第12章 IP 访 问 表

本章主题

- 细节概述
- 访问表的术语
- 标准IP访问表
- 扩展IP访问表
- 带有Established选项的扩展IP访问表
- 动态IP访问表
- 加密解密（lock-and-key）如何工作
- 可控VTY访问
- 详细的故障查找示例

12.1 引言

路由器用访问表管理进入和离开一个特定接口的数据流。下面列出了访问表可以用的一些方法：

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应用定义有趣的数据流。
3) 过滤路由更新的内容。
4) 控制虚拟终端线的访问。
5) 提供流量控制。

本章说明了如何用静态和动态访问表控制报文流过路由器。

12.2 IP访问表技术概述

访问表，或访问控制表，提供了基本的数据流过滤能力。它可以用来控制进入或离开一网络的访问，也可以在路由器的输入或输出端口过滤报文。

基于前面定义的标准，访问表通过用路由器决定转发还是丢弃报文来过滤网络的数据流。这个标准由访问表定义，返回来又应用于接口。

依据访问表的定义，匹配标准可能很简单（标准访问表），也可能很复杂（扩展访问表）。访问表提供了检测流入或流出路由器端口的报文的一种方法，也使路由器通过一定的标准控制那些报文。

访问表中的术语

在Cisco路由器上处理访问表，必须理解所用到的一些术语。

1) 通配符屏蔽字：通配符屏蔽字规定了当一个 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。

通配符屏蔽字中的“ 1 ”表示忽略IP地址中对应的位，而“ 0 ”则表示该位必须保留。

注意　对一标准访问表来说，如果忽略了某入口的通配符屏蔽字，0.0.0.0将被认为是缺省的屏蔽字。

例如：下面的访问表（访问表 1）指明了数据流被允许通过的顺序，前 3个八位字节组必须匹配（150.1.1）。这个访问表允许主机号为 1~255的主机连在网络150.1.1.0上。

```
access-list 1 permit 150.1.1.0 0.0.0.255
```

```
   150        1          1          0        ←IP address
10010110  00000001   00000001   00000000   ←Binary representation of IP address
00000000  00000000   00000000   11111111   ←Binary representation of Wildcard mask
-------------------------------------------------------------------------------
10010110  00000001   00000001   xxxxxxxx
   ↑          ↑          ↑          ↑
   150        1          1          x    ← When comparing IP addresses, match the first three octets
                                           and ignore the last octet.
```

2) Inbound和outbound：当在一接口应用访问表时，用户指明访问表是应用于流入数据还是流出数据（或两方向都有）。缺省的设置是应用于流出数据。

数据流的流向同路由器的接口有关。例如，在图 12-1中。

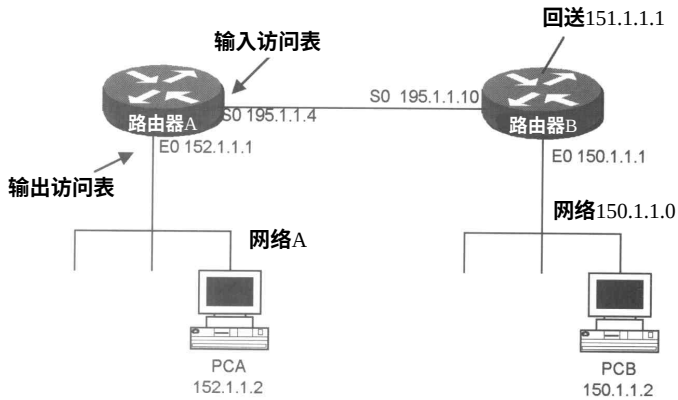

图12-1　访问表术语

路由器A想拒绝所有从主机 150.1.1.2到主机PCA（152.1.1.2）的数据流。那么在路由器 A上有两个位置可应用访问表。一个接入 (inbound)访问表可以设置在串行接口，或者一个接出(outbound)访问表设置在以太网接口。最优选择是将访问表应用于离那些被拒绝的数据流最近的地方。

注意　接出访问表应用于满足下面条件的报文（packet）：已做出了路由决定，并且该报文向适当的接口路由。此时，报文与访问表相对应，报文可能被转发或被丢弃。经过路由器路由一个报文是没用的，该报文只会在输出端口被丢弃。一个好的设计是在那些离将被拒绝的数据流最近的接口上应用访问表。

12.3　本章所讨论的命令

- **access-class** access-list-number {in | out}

- **access-enable** [host] [timeout minutes]
- **access-list** access-list-number {deny | permit} source [source-wildcard]
- **access-list** access-list-number {deny | permit}protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log]
- **access-list** access-list-number [**dynamic** dynamic-name [timeout minutes]]
- **access-template** [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
- **autocommand**
- **clear access-list counters** {access-list-number | name}
- **clear access-template** [access-list-number | name] [dynamic-name] [source] [destination]
- **ip access-group** {access-list-number | name}{in | out}
- **ip telnet source-interface**
- **show access-lists** [access-list-number | name]
- **show ip access-list** [access-list-number | name]
- **username** [name] **password** [password]

