Your Short Cut to Knowledge

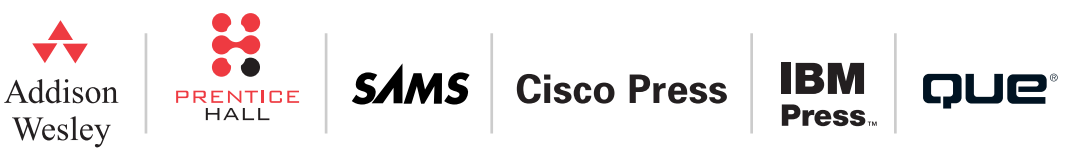
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Securing Administrative Access to Routers

It is critical to secure administrative access to the routers that help power your network infrastructure. This section details exactly how this should be carried out.

Router security principles

There are three areas of router security:

- Physical security
- Operating system
- Router hardening

Cisco Integrated Services Router family

Cisco Integrated Services Routers feature comprehensive security services, embedding data, security, voice, and wireless in the platform portfolio for fast, scalable delivery of mission-critical business applications. Models include the 800 Series, 1800 Series, 2800 Series, and 3800 Series.

Configuring secure administrative access

You need to secure administrative access for local access (console port) and remote access such as HTTP or Telnet/SSH.

 Please see page 88 for more details.

Be sure to password-protect your router. These commands can be used:

- Console password

```
line console 0
login
password cisco
```

- Virtual terminal password

```
line vty 0 4
login
password cisco
```

- Enable password

```
enable password cisco
```

- Secret password

```
enable secret cisco
```

All these passwords are in clear text in the configuration files with the exception of the **enable secret** command. To encrypt the passwords that are clear text, use the command **service password-encryption**.

To configure idle timeouts for router lines, use the command **exec-timeout** *minutes* [*seconds*].

You can also configure minimum password lengths with the **security passwords min-length** *length* command.

To create username and password entries in the local accounts database, use the syntax **username** *name* **secret** {[**0**] *password* | **5** *encrypted-secret*}.

 Please see page 88 for more details.

To disable the ability to access ROMMON to disable password recovery on your router, use **no service password-recovery**.

Setting multiple privilege levels

You can configure multiple privilege levels on the router for different levels of your administrators. There are 16 privilege levels, 0 to 15. Level 0 is reserved for user-level access privileges, levels 1 to 14 are levels you can customize, and level 15 is reserved for privileged mode commands. To assign privileges to levels 2 to 14, use the **privilege** command from global configuration mode. The syntax for this command is **privilege mode** {**level** *level command* | **reset** *command*}. Remember that privilege levels are "cascading." If a user has level 13 access, that user also gains access to the commands in levels 1 through 12.

Role-based CLI access

A new approach to having various levels of access for different administrators is called role-based CLI access. Using this approach, different administrators have different "views" of the CLI. These views contain the specific commands that are available for different administrators. To configure role-based CLI, complete the following steps:

Step 1. Enable AAA.

Step 2. Use the **enable view** command to enable the feature.

Step 3. Use the **configure terminal** command to enter global configuration mode.

Step 4. Use the **parser view** *view-name* command to create a new view.

Step 5. Use the **secret** command to assign a password to the view.

 Please see page 88 for more details.

Step 6. Use the command **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] to assign commands to the selected view.

Step 7. Verify using the **enable view** command.

Securing the Cisco IOS image and configuration files

You can now secure copies of the IOS and your configuration file in memory so that they cannot be maliciously or accidentally erased. The **secure boot-image** command protects the IOS image, and the command **secure boot-config** protects the running configuration. These protected files will not even appear in a **dir** listing of flash. To see these protected files, use the **show secure bootset** command.

Enhanced security for virtual logins

The following commands have been added to enhance security for virtual logins:

- **login block-for** *seconds* **attempts** *tries* **within** *seconds*

  This command configures your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection. This command is mandatory; all other commands here are optional.

- **login quiet-mode** *access-class* {*acl-name* | *acl-number*}

  This command specifies an ACL that is to be applied to the router when it switches to quiet mode. The devices that match a **permit** statement in the ACL are exempt from the quiet period.

- **login delay** *seconds*

  Configures a delay between successive login attempts.

- **login on-failure log** [**every** *login*]

  Generates logging messages for failed login attempts.

 Please see page 88 for more details.

- **login on-success log** [**every** *login*]

  Generates logging messages for successful login attempts.

- **show login**

  Verifies that the **login block-for** command is issued.

Banner messages

Banner messages are important. With these messages, you can ensure that unauthorized personnel are informed that they will be prosecuted for illegal access. The syntax for this command is **banner** {**exec** | **incoming** | **login** | **motd** | **slip-ppp**} *d message d*.

Cisco Security Device Manager (SDM)

SDM is a powerful graphical user interface you can use to configure and monitor your Cisco router.

Supporting SDM

Cisco SDM is factory-installed on some router models. It is also available on a CD-ROM that is included with new routers, and it can be downloaded from Cisco.com. In addition to the full SDM, an SDM Express version is available.

If the router is an existing router and is not configured with the Cisco SDM default configuration, configure the following services for Cisco SDM to access the router properly:

- Set up a username and password that has privilege level 15:

```
username name privilege 15 secret password
```

 Please see page 88 for more details.