

一、环境准备

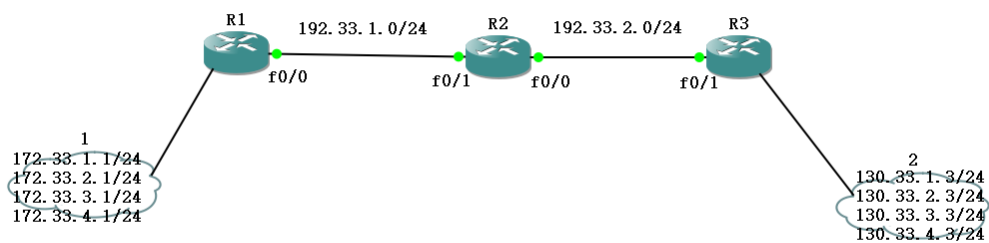
1. 软件：GNS3
2. 路由：c7200

二、实验操作

实验要求：

- 1、掌握标准 ACL、扩展 ACL 的配置方法。
- 2、掌握命名 ACL 的配置方法。
- 3、掌握访问控制列表配置中 `established` 参数的作用。
- 4、掌握在命名访问控制列表中插入一条规则或删除一条规则的方法。
- 5、掌握反射访问控制列表的工作原理和配置方法。
- 6、掌握动态 ACL 的原理和配置方法。

实验拓扑：



实验过程：

- 1、根据实验拓扑，对路由器各接口配置 IP 地址。注：对 loopback 接口配 IP 时每个 loopback 接口配一个 IP，即在 R1 和 R3 中各启用 4 个 loopback 接口（lo1-lo4）。

查看各个接口 IP 状态：

R1

```
R1#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.33.1.1      YES manual    up          up
FastEthernet0/1 unassigned      YES unset     administratively down down
Serial1/0       unassigned      YES unset     administratively down down
Serial1/1       unassigned      YES unset     administratively down down
Serial1/2       unassigned      YES unset     administratively down down
Serial1/3       unassigned      YES unset     administratively down down
SSLVPN-VIF0     unassigned      NO  unset     up          up
Loopback1       172.33.1.1      YES manual    up          up
Loopback2       172.33.2.1      YES manual    up          up
Loopback3       172.33.3.1      YES manual    up          up
Loopback4       172.33.4.1      YES manual    up          up
R1#
```

R2

```
R2#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.33.2.2      YES manual    up          up
FastEthernet0/1 192.33.1.2      YES manual    up          up
Serial1/0       unassigned      YES unset     administratively down down
Serial1/1       unassigned      YES unset     administratively down down
Serial1/2       unassigned      YES unset     administratively down down
Serial1/3       unassigned      YES unset     administratively down down
SSLVPN-VIF0     unassigned      NO  unset     up          up
Loopback1       unassigned      YES unset     up          up
R2#
```

R3

```
R3#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 unassigned      YES unset     administratively down down
FastEthernet0/1 192.33.2.3      YES manual    up          up
Serial1/0       unassigned      YES unset     administratively down down
Serial1/1       unassigned      YES unset     administratively down down
Serial1/2       unassigned      YES unset     administratively down down
Serial1/3       unassigned      YES unset     administratively down down
SSLVPN-VIF0     unassigned      NO  unset     up          up
Loopback1       130.33.1.3      YES manual    up          up
Loopback2       130.33.2.3      YES manual    up          up
Loopback3       130.33.3.3      YES manual    up          up
Loopback4       130.33.4.3      YES manual    up          up
R3#
```

2、在各路由器上配置 EIGRP 协议，关闭自动汇总，使整个网络连通。

3、配置标准访问控制列表，使 172.33.1.0/24 这个子网无法访问 R3 上的网络。

参考命令：

```
R2(config)#access-list 33 deny 172.33.1.0 0.0.0.255
```

```
R2(config)#access-list 33 permit any
```

```
R2(config)#interface f0/0
```

```
R2(config-if)#ip access-group 33 out
```

