第 9 章　ACL

随着大规模开放式网络的开发，网络面临的威胁也就越来越多。网络安全问题成为网络管理员最为头疼的问题。一方面，为了业务的发展，必须允许对网络资源的开发访问，另一方面，又必须确保数据和资源的尽可能安全。网络安全采用的技术很多，而通过访问控制列表（ACL）可以对数据流进行过滤，是实现基本的网络安全手段之一。本章只研究基于 IP 的 ACL。

9.1　ACL 概述

访问控制列表简称为 ACL，它使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分很多种，不同场合应用不同种类的 ACL。

1. 标准 ACL

标准 ACL 最简单，是通过使用 IP 包中的源 IP 地址进行过滤，表号范围 1-99 或 1300-1999；

2. 扩展 ACL

扩展 ACL 比标准 ACL 具有更多的匹配项，功能更加强大和细化，可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP 连接建立等进行过滤，表号范围 100-199 或 2000-2699；

3. 命名 ACL

以列表名称代替列表编号来定义 ACL，同样包括标准和扩展两种列表。

在访问控制列表的学习中，要特别注意以下两个术语。

1. 通配符掩码：一个 32 比特位的数字字符串，它规定了当一个 IP 地址与其他的 IP 地址进行比较时，该 IP 地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略 IP 地址中对应的位，而“0”则表示该位必须匹配。两种特殊的通配符掩码是“255.255.255.255”和“0.0.0.0”，前者等价于关键字“any”，而后者等价于关键字“host”；

2. Inbound 和 outbound：当在接口上应用访问控制列表时，用户要指明访问控制列表是应用于流入数据还是流出数据。

总之，ACL 的应用非常广泛，它可以实现如下的功能：

1. 拒绝或允许流入（或流出）的数据流通过特定的接口；
2. 为 DDR 应用定义感兴趣的数据流；
3. 过滤路由更新的内容；
4. 控制对虚拟终端的访问；
5. 提供流量控制。

9.2 实验 1：标准 ACL

1.实验目的

通过本实验可以掌握：

（1）ACL 设计原则和工作过程

（2）定义标准 ACL

（3）应用 ACL

（4）标准 ACL 调试

2.拓扑结构

实验拓扑如图 9-1 所示。

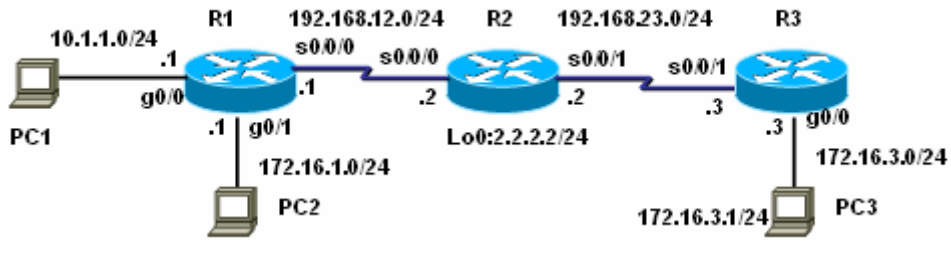

图 9-1 标准 ACL 配置

本实验拒绝 PC2 所在网段访问路由器 R2,同时只允许主机 PC3 访问路由器 R2 的 TELNET 服务。整个网络配置 EIGRP 保证 IP 的连通性。

3.实验步骤

（1）步骤 1：配置路由器 R1

```
R1(config)#router eigrp 1
R1(config-router)#network 10.1.1.0 0.0.0.255
R1(config-router)#network 172.16.1.0 0.0.0.255
R1(config-router)#network 192.168.12.0
R1(config-router)#no auto-summary
```

（2）步骤 2：配置路由器 R2

```
R2(config)#router eigrp 1
R2(config-router)#network 2.2.2.0 0.0.0.255
R2(config-router)#network 192.168.12.0
R2(config-router)#network 192.168.23.0
R2(config-router)#no auto-summary
R2(config)#access-list 1 deny   172.16.1.0 0.0.0.255 //定义 ACL
R2(config)#access-list 1 permit any
R2(config)#interface Serial0/0/0
R2(config-if)#ip access-group 1 in    //在接口下应用 ACL
R2(config)#access-list 2 permit 172.16.3.1
R2(config-if)#line vty 0 4
R2(config-line)#access-class 2 in    //在 vty 下应用 ACL
R2(config-line)#password cisco
R2(config-line)#login
```