命令的定义

- access-class：access-class命令用来限制在Cisco路由器上特殊的一个VTY线与访问表指定的一个地址之间的进入和离开的VTY连接。这个线配置命令把指定的访问表[1-99]应用到一个VTY线。用关键词“in”限制进入的连接，用关键词“out”限制接出的连接。
- access-enable：基于前面定义的标准，这条可执行命令用来在动态访问表中创建一临时的访问表入口项。主机关键词告知IOS只允许访问那些产生telnet会话的特定主机。计时满关键词指定一空闲的计时期限。如果在这段时间内访问表入口项没被使用，则该访问表入口项被删除。如果访问表入口项被删除，用户再想访问网络就必须重新获得认证。
- access-list[1-99]：序号从1~99的访问表定义为标准访问表。标准访问表只是基于源IP地址来允许或拒绝报文。源IP地址是指发送报文的主机或网络的地址。源IP地址后附有一个通配符屏蔽码，用来指定哪些位应被忽略，哪些应该匹配。

通配符屏蔽码在本章的后面有更详细的定义。本命令是一条全局配置命令。

- access-list[100-199]：带有号码100~199的访问表定义为扩展访问表。扩展访问表可以设置为静态的或动态的。静态的为缺省设置，也可以用关键词“dynamic”设置为动态的。本章后面将会有对两者更详细的描述。扩展访问表用来允许或拒绝报文（基于多种因素，如：协议、源IP地址、目的IP地址、优先权、TOS和端口号），比标准访问表提供了更多的内容。扩展访问表允许登录，该登录创建了一提供关于匹配访问表的任何报文的登录信息。这个操作在访问表疑难解答时最有用。
- access-list[100-199][dynmaic]：带有号码100~199并且用关键词“dynamic”的访问表定义为动态扩展访问表。本命令为一全局配置命令。
- access-template：这条可执行命令使用户可以在路由器上手工配置一暂时的动态访问表。
- autocommand：当一个用户连接到一特定线路上时，这条全局配置命令将执行一条命令。

在本章后面配置动态访问表时会用到此命令。

- clear access-list counters：这条可执行命令清除所有访问表计数器，有些访问表用一些计数器来计算匹配某一特定表的每一条线的报文的个数。当然也可以指定访问表的名字和序号，缺省时，系统将清除所有计数器。
- clear access-template：这条可执行命令清除所有动态访问表入口项。
- ip access-group：基于在访问表中定义的标准，这条命令用来允许或拒绝一特定接口上的进入和流出的报文。这条接口配置命令把一指定的访问表 [1-199]应用于一个路由器接口。流入的报文用关键字“ in ”过滤，流出的报文用关键字“ out ”。
- ip telnet source-interface：这条全局配置命令使用户能够选择一个接口的一个地址作为telnet连接的源地址。缺省为：源地址是离目的地址最近的接口地址。
- show access-lists：这条可执行命令显示当前所有 IP访问表的内容，也可以指定具体的访问表。缺省的设置为：系统显示所有的扩展和标准访问表。
- username：这条全局配置命令用来定义一个基于用户的认证系统。

12.4 IOS要求

访问表最初出现在IOS 10.0，然而本章所描述的一些命令需要更高的版本。

12.5 实验48：标准IP访问表

12.5.1 所需设备

下面列出了本实验所需的设备：

1) 两台Cisco路由器，每台有一个Ethernet端口和一个串行接口；
2) 一台运行终端仿真程序的PC；
3) Cisco IOS 10.0或更高的；
4) 一根Cisco DTE/DCE交叉电缆；
5) 一根Cisco扁平电缆。

12.5.2 配置概述

这一配置将演示用标准访问表进行报文过滤。如图 12-2所示。

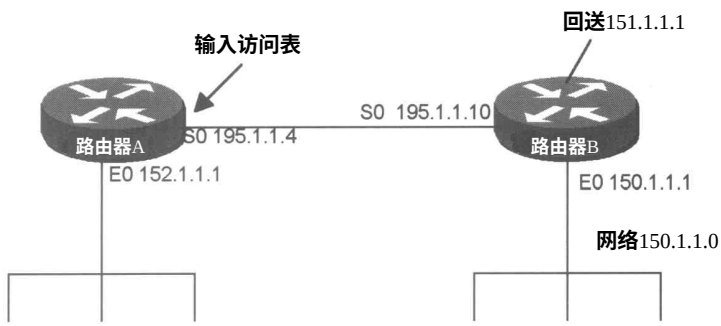

图12-2 基本访问表

路由器A将允许所有从网络150.1.1.0来的数据流通过，而拒绝所有其他网络来的数据。

路由器A和B用交叉电缆串行连接。路由器 B作为DCE为A提供时钟。IP地址的分配如图12-2中所示，B定义了一个回送接口（IP地址为151.1.1.1）作为测试点。

在路由器A的串行接口上应用接入访问表，允许所有从网络 150.1.1.0来的数据通过，拒绝其他数据通过。路由器 B用扩展的ping命令ping A的串行接口（195.1.1.4），从而从多个IP地址中为报文选源IP地址。

注意 访问表是一个应用于IP地址的、表述允许或拒绝的有序集合。路由器对照访问表一个个检查地址。访问表中的条件的顺序是很关键的，因为在一个访问表中第一次匹配是被使用（然后路由器停止测试条件是否满足）。如果没有发现任何匹配，报文就会被拒绝，因为在每一个访问表的最后就隐含着拒绝报文的通过。