问题 1: 配置后在 R1 上直接 ping 130.33.1.3, 能否 ping 通? 为什么?

```
R1#ping 130.33.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.33.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/65/76 ms
R1#
```

答: 在 R1 上直接 ping 130.33.1.3, 能 ping 通。因为在 R2 上没有限制 192.33.1.0 网络。

问题 2: 使用扩展 ping, 用 172.33.1.1 做源地址, 能否 ping 通?

```
R1#ping 130.33.1.3 source 173.33.1.1
% Invalid source address- IP address not on any of our up interfaces
R1#
```

答: 用 172.16.1.1 做源地址, 不能 ping 通。

4、配置扩展访问控制列表, 实现允许 172.33.2.0 子网 telnet 到 130.33.0.0, 不允许其他子网的用户 telnet 到 130.33.0.0, 同时不能妨碍其他网络数据的传递。

参考命令:

在 R3 中配置, 允许其他主机 telnet

```
R3(config)#username xcu password cisco

R3(config)#line vty 0 3

R3(config-line)#login local
```

在 R2 中创建扩展访问控制列表

```
R2(config)#access-list 133 permit tcp 172.33.2.0 0.0.0.255 130.33.0.0 0.0.2
55.255 eq 23

R2(config)#access-list 133 deny tcp any 130.33.0.0 0.0.255.255 eq 23

R2(config)#access-list 133 permit ip any any

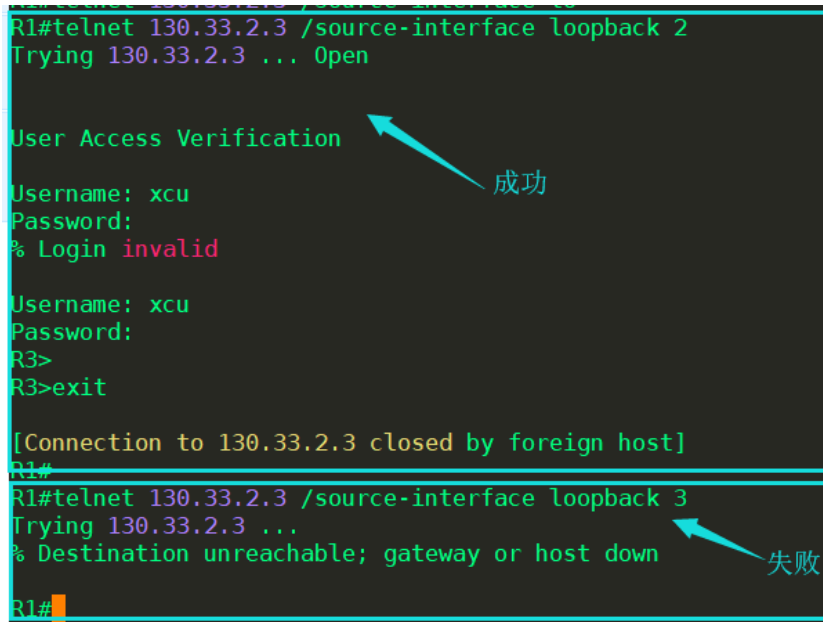
R2(config)#int f0/1
口 f0/1 更接近源
```

注: 在这里选择接

```
R2(config-if)#ip access-group 133 in
```

问题 3: 在 R1 上 telnet 130.33.2.3, 以 172.33.2.1 作为源地址, 能否登陆? 如果以 172.33.3.1 或 172.33.4.1 为源地址, 能否登陆?

参考命令:



```
R1#telnet 130.33.2.3 /source-interface loopback 2
Trying 130.33.2.3 ... Open

User Access Verification

Username: xcu
Password:
% Login invalid

Username: xcu
Password:
R3>
R3>exit

[Connection to 130.33.2.3 closed by foreign host]
R1#
R1#telnet 130.33.2.3 /source-interface loopback 3
Trying 130.33.2.3 ...
% Destination unreachable; gateway or host down
R1#
```

5、配置命名访问控制列表, 实现 172.33.0.0 能够 telnet 130.33.0.0, 而 130.33.0.0 无法 telnet 到 172.33.0.0。

