This chapter covers the following topics:

ISR overview and providing secure administrative access: This section describes methods of securely accessing a router prompt for purposes of administration. Additionally, this section provides an overview of the Cisco Integrated Services Router (ISR) line of routers.

Cisco Security Device Manager overview: This section examines the Cisco Security Device Manager (SDM) interface. The graphical interface provided by SDM allows administrators to configure a variety of router features using a collection of wizards and other configuration aids, which use best-practice recommendations from the Cisco Technical Assistance Center (TAC).

CHAPTER 3

Defending the Perimeter

In addition to Cisco firewall, virtual private network (VPN), and intrusion prevention system (IPS) appliances that can sit at the perimeter of a network, Cisco IOS routers offer perimeter-based security. For example, the Cisco Integrated Services Routers (ISR) can be equipped to provide high-performance security features, including firewall, VPN termination, and IPS features, in addition to other services such as voice and quality-of-service (QoS) services. This chapter introduces various ISR models.

Because perimeter routers can be attractive targets for attack, they should be configured to secure administrative access. Therefore, this chapter also discusses specific approaches to "harden" administrative access to ISRs.

Configuring advanced ISR router features can be a complex process. Fortunately, many modern Cisco routers can be configured using the graphical Cisco Security Device Manager (SDM) interface. SDM contains multiple wizard-like configuration utilities, which are introduced in this chapter.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you determine your level of knowledge of this chapter's topics before you begin. Table 3-1 details the major topics discussed in this chapter and their corresponding quiz questions.

Table 3-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
ISR Overview and Providing Secure Administrative Access	1 to 10
Cisco Security Device Manager Overview	11 to 13

1. Which of the following are considered IOS security features? (Choose four.)
   a. Stateful firewall
   b. MARS
   c. IPS
   d. VRF-aware firewall
   e. VPN
   f. ACS
2. Some ISRs include a USB port, into which a flash drive can connect. What are three common uses for the flash drive? (Choose three.)
   a. Storing configuration files
   b. Storing a digital certificate
   c. Storing a copy of the IOS image
   d. Storing a username/password database
3. The enable secret password appears as an MD5 hash in a router's configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption service is not enabled). Why does Cisco still support the use of both enable secret and enable passwords in a router's configuration?
   a. Because the enable secret password is a hash, it cannot be decrypted. Therefore, the enable password is used to match the password that was entered, and the enable secret is used to verify that the enable password has not been modified since the hash was generated.
   b. The enable password is used for IKE Phase I, whereas the enable secret password is used for IKE Phase II.
   c. The enable password is considered to be a router's public key, whereas the enable secret password is considered to be a router's private key.
   d. The enable password is present for backward compatibility.
4. What is an IOS router's default response to multiple failed login attempts after the **security authentication failure** command has been issued?
   a. The login process is suspended for 10 seconds after 15 unsuccessful login attempts.
   b. The login process is suspended for 15 seconds after 10 unsuccessful login attempts.
   c. The login process is suspended for 30 seconds after 10 unsuccessful login attempts.
   d. The login process is suspended for 10 seconds after 30 unsuccessful login attempts.

5. What line configuration mode command would you enter to prevent a line (such as a console, aux, or vty line) connection from timing out because of inactivity?

   a. no service timeout

   b. timeout-line none

   c. exec-timeout 0 0

   d. service timeout default

6. An IOS router's privileged mode, which you can access by entering the **enable** command followed by the appropriate password, has which privilege level?

   a. 0

   b. 1

   c. 15

   d. 16

7. How is a CLI view different from a privilege level?

   a. A CLI view supports only commands configured for that specific view, whereas a privilege level supports commands available to that level and all the lower levels.

   b. A CLI view can function without a AAA configuration, whereas a privilege level requires AAA to be configured.

   c. A CLI view supports only monitoring commands, whereas a privilege level allows a user to make changes to an IOS configuration.

   d. A CLI view and a privilege level perform the same function. However, a CLI view is used on a Catalyst switch, whereas a privilege level is used on an IOS router.

8. To protect a router's image and configuration against an attacker's attempt to erase those files, the Cisco IOS Resilient Configuration feature keeps a secure copy of these files. What are these files called?

   a. The bootset

   b. The configset

   c. The backupset

   d. The backup-config

9. When you configure Cisco IOS login enhancements for virtual connections, what is the "quiet period"?
   a. The period of time between successive login attempts
   b. A period of time when no one is attempting to log in
   c. The period of time in which virtual login attempts are blocked, following repeated failed login attempts
   d. The period of time in which virtual logins are blocked as security services fully initialize
10. In the **banner motd #** command, what does **#** represent?
   a. A single text character that will appear as the message of the day
   b. A delimiter indicating the beginning and end of a message of the day
   c. A reference to a system variable that contains a message of the day
   d. The enable mode prompt from where the message of the day will be entered into the IOS configuration
11. What Cisco IOS feature provides a graphical user interface (GUI) for configuring a wide variety of features on an IOS router and also provides multiple "smart wizards" and configuration tutorials?
   a. QPM
   b. SAA
   c. SMS
   d. SDM
12. What are two options for running Cisco SDM? (Choose two.)
   a. Running SDM from a router's flash
   b. Running SDM from the Cisco web portal
   c. Running SDM from within CiscoWorks
   d. Running SDM from a PC
13. Which of the following are valid SDM configuration wizards? (Choose three.)
   a. Security Audit
   b. VPN
   c. ACS
   d. NAT
   e. STP

Foundation Topics

ISR Overview and Providing Secure Administrative Access

This section begins by introducing the security features offered in the Cisco line of ISR routers. Additional hardware options for these routers are also discussed. Then, with a foundational understanding of the underlying hardware, you will learn a series of best practices for security administrative access to a router. For example, a router can be configured to give different privilege levels to different administrative logins.

IOS Security Features

Although they are not a replacement for dedicated security appliances in large enterprise networks, modern Cisco routers, such as the ISR series, offer multiple integrated security features. Table 3-2 provides examples of these features, which vary by IOS feature set.

Table 3-2 *IOS Security Features*

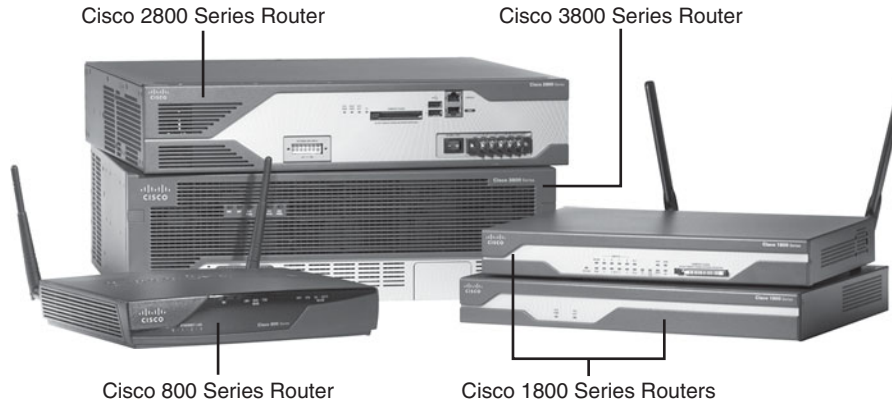
Feature	Description
Stateful firewall	The Cisco IOS firewall feature allows an IOS router to perform stateful inspection of traffic (using Context-Based Access Control [CBAC]), in addition to basic traffic filtering using access control lists (ACL).
Intrusion Prevention System	The IOS Intrusion Prevention System (IPS) feature can detect malicious network traffic inline and stop it before it reaches its destination.
VPN Routing and Forwarding-aware (VRF-aware) firewall	A VRF-aware firewall maintains a separate routing and forwarding table for each VPN, which helps eliminate issues that arise from more than one VPN using the same address space.
Virtual private networks	Cisco IOS routers can participate in virtual private networks (VPN). For example, a router at a headquarters location and at a branch office location could interconnect via an IPsec-protected VPN. This approach would allow traffic to pass securely between those sites, even if the VPN crossed an "untrusted" network, such as the Internet.

