第 2 章　路由器基本配置及路由器安全管理配置

实训 2-1　路由器配置向导

【实训目的】

1．掌握利用配置向导对路由器进行初始配置的步骤和命令。
2．掌握查看路由器状态和配置的命令。

【实训任务】

利用配置向导配置路由器的基本参数，并查看路由器状态和配置信息。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

为了便于实训环境的搭建，这里我们还是利用路由器模拟软件 Dynamips/Dynagen 在 PC 工作站上模拟真实路由器来完成本实训，如图 2-1 所示。

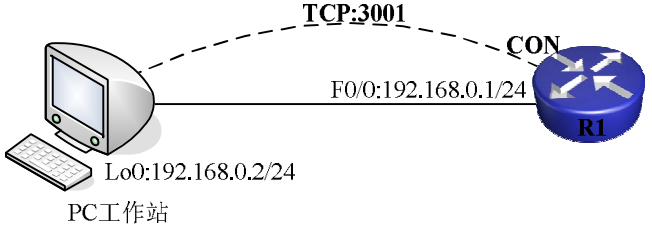

图 2-1　“路由器配置向导”实训环境

在本实训环境中，PC 工作站通过逻辑网络适配器 Loopback 0（简称 Loop0 或 Lo0）和路由器 R1 的快速以太网接口（Fastethernet 0/0，简称 Fe 0/0 或 F 0/0）连接。对路由器 R1 的初始配置则是通过 PC 工作站端 telnet 程序连接到模拟路由器的监听端口 3001 来实现（详见实训 1-1 或附录 A）。

【相关知识】

当路由器的 NVRAM 中没有启动配置文件（如一个新路由器进行第一次加电启动）或路由器被配置为启动时忽略 NVRAM 中的启动配置文件时，路由器会自动运行配置向导（也称

为配置对话），如图 2-2 所示。

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

图 2-2　路由器配置向导（片段）

利用配置向导，用户可以通过问答的形式对路由器进行初始配置（如路由器名称、登录口令、接口IP地址等）。这对于没有路由器配置经验的网络管理人员来说无疑提供了很大的方便。

需要说明的是，不同路由器平台、不同 IOS 版本的路由器配置向导的提示配置步骤可能会稍有不同。下面以 Cisco 1760 平台的 IOS 版本 12.3（26）（IOS 镜像文件：c1700-ipbase-mz.123-26.bin）为参照介绍路由器配置向导的使用。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-1 设计、编写 Dynagen 所需 Lab 2-1.net 文件，内容如下：

```
#Lab 2-1
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[1760]]
        ram = 128
        image = C:\Dynamips\images\c1700-ipbase-mz.123-26.img
        WIC0/0 = WIC-2T
        idlepc = 0x802b3d2c
    [[router r1]]
        model = 1760
        console = 3001
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
```

其中：

- “WIC0/0 = WIC-2T”表示在所有型号为 1760 的路由器的广域网接口卡插槽（模拟）插入一块 WIC-2T 接口卡（详见附录 A）。该接口卡含两个广域网接口（在 IOS 命令行中分别用 Serial 0/0，Serial 0/1 来引用）。

- 最后一行中的以太网卡注册表串值“910A39C1-3C12-48AF-AFF6-D8C98160D749”需换成读者终端要与 Dynamips 通信的网卡的注册表串值，后续实训同。

3. 启动、登录路由器 R1

（1）双击桌面上的“Dynamips Server”图标启动 Dynamips 后台服务程序。

（2）右击新创建的 Lab 2-1.net 文件，选择“打开方式”为“dg-local”。

（3）在弹出的 Dynagen 管理控制台中键入命令 list（注意命令大小写）列出当前.net 配置文件中的路由器列表。

（4）在 Dynagen 管理控制台中键入命令 start R1 启动模拟路由器 R1。

（5）通过 telnet 客户端程序（如 MS-DOS 命令 telnet、超级终端应用程序或 SecureCRT 软件）连接到模拟路由器的控制台。

4. 利用配置向导配置路由器 R1

（1）登录到路由器控制台后，会观察到如图 2-2 所示的自动启动的路由器配置向导提示。（如果配置向导没有自动启动，可以关闭 Dynamips 后台服务程序、Dynagen 管理控制台、删除 Dynagen 临时文件夹 tmp 下产生的临时文件，然后再次重新启动 Dynamips 后台服务程序、Dynagen 管理控制台并启动路由器 R1；如果使用的是真实路由器，可以使用命令 erase startup-config 删除启动配置文件并利用命令 reload 重新启动路由器）。

（2）系统询问是否开始配置向导的执行，键入“y”并回车，开始使用配置向导。

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:y
```

（3）系统提示：配置过程中键入“?”可以随时取得帮助；配置过程中可以随时键入“Ctrl+C”中止配置；在“[ ]”中显示的是缺省配置。系统询问是否只进行基本配置。键入“n”并回车，开始带有扩展配置功能（可以配置路由协议、桥接、各接口 IP 地址等信息）的配置向导。

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: n
```

（4）系统询问是否显示接口状态总结信息，直接“回车”显示接口状态总结信息，包括接口名称、IP 地址、工作状态等信息。

```
First, would you like to see the current interface summary? [yes]:
Interface        IP-Address  OK? Method Status                Protocol
FastEthernet0/0  unassigned  YES unset  administratively down down
Serial 0/0       unassigned  YES unset  administratively down down
Serial 0/1       unassigned  YES unset  administratively down down
```

（5）系统要求指定路由器的名称，键入“R1”将本路由器命名为 R1。

```
Configuring global parameters:
  Enter host name [Router]: R1
```

（6）系统提示：键入加密使能密码，此密码会使用 MD5 加密，且在显示配置文件内容时，无法用明文显示。键入“cisco”设置加密使能密码为 cisco。

```
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: cisco
```

（7）系统提示：键入使能密码，若设置了加密使能密码，此密码无效。如果不使用额外的 IOS 配置命令，此密码在显示配置文件内容时会以明文显示。键入“junk”设置使能密码为 junk（此密码不能和加密使能密码相同）。

```
The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: junk
```

（8）系统提示：键入虚拟终端访问密码，在以 Telnet 方式访问路由器时需要此密码进入路由器，键入“cisco”设置虚拟终端访问密码为 cisco。

```
The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password:cisco
```

（9）系统提示：是否配置 SNMP 相关特性，直接回车不配置对 SNMP 功能的支持。

```
Configure SNMP Network Management? [no]:
```

（10）系统提示：是否配置 IP 参数，直接回车确认要配置 IP 参数。

```
Configure IP? [yes]:
```

（11）系统提示：是否配置动态路由协议 RIP，键入“n”不配置动态路由协议 RIP。

```
Configure RIP routing? [yes]: n
```

（12）系统提示：是否配置桥接参数，直接回车确认不配置桥接参数。

```
  Configure bridging? [no]:
```

（13）系统提示：异步线路可以接受 Modem 呼入请求，如果有用户需要通过 Modem 拨入，则需要配置这些异步线路。键入“n”不配置异步线路参数。

```
Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.
  Configure Async lines? [yes]: n
```

（14）系统提示：是否配置快速以太网接口 fastEthernet 0/0 的参数，键入“y”配置此接口参数。

```
Do you want to configure FastEthernet0/0  interface? [no]: y
```

（15）系统提示：此快速以太网接口是否使用 100Base-TX 连接器，直接回车确认使用 100Base-TX 连接器。

```
  Use the 100 Base-TX (RJ-45) connector? [yes]:
```

（16）系统提示：此接口是否工作在全双工模式，键入“y”配置此接口工作在全双工模式。

```
 Operate in full-duplex mode? [no]:y
```

（17）系统提示：是否配置此接口 IP 参数，键入“y”确认配置接口 IP 参数。

```
  Configure IP on this interface? [no]:y
```

（18）系统要求输入此接口的 IP 地址，键入“192.168.0.1”设置此接口 IP 地址为 192.168.0.1。

```
  IP address for this interface:192.168.0.1
```

（19）系统要求输入此接口的子网掩码信息，直接回车确认设置此接口的子网掩码为“255.255.255.0”。

```
Subnet mask for this interface [255.255.255.0] :
Class C network is 192.168.0.0, 24 subnet bits; mask is /24
```

（20）系统提示：是否配置串行接口 serial 0/0 的参数，直接回车确认不配置串行接口 0/0 的参数。

```
Do you want to configure Serial 0/0  interface? [no]:
```

（21）系统提示：是否配置串行接口 serial 0/1 的参数，直接回车确认不配置串行接口 0/1 的参数。

```
Do you want to configure Serial 0/1  interface? [no]:
```

（22）系统提示：是否配置并检查自动安全配置，键入“n”不配置自动安全特性。系统接下来提示稍后可以通过 CLI 命令“auto secure”启动并配置自动安全特性。

```
Would you like to go through AutoSecure configuration? [yes]: n
AutoSecure dialog can be started later using "auto secure" CLI
```

（23）配置工作结束，系统自动显示根据配置向导生成的配置文件内容。随后提示：是否不保存配置并返回 CLI，还是不保存配置并重新配置，或者保存配置到 NVRAM 并退出，直接回车保存配置到 NVRAM 并退出。

```
The following configuration command script was created:
hostname R1
enable secret 5 $1$GCZR$WHITfcUCTpLvhsvCRvl90.
enable password junk
line vty 0 4
password cisco
no snmp-server
!
ip routing
no bridge 1
!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
full-duplex
ip address 192.168.0.1 255.255.255.0
!
interface Serial 0/0
shutdown
no ip address
!
interface Serial 0/1
shutdown
no ip address
dialer-list 1 protocol ip permit
!
```

```
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:
```

（24）根据配置情况，有可能个别配置会出错。如下所示，系统提示“media-type 100BaseX”命令出错（本 IOS 平台版本不支持设置以太网接口类型），忽略此提示即可。

```
 media-type 100BaseX
 ^
% Invalid input detected at '^' marker.
```

（25）按若干次回车键进入普通用户模式。

```
R1>
```

5. 查看路由器版本及配置信息

（1）键入命令 show version 并回车，查看路由器硬件配置、软件版本等信息。注意观察命令输出中的加粗字体部分。

```
R1>show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-IPBASE-M), Version 12.3(26), RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:24 by dchih
ROM: ROMMON Emulation Microcode
ROM: C1700 Software (C1700-IPBASE-M), Version 12.3(26), RELEASE SOFTWARE (fc2)
R1 uptime is 2 hours, 1 minute
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT]
0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"
cisco 1760 (MPC860T) processor (revision 0x202) with 114688K/16384K bytes of
memory.
Processor board ID 00000000000 (1880125456), with hardware revision 0000
MPC860T processor: part number 0, mask 0
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

（2）键入“enable”命令并回车。键入使能密码“junk”并回车尝试进入特权模式。

```
R1>enable
Password:
```

（3）键入加密使能密码“cisco”并回车尝试进入特权模式。

```
Password:
R1#
```

（4）成功进入特权模式后，键入“show startup-config”命令显示启动配置文件内容。注意观察命令输出中的加粗字体部分。

```
R1#show startup-config
Using 731 out of 29688 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
… …（节略）
```

（5）键入“show running-config”命令显示运行配置文件内容。注意观察命令输出中的加粗字体部分。

```
R1#show running-config
Building configuration...