参考命令:

首先, 参照步骤 4, 在 R1 中实现远程登录功能。

```
R1(config)#username xcu password cisco
```

```
R1(config)#line vty 0 3
```

```
R1(config-line)#login local
```

在 R2 中创建命名访问控制列表

```
R2(config)#ip access-list extended xcu
```

```
R2(config-ext-nacl)#permit tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255
5 established

R2(config-ext-nacl)#deny tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255

R2(config-ext-nacl)#permit ip any any

R2(config)#int f0/0

R2(config-if)#ip access-group xcu in
```

问题 4: 在 R1 上 telnet 130.33.2.3, 以 172.33.2.1 作为源地址, 能否登陆? 如果以 172.33.3.1 或 172.33.4.1 为源地址, 能否登陆? 为什么?

```
R1#telnet 130.33.2.3 /source-interface loopback 3
*May 16 11:07:03.911: %SYS-5-CONFIG_I: Configured from console by console
R1#telnet 130.33.2.3 /source-interface loopback 2
Trying 130.33.2.3 ... Open

User Access Verification

Username: xcu
Password:
% Login invalid

Username: xcu
Password:
% Login invalid

Username: xcu
Password:
R3>
R3>
R3>exit

[Connection to 130.33.2.3 closed by foreign host]
R1#
```

答: 在 R1 上 telnet 130.33.2.3, 以 172.33.2.1 作为源地址, 能登陆。

```
R1#telnet 130.33.2.3 /source-interface loopback 3
Trying 130.33.2.3 ...
% Destination unreachable; gateway or host down

R1#
```

```

R2#show access-lists
Standard IP access list 33
 10 deny 172.33.1.0, wildcard bits 0.0.0.255
 20 permit any (229 matches)
Extended IP access list 133
 10 permit tcp 172.33.2.0 0.0.0.255 130.33.0.0 0.0.255.255 eq telnet (229 matches)
 20 deny tcp any 130.33.0.0 0.0.255.255 eq telnet (9 matches)
 30 permit ip any any (1204 matches)
Extended IP access list xcu
 10 permit tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255 established (145 matches)
 20 deny tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255
 30 permit ip any any (600 matches)
R2#show access-lists
Standard IP access list 33
 10 deny 172.33.1.0, wildcard bits 0.0.0.255
 20 permit any (229 matches)
Extended IP access list 133
 10 permit tcp 172.33.2.0 0.0.0.255 130.33.0.0 0.0.255.255 eq telnet (229 matches)
 20 deny tcp any 130.33.0.0 0.0.255.255 eq telnet (10 matches)
 30 permit ip any any (1208 matches)
Extended IP access list xcu
 10 permit tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255 established (145 matches)
 20 deny tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255
 30 permit ip any any (604 matches)
R2#

```

答：在 R1 上 telnet 130.33.2.3，以 172.33.3.1 作为源地址，不能登陆。因为受 ACL 133 配置的限制。

问题 5：在 R3 中 telnet 172.33.2.1，以 130.33.1.3 为源地址，能否登陆？为什么？

```

R2#show access-lists
Standard IP access list 33
 10 deny 172.33.1.0, wildcard bits 0.0.0.255
 20 permit any (229 matches)
Extended IP access list 133
 10 permit tcp 172.33.2.0 0.0.0.255 130.33.0.0 0.0.255.255 eq telnet (229 matches)
 20 deny tcp any 130.33.0.0 0.0.255.255 eq telnet (10 matches)
 30 permit ip any any (1208 matches)
Extended IP access list xcu
 10 permit tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255 established (145 matches)
 20 deny tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255
 30 permit ip any any (604 matches)
R2#show access-lists
Standard IP access list 33
 10 deny 172.33.1.0, wildcard bits 0.0.0.255
 20 permit any (229 matches)
Extended IP access list 133
 10 permit tcp 172.33.2.0 0.0.0.255 130.33.0.0 0.0.255.255 eq telnet (229 matches)
 20 deny tcp any 130.33.0.0 0.0.255.255 eq telnet (10 matches)
 30 permit ip any any (1318 matches)
Extended IP access list xcu
 10 permit tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255 established (145 matches)
 20 deny tcp 130.33.0.0 0.0.255.255 172.33.0.0 0.0.255.255 (1 match)
 30 permit ip any any (714 matches)
R2#

