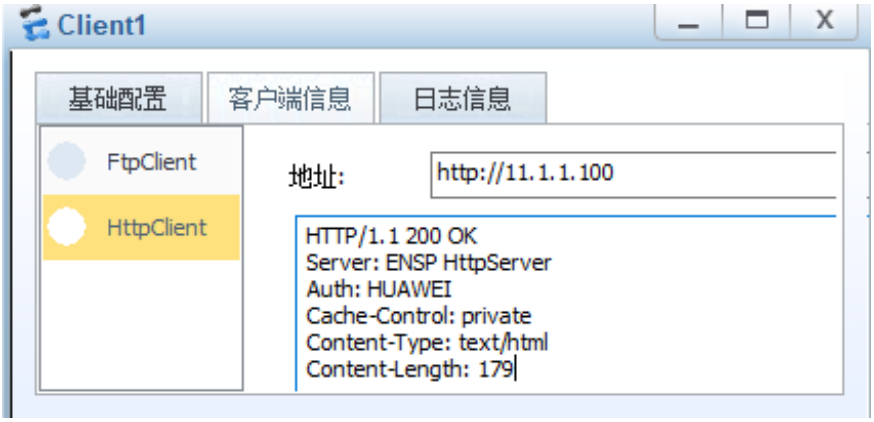
作者：豆豆老师

测试：10.1.1.0 /24 -> 10.1.2.0/24

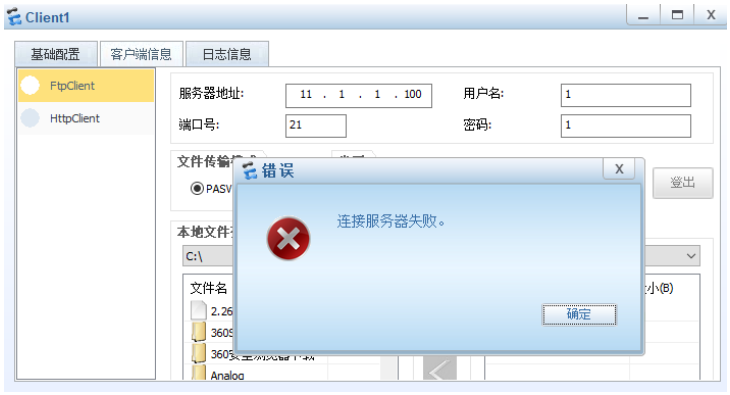


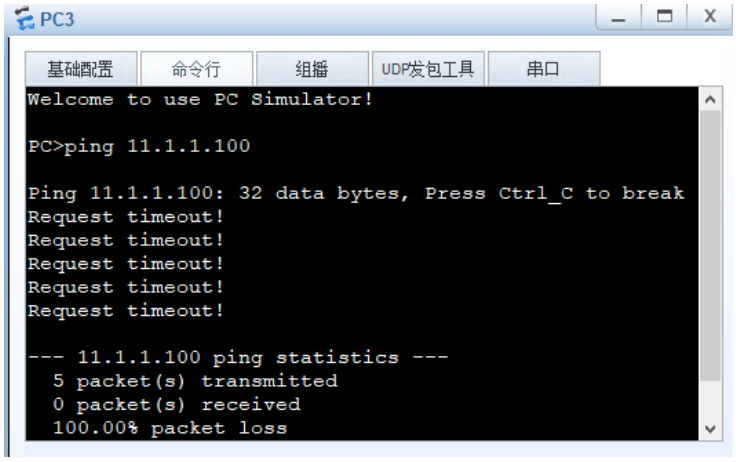


10.1.1.0-> 11.1.1.0/24



作者：豆豆老师





查看：

```
[AR1]display acl 3000
Advanced ACL 3000, 4 rules
Acl's step is 5
 rule 5 deny icmp source 10.1.1.0 0.0.0.255 destination 10.1.2.200 0 (2 matches)

 rule 10 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 (28
matches)
 rule 15 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www (11 matche
s)
 rule 20 deny ip (280 matches)
```

重要知识点

ACL (Access Control List)

功能： 1）包过滤—实现安全功能　　2）流量匹配---NAT/路由策略/QoS…..

分类： 1) 基本 ACL　2)高级 ACL　3)二层 ACL

ACL: 由一系列的规则组成，每条规则都包含条件和动作

基本 ACL：只能根据源 IP 地址制定规则，不能精确匹配流量

高级 ACL: 可以根据五元组（源 IP 地址、目的 IP 地址、源端口、目标端口、协议 ）制定规则，可以实现精确匹配流量

注意事项：入站和出站应用