（3）步骤 3：配置路由器 R3

```
R3(config)#router eigrp 1
R3(config-router)#network 172.16.3.0 0.0.0.255
R3(config-router)#network 192.168.23.0
R3(config-router)#no auto-summary
```

【技术要点】

（1）ACL 定义好，可以在很多地方应用，接口上应用只是其中之一，其它的常用应用包括在 route map 中的 match 应用（21 章介绍）和在 vty 下用“access-class”命令调用，来控制 telnet 的访问；

（2）访问控制列表表项的检查按自上而下的顺序进行，并且从第一个表项开始，所以必须考虑在访问控制列表中定义语句的次序；

（3）路由器不对自身产生的 IP 数据包进行过滤；

（4）访问控制列表最后一条是隐含的拒绝所有；

（5）每一个路由器接口的每一个方向，每一种协议只能创建一个 ACL；

（6）“access-class”命令只对标准 ACL 有效。

4.实验调试

在 PC1 网络所在的主机上 ping 2.2.2.2，应该通，在 PC2 网络所在的主机上 ping 2.2.2.2，应该不通，在主机 PC3 上 TELNET 2.2.2.2，应该成功。

（1）show ip access-lists

该命令用来查看所定义的 IP 访问控制列表。

```
R2#show ip access-lists
Standard IP access list 1
    10 deny   172.16.1.0, wildcard bits 0.0.0.255 (11 matches)
    20 permit any (405 matches)
Standard IP access list 2
    10 permit 172.16.3.1 (2 matches)
```

以上输出表明路由器 R2 上定义的标准访问控制列表为“1”和“2”，括号中的数字表示匹配条件的数据包的个数，可以用“clear access-list counters”将访问控制列表计数器清零。

（2）show ip interface

```
R2#show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 1
  ......
```

以上输出表明在接口 s0/0/0 的入方向应用了访问控制列表 1。

9.3 实验 2：扩展 ACL

1.实验目的

通过本实验可以掌握：

（1）定义扩展 ACL

（2）应用扩展 ACL

（3）扩展 ACL 调试

2.拓扑结构

实验拓扑如图 9-1 所示。

本实验要求只允许 PC2 所在网段的主机访问路由器 R2 的 WWW 和 TELNET 服务，并拒绝 PC3 所在网段 PING 路由器 R2。删除实验 1 中定义的 ACL，保留 EIGRP 的配置。

3.实验步骤

（1）步骤 1：配置路由器 R1

```
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq www
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq www
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq www
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq telnet
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq telnet
R1(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq telnet
R1(config)#interface g0/0
R1(config-if)#ip access-group 100 in
```

（2）步骤 2：配置路由器 R2

```
R2(config)#no access-list 1  //删除 ACL
R2(config)#no access-list 2
R2(config)#ip http server   //将路由器配置成 WEB 服务器
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
```

（3）步骤 3：配置路由器 R3

```
R3(config)#access-list 101 deny icmp 172.16.3.0 0.0.0.255 host 2.2.2.2 log
R3(config)#access-list 101 deny icmp 172.16.3.0 0.0.0.255 host 192.168.12.2 log
R3(config)#access-list 101 deny icmp 172.16.3.0 0.0.0.255 host 192.168.23.2 log
R3(config)#access-list 101 permit ip any any
R3(config)#interface g0/0
R3(config-if)#ip access-group 101 in
```

【技术要点】

（1）参数“log”会生成相应的日志信息，用来记录经过 ACL 入口的数据包的情况；

（2）尽量考虑将扩展的访问控制列表放在靠近过滤源的位置上，这样创建的过滤器就不会反过来影响其它接口上的数据流。另外，尽量使标准的访问控制列表靠近目的，由于标准访问控制列表只使用源地址，如果将其靠近源会阻止数据包流向其他端口。