12.5.3 路由器配置

下面给出了本例两台路由器的配置：

1. 路由器A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
!interface Ethernet0
 ip address 152.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the ethernet interface, allows the
              interface to stay up when it is not attached to a hub.
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip access-group 1 in←Applies access-list 1 to all inbound traffic on serial 0.
!
no ip classless
ip route 150.1.1.0 255.255.255.0 Serial0←Static route is used because no
                                         dynamic routing protocol is
                                         configured.
Ip route 151.1.1.1 255.255.255.255 Serial0←Static route is used because no
                                           dynamic routing protocol is
                                           configured
access-list 1 permit 150.1.1.0 0.0.0.255←Defines access-list 1 permitting
                     Wildcard mask ↑        traffic from network 150.1.1.0.
(Note: all other access implicitly denied)←All access-lists end with an
                                           implied deny all.
!
   line con 0
   line vty 0 4
    login
   !
   end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
```

```
interface Loopback0←Defines a virtual interface that will be used as a test
                    point.
 ip address 151.1.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 150.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the ethernet interface, allows the
              interface to stay up when it is not attached to a hub.
!
interface Serial0/0
 ip address 195.1.1.10 255.255.255.0
 clockrate 500000←Acts as DCE providing clock
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

12.5.4 监测配置

为了测试对路由器的配置，在B上用扩展ping命令ping A(195.1.1.4)，从回送接口为数据找出源地址。这只要在特权级别键入“ ping ”即完成。

```
routerB#ping
Protocol [ip]:
Target IP address: 195.1.1.4
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 151.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
```

在路由器A上用debug ip packet命令监视流入的报文。下面给出了该命令的输出，注意该报文已被拒绝，并且向B发送了一个ICMP主机不可达的信息。

```
IP: s=151.1.1.1 (Serial0), d=195.1.1.4, len 100, access denied
IP: s=195.1.1.4 (local), d=151.1.1.1 (Serial0), len 56, sending←Host unreachable
                                                          message.
```

下面给出了在 A上执行 show access-list 1 命令的输出。注意，通配符掩码允许网络150.1.1.0中的所有主机。

```
RouterA#show ip access-lists 1
Standard IP access list 1
permit 150.1.1.0, wildcard bits 0.0.0.255
```

12.6 实验49：扩展IP访问表

12.6.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，每台都有一个Ethernet端口和一个串行接口；

2) Cisco IOS 10.0或更高的；
3) 一台运行防真程序的PC；
4) 一根Cisco DTE/DCE交叉电缆；
5) 一根Cisco扁平电缆。

12.6.2 配置概述

这个配置将演示用扩展访问表进行报文过滤。路由器 A允许所有从PCC（150.1.1.2）到PCA（152.1.1.2）的数据通过，而将拒绝所有从PCC（150.1.1.2）到PCB（152.1.1.3）的数据通过。因为是对源IP地址和目的IP地址一起过滤，所以使用扩展访问表。

路由器A和B用交叉电缆串行连接。路由器B做为DEC向路由器A提供时钟。图12-3给出了IP地址的分配。在以太网接口，路由器A和B都定义了二级IP地址，用来作为测试点。

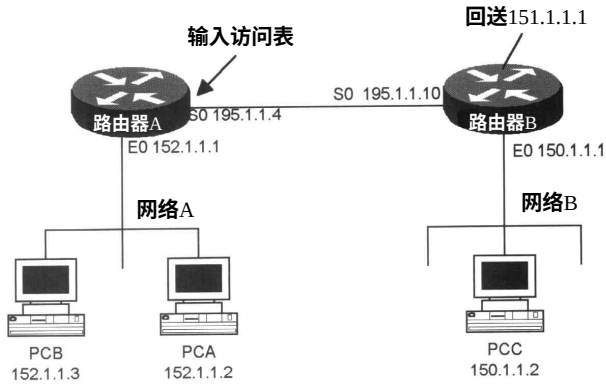

图12-3 扩展IP访问表

在A的串行接口应用接入访问表，允许从 PCC（150.1.1.2）到PCA的报文通过，拒绝PCC到PCB的数据通过。

注意 当创建一个访问表时，所有的入口项按它们进入的顺序排放。任何后来的入口项都放在访问表的结尾。创建访问表时一个比较好的策略是脱线编辑访问表，然后剪切或者粘帖它们到一个路由器配置，或者从一个服务器上TFTP它们。

12.6.3 路由器配置

下面给出了本例中两台路由器的配置：

1. 路由器A

```
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
interface Ethernet0
ip address 152.1.1.2 255.255.255.0 secondary←Secondary IP addresses are used
                                                as test points
 ip address 152.1.1.3 255.255.255.0 secondary
```

```
 ip address 152.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the ethernet interface,  allows the
              interface to stay up when it is not attached to a hub.
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip access-group 100 in←Applies access-list 100 to all inbound traffic on
                        serial 0.
!
no ip classless
ip route 150.1.1.0 255.255.255.0 Serial0←Static route is used because no dynamic
                                         routing protocol is configured.
ip route 151.1.1.1 255.255.255.255 Serial0

                                           Host specific is the same as
                                          ↓wildcard mask 0.0.0.0
access-list 100 permit ip host 150.1.1.2 host 152.1.1.2 log←Generates an
                 ↑Permit any IP packet      informational logging message
                  from 150.1.1.2 to         about any packet that matches the
                  152.1.1.2                 entry

access-list 100 deny  ip host 150.1.1.2 host 152.1.1.3 log←Generates an
!                ↑Deny any IP packet        informational logging message
                  from 150.1.1.2 to         about any packet that matches the
                  152.1.1.3                 entry

(Note: all other access implicitly denied)←All access-lists end with an
                                           implied deny all.
!
!
line con 0
line vty 0 4
 login
!
end
```