Cisco Integrated Services Routers

Cisco offers a series of routers called *Integrated Services Routers* (ISR). As their name suggests, these routers integrate various services (such as voice and security services) into

the router architecture. Although Cisco offers a wide range of router platforms, ISR models are easy to identify, because the last three digits of their model begin with the number 8. As shown in Figure 3-1, the ISR family of routers includes the 800 series, 1800 series, 2800 series, and 3800 series.

Figure 3-1 *800 Series, 1800 Series, 2800 Series, and 3800 Series ISRs*



Cisco 800 Series

The Cisco 800 series of ISRs is designed for teleworkers and small-office environments. These routers can connect to the Internet via a cable modem or DSL modem connection and offer secure connections over the Internet. Table 3-3 contrasts some of the features available in the Cisco 850 and 870 series of ISRs.

Table 3-3 *Cisco 800 Series of ISRs*

Feature	Cisco 850 Series	Cisco 870 Series
WAN technology support	ADSL Annex A (Cisco 857)	ADSL Annex B (Cisco 876), ADSL Annex A (Cisco 877), G.SHDSL (Cisco 878)
Built-in routed/WAN Ethernet	One 10/100 WAN (Cisco 851)	One 10/100 WAN (Cisco 871)
Integrated cryptographic hardware	Yes	Yes
Maximum flash memory	20 MB	52 MB
Maximum SRAM	64 MB	256 MB
Support for Cisco Security Device Manager (SDM)	Yes	Yes

Table 3-3 *Cisco 800 Series of ISRs (Continued)*

Feature	Cisco 850 Series	Cisco 870 Series
Maximum number of VPN tunnels	10	20
Stateful firewall support	Yes	Yes
Intrusion Prevention System (IPS) support	No	Yes

Cisco 1800 Series

The Cisco 1800 series of ISRs is designed for small businesses and smaller enterprise branch offices. These routers are designed for connectivity via cable modem/DSL, Metro Ethernet, and wireless technologies. Table 3-4 contrasts some of the features available in the Cisco 1800 and 1841 series of ISRs.

Table 3-4 *Cisco 1800 Series of ISRs*

Feature	Cisco 1800 Series (Fixed Interface)	Cisco 1841 Series (Modular)
WAN technology support	ADSL Annex A (Cisco 1801), ADSL Annex B (Cisco 1802), G.SHDSL (Cisco 1803)	ADSL and optional G.SHDSL WICs
Built-in routed/WAN Ethernet	One 10/100 (Cisco 1801-1803) Two 10/100 (Cisco 1811, 1812)	Two 10/100
Integrated cryptographic hardware	Yes	Yes
Maximum flash memory	128 MB	128 MB
Maximum SRAM	384 MB	384 MB
Support for Cisco Security Device Manager (SDM)	Yes	Yes
Maximum number of VPN tunnels	50	800
Stateful firewall support	Yes	Yes
Intrusion Prevention System (IPS) support	Yes	Yes

Cisco 2800 Series

The Cisco 2800 series of ISRs is designed for small-to-medium businesses and enterprise branch offices. These routers can securely provide voice, data, and video services. Table 3-5 contrasts some of the features available in the Cisco 2801, 2811, 2821, and 2851 series of ISRs.

Table 3-5 *Cisco 2800 Series of ISRs*

Feature	Cisco 2801 Series	Cisco 2811 Series	Cisco 2821 Series	Cisco 2851 Series
WAN technology support	ADSL and optional G.SHDSL WICs	ADSL and optional G.SHDSL WICs	ADSL and optional G.SHDSL WICs	ADSL and optional G.SHDSL WICs
Built-in routed/ WAN Ethernet	Two 10/100	Two 10/100	Two 10/100/1000	Two 10/100/1000
Integrated cryptographic hardware	Yes	Yes	Yes	Yes
Maximum flash memory	128 MB	256 MB	256 MB	256 MB
Maximum SRAM	384 MB	769 MB	1024 MB	1024 MB
Support for Cisco Security Device Manager (SDM)	Yes	Yes	Yes	Yes
Maximum number of VPN tunnels	1500	1500	1500	1500
Stateful firewall support	Yes	Yes	Yes	Yes
Intrusion Prevention System (IPS) support	Yes	Yes	Yes	Yes

Cisco 3800 Series

The Cisco 3800 series of ISRs is designed for medium to large businesses and enterprise branch offices. These routers offer multiple security, IP telephony, video, network analysis, and web application features. Table 3-6 contrasts some of the features available in the Cisco 3825 and 3845 series of ISRs.

Table 3-6 *Cisco 3800 Series of ISRs*

Feature	Cisco 3825 Series	Cisco 3845 Series
WAN technology support	ADSL and optional G.SHDSL WICs	ADSL and optional G.SHDSL WICs
Built-in routed/WAN Ethernet	Two 10/100/1000	Two 10/100/1000
Integrated cryptographic hardware	Yes	Yes
Maximum flash memory	256 MB	256 MB
Maximum SRAM	1024 MB	1024 MB
Support for Cisco Security Device Manager (SDM)	Yes	Yes
Maximum number of VPN tunnels	2000	2500
Stateful firewall support	Yes	Yes
Intrusion Prevention System (IPS) support	Yes	Yes

ISR Enhanced Features

Although traditional Cisco routers (that is, non-ISRs) offer features similar to those highlighted in the preceding tables, ISRs are unique in that they contain integrated hardware components (that vary by platform) to enhance performance. For example, most ISR models include the following enhancements:

- **Integrated VPN acceleration**: By using dedicated hardware for VPN encryption, ISRs reduce the overhead placed on a router's processor, thereby increasing VPN performance and scalability. Specifically, the built-in VPN acceleration hardware supports 3DES and Advanced Encryption Standard (AES).

- **Dedicated voice hardware**: IP telephony applications often use digital signal processors (DSP) to mix multiple voice streams in a conference. They also encrypt voice packets and convert between high-bandwidth and low-bandwidth codecs (that is, a coder/decoder, such as G.711 and G.729, which specify how voice samples are digitally represented in a voice packet). Voice traffic uses Real-time Transport Protocol (RTP), a Layer 4 protocol, to transport voice in a network. For increased security, Secure RTP (SRTP) can be used, which provides AES encryption for voice. However, because of the processor overhead required for SRTP's encryption, dedicated DSP hardware is required. Fortunately, ISRs can use packet voice DSP modules (PVDM) to take over the processing of such tasks.

