第 4 章　路由器安全管理

本章学习目标

本章介绍路由器的安全管理方法，包括 Telnet 会话管理、访问控制列表、路由器管理方式等。通过本章的学习，读者应该掌握以下内容:

- 掌握呼入、呼出 Telnet 会话管理方法
- 掌握访问控制列表的基本概念和工作原理
- 掌握标准访问控制列表和扩展访问控制列表的命令格式和配置方法
- 掌握路由器的安全管理相关配置
- 掌握路由器的 HTTP、HTTPS、SSH 管理方式的配置方法

4.1　Telnet 会话管理

路由器上提供的 telnet 命令使我们在从本地终端远程登录到路由器上后，还可以进一步登录到其他网络设备并对其进行配置、管理。这无疑大大扩展了网络管理人员的管理范围，使设备的远程管理变得更容易。但是，另一方面，这也给路由器等网络互连设备的安全管理带来了负面的影响。本节讲述如何对路由器上的 Telnet 会话进行管理。

4.1.1　呼出 Telnet 会话管理

虚拟终端协议 telnet 用来远程登录到目标主机，在绝大多数网络设备中都内置了 Telnet 功能。我们可以从一台网络设备远程登录到另一台网络设备进行设备管理。如图 4-1 所示，是在路由器 R1 上远程登录到交换机 Sw1 的过程。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ... Open


User Access Verification

Password:
Sw1>
```

图 4-1　远程登录

如果设置了 IP HOST 主机地址解析或指定了 DNS 服务器，也可以直接输入目标设备的名称。如图 4-2 所示。

当登录到目标主机后，可以使用 exit 命令断开当前 Telnet 会话回到本地设备，也可以使用“退出序列”不切断当前 Telnet 连接而暂时回到原设备。方法是：同时按键盘上的 Ctrl+Shift+6 快捷键，然后释放这些键，再键入字母“x”。

```
Sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#ip host R1 12.0.0.1
Sw1(config)#end
Sw1#r1
Translating "r1"
Trying R1 (12.0.0.1)... Open


User Access Verification

Password:
R1>
```

图 4-2　使用主机名直接远程登录

回到本地设备后，可以使用命令 show sessions 显示从当前设备发出的所有呼出 Telnet 会话，如图 4-3 所示。其中，第 4 行连接编号前的“*”表示最近的一次 Telnet 会话。

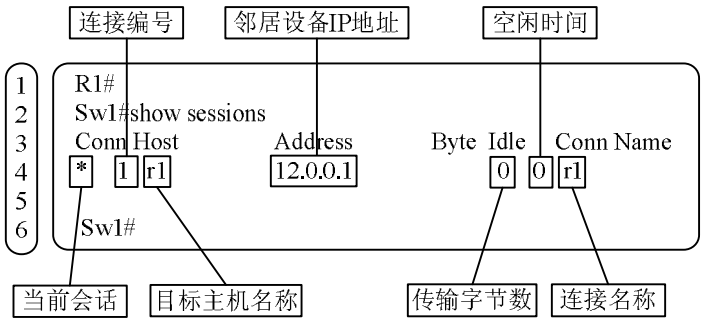

图 4-3　显示呼出 Telnet 会话

回到本地设备后，可以输入 CLI 命令对本地设备进行配置、管理，也可以在 CLI 提示符后直接按“回车”键返回最近的一次 Telnet 会话过程。还可以键入命令 disconnect 断开与远程目标主机的 Telnet 会话。

如图 4-4 所示，当输入 disconnect 命令并确认后可以从本地断开到目标主机的 Telnet 连接。

我们可以在原设备同时发起到不同目标主机的多个 Telnet 会话。如图 4-5 所示，是在交换机 Sw1 上分别远程登录到路由器 r1、r2 后，在本地设备 Sw1 显示出的 Telnet 会话情况汇总。

```
Sw1#
[Resuming connection 1 to r1 ... ]

R1#
Sw1#disconnect
Closing connection to r1 [confirm]
Sw1#
```

图 4-4　断开呼出 Telnet 会话

```
Sw1#show sessions
Conn Host          Address          Byte  Idle  Conn Name
    1  r1          12.0.0.1            0     0  r1
*   2  r2          23.0.0.3            0     0  r2

Sw1#
```

图 4-5　同时发起多个 Telnet 会话

这时，如果按“回车”键则返回从本地发出的最近一次 Telnet 会话过程，即图 4-5 中标有“*”的到路由器 r2 的 Telnet 连接。

如果想要返回到指定的那一次 Telnet 会话过程，可以使用 resume 命令并在 resume 命令后的参数中指明 Telnet 连接编号或连接名称，还可以在提示符后直接输入连接编号并按“回车”

键返回到对应的 Telnet 会话过程，如图 4-6 所示。

```
Sw1#show sessions
Conn Host            Address          Byte  Idle Conn Name
     1  r1           12.0.0.1            0     2  r1
*    2  r2           23.0.0.3            0     2  r2

Sw1#resume r1
[Resuming connection 1 to r1 ... ]

R1>
Sw1#resume 2
[Resuming connection 2 to r2 ... ]

R2>
Sw1#show sessions
Conn Host            Address          Byte  Idle Conn Name
     1  r1           12.0.0.1            0     0  r1
*    2  r2           23.0.0.3            0     0  r2

Sw1#resume
[Resuming connection 2 to r2 ... ]

R2>
```

图 4-6　返回某次 Telnet 会话过程

同理，在利用命令 disconnect 断开 Telnet 连接时，也需要指定要断开的 Telnet 会话连接编号或连接名称，如图 4-7 所示。否则，将断开最近一次 Telnet 会话过程。

```
Sw1#show sessions
Conn Host            Address          Byte  Idle Conn Name
     1  r1           12.0.0.1            0     3  r1
*    2  r2           23.0.0.3            0     0  r2

Sw1#disconnect 1
Closing connection to r1 [confirm]
Sw1#show sessions
Conn Host            Address          Byte  Idle Conn Name
*    2  r2           23.0.0.3            0     0  r2

Sw1#
```

图 4-7　断开指定 Telnet 连接

4.1.2　呼入 Telnet 会话管理

网络环境中的路由器、交换机等也可以作为被管理设备接受远程主机的呼入 Telnet 连接。

当有远程主机 Telnet 到本地设备时，可以使用命令 show users 查看呼入 Telnet 会话情况，包括远程主机登录的线路编号、线路名称、登录用户名称（仅当路由器要求本地认证时显示，见 4.3.1 节）、主机空闲时间、登录远程主机 IP 地址等内容。如图 4-8 所示。

图 4-8 中的线路编号采用的是绝对线路编号（绝对线号，参见 10.3.5 节）。线路名称采用的是相对线路编号（相对线号）。如 con 0 表示控制台线路，vty 0 表示第一条虚拟终端线路等。

有时，出于管理的需求可能需要断开远程主机的 Telnet 连接。这时，需要使用 clear line 命令。如图 4-9 所示，是采用相对线路编号断开远程 Telnet 连接的例子。而图 4-10 则是采用

绝对线号断开远程 Telnet 连接的例子。

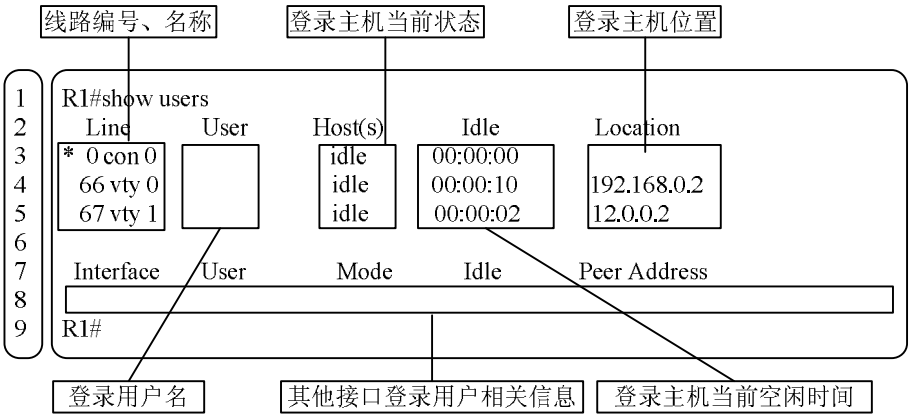

图 4-8　显示呼入 Telnet 连接