Current configuration : 731 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
… …（节略）
```

6. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>ipconfig
Windows IP Configuration
Ethernet adapter Loop 0:
       Connection-specific DNS Suffix  . :
       IP Address. . . . . . . . . . . . : 192.168.0.2
       Subnet Mask . . . . . . . . . . . : 255.255.255.0
       Default Gateway . . . . . . . . . : 192.168.0.1
```

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

```
C:\WINDOWS\system32>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=21ms TTL=255
Reply from 192.168.0.1: bytes=32 time=16ms TTL=255
Reply from 192.168.0.1: bytes=32 time=15ms TTL=255
```

```
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 13ms
```

7. telnet 登录测试

利用 MS-DOS 命令 telnet 192.168.0.1 尝试登录路由器 R1（使用虚拟终端访问密码：cisco），如图 2-3 所示。如果没有登录成功，按照本实训前面的步骤进行检查并重新进行 telnet 登录测试直至成功。

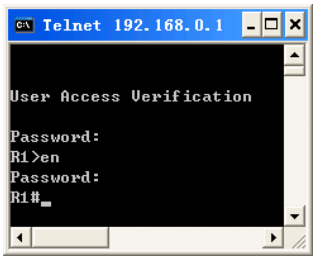

图 2-3　telnet 登录测试

【实训报告要求】

1．写出 Lab 2-1.net 文件内容中各参数的意义。
2．写出本实训用到的路由器配置命令清单。

实训 2-2　路由器手工配置

【实训目的】

1．掌握手工对路由器进行初始配置的步骤和命令。
2．理解 IOS 上下文帮助的功能。
3．掌握 IOS 常见配置模式及模式之间的转换方法。

【实训任务】

利用 IOS 命令对路由器进行初始手工配置。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-4 所示。

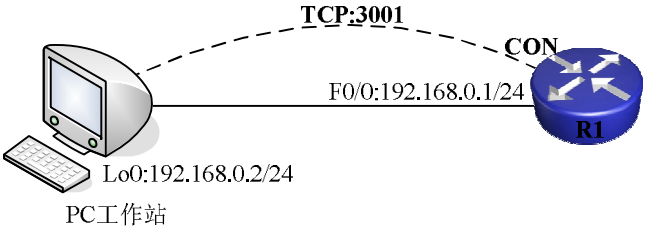

图 2-4　“路由器手工配置”实训环境

【相关知识】

1. IOS 命令行接口 CLI

使用路由器配置向导可以方便、快捷地对路由器进行初始配置。但是，配置向导只被设计用来执行一些基本的初始配置。对于更为详细的参数、选项设置，只能由路由器管理员通过各种 IOS 命令来完成。

IOS 配置通常是通过基于文本的命令行接口（Command Line Interface，CLI）进行的。IOS 命令解释器（Command Interpreter）负责解释用户键入的路由器配置命令。当用户键入一条命令并回车后，命令解释器检测该命令，如果命令正确的话，用户所键入的命令被执行。

2. 配置模式

为了通过 IOS 命令完成对路由器不同功能、特性的配置，必须首先转换到适当的路由器配置模式，如特权用户模式（命令提示符 Router#）、全局配置模式（命令提示符 Router(config)#）、路由配置模式（命令提示符 Router(config-router)#）、接口配置模式（命令提示符 Router(config-if)#）等。

IOS 通过不同的配置模式提示符来标识当前的路由器配置模式并通过不同的 IOS 命令进行模式间的转换。请读者参考本书配套主教材《网络互连技术——路由、交换与远程访问》中的相关章节的叙述。

3. IOS 上下文帮助功能

IOS 提供了很多上下文帮助功能，使得用户可以方便地对路由器进行配置。如命令缩写、命令补齐、命令及参数查询、命令错误指示等。

4. 历史命令和命令编辑快捷键

在默认情况下，IOS 将用户输入的最近 20 条命令保存在内存中的命令历史缓冲区内并可以通过命令快捷键快速浏览、重新输入或修改曾经键入的命令。如快捷键 Ctrl+P 可以将上一条命令显示在当前的路由器提示符后，而快捷键 Ctrl+N 可以显示后一条命令等。

表 2-1 列出了一些常用的命令编辑快捷键及其作用。

表 2-1　常用命令编辑快捷键

命令编辑快捷键	作用
Backspace，Ctrl+H	删除当前光标左侧的一个字符
Ctrl+P 或上箭头	重新显示前一命令
Ctrl+N 或下箭头	重新显示后一命令
Ctrl+A	到行首
Ctrl+E	到行尾
Ctrl+B	回退一个字符（并不删除）
Ctrl+F	前进一个字符
Ctrl+D	删除光标处的一个字符
Ctrl+K	删除从光标开始直到行尾的所有字符
Ctrl+X	删除光标之前的所有字符
Ctrl+W	删除一个字

续表

命令编辑快捷键	作用
Ctrl+U	删除一行
Ctrl+R	刷新刚输入的字符
Esc+B	回退一个单词
Esc+F	前进一个单词
Esc+D	删除光标后的一个单词

5. 搜索、过滤 show 命令的输出结果

show 命令用来显示路由器的各种相关信息，如配置文件内容、接口参数、协议参数等。当一个 show 命令输出内容很多的时候，可以通过管道符来过滤 show 命令的输出结果，以搜索我们关心的特定关键词。具体命令的格式如下：

```
command | {begin | include | exclude} regular-expression
```

这里，Command 是带有若干参数的 show 命令；“|”是管道符，用于过滤前面 show 命令的输出结果；regular-expression 为正则表达式，用来限定关键词；begin 表示从 show 命令输出结果中包含限定关键词的首行开始显示 show 命令的输出；include 表示只显示 show 命令输出结果中包含限定关键词的那些行；exclude 表示只显示 show 命令输出结果中不包含限定关键词的那些行。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-4 设计、编写 Dynagen 所需 Lab 2-2.net 文件，内容如下：

```
#Lab 2-2
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[1760]]
        ram = 128
        image = C:\Dynamips\images\c1700-ipbase-mz.123-26.img
        idlepc = 0x802b3d2c
    [[router r1]]
        model = 1760
        console = 3001
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
```

3. 启动、登录路由器 R1

按照实训 2-1 中的步骤启动并登录路由器 R1 的控制台。

4. 利用 IOS 命令配置路由器 R1

（1）登录到路由器控制台后，待路由器启动完毕出现“Press RETURN to get started!”提

示后，按回车键直到出现普通用户模式提示符 Router>（若为新路由器或空配置的路由器，则在路由器启动结束，出现配置向导时键入“n”退出，回到路由器 CLI 提示符 Router>）。

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:n
```

（2）键入命令 enable 并回车进入特权用户模式。

```
Router>enable
Router#
```

（3）键入命令 configure terminal 并回车进入全局配置模式。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

（4）键入命令 hostname R1 并回车为路由器命名，注意 CLI 提示符的变化（CLI 下的命令是立即生效的）。

```
Router(config)#hostname R1
R1(config)#
```

（5）键入命令 enable secret cisco 并回车设置加密使能口令。

```
R1(config)#enable secret cisco
```

（6）键入命令 interface fastEthernet 0/0 并回车进入接口配置模式，注意配置模式提示符的变化。

```
R1(config)#interface fastethernet 0/0
R1(config-if)#
```

（7）键入命令 speed 100 并回车设置接口速率为 100Mbps。

```
R1(config-if)#speed 100
```

（8）键入命令 duplex full 并回车设置接口工作在双工模式。

```
R1(config-if)#duplex full
```

（9）键入命令 ip address 192.168.0.1 255.255.255.0 并回车设置快速以太网接口 fastEthernet 0/0 的 IP 地址和子网掩码。

```
R1(config-if)#ip address 192.168.0.1 255.255.255.0
```

（10）键入命令 no shutdown 并回车激活快速以太网接口 fastEthernet 0/0。注意观察命令输出中的加粗字体部分。

```
R1(config-if)#no shutdown
*Mar  1 00:00:43.851: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar  1  00:00:44.851:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to up
```

（11）键入命令 exit 并回车退出接口配置模式。注意配置模式提示符的变化。

```
R1(config-if)#exit
R1(config)#
```

（12）键入命令 line console 0 并回车进入控制台端口配置模式。注意配置模式提示符的变化。

```
R1(config)#line console 0
R1(config-line)#
```

（13）键入命令 exec-timeout 5 30 并回车设置控制台端口超时时间为 5 分钟 30 秒钟（在

这段时间范围内，若没有收到任何键盘信息，路由器将断开和 PC 机之间的连接）。

```
R1(config-line)#exec-timeout 5 30
```

（14）键入命令 line vty 0 15 并回车配置 0 号到 15 号虚拟终端线。

```
R1(config-line)#line vty 0 15
```

（15）键入命令 exec-timeout 0 0 并回车设置虚拟终端线永不超时。

```
R1(config-line)#exec-timeout 0 0
```

（16）键入命令 password cisco 并回车设置虚拟终端线口令为 cisco。

```
R1(config-line)#password cisco
```

（17）键入 Ctrl+Z 或 end 并回车回到特权用户模式。注意观察命令输出中的加粗字体部分。

```
R1(config-line)#^Z
R1#
*Mar  1 00:09:30.283: %SYS-5-CONFIG_I: Configured from console by console
```

（18）键入命令 startup-config 并回车检查启动配置文件内容。由于还未将运行配置文件的内容存入 NVRAM 中，所以启动配置文件并不存在。

```
R1#show startup-config
startup-config is not present
```

（19）键入命令 show running-config 命令检查运行配置文件内容。

```
R1#show running-config
Building configuration...
Current configuration : 610 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
…… …（节略）
```

（20）检查配置正确无误后，键入命令 copy running-config startup-config 或 write 并回车将运行配置保存到 NVRAM。

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

（21）再次键入命令 show startup-config 并回车查看启动配置文件内容。

```
R1#show startup-config
Using 610 out of 29688 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname R1
… …（节略）
```

5. 连通性测试

（1）利用 MS-DOS 命令 ipconfig 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

6. telnet 登录测试

利用 MS-DOS 命令 telnet 192.168.0.1 尝试登录路由器 R1（使用虚拟终端访问密码：cisco）。如果没有登录成功，按照本实训前面的步骤进行检查并重新进行 telnet 登录测试直至成功。登录成功后键入命令 enable 并输入加密使能密码进入特权用户模式。

```
User Access Verification
Password:
R1>enable
Password:
R1#
```

7. IOS 上下文帮助功能测试

（1）键入命令“disable”并回车，转换到普通用户模式；键入“?”命令并回车，查看普通用户配置模式下支持的命令汇总。

```
R1#disable
R1>?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear           Reset functions
  connect         Open a terminal connection
  disable         Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable          Turn on privileged commands
… …（节略）
```

（2）键入命令“enable”并回车，输入加密使能密码转换到特权用户模式，再次键入“?”命令并回车，查看特权用户模式下支持的命令汇总。注意和普通用户配置模式下命令的不同。

```
R1#?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive         manage archive files
  auto            Exec level Automation
  bfe             For manual emergency modes setting
```

```
… …（节略）
```

（3）键入命令“dis?”并回车，列出当前配置模式下所有以字母 dis 开头的命令。

```
R1#dis?
disable  disconnect
```

（4）键入命令“show ?”并回车，列出当前配置模式下 show 命令的所有可用参数列表。

```
R1#show?
  aaa                Show AAA values
  access-expression    List access expression
      disable  disconnect
… …（节略）
```

（5）键入命令“show con?”并回车，列出当前配置模式下 show 命令中第一个参数以字母 con 开头的所有可用参数列表。

```
R1#show con?
configuration  connection  context  controllers
```

（6）键入命令“sh run”并回车，检查 IOS 对命令缩写的支持。

```
R1#sh run
Building configuration...
Current configuration : 610 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
… …（节略）
 --More--
… …（节略）
```

（7）在前面命令输出的基础上，键入回车键查看命令输出的下一行，键入空格键查看命令输出的下一页，键入其他字符终止显示回到 IOS 提示符。

（8）键入命令“show runing-config”并回车，检查 IOS 对错误命令及参数检测的支持。

```
R1#show runing-config
           ^
% Invalid input detected at '^' marker.
```

（9）键入“con”命令并回车，系统提示命令歧义的信息。

```
R1#con
% Ambiguous command:  "con"
```

（10）键入“conf t”命令并按键盘上的“Tab”键将参数 t 补齐。

```
R1#conf t
R1#conf terminal
```

（11）键入“copy running-config”命令并回车，系统提示命令参数不全。

```
R1#copy running-config
% Incomplete command.
```

8. 历史命令和命令编辑快捷键

（1）键入命令“show history”并回车，显示命令历史缓冲区内用户最近输入的 20 条命令。

```
R1#show history
  copy running-config startup-config
  show startup-config
  disable
  show run
  show running-config
… …（节略）
  show history
```

（2）键入命令“terminal history size 6”并回车，设置命令历史缓冲区只保留用户最近输入的 6 条命令。键入“show hist”并回车，显示命令历史缓冲区内用户最近输入的 6 条命令。

```
R1#terminal history size 6
R1#show hist
  show startup-config
  disable
  show run
  show history
      terminal history size 6
  show hist
```

（3）参考表 2-1，练习命令快捷键“Ctrl+P”、“Ctrl+N”、“Ctrl+A”、“Ctrl+E”、“Ctrl+W”、“Ctrl+U”、“Ctrl+R”的使用。

9. 搜索、过滤 show 命令的输出结果

（1）键入命令“show interfaces fastEthernet 0/0 | begin 5 minute”并回车，从包含“5 minute”的行开始显示快速以太网接口 fastEthernet 0/0 的参数。

```
R1#show interfaces fastEthernet 0/0 | begin 5 minute
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     208 packets input, 20756 bytes
… …（节略）
```

（2）键入命令“show interfaces fastEthernet 0/0 | include 5 minute”并回车，显示快速以太网接口 fastEthernet 0/0 的参数输出中包含“5 minute”的行。

```
R1#show interfaces fastethernet 0/0 | include 5 minute
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

（3）键入命令“show interfaces fastethernet 0/0 | exclude 0”并回车，显示快速以太网接口 fastEthernet 0/0 的参数输出中不包含“0”的那些行。

```
R1#show interfaces fastethernet 0/0 | exclude 0
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
```