2. 路由器B

```
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
!interface Loopback0
 ip address 151.1.1.1 255.255.255.0←Virtual interface used as a test point
!
interface Ethernet0/0
 ip address 150.1.1.2 255.255.255.0 secondary←Secondary IP addresses are used
                                              as test points
 ip address 150.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the ethernet interface, allows the
              interface to stay up when it is not attached to a hub.
!
interface Serial0/0
 clockrate 500000←Acts as DCE providing clock
!
no ip classless
ip route 152.1.1.0 255.255.255.0 Serial0/0←Static route is used, because no
                                           dynamic routing protocol is
                                           configured.
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

12.6.4 监测配置

下面的例子，均是在路由器B上用扩展ping命令从在配置中定义的二级IP地址中为报文选择源地址。这条命令用来代替连在路由器B的局域网上的多台微机。

(1) 从路由器B，用源地址150.1.1.2 ping 152.1.1.3

在路由器A上执行debug ip packet命令，可以看到报文被拒绝，而一个ICMP主机不可达报文被发送。

```
IP: s=150.1.1.2 (Serial0), d=152.1.1.3, len 100, access denied
IP: s=195.1.1.4 (local), d=150.1.1.2 (Serial0), len 56, sending←ICMP host
                                                              unreachable
```

下面的例子给出了执行show ip access list命令的输出。注意输出显示定义了哪些访问表及与这些访问表分别对应的匹配数。

```
RouterA#show ip access-lists
Extended IP access list 100
permit ip host 150.1.1.2 host 152.1.1.2 log (5 matches)
deny ip host 150.1.1.2 host 152.1.1.3 log (105 matches)
```

下面的例子给出了执行log选项的输出。Log选项将产生一个关于任何与扩展访问表匹配的报文的运行记录的信息报文。

Logging选项作为一个关键词可以加到每个访问表描述的末尾。当应用访问表疑难解答时，information-logging报文是一个极好的工具。

```
SEC-6-IPACCESSLOGDP: list 100 denied icmp 150.1.1.2 -> 152.1.1.3 (0/0), 4 packets
```

(2) 从路由器B，用源地址150.1.1.2 ping 152.1.1.3。

在路由器A上执行debug ip packet命令，从输出结果可以看到报文允许通过。

```
IP: s=150.1.1.2 (Serial0), d=152.1.1.2, len 100, rcvd 7
```

下面的例子给出执行show ip access-list命令的输出;注意输出显示定义了哪些访问表及与这些访问表分别对应的匹配数。