```

答：在 R3 中 telnet 172.33.2.1，以 130.33.1.3 为源地址，不能登陆。因为受 ACL xcu 配置的限制。

问题 6：此时在 R3 中 ping 172.33.2.1，以 130.33.1.3 为源地址，能否 ping 通？

参考命令：ping 172.33.2.1 source 130.33.1.3

```

R3#ping 172.33.2.1 source 130.33.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.33.2.1, timeout is 2 seconds:
Packet sent with a source address of 130.33.1.3
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/58/64 ms
R3#
R3#
R3#

```

答：在 R3 中 ping 172.33.2.1，以 130.33.1.3 为源地址，能 ping 通。因为 ACL xcu 配置限制的是 TCP 协议，ping 测试使用的是 ICMP 网络层协议。

5、在命名访问控制列表 xcu 中的第二条和第三条之间添加两条规则，添加后删除这两条中的一条。

参考命令：

```

R2(config)#ip access-list extended xcu

R2(config-ext-nacl)#24 permit ip host 192.33.2.3 any

R2(config-ext-nacl)#28 deny ip 192.33.2.0 0.0.0.255 any

```

删除一条记录：

```

R2(config-ext-nacl)#no 28          注：删除第 28 条规则

```

6、配置命名访问控制列表，实现 172.33.0.0 能够访问 130.33.0.0，而 130.33.0.0 无法访问到 172.33.0.0。

参考命令：

```

R2(config)#ip access-list extended ref_xcu          注：定义反射 acl

R2(config-ext-nacl)#permit ip 172.33.0.0 0.0.255.255 any reflect ref_xcu1
注：定义反射 acl

R2(config-ext-nacl)#permit eigrp any any          注：这条命令允许 eigrp
的数据正常传输

R2(config)#ip access-list extended ref_xcu2          注：定义反射 acl

R2(config-ext-nacl)#evaluate ref_xcu1          注：调用定义的反射 ac
l

R2(config-ext-nacl)#permit eigrp any any          注：这条命令允许 eigrp
的数据正常传输

```

```
R2(config)#int f0/0

R2(config-if)#ip access-group ref_xcu out

R2(config-if)#ip access-group ref_xcu2 in
```

问题 7：在 R2 上用 `show access-lists ref_xcu1` 查看反射访问控制列表 `ref_xcu1` 的内容，里面是否为空？

```
R2#show access-lists ref_xcu1
Reflexive IP access list ref_xcu1
R2#
R2#
R2#
```

答：此时 R1 和 R3 之间没有通信，反射访问控制列表 `ref_xcu1` 为空。

问题 8：配置后，在 R1 中以 172.33.2.1 为源地址 ping 130.33.2.3，看能否 ping 通？
在 R3 中以 130.33.2.3 为源，ping 172.33.2.1 能否 ping 通？

参考命令：

```
R1#ping 130.33.2.3 source 172.33.2.1
```

```
R1#ping 130.33.2.3 source 172.33.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.33.2.3, timeout is 2 seconds:
Packet sent with a source address of 172.33.2.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/56/80 ms
R1#
R1#
R1#
```

答：在 R1 中以 172.33.2.1 为源地址 ping 130.33.2.3，能 ping 通。

```
R3#ping 172.33.2.1 source 130.33.2.3
```

```
R3#ping 172.33.2.1 source 130.33.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.33.2.1, timeout is 2 seconds:
Packet sent with a source address of 130.33.2.3
UUUUU
Success rate is 0 percent (0/5)
R3#
R3#
R3#
```

在 R3 中以 130.33.2.3 为源，ping 172.33.2.1 不能 ping 通。

问题 9: 在 R1 中以 172.33.2.1 为源地址 telnet 130.33.2.3, 看能否登陆成功?
在 R3 中以 130.33.2.3 为源, telnet 172.33.2.1 能否登陆成功?