（4）键入命令“show running-config interface fastEthernet 0/0”并回车，仅显示运行配置文件中快速以太网接口 fastEthernet 0/0 的配置。

```
R1#show running-config interface fastEthernet 0/0
Building configuration...
Current configuration : 83 bytes
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 speed 100
     duplex full
end
```

【实训报告要求】

1．画出 IOS 配置模式转换图。
2．写出常见命令快捷键及其作用。
3．写出本实训用到的路由器配置命令清单。

实训 2-3　常用路由器配置命令

【实训目的】

掌握常用路由器配置命令的用法。

【实训任务】

练习常用路由器配置命令。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-5 所示。

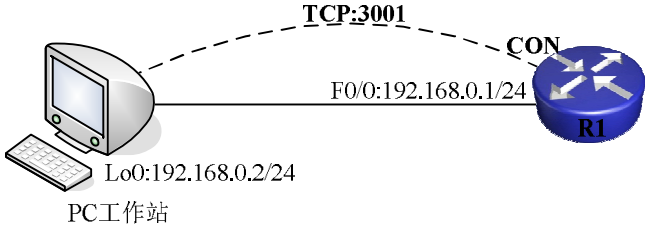

图 2-5　“常用路由器配置命令”实训环境

【相关知识】

本实训用来练习一些常用的路由器基本配置命令。在练习这些命令时，必须注意命令使

用的配置模式。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-5 设计、编写 Dynagen 所需 Lab 2-3.net 文件，内容如下：

```
#Lab 2-3
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[1760]]
        ram = 128
        image = C:\Dynamips\images\c1700-ipbase-mz.123-26.img
        idlepc = 0x802b3d2c
    [[router r1]]
        model = 1760
        console = 3001
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
```

3. 启动、登录路由器 R1

按照实训 2-1 中的实训步骤 3 启动并登录路由器 R1。

4. 配置路由器 R1 基本参数

按照实训 2-2 中的实训步骤 4 配置路由器 R1 的基本参数。

5. 配置路由器系统时钟

（1）确保处于特权用户模式，键入命令 show clock 并回车显示当前系统时钟信息。

```
R1#show clock
*00:03:48.671 UTC Mon Mar 1 1993
```

（2）键入命令 conf t 并回车进入全局配置模式，键入命令 clock timezone GMT 8 并回车设置当前系统时区为 GMT+8。

```
R1#conf t
R1(config)#clock timezone GMT 8
```

（3）键入命令 exit 并回车退回到特权用户模式，键入命令 clock set 12:25:00 july 1 2009 并回车设置当前系统时钟为 2009 年 7 月 1 日 12 点 25 分。

```
R1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
R1#clock set 12:25:00 july 1 2009
```

（4）再次键入命令 show clock 并回车查看时区、时钟设定结果。

```
R1#show clock
12:31:30.819 GMT Wed Jul 1 2009
```

6. 关闭域名解析特性

（1）在特权用户模式，键入命令 showw 并回车，观察路由器的输出提示。

```
R1#showw
Translating "showw"...domain server (255.255.255.255)

Translating "showw"...domain server (255.255.255.255)
 (255.255.255.255)
Translating "showw"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

（2）键入命令 conf t 并回车进入全局配置模式，键入命令 no ip domain-lookup 并回车关闭路由器域名解析特性，键入命令 end 返回特权用户模式。

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#end
R1#
```

（3）再次键入命令 showw 并回车，观察、对比路由器的输出提示。

```
R1#showw
Translating "showw"

Translating "showw"
% Unknown command or computer name, or unable to find computer address
```

7. 配置日志同步特性

（1）在特权用户模式，键入命令 conf t 并回车进入全局配置模式，键入^Z 返回特权用户模式后立即输入 show run，观察路由器的输出提示。

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#^Z
R1#show
*Mar  1 00:54:25.035: %SYS-5-CONFIG_I: Configured from console by consolerun
```

（2）键入命令 conf t 并回车进入全局配置模式，键入命令 line con 0 并回车进入控制台线路配置模式，键入 logging synchronous 并回车启用日志同步特性，键入^Z 返回特权用户模式后立即输入 show run，观察、对比路由器的输出提示。

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#^Z
R1#show r
*Mar  1 00:57:04.883: %SYS-5-CONFIG_I: Configured from console by console
R1#show run
```

8. 配置零子网特性

（1）在全局配置模式下，键入命令 no ip subnet-zero 并回车关闭路由器对零子网的支持特性，键入命令 interface serial 0/0 并回车进入串行接口配置模式，键入命令 ip address 192.168.1.1 255.255.255.128 并回车设置串行接口 serial 0/0 接口地址为 192.168.1.1、子网掩码为 255.255.255.128 并回车，观察路由器输出提示。

```
R1(config)#no ip subnet-zero
R1(config)#interface serial 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.128
Bad mask /25 for address 192.168.1.1
```

（2）键入命令 exit 并回车退回到全局配置模式，键入命令 ip subnet-zero 并回车启用路由器对零子网的支持特性，键入命令 interface serial 0/0 并回车进入串行接口配置模式，再次键入命令 ip address 192.168.1.1 255.255.255.128 并回车设置串行接口 serial 0/0 接口地址为 192.168.1.1、子网掩码为 255.255.255.128，观察、对比路由器输出提示。

```
R1(config-if)#exit
R1(config)#ip subnet-zero
R1(config)#interface serial 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.128
```

9. 配置接口描述及接口带宽描述

（1）在特权用户模式下，键入命令 show ip interface brief 显示当前路由器接口状态汇总列表。

```
R1#show ip interface brief
Interface          IP-Address    OK? Method Status                  Protocol
FastEthernet0/0    192.168.0.1   YES NVRAM  up                      up
Serial 0/0         192.168.1.1   YES manual administratively down   down
Serial 0/1         unassigned     YES NVRAM  administratively down   down
```

（2）在特权用户模式下，键入命令 show interface serial 0/0 并回车显示串行接口 serial 0/0 的相关信息。

```
R1#show interface serial 0/0
Serial 0/0 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 192.168.1.1/25
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
… …（节略）
```

（3）在全局配置模式下，键入命令 interface serial 0/0 并回车进入串行接口配置模式，键入命令 description Line_To_Shanghai 并回车为串行接口 serial 0/0 设置描述，键入命令 bandwidth 128 并回车设置串行接口 serial 0/0 带宽描述为 128kB，键入命令 end 并回车返回特权用户模式。

```
R1(config)#interface serial 0/0
R1(config-if)#description Line_To_Shanghai
R1(config-if)#bandwidth 128
R1(config-if)#end
R1#
```

（4）在特权用户模式下，再次键入命令 show interface serial 0/0 并回车显示串行接口 serial 0/0 的相关信息，注意观察命令输出中的加粗字体部分。

```
R1#show interface serial 0/0
```

```
Serial 0/0 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  Description: Line_To_Shanghai
  Internet address is 192.168.1.1/25
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
… …（节略）
```

10. 配置每日消息（Message Of ToDay，MOTD）

（1）在全局配置模式下，输入“banner motd #”命令并回车，输入消息内容并以“#”结束，键入 end 返回特权用户模式。

```
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access will be prosecuted!!!#
R1(config)#end
R1#
```

（2）在特权用户模式下键入命令 exit 并回车退出路由器控制台登录并再次回车登录路由器控制台，注意观察路由器控制台输出消息提示中的加粗字体部分。

```
R1 con0 is now available
... ...
Press RETURN to get started.
... ...
Unauthorized access will be prosecuted!!!
R1>
```

11. 关闭虚拟终端线登录验证特性

（1）利用 MS-DOS 命令 telnet 192.168.0.1 登录路由器 R1（使用虚拟终端访问密码：cisco）。登录成功后键入命令 enable 并输入加密使能密码进入特权用户模式，键入命令 exit 退出 telnet 登录。

```
Unauthorized access will be prosecuted!!!
User Access Verification
Password:
R1>enable
Password:
R1#exit
```

（2）在路由器全局配置模式下键入命令 line vty 0 15 并回车进入虚拟终端线配置模式，键入命令 no login 并回车关闭虚拟终端线登录验证特性。

```
R1(config)#line vty 0 15
R1(config-line)#no login
```

（3）利用 MS-DOS 命令 telnet 192.168.0.1 登录路由器 R1（不需要输入任何访问密码）。登录成功后键入命令 enable 并回车，输入加密使能密码进入特权用户模式，键入命令 exit 并回车退出 telnet 登录。

```
Unauthorized access will be prosecuted!!!
R1>enable
```

```
Password:
R1#exit
```

12. ping 命令的使用

（1）在特权用户模式下键入命令 ping 192.168.0.2 并回车，观察路由器的输出提示。

```
R1#ping 192.168.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

（2）在特权用户模式下键入命令 ping 192.168.0.3 并回车，随后键入退出序列 Ctrl+Shift+6+x 终止 ping 命令的执行。

```
R1#ping 192.168.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
..
Success rate is 0 percent (0/2)
R1#
```

（3）在特权用户模式下键入命令 ping 并回车，再次回车确认采用 ip 协议发送 icmp 数据包，键入目标 IP 地址为 192.168.0.2 并回车，键入 20 并回车选择 ping 包数量为 20，键入 200 并回车选择每个数据包大小为 200 字节，回车确认超时时间为 2 秒，再回车确认不进行命令选项扩展，再次回车确认在 ping 包发送过程中不递进改变 ping 数据包大小，观察路由器的输出提示。

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.0.2
Repeat count [5]: 20
Datagram size [100]: 200
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 200-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/2/4 ms
```

13. traceroute 命令的使用

在特权用户模式下键入命令 traceroute 192.168.0.2 并回车，观察路由器的输出提示。

```
R1#traceroute 192.168.0.2
Type escape sequence to abort.
Tracing the route to 192.168.0.2
  1 192.168.0.2 0 msec 0 msec 4 msec
R1#
```

14. 启用终端消息监听特性

（1）利用 MS-DOS 命令 telnet 192.168.0.1 登录路由器 R1。登录成功后键入命令 en 并回车，输入加密使能密码进入特权用户模式，键入命令 conf t 并回车进入全局配置模式，键入

命令 interface serial 0/0 并回车进入接口配置模式，键入命令 no shut 并回车激活接口，键入命令 shut 并回车关闭接口，观察路由器的输出提示。

```
Unauthorized access will be prosecuted!!!
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.
R1(config)#interface serial 0/0
R1(config-if)#no shut
R1(config-if)#shut
```

（2）键入命令 end 并回车退回到特权用户模式，键入命令 terminal monitor 并回车启用终端消息监听特性，再次键入命令 conf t 并回车进入全局配置模式，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 no shut 并回车激活接口，观察、对比路由器的输出提示。注意观察路由器虚拟终端输出消息提示中的加粗字体部分。

```
R1(config-if)#end
R1#terminal monitor
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0
R1(config-if)#no shut
R1(config-if)#
*Mar  1 01:54:10.359: %LINK-3-UPDOWN: Interface Serial 0/0, changed state to
up
R1(config-if)#
*Mar  1 01:54:11.363: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial
0/0, changed state to up
```

【实训报告要求】

1．写出本实训中用到的配置命令。

2．练习路由器上的 ping、traceroute 命令的使用。

实训 2-4　IOS 及配置文件管理

【实训目的】

1．掌握路由器配置文件备份、恢复的步骤和命令。

2．掌握路由器 IOS 备份、恢复（升级）的步骤和命令。

【实训任务】

利用 TFTP 服务器备份、恢复路由器配置文件、IOS 文件。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；TFTP 服务器软

件 TFTPD32、超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-6 所示。

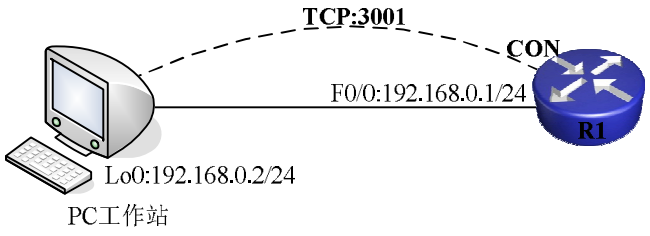

图 2-6　“IOS 及配置文件管理”实训环境

【相关知识】

配置文件是路由器软件中必不可少的组成部分。路由器操作系统依靠配置文件中的内容配置、运行路由器的各种进程。当通过路由器的命令行接口对路由器进行配置时，配置命令被立即执行，同时添加到驻留在路由器内存（Dynamic Random Access Memory，DRAM）中的运行配置文件中。

但是，这些新添加的配置命令不会被自动保存到非易失性内存（Nonvolatile RAM，NVRAM）中。当路由器断电或重新启动后，对路由器配置所做的修改就会完全丢失。因此，通常当对路由器进行了重新配置或修改后应该将当前的运行配置保存到 NVRAM 中变成启动配置文件（使用命令 copy running-config startup-config 或 write）。