4.实验调试

（1)分别在 PC2 上访问路由器 R2 的 TELNET 和 WWW 服务,然后查看访问控制列表 100：

```
R1#show ip access-lists
Extended IP access list 100
```

```
    10 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq www (8 matches)
    20 permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq www
    30 permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq www
    40 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq telnet (20 matches)
    50 permit tcp 172.16.1.0 0.0.0.255 host 12.12.12.2 eq telnet (4 matches)
    60 permit tcp 172.16.1.0 0.0.0.255 host 23.23.23.2 eq telnet (4 matches)
```

（2）在 PC3 所在网段的主机 ping 路由器 R2，路由器 R3 会出现下面的日志信息：

```
*Feb 25 17:35:46.383: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 172.16.3.1 -> 2.2.2.2
(0/0), 1 packet
*Feb 25 17:41:08.959: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 172.16.3.1 -> 2.2.2.2
(0/0), 4 packets
*Feb 25 17:42:46.919: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 172.16.3.1 ->
192.168.12.2 (0/0), 1 packet
*Feb 25 17:42:56.803: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 172.16.3.1 ->
192.168.23.2 (0/0), 1 packet
```

以上输出说明在访问控制列表 101 在有匹配数据包的时候，系统作了日志。

（3）在路由器 R3 上查看访问控制列表 101：

```
R3#show access-lists
Extended IP access list 101
    10 deny icmp 172.16.3.0 0.0.0.255 host 2.2.2.2 log (5 matches)
    20 deny icmp 172.16.3.0 0.0.0.255 host 192.168.12.2 log (5 matches)
    30 deny icmp 172.16.3.0 0.0.0.255 host 192.168.23.2 log (5 matches)
    40 permit ip any any (6 matches)
```

9.4 实验 3：命名 ACL

命名 ACL 允许在标准 ACL 和扩展 ACL 中，使用字符串代替前面所使用的数字来表示 ACL。命名 ACL 还可以被用来从某一特定的 ACL 中删除个别的控制条目，这样可以让网络管理员方便地修改 ACL。

1.实验目的

通过本实验可以掌握：

（1）定义命名 ACL

（2）应用命名 ACL

2.拓扑结构

实验拓扑如图 9-1 所示。

3.实验步骤

本实验给出如何用命名 ACL 来实现 9.2 实验 1 中和 9.3 实验 2 中的要求。

（1）在路由器 R2 上配置命名的标准 ACL 实现 9.2 实验 1 的要求

```
R2(config)#ip access-list standard stand
R2(config-std-nacl)#deny 172.16.1.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config)#interface Serial0/0/0
R2(config-if)#ip access-group stand in
R2(config)#ip access-list standard class
```

R2(config-std-nacl)#permit 172.16.3.1
R2(config-if)#line vty 0 4
R2(config-line)#access-class class in

（2）在路由器 R2 上查看命名访问控制列表

```
R2#show access-lists
Standard IP access list class
    10 permit 172.16.3.1
Standard IP access list stand
    10 deny   172.16.1.0, wildcard bits 0.0.0.255
    20 permit any (42 matches)
```

（3）在路由器 R1 和 R3 上配置命名的扩展 ACL 实现 9.3 实验 2 的要求

R1(config)#ip access-list extended ext1
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq www
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq www
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq www
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq telnet
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq telnet
R1(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq telnet
R1(config)#interface g0/0
R1(config-if)#ip access-group ext1 in
R3(config)#ip access-list extended ext3
R3(config-ext-nacl)#deny icmp 172.16.3.0 0.0.0.255 host 2.2.2.2 log
R3(config-ext-nacl)#deny icmp 172.16.3.0 0.0.0.255 host 192.168.12.2 log
R3(config-ext-nacl)#deny icmp 172.16.3.0 0.0.0.255 host 192.168.23.2 log
R3(config-ext-nacl)#permit ip any any
R3(config)#interface g0/0
R3(config-if)#ip access-group ext3 in