  The Cisco 2800 series of ISRs can use PVDM2 modules with onboard voice interface cards (VIC). Additionally, PVDM2 modules can be inserted into Cisco High-Density Analog (HDA) network modules and the Cisco Digital Extension Module for Voice and Fax, which can be inserted into the Cisco 2821, 2851, 3825, and 3845 ISR models.

- **Advanced Integration Modules**: Cisco offers a variety of Advanced Integration Modules (AIM), which can offload processor-intensive tasks from a router's processor. For example, AIMs can be used for VPN processing, including a variety of standards for encryption, authentication, and data integrity. The following are some AIM models:
  - **AIM-VPN/BPII-PLUS**: Used in Cisco 1800 series ISRs, which can support a single AIM
  - **AIM-VPN/EPII-PLUS**: Used in Cisco 2800 series ISRs and the Cisco 3825 ISR, all of which can accommodate two AIMs
  - **AIM-VPN/HPII-PLUS**: Used in the Cisco 3845 ISR, which supports two AIMs
- **USB port**: All Cisco ISRs, with the exception of the Cisco 850 ISR, include one or two Universal Serial Bus (USB) ports. These ports can be used with a USB flash drive to store IOS images or configuration files. Also, from a security perspective, a USB eToken containing a signed digital certification can be inserted for VPN use.

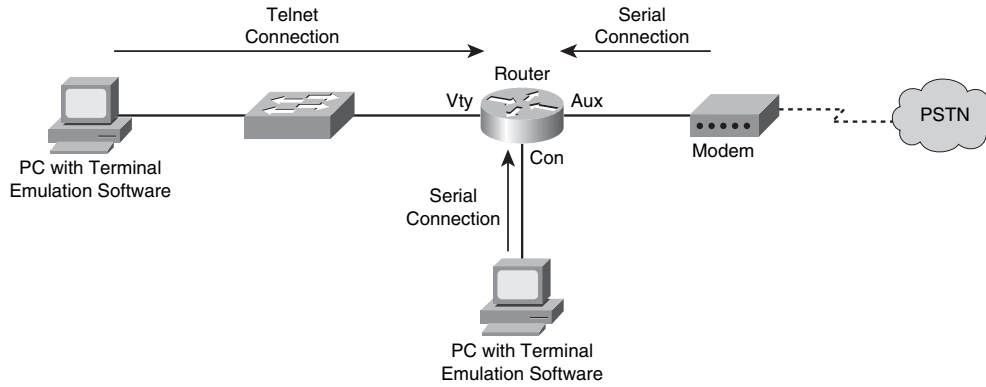
WAN connectivity network modules such as the WIC-2T, WIC-1B, and VWIC-1MFT offer flexibility in how various ISRs connect to the WAN. Here are some examples of other network modules supported on various ISR models:

- **Cisco HWIC-AP**: An IEEE 802.11 wireless module supporting a variety of wireless standards.
- **Cisco IDS Network Module**: Includes a hard drive containing multiple signatures of well-known attacks. Can be used to detect and subsequently prevent malicious traffic.
- **Cisco Content Engine**: Includes either a 40-GB or 80-GB hard drive for caching web content. This makes it available for quick retrieval by local clients, as opposed to the client's having to retrieve all the information from the web.
- **Cisco Network Analysis Module (NAM)**: Provides a detailed analysis of traffic flow.

Password-Protecting a Router

Administrators can access a router for administrative purposes in a variety of ways. For example, as shown in Figure 3-2, a PC running terminal emulation software can telnet into a router. The Telnet connection is considered to be using a vty line (a "virtual tty" line). Alternatively, a PC using terminal emulation software can connect directly to a router's console ("con") line over a serial connection. For remote administrative access, many Cisco routers also have an auxiliary line ("aux") that might connect to a modem.

Figure 3-2 *Administrative Access to a Router*



Telnet sends data in clear text. Therefore, if an attacker intercepted a series of Telnet packets, he could view their contents, such as usernames and passwords. For a more secure connection, administrators might choose to use Secure Shell (SSH) for access over a vty line. Modern Cisco routers also offer a graphical interface called Cisco Security Device Manager (SDM), which is accessible over the network using HTTP or HTTPS.

However, regardless of how an administrator chooses to access a router, the router typically challenges the administrator to provide either a password or a username/password combination before access is granted. As soon as an administrator is granted access to the router, she might be in *user mode*, where she has a limited number of commands she can issue. However, most router administration is performed from *privileged mode*. To access privileged mode from user mode, the administrator enters the **enable** command. Typically, the administrator then is prompted to enter another password, sometimes called the enable password. Interestingly, by default, a router has no password protection of any kind.

To protect a router from unauthorized access, a "strong" password should be selected. A strong password is one that is difficult for an attacker to guess or compromise by launching a *dictionary attack* or *brute-force attack*. A dictionary attack occurs when an attacker tries to use passwords from a file containing commonly used passwords. A brute-force attack occurs when an attacker tries all combinations of characters until a match is found. Recommended Cisco guidelines for selecting a strong router password include the following:

- Select a password that is at least ten characters long. The **security password min-length 10** global configuration mode command can be used to enforce this password length recommendation.

- Use a mixture of alphabetic (both uppercase and lowercase), numeric, and special characters.
- The password should not be a common word found in a dictionary.
- Create a policy that dictates how and when passwords are to be changed.

NOTE A space is a valid special character that can be used in a password. However, any leading space (that is, one or more spaces at the beginning of the password) is ignored.

When an administrator initially either sets up a router from the factory and chooses to run the setup script or issues the **setup** command, the System Configuration dialog appears. The administrator is prompted to enter basic router configuration parameters, including the passwords described in Table 3-7.

Table 3-7 *Passwords Configured During the SETUP Script*

Password Type	Description
Enable secret password	This password is used to permit access to a router's privileged mode. The password is stored in the router's configuration as an MD5 hash value, making it difficult for an attacker to guess and impossible to see with the naked eye.
Enable password	This password is not encrypted (or hashed) by default. Therefore, the enable password is considered weaker than the enable secret password. However, Cisco IOS still supports the enable password for backward compatibility. For example, if the IOS version on a router were rolled back to a version that supported the enable password but not the enable secret password, the enable password would offer some level of security.
vty password	When an administrator connects to a router over a network connection (such as a Telnet or SSH connection), she might be prompted to enter a vty password to have access to the virtual tty line to which she is connecting.

Even after the System Configuration dialog completes, and the router is functioning in a production environment, administrators can still change the router passwords. For example, the **enable secret** *password* global configuration mode command can be used to set the router's enable secret password. Consider Example 3-1, which shows an enable secret password being set to Cisc0Pr3$$. Notice how the enable secret password then appears in the running configuration. The string of characters shown is not an *encrypted* version of the password. Rather, the string is the result of an MD5 hash function, which always yields a 128-bit hash value that is also known as a "digest."

Example 3-1 *Setting the Enable Secret Password*

```
R1(config)# enable secret Cisc0Pr3$$
R1(config)# end
R1# show running-config

!
hostname R1
!
enable secret 5 $1$kmOB$rL419kUxmQphzVVTgO4sP1
!
```

To configure a password for a router's console, the administrator enters line configuration mode for **con 0** and specifies a password with the **password** command. Then, to force console connections to require a password, the **login** command is issued, as shown in Example 3-2.