此外，也可以利用 copy startup-config running-config 命令，将 NVRAM 中的启动配置文件的内容复制到当前内存中。需要注意的是，与将运行配置文件复制到 NVRAM 中变成启动配置文件不同，从 NVRAM 到内存的配置文件复制并不覆盖当前的运行配置文件内容，而只是添加当前的运行配置文件中没有的内容。对于相同的部分，则用启动配置文件中的语句改写运行配置文件中的语句。

随着配置文件中配置命令的增多、复杂性的增强，配置文件的安全和备份也越来越重要。我们经常需要在某处保存一份配置文件的副本，以便路由器出现故障时快速恢复它的运行。可以利用 FTP（File Transfer Protocol）或 TFTP（Trival File Transfer Protocol）服务器保存运行配置文件或启动配置文件。图 2-7 给出了常见的几种拷贝方式及其命令。

在路由器的启动过程中，需要将闪存（FLASH）中保存的 IOS 操作系统镜像文件读入到内存中运行。因此，作为路由器操作系统的 IOS 镜像文件，其重要性不用多言。应该养成及时备份新路由器 IOS 镜像文件的习惯。FTP/TFTP 服务器同样可以用来备份 IOS 镜像文件。同时，FTP/TFTP 服务器还可以实现路由器的 IOS 升级操作。如图 2-8 所示是对 IOS 文件进行管理的命令示意图。

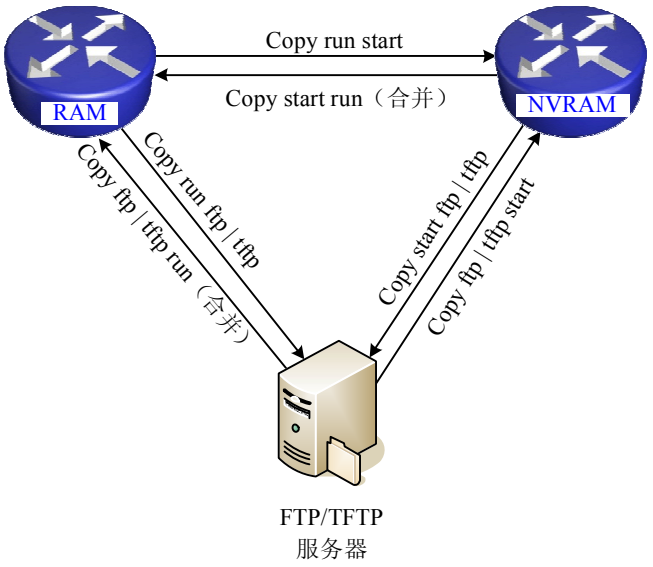

图 2-7　常见的几种拷贝方式及其命令

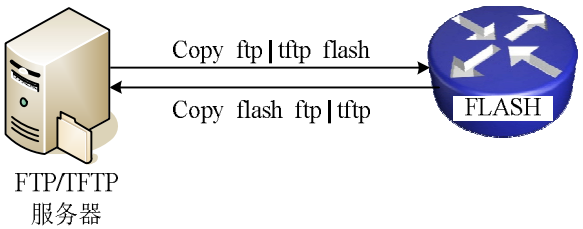

图 2-8　IOS 文件管理命令示意图

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-6 设计、编写 Dynagen 所需 Lab 2-4.net 文件（这里采用 Cisco 2621 镜像文件 c2600-i-mz.121-3.T.bin，注意使用前将其解压缩并重命名为 c2600-i-mz.121-3.T.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

```
#Lab 2-4
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[2621]]
        ram = 64
        image = C:\Dynamips\images\c2600-i-mz.121-3.T.img
        idlepc = 0x802c0730
```

- [[router r1]]
  - model = 2621
  - console = 3001
- f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}

3. 启动、登录路由器 R1

按照实训 2-1 中的步骤启动并登录路由器 R1。

4. 配置路由器 R1 基本参数

按照实训 2-2 中的步骤配置路由器 R1 的基本参数。

5. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2)利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

6. 安装、配置 TFTP 服务器

下面以 Philippe Jounin 编写的程序 TFTPD32（Version 1.1）为例，讲述该 TFTP 服务器安装、配置步骤。

实际上 TFTPD32 是一个绿色程序，不需要安装，可以直接运行，如图 2-9 所示，是 TFTPD32 服务器启动后的窗口界面。从该窗口可以看到此 TFTP 服务器的根目录位置、服务 IP 地址（本地环回地址）和服务侦听端口号。单击图 2-9 中的“Settings”按钮，在弹出的设置对话框中可以设置 TFTP32 服务器的各个参数，如图 2-10 所示，设置 TFTP32 程序当前所在目录下的 ROOT 子目录为工作根目录。

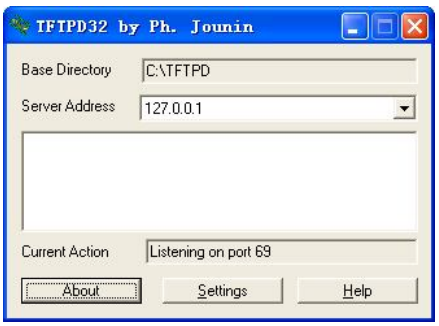

图 2-9　TFTPD32 服务器启动后的窗口界面

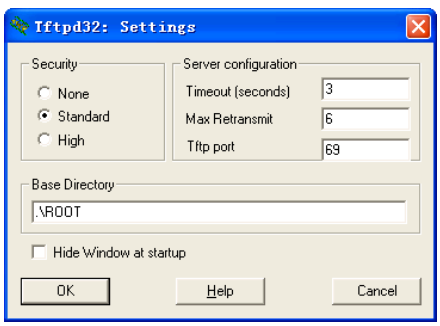

图 2-10　TFTPD32 服务器设置

7. 备份运行配置文件和启动配置文件

（1）在路由器的特权用户模式下，键入命令 copy running-config tftp 并回车，输入 TFTPD32 服务器 IP 地址（PC 工作站网卡 Loopback0 的 IP 地址）：192.168.0.2 并回车；按系统提示输入目标文件名：R1-running-cfg，系统开始传输运行配置文件到 TFTP 服务器并在复制完成之后提示文件被复制的信息（包括实际复制的字节大小、花费时间）。

```
R1#copy running-config tftp
Address or name of remote host []? 192.168.0.2
Destination filename [R1-confg]? R1-running-cfg
!!
```

```
568 bytes copied in 0.944 secs
R1#
```

（2）在 TFTPD32 服务器程序窗口观察 TFTP 客户端连接及文件传送情况，如图 2-11 所示。同时在 TFTPD 根目录下找到接收到的文件，如图 2-12 所示。利用 Windows XP 自带的“写字板”打开该文件并查看其内容。

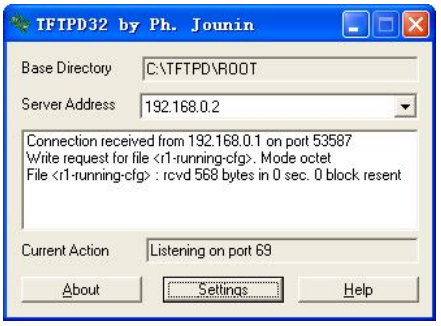

图 2-11　TFTPD32 服务器启动后的窗口界面

图 2-12　TFTPD32 服务器启动后的窗口界面

（3）按照类似的步骤备份路由器的启动配置文件。

```
R1#copy startup-config tftp
Address or name of remote host []? 192.168.0.2
Destination filename [R1-confg]? R1-startup-cfg
!!
568 bytes copied in 0.112 secs
```

（4）在路由器的特权用户模式下，键入命令 erase startup-config 并回车删除启动配置文件，系统提示确认后回车继续，再次回车确认删除 NVRAM 中的启动配置文件。

```
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
R1#
```

（5）在路由器的特权用户模式下，键入命令 show startup-config 并回车显示启动配置文件，系统提示启动配置文件无法访问（即不存在）。

```
R1#show startup-config
%% Non-volatile configuration memory is being written, Try again later
```

（6）在路由器的特权用户模式下，键入命令 copy tftp startup-config 并回车将 TFTP 服务器上保存的启动配置文件恢复到路由器的 NVRAM 中；按系统提示输入 TFTP32 服务器的 IP 地址：192.168.0.2 并回车；按系统提示输入源文件名：R1-startup-cfg；系统提示输入目标文件名，直接回车采用默认值：startup-config，系统提示访问 TFTP 服务器、装入配置文件、文件传输情况及启动配置文件被替换的系统信息。

```
R1#copy tftp startup-config
Address or name of remote host []? 192.168.0.2
Source filename []? R1-startup-cfg
Destination filename [startup-config]?
```

```
Accessing tftp://192.168.0.2/R1-startup-cfg...
Loading R1-startup-cfg from 192.168.0.2 (via FastEthernet0/0): !
[OK - 568/1024 bytes]
[OK]
568 bytes copied in 10.36 secs (56 bytes/sec)
R1#
00:06:05: %SYS-5-CONFIG_NV: Nonvolatile storage configured from tftp://
192.168.0.2/R1-startup-cfg
R1#
```

8. 备份、恢复（升级）IOS 文件

（1）在路由器的特权用户模式下，键入命令 dir flash:并回车列出闪存中保存的 IOS 操作系统镜像文件名称。由于采用的不是实际的物理路由器，而是 dynamips 模拟出来的虚拟路由器，所以此处显示该闪存中没有任何文件和目录，但是可以看到闪存的空余空间大小。

```
R1#dir flash:
Directory of flash:/
No files in directory
8388608 bytes total (8388608 bytes free)
R1#
```

（2）在路由器的特权用户模式下，键入命令 copy tftp flash 并回车，再次直接回车采用系统提供的默认 TFTP 服务器 IP 地址：192.168.0.2，按照系统提示输入源文件名：c2600-i-mz.121-3.T.bin 并回车，按照系统提示直接回车采用默认的目标文件名。随后，按照系统提示直接回车确认清除闪存中的所有数据，再次直接回车确认清除闪存中的所有数据。系统提示清除闪存中的所有数据、装入 IOS 镜像文件及文件传输情况。

```
R1#copy tftp flash
Address or name of remote host [192.168.0.2]?
Source filename [R1-startup-cfg]? c2600-i-mz.121-3.T.bin
Destination filename [c2600-i-mz.121-3.T.bin]?
Accessing tftp://192.168.0.2/c2600-i-mz.121-3.T.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
Loading c2600-i-mz.121-3.T.bin from 192.168.0.2 (via FastEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! ……（节略）
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3813950/7627776 bytes]
Verifying checksum... OK (0x8E13)
3813950 bytes copied in 108.616 secs (35314 bytes/sec)
```

（3）在使用实际的物理路由器的情况下，一般还需要使用全局配置命令 boot system flash:c2600-i-mz.121-3.T.bin 指定路由器在重启后使用新的 IOS 镜像文件。但在此处由于使用的是 dynamips 模拟出来的虚拟路由器，所以此处可忽略此步骤。

【实训报告要求】

1．简述 TFTP 服务器的用途。

2．写出 TFTP 服务器的配置、使用方法。

3．写出备份、恢复路由器配置文件及 IOS 文件的步骤和命令。

实训 2-5　telnet 管理

【实训目的】

掌握管理呼入、呼出 telnet 会话的方法。

【实训任务】

管理呼入、呼出 telnet 会话。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

在本实训环境中， PC 工作站通过逻辑网络适配器 Loopback 0（简称 Loop0 或 Lo0）和路由器 R1 的快速以太网接口 fastEthernet 0/0 连接。路由器 R1 通过串行接口 serial 0/0 和路由器 R2 的串行接口 serial 0/0 连接。对路由器 R1 的初始配置是通过 PC 工作站端 telnet 程序连接到模拟路由器的监听端口 3001 来实现，对路由器 R2 的初始配置是通过 PC 工作站端 telnet 程序连接到模拟路由器的监听端口 3002 来实现。

实训环境如图 2-13 所示。

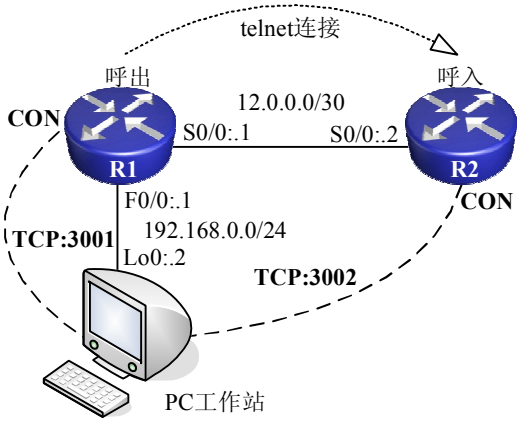

图 2-13　“telnet 管理”实训环境

【相关知识】

为方便网络管理人员管理网络设备，绝大多数网络设备都既可以作为 telnet 服务器供我

们从本地终端远程登录到远程网络设备上进行配置。同时，在登录到网络设备后，还可以进一步作为 telnet 客户端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。