```
RouterA#show ip access-lists
Extended IP access list 100
    permit ip host 150.1.1.2 host 152.1.1.2 log (308 matches)
    deny   ip host 150.1.1.2 host 152.1.1.3 log
```

12.7 实验50: 带有Established选项的扩展访问表

12.7.1 所需设备

下面列出了本实验所需的设备：

1) 两台Cisco路由器各有一个Ethernet端口和一个串行端口；
2) Cisco IOS 10.0或更高的；
3) 一台运行终端仿真程序的PC；
4) 一根Cisco扁平电缆；
5) 一根Cisco DTE/DCE交叉电缆。

12.7.2 概述

带有关键词established的扩展访问表允许内部的用户访问外部网络，而拒绝外部用户访问内部网络。而没带关键词established的标准访问表和扩展访问表就没有这个特性。

问题是标准访问表和基本的扩展访问表将拒绝所有匹配访问表标准的报文，即使报文是响应报文。在图12-4中，路由器A的串行接口应用一个标准访问表，拒绝所有外部数据与 PCA建立一连接，即使这个过程是安全的，也会阻止 PCA与Internet上的任何服务器建立连接。路由器A上的访问表也将会拒绝回到PCA的响应报文。

注意 当创建一个标准访问表或扩展访问表时，缺省的设置是在访问表最后放的是“拒绝所有”——这意味着任何不匹配访问表中入口项的条件的报文都将被拒绝。

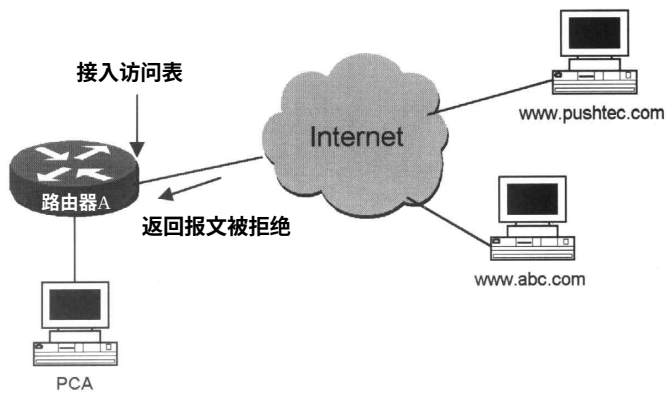

图12-4 Established连接

带有关键词established的扩展访问表允许从已建立的连接来的返回报文通过访问表。路由器查看TCP报文，如果ACK或RST位被设置为“1”，则报文被允许通过。

1) PCA向服务器www.pushtec.com发送HTTP报文。

2) 服务器www.pushtec.com响应。

3) 路由器A对报文应用访问表，如果返回报文中的 ACK或RST被置位，则报文允许通过。如果服务器www.pushtec.com试图与PCA建立一条链接，SYN位将被置位，并且报文也将被拒绝。同步段是TCP协议发送的第一个段，它用来同步准备打开一个新的链接的连接的两个端主机。

12.7.3 配置概述

这个配置将演示带有关键词 established的扩展访问表，路由器 A上的访问表将拒绝所有流向网络A的non-established的IP报文。

路由器A和B用交叉电缆串行联接。 B作为DCE为A提供时钟。IP地址的分配如图12-5中所示。在A的串行接口上应用接入访问表。

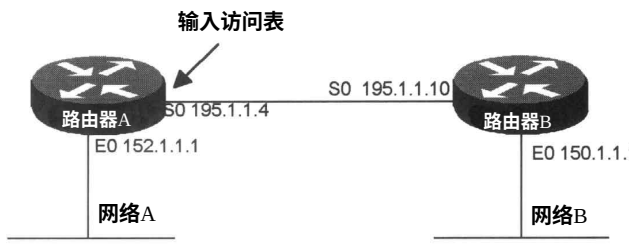

图12-5 带有Established选项的扩展访问表

12.7.4 路由器配置

下面给出了本例中的两台路由器的配置：

1. 路由器A

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
ip telnet source-interface Ethernet0←Sources all Telnet packets from E0 ip add
                                     152.1.1.1
!
interface Ethernet0
 ip address 152.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the ethernet interface; enables the
              interface to stay up when it is not attached to a hub
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip access-group 100 in←Applies access-list 100 to all inbound traffic on
                        serial 0.
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!

ip route 150.1.1.0 255.255.255.0 Serial0←Static route is used because no
                                         dynamic routing protocol is configured
ip route 151.1.1.1 255.255.255.255 Serial0←Static route is used because no
                                           dynamic routing protocol is configured
access-list 100 permit tcp any host 152.1.1.1 established log←Permit any traffic
                                                              destined for
                                                              152.1.1.1 with the
                                                              ACK or RST bit set.
access-list 100 deny ip any log←This statement is not needed. By default, all
                                traffic is denied. By adding this statement,
                                however, we can monitor how many packets
                                matched the access-list and were denied.
(Note: all other access implicitly denied)←All access lists end with an
                                           implied deny all.
!
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

2. 路由器B

```
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
interface Ethernet0
```

```
  ip address 150.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the Ethernet interface; allows the
              interface to stay up when it is not attached to a hub
!
interface Serial0
 ip address 195.1.1.10 255.255.255.0
clockrate 500000←Acts as DCE, providing clock

!
interface Serial1
 no ip address
 shutdown
!
ip route 152.1.1.0 255.255.255.0 Serial0←Static route is used because no dynamic
                                         routing protocol is configured

!
!
line con 0
line aux 0
line vty 0 4
 login←Allows telnet access to the router.
!
end
```

12.7.5 监测配置

为了测试本配置，在A了B之间建立telnet链接。配置路由器A，用Ethernet接口的IP地址做为远程通信报文的源地址。这个设置可以在 A上执行IP telnet source-interface e0命令来完成。

1) 用debug ip packet detailed命令监视IP报文流入还是离开路由器A。

2) 从A（152.1.1.1）Telnet B(150.1.1.1)。

下面的例子给出了在路由器 A上执行debug ip packet detailed命令的输出。注意所有从150.1.1.1到152.1.1.1的报文的ACK或RST已被置位。

```
IP: s=152.1.1.1 (local), d=150.1.1.1 (Serial0), len 44, sending
    TCP src=11004, dst=23, seq=682801374, ack=0, win=4288 SYN
IP: s=150.1.1.1 (Serial0), d=152.1.1.1, len 44, rcvd 4
    TCP src=23, dst=11004, seq=426675527, ack=682801375, win=2144 ACK SYN
IP: s=152.1.1.1 (local), d=150.1.1.1 (Serial0), len 40, sending
    TCP src=11004, dst=23, seq=682801375, ack=426675528, win=4288 ACK
    TCP src=11004, dst=23, seq=682801375, ack=426675528, win=4288 ACK PSH
IP: s=152.1.1.1 (local), d=150.1.1.1 (Serial0), len 40, sending
    TCP src=11004, dst=23, seq=682801384, ack=426675528, win=4288 ACK
IP: s=150.1.1.1 (Serial0), d=152.1.1.1, len 52, rcvd 4
    TCP src=23, dst=11004, seq=426675528, ack=682801375, win=2144 ACK PSH
```

下面的例子给出了log选项的输出，log操作产生一个关于任何与扩展访问表匹配的报文的logging信息报文。

从150.1.1.1来的回应报文与访问表100匹配并被允许通过。

