试验1：ACL 实验解析

实验需求：

1）全网EIGRP

2）在R2 上利用标准ACL使得只有源于10.1.1.0 可以通过

3）在R2上利用扩展ACL 使得只有源于11 去向3.3.3.3的流量可以通过

步骤1：完成基础配置

此时全网的通讯，无论源和目的都是畅通无阻

R1#ping 3.3.3.3 so 10.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/73/96 ms

R1#ping 3.3.3.3 so 11.11.11.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 11.11.11.11

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/67/88 ms

如上现象表明网络通讯没有任何阻碍

步骤2：在R2上完成标准ACL，实现需求2

R2

access-list 1 permit 10.1.1.0 0.0.0.255

access-list 1 permit host 12.12.12.1

!

interface fa 0/0

ip access-group 1 in

步骤3：完成扩展ACL

R2

access-list 100 permit ip 11.11.11.0 0.0.0.255 3.3.3.0 0.0.0.255

access-list 100 permit eigrp any any

!

int fa0/0

ip access-group 100 in

此时如上配置完成后，只有11可以pING通33，现象如下：

R1#ping 3.3.3.3 so 10.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.1

UUUUU

Success rate is 0 percent (0/5)

R1#ping 3.3.3.3 so 11.11.11.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 11.11.11.11

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/96 ms

R1#

！！补充

命名的ACL：允许管理员，针对某个具体条目进行编辑

编号的ACL