（4）在路由器 R1 和 R3 上查看命名访问控制列表

```
R1#show access-lists
Extended IP access list ext1
    10 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq www
    20 permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq www
    30 permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq www
    40 permit tcp 172.16.1.0 0.0.0.255 host 2.2.2.2 eq telnet
    50 permit tcp 172.16.1.0 0.0.0.255 host 192.168.12.2 eq telnet
    60 permit tcp 172.16.1.0 0.0.0.255 host 192.168.23.2 eq telnet
R3#show access-lists
Extended IP access list ext3
    10 deny icmp 172.16.3.0 0.0.0.255 host 2.2.2.2 log
    20 deny icmp 172.16.3.0 0.0.0.255 host 192.168.12.2 log
    30 deny icmp 172.16.3.0 0.0.0.255 host 192.168.23.2 log
```

40 permit ip any any

9.5 实验 4：基于时间 ACL

1.实验目的

通过本实验可以掌握：

（1）定义 time-range

（2）配置基于时间 ACL

（3）基于时间 ACL 调试

2.拓扑结构

实验拓扑如图 9-1 所示。

本实验要求只允许PC3主机在周一到周五的每天的8:00-18:00访问路由器R2的TELNET服务。

3.实验步骤

R3(config)#**time-range time**　　//定义时间范围

R3(config-time-range)#**periodic weekdays 8:00 to 18:00**

R3(config)#**access-list 111 permit tcp host 172.16.3.1 host 2.2.2.2 eq telnet time-range time**　//在访问控制列表中调用 time-range

R3(config)#**access-list 111 permit tcp host 172.16.3.1 host 192.168.12.2 eq telnet time-range time**

R3(config)#**access-list 111 permit tcp host 172.16.3.1 host 192.168.23.2 eq telnet time-range time**

R3(config)#**interface g0/0**

R3(config-if)#**ip access-group 111 in**

4.实验调试

（1）用“clock”命令将系统时间调整到周一至周五的 8:00-18:00 范围内，然后在 PC3 上 TELNET 路由器 R2，此时可以成功，然后查看访问控制列表 111：

R3#**show access-lists**

Extended IP access list 111

10 permit tcp host 172.16.3.1 host 2.2.2.2 eq telnet time-range time (**active**) (**15 matches**)

20 permit tcp host 172.16.3.1 host 192.168.12.2 eq telnet time-range time (**active**)

30 permit tcp host 172.16.3.1 host 192.168.23.2 eq telnet time-range time (**active**)

（2）用“clock”命令将系统时间调整到 8:00-18:00 范围之外，然后在 PC3 上 TELNET 路由器 R2，此时不可以成功，然后查看访问控制列表 111：

R3#**show access-lists**

Extended IP access list 111

10 permit tcp host 172.16.3.1 host 2.2.2.2 eq telnet time-range time (**inactive**) (**45 matches**)

20 permit tcp host 172.16.3.1 host 192.168.12.2 eq telnet time-range time (**inactive**)

30 permit tcp host 172.16.3.1 host 192.168.23.2 eq telnet time-range time (**inactive**)

（3）**show time-range**

该命令用来查看定义的时间范围。

R3#**show time-range**

time-range entry: time (**active**)

periodic weekdays 8:00 to 18:00

used in: IP ACL entry

used in: IP ACL entry

used in: IP ACL entry

以上输出表示在 3 条 ACL 中调用了该 time-range。

9.6 实验 5：动态 ACL

动态 ACL 是 Cisco IOS 的一种安全特性，它使用户能在防火墙中临时打开一个缺口，而不会破坏其它已配置了的安全限制。

1.实验目的

通过本实验可以掌握：

（1）动态 ACL 工作原理

（2）配置 VTY 本地登录

（3）配置动态 ACL

（4）动态 ACL 调试

2.拓扑结构

实验拓扑如图 9-1 所示。

本实验要求如果 PC3 所在网段想要访问路由器 R2 的 WWW 服务，必须先 TELNET 路由器 R2 成功后才能访问。

3.实验步骤

R2(config)#username ccie password cisco   //建立本地数据库

R2(config)#access-list 120 permit tcp 172.16.3.0 0.0.0.255 host 2.2.2.2 eq telnet //打开 TELNET 访问权限