```
%SEC-6-IPACCESS LOGP: list 100 permitted tcp 150.1.1.1(23) -> 152.1.1.1(11002),
                                                              1 packet
```

3) 用show ip access-list命令显示哪些访问表被配置，共有多少报文匹配访问表的标准。下面给出了命令的输出结果。注意 6个报文被允许， 1个被拒绝。这条命令在访问表疑难解答中非常有用，使你很快得知报文匹配那些线。

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

```
        permit tcp any host 152.1.1.1 established log (6 matches)
        deny   ip any any log (1 match)
```

4) 现在，试着在相反的方向建立一 telnet链接，从B（150.1.1.1）到A(152.1.1.1)。路由器B用Ethernet接口的IP地址作为所有telnet报文的源地址。

5) 用debug ip packet detailed命令监视IP报文进入还是离开路由器 A。下面的例子给出了执行结果。注意SYN已被置位，访问表只允许那些路由器 A决定的是否ACK或RST位已被置位的established链接。同步段（SYN）是TCP协议发送的第一段，它用来同步准备建立一个新链接的连接的两个端主机。而 ACK位由接收者置位从而向发送者表明数据已成功接收。 RST位（reset位）说明什么时候重新启动链接

```
IP: s=150.1.1.1 (Serial0), d=152.1.1.2, len 44, access denied
    TCP src=11004, dst=23, seq=2826185914, ack=0, win=2144 SYN
IP: s=195.1.1.4 (local), d=150.1.1.1 (Serial0), len 56, sending
    ICMP type=3, code=13
```

12.8 实验51：动态IP访问表

12.8.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，各有一Ethernet端口和一串行端口；
2) Cisco IOS 11.1或更高的；
3) 一台运行终端仿真程序的微机；
4) 一根Cisco DTE/DCE交叉电缆；
5) 一根Cisco扁平电缆。

12.8.2 概述

基于用户认证，动态访问表允许或拒绝数据经过。如果用户想通过路由器访问一台主机，用户必须首先telnet路由器并获得认证，一旦获得认证，路由器建立一临时访问表使用户能够到达目的主机。

通过Lock-and-key Security，可以指定允许哪些用户访问哪些源或目的主机，如图 12-6所示。

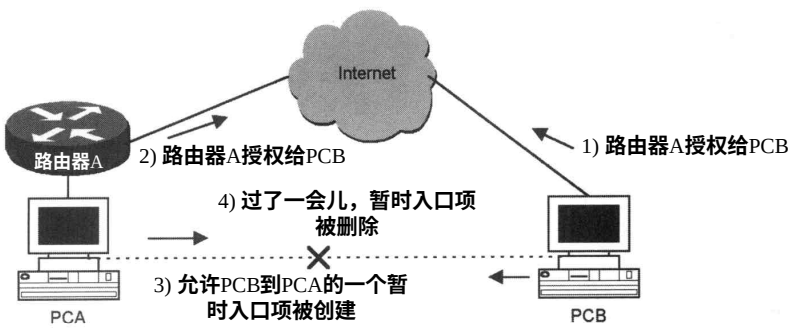

图12-6 Lock-and-key安全性

基于用户认证，在访问表中建立一临时的入口项。

12.8.3 Lock-and-key 的工作过程

1) PCB通过虚拟的终端接口远程登录到路由器 A。

2) 路由器A打开telnet对话框并提示用户输入用户名和口令。如果用户通过认证过程，则允许通过路由器访问。

3) PCB随后自动退出telnet对话框，动态访问表中也建立一临时入口项。这个临时的入口项，是基于用户认证的，这在配置过程中已做过定义。例如：可以配置访问表使 PCB只能远程访问到PCA，而拒绝所有其他的访问。

4) 然后从PCB来的数据流就能够通过路由器 A。

5) 预定义超时期后，路由器删掉临时的访问表。一旦删掉临时访问表，用户的数据再想通过路由器A就必须重新获得认证。

12.8.4 配置概述

如图12-7所示，这个配置将演示通过使用一动态扩展访问表获得的 lock-and key安全性。

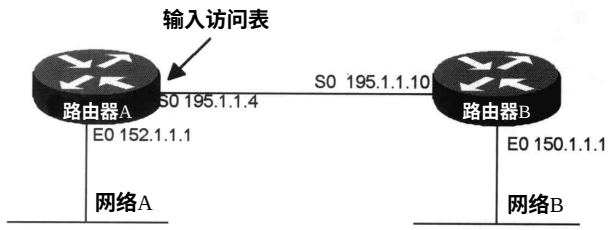

图12-7 Lock and-key安全性

路由器A根据用户名和口令验证登录，一旦路由器 B通过认证，则可以注册进入到 A，随后路由器A建立一个时间为 5分钟长的临时访问表入口项，使路由器 B（150.1.1.1）能够远程登录到A(152.1.1.1)。

路由器A和B通过交叉电缆串行连接。路由器 B作为DCE为路由器A提供时钟。 IP地址的分配如图12-7所示，在A的串行接口上应用一接入访问表。

12.8.5 路由器配置

下面给出了本例中两台路由器的配置：

1. 路由器A

```
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
!
username pcb password 0 pcb←Establish a username-based authentication system
                  Causes the specified command to be issued automatically
                ↓after the user logs in
username pcb autocommand access-enable timeout 5←If the access list entry is
                            ↑Adds the              not accessed within 5
                             temporary entry       minutes, it is automatically
                             to access-list.       deleted and requires the user
```

```
                                                    to authenticate again.