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。当从一台本地网络设备 telnet 到另一台远程网络设备时，我们称本地网络设备发起了一次呼出 telnet 会话；而此时对于远程网络设备而言，其接受了一次 telnet 呼入会话。本实训帮助读者掌握路由器上的 Telnet 呼入、呼出会话管理方法。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-13 设计、编写 Dynagen 所需 Lab 2-5.net 文件（这里采用 Cisco 2621 镜像文件 c2600-i-mz.121-3.T.bin，注意使用前将其解压缩并重命名为 c2600-i-mz.121-3.T.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

```
#Lab 2-5
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[2621]]
        ram = 64
        image = C:\Dynamips\images\c2600-i-mz.121-3.T.img
        idlepc = 0x802c0730
    [[router r1]]
        model = 2621
        console = 3001
        s0/0 = R2 s0/0
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
    [[router r2]]
        model = 2621
        console = 3002
```

3. 启动、登录路由器 R1、R2

按照实训 2-1 中的步骤启动并登录路由器 R1、R2。

4. 配置路由器 R1、R2 基本参数

按照实训 2-2 中的步骤配置路由器 R1、R2 的基本参数。

5. 配置路由器 R1、R2 接口参数

按照图 2-13 配置路由器 R1 的串行接口 serial 0/0 接口 IP 地址（12.0.0.1/30）、路由器 R2 的串行接口 serial 0/0 接口 IP 地址（12.0.0.2/30）并同时激活接口（在实际的物理路由器间直接通过串口互连的情况下，还需要配置某台路由器的串行接口的时钟频率，后续实训同）。

6. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2)利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（3）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

7. 呼出 Telnet 会话管理

（1）在路由器 R1 的特权用户模式下，键入命令 telnet 12.0.0.2 并回车，当系统提示输入口令时输入路由器 R2 的 telnet 口令（cisco）并回车远程登录到路由器 R2，键入命令 exit 并回车断开当前的 telnet 会话回到路由器 R1。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ... Open
User Access Verification
Password:
R2>exit
 [Connection to 12.0.0.2 closed by foreign host]
R1#
```

（2）在路由器 R1 的全局配置模式下，键入命令 ip host R2 12.0.0.2 并回车，键入命令 end 返回特权用户模式，键入命令 R2 并回车，当系统提示输入口令时输入路由器 R2 的 telnet 口令（cisco）并回车远程登录到路由器 R2，键入退出序列（Ctrl+Shift+6+x）暂时挂起到 R2 的 telnet 会话回到路由器 R1，键入命令 show sessions 显示路由器 R1 当前发起的呼出 telnet 连接统计信息。

```
R1(config)#ip host R2 12.0.0.2
R1(config)#end
R1#R2
Trying R2 (12.0.0.2)... Open
User Access Verification
Password:
R2>
R1#show sessions
Conn Host              Address           Byte  Idle Conn Name
*  1  r2               12.0.0.2             0     0   r2
```

（3）键入 1 或直接回车恢复到路由器 R2 的 telnet 连接。

```
   R1#1
[Resuming connection 1 to r2 ... ]
R2>
```

（4）在路由器 R2 的普通用户模式下，再次键入退出序列（Ctrl+Shift+6+x）暂时挂起到 R2 的 telnet 会话回到路由器 R1，键入命令 disconnect 1 并回车，再次回车确认断开到 R2 的 telnet 连接，键入命令 show sessions 显示路由器 R1 当前发起的呼出 telnet 连接统计信息。

```
R2>
R1#disconnect 1
Closing connection to r2 [confirm]
R1#show sessions
% No connections open
R1#
```

8. 呼入 Telnet 会话管理

（1）在路由器 R2 的特权用户模式下，键入命令 telnet 12.0.0.1 并回车，当系统提示输入口令时输入路由器 R1 的 telnet 口令（cisco）并回车远程登录到路由器 R1。

```
R2#telnet 12.0.0.1
Trying 12.0.0.1 ... Open
User Access Verification
Password:
R1>
```

（2）在 PC 工作站上利用 MS-DOS 命令 telnet 192.168.0.1 登录路由器 R1（使用虚拟终端访问密码：cisco）。

（3）在路由器 R1 的特权用户模式下，键入命令 show users 或 who 并回车查看路由器 R1 的当前呼入 telnet 会话情况。

```
R1#show users
    Line      User      Host(s)            Idle      Location
*  0 con 0              idle               00:00:00
  66 vty 0               idle               00:00:04   R2
  67 vty 1               idle               00:01:34   192.168.0.2
  Interface  User     Mode                   Idle Peer Address
```

（4）在路由器 R1 的特权用户模式下，键入命令 show line 并回车查看路由器 R1 的当前呼入终端线路使用统计信息。

```
R1#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      4       0     0/0       -
    65 AUX   9600/9600  -    -      -    -    -      0       0     0/0       -
*   66 VTY              -    -      -    -    -      3       0     0/0       -
*   67 VTY              -    -      -    -    -      1       0     0/0       -
    68 VTY              -    -      -    -    -      0       0     0/0       -
    69 VTY              -    -      -    -    -      0       0     0/0       -
    70 VTY              -    -      -    -    -      0       0     0/0       -
Line(s) not in async mode -or- with no hardware support:
1-64
```

（5）在路由器 R1 的特权用户模式下，键入命令 clear line 67 并回车两次断开 PC 工作站到路由器 R1 的 telnet 连接，键入命令 show users 并回车再次显示路由器 R1 的当前呼入 telnet 会话情况。

```
R1#clear line 67
[confirm]
 [OK]
R1#show users
    Line      User      Host(s)            Idle      Location
```

```
*  0 con 0              idle              00:00:00
  66 vty 0              idle              00:03:15 R2
  Interface  User       Mode              Idle Peer Address
```

（6）在 PC 工作站上观察收到的提示信息。

（7）在路由器 R1 的特权用户模式下，键入命令 clear line vty 0 并回车两次断开路由器 R2 到路由器 R1 的 telnet 连接，键入命令 show users 并回车再次显示路由器 R1 的当前呼入 telnet 会话情况。

```
R1#clear line vty 0
[confirm]
 [OK]
R1#show users
    Line      User      Host(s)            Idle      Location
*  0 con 0              idle              00:00:00
  Interface   User      Mode              Idle Peer Address
```

（8）在路由器 R2 上观察收到的提示信息。

```
R1>
[Connection to 12.0.0.1 closed by foreign host]
R2#
```

【实训报告要求】

1．简述呼入、呼出会话的区别。

2．写出管理呼入、呼出会话的 CLI 命令。

实训 2-6　标准 ACL 配置

【实训目的】

1．了解 ACL 的概念、分类及工作机制。

2．掌握标准 ACL 的配置、验证方法。

3．掌握标准命名 ACL 的配置、验证方法。

【实训任务】

1．配置标准 ACL 使得只有指定子网可以访问其他子网。

2．配置标准命名 ACL 使得只有指定子网可以访问其他子网。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-14 所示。

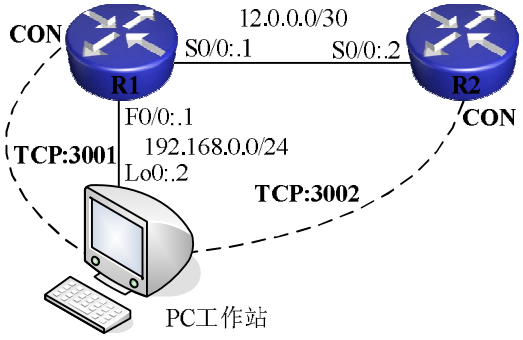

图 2-14　“标准 ACL 配置”实训环境

【相关知识】

访问控制列表（Access Control List，ACL）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。

配置标准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），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}
```

第二步，将访问列表应用到路由器的具体接口（应用访问组），IP 访问控制组语句的命令格式为：

```
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。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。其中，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 访问控制列表使用的号码范围为：1～99 及 1300～1999；扩展 IP 访问控制列表使用的号码范围为：100～199 及 2000～2699。

为了便于识别某一组 ACL 的用途，在 IOS 11.2 版本后，可以使用命名访问控制列表，即命名 ACL。

在配置 IP 访问控制列表时需要特别注意以下问题：

- IP 访问控制列表使用通配符掩码来代替子网掩码来定义要匹配的网络范围。
- 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不匹配任何语句的数据包的操作（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。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。
- 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。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-14 设计、编写 Dynagen 所需 Lab 2-6.net 文件（这里采用 Cisco 2691 镜像文件 c2691-jk9s-mz.123-18a.bin，注意使用前将其解压缩并重命名为 c2691-jk9s-mz.123-18a.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

```
#Lab 2-6
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[2691]]
        ram = 128
        image = C:\Dynamips\images\c2691-jk9s-mz.123-18a.img
        idlepc = 0x604bfef0
    [[router r1]]
        model = 2691
        console = 3001
        s0/0 = R2 s0/0
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
    [[router r2]]
        model = 2691
        console = 3002
```

3. 启动、登录路由器 R1、R2

按照实训 2-1 中的步骤启动并登录路由器 R1、R2。

4. 配置路由器 R1、R2 基本参数

按照实训 2-2 中的步骤配置路由器 R1、R2 的基本参数。

5. 配置路由器 R1、R2 接口参数

按照图 2-14 配置路由器 R1 的串行接口 serial 0/0 接口 IP 地址（12.0.0.1/30）、路由器 R2 的串行接口 serial 0/0 接口 IP 地址（12.0.0.2/30）并同时激活接口。

6. 配置路由器 R2 上的静态路由

为了使得路由器 R2 可以将数据包发往 192.168.0.0/24 网段，还需要在路由器 R2 上设置一条指向路由器 R1 的静态路由。

在路由器 R2 的全局配置模式下，键入命令 ip route 192.168.0.0 255.255.255.0 12.0.0.1 并回车，设置去往网络 192.168.0.0/24 的数据包的下一跳是路由器 R1 的串行接口 serial 0/0 的地址。

```
R2(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.1
```

7. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（3）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（4）利用 MS-DOS 命令 ping 12.0.0.2 测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

8. 配置、测试标准 ACL

（1）在路由器 R2 全局配置模式下，键入命令 access-list 1 permit 192.168.0.0 0.0.0.255 并回车，创建编号为 1 的标准 ACL 并允许来自 192.168.0.0/24 网段的数据包，键入命令 access-list 1 deny any 并回车拒绝所有来自其他网段的流量，键入命令 end 并回车返回特权用户模式，键入命令 show access-lists 显示已创建的 ACL 内容。

```
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R2(config)#access-list 1 deny any
R2(config)#end
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 deny   any
```

（2）在路由器 R2 全局配置模式下，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 ip access-group 1 in 并回车将刚才定义的 1 号 ACL 应用到路由器 R2 的串行接口 serial 0/0 的入方向，即指明在数据包流入路由器 R2 的串行接口 serial 0/0 时进行 ACL 检查。

```
R2(config)#interface serial 0/0
R2(config-if)#ip access-group 1 in
```

（3）在 PC 工作站上利用 MS-DOS 命令 ping 12.0.0.2 测试路由器 R2 上的 ACL 工作情况。

```
C:\WINDOWS\system32>ping 12.0.0.2
Pinging 12.0.0.2 with 32 bytes of data:
Reply from 12.0.0.2: bytes=32 time=81ms TTL=254
Reply from 12.0.0.2: bytes=32 time=46ms TTL=254
```

```
Reply from 12.0.0.2: bytes=32 time=49ms TTL=254
Reply from 12.0.0.2: bytes=32 time=47ms TTL=254
Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 81ms, Average = 55ms
C:\WINDOWS\system32>
```

（4）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试路由器 R2 上的 ACL 工作情况。注意，ping 命令输出结果中的 U 代表目标不可达，“.”表示超时。

```
R1#ping 12.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R1#
```

（5）在路由器 R2 特权用户模式下，键入命令 show access-lists 并回车显示已创建的 ACL 内容及数据包命中情况。

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255 (12 matches)
    20 deny   any (11 matches)
```

（6）在路由器 R2 全局配置模式下，键入命令 no access-list 1 并回车删除原 ACL 定义，键入命令 access-list 1 permit 192.168.0.0 0.0.0.255 log 并回车，创建编号为 1 的标准 ACL 并允许来自 192.168.0.0/24 网段的数据包并做日志，键入命令 access-list 1 deny any log 并回车拒绝所有来自其他网段的流量并做日志，键入命令 logging on 并回车打开日志功能，键入命令 logging buffered 并回车开启日志缓存功能，键入命令 end 并回车返回特权用户模式，键入命令 show access-lists 并回车显示已创建的 ACL 内容。

```
R2(config)#no access-list 1
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255 log
R2(config)#access-list 1 deny any log
R2(config)#logging on
R2(config)#logging buffered
R2(config)#end
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255 log
    20 deny   any log
```