R2(config)#access-list 120 permit tcp 172.16.3.0 0.0.0.255 host 12.12.12.2 eq telnet

R2(config)#access-list 120 permit tcp 172.16.3.0 0.0.0.255 host 23.23.23.2 eq telnet

R2(config)#access-list 120 permit eigrp any any //允许 EIGRP 协议

R2(config)#access-list 120 dynamic test timeout 120 permit ip 172.16.3.0 0.0.0.255 host 2.2.2.2

//“dynamic”定义动态 ACL，“timeout”定义动态 ACL 绝对的超时时间

R2(config)#access-list 120 dynamic test1 timeout 120 permit ip 172.16.3.0 0.0.0.255 host 23.23.23.2

R2(config)#access-list 120 dynamic test2 timeout 120 permit ip 172.16.3.0 0.0.0.255 host 12.12.12.2

R2(config)#interface s0/0/1

R2(config-if)#ip access-group 120 in

R2(config)#line vty 0 4

R2(config-line)#login local   //VTY 使用本地验证

R2(config-line)#autocommand access-enable host timeout 5

//在一个动态 ACL 中创建一个临时性的访问控制列表条目，“timeout”定义了空闲超时值，空闲超时值必须小于绝对超时值。

【技术要点】

如果用参数“host”，那么临时性条目将只为用户所用的单个 IP 地址创建，如果不使用，

那用户的整个网络都将被该临时性条目允许。

4.实验调试

（1）没有 TELNET 路由器 R2，在 PC3 上直接访问路由器 R2 的 WWW 服务，不成功，路由器 R2 的访问控制列表：

```
R2#show access-lists
Extended IP access list 120
    10 permit tcp 172.16.3.0 0.0.0.255 host 2.2.2.2 eq telnet (114 matches)
    20 permit tcp 172.16.3.0 0.0.0.255 host 12.12.12.2 eq telnet
    30 permit tcp 172.16.3.0 0.0.0.255 host 23.23.23.2 eq telnet
    40 permit eigrp any any (159 matches)
    50 Dynamic test permit ip 172.16.3.0 0.0.0.255 host 2.2.2.2
    60 Dynamic test1 permit ip 172.16.3.0 0.0.0.255 host 23.23.23.2
    70 Dynamic test2 permit ip 172.16.3.0 0.0.0.255 host 12.12.12.2
```

（2）TELNET 路由器 R2 成功之后，在 PC3 上访问路由器 R2 的 WWW 服务，成功，路由器 R2 的访问控制列表：

```
R2#show access-lists
Extended IP access list 120
    10 permit tcp 172.16.3.0 0.0.0.255 host 2.2.2.2 eq telnet (114 matches)
    20 permit tcp 172.16.3.0 0.0.0.255 host 12.12.12.2 eq telnet
    30 permit tcp 172.16.3.0 0.0.0.255 host 23.23.23.2 eq telnet
    40 permit eigrp any any (159 matches)
    50 Dynamic test permit ip 172.16.3.0 0.0.0.255 host 2.2.2.2
       permit ip host 172.16.3.1 host 2.2.2.2 (15 matches) (time left 288)
    60 Dynamic test1 permit ip 172.16.3.0 0.0.0.255 host 23.23.23.2
    70 Dynamic test2 permit ip 172.16.3.0 0.0.0.255 host 12.12.12.2
```

从(1)和(2)的输出结果可以看到，从主机 172.16.3.1 telnet 2.2.2.2,如果通过认证，该 telnet 会话就会被切断，IOS 软件将在动态访问控制列表中动态建立一临时条目“**permit ip host 172.16.3.1 host 2.2.2.2**”，此时在主机 172.16.3.1 上访问 2.2.2.2 的 Web 服务，成功。