```
R1#show users
   Line      User       Host(s)     Idle         Location
*  0 con 0              idle        00:00:00
  66 vty 0              idle        00:16:02    192.168.0.2
  67 vty 1              idle        00:07:05    12.0.0.2

  Interface    User           Mode       Idle     Peer Address

R1#clear line vty 0
[confirm]
 [OK]
R1#show users
   Line      User       Host(s)     Idle         Location
*  0 con 0              idle        00:00:00
  67 vty 1              idle        00:07:12    12.0.0.2

  Interface    User           Mode       Idle     Peer Address
```

图 4-9　采用相对线路编号断开远程 Telnet 连接

```
R1#show users
   Line      User       Host(s)     Idle         Location
*  0 con 0              idle        00:00:00
  67 vty 1              idle        00:07:12    12.0.0.2

  Interface    User           Mode       Idle     Peer Address

R1#clear line 67
[confirm]
 [OK]
R1#show users
   Line      User       Host(s)     Idle         Location
*  0 con 0              idle        00:00:00

  Interface    User           Mode       Idle     Peer Address
```

图 4-10　用绝对线路编号断开远程 Telnet 连接

当在本地主机采用 clear line 命令断开远程 Telnet 连接后，远程设备会收到“由外部主机

关闭”的消息。如图 4-11 所示。

```
R1#
[Connection to r1 closed by foreign host]
Sw1#
```

图 4-11　“由外部主机关闭”消息

如果远程设备是 Windows 系统，则会显示“失去了跟主机的连接”，如图 4-12 所示。

图 4-12　“失去了跟主机的连接”消息

4.2　访问控制列表——ACL

4.2.1　访问控制列表概述

1. 访问控制列表概述

访问控制列表（Access Control List，ACL）是控制流入、流出路由器数据包的一种方法。它通过在数据包流入路由器或流出路由器时进行检查、过滤达到流量管理的目的。

访问控制列表不但可以起到控制网络流量、流向的作用，而且在很大程度上起到保护网络设备、服务器的关键作用。作为外网进入企业内网的第一道关卡，路由器上的访问控制列表成为保护内网安全的有效手段。

此外，在路由器的许多其他配置任务中都需要使用访问控制列表，如网络地址转换（Network Address Translation，NAT）、按需拨号路由（Dial on Demand Routing，DDR）、路由重分布（routing redistribution）、策略路由（Policy-Based Routing，PBR）等很多场合都需要使用访问控制列表。

2. 配置访问控制列表

访问控制列表是一个有序的语句集合，它通过匹配报文信息与访问列表参数，来允许报文或拒绝报文通过某个接口。因此，访问控制列表也被称为包过滤器。

配置访问控制列表需要两个步骤。第一步，定义允许或禁止报文的描述语句（访问列表）；第二步，将访问列表应用到路由器的具体接口（应用访问组）。这样，当数据包出入相应的接口时，路由器将检查数据包的类型并按照预先定义的访问控制列表对数据包进行处理：放行或丢弃。

有不同类型的访问控制列表。访问控制列表按照号码的范围划分为不同的类别，分别用于不同的协议和选项。表 4-1 列出了使用访问控制列表的协议以及协议有效的访问控制列表号码范围。

表 4-1 通过编号指定的访问列表所支持的协议

协议	范围
标准 IP 协议	1～99
扩展 IP 协议	100～199
Ethernet 类型码	200～299
DECnet	300～399
XNS	400～499
扩展 XNS	500～599
AppleTalk	600～699
Ethernet 地址	700～799
IPX	800～899
扩展 IPX	900～999
IPX SAP	1000～1099
MAC	1100～1199
IPX 汇总地址	1200～1299

在 IOS 12.0 版本后增加了标准 IP 协议及扩展 IP 协议的表号范围：

- 标准 IP 协议：1300～1999
- 扩展 IP 协议：2000～2699

每种协议都有用于提供包过滤的特定任务和规则。这里主要讲解 IP 访问控制列表。

有两种基本的 IP 访问控制列表：标准 IP 访问控制列表和扩展 IP 访问控制列表。标准 IP 访问控制列表仅依据 IP 数据包的源地址来决定是否过滤数据包。扩展 IP 访问控制列表不但可以检查源地址、目标地址，而且可以检查源和目标的端口号等字段，因此有更大的灵活性，应用也更广泛。

4.2.2 标准 ACL 配置方法

1. 标准 IP 访问控制列表语句

标准 IP 访问控制列表的命令格式为：

```
ACCESS-LIST access-list-number {DENY|PERMIT|REMARK} {SOURCE [source-wildcard]|ANY}
```

标准 IP 访问控制列表的号码（access-list-number）范围介于 1～99 之间。可以使用这个范围之内的任意号码。下一个关键字中的 DENY|PERMIT 指出该访问控制列表是允许还是拒绝数据包（REMARK 关键字用来对 ACL 语句进行描述，路由器在执行检查时会跳过含有 REMARK 关键字的 ACL 语句）。最后，可以选择主机或网络的源地址，或者使用关键字 ANY。

要匹配某个主机，需要输入该主机的 IP 地址。要匹配某个网络，则需要输入网络号，后面跟上通配符掩码。要匹配所有的网络和主机，需要使用关键字 ANY。这里，通配符掩码与

源地址或目标地址一起来定义要匹配的网络范围。因此，正确理解并使用它非常重要。

像子网掩码标明 IP 地址的哪些位属于网络号一样，通配符掩码标明为了判断匹配地址，它需要检查 IP 地址中的哪些位。将通配符掩码位设为 1，表示 IP 地址中的对应位既可以是 1 也可以是 0。将通配符掩码位设为 0，则表示 IP 地址中对应位必须被精确匹配。

例如：210.31.10.0 0.0.0.255 表示 IP 地址的前 3 个位域（Octets）必须是 210.31.10，而最后一个位域无所谓，是什么值都可以，即 1～255 均可。因此，这个例子表示 210.31.10.0 整个网段。

又如：210.31.10.1 0.0.0.0 表示 IP 地址中的每一位都必须精确匹配。即必须是一台 IP 地址为 210.31.10.1 的单机。这时，也可以用另外一种形式来表示：host 210.31.10.1。

再如：0.0.0.0 255.255.255.255 则表示任何主机地址，这时往往用一个省略的写法：ANY 来表示任意主机。

2. IP 访问控制组语句

定义好了 IP 访问控制列表语句后，需要将 IP 访问控制列表应用到具体接口。

首先，进入路由器某个接口的接口配置模式，如 interface serial 0/0。接下来输入 IP 访问控制组语句：