Example 3-2 *Setting the Console Password*

```
R1(config)# line con 0
R1(config-line)# password 1mA$3cr3t
R1(config-line)# login
```

Similarly, you can set a password for the auxiliary port. Enter line configuration mode for **aux 0** and specify a password and require a login, like the console port configuration illustrated in Example 3-3.

Example 3-3 *Setting the Auxiliary Port Password*

```
R1(config)# line aux 0
R1(config-line)# password @uxP@$$w0rd
R1(config-line)# login
```

In addition to physically connecting to a router via the console or auxiliary port, administrators can connect to a router using a Telnet or SSH connection. Instead of connecting to physical ports, these types of connections use virtual ports. Specifically, by default a router has five virtual tty lines (that is, "vty"), vty 0 to vty 4, over which administrators can remotely connect. Similar to the console and auxiliary ports, passwords can be assigned to these vty lines, as shown in Example 3-4.

Example 3-4 *Setting the vty Line Password*

```
R1(config)# line vty 0 4
R1(config-line)# login
R1(config-line)# password MyP@$$w0rd
```

The enable secret password appears in the running configuration as an MD5 hash value. However, the console, auxiliary, and vty line passwords appear in the running configuration as plain text, as shown in Example 3-5.

Example 3-5 *Line Passwords Appearing in Plain Text*

```
R1# show running-config

!
line con 0
 password 1mA$3cr3t
 login
line aux 0
 password @uxP@$$w0rd
 login
line vty 0 4
 password MyP@$$w0rd
 login
```

To better secure these passwords, a *password encryption* service can be enabled on the router. This service uses a Cisco-proprietary algorithm that is based on a Vigenere cipher. This algorithm is far from secure. Its password can be easily compromised with downloadable utilities freely available on the Internet (such as the GetPass utility from Boson Software). However, enabling the password encryption service does help prevent someone from obtaining a password from the casual inspection of a router's configuration.

The password encryption service is enabled in global configuration mode using the **service password-encryption** command. After enabling this service, the console, auxiliary, and vty line passwords appear in an encrypted format. The 7 that appears after the **password** command indicates that the password has been encrypted using this Cisco-proprietary encryption algorithm, as shown in Example 3-6.

Example 3-6 *Cisco-Proprietary Password Encryption Results*

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

!
line con 0
 password 7 091D43285D5614005818
 login
line aux 0
 password 7 06261A397C6E4D5D1247000F
 login
line vty 0 4
 password 7 096157393941530 55B1E00
 login
```

Aside from having a single password for all administrators, individual user accounts can be used to give different login credentials (that is, username/password combinations) to different administrators. Although an external user database (such as a Cisco Secure Access Control Server [ACS]) could be used, a simple way to configure a user database is to add the username/password combinations to a router's configuration. Example 3-7 shows the addition of a username and password using the **username kevinw secret $up3r$3cr3t** command. The password will appear in the router's configuration as an MD5 hash value.

Example 3-7 *Configuring a Local User Database*

```
R1(config)# username kevinw secret $up3r$3cr3t
R1(config)# end
R1# show run

!
username kevinw secret 5 $1$geU5$vc/uDRS5dWiOrpQJTimBw/
!
```

NOTE If you already know the MD5 hash value of the password you are setting for a user, you can enter the hash value, instead of the password, using the **username** *username* **secret 5** *hash_value* command. The 5 indicates that the string you are entering for the password is the result of an MD5 hash of the password, as opposed to the plain-text password. You could optionally indicate the plain-text password with a 0 in place of the 5.

If an attacker gains physical access to a router, he could connect to the router's console port and reboot the router. During the bootup process, the attacker could generate a break sequence, causing the router to enter ROM monitor (ROMMON) mode. From ROMMOM mode, the attacker could reset the router's password and thereby gain access to the router's configuration.

Although the ability to perform this type of *password recovery* often proves useful to administrators, if the router's physical security cannot be guaranteed, this feature opens a vulnerability for attackers. To mitigate this threat, an administrator can disable the password recovery feature by issuing the **no service password-recovery** command in global configuration mode. After entering this command, the administrator is cautioned not to execute this command without another plan for password recovery, because ROMMON will no longer be accessible.

Limiting the Number of Failed Login Attempts

If an attacker uses a brute-force attack or a dictionary attack when attempting to log in to a device, such as a router, multiple login attempts typically fail before the correct credentials are found. To mitigate these types of attacks, a Cisco IOS router can suspend the login process for 15 seconds, following a specified number of failed login attempts. By default, a 15-second delay is introduced after ten failed login attempts. However, the **security authentication failure** *rate number_of_failed_attempts* **log** configuration command (issued in global configuration mode) can be used to specify the maximum number of failed attempts (in the range of 2 to 1024) before introducing the 15-second delay.

Example 3-8 illustrates setting the maximum number of attempts to five. Also, notice the **log** command, which causes a TOOMANY_AUTHFAILS syslog message to be written to a syslog server.

Example 3-8 *Setting the Number of Failed Login Attempts*

```
R1# conf term
R1(config)# security authentication failure rate 5 log
R1(config)# end
```

Setting a Login Inactivity Timer

After an administrator provides appropriate credentials and successfully logs into a router, the router could become vulnerable to attack if the administrator walks away. To help prevent an unattended router from becoming a security weakness, a 10-minute inactivity timer is enabled by default. However, Cisco recommends that inactivity timers be set to no more than 3 minutes. Fortunately, administrators can adjust the inactivity windows with the **exec-timeout** *minutes* [*seconds*] command, issued in line configuration mode. Consider Example 3-9, which shows setting the inactivity timer for the console, auxiliary, and vty lines to 2 minutes and 30 seconds.

Example 3-9 *Setting an Inactivity Timer*

```
R1# conf term
R1(config)# line con 0
R1(config-line)# exec-timeout 2 30
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# exec-timeout 2 30
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 2 30
```

NOTE Although it isn't recommended, you can disable the inactivity timer by entering a 0 for both the *minutes* and *seconds* arguments in the **exec-timeout** command (that is, **exec-timeout 0 0**).

Configuring Privilege Levels

Larger enterprise environments might need to support multiple administrative privilege levels for router configuration. For example, help desk staff might need access to a subset of the IOS commands available to the primary router configuration team.

Cisco IOS routers normally use two of the 16 supported privilege levels. Specifically, Cisco IOS routers support privilege levels in the range 0 to 15. By default, when you attach to a router, you are in *user* mode, which has a privilege level of 0. After entering the **enable** command and providing appropriate credentials, you are moved to *privileged* mode, which has a privilege level of 15.

However, for a finer granularity of administrative privileges, you can configure privilege levels in the range 1 to 14 using the **privilege** *mode* {**level** *level command* | **reset** *command*} command in global configuration mode. **reset** is used to reset the privilege level of a command to its original privilege level. To illustrate, Example 3-10 shows how to configure the **debug** command to be a privilege level 5 command and how to set the enable secret password for level 5 administrative access.

Example 3-10 *Configuring a Privilege Level*

```
R1# config term
R1(config)# privilege exec level 5 debug
R1(config)# enable secret level 5 L3v3l5P@55
R1(config)# end
```

After additional privilege levels are configured, an administrator can specify the privilege level she wants to change to using the **enable** *level* command. For example, for an administrator to switch to the previously configured privilege level of 5, she would enter the **enable 5** command. After switching to a privilege level of 5, the administrator would have access to all commands associated not only with privilege level 5, but also all lower privilege levels.

Creating Command-Line Interface Views

Similar to making different commands available to different administrators using privilege levels, role-based *command-line interface (CLI) views* can be used to provide different sets of configuration information to different administrators. However, unlike making commands available via privilege levels, using role-based CLI views you can control

exactly what commands an administrator has access to. Following are the steps required to configure these views:

Step 1 **Enable AAA**: Authentication, authorization, and accounting (AAA) is discussed in detail in Chapter 4, "Configuring AAA." For now, just realize that AAA must be enabled to support views. Example 3-11 shows how to enable AAA on an IOS router.

Example 3-11 *Enabling AAA*

```
R1# conf term
R1(config)# aaa new-model
R1(config)# end
```

Step 2 **Enable the root view**: The root view is represented by the set of commands available to an administrator logged in with a pri'vilege level of 15. You might be required to provide the enable secret password to enable the root view, as shown in Example 3-12.

Example 3-12 *Enabling the Root View*

```
R1# enable view

Password:
R1#
```

Step 3 **Create a view**: Use the **parser view** *name* command to create a new view, as shown in Example 3-13.

Example 3-13 *Creating a View*

```
R1# config term
R1(config)# parser view HELPDESK

R1(config-view)#
```

Step 4 **Set a password for the view**: Use the **secret 0** *password* command to set the password required to invoke the view. The 0 in the command indicates that the password provided is in plain text, as opposed to an MD5 hash value. Example 3-14 shows how to configure a view's password.

Example 3-14 *Setting a Password for a View*

```
R1(config-view)# secret 0 H3lpD3skP@55

R1(config-view)#
```

Step 5 **Add available commands to the view**: The **commands** *parser_mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface_identifier* | *command*] command, issued in view configuration mode, allows an administrator to specify a command (or interface) available to a particular view. Example 3-15 shows how to specify that the **copy** command (followed by any keywords), the **traceroute** command, and the **ping** command will be available to a specific view (HELPDESK in this example).

Example 3-15 *Specifying Commands Available to a View*

```
R1(config-view)# commands exec include all copy
R1(config-view)# commands exec include traceroute
R1(config-view)# commands exec include ping
```

Step 6 **Verify the role-based CLI view configuration**: After creating a view, you can switch to that view with the **enable view** *name* command. After switching to the new view, you enter a **?**, for context-sensitive help, to see what commands are available in your new view, as demonstrated in Example 3-16.

Example 3-16 *Confirming Role-Based CLI Configuration*

```
R1# enable view HELPDESK

Password:

R1#?
Exec commands:
  <1-99>      Session number to resume
  copy        Copy from one file to another
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
  traceroute  Trace route to destination
```

Protecting Router Files

To protect a router's image and configuration from an attacker's attempt to erase those files, the *Cisco IOS Resilient Configuration* feature keeps a secure copy of these files. These files are called the *bootset*. Table 3-8 details the steps required to configure Cisco IOS Resilient Configuration.

Key Topic

Table 3-8 *Cisco IOS Resilient Configuration Steps*

Step	Description
Step 1: Enable image resilience	The **secure boot-image** command, issued in global configuration mode, secures the Cisco IOS image. The secured image is hidden so that it does not appear in a directory listing of files.
Step 2: Secure the boot configuration	The **secure boot-config** command, issued in global configuration mode, archives the running configuration of a router to persistent storage.
Step 3: Verify the security of the bootset	The **show secure bootset** command can be used to verify that Cisco IOS Resilient Configuration is enabled and that the files in the bootset have been secured.

Enabling Cisco IOS Login Enhancements for Virtual Connections

Administrators, and therefore attackers, can create virtual connections to an IOS router using Telnet, SSH, and HTTP. Because an attacker does not need physical access to a router to attempt one of these "virtual" connections, you should further secure these connection types using the Cisco IOS Login Enhancements feature. This feature adds the following requirements to the login process:

Key Topic

- Create a delay between repeated login attempts.
- Suspend the login process if a denial-of-service (DoS) attack is suspected.
- Create syslog messages upon the success and/or failure of a login attempt.

These login enhancements are not enabled by default. To enable the login enhancements with their default settings, you can issue the **login block-for** command in global configuration mode. The default login settings specify the following:

- A delay of 1 second occurs between successive login attempts.
- No virtual connection (that is, a connection using Telnet, SSH, or HTTP) can be made during the "quiet period," which is a period of time in which virtual login attempts are blocked, following repeated failed login attempts.

You, as an administrator, might want to alter the supported virtual login parameters to better detect and protect against DoS and/or dictionary attacks. Table 3-9 provides a command reference for these parameters.

Table 3-9 *Commands for Enhancing Virtual Login Support*

Command	Description
Router(config)# **login block-for** *seconds* **attempts** *attempts* **within** *seconds*	Specifies the number of failed login attempts (within a specified time period) that trigger a *quiet period*, during which login attempts would be blocked.
Router(config)# **login quiet-mode access-class** {*acl-name* | *acl-number*}	Specifies an ACL that identifies exemptions from the previously described quiet period.
Router(config)# **login delay** *seconds*	Specifies a minimum period of time that must pass between login attempts. The default time period is 1 second.
Router(config)# **login on-failure log** [**every** *login_attempts*]	Creates log messages for failed login attempts.
Router(config)# **login on-success log** [**every** *login_attempts*]	Creates log messages for successful login attempts.
Router# **show login**	Can be used to verify that enhanced support for virtual logins is configured and to view the login parameters.

Consider the enhanced support for virtual logins configuration shown in Example 3-17. After entering global configuration mode, the **login block-for 30 attempts 5 within 10** command is used to block login attempts for 30 seconds after five failed login attempts occur within a 10-second time period. If logins are then blocked based on the first command, the period of time that logins are blocked is called the quiet period. However, in this example, the **login quiet-mode access-class 101** command specifies that during the quiet period, traffic permitted by ACL 101 still is allowed to log in via Telnet, SSH, or HTTP. The delay between successive login attempts is configured to 3 seconds with the **login delay 3** command. This configuration specifies that log messages should be generated upon every failed or successful login attempt using the **login on failure log** and **login on-success log** commands. Finally, the **show login** command is issued to confirm the configuration of these virtual login parameters.

Example 3-17 *Configuring Enhanced Support for Virtual Logins*

```
R1# conf term
R1(config)# login block-for 30 attempts 5 within 10
R1(config)# login quiet-mode access-class 101
R1(config)# login delay 3
R1(config)# login on failure log
R1(config)# login on-success log
R1(config)# end
R1# show login

     A login delay of 3 seconds is applied.
     Quiet-Mode access list 101 is applied.
     All successful login is logged.
     All failed login is logged.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 10 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 9 seconds.
         Login failures for current window: 0.
     Total login failures: 0.
R1#
```

Creating a Banner Message

When someone connects to one of your routers, he sees some sort of message or prompt. For legal reasons, Cisco suggests that a banner message be displayed to warn potential attackers not to attempt a login. For example, you wouldn't want to use a banner message that says, "Welcome! You are connected to Router 1." An attacker could use such a message as part of his legal defense, stating that he was told that he was welcomed to your router.

Please consult competent legal counsel when phrasing the banner message. However, as soon as you have the appropriate verbiage for your banner message, you can apply the message to your router with the **banner motd** *delimiter message_body delimiter* command. The **motd** parameter stands for "message of the day," and the *delimiter* is a character you choose to indicate the beginning and end of the banner message. Therefore, you should choose a delimiter that will not appear in the message body. Example 3-18 shows how to create a banner message. Notice that the $ character is used as the delimiter. Example 3-19 shows the new banner message presented to a user who just connected to the router via Telnet.

Example 3-18 *Creating a Message-of-the-Day Banner*


```
R1# conf term

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# banner motd $

Enter TEXT message.  End with the character '$'.
WARNING: This router is the private property of Cisco Press.
    Disconnect now if you are not an authorized user.
    Violators will be prosecuted.
$
R1(config)#end
```

Example 3-19 *Login Prompt with a Banner Message*

```
WARNING: This router is the private property of Cisco Press.
    Disconnect now if you are not an authorized user.
    Violators will be prosecuted.

User Access Verification

Password:
```

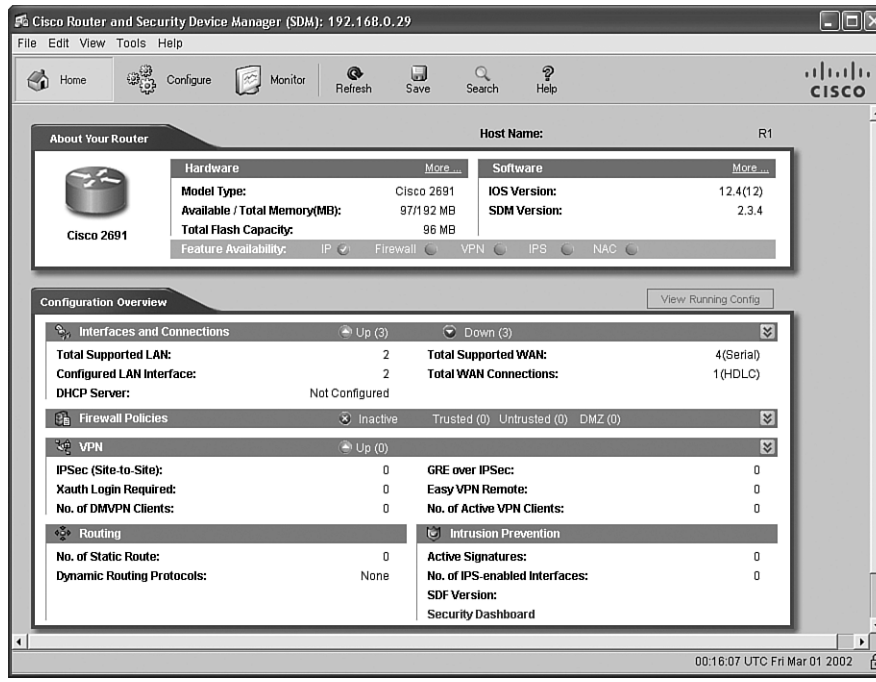
Cisco Security Device Manager Overview

Cisco IOS routers support many features (including security features) that require complex configurations. To aid in a number of these configuration tasks, Cisco introduced the Cisco Security Device Manager (SDM) interface. This section introduces SDM, discusses how to configure and launch SDM, and how to navigate the SDM wizards.

Introducing SDM

Cisco SDM provides a graphical user interface (GUI) for configuring a wide variety of features on an IOS router, as shown in Figure 3-3. Not only does SDM offer multiple "smart wizards," but configuration tutorials also are provided. Even though SDM stands for Security Device Manager, several nonsecurity features also can be configured via SDM, such as routing and quality-of-service (QoS) features.

Figure 3-3 *SDM Home Screen*



Some newer Cisco routers come with SDM preinstalled, but SDM needs to be installed on other supported platforms. Go to http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm to download the current version of SDM and its release notes. Cisco SDM offers the following benefits:

Key Topic

- SDM's smart wizards use Cisco TAC best-practice recommendations for a variety of configuration scenarios.
- SDM intelligently determines an appropriate security configuration based on what it learns about a router's configuration (for example, a router's interfaces, NAT configuration, and existing security configuration).
- SDM supports multiple security features such as wizard-based VPN configuration, router security auditing, and One-Step Lockdown configuration.
- SDM, which is supported in Cisco IOS 12.2(11)T6 and later, does not impact a router's DRAM or CPU.

Preparing to Launch Cisco SDM

If you plan to run SDM on a router that does not already have SDM installed, you need to install SDM either from a CD accompanying the router or from a download from the Cisco IOS Software Center. The installation is wizard-based. You are prompted to install SDM either on an administrator's PC, in the router's flash, or both.

SDM can connect to the managed router using secure HTTP (that is, HTTPS). The commands shown in Table 3-10 can be used to configure the router for HTTP support. Example 3-20 illustrates the use of these commands.

Table 3-10 *HTTPS Configuration Commands*

Command	Function
Router(config)# **ip http server**	Enables an HTTP server on a router
Router(config)# **ip http secure-server**	Enables a secure HTTP (HTTPS) server on a router
Router(config)# **ip http authentication local**	Configures a local authentication method for accessing the HTTPS server
Router(config)# **username** *name* **privilege 15 secret 0** *password*	Configures a username and password to be used for authentication local to the router

Example 3-20 *HTTPS Server Configuration for R1*

```
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip http authentication local
R1(config)# username kevin privilege 15 secret 0 cisco
```

To verify that the required SDM files are installed on a router, you can issue the **show flash** command. The output of this command should show, at a minimum, the following SDM files:

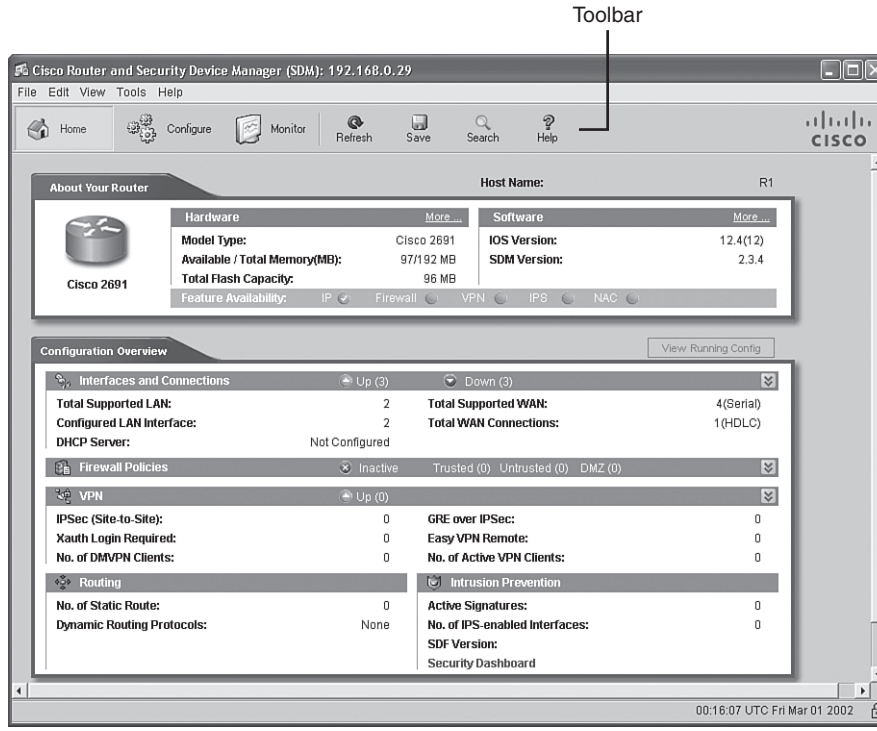
- sdmconfig-*router_platform*.cfg
- sdm.tar
- es.tar
- common.tar
- home.shtml
- home.tar

If you run SDM from a router's flash, as opposed to running SDM from a PC, the first time you connect to the router via a browser, you are taken to the Cisco SDM Express interface. Specifically, on a new router that has SDM installed, you point your browser to http://10.10.10.1. Alternatively, on an existing router, you point your browser to an active IP address on the router. Cisco SDM Express guides you through the initial SDM configuration on a router. Subsequent connections to your router via a browser take you directly to SDM, as opposed to Cisco SDM Express. However, if you run SDM from a PC, you can launch Cisco SDM by choosing **Start > Programs > Cisco Systems > Cisco SDM**.

Exploring the Cisco SDM Interface

Notice the toolbar across the top of the SDM page, as highlighted in Figure 3-4. You can use this toolbar to navigate between the Home, Configure, and Monitor views.

Figure 3-4 *SDM Toolbar*



The Home view provides summary information about the router platform. For example, this summary information shows you the router model, memory capacity, flash capacity, IOS version, and an interface summary.

After clicking the **Configure** button, you see a screen similar to the one shown in Figure 3-5. Notice the wizards available in the Tasks bar. Available configuration wizards are described in Table 3-11.

Figure 3-5 *Configuration Tasks Bar*

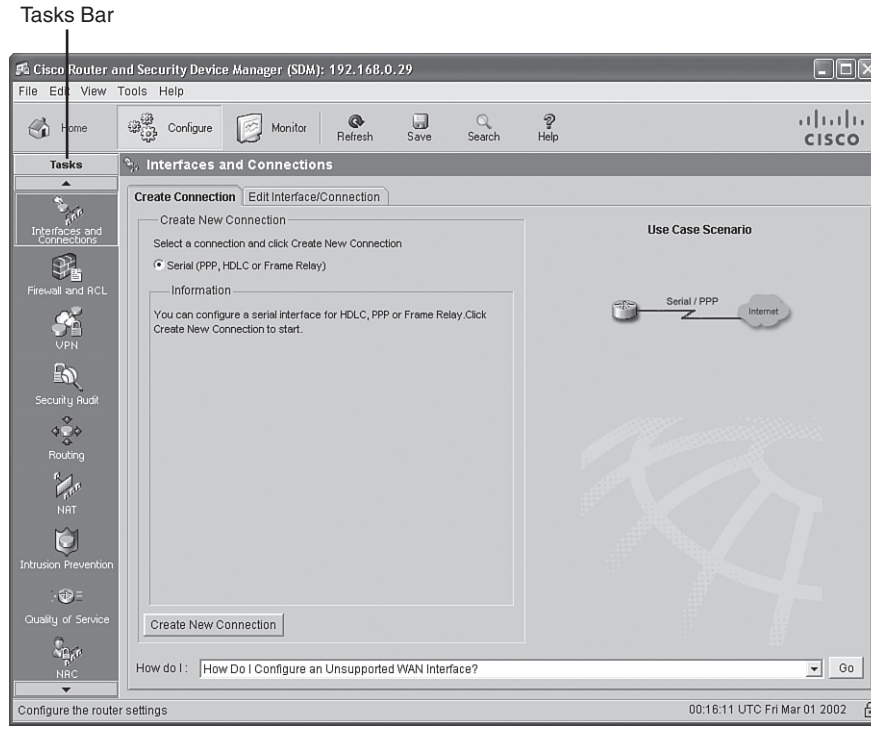


Table 3-11 *Cisco SDM Wizards*

Key Topic

Cisco SDM Wizard	Description
Interfaces and Connections	Helps you configure LAN and WAN interfaces
Firewall and ACL	Supports the configuration of basic and advanced IOS-based firewalls
VPN	Helps you configure a secure site-to-site VPN, Cisco Easy VPN Server, Cisco Easy VPN Remote, and DMVPN
Security Audit	Identifies potential security vulnerabilities in a router's current configuration and tweaks the router's configuration to eliminate those weaknesses

continues

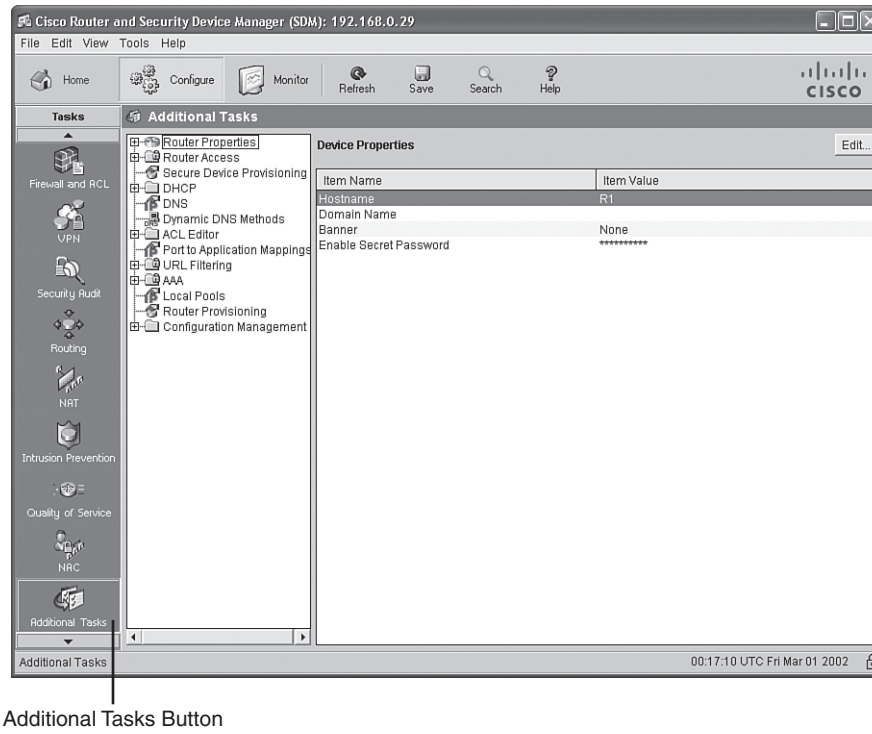
Key Topic

Table 3-11 *Cisco SDM Wizards (Continued)*

Cisco SDM Wizard	Description
Routing	Allows an administrator to modify and view routing configurations for the RIP, OSPF, or EIGRP routing protocols
NAT	Helps you configure Network Address Translation (NAT)
Intrusion Prevention	Walks an administrator through the process of configuring an IOS-based IPS
Quality of Service	Provides wizards for configuring Network Admission Control (NAC) features such as Extensible Authentication Protocols (EAP)
NAC	Helps you configure NAC

In addition to the configuration wizards, notice the **Additional Tasks** button, as shown in Figure 3-6.

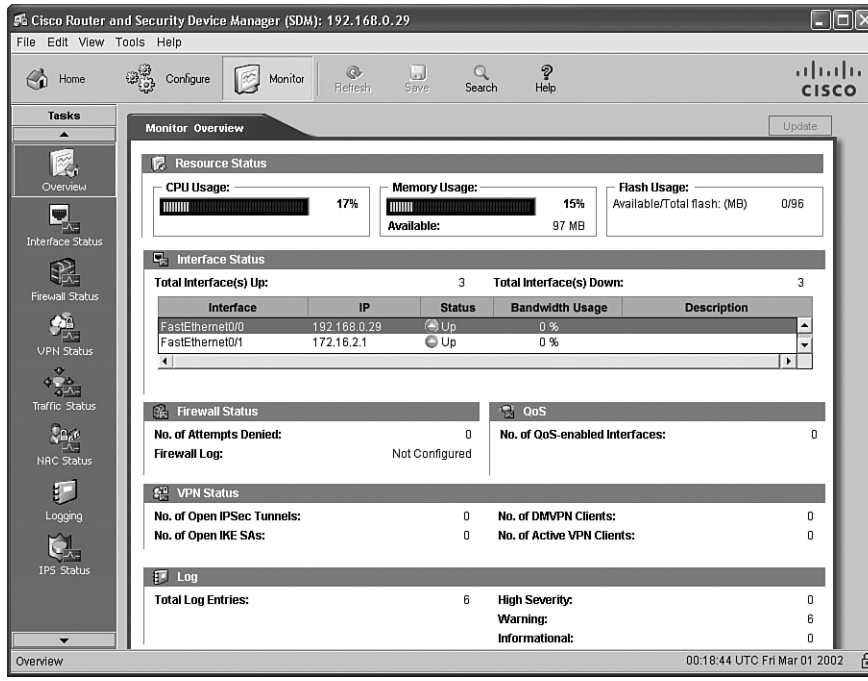
Figure 3-6 *Additional Tasks Button*



Advanced administrators can use graphical interfaces to configure these additional tasks. Examples of these tasks are DHCP configuration, DNS configuration, and AAA configuration.

After clicking the **Monitor** button, you see a screen similar to the one shown in Figure 3-7. Clicking the various buttons in the Tasks bar allows you to monitor the status of various router features. Examples are firewall status, VPN status, and IPS status.

Figure 3-7 *Monitoring Tasks*



This chapter has introduced SDM. Subsequent chapters will detail how you can leverage SDM to configure a variety of security options. For exam purposes, you should be comfortable with navigating the various SDM screens and performing basic configuration tasks.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, denoted with the Key Topic icon. Table 3-12 lists these key topics and the page where each is found.

Table 3-12 *Key Topics for Chapter 3*

Key Topic Element	Description	Page Number
Table 3-2	IOS security features	**81**
List	ISR enhancements	**85**
Table 3-7	Passwords configured during the SETUP script	**88**
Table 3-8	Cisco IOS Resilient Configuration steps	**96**
List	Requirements added by Cisco IOS Login Enhancements for Virtual Connections	**96**
Example 3-18	Creating a message-of-the-day banner	**99**
List	Cisco SDM benefits	**100**
Table 3-11	Cisco SDM wizards	**103-104**

Complete the Tables and Lists from Memory

Print a copy of Appendix D, "Memory Tables," (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Tables Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Definition of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

Integrated Services Router (ISR), dictionary attack, brute-force attack, privilege level, role-based command-line interface (CLI) view, bootset, Cisco Security Device Manager (SDM)

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. To see how well you have memorized the commands as a side effect of your other studies, cover the left side of the table with a piece of paper, read the descriptions on the right side, and see whether you remember the commands.

Table 3-13 *Chapter 3 Configuration Command Reference*

Command	Description
enable secret *password*	A global configuration mode command that configures a router's enable secret password
password *password*	A line configuration mode command that configures a password for a line (such as a con, aux, or vty line)
login	A line configuration mode command that configures a line to require a login
service password-encryption	A global configuration mode command that encrypts plain-text passwords in a router's configuration
exec-timeout *minutes* [*seconds*]	A line configuration mode command that specifies an inactivity period before logging out a user
security authentication failure *rate number_of_failed_attempts* **log**	A global configuration mode command used to specify the maximum number of failed attempts (in the range of 2 to 1024) before introducing a 15-second delay; also generates a log message if the specified threshold is exceeded
privilege *mode* {**level** *level command* | **reset** *command*}	A global configuration mode command used to associate a command (issued in a specific mode) with a specified privilege level, in the range 0 to 15 (although custom privilege levels are in the range 1 to 14), or to reset a command to its default level
aaa new-model	A global configuration mode command used to enable authentication, authorization, and accounting (AAA)
parser view *view_name*	A global configuration mode command used to create a new view
secret 0 *password*	A view configuration mode command used to set the password required to invoke the view
commands *parser_mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface_identifier* | *command*]	A view configuration mode command that allows an administrator to specify a command (or interface) available to a particular view

continues

Table 3-13 *Chapter 3 Configuration Command Reference (Continued)*

Command	Description
secure boot-image	A global configuration mode command used to enable image resilience
secure boot-config	A global configuration mode command that archives the running configuration of a router to persistent storage
login block-for *seconds* **attempts** *attempts* **within** *seconds*	A global configuration mode command that specifies the number of failed login attempts (within a specified time period) that trigger a quiet period, during which login attempts will be blocked
login quiet-mode access-class {*acl-name* | *acl-number*}	A global configuration mode command that specifies an ACL that identifies exemptions from the previously described quiet period
login delay *seconds*	A global configuration mode command that specifies a minimum period of time that must pass between login attempts
login on-failure log [**every** *login_attempts*]	A global configuration mode command that creates log messages for failed login attempts
login on-success log [**every** *login_attempts*]	A global configuration mode command that creates log messages for successful login attempts
banner motd *delimiter message_body delimiter*	A global configuration mode command that configures a message to be displayed when a user administratively connects to a router
ip http server	A global configuration mode command that enables an HTTP server on a router
ip http secure-server	A global configuration mode command that enables a secure HTTP (HTTPS) server on a router
ip http authentication local	A global configuration mode command that configures a local authentication method for accessing the HTTPS server
username *name* **privilege 15 secret 0** *password*	A global configuration mode command that configures a username and password to be used for authentication local to the router

Table 3-14 *Chapter 3 EXEC Command Reference*

Command	Description
enable view	Enables the root view, which is represented by the set of commands available to an administrator logged in with a privilege level of 15
enable view *view_name*	Switches to the specific view (after the required credentials are provided)
show secure bootset	Used to verify that Cisco IOS Resilient Configuration is enabled and that the files in the bootset have been secured
show login	Can be used to verify that enhanced support for virtual logins is configured and to view the login parameters