9.7 实验 6：自反 ACL

1.实验目的

通过本实验可以掌握：

（1）自反 ACL 工作原理

（2）配置自反 ACL

（3）自反 ACL 调试

2.拓扑结构

实验拓扑如图 9-2 所示。

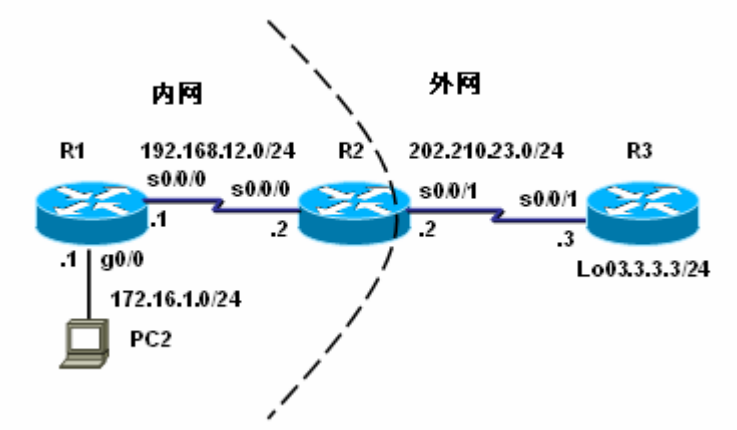

图 9-2 自反 ACL 配置

本实验要求内网可以主动访问外网，但是外网不能主动访问内网，从而有效保护内网。

3. 实验步骤

（1）步骤 1：分别在路由器 R1 和 R3 配置默认路由确保 IP 连通性

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2
R3(config)#ip route 0.0.0.0 0.0.0.0 202.210.23.2
```

（2）步骤 2：在路由器 R2 上配置自反 ACL

```
R2(config)#ip access-list extended ACLOUT
R2(config-ext-nacl)#permit tcp any any reflect REF  //定义自反 ACL
R2(config-ext-nacl)#permit udp any any reflect REF
R2(config)#ip access-list extended ACLIN
R2(config-ext-nacl)#evaluate REF //评估反射
R2(config)#int s0/0/1
R2(config-if)#ip access-group ACLOUT out
R2(config-if)#ip access-group ACLIN in
```

【技术要点】

1. 自反 ACL 永远是 permit 的；
2. 自反 ACL 允许高层 Session 信息的 IP 包过滤；
3. 利用自反 ACL 可以只允许出去的流量，但是阻止从外部网络产生的向内部网络的流量，从而可以更好地保护内部网络；
4. 自反 ACL 是在有流量产生时（如出方向的流量）临时自动产生的，并且当 Session 结束条目就删除；
5. 自反 ACL 不是直接被应用到某个接口下的，而是嵌套在一个扩展命名访问列表下的。

4. 实验调试

（1）同时在路由器 R1 和 R3 都打开 TELNET 服务，在 R1(从内网到外网)TELNET 路由器 R3 成功，同时在路由器 R2 上查看访问控制列表：

```
R2#show access-lists
Extended IP access list ACLIN
    10 evaluate REF
Extended IP access list ACLOUT
```

```
        10 permit tcp any any reflect REF
        20 permit udp any any reflect REF
    Reflexive IP access list REF
         permit tcp host 202.210.23.3 eq telnet host 192.168.12.1 eq 11002 (48 matches) (time left 268)
```

以上输出说明自反列表是在有内部到外部 TELNET 流量经过的时候，临时自动产生一条列表。

（2）在路由器 R1 打开 TELNET 服务，在 R3(从外网到内网)TELNET 路由器 R1 不能成功，同时在路由器 R2 上查看访问控制列表：

```
R2#show access-lists
Extended IP access list ACLIN
    10 evaluate REF
Extended IP access list ACLOUT
    10 permit tcp any any reflect REF
    20 permit udp any any reflect REF
Reflexive IP access list REF
```

以上输出说明自反列表是在有外部到内部 TELNET 流量经过的时候，不会临时自动产生一条列表，所以不能访问成功。

9.8 ACL 命令汇总

表 9-1 列出了本章涉及到的主要的命令。

表 9-1 本章命令汇总

命令	作用
show ip access-lists	查看所定义的 IP 访问控制列表
clear access-list counters	将访问控制列表计数器清零
access-list	定义 ACL
ip access-group	在接口下应用 ACL
access-class	在 vty 下应用 ACL
ip access-list	定义命名的 ACL
time-range time	定义时间范围
username *username* password *password*	建立本地数据库
autocommand	定义自动执行的命令