```
IP ACCESS-GROUP access-list-number {IN|OUT}
```

其中，access-list-number 是在前一步中定义的 IP 访问控制列表表号，关键字 IN|OUT 表示对流入还是流出（也称为入站/出站）路由器的数据包进行检查。

3. 标准 IP 访问控制列表配置实例 1

下面，我们用例子来说明标准 IP 访问控制列表的用法。

在如图 4-13 所示的网络环境中，路由器有两个接口，以太网接口 ethernet 0 连接内网。内网用户通过串行接口 serial 0 访问 Internet。假设在系统调试期间，我们只想允许 IP 地址为 210.31.10.20 的服务器访问 Internet，禁止其他 PC 机对 Internet 的访问。可以按照以下的步骤设置 ACL。

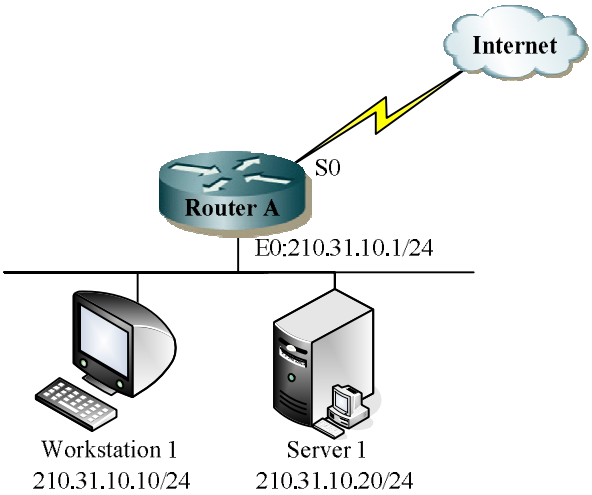

图 4-13　实例 1 的网络拓扑结构

（1）在路由器的全局配置模式下输入访问控制列表命令：access-list 1 permit host

210.31.10.20，允许 IP 地址为 210.31.10.20 的主机。

（2）在路由器的全局配置模式下输入访问控制列表命令：access-list 1 deny any，禁止所有其他主机。

（3）在路由器的全局配置模式下输入命令：interface ethernet 0，进入接口配置模式。

（4）在路由器的接口配置模式下输入访问控制组命令：ip access-group 1 in，设置在接口 ethernet 0 的入站方向按 1 号访问控制列表对数据包进行过滤。

4. 标准 IP 访问控制列表配置实例 2

在如图 4-14 所示的网络环境中，路由器有三个接口，以太网接口 ethernet 0 连接内网 210.31.10.0/24，ethernet 1 连接内网 210.31.20.0/24。所有内网用户通过串行接口 serial 0 访问 Internet。假设在系统调试期间，我们只想允许以太网接口 ethernet 0 所连接的内网用户访问 Internet，禁止其他网段对 Internet 的访问。

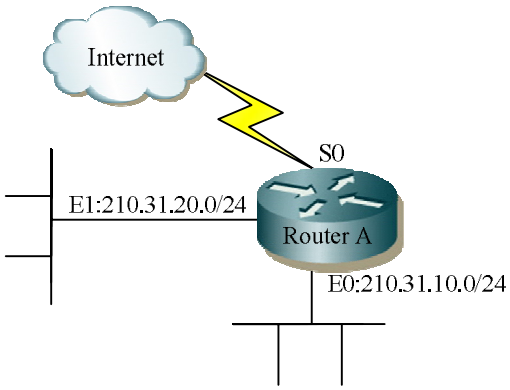

图 4-14　实例 2 的网络拓扑结构

可以按照以下的步骤设置 ACL。

（1）在路由器的全局配置模式下输入访问控制列表命令：access-list 1 permit 210.31.10.0 0.0.0.255，允许在 210.31.10.0/24 网段的主机访问。

（2）在路由器的全局配置模式下输入访问控制列表命令：access-list 1 deny any，禁止所有其他网段的主机。

（3）在路由器的全局配置模式下输入命令：interface serial 0，进入接口配置模式下。

（4）在路由器的接口配置模式下输入访问控制组命令：ip access-group 1 out，设置在接口 serial 0 的出站方向按 1 号访问控制列表对数据包进行过滤。

5. 需要注意的问题

在配置 IP 访问控制列表时需要特别注意以下问题：

- IP 访问控制列表是允许或禁止语句的集合。对于每个数据包，路由器顺序检查访问控制列表中的每个规则。
- 如果遇到 IP 数据包匹配某条语句，则跳出访问控制列表语句并执行放行或阻塞数据包的操作。
- 如果到达了访问控制列表的底端（最后一个访问控制列表语句）仍未找到与该数据包匹配的语句，则丢弃该数据包。即所有访问控制列表的最后有一个隐含的 DENY

ANY。所以，应保证每个访问控制列表都必须至少包含一个 PERMIT 语句；或在访问控制列表的底端明确地用语句指出对都不匹配的数据包的操作(是允许还是禁止)。

- 访问控制列表建立后，任何对该表语句的增加都被放在表的末端。这表示无法有选择地对访问控制列表中的个别语句进行修改、删除。因此，如果想要编辑访问控制列表，可以将 ACL 语句粘贴到“记事本”等文本编辑器中编辑后再重新粘贴到路由器（注意先删除原有的 ACL 语句)。
- 访问控制列表只对流入、流出路由器的流量进行过滤，无法对路由器本身产生的流量进行过滤。

4.2.3　扩展 ACL 配置方法

1. 扩展 IP 访问控制列表语句

扩展 IP 访问控制列表的命令格式为：

```
ACCESS-LIST  access-list-number  {DENY|PERMIT|REMARK}  protocol  source
source-wildcard destination destination-wildcard option
```

扩展 IP 访问控制列表的号码（access-list-number）范围介于 100～199 之间。可以使用这个范围之内的任意号码。和标准 IP 访问控制列表一样，下一个关键字指出该访问控制列表是允许还是拒绝数据包或者是对 ACL 语句的描述。接下来的 protocol 关键字指明要匹配使用何种协议的数据包，如 TCP、UDP、ICMP、IP 等。接下来，可以选择主机或网络的源地址、目标地址及通配符掩码，或者使用关键字 ANY。最后，是一些进一步定义数据包特征的可选项。

2. IP 访问控制组语句

和标准 IP 访问控制列表一样，定义好扩展 IP 访问控制列表语句后，需要将 IP 访问控制列表应用到具体接口。首先，进入路由器某个接口的接口配置模式，如 interface serial 0/0。接下来输入 IP 访问控制组语句：

```
IP ACCESS-GROUP access-list-number {IN|OUT}
```

其中，access-list-number 是在前一步中定义的 IP 访问控制列表，关键字 IN|OUT 表示对入站还是出站的数据包进行检查。

3. 扩展 IP 访问控制列表实例

下面，我们用一个例子来说明扩展 IP 访问控制列表的设计方法。

在如图 4-15 所示的网络结构中，路由器 A 一端的局域网 210.31.225.0/24、210.31.226.0/24 上的用户通过路由器 A 自己的串行接口 serial 0 连到路由器 B 的串行接口 serial 0，并通过路由器 B 的 serial 1 接口接入 Internet；同时通过路由器 B 的以太网接口 ethernet 0 接口与路由器 B 一侧的局域网 210.31.224.0/24 互连。

要求路由器 A 一端的局域网用户可以访问 Internet；同时只允许路由器 A 一端的局域网 210.31.225.0/24 上的用户访问路由器 B 一侧的服务器 210.31.224.11 上的 Telnet 服务。只允许路由器 A 一端的局域网 210.31.226.0/24 上的用户访问路由器 B 一侧的服务器 210.31.224.11 上的 WWW 服务。允许 210.31.0.0/16 网段的用户使用 ping 命令（使用协议 ICMP）测试到路由器 B 一侧局域网的连通性。除此之外到路由器 B 一侧局域网的所有通信都不允许。

首先，可以设计如下的访问控制列表：

- access-list 101 permit tcp 210.31.225.0 0.0.0.255 host 210.31.224.11 eq Telnet

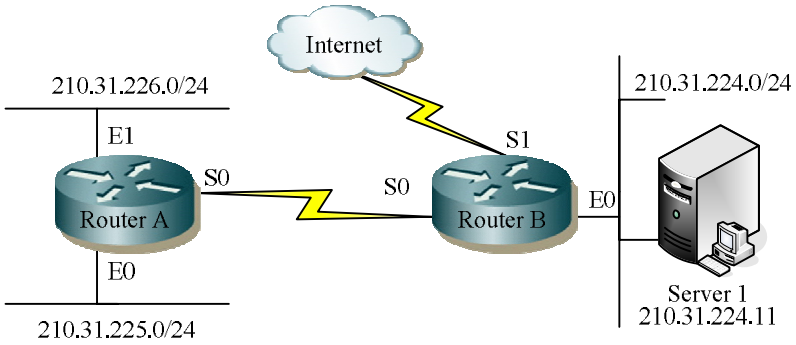

图 4-15　例 3 的网络拓扑结构

允许源自 210.31.225.0/24 网段的、以 TCP 协议方式访问服务器 210.31.224.11 上运行的 Telnet 服务的数据包。因为 Telnet 协议使用 TCP 的 23 端口，所以上述命令也可写为：