（7）在 PC 工作站上利用 MS-DOS 命令 ping 12.0.0.2 测试路由器 R2 上的 ACL 工作情况。注意观察路由器 R2 控制台上的消息输出。

```
R2#
*Mar 1 01:02:01.755: %SEC-6-IPACCESSLOGS: list 1 permitted 192.168.0.2  4
packets
```

（8）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试路由器 R2 上的 ACL 工作情况。注意观察路由器 R2 控制台上的消息输出。

```
R2#
*Mar  1 01:03:01.751: %SEC-6-IPACCESSLOGS: list 1 denied 12.0.0.1 5 packets
```

（9）在路由器 R2 全局配置模式下，键入命令 show logging 显示日志情况，注意观察命令输出中的加粗字体部分。

```
R2#show logging
Syslog logging: enabled (9 messages dropped, 1 messages rate-limited, 0 flushes,
0 overruns, xml disabled)
    Console logging: level debugging, 48 messages logged, xml disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 15 messages logged, xml disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 44 message lines logged
Log Buffer (4096 bytes):
*Mar 1 01:01:30.379: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 01:02:01.755: %SEC-6-IPACCESSLOGS: list 1 permitted 192.168.0.2  4
packets
*Mar 1 01:03:01.751: %SEC-6-IPACCESSLOGS:list 1 denied 12.0.0.1  5packets
R2#
```

9. 配置、测试标准命名 ACL

（1）在路由器 R2 全局配置模式下，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 no ip access-group 1 in 并回车删除 1 号 ACL 在路由器 R2 的串行接口 serial 0/0 的入方向上的应用，键入命令 exit 并回车退回到全局配置模式，键入命令 no access-list 1 并回车删除 1 号 ACL。

```
R2(config)#interface serial 0/0
R2(config-if)#no ip access-group 1 in
R2(config-if)#exit
R2(config)#no access-list 1
```

（2）在路由器 R2 全局配置模式下，键入 ip access-list standard STDACL1 并回车创建名称为“STDACL1”的标准命名 ACL 并进入标准命名 ACL 配置模式，键入命令 permit host 12.0.0.1 并回车允许源地址为 12.0.0.1/32 的数据包，键入命令 deny any 并回车拒绝所有源自其他网段的数据包，键入命令 exit 并回车退回到全局配置模式，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 ip access-group STDACL1 in 并回车将刚才定义的标准命名 ACL 应用到路由器 R2 的串行接口 serial 0/0 的入方向，即指明在数据包流入路由器 R2 的串行接口 serial 0/0 时进行 ACL 检查，键入命令 end 并回车返回特权用户模式，键入命令 show access-lists 显示已创建的 ACL 内容。

```
R2(config)#ip access-list standard STDACL1
R2(config-std-nacl)#permit host 12.0.0.1
R2(config-std-nacl)#deny any
R2(config-std-nacl)#exit
R2(config)#interface serial 0/0
R2(config-if)#ip access-group STDACL1 in
R2(config-if)#end
```

```
R2#show access-lists
Standard IP access list STDACL1
    10 permit 12.0.0.1
    20 deny   any
```

（3）在 PC 工作站上利用 MS-DOS 命令 ping 12.0.0.2 测试路由器 R2 上的 ACL 工作情况。

```
C:\WINDOWS\system32>ping 12.0.0.2
Pinging 12.0.0.2 with 32 bytes of data:
Reply from 12.0.0.2: Destination net unreachable.
Reply from 12.0.0.2: Destination net unreachable.
Reply from 12.0.0.2: Destination net unreachable.
Reply from 12.0.0.2: Destination net unreachable.
Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS\system32>
```

（4）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试路由器 R2 上的 ACL 工作情况。

```
R1#ping 12.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/35/64 ms
```

（5）在路由器 R2 特权用户模式下，键入命令 show access-lists 显示已创建的 ACL 内容及数据包命中情况。

```
R2#show access-lists
Standard IP access list STDACL1
    10 permit 12.0.0.1 (15 matches)
    20 deny   any (12 matches)
```

【实训报告要求】

1．简述 ACL 的概念和分类。
2．简述标准 ACL 的工作机制。
3．写出配置和查看标准 ACL 的步骤和命令。
4．写出配置命名标准 ACL 的步骤和命令。

实训 2-7　扩展 ACL 配置

【实训目的】

1．了解扩展 ACL 的特点。
2．掌握扩展 ACL 的配置、验证方法。
3．掌握扩展命名 ACL 的配置、验证方法。

【实训任务】

1．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。
2．配置扩展命名 ACL 对流入、流出路由器的不同类型服务数据加以限制。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

在本实训环境中，PC 工作站通过逻辑网络适配器 Loopback 0（简称 Loop0 或 Lo0）和路由器 R1 的快速以太网接口 fastEthernet 0/0 连接。路由器 R1 通过接口 serial 0/0 和路由器 R2 的 serial 0/0 接口连接。对路由器 R1 的初始配置是通过 PC 工作站端 telnet 程序连接到模拟路由器的监听端口 3001 来实现，对路由器 R2 的初始配置是通过 PC 工作站端 telnet 程序连接到模拟路由器的监听端口 3002 来实现。为了模拟路由器 R2 连接的第二个网段，在路由器 R2 上创建了一个环回接口 loopback0 并设置 IP 地址为 2.2.2.2/32。

实训环境如图 2-15 所示。

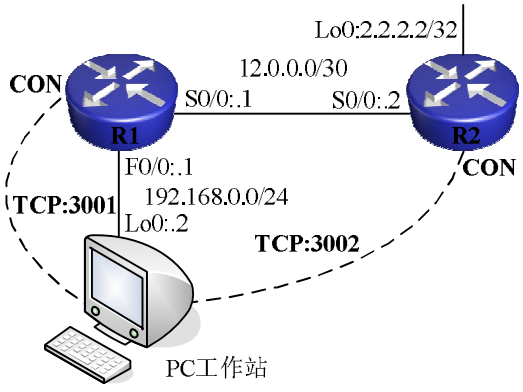

图 2-15　“扩展 ACL 配置”实训环境

【相关知识】

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。

配置标准访问控制列表也需要两个步骤：

第一步，定义允许或禁止报文的描述语句（访问列表），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 及 2000～2699 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。

第二步，将访问列表应用到路由器的具体接口（应用访问组），IP 访问控制组语句的命令格式为：

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

在配置扩展 IP 访问控制列表时需要特别注意以下问题：

- 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。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-15 设计、编写 Dynagen 所需 Lab 2-7.net 文件（这里采用 Cisco 2691 镜像文件 c2691-jk9s-mz.123-18a.bin，注意使用前将其解压缩并重命名为 c2691-jk9s-mz.123-18a.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

```
#Lab 2-7
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[2691]]
        ram = 128
        image = C:\Dynamips\images\c2691-jk9s-mz.123-18a.img
        idlepc = 0x604bfef0
    [[router r1]]
        model = 2691
        console = 3001
        s0/0 = R2 s0/0
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
    [[router r2]]
        model = 2691
        console = 3002
```

3. 启动、登录路由器 R1、R2

按照实训 2-1 中的步骤启动并登录路由器 R1、R2。

4. 配置路由器 R1、R2 基本参数

按照实训 2-2 中的步骤配置路由器 R1、R2 的基本参数。

5. 配置路由器 R1、R2 接口参数

按照图 2-15 配置路由器 R1 的串行接口 serial 0/0 接口 IP 地址（12.0.0.1/30）、路由器 R2 的串行接口 serial 0/0 接口 IP 地址（12.0.0.2/30）并同时激活接口。

6. 配置路由器 R2 上的环回接口 loopback0

在路由器 R2 的全局配置模式下，键入命令 interface loopback 0 并回车进入接口配置模式，键入命令 ip address 2.2.2.2 255.255.255.255 并回车设置环回接口的 IP 地址为 2.2.2.2/32。

```
R2(config)#interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
```

7. 配置路由器 R1 上的静态路由

为了使得路由器 R1 可以将数据包发往 2.2.2.2/32 网段，可以在路由器 R1 上设置一条指向路由器 R2 的静态路由。这里配置一条指向路由器 R1 的默认路由。

在路由器 R1 的全局配置模式下，键入命令 ip route 0.0.0.0 0.0.0.0 12.0.0.2 并回车，设置去往未知网络的数据包的下一跳是路由器 R2 的串行接口 serial 0/0 的地址。

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.0.0.2
```

8. 配置路由器 R2 上的静态路由

为了使得路由器 R2 可以将数据包发往 192.168.0.0/24 网段，需要在路由器 R2 上设置一条指向路由器 R1 的静态路由。

在路由器 R2 的全局配置模式下，键入命令 ip route 192.168.0.0 255.255.255.0 12.0.0.1 并回车，设置去往网络 192.168.0.0/24 的数据包的下一跳是路由器 R1 的串行接口 serial 0/0 的地址。

```
R2(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.1
```

9. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（3）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（4）利用 MS-DOS 命令 ping 2.2.2.2 测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

10. 配置、测试扩展 ACL

（1）在路由器 R1 全局配置模式下，键入命令 access-list 100 deny icmp 192.168.0.0 0.0.0.255 host 2.2.2.2 并回车，创建编号为 100 的扩展 ACL 并拒绝源自 192.168.0.0/24 网段、目标地址是 2.2.2.2/32 的 ICMP 类型数据包，键入命令 access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 23 并回车允许源自 192.168.0.0/24 网段、到任意目标地址的 TCP 类型、目标端口号是 23（telnet 服务）的数据包，键入命令 access-list 100 deny ip any any 并回车拒绝所有其他流量，键入命令 end 并回车返回特权用户模式，键入命令 show access-lists 并回车显示已

创建的 ACL 内容。

```
R1(config)#access-list 100 deny icmp 192.168.0.0 0.0.0.255 host 2.2.2.2
R1(config)#access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 23
R1(config)#access-list 100 deny ip any any
R1(config-if)#end
R1#show access-lists
Extended IP access list 100
    10 deny icmp 192.168.0.0 0.0.0.255 host 2.2.2.2
    20 permit tcp 192.168.0.0 0.0.0.255 any eq telnet
    30 deny ip any any
```

（2）在路由器 R1 全局配置模式下，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 ip access-group 100 out 并回车将刚才定义的 100 号 ACL 应用到路由器 R1 的串行接口 serial 0/0 的出方向，即指明在数据包流出路由器 R1 的串行接口 serial 0/0 时进行 ACL 检查。

```
R1(config)#interface serial 0/0
R1(config-if)#ip access-group 100 out
```

（3）在 PC 工作站上利用 MS-DOS 命令 ping 2.2.2.2 测试路由器 R1 上的 ACL 工作情况。

```
C:\WINDOWS\system32>ping 2.2.2.2
Pinging 2.2.2.2 with 32 bytes of data:
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Ping statistics for 2.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS\system32>
```

（4）在 PC 工作站上利用 MS-DOS 命令 telnet 2.2.2.2 测试路由器 R1 上的 ACL 工作情况。

```
User Access Verification
Password:
R2>
```

（5）在路由器 R1 特权用户模式下，键入命令 show access-lists 显示已创建的 ACL 内容及数据包命中情况。

```
R1#show access-lists
Extended IP access list 100
    10 deny icmp 192.168.0.0 0.0.0.255 host 2.2.2.2 (8 matches)
    20 permit tcp 192.168.0.0 0.0.0.255 any eq telnet (19 matches)
    30 deny ip any any (8 matches)
```

11. 配置、测试扩展命名 ACL

（1）在路由器 R1 全局配置模式下，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 no ip access-group 100 in 并回车删除 100 号 ACL 在路由器 R1 的串行接口 serial 0/0 的出方向上的应用，键入命令 exit 并回车退回到全局配置模式，键入命令 no access-list 100 并回车删除 100 号 ACL。

```
R1(config)#interface serial 0/0
R1(config-if)#no ip access-group 100 out
R1(config-if)#exit
R1(config)#no access-list 100
```

（2）在路由器 R1 全局配置模式下，键入 ip access-list extended ETDACL1 并回车创建名称为“ETDACL1”的扩展命名 ACL 并进入扩展命名 ACL 配置模式，键入命令 permit icmp 192.168.0.0 0.0.0.255 host 2.2.2.2 并回车允许源自 192.168.0.0/24 网段、目标地址是 2.2.2.2/32 的 ICMP 类型数据包，键入命令 permit tcp 192.168.0.0 0.0.0.255 host 2.2.2.2 eq telnet 并回车允许源自 192.168.0.0/24 网段、目标地址是 2.2.2.2/32 的 telnet 数据包，键入命令 deny ip any any 并回车拒绝所有其他流量，键入命令 end 并回车返回特权用户模式，键入命令 show access-lists 显示已创建的 ACL 内容。