ip telnet source-interface Ethernet0←Sources all telnet packets from E0 ip add
                                        152.1.1.1

!
interface Ethernet0
 ip address 152.1.1.1 255.255.255.0
no keepalive←Disables the keepalive on the Ethernet interface and enables the
             interface to stay up when it is not attached to a hub

!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip access-group 100 in←Applies access-list 100 to all inbound traffic on
                        serial 0

 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!

no ip classless
ip route 150.1.1.0 255.255.255.0 Serial0←Static route is used because no dynamic
                                         routing protocol is configured
                                ↓dynamic-name
access-list 100 dynamic tempaccess permit tcp host 150.1.1.1 host 152.1.1.1 eq
      telnet log                                              ↑Only permit telnet
                                                               traffic between
                                                               150.1.1.1 and 152.1.1.1
access-list 100 permit tcp any host 195.1.1.4 eq telnet log←Telnet access must be
                                                             allowed to enable user
                                                             authentication.
access-list 100 deny ip any any log←This statement is not needed. By default, all
                                    traffic is denied. By adding this statement,
                                    however, we can monitor how many packets
                                    matched the access-list and were denied.

(Note: All other access implicitly denied)←All access lists end with an
                                           implied deny all.
!
line con 0
line aux 0
line vty 0 4
  login local←Enables local password checking at login
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
interface Ethernet0
  ip address 150.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the Ethernet interface; enables the
              interface to stay up when it is not attached to a hub

!
interface Serial0
 ip address 195.1.1.10 255.255.255.0
```

```
 clockrate 500000←Acts as the DCE, providing clock
!
interface Serial1
 no ip address
 shutdown
!
ip route 152.1.1.0 255.255.255.0 Serial0←Static route is used because no dynamic
                                          routing protocol is configured
!
line con 0
line aux 0
line vty 0 4
login←Enables telnet access to the router
!
end
```

12.8.6 监测配置

从路由器B到A(195.1.1.4)建立一远程登录链接以测试本配置。用用户名 PCB和口令PCB注册进入A。下面的例子给出一旦用户通过认证将会看到的结果。注意一旦键入口令， telnet链接就立即被断开。通过认证后，路由器 A建立临时访问表100。

```
RouterB#telnet 195.1.1.4
Trying 195.1.1.4 ... Open
User Access Verification
Username: pcb
Password: pcb
[Connection to 195.1.1.4 closed by foreign host]
```

下面的例子给出一在路由器A上执行show ip access-list命令的结果。注意临时的入口项已经加入到了访问表中。

```
RouterA#show ip access-lists
Extended IP access list 100
    Dynamic tempaccess permit tcp host 150.1.1.1 host 152.1.1.1 eq telnet log
       permit tcp host 150.1.1.1 host 152.1.1.1 eq telnet log idle-time 5 min.
    permit tcp any host 195.1.1.4 eq telnet log (72 matches)
    deny   ip any any log (1 match)
```

从路由器B（150.1.1.1）到152.1.1.1建立一telnet链接，路由器B配置Ethernet接口的IP地址为所有telnet报文的源地址，通过在A上执行ip telnet source-interface e0命令完成配置。

下面的例子是路由器A上的访问表log命令输出的一简单样本。 Log命令是在配置过程中加到访问表的一个操作。 Log关键词产生一个任何与扩展访问表匹配的报文 log信息报文。与临时的入口项匹配的从150.1.1.1来的telnet报文都加入到访问表100中。

```
%SEC-6-IPACCESSLOGP: list 100 permitted tcp 150.1.1.1(11010) -> 152.1.1.1(23), 1
 packet
```

telnet对话被允许，那么现在，在路由器 A上用下面的可执行命令从访问表中删除临时入口项。

```
clear access-template 100 tempaccess 150.1.1.1 0.0.0.0 152.1.1.1 0.0.0
```

用show ip access-list命令查看配置了哪些访问表和有多少报文与标准匹配。下面给出了命令的执行结果。注意临时入口项已从动态访问表中删掉。

```
RouterA#show ip access-lists
Extended IP access list 100
    Dynamic tempaccess permit tcp host 150.1.1.1 host 152.1.1.1 eq telnet log
```

```
permit tcp any host 195.1.1.4 eq telnet log (124 matches)
deny   ip any any log (1 match)
```

从路由器B（150.1.1.1）远程登录到152.1.1.1。注意这次连接失败了。PCB必须由路由器A重新认证才能telnet到152.1.1.1。