```
access-list 101 permit tcp 210.31.225.0 0.0.0.255 host 210.31.224.11 eq 23
```

- access-list 101 permit tcp 210.31.226.0 0.0.0.255 host 210.31.224.11 eq WWW

允许源自 210.31.226.0/24 网段的、以 TCP 协议方式访问服务器 210.31.224.11 上运行的 WWW 服务的数据包。因为 http 协议使用 TCP 的 80 端口，所以上述命令也可写为：

```
access-list 101 permit tcp 210.31.226.0 0.0.0.255 host 210.31.224.11 eq 80
```

- access-list 101 permit icmp 210.31.0.0 0.0.255.255 any

允许源自 210.31.0.0/16 网段的任何协议类型为 icmp 的数据包。因为 ping 命令使用 icmp 协议，所以这条访问控制列表语句的意义是允许 210.31.0.0/16 网段的主机使用 ping 命令对路由器 B 一侧局域网的连通性进行测试。

- access-list 101 deny ip any any

除以上语句规定外的所有数据包都被禁止（丢弃）。

然后，将定义好的访问控制列表应用到路由器 B 的以太网接口 ethernet 0 接口：

- interface ethernet 0

进入接口配置模式。

- ip access-group 101 out

定义访问控制组命令，按照定义好的 101 号访问控制列表对从以太网接口 ethernet 0 输出的数据包进行过滤。

4. 需要注意的问题

在配置扩展 IP 访问控制列表时还需要注意以下问题：

- 在访问控制列表中除了可以用“eq”关键字指出单一的端口号外，也可以规定端口号的范围。如用“gt 1024”表示端口号大于 1024；用“lt 1024”表示端口号小于 1024；而“range 100 200”则表示端口号介于 100 和 200 之间。
- 一定要牢记，在每个访问控制列表的底端都有一个默认的“DENY ANY”。所以，建议在每个访问控制列表的最后一条语句明确地指出对其余通信量的处理方式。

4.2.4　命名访问控制列表

当路由器上的各种 ACL 逐渐增多时，有时候我们会忘记某一组 ACL 的作用。为了解决

类似的问题，在 IOS 11.2 版本后，可以使用命名访问控制列表，即命名 ACL。

命名访问控制列表也分为标准命名访问控制列表和扩展命名访问控制列表。不管是什么类型的命名访问控制列表，其配置步骤都一样，需要两步：配置访问控制列表语句和配置访问控制组语句。

1. 标准命名访问控制列表

标准命名访问控制列表语句的命令格式为：

```
ip access-list standard aclname
```

标准命名访问控制组语句的命令格式为：

```
ip access-group aclname [in|out]
```

如图 4-16 所示，是采用标准命名访问控制列表配置 4.2.2 节中实例 1 的步骤。

```
Router(config)#ip access-list standard stdacl
Router(config-std-nacl)#permit host 210.31.10.20
Router(config-std-nacl)#deny any
Router(config-std-nacl)#exit
Router(config)#interface Ethernet 0
Router(config-if)#ip access-group stdacl in
```

图 4-16　标准命名访问控制列表配置实例

2. 扩展命名访问控制列表

扩展命名访问控制列表语句的命令格式为：

```
ip access-list extended aclname。
```

扩展命名访问控制组语句的命令格式为：

```
ip access-group aclname [in|out]。
```

如图 4-17 所示，是采用扩展命名访问控制列表配置方法配置 4.2.3 节中实例的步骤。

```
R1(config)#ip access-list extended extacl1
R1(config-ext-nacl)#permit tcp 210.31.225.0 0.0.0.255 host 210.31.224.11 eq telnet
R1(config-ext-nacl)#permit tcp 210.31.226.0 0.0.0.255 host 210.31.224.11 eq www
R1(config-ext-nacl)#permit icmp 210.31.0.0 0.0.255.255 any
R1(config-ext-nacl)#deny ip any any
R1(config-ext-nacl)#exit
R1(config)#int Ethernet 0
R1(config-if)#ip access-group extacl1 out
```

图 4-17　扩展命名访问控制列表配置实例

使用命名访问控制列表的另一个好处是可以对现有的命名 ACL 进行修改。如图 4-18 所示，是删除图 4-18 中的 icmp 相关控制语句。

4.2.5　ACL 日志

当一组 ACL 配置完成之后，应该经常对其工作状况进行检查。

命令 show [ip] access-lists 用来查看 ACL 日志的内容。如果该命令后面没有任何参数，则显示出路由器所定义的所有 ACL 日志信息，也可以显示指定的 ACL 日志。如图 4-19 所示，显示了编号为 102 的 ACL 日志信息。

```
R1#show running-config | begin ip access-list
ip access-list extended extacl1
 permit tcp 210.31.225.0 0.0.0.255 host 210.31.224.11 eq telnet
 permit tcp 210.31.226.0 0.0.0.255 host 210.31.224.11 eq www
 permit icmp 210.31.0.0 0.0.255.255 any
 deny   ip any any
!
… …
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended extacl1
R1(config-ext-nacl)#no  permit icmp 210.31.0.0 0.0.255.255 any
R1(config-ext-nacl)#end
R1#show running-config | begin ip access-list
ip access-list extended extacl1
 permit tcp 210.31.225.0 0.0.0.255 host 210.31.224.11 eq telnet
 permit tcp 210.31.226.0 0.0.0.255 host 210.31.224.11 eq www
 deny   ip any any
!
… ...
```

图 4-18　修改命名 ACL

```
R1#show access-lists 102
Extended IP access list 102
    permit ip 219.148.95.128 0.0.0.127 any (200729 matches)
    deny tcp any host 210.31.235.129 eq www (2511 matches)
    deny tcp any any range 135 139 (202078 matches)
    deny udp any any range 135 netbios-ss (3231 matches)
    deny tcp any any eq 445 (3446978 matches)
    deny tcp any any eq 593
    deny tcp any any eq 4444 (587 matches)
    deny tcp any any eq 1434 (9308 matches)
    deny tcp any any eq 2002 (2729 matches)
    deny tcp any any eq 1978 (12121 matches)
    deny tcp any any eq 4156 (811 matches)
    permit ip any any (172288130 matches)
R1#
```

图 4-19　用 show access-lists 命令检查 ACL 的工作日志

从图 4-19 中可以看到路由器收到的满足某条 ACL 条件的数据包数量。如屏蔽了 587 个采用 TCP 协议、目的端口号是 4444 的数据包；屏蔽了 9308 个采用 TCP 协议、目的端口号是 1434 的数据包等。

```
R1(config)#ip access-list extended NO_TELNET_FROM_LAN
R1(config-ext-nacl)#deny   tcp 192.168.0.0 0.0.0.255 any eq telnet log
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#end
R1#
```

图 4-20　ACL 语句中的关键字“log”

在上述 ACL 日志中虽然可以看到某条 ACL 被命中的次数，却不能记录命中此条 ACL 的

数据包来源等信息。我们可以通过 ACL 语句中的关键字“log”来将命中 ACL 的事件集中记录到路由器系统日志中，如图 4-20 所示。

```
R1#show logging
Syslog logging: enabled (9 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled)
    Console logging: level debugging, 49 messages logged, xml disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 3 messages logged, xml disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 53 message lines logged

Log Buffer (4096 bytes):

*Mar  1 02:05:05.219: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 02:05:15.079: %SEC-6-IPACCESSLOGP: list NO_TELNET_FROM_LAN denied tcp 192.168.0.2(1407) -> 3.3.3.3(23), 1 packet
*Mar  1 02:05:34.955: %SEC-6-IPACCESSLOGP: list NO_TELNET_FROM_LAN denied tcp 192.168.0.2(1408) -> 3.3.3.3(23), 1 packet
```

图 4-21　显示路由器系统日志

如图 4-21 所示，是使用命令 show logging 显示路由器系统日志的输出结果。

注意：必须在全局配置模式下使用命令 logging on 打开日志功能，并使用命令 logging buffered 开启日志缓存功能才能将上述 ACL 命中事件记录在日志缓存中，如图 4-22 所示。