参考命令:

```
R1#telnet 130.33.2.3 /source-interface lo2
```

```
R1#telnet 130.33.2.3 /source-interface lo2
Trying 130.33.2.3 ... Open

User Access Verification

Username: xcu
Password:
R3>e
% Ambiguous command: "e"
R3>
R3>exit

[Connection to 130.33.2.3 closed by foreign host]
R1#
R1#
R1#
```

答: 能登陆成功。

```
R3#telnet 172.33.2.1 /source-interface lo2
```

```
R3#
R3#telnet 172.33.2.1 /source-interface lo2
Trying 172.33.2.1 ...
% Destination unreachable; gateway or host down

R3#
```

答: 限制登陆。

问题 10: 做完问题 8 和问题 9 后马上在路由器 R2 上用 show access-lists ref_xcu1 查看反射访问控制列表 ref_xcu1 的内容, 和问题 7 看到的有什么不同?

```
R2#show access-lists ref_xcu1
Reflexive IP access list ref_xcu1
    permit tcp host 130.33.2.3 eq telnet host 172.33.2.1 eq 37359 (14 matches) (time left 293)
R2#
R2#
```

答: 写入了 130.33.2.3 和 172.33.2.1 的 tcp 映射。

7、创建动态 ACL 实现 R1 必须先成功登录 R2 才能访问 R3 的功能。

参考命令:

首先, 参照步骤 4, 在 R1 中实现远程登录功能。

在 R2 中配置动态访问控制列表

```
R2(config)#ip access-list extended dynamic_xcu
```

```

R2(config-ext-nacl)#permit eigrp any any
允许 eigrp 的数据正常传输

R2(config-ext-nacl)#permit tcp any host 192.33.1.2 eq 23
telnet 到 R2

R2(config-ext-nacl)#dynamic XCU timeout 10 permit tcp any 130.33.0.0 0.0.255.255

R2(config)#int f0/1

R2(config-if)#ip access-group dynamic_xcu in

R2(config)#line vty 0 3

R2(config-line)#login local

R2(config-line)#autocommand access-enable host timeout 3

```

注：这条命令

允许 R1

问题 11：配置后在 R2 中查看访问控制列表 dynamic_xcu，有几条选项？

```

R2#show access-lists dynamic_xcu
Extended IP access list dynamic_xcu
 10 permit eigrp any any (390 matches)
 20 permit tcp any host 192.33.1.2 eq telnet
 30 Dynamic XCU permit tcp any 130.33.0.0 0.0.255.255
R2#
R2#
R2#

```

答：3 条。

问题 11：配置后直接在 R1 中输入 telnet 130.33.2.3 /source-interface lo2 能否登陆成功？

```

R1#
R1#telnet 130.33.2.3 /source-interface lo2
Trying 130.33.2.3 ...
% Destination unreachable; gateway or host down
R1#
R1#
R1#
R1#

```

答：不能登陆成功。

问题 12: 在 R1 中用 telnet 192.33.1.2 /source-interface lo2 登陆 R2, 马上在 R2 中查看访问控制列表 dynamic_xcu, 有几条选项?

```
R2#show access-lists dynamic_xcu
Extended IP access list dynamic_xcu
 10 permit eigrp any any (828 matches)
 20 permit tcp any host 192.33.1.2 eq telnet (504 matches)
 30 Dynamic XCU permit tcp any 130.33.0.0 0.0.255.255
    permit tcp host 172.33.2.1 130.33.0.0 0.0.255.255
R2#
```

答: 4 条选项。

问题 13: 此时再次在 R1 中输入 telnet 130.33.2.3 /source-interface lo2 能否登陆成功?

```
R1# telnet 130.33.2.3 /source-interface lo2
Trying 130.33.2.3 ... Open

User Access Verification

Username: xcu
Password:
R3>
R3>
R3>
R3>
R3>exit

[Connection to 130.33.2.3 closed by foreign host]
R1#
R1#
```

答: 能成功登陆。