```
RouterB#telnet 152.1.1.1
Trying 152.1.1.1 ...
% Destination unreachable; gateway or host down
```

12.9 实验52：可控VTY 访问

12.9.1 所需设备

下面列出本实验所需设备：

1) 两台Cisco路由器各有一Ethernet端口和一个串行端口；
2) Cisco IOS 10.0或更高的；
3) 一台运行终端仿真程序的微机；
4) 一根Cisco DTE/DCE交叉电缆；
5) 一根Cisco扁平电缆。

12.9.2 概述

本实验演示了如何用访问表控制到路由器的 VTY连接。在一个production环境中，很有必要限制只有那些授权用户才能访问路由器，可以用口令认证和访问控制表完成这项功能。

基于源IP地址，访问控制表可以规定哪些主机访问路由器。路由器访问应该限定一些指定的工作站才能有权访问。一个好的实现方法是建立一台堡垒主机，只允许特定的一些 IP地址VTY访问自己的所有路由器。网络管理员telnet到堡垒主机，然后才能到外面特定的路由器。堡垒主机首先是一台计算机，它是安全防火墙的一部分，运行与一个组织外部的计算机互相通信的应用程序。

12.9.3 配置概述

本配置演示了如何用标准访问表控制对路由器的 VTY访问。路由器A将只允许从主机 150.1.1.1发出的VTY访问，所有其他的会话都会被拒绝。

路由器A和B用交叉电缆串行连接起来，路由器B作为DCE为A提供时钟。IP地址的分配如图12-8所示。

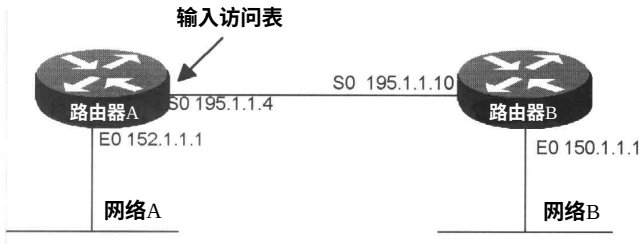

图12-8 VTY访问控制

在路由器A的串行接口应用一个接入访问表。

12.9.4 路由器配置

下面给出了本例中两台路由器的配置：

1. 路由器A

```
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
interface Ethernet0
  ip address 152.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the Ethernet interface; allows the
              interface to stay up when it is not attached to a hub
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
no ip classless
ip route 150.1.1.0 255.255.255.0 Serial0←Static route is used because no dynamic
                                          routing protocol is configured
access-list 1 permit 150.1.1.1←Standard access list permits access from host
                                150.1.1.1.
(Note: all other access implicitly denied)←All access lists end with an
                                          implied deny all.

!
line con 0
line aux 0
line vty 0 4
 access-class 1 in←Applies standard access list 1 to all inbound VTY
                   connections
 password cisco
 login
!
end
```

2. 路由器B

```
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
ip telnet source-interface Ethernet0
!
interface Ethernet0
  ip address 150.1.1.1 255.255.255.0
 no keepalive←Disables the keepalive on the Ethernet interface;  permits the
              interface to stay up when it is not attached to a hub

!
interface Serial0
 ip address 195.1.1.10 255.255.255.0
 clockrate 500000←Acts as DCE providing clock

!
interface Serial1
 no ip address
 shutdown
!
ip route 152.1.1.0 255.255.255.0 Serial0←The static route is used, because no
```

```
                                                    dynamic routing protocol is
                                                    configured.
!
line con 0
line aux 0
line vty 0 4
!
end
```

12.9.5 监测配置

从路由器B到A（195.1.1.4）建立一telnet链接以测试本次配置。在路由器B上执行ip telnet source interface Ethernet 0命令，定义telnet报文的源IP地址为150.1.1.1。

下面的代码示例给出了如果telnet连接成功，用户将会看到的内容：

```
RouterB#telnet 195.1.1.4
Trying 195.1.1.4 ... Open

User Access Verification
Password:
```

在路由器B上，再配置所有的telnet报文都从串行接口发出。这只需在全局配置模式下做下面的操作：

```
RouterA(config)#
no ip telnet source-interface Ethernet0
ip telnet source-interface serial0
```

那么，现在从路由器B远程登录到A（195.1.1.1）连接请求被拒绝，因为telnet报文的源地址已与路由器A上访问控制表不匹配。

```
RouterB#telnet 152.1.1.1
Trying 152.1.1.1 ...
% Connection refused by remote host
```

12.10 IP访问表故障查找

Cisco IOS为访问表疑难解答提供了许多工具。下面列出了一些关键的命令以及每条命令的部分执行结果采样。

show access-list 这条特权级可执行命令显示当前所有访问表的内容。也可以指定具体的访问表（根据序号）。

```
RouterA# show access-lists 1
Standard IP access list 1
    permit 150.1.1.1
```

show ip access-list 这条特权级可执行命令显示当前所有IP访问表的内容。也可以根据序号指定具体的某些IP访问表。

```
RouterA#show ip access-lists 1
Standard IP access list 1
permit 150.1.1.0, wildcard bits 0.0.0.255
```

clear access list counters 有些访问表用一些计数器来统计通过访问表每条线的报文个数。用clear access list counters命令可以为某一特定访问表将计数器复位到0。

```
RouterA#clear access-list counters
```

debug ip packet 这条可执行命令显示有关路由器收到的、产生的或转发的报文的信息。

当在路由器上应用访问表时，从调试命令的输出可得知报文是被允许还是被拒绝。

```
RouterA#Debug ip packet
IP: s=150.1.1.2 (Serial0), d=152.1.1.3, len 100, access denied
IP: s=195.1.1.4 (local), d=150.1.1.2 (Serial0), len 56, sending
```

12.11 结论

访问表是Cisco IOS的一个完整部分，它使路由器根据制定的标准作出决策。本章主要描述了用标准和扩展访问表对报文的过滤和对路由器访问的控制。当然，访问表还有很多其他的功能本章并没有讨论，例如，过滤路由更新、决定 DDR有趣数据流和流量控制等。这些高级的内容将在它们各自的章节进行讨论。