```
R1#configure terminal
Enter configuration commands, one perline. End with CNTL/Z.
R1(config)#logging on
R1(config)#logging buffered
R1(config)#end
R1#
```

图 4-22　打开日志缓存功能

4.3　路由器的安全管理

处在园区网内网、外网间的路由器，其自身安全的重要性不言而喻。因此必须对路由器的访问方式、访问源位置等加以限制以保证路由器自身的安全。

4.3.1　本地登录认证

默认情况下，对虚拟终端线的登录认证（Authentication）方式是简单的密码认证（通过线命令 login 启用此功能，默认启用），即“What do you know?”的认证方式。为了增强安全性及增加审计的可能性，一般建议结合采用“Who are you?”的身份认证方式。

如图 4-23 所示，给出了本地登录认证的配置步骤。

在配置了路由器的本地登录认证功能后，再次从远程设备登录路由器，除了要提供正确密码外，还要求输入相应的用户名，如图 4-24 所示。

4.3.2　访问类语句

为了加强路由器自身的安全，对路由器的远程访问的位置加以限制（“Where are you?”）

也是常用的访问控制方法。如图 4-25 所示，要求只允许作为网管工作站的 Workstation 1 访问并配置路由器 A。

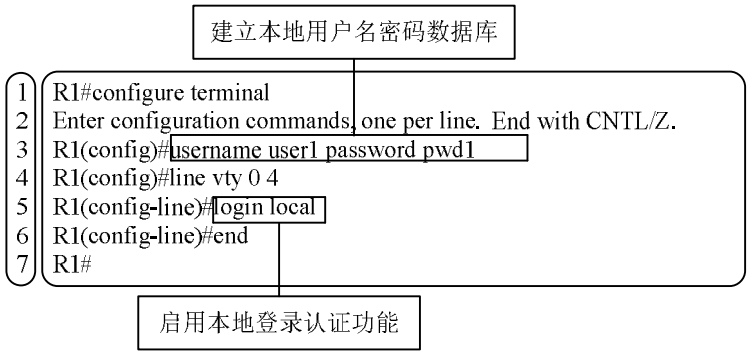

图 4-23　配置本地登录认证

```
R2#r1
Translating "r1"
Trying R1 (12.0.0.1)... Open


User Access Verification

Username: user1
Password:
R1>
```

图 4-24　本地登录认证

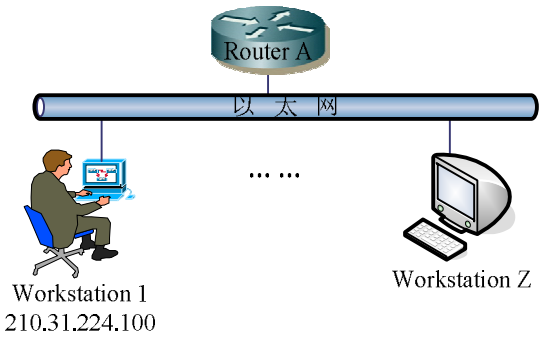

图 4-25　限制对路由器的管理性访问

这时，可以使用访问类语句进行 VTY 访问控制。具体配置步骤如图 4-26 所示。

```
RouterA(config)#line vty 0 4
RouterA(config-line)#login
RouterA(config-line)#password abc
RouterA(config-line)#access-class 1 in
RouterA(config-line)#access-list 1 permit host 210.31.224.100
RouterA(config)#access-list 1 deny any
```

图 4-26　进行 VTY 访问控制

4.3.3　HTTP/HTTPS

为了方便网络管理人员管理路由器，IOS 还提供了较为友好的 HTTP 界面访问方式。用户可以通过 HTTP 或 HTTPS 方式来管理路由器。

1. HTTP 管理方式

Cisco 路由器的 HTTP 管理方式是默认启用的。我们只需在浏览器中输入一个可达的路由器的接口 IP 地址，并在正确提供了加密使能密码后就可以以 HTTP 方式来访问路由器了。如

图 4-27 和图 4-28 所示。

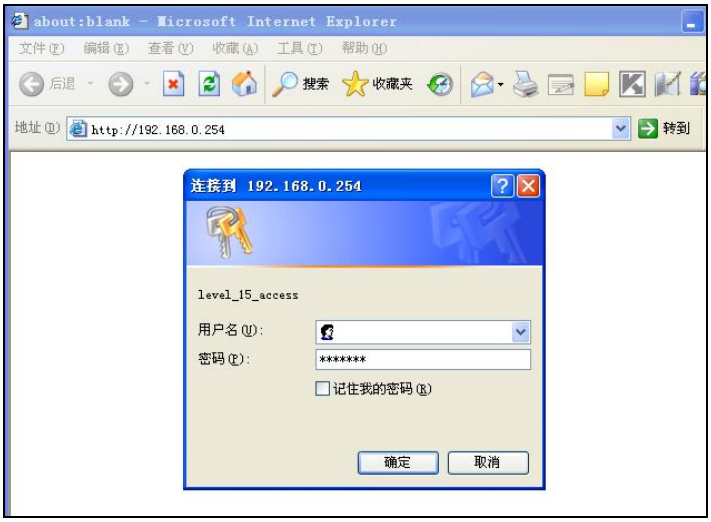

图 4-27　输入加密使能密码

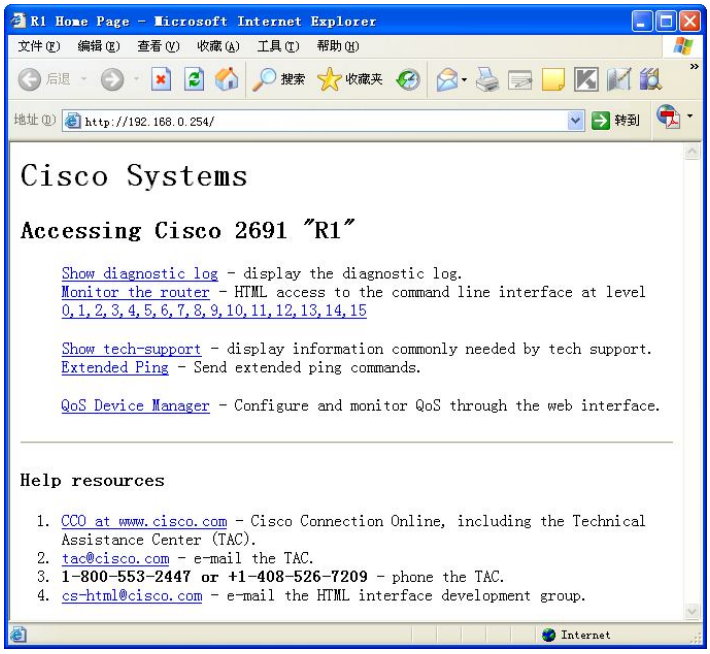

图 4-28　以 HTTP 方式来访问路由器

同样，可以通过要求登录用户提供用户名及密码的方式增强 HTTP 访问方式的安全性。如图 4-29 所示。

在图 4-29 中，首先是建立一个本地用户及其密码（注意，HTTP 登录要求提供具有 15 级权限的用户名和密码，所以此处要设置用户级别为 15 级），然后需要在全局下启用对 HTTP 登录方式的本地认证方式。

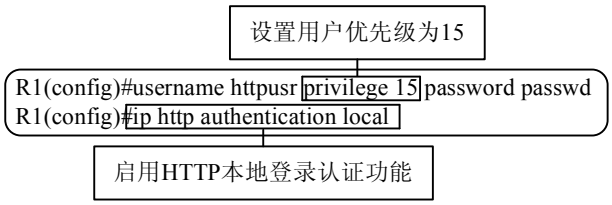

图 4-29　HTTP 访问本地认证配置

做完上述设置后，用户必须同时提供正确的用户名和密码才能以 HTTP 方式访问路由器，如图 4-30 所示。

图 4-30　HTTP 访问本地认证

说明：Cisco 路由器提供了 0~15 级的访问优先（privilege）级别，当用户成功登录路由器后，级别 0 将用户置于普通用户模式下，级别 15 将用户置于特权用户模式下。

同样，可以通过 ACL 限制 HTTP 访问位置。如图 4-31 所示，设置了只有 IP 是 192.168.0.9 的主机才被允许以 HTTP 方式访问路由器。其他主机以 HTTP 方式访问路由器会被提示“无法显示网页”，如图 4-32 所示。