```
R1(config)#ip access-list extended ETDACL1
R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 2.2.2.2
R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.0.255 host 2.2.2.2 eq telnet
R1(config-ext-nacl)#deny ip any any
R1(config-std-nacl)#end
R1#show access-list
Extended IP access list ETDACL1
    10 permit icmp 192.168.0.0 0.0.0.255 host 2.2.2.2
    20 permit tcp 192.168.0.0 0.0.0.255 host 2.2.2.2 eq telnet
    30 deny ip any any
```

（3）在路由器 R1 全局配置模式下，键入命令 interface serial 0/0 并回车进入接口配置模式，键入命令 ip access-group ETDACL1 out 并回车将刚才定义的扩展命令 ACL 应用到路由器 R1 的串行接口 serial 0/0 的出方向，即指明在数据包流出路由器 R1 的串行接口 serial 0/0 时进行 ACL 检查。

```
R1(config)#interface serial 0/0
R1(config-if)#ip access-group ETDACL1 out
```

（4）在 PC 工作站上分别 ping 2.2.2.2 和 12.0.0.2 测试路由器 R2 上的 ACL 工作情况。

```
C:\WINDOWS\system32>ping 2.2.2.2
Pinging 2.2.2.2 with 32 bytes of data:
Reply from 2.2.2.2: bytes=32 time=69ms TTL=254
Reply from 2.2.2.2: bytes=32 time=46ms TTL=254
Reply from 2.2.2.2: bytes=32 time=46ms TTL=254
Reply from 2.2.2.2: bytes=32 time=15ms TTL=254
Ping statistics for 2.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 69ms, Average = 44ms
C:\WINDOWS\system32>ping 12.0.0.2
Pinging 12.0.0.2 with 32 bytes of data:
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
```

```
Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS\system32>
```

（5）在 PC 工作站上 telnet 2.2.2.2 测试路由器 R1 上的 ACL 工作情况。

```
User Access Verification
Password:
R2>
```

（6）在 PC 工作站上 telnet 12.0.0.2 测试路由器 R1 上的 ACL 工作情况。

```
C:\WINDOWS\system32>telnet 12.0.0.2
正在连接到 12.0.0.2...不能打开到主机的连接， 在端口 23：连接失败
```

（7）在路由器 R1 特权用户模式下，键入命令 show access-lists 显示已创建的 ACL 内容及数据包命中情况。

```
R1#show access-lists
Extended IP access list ETDACL1
    10 permit icmp 192.168.0.0 0.0.0.255 host 2.2.2.2 (4 matches)
    20 permit tcp 192.168.0.0 0.0.0.255 host 2.2.2.2 eq telnet (19 matches)
    30 deny ip any any (14 matches)
```

【实训报告要求】

1．简述扩展 ACL 的工作机制。
2．写出配置扩展 ACL 的步骤和命令。
3．写出配置扩展命名 ACL 的步骤和命令。

实训 2-8　加强路由器登录安全性

【实训目的】

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。

【实训任务】

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。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-16 所示。

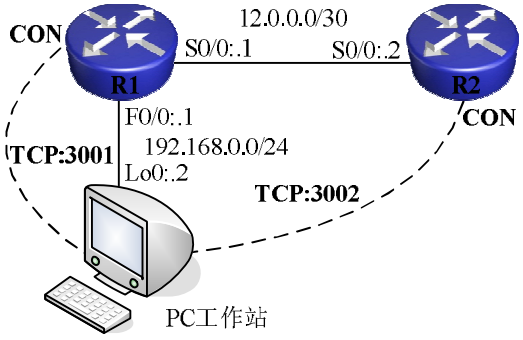

图 2-16　“加强路由器登录安全性”实训环境

【相关知识】

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）。为了增强安全性及增加审计的可能性，一般建议结合采用用户名的身份认证方式。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。

为了加强路由器自身的安全，还可以对路由器的远程 telnet 访问的位置加以限制。这可以使用访问类语句进行 VTY 访问控制。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-16 设计、编写 Dynagen 所需 Lab 2-8.net 文件（这里采用 Cisco 2691 镜像文件 c2691-jk9s-mz.123-18a.bin，注意使用前将其解压缩并重命名为 c2691-jk9s-mz.123-18a.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

```
#Lab 2-8
autostart = False
[localhost]
    workingdir = C:\Dynamips\tmp
    [[2691]]
        ram = 128
        image = C:\Dynamips\images\c2691-jk9s-mz.123-18a.img
        idlepc = 0x604bfef0
    [[router r1]]
        model = 2691
        console = 3001
        s0/0 = R2 s0/0
    f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}
    [[router r2]]
```

- model = 2691
- console = 3002

3. 启动、登录路由器 R1、R2

按照实训 2-1 中的步骤启动并登录路由器 R1、R2。

4. 配置路由器 R1、R2 基本参数

按照实训 2-2 中的步骤配置路由器 R1、R2 的基本参数。

5. 配置路由器 R1、R2 接口参数

按照图 2-16 配置路由器 R1 的串行接口 serial 0/0 接口 IP 地址（12.0.0.1/30）、路由器 R2 的串行接口 serial 0/0 接口 IP 地址（12.0.0.2/30）并同时激活接口。

6. 配置路由器 R2 上的静态路由

为了使得路由器 R2 可以将数据包发往 192.168.0.0/24 网段，需要在路由器 R2 上设置一条指向路由器 R1 的静态路由。

在路由器 R2 的全局配置模式下，键入命令 ip route 192.168.0.0 255.255.255.0 12.0.0.1 并回车，设置去往网络 192.168.0.0/24 的数据包的下一跳是路由器 R1 的串行接口 serial 0/0 的地址。

```
R2(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.1
```

7. 连通性测试

（1）利用 MS-DOS 命令 ipconfig 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（3）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（4）利用 MS-DOS 命令 ping 12.0.0.2 测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

8. 配置、测试本地身份认证

（1）在路由器 R1 特权用户模式下，键入命令 telnet 12.0.0.2 并回车，输入口令 cisco 并回车登录到路由器 R2，键入命令 enable 并回车，输入口令 cisco 并回车进入路由器 R2 的特权用户模式，键入命令 exit 退出路由器 R2 回到路由器 R1 的特权用户模式。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ... Open
User Access Verification
Password:
R2>enable
Password:
R2#exit
[Connection to 12.0.0.2 closed by foreign host]
R1#
```

（2）在路由器 R2 全局配置模式下，键入命令 username usr1 password usr1pwd 并回车建立本地用户名 usr1，对应的口令为 usr1pwd，键入命令 line vty 0 4 并回车转换到虚拟终端线配置模式，键入命令 login local 并回车将虚拟终端线的默认身份认证方式（口令认证）改为本

地认证。

```
R2(config)#username usr1 password usr1pwd
R2(config)#line vty 0 4
R2(config-line)#login local
```

（3）在路由器 R1 特权用户模式下，键入命令 telnet 12.0.0.2 并回车，输入用户名 usr1 并回车，输入口令 usr1pwd 并回车登录到路由器 R2，键入命令 enable 并回车，输入口令 cisco 并回车进入路由器 R2 的特权用户模式，键入命令 exit 并回车退出路由器 R2 回到路由器 R1 的特权用户模式。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ... Open
User Access Verification
Username: usr1
Password:
R2>enable
Password:
R2#exit
[Connection to 12.0.0.2 closed by foreign host]
R1#
```

9. 配置、测试 telnet 访问位置限制

（1）在 PC 工作站上 telnet 12.0.0.2 测试路由器 R2 上的服务情况。

```
User Access Verification
Username: usr1
Password:
R2>
```

（2）在路由器 R2 全局配置模式下，键入命令 access-list 1 permit 192.168.0.0 0.0.0.255 并回车，创建编号为 1 的标准 ACL 并允许来自 192.168.0.0/24 网段的数据包，键入命令 line vty 0 4 并回车转换到虚拟终端线配置模式，键入命令 access-class 1 in 并回车将上述 ACL 应用到虚拟终端线。

```
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R2(config)#line vty 0 4
R2(config-line)#access-class 1 in
```

（3）在 PC 工作站上 telnet 12.0.0.2 测试路由器 R2 上访问类语句的工作情况。

```
User Access Verification
Username: usr1
Password:
R2>
```

（4）在路由器 R1 特权用户模式下，键入命令 telnet 12.0.0.2 并回车测试路由器 R2 上访问类语句的工作情况。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ...
% Connection refused by remote host
R1#
```

【实训报告要求】

1．写出路由器本地登录认证的配置步骤和命令。
2．写出对路由器的管理位置加以限制的步骤和命令。

实训 2-9　HTTP/HTTPS/SSH 配置

【实训目的】

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

【实训任务】

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。
3．启用、测试路由器上 SSH 服务。

【实训设备】

PC 工作站一台（运行 Windows XP 操作系统）；Dynamips/Dynagen 软件；超级终端应用程序或 SecureCRT 软件。

【实训环境】

实训环境如图 2-17 所示。

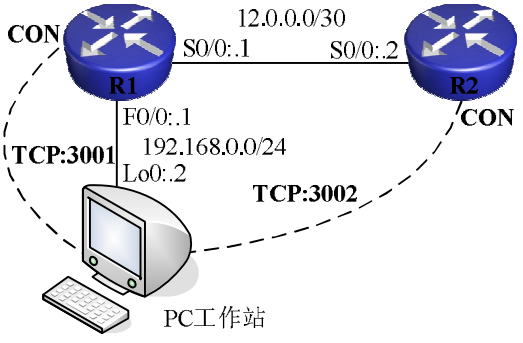

图 2-17　“HTTP/HTTPS/SSH 配置”实训环境

【相关知识】

除了通过 CLI 命令行的方式来配置路由器外，IOS 还提供了较为友好的 HTTP 界面访问

方式，方便网络管理人员管理路由器。用户可以通过 HTTP 或 HTTPS 方式来管理路由器。

在某些版本的 IOS 中，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接口 IP 地址，并输入正确的加密使能密码后就可以以 HTTP 方式来访问路由器了。

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，还可以通过 ACL 限制 HTTP 访问位置。但尽管可以通过上述方法增强路由器的 HTTP 访问安全性，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。如果想要以一种安全的方式使用 HTTP 方式访问界面，可以配置路由器启用安全的 HTTP 服务，即 HTTPS，通过证书认证，密钥交换等技术加密 HTTP 会话数据。

此外，虽然绝大多数网络设备支持远程登录协议 telnet，但由于 telnet 协议的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 协议的 22 号端口，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 等加密算法）。SSH 通常有 2 个主要版本，即 SSHv1、SSHv2。

Cisco 路由器不但可以作为 SSH 服务器端，还可以作为 SSH 客户端以 SSH 的方式登录到其他网络设备上。

【实训步骤】

1. PC 工作站网卡配置

将 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址配置为 192.168.0.2，子网掩码配置为 255.255.255.0，默认网关配置为 192.168.0.1。

2. 设计、编写 Dynagen 所需.net 文件

按照图 2-17 设计、编写 Dynagen 所需 Lab 2-9.net 文件（这里采用 Cisco 2691 镜像文件 c2691-advsecurityk9-mz.124-11.T2.bin，注意使用前将其解压缩并重命名为 c2691-advsecurityk9-mz.124-11.T2.img 并将其复制到 C:\Dynamips\images 文件夹下），内容如下：

- `#Lab 2-9`
- `autostart = False`
- `[localhost]`
  - `workingdir = C:\Dynamips\tmp`
  - `[[2691]]`
    - `ram = 128`
    - `image = C:\Dynamips\images\c2691-advsecurityk9-mz.124-11.T2.img`
    - `idlepc = 0x60c1054c`
  - `[[router r1]]`
    - `model = 2691`
    - `console = 3001`
    - `s0/0 = R2 s0/0`
  - `f0/0 = NIO_gen_eth:\Device\NPF_{910A39C1-3C12-48AF-AFF6-D8C98160D749}`
  - `[[router r2]]`

- model = 2691
- console = 3002

3. 启动、登录路由器 R1、R2

按照实训 2-1 中的步骤启动并登录路由器 R1、R2。

4. 配置路由器 R1、R2 基本参数

按照实训 2-2 中的步骤配置路由器 R1、R2 的基本参数。

5. 配置路由器 R1、R2 接口参数

按照图 2-17 配置路由器 R1 的串行接口 serial 0/0 接口 IP 地址（12.0.0.1/30）、路由器 R2 的串行接口 serial 0/0 接口 IP 地址（12.0.0.2/30）并同时激活接口。

