Overview

This documentation supports Cisco 1800 Series Integrated Services Routers (Modular), providing a chassis in which you can install WAN interface cards (WICs), voice/WAN interface cards (VWICs) (data mode only for the Cisco 1841 router), and high-speed WAN interface cards (HWICs.)

The Cisco 1841 router is a data-only router with two HWIC/WIC/VWIC slots, capable of supporting single-wide HWICs and one advanced integration module (AIM) slot. It can be placed on a desktop or wall-mounted.

Note Although you can use VWICs in the Cisco 1841 router, they will only function in data modes. Voice interfaces are not supported.

Note The interface numbering and asynchronous line numbering on Cisco 1800 series routers are different from the numbering schemes used on other Cisco modular routers. For details, see the hardware installation documentation for your router.

Cisco 1800 Series Software Configuration Documentation

Unlike traditional documentation, wherein all of the information appears within one printed book, the Cisco 1800 series routers software configuration documentation takes advantage of the capabilities inherent in web-based presentation. This includes extensive hyperlinking to other information, tools, and many other resources on Cisco.com.

Instead of chapters, each topic area can be accessed independently. At the top level, available at "Cisco 1800 Series Software Configuration," the main software configuration topics include:

- Basic Software Configuration
    - Basic Software Configuration Using the Setup Command Facility
    - Basic Software Configuration Using the Cisco IOS Command-Line Interface
- Finding Feature Documentation
- Configuration Examples
- Troubleshooting and Maintenance

Cisco Systems, Inc.
www.cisco.com

- – [Upgrading the System Image]
- – [Using CompactFlash Memory Cards]
- – [Using the ROM Monitor]
- – [Changing the Configuration Register Settings]
- – [Troubleshooting Links]
- [Cisco 1800 Series Cards and Modules]

> **Note** Besides the setup facility and the IOS command-line interface, a third way of configuring Cisco routers is through the Cisco Router and Security Device Manager. Additional information about SDM features, is available at this URL: http://www.cisco.com/go/sdm

> **Note** You must have an account on Cisco.com to access many of the available tools. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions.

Contents

Following is a list of the main topics covered in the remainder of this overview:

Performing Initial Configuration

You can configure your router by using one of the following methods:

Initial Configuration Using the Cisco Router and Security Device Manager

> **Note** We recommend that you use the Cisco Router and Security Device Manager to configure your router. Built-in verification systems and sanity checks help to ensure both correct configurations and robust security practices.

The Cisco Router and Security Device Manager (SDM) is an easy-to-use device management tool that allows you to configure Cisco IOS security features and network connections through an intuitive web-based graphical user interface. You can use SDM wizards to:

- Configure additional LAN and WAