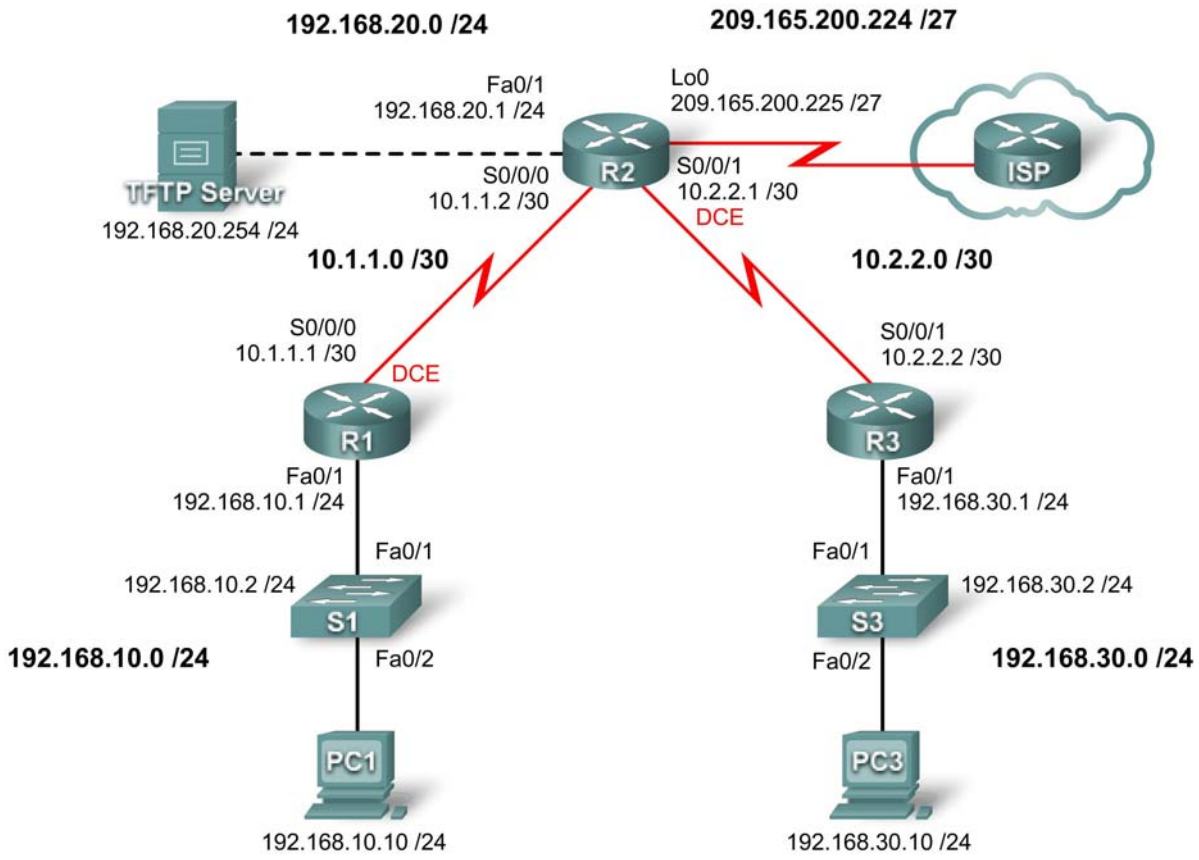
实验 4.6.1：基本安全配置

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	**Fa0/1**	192.168.10.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
R2	**Fa0/1**	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	不适用

R3	**Fa0/1**	192.168.30.1	255.255.255.0	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用
S1	**VLAN10**	192.168.10.2	255.255.255.0	不适用
S3	**VLAN20**	192.168.30.2	255.255.255.0	不适用
PC1	**网卡**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**网卡**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**网卡**	192.168.20.254	255.255.255.0	192.168.20.1

学习目标

完成本实验后，您将能够：

- 根据拓扑图完成网络电缆连接
- 清除启动配置，重新启动路由器使其处于默认状态
- 在路由器上执行基本配置任务
- 配置基本路由器安全功能
- 禁用未使用的 Cisco 服务和接口
- 保护企业网络免遭基本的外部和内部攻击
- 了解并管理 Cisco IOS 配置文件和 Cisco 文件系统
- 设置并使用 Cisco SDM（安全设备管理器）和 SDM Express 来配置基本的路由器安全功能
- 在交换机上配置 VLAN

场景

在本实验中，您将学习如何对拓扑图中显示的网络配置基本的网络安全性。您会学习如何以三种方式配置路由器安全性：CLI、auto-secure 功能以及 Cisco SDM。您还将学习如何管理 Cisco IOS 软件。

任务 1：准备网络

步骤 1：根据拓扑图所示完成网络电缆连接。

您可使用实验室中现有的、具有拓扑中所示接口的路由器。

注：开发和测试本实验时使用的是 1841 路由器。如果使用 1700、2500 或 2600 系列路由器，其路由器输出和接口描述可能会有所不同。

步骤 2：清除路由器的所有配置。

任务 2：执行基本的路由器配置

步骤 1：配置路由器。

根据以下说明配置 R1、R2 和 R3 路由器：

- 依照拓扑图配置路由器主机名。
- 禁用 DNS 查找。
- 配置当日消息标语。
- 在 R1、R2 和 R3 上配置 IP 地址。
- 在所有路由器上对所有网络启用 RIP 第 2 版。
- 在 R2 上创建环回接口以模拟通往 Internet 的连接。
- 在 R2 上配置 TFTP 服务器。如果您需要下载 TFTP 服务器软件，则可访问：http://tftpd32.jounin.net/

步骤 2：配置以太网接口。

使用本实验开头部分地址表中的 IP 地址和默认网关配置 PC1、PC3 和 TFTP Server 的以太网接口。

步骤 3：通过在每台 PC 和 TFPT Server 上 ping 默认网关来测试 PC 配置。

任务 3：保护路由器免遭未授权访问

步骤 1：配置加密口令和 AAA 身份验证。

使用 R1 上的本地数据库来配置加密口令。在本实验中，请统一使用 **ciscoccna** 口令。

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

配置使能加密口令在避免路由器遭受攻击方面能发挥怎样的作用？

_____

_____

_____

username 命令用于创建用户名和口令，并将它们存储在路由器本地。用户的默认权限等级是 0（最低访问等级）。您可通过在 **password** 关键字前添加关键字 **privilege** *0-15* 来更改用户的访问等级。

```
R1(config)#username ccna password ciscoccna
```

aaa 命令用于在路由器上全局启用 AAA（身份验证、授权和记帐）。此功能会在连接路由器时用到。

```
R1(config)#aaa new-model
```

您可以创建一份身份验证列表并应用到 vty 和控制台线路上，当有人试图登录设备时，设备就会对照列表进行检查。**local** 关键字指出该用户数据库存储在路由器本地。

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

以下命令告诉路由器：对试图连接到路由器的用户，必须使用刚才创建的列表验证其身份。

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

观察下面一段运行配置，您认为哪个地方存在安全隐患？

```
R1#show run
〈省略部分输出〉
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
〈省略部分输出〉
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 logging synchronous
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

_____

_____

_____

要对口令进行简单加密，在全局配置模式下输入以下命令：

```
R1(config)#service password-encryption
```

使用 **show run** 命令进行检验。

```
R1#show run
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
〈省略部分输出〉
```

```
!
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 logging synchronous
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

步骤 2：保护控制台线路和 vty 线路。

您可设置路由器，使其注销空闲时间达到指定时间的线路。如果网络工程师登录到一台网络设备上，然后突然有事离开，此命令便会在指定时间后自动将该用户注销。以下命令在 5 分钟后注销线路。

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

以下命令用于防止暴力型登录尝试。当有人在 2 分钟内 5 次登录失败时，路由器将禁止其在接下来的 5 分钟内登录。为方便实验，此处我们将该值特意设得较低。此外，每次发生这种情况时，将其记录到日志中。

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 5 log
```

要检验这些命令的作用，请使用不正确的用户名和口令通过 Telnet 从 R2 连接 R1。

在 **R2** 上：

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication failed

User Access Verification

Username: cisco
Password:

% Authentication failed

[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

在 **R1** 上：

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

任务 4：保护对网络的访问

步骤 1：阻止 RIP 路由更新传播。

在启用了 RIP 的网段上，谁能接收 RIP 更新？此设置是否有必要？

_____

_____

_____

passive-interface 命令可防止路由器发送路由更新到所有接口，只有配置为参与路由更新的接口才能接收。配置 RIP 时应使用此命令。

第一条命令将所有接口置于 passive（被动）模式（即接口仅接收 RIP 更新）。第二条命令将特定接口从 passive 恢复为 active（主动）模式（即可发送也可接收 RIP 更新）。

R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```

步骤 2：阻止非法接收 RIP 更新。

阻止不必要的 RIP 更新传播到整个网络只是保护 RIP 的第一步。接下来应该对 RIP 更新实行口令保护。为此，您必须首先配置要使用的密钥。

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

必须对即将接收 RIP 更新的每台路由器都配置此密钥。

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

要使用密钥，参与 RIP 更新的每个接口都需要进行配置。这些要配置的接口就是之前使用 **no passive-interface** 命令启用的接口。

R1
```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

此时，R1 不再从 R2 接收 RIP 更新，因为 R2 还没有配置为使用路由更新密钥。您可在 R1 上发出 **show ip route** 命令，您会看到路由表中没有来自 R2 的路由。

使用 **clear ip route *** 清除 IP 路由，或等待路由超时。

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *- candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C    192.168.10.0 is directly connected, Serial0/0/0
```

将 R2 和 R3 配置为使用路由验证。记住每个主动接口都必须配置。

R2
```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```

R3
```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

步骤 3：确保 RIP 路由仍能正常工作。

在所有三台路由器都配置为使用路由验证后，路由表中应重新添加了所有 RIP 路由。R1 现在应具有 RIP 传播的所有路由。可使用 **show ip route** 命令来确认这一点。

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *-candidate default, U-per-user static route
       o - ODR, P - periodic downloaded static route
```



```
Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R       10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C       10.1.1.0/24 is directly connected, Serial0/0/0
```

任务 5：使用 SNMP（简单网络管理协议）记录活动

步骤 1：将 SNMP 日志记录配置为发送到 syslog 服务器。

SNMP 日志对于监控网络活动非常有用。其捕获的信息可以发送到网络上的 syslog 服务器，然后可以在服务器上进行分析和归档。在路由器上配置日志记录 (syslog) 时务必非常小心。当选择目标日志主机时，请记住日志主机应该连接到可信的或受保护的网络，或者隔离的专用路由器接口。

在本实验中，将 PC1 配置为 R1 的 syslog 服务器。使用 **logging** 命令来选择 SNMP 消息的目的设备的 IP 地址。在本例中，我们使用 PC1 的 IP 地址。

```
R1(config)#logging 192.168.10.10
```

注：若您想查看 syslog 消息，那么 PC1 应安装有 syslog 软件并运行该软件。

在下一步中，您将定义要发送到 syslog 服务器的消息的严重级别。

步骤 2：配置 SNMP 严重级别。

SNMP 消息的级别可以调整，以便管理员决定要将哪种类型的消息发送到 syslog 设备。路由器支持不同级别的日志记录。这些级别从 0（紧急）到 7（调试），一共分为 8 个级别。其中 0 级表示系统不稳定，7 级则会发送包含路由器信息的消息。要配置严重级别，您需使用各个级别关联的关键字，如下表所示。

严重级别	关键字	说明
0	emergencies	系统不稳定
1	alerts	需要立即采取措施
2	critical	严重情况
3	errors	错误情况
4	warnings	警告情况
5	notifications	正常、但比较重要的情况
6	informational	参考性消息
7	debugging	调试消息

logging trap 命令用于设置严重级别。严重级别包括所指定的级别及更低的级别（智能严重性设置）。将 R1 设置为级别 4，以捕获严重级别为 4、5、6 和 7 的消息。

```
R1(config)#logging trap warnings
```

将严重性设置得过低或过高存在怎样的危险？

_____

_____

_____

注：如果在 PC1 上安装了 syslog 软件，则可利用此软件生成消息并进行查看。

任务 6：禁用未使用的 Cisco 网络服务

步骤 1：禁用未使用的接口。

为什么您应该在网络设备上禁用未使用的接口？

_____

_____

_____

在拓扑图中，您可以看到 R1 应仅使用接口 S0/0/0 和 Fa0/1。R1 上的所有其它接口都应该使用 **shutdown** 接口配置命令管理性关闭 。

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown

*Sep 10 13:40:24.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Sep 10 13:40:25.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

要确定 R1 的所有非活动接口都已关闭，请使用 **show ip interface brief** 命令。手动关闭的接口会显示为 administratively down。

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.10.1    YES manual up                    up
Serial0/0/0            10.1.0.1        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
```

步骤 2：禁用未使用的全局服务。

许多服务在大多数现代网络中都没有必要。未使用的服务保留为启用状态会致使对应端口打开，这些端口可能被网络攻击利用。在 R1 上逐项禁用这些服务。

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
```

```
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

步骤 3：禁用未使用的接口服务。

这些命令在接口级别输入，而且应该应用到 R1 的每个接口上。

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachables
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

禁用 IP 重定向、IP 不可达以及 IP 定向广播可防范哪一类攻击？

_____

_____

_____

步骤 4：使用 AutoSecure 来保护 Cisco 路由器。

只需在 CLI 模式下发出一条命令启用 AutoSecure 功能，您便可禁用可能被网络攻击所利用的常见 IP 服务，同时启用那些可增强网络安全性的 IP 服务和功能。AutoSecure 简化并增强了路由器的安全配置。

利用 AutoSecure 功能，您可更快速地对路由器应用先前配置的那些安全功能（RIP 保护除外）。由于您已对 R1 应用了安全设置，所以请在 R3 上使用 **auto secure** 命令。

```
R3#auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1

Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0/0            unassigned      YES unset  down        down
FastEthernet0/1            192.168.30.1    YES manual up          up
Serial0/0/0                unassigned      YES manual down        down
Serial0/0/1                10.2.2.2        YES manual up          up
```



```
Enter the interface name that is facing the internet: Serial0/0/1
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or
 Is the same as enable password
Enter the new enable password: ciscoccna
Confirm the enable password: ciscoccna
Enter the new enable password: ccnacisco
Confirm the enable password: ccnacisco

Configuration of local user database
Enter the username: ccna
Enter the password: ciscoccna
Confirm the password: ciscoccna
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 300

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 120

Configure SSH server? Yes
Enter domain-name: cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply

Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
```

```
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC firewall feature: no
Tcp intercept feature is used prevent tcp syn attack
On the servers in the network. Create autosec_tcp_intercept_list
To form the list of servers to which the tcp traffic is to be observed

Enable TCP intercept feature: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
line tty 192
 login authentication local_auth
 exec-timeout 15 0
login block-for 300 attempts 5 within 120
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

```
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end
```

```
Apply this configuration to running-config? [yes]:yes

The name for the keys will be: R3.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R3#
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

如您所见，AutoSecure 功能比一行一行地配置速度要快得多。不过，手动操作有自己的优势，我们将在故障排除实验介绍。当您使用 AutoSecure 时，您可能会禁用需要的服务。在使用 AutoSecure 之前，务必认真考虑您到底需要哪些服务。

任务 7：管理 Cisco IOS 和配置文件

步骤 1：显示 Cisco IOS 文件。

Cisco IOS 是路由器运行所需的软件。您的路由器的内存可能足以存储多个 Cisco IOS 映像。您必须知道哪些文件存储在您的路由器上。

发出 **show flash** 命令来查看路由器闪存的内容。

注意：使用有关闪存的命令时必须非常小心。错误键入命令可能导致 Cisco IOS 映像被删除。

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4       833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar

8679424 bytes available (23252992 bytes used)
```

通过观察上面的列表，我们可确定以下事项：

- 此映像用于 1841 路由器 (c**1841**-ipbase-mz.124-1c.bin)。
- 此路由器使用 IP base 映像 (c1841-**ipbase**-mz.124-1c.bin)。
- Cisco IOS 的版本是 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin)。
- 此设备上安装了 SDM (**sdm**config-18xx.cfg, **sdm**.tar)。

您可使用 **dir all** 命令来显示路由器上的所有文件。

```
R2#dir all
Directory of archive:/

No files in directory

No space information available
Directory of system:/

 3  dr-x           0                    <no date>  memory
 1  -rw-         979                    <no date>  running-config
 2  dr-x           0                    <no date>  vfiles
```



```
No space information available
Directory of nvram:/

 189  -rw-         979                    <no date>  startup-config
 190  ----           5                    <no date>  private-config
 191  -rw-         979                    <no date>  underlying-config
   1  -rw-           0                    <no date>  ifIndex-table

196600 bytes total (194540 bytes free)
Directory of flash:/

 1 -rw- 13937472  May 05 2007 20:08:50 +00:00  c1841-ipbase-mz.124-1c.bin
 2 -rw-     1821  May 05 2007 20:25:00 +00:00  sdmconfig-18xx.cfg
 3 -rw-  4734464  May 05 2007 20:25:38 +00:00  sdm.tar
 4 -rw-   833024  May 05 2007 20:26:02 +00:00  es.tar
 5 -rw-  1052160  May 05 2007 20:26:30 +00:00  common.tar
 6 -rw-     1038  May 05 2007 20:26:56 +00:00  home.shtml
 7 -rw-   102400  May 05 2007 20:27:20 +00:00  home.tar
 8 -rw-   491213  May 05 2007 20:27:50 +00:00  128MB.sdf
 9 –rw-   398305  May 05 2007 20:29:08 +00:00  sslclient-win-1.1.0.154.pkg
 10 -rw- 1684577  May 05 2007 20:28:32 +00:00  securedesktop-ios-3.1.1.27-
k9.pkg

31932416 bytes total (8679424 bytes free)
```

步骤 2：使用 TFTP 传输文件。

归档和更新设备的 Cisco IOS 软件时会用到 TFTP。不过在本实验中，我们并不使用实际的 Cisco IOS 文件，因为输入命令时所犯的任何错误都可能导致清除设备的 Cisco IOS 映像。在本节的末尾，有一个示例展示了 Cisco IOS TFTP 传输是怎样的。

为什么拥有 Cisco IOS 软件的更新版本很重要？

_____

_____

_____

当使用 TFTP 传输文件时，务必确保 TFTP 服务器和路由器能够通信。测试通信的方法之一是在两台设备之间 ping。

要开始传输 Cisco IOS 软件，先在 TFTP 服务器的 TFTP 根文件夹下创建一个名为 **test** 的文件。此文件可以是空白的文本文件，因为此步骤的作用仅仅是展示所需的步骤。每个 TFTP 程序存储文件的位置有所不同。参考您 TFTP 服务器的帮助文件以确定根文件夹。

从 R1 检索该文件并将其保存在闪存中。

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254 （TFTP 服务器的 IP 地址）
Source filename []? Test （您创建并保存到 TFTP 服务器的文件的名称）
Destination filename [test]? test-server （该文件保存到路由器时所用的名称，可任意取名）
Accessing tftp://192.168.20.254/test...
Loading test from 192.168.20.254 (via FastEthernet0/1): !
[OK - 1192 bytes]

1192 bytes copied in 0.424 secs (2811 bytes/sec)
```


使用 **show flash** 命令确认该文件已存在于闪存中。

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server

8675328 bytes available (23257088 bytes used)
```

路由器也可充当 TFTP 服务器。当一台设备需要的映像可在另一台设备中找到时，此功能便很有用。我们将把 R2 设置为 R1 的 TFTP 服务器。记住 Cisco IOS 映像特定于路由器平台和内存需求。将 Cisco IOS 映像从一台路由器传输到另一台路由器时务必非常小心。

命令语法为： **tftp-server nvram:** [*filename1* [**alias** *filename2*]

下面的命令用于将 R2 配置为 TFTP 服务器。R2 通过 TFTP 将自己的启动配置文件提供给请求该文件的设备（为简便起见，本例使用启动配置作为例子）。**alias** 关键字允许设备使用别名 **test** 而不是完整文件名来请求文件。

```
R2(config)#tftp-server nvram:startup-config alias test
```

现在我们可以从 R1 向 R2 请求该文件。

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? test
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]

1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

发出 **show flash** 命令，再次确认文件 **test** 是否已成功复制。

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
```

```
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server
12        1192 Sep 12 2007 07:51:04 +00:00 test-router

8671232 bytes available (23261184 bytes used)
```

我们不希望无用的文件占用宝贵的内存空间，所以现在将它们从 R1 的闪存中删除。**执行此操作时请小心谨慎！**若意外清除闪存，您就必须为该路由器重新安装整个 IOS 映像。如果路由器出现提示 **erase flash**（清除闪存），则表示您的操作有误。相信您一般不会希望清除整个闪存。只有当您将 IOS 升级为较大的 IOS 映像时，才可能需要清除整个闪存。如果您看到如示例所示的 **erase flash** 提示，请立即停止操作。不要按 enter 键。马上向教师寻求帮助。

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

使用 **show flash** 命令检查文件是否确实已删除。**这只是一个示例。请勿完成此任务。**

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg

8679424 bytes available (23252992 bytes used)
```

以下是 TFTP 传输 Cisco IOS 映像文件的示例。

请勿在您的路由器上执行此任务。阅读下列代码即可。

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via
Serial0/0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
〈省略部分输出〉
!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]

13937472 bytes copied in 1113.948 secs (12512 bytes/sec)
```

步骤 3：使用 ROMmon 恢复密码。

如果由于口令的缘故（比如不知道口令、丢失口令或忘记口令），您无法再访问设备，那么您可通过更改配置寄存器来获取访问权。配置寄存器告诉路由器在启动时加载哪个配置。在配置寄存器中，您可指示路由器从没有口令保护的空配置启动。

更改配置寄存器的第一步是使用 **show version** 命令查看当前设置。以下步骤在 R3 上执行。

```
R3#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

R3 uptime is 25 minutes
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"

Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
Processor board ID FTX1118X0BN
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

下一步，重新启动路由器并在启动期间执行 break 操作。不同计算机上的 **Break** 键位置有所不同。一般情况下，该键位于键盘的右上角。按 Break 会使设备进入 ROMmon 模式。此模式不需要设备访问 Cisco IOS 映像文件。

```
R3#reload
Proceed with reload? [confirm]

*Sep 12 08:27:28.670: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload command.
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Readonly ROMMON initialized
rommon 1 >
```

更改配置寄存器的值，使之加载路由器的初始配置。此配置没有口令保护，但支持 Cisco IOS 命令。将配置寄存器的值更改为 0x2142。

```
rommon 1 > confreg 0x2142
```

既然已进行了更改，现在我们就可使用 **reset** 命令来启动设备。

```
rommon 2 > reset
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0xd4a9a0
Self decompressing the image :
############################################################
################################################################################
# [OK]
```

〈省略部分输出〉

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

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


Press RETURN to get started!
```

步骤 4：恢复路由器配置。

现在我们将启动配置复制到运行配置，恢复配置，然后将配置寄存器改回默认值 (0x2102)。

要将启动配置从 NVRAM 复制到运行内存，键入 **copy startup-config running-config**。小心！请 *不要* 键入 copy running-config startup-config，否则您会清除启动配置。

```
Router#copy startup-config running-config
Destination filename [running-config]? {enter}

2261 bytes copied in 0.576 secs (3925 bytes/sec)

R3#:show running-config
〈省略部分输出〉
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
!
〈省略部分输出〉
!
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
```



```
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
〈省略部分输出〉
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

在本配置中，由于所有接口当前都是关闭状态，因此所有接口下都出现 **shutdown** 命令。最重要的是，您现在可以看到加密格式或未加密格式的口令（使能口令、使能加密口令、VTY 口令、控制台口令）。您可以重新使用未加密的口令。但已加密的口令就必须更改为新口令。

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret ciscoccna
R3(config)#username ccna password ciscoccna
```

对每个您想使用的接口发出 **no shutdown** 命令。

```
R3(config)#interface FastEthernet0/1
R3(config-if)#no shutdown
R3(config)#interface Serial0/0/0
R3(config-if)#no shutdown
```

您可以发出 **show ip interface brief** 命令来确认接口配置是否正确。每个您想使用的接口的状态都应该显示为 up up。

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
FastEthernet0/1        192.168.30.1    YES NVRAM  up                    up
Serial0/0/0            10.2.2.2        YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
```

键入 **config-register** *configuration register value*。变量 *configuration register value* 是您在步骤 3 设置的值或 0x2102。保存运行配置。

```
R3(config)#config-register 0x2102
R3(config)#end
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

口令恢复这一功能有哪些不足？

_____

_____

_____

任务 8：使用 SDM 保护路由器

在本实验中，您将使用 GUI 界面的安全设备管理器 (SDM) 来保护路由器 R2。与逐条键入每条命令相比，SDM 的速度更快，而且功能比 AutoSecure 更强。

检查您的路由器是否安装了 SDM：

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 Sep 12 2007 08:31:42 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        2261 Sep 25 2007 23:20:16 +00:00 Tr(RIP)
12        2506 Sep 26 2007 17:11:58 +00:00 save.txt
```

如果您的路由器上没有安装 SDM，则必须先安装才能继续下面的操作。请咨询您的教师以获得相关说明。

步骤 1：使用 TFTP Server 连接到 R2。

在 R2 上创建用户名和口令。

```
R2(config)#username ccna password ciscoccna
```

在 R2 上启用 http secure server 命令，并在 TFTP Server 上使用 Web 浏览器连接到 R2。

```
R2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue
"write memory" to save new certificate
R2(config)#end
R2#copy run start
```

在 TFTP Server 上打开 Web 浏览器并导航至 https://192.168.20.1/。使用之前配置的用户名和口令登录：

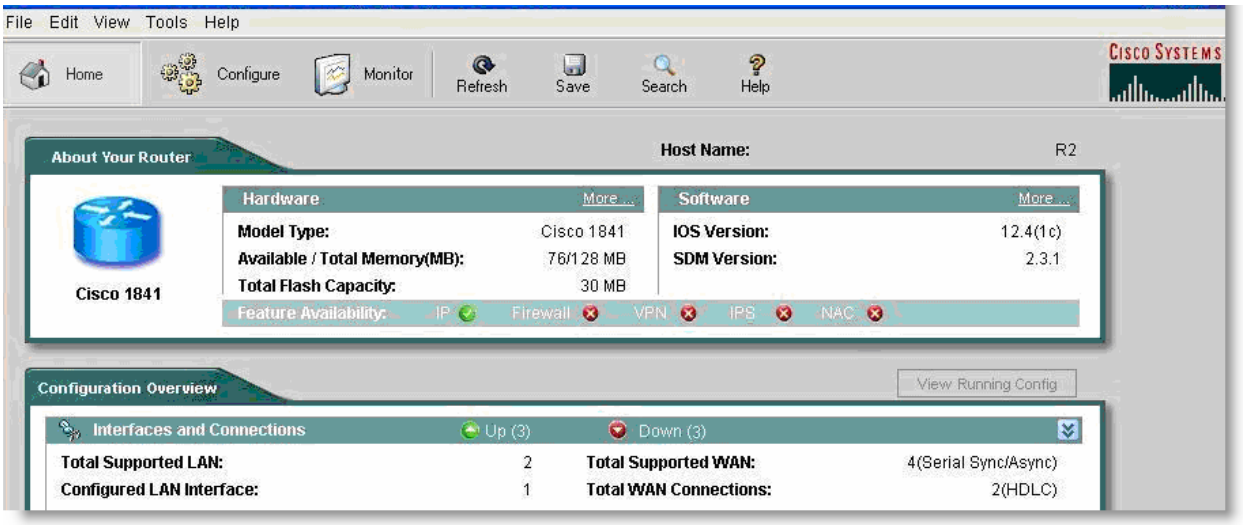
用户名： **ccna**

口令： **ciscoccna**

选择 **Cisco Router and Security Device Manager（Cisco 路由器和安全设备管理器）**

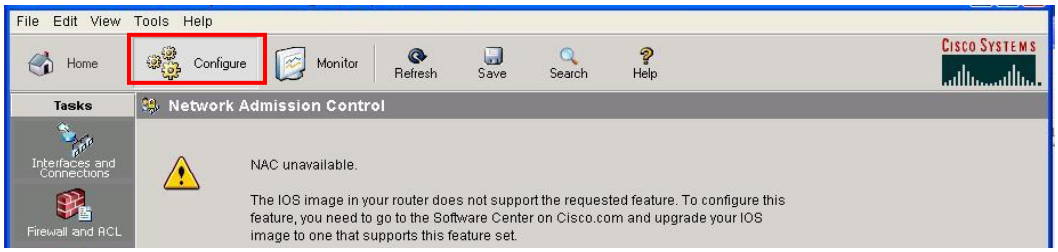
打开 Internet Explorer 并在地址栏输入 R2 的 IP 地址。一个新窗口随即打开。确保您关闭了浏览器上的所有弹出窗口拦截器。此外还需确保您安装并更新了 JAVA。

加载完成后，会为 SDM 打开一个新窗口。

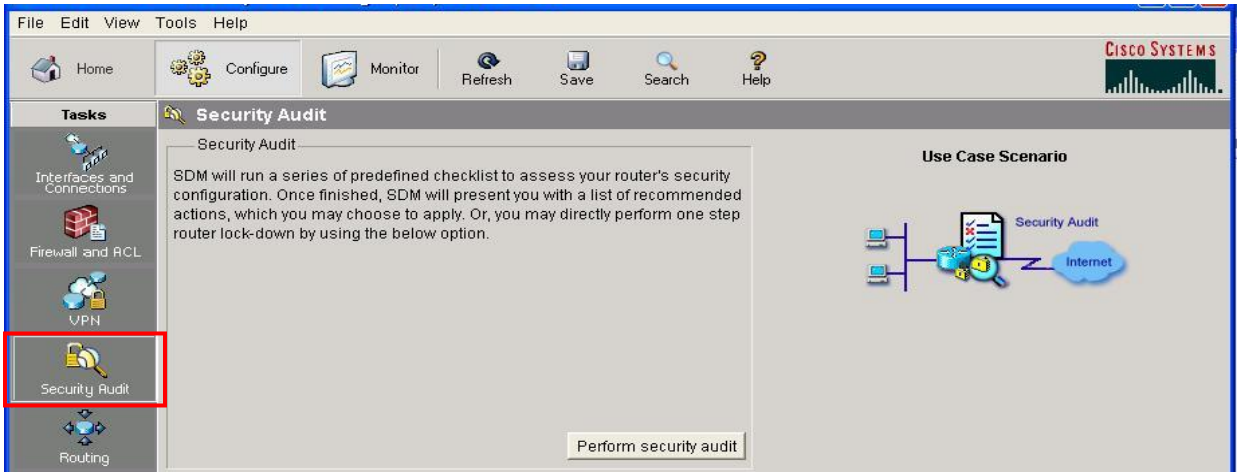


步骤 2：导航至“安全审计”功能。

单击窗口左上方的 **Configure（配置）**按钮。

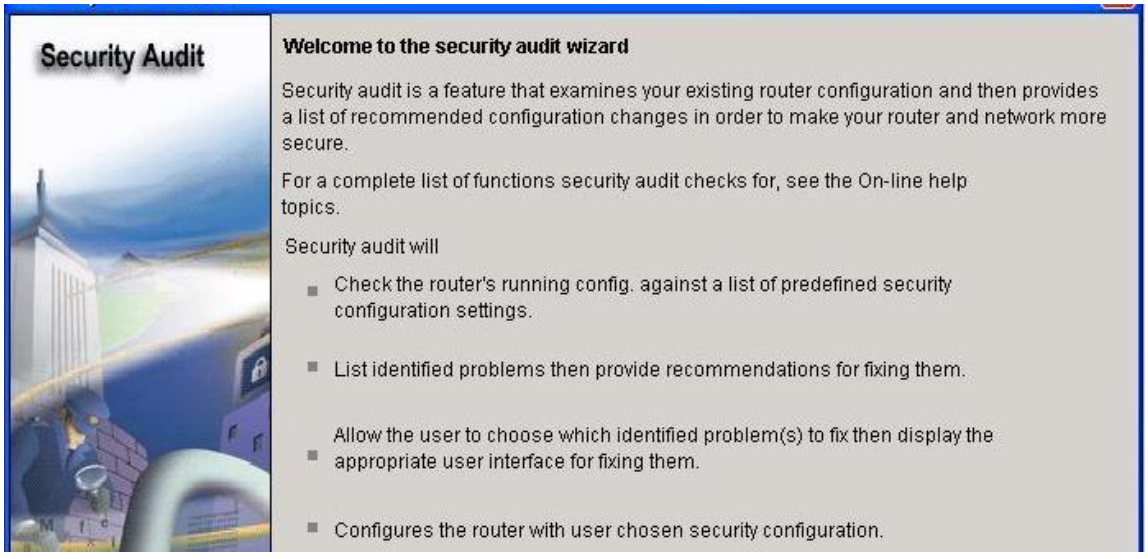


在左侧的面板上找到 **Security Audit（安全审计）**并单击它。

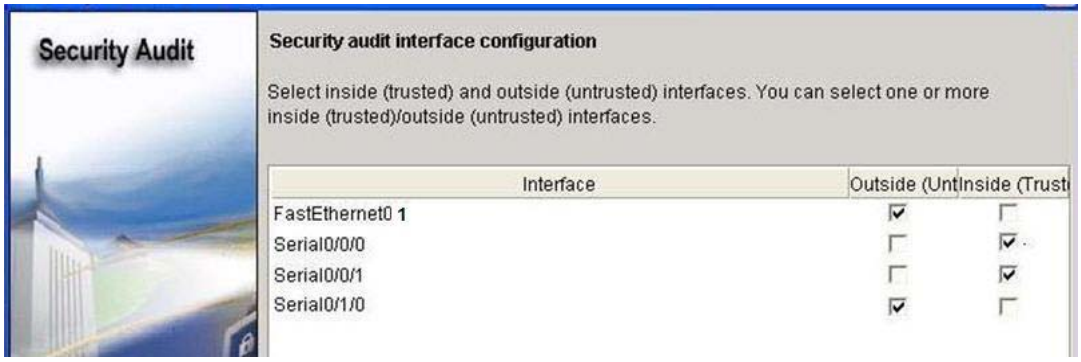


当您单击 **Security Audit（安全审计）**时，另一个窗口随之打开。

步骤 3：执行安全审计。

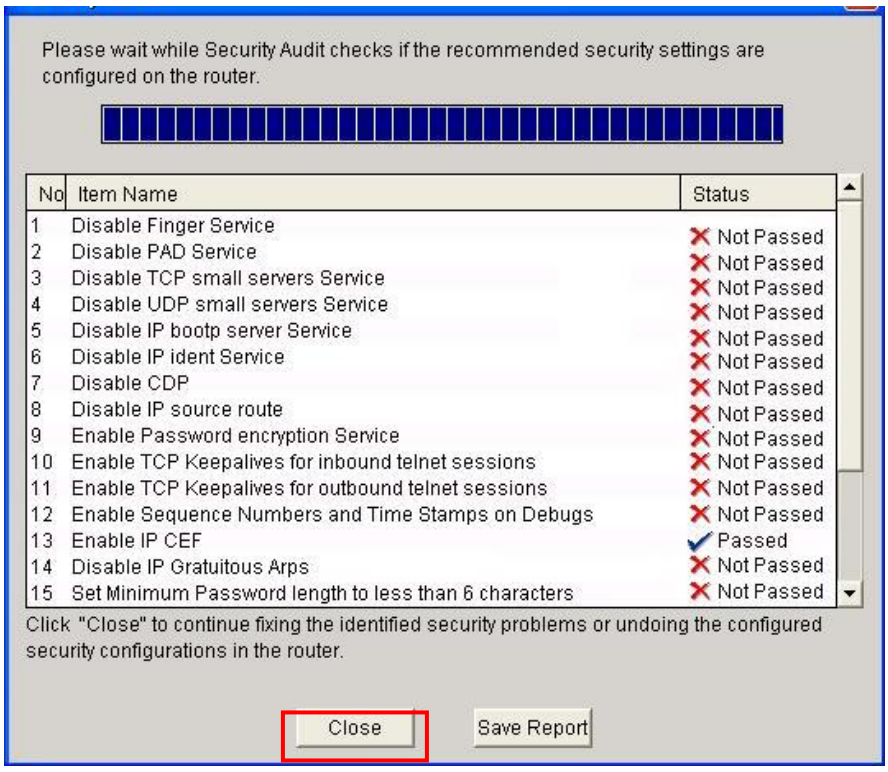


此画面简要介绍了安全审计功能的作用。单击 **Next（下一步）**打开 Security Audit Interface configuration（安全审计接口配置）窗口。



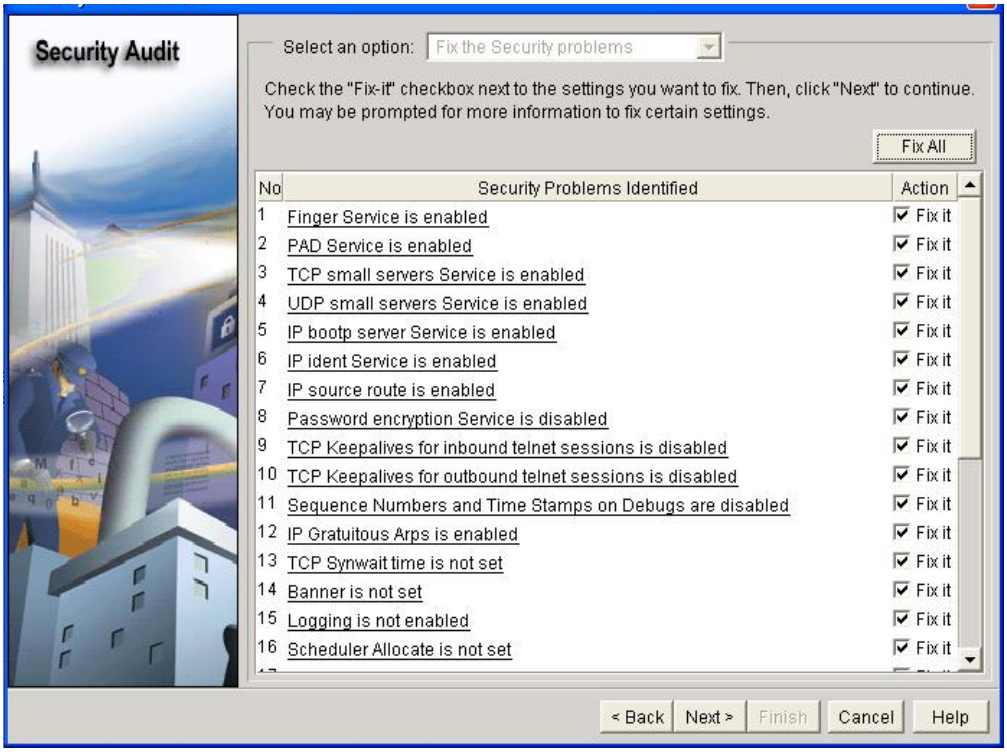
如果您不确定从某接口传入的流量的合法性，则应该将该接口分类为 outside (untrusted)（外部（不受信任））。在本例中，FastEthernet0/1 和 Serial0/1/0 都是不受信任的接口，因为 Serial0/1/0 面向 Internet，Fastethernet0/1 面向网络的接入部分，可能会生成非法流量。

选择外部和内部接口后，单击 **Next（下一步）**。新的窗口随即打开，表示 SDM 正在执行安全审计。

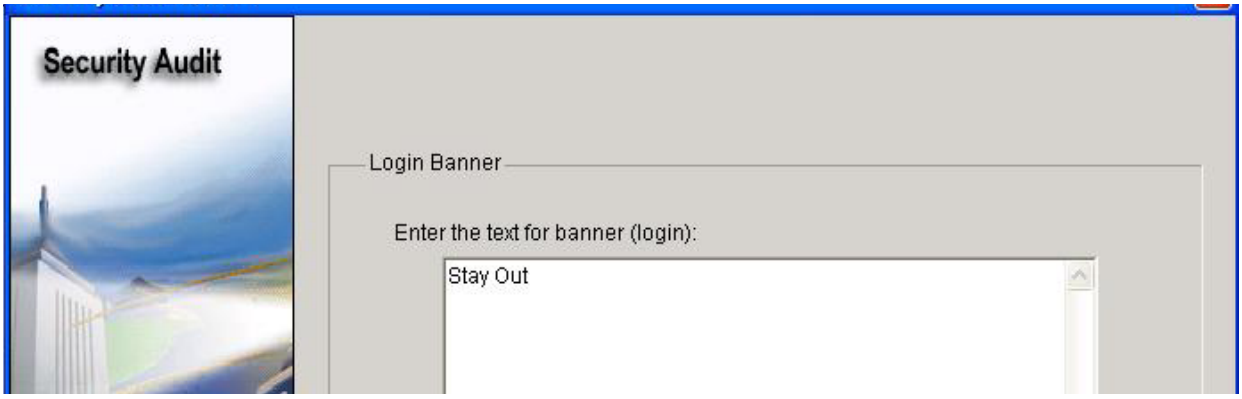


您可以看到，默认配置是不安全的。单击 **Close（关闭）**按钮继续。

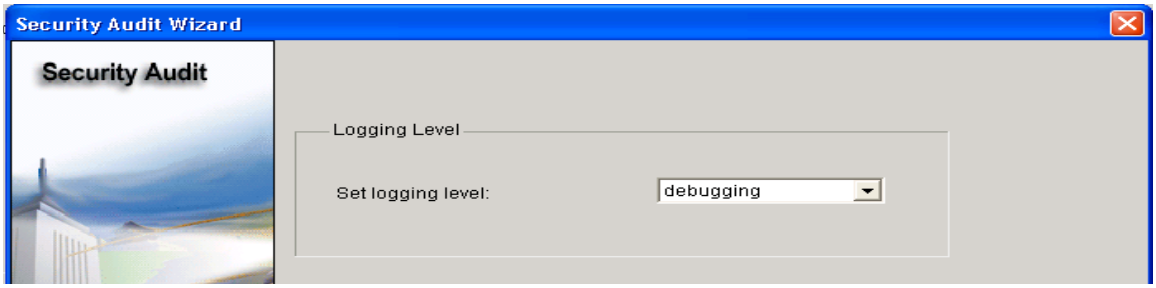
步骤 4：对路由器应用设置。



单击 **Fix All（全部修复）**按钮执行所有建议的安全更改。然后单击 **Next（下一步）**按钮。

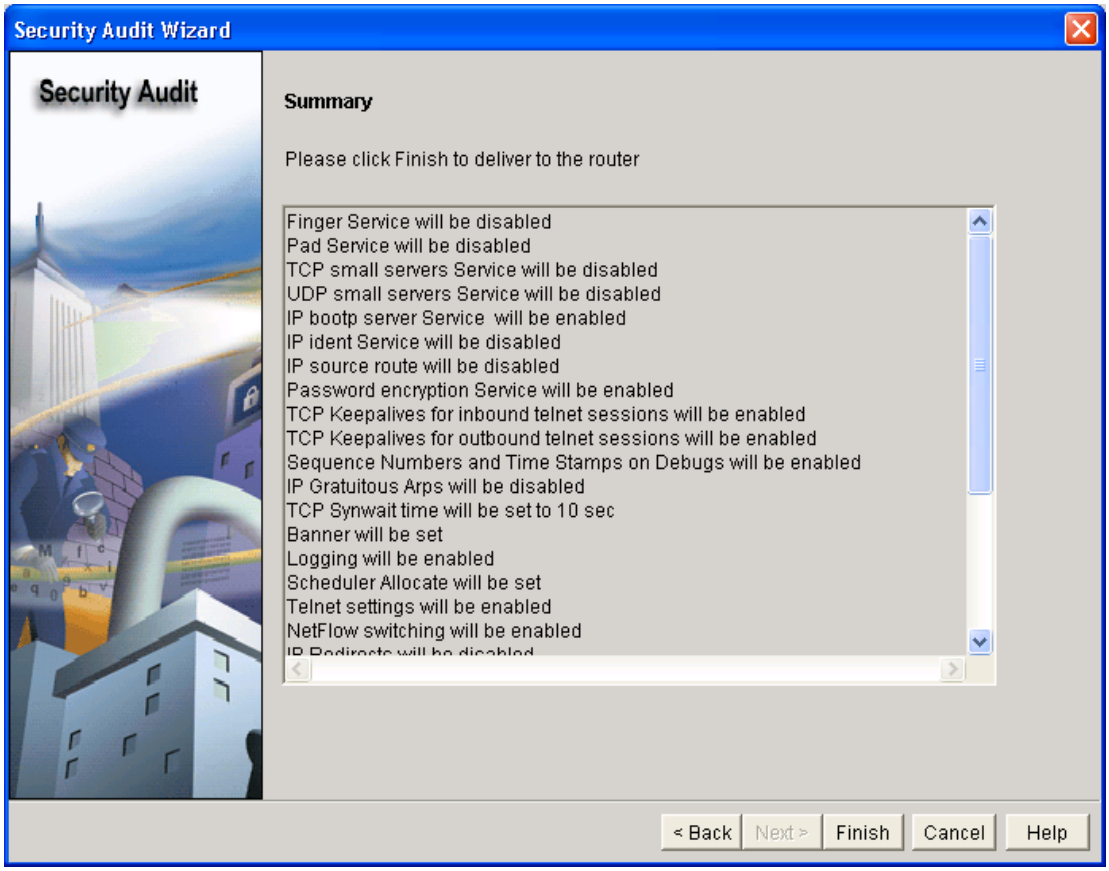


输入要用作路由器的当日消息的标语，然后单击 **Next（下一步）**。

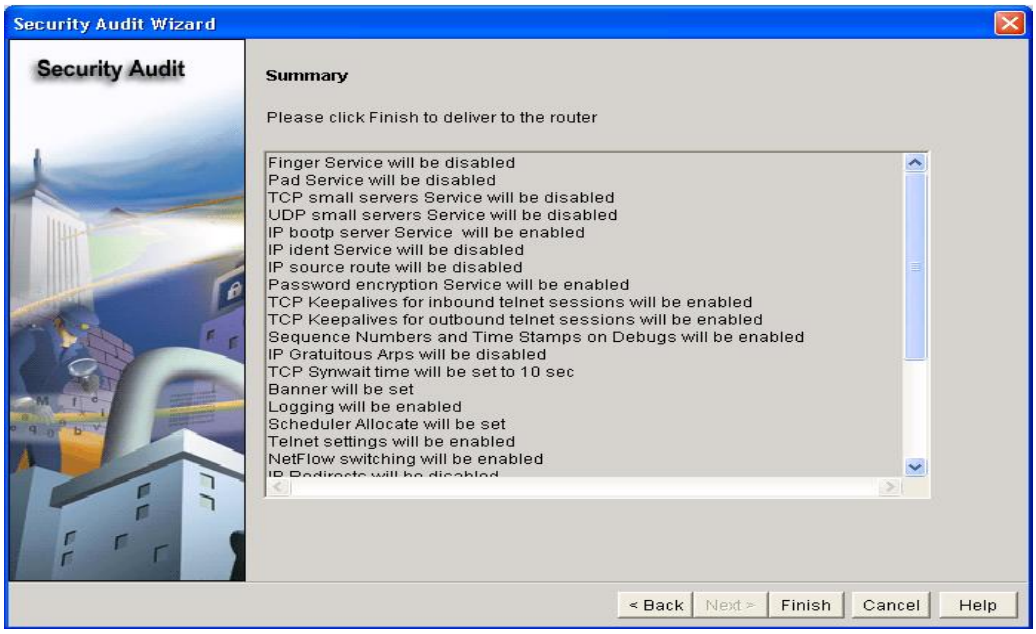


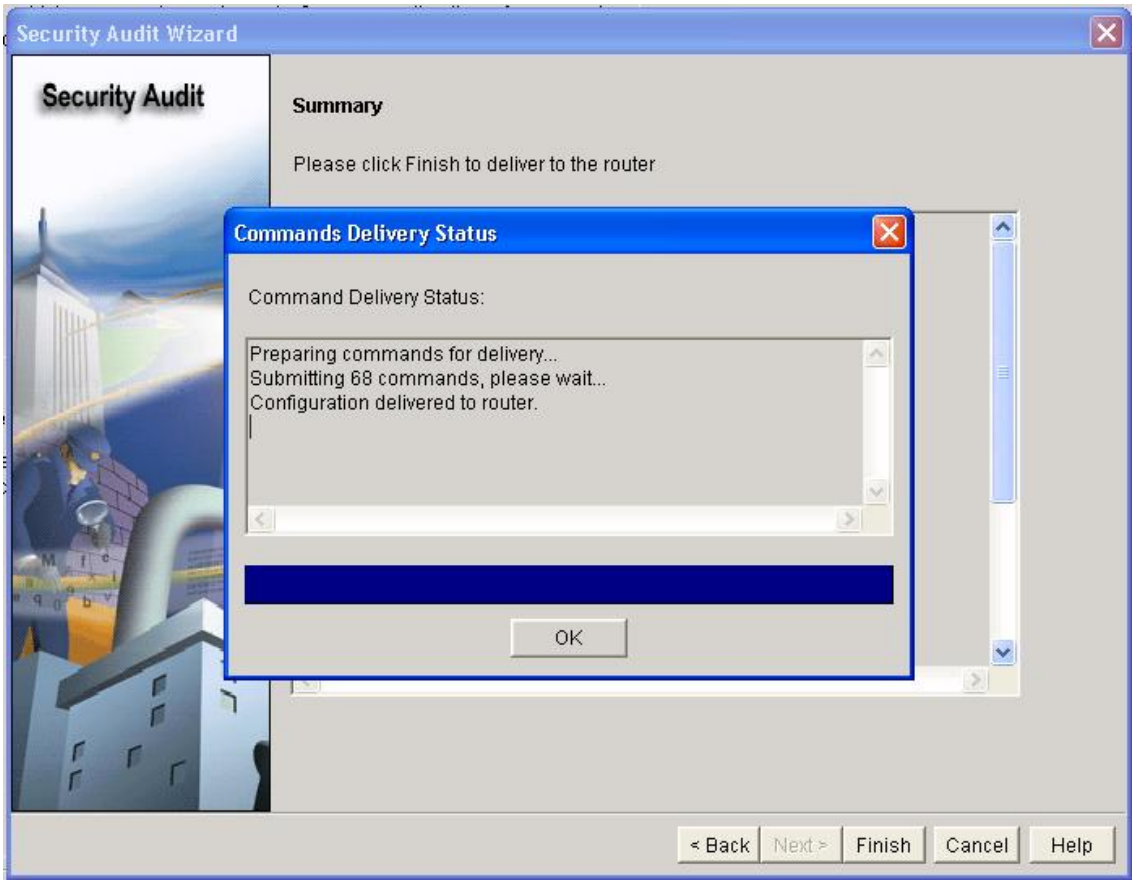
接下来，设置希望路由器发送到 syslog 服务器的日志陷阱的严重级别。本场景中严重级别设置为 debugging（调试）。单击 **Next（下一步）**查看对路由器所作更改的汇总。

步骤 5：将配置提交至路由器。



检查完毕要提交的更改后，单击 **Finish（完成）**。





单击 **OK（确定）**退出 SDM。

任务 9：记录路由器配置

在每台路由器上发出 **show run** 命令，并捕获配置信息。

任务 10：实验后清理

删除配置，然后重新启动路由器。拆下电缆并放回保存处。对于通常连接到其它网络（例如学校 LAN 或 Internet）的 PC 主机，请重新连接相应的电缆并恢复原有的 TCP/IP 设置。