6. 配置路由器 R2 上的静态路由

为了使得路由器 R2 可以将数据包发往 192.168.0.0/24 网段，需要在路由器 R2 上设置一条指向路由器 R1 的静态路由。

在路由器 R2 的全局配置模式下，键入命令 ip route 192.168.0.0 255.255.255.0 12.0.0.1 并回车，设置去往网络 192.168.0.0/24 的数据包的下一跳是路由器 R1 的串行接口 serial 0/0 的地址。

```
R2(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.1
```

7. 连通性测试

（1）利用 MS-DOS 命令 IPCONFIG 检查 PC 工作站逻辑网络适配器 Loopback 0 的 IP 地址信息配置是否正确。

（2）利用 MS-DOS 命令 ping 192.168.0.1 测试到路由器 R1 的快速以太网接口 fastEthernet 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（3）在路由器 R1 的特权用户模式下键入命令 ping 12.0.0.2 并回车，测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

（4）利用 MS-DOS 命令 ping 12.0.0.2 测试到路由器 R2 的串行接口 serial 0/0 的连通性。如果没有测试成功，按照本实训前面的步骤进行检查并重新测试直至成功。

8. 配置、测试 HTTP 服务

（1）在路由器 R2 特权用户模式下，键入命令 show running-config | include http server 并回车查看本 IOS 对 HTTP 服务的默认配置。

```
R2#show running-config | include http
server
ip http server
```

（2）在 PC 工作站打开浏览器程序，在浏览器地址栏中输入路由器 R2 的串行接口 serial 0/0 的 IP 地址（12.0.0.2）并回车，在弹出的“连接到…”对话框中保持用户名为空白，输入加密使能密码（cisco），单击“确定”按钮后以 HTTP 方式来访问路由器，如图 2-18 和图 2-19 所示。

图 2-18　输入加密使能密码

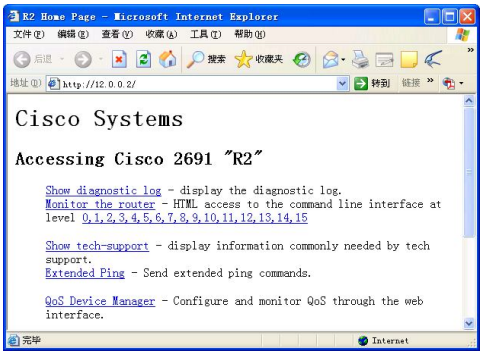

图 2-19　以 HTTP 方式来访问路由器

（3）在路由器 R2 特权用户模式下，键入命令 show ip http server status 显示路由器 R2 上的 HTTP/HTTPS 服务状态信息。注意观察命令输出中的加粗字体部分。

```
R2#show ip http server status
HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5
rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

（4）在路由器 R2 全局配置模式下，键入命令 access-list 1 permit host 192.168.0.2 并回车创建编号为 1 的标准 ACL，允许源自 IP 地址为 192.168.0.2 的主机访问，键入命令 access-list 1 deny any 并回车拒绝所有源自其他 IP 地址的访问，键入命令 ip http access-class 1 并回车设置按照编号为 1 的 ACL 检查对路由器 R2 的 HTTP 访问。

```
R2(config)#access-list 1 permit host 192.168.0.2
R2(config)#access-list 1 deny any
R2(config)#ip http access-class 1
```

（5）将 PC 工作站的逻辑网络适配器 Loopback 0 的 IP 地址更改为 192.168.0.3，子网掩码和默认网关保持不变。再次打开浏览器程序访问路由器 R2 的串行接口 serial 0/0 的 IP 地址（12.0.0.2）并回车，观察浏览器提示的“无法显示网页”的信息。

9. 配置、测试 http 访问身份认证方式

（1）将 PC 工作站的逻辑网络适配器 Loopback 0 的 IP 地址更改为 192.168.0.2，子网掩码和默认网关保持不变。

（2）在路由器 R2 全局配置模式下，键入命令 username usr1 privilege 15 password usr1pwd 并回车建立一个级别为 15 级、用户名 usr1、对应的口令为 usr1pwd 的本地用户，键入命令 ip http authentication local 并回车设置对路由器 R2 上的 HTTP 服务的身份认证方式为本地认证。

```
R2(config)#username usr1 privilege 15 password usr1pwd
R2(config)#ip http authentication local
```

（3）在 PC 工作站打开浏览器程序，在浏览器地址栏中输入路由器 R2 的串行接口 serial 0/0 的 IP 地址（12.0.0.2）并回车，在弹出的“连接到…”对话框中，输入用户名为 usr1，输入密码为 usr1pwd，单击“确定”按钮后以 HTTP 方式来访问路由器。

10. 关闭 HTTP 服务

（1）在路由器 R2 全局配置模式下，键入命令 no ip http server 并回车关闭路由器 R2 上的 HTTP 服务。

```
R2(config)#no ip http server
```

（2）打开 PC 工作站的浏览器程序，并访问路由器 R2 的串行接口 serial 0/0 的 IP 地址（12.0.0.2）并回车，观察浏览器提示的“无法显示网页”的信息。

11. 配置、测试 HTTPS 服务

（1）在路由器 R2 全局配置模式下，键入命令 ip domain-name mydomain.com 并回车设置路由器 R2 的域名为“mydomain.com”，键入命令 ip http secure-server 并回车启用 HTTPS 服务，键入命令 crypto key generate rsa 并回车产生 HTTPS 所需的 RSA 密钥对，当要求输入 RSA 密钥长度时，输入 1024 位并回车完成 HTTPS 的配置。当密钥产生后，控制台会出现 SSH 服务被启用的提示，注意观察命令输出中的加粗字体部分。

```
R2(config)#user httpsusr privilege 15 password passwd
R2(config)#ip domain-name mydomain.com
R2(config)#ip http secure-server
R2(config)#crypto key generate rsa
The name for the keys will be: R2.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]: 1024
% Generating 1024 bit RSA keys ...[OK]
R2(config)#
*Mar  1 07:33:37.890: %SSH-5-ENABLED: SSH 1.5 has been enabled
R2(config)#
```

（2）在路由器 R2 特权用户模式下，键入命令 show ip http server secure status 并回车显示路由器 R2 上的 HTTPS 服务状态信息。

```
R2#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5
rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

（3）在 PC 工作站打开浏览器程序，在浏览器地址栏中输入“https://12.0.0.2”并回车，在弹出的“安全警报”对话框中单击“是”按钮确定，如图 2-20 所示。在随后弹出的“连接到…”对话框中输入用户名为 usr1，输入密码为 usr1pwd，如图 2-21 所示。单击“确定”按钮后以 HTTPS 方式来访问路由器。

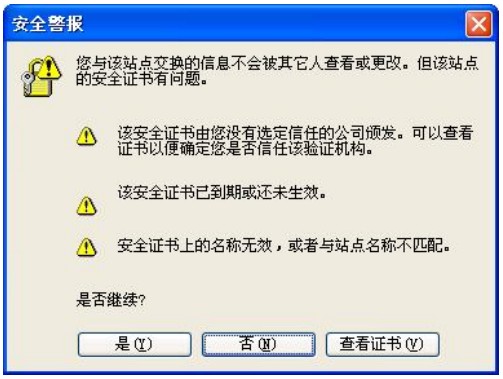

图 2-20　“安全警报”对话框

图 2-21　输入用户名和密码

（4）在路由器 R2 全局配置模式下，键入命令 ip http secure-port 4444 并回车将 HTTPS 的服务端口改为 4444（默认为 443）。

```
R2(config)#ip http secure-port 4444
```

（5）在 PC 工作站打开浏览器程序，在浏览器地址栏中输入“https://12.0.0.2”并回车，观察浏览器提示的“无法显示网页”的信息。随后，在浏览器地址栏中输入“https://12.0.0.2:4444”并回车，在弹出的“连接到…”对话框中输入用户名为 usr1，输入密码为 usr1pwd，单击“确定”按钮后以端口号 4444 访问路由器 R2 上的 HTTPS 服务。

12. 配置、测试 SSH 服务

（1）在路由器 R2 全局配置模式下，键入命令 ip domain-name mydomain.com 并回车设置路由器 R2 的域名为“mydomain.com”，键入命令 username sshusr privilege 15 password sshusrpwd 并回车建立级别为 15 的本地用户 sshusr，口令为 sshusrpwd，键入命令 line vty 0 4 并回车进入 VTY 线路配置模式，键入命令 login local 并回车启用本地用户名、口令验证，键入命令 exit 并回车回到全局配置模式，键入命令 crypto key generate rsa 并回车产生 HTTPS 所需的 RSA 密钥对，当要求输入 RSA 密钥长度时，输入 1024 位并回车完成 SSH 的配置。当密钥产生后，控制台会出现 SSH 服务被启用的提示，注意观察命令输出中的加粗字体部分。

```
R2(config)#ip domain-name mydomain.com
R2(config)#username sshusr privilege 15 password sshusrpwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#exit
R2(config)#crypto key generate rsa
The name for the keys will be: R2.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#
*Mar  1 00:02:45.567: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#
```

（2）在路由器 R2 特权用户模式下，键入命令 show ip ssh 并回车显示路由器 R2 上的 SSH 服务状态信息。

```
R2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

（3）启动 PC 工作站上的 SecureCRT 软件，在 SecureCRT 工具栏上单击“快速连接”图标，如图 2-22 所示。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 R2 的 IP 地址（12.0.0.2），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 2-23 所示。

图 2-22 “快速连接”图标

图 2-23 “快速连接”对话框

（4）随后弹出窗口询问，对于新建主机密钥的保存方式，如图 2-24 所示，选择“只接受一次”或“接受并保存”继续。

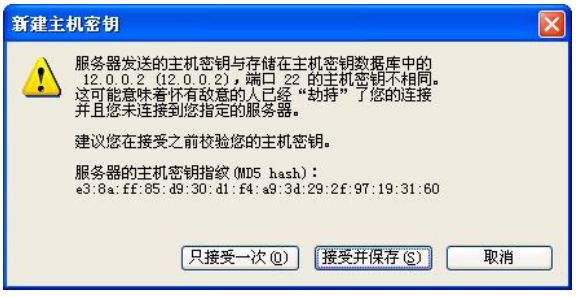

图 2-24 “新建主机密钥”对话框

（5）在随后弹出的对话框中输入口令，单击“确定”按钮继续，如图 2-25 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 2-26 所示。

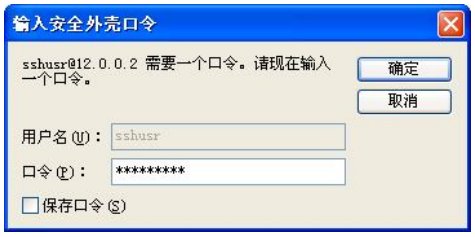

图 2-25　输入口令

图 2-26　以 SSH 方式成功登录到路由器

（6）在路由器 R2 特权用户模式下，键入命令 show ssh 并回车显示当前 ssh 服务器连接状态，注意观察命令输出中的加粗字体部分。

```
R2#show ssh
Connection      Version Encryption      State                 Username
0               1.5     3DES            Session started       sshusr
%No SSHv2 server connections running.
```

（7）在路由器 R1 特权用户模式下，键入命令 ssh -l sshusr 12.0.0.2 并回车，在输入正确的密码后，以用户名 sshusr 登录路由器 R2。

```
R1#ssh -l sshusr 12.0.0.2
Password:
R2#
```

（8）在路由器 R2 全局配置模式下，键入命令 line vty 0 4 并回车进入 VTY 线路配置模式，键入命令 transport input ssh 并回车设置 VTY 线路只接受 SSH 方式登录。

```
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
```

（9）在路由器 R1 特权用户模式下，键入命令 telnet 12.0.0.2 并回车尝试以 telnet 方式登录路由器 R2。

```
R1#telnet 12.0.0.2
Trying 12.0.0.2 ...
% Connection refused by remote host
R1#
```

（10）在路由器 R2 全局配置模式下，键入命令 ip ssh version 2 并回车设置本 SSH 服务的版本号为 2。

```
R2(config)#ip ssh version 2
```

（11）仿照前面的步骤（3）~（5），在 SecureCRT 软件创建“快速连接”，不同的是本次选择连接协议为 SSH2。在以 SSH 方式成功登录到路由器 R2 后，键入命令 show ip ssh 并回车显示路由器 R2 上的 SSH 服务状态信息。键入命令 show ssh 并回车显示当前 ssh 服务器连接状态，注意观察命令输出中的加粗字体部分。

```
R2#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R2#show ssh
Connection Version Mode Encryption  Hmac        State               Username
0          2.0     IN   aes256-cbc  hmac-sha1   Session started     sshusr
0          2.0     OUT  aes256-cbc  hmac-sha1   Session started     sshusr
```

```
%No SSHv1 server connections running.
```

【实训报告要求】

1．写出配置、测试路由器上 HTTP 服务的步骤和命令。
2．写出配置、测试路由器上 HTTPS 服务的步骤和命令。
3．写出配置、测试路由器上 SSH 服务的步骤和命令。