```
R1(config)#ip http access-class 1
R1(config)#access-list 1 permit host 192.168.0.9
```

图 4-31　限制 HTTP 访问位置

图 4-32　非法用户访问路由器出错

尽管可以通过上述方法增强路由器的 HTTP 访问安全性，但 HTTP 协议本身并没有提供足够的安全特性，其会话交互的内容是没有加密的，很容易被窃听。因此，一般建议关闭路由器上的 HTTP 服务，如图 4-33 所示。

```
R1(config)#no ip http server
```

图 4-33　关闭路由器上的 HTTP 服务

2. HTTPS 管理方式

为了增强 HTTP 的安全性，RFC 提出了安全的 HTTP，即 HTTPS，其原理是通过证书认证，密钥交换等技术加密会话数据。

如图 4-34 所示，是配置路由器支持 HTTPS 访问方式的步骤。

```
1  R1(config)#user httpsusr privilege 15 password passwd
2  R1(config)#ip domain-name mydomain.com
3  R1(config)#ip http secure-server
4  R1(config)#crypto key generate rsa
5  The name for the keys will be: R1.mydomain.com
6  Choose the size of the key modulus in the range of 360 to 2048 for your
7    General Purpose Keys. Choosing a key modulus greater than 512 may take
8    a few minutes.
9
10 How many bits in the modulus [512]:
11 % Generating 512 bit RSA keys ...[OK]
12
13 R1(config)#
14 *Mar  1 04:18:53.770: %SSH-5-ENABLED: SSH 1.5 has been enabled
15 R1(config)#
```

图 4-34　配置路由器支持 HTTPS 访问方式

在图 4-34 中，

第 1 行用来创建一个优先级为 15 的本地用户及其密码。

第 2 行用来创建一个 IP 域名，路由器需要此信息构造安全密钥及证书。

第 3 行用来启用路由器上的 HTTPS 服务。

第 4～11 行用来产生 HTTPS 所需的 RSA 密钥对，此密钥对在产生路由器的证书过程中需要使用。其中，第 10 行要求用户输入 RSA 密钥长度（范围：360～2048，默认为 512 位，较长的密钥具有较高的安全性，但需要较长的计算时间产生此密钥）。

当密钥产生后，控制台会出现 SSH 服务被启用的提示，如图 4-34 中的第 14 行所示。

注意：路由器的名称不能是默认的“Router”，路由器需要此信息构造安全密钥及证书。

当上述配置过程结束后，就可以在浏览器中通过 HTTPS 方式访问路由器了，如图 4-35 所示。

在图 4-35 中单击“是”确认安全警报，并输入用于访问路由器的用户名、密码，如图 4-36 所示。

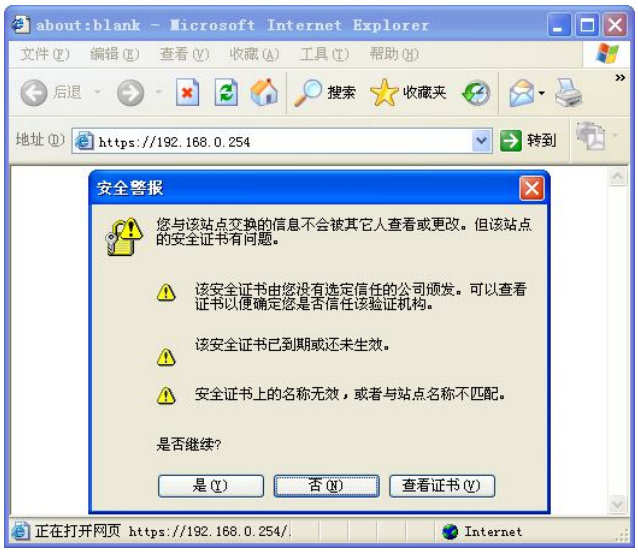

图 4-35　证书安全警报

图 4-36　输入用于访问路由器的用户名、密码

在提供了正确的用户名、密码后便可以以 HTTPS 的方式访问路由器了，如图 4-37 所示。默认的 HTTPS 服务端口为 443，我们通过全局配置命令对此进行修改，如图 4-38 所示。

4.3.4　SSH

一直以来 telnet 都是绝大多数网络设备支持的远程登录协议。但由于 telnet 协议自身的缺陷（其数据包在网络上是明文传输的，在共享结构的局域网上很容易被 sniffer 侦听），越来越多的网络设备开始支持较为安全的 SSH（Secure Shell）远程登录方式。

SSH 服务使用 TCP 22 端口，客户端软件发起连接请求后从服务器接受公钥，协商加密方法，成功后所有的通信都是加密的（使用 DES、3DES 加密算法）。

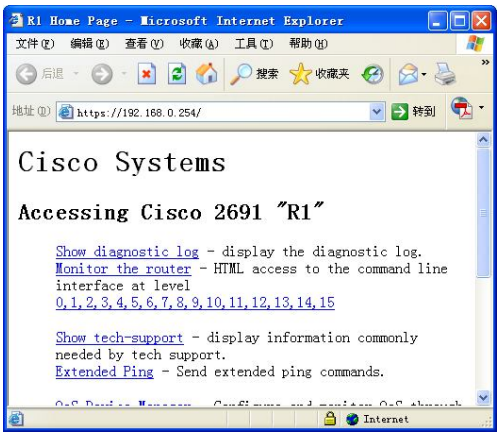

图 4-37　以 HTTPS 的方式访问路由器

```
R1(config)#ip http secure-port ?
  <0-65535>  Secure port number(above 1024 or default 443)
```

图 4-38　修改 HTTPS 服务端口号

SSH 通常有 3 个版本，即 SSHv1、SSHv1.5、SSHv2。

Cisco 路由器本身可以同时提供 SSH 服务器端及客户端服务。

1. SSH 服务器

Cisco 路由器上的 SSH 服务器配置步骤几乎和 HTTPS 的配置完全相同，所不同的是 SSH 的配置不需要启用 HTTPS 服务。因此，如果不需要 HTTPS 访问方式，可以使用全局命令 no ip http secure-server 禁用 HTTPS 服务。

如图 4-39 所示，是配置路由器上的 SSH 服务的步骤。

```
R1(config)#user sshusr privilege 15 password guestwhat
R1(config)#ip domain-name mydomain.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.mydomain.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Mar  1 05:29:41.274: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#
```

图 4-39　配置路由器上的 SSH 服务的步骤

注意：路由器的名称不能是默认的“Router”，路由器需要此信息构造安全密钥及证书。

当上述配置过程完成后，就可以使用 SSH 客户端通过 SSH 方式访问路由器了。我们以软件 SecureCRT 为例来讲解 SSH 客户端的配置和使用方法。

首先，在软件 SecureCRT 的工具栏上单击“快速连接”图标，如图 4-40 所示。

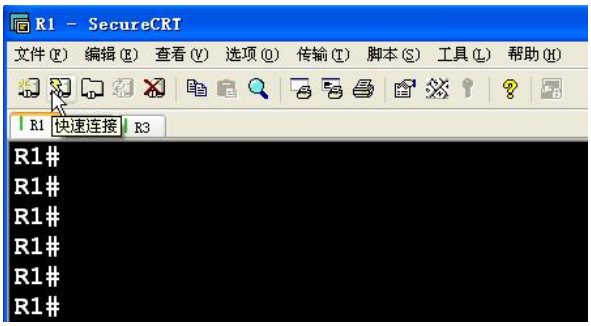

图 4-40　建立快速连接

在随后弹出的“快速连接”对话框中，选择协议类型为 SSH1，输入路由器的 IP 地址，输入用户名，保持其他选项为默认值，单击“连接”按钮继续，如图 4-41 所示。

图 4-41　“快速连接”对话框

如果输入的信息无误，则会弹出窗口询问，对于新建主机密钥的保存方式，如图 4-42 所示，选择“只接受一次”或“接受并保存”继续。

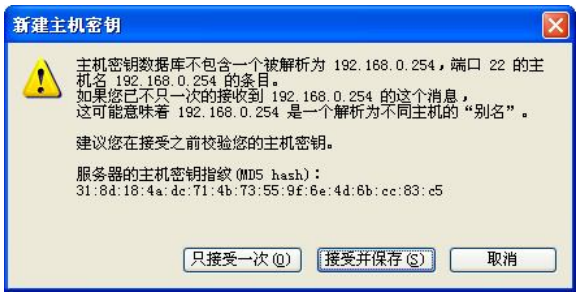

图 4-42　“新建主机密钥”对话框

在随后弹出的对话框中输入口令，单击“确定”按钮继续，如图 4-43 所示。

如果输入的口令正确，则会以 SSH 方式成功登录到路由器，如图 4-44 所示。

注意：

（1）由于登录用户 sshusr 的优先级为 15，所以登录后的 CLI 提示符为“R1#”，即登录

后用户即处于特权用户配置模式。

（2）在成功启用了路由器上的 SSH 服务器特性后，建议禁止以其他方式远程登录到路由器。如图 4-45 所示，设置了 0～4 号虚拟终端线只接受 SSH 登录。此后，路由器 R1 会拒绝再次 telnet 到 R1 的尝试，如图 4-46 所示。

图 4-43　输入口令

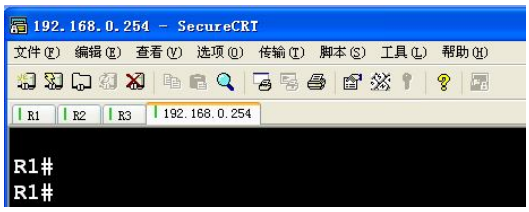

图 4-44　以 SSH 方式成功登录到路由器

```
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
```

图 4-45　设置虚拟终端线只接受 SSH 登录

```
R2#r1
Translating "r1"
Trying R1 (12.0.0.1)...
% Connection refused by remote host
```

图 4-46　拒绝 telnet 登录尝试

（3）还可以结合访问类语句 access-class 限制采用 SSH 登录到路由器的源主机 IP，来进一步增强路由器管理的安全性。

2. SSH 客户端

IOS 不但可以提供 SSH 服务器端服务，还提供 SSH 客户端服务。即，我们可以从一台路由器以 SSH 的方式登录到其他网络设备上。如图 4-47 所示，是 IOS 提供的关于 SSH 命令的上下文帮助信息。

```
R2#ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system

R2#
```

图 4-47　SSH 命令的上下文帮助信息

如图 4-48 所示，显示了在路由器 R2 上以用户名 cisco 成功登录到路由器 R1 的过程。

```
R2#ssh -l cisco 12.0.0.1

Password:

R1#
```

图 4-48　以 SSH 方式登录到路由器 R1

注意：

（1）SSH 服务器特性只在 12.0.5.S 以上的特定 IOS 版本中提供。

（2）SSH 客户端特性只在 12.1.3.T 以上的特定 IOS 版本中提供。

实验 4-1　Telnet 会话管理

一、实验目的

掌握管理呼入、呼出 Telnet 会话的方法。

二、实验任务

管理呼入、呼出 Telnet 会话。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-49 所示。

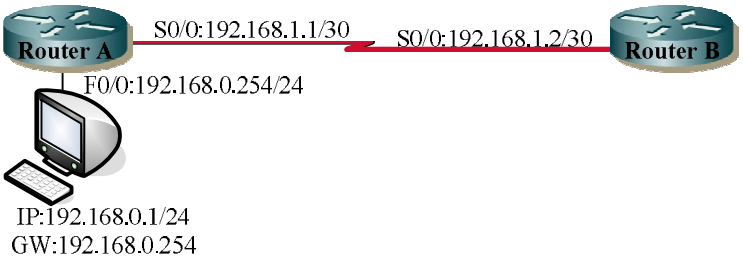

图 4-49　“Telnet 会话管理”实验环境

五、实验步骤

1．按图 4-49 设计、编写 Dynagen 所需.NET 文件。

2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。

3．按照 3.3.5 节配置路由器基本参数。

4．配置路由器 A 的串行接口 serial 0/0 接口 IP 地址（192.168.1.1/30）、路由器 B 的串行接口 serial 0/0 接口 IP 地址（192.168.1.2/30）并同时激活接口。

5．配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。

6．使用 ping 命令测试路由器 A 和路由器 B 之间的连通性。

7．练习 4.1 节中介绍的管理 Telnet 会话的各种命令。

实验 4-2　标准 ACL

一、实验目的

1．掌握标准 ACL 的配置方法。
2．掌握标准命名 ACL 的配置方法。

二、实验任务

1．配置标准 ACL 使得在某子网中只有指定工作站可以访问其他子网。
2．配置标准命名 ACL 使得在某子网中只有指定工作站可以访问其他子网。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-50 所示。

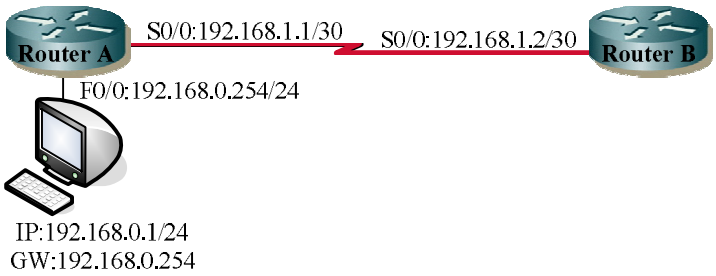

图 4-50　“标准 ACL”实验环境

五、实验步骤

1．按图 4-50 设计、编写 Dynagen 所需.NET 文件。
2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。
3．按照 3.3.5 节配置路由器基本参数。
4．按图 4-50 配置路由器和各工作站的 IP 地址等参数。配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。
5．使用 ping 命令测试 PC 终端和路由器 A 之间、路由器 A 和路由器 B 之间的连通性。
6．配置路由器上的标准 ACL，使得子网 192.168.0.0/24 中只有 192.168.0.1 可以访问子网 192.168.1.0/24，禁止其他通信量。
7．测试、检查配置好的 ACL。
8．改用标准命名访问控制列表实现本实验需求。

实验 4-3　扩展 ACL

一、实验目的

1．掌握扩展 ACL 的配置方法。
2．掌握扩展命名 ACL 的配置方法。

二、实验任务

1．配置扩展 ACL 对跨网段的 ICMP 协议数据进行限制。
2．配置扩展 ACL 对流入、流出路由器的不同类型服务数据加以限制。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-51 所示。

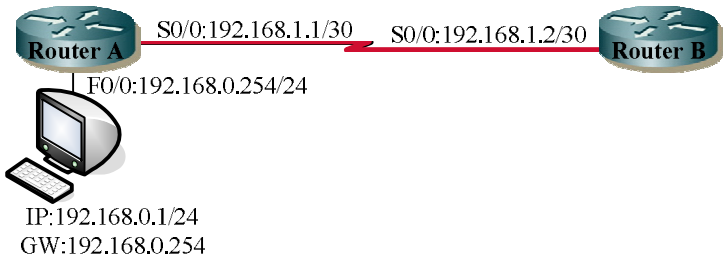

图 4-51　“扩展 ACL”实验环境

五、实验步骤

1．按图 4-51 设计、编写 Dynagen 所需.NET 文件。
2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。
3．按照 3.3.5 节配置路由器基本参数。
4．按图 4-51 配置路由器和 PC 终端的 IP 地址等参数。配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。
5．使用 ping 命令测试 PC 终端和路由器 A 之间、路由器 A 和路由器 B 之间的连通性。
6．在路由器 B 的全局配置模式下添加默认路由命令：ip route 0.0.0.0 0.0.0.0 192.168.1.1。
7．在 PC 终端上测试以 HTTP 方式、Telnet 方式访问路由器 B。
8．配置扩展 ACL 使得 PC 终端无法 ping 通路由器 B，允许其他通信量。
9．测试、检查配置好的 ACL。
10．配置扩展 ACL 使得 PC 终端无法访问路由器 B 上运行的 WWW 服务，允许其他通信量。

11．测试、检查配置好的 ACL。
12．改用扩展命名访问控制列表实现本实验需求。

实验 4-4　加强路由器登录安全性

一、实验目的

1．掌握路由器本地登录认证的配置方法。
2．掌握对路由器的管理位置加以限制的方法。

二、实验任务

1．配置路由器本地登录认证。
2．配置相关 ACL 命令对路由器的管理位置加以限制。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-52 所示。

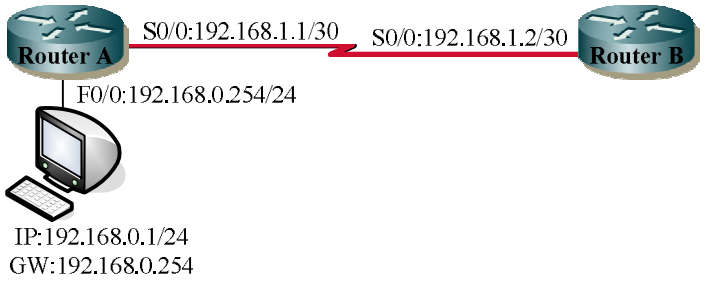

图 4-52　“加强路由器登录安全性”实验环境

五、实验步骤

1．按图 4-52 设计、编写 Dynagen 所需.NET 文件。
2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。
3．按照 3.3.5 节配置路由器基本参数。
4．按图 4-52 配置路由器和 PC 终端的 IP 地址等参数。配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。
5．使用 ping 命令测试 PC 终端和路由器 A 之间、路由器 A 和路由器 B 之间的连通性。
6．在路由器 B 的全局配置模式下添加默认路由命令：ip route 0.0.0.0 0.0.0.0 192.168.1.1。
7．在 PC 终端上测试以 Telnet 方式访问路由器 B。
8．将路由器 B 的虚拟终端线登录认证方式改为本地登录认证。

9．在 PC 终端上再次测试以 Telnet 方式访问路由器 B。

10．配置访问类语句使得子网 192.168.0.0/24 中只有 192.168.0.1 可以通过 Telnet 对路由器 B 进行配置、管理，允许除此之外的其他通信量。

11．测试、检查配置好的 ACL。

实验 4-5　以 HTTP/HTTPS 方式访问路由器

一、实验目的

1．掌握开启/关闭路由器上 HTTP 服务的配置方法。

2．掌握启用路由器上 HTTPS 服务的配置方法。

二、实验任务

1．开启/关闭、测试路由器上 HTTP 服务。

2．启用、测试路由器上 HTTPS 服务。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-53 所示。

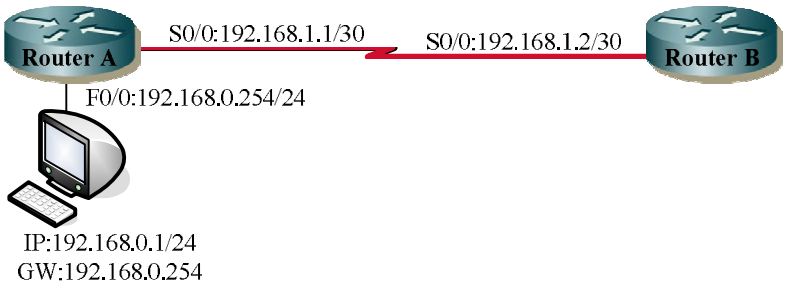

图 4-53　“HTTP/HTTPS”实验环境

五、实验步骤

1．按图 4-53 设计、编写 Dynagen 所需.NET 文件。

2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。

3．按照 3.3.5 节配置路由器基本参数。

4．按图 4-53 配置路由器和 PC 终端的 IP 地址等参数。配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。

5．使用 ping 命令测试 PC 终端和路由器 A 之间、路由器 A 和路由器 B 之间的连通性。

6．在路由器 B 的全局配置模式下添加默认路由命令：ip route 0.0.0.0 0.0.0.0 192.168.1.1。

7．在 PC 终端上测试以 HTTP 方式访问路由器 B。
8．关闭路由器 B 上的 HTTP 服务。
9．在 PC 终端上再次测试以 HTTP 方式访问路由器 B。
10．配置路由器 B 上的 HTTPS 服务。
11．在 PC 终端上测试以 HTTPS 方式访问路由器 B。

实验 4-6　以 SSH 方式访问路由器

一、实验目的

1．掌握启用路由器上 SSH 服务的配置方法。
2．掌握以 SSH 方式访问路由器的方法。

二、实验任务

启用、测试路由器上 SSH 服务。

三、实验设备

PC 终端一台，Dynamips/Dynagen 路由器模拟软件一套。

四、实验环境

实验环境如图 4-54 所示。

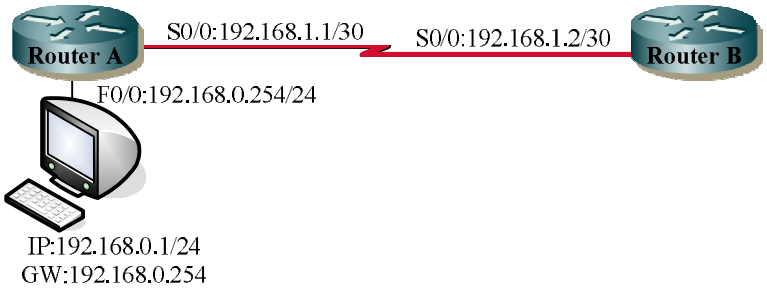

图 4-54　“以 SSH 方式访问路由器”实验环境

五、实验步骤

1．按图 4-54 设计、编写 Dynagen 所需.NET 文件。
2．通过 Dynagen 运行编写好的.NET 网络拓扑文件。
3．按照 3.3.5 节配置路由器基本参数。
4．按图 4-54 配置路由器和 PC 终端的 IP 地址等参数。配置路由器 A 的串行接口 serial 0/0 接口时钟频率为 64000。
5．使用 ping 命令测试 PC 终端和路由器 A 之间、路由器 A 和路由器 B 之间的连通性。
6．在路由器 B 的全局配置模式下添加默认路由命令：ip route 0.0.0.0 0.0.0.0 192.168.1.1。

7．配置路由器 B 上的 SSH 服务。
8．在 PC 终端上测试以 SSH 方式访问路由器 B。
9．在路由器 A 上测试以 SSH 方式访问路由器 B。
10．配置路由器 B 使其只接受 SSH 方式的远程管理。
11．配置路由器 B 使其只接受来自 192.168.0.1 的 SSH 方式远程管理。

思考与练习

1．写出标准 IP 访问控制列表和扩展 IP 访问控制列表的表号范围。
2．标准 IP 访问控制列表和扩展 IP 访问控制列表有何异同？
3．访问控制列表日志的作用是什么？如何启用？
4．写出配置路由器本地登录认证的步骤和命令。
5．写出配置路由器的 HTTPS 服务的步骤和命令。
6．配置路由器的 HTTPS 服务和路由器的 SSH 服务有何异同？
7．以 HTTPS 方式访问路由器和以 SSH 方式访问路由器有何不同？
8．练习管理呼入、呼出 Telnet 会话的方法。
9．练习配置标准、标准命名 IP 访问控制列表。
10．练习配置扩展、扩展命名 IP 访问控制列表。
11．练习启用/禁用路由器上的 HTTP 服务。
12．练习配置配置路由器上 HTTPS 服务。
13．练习配置配置路由器上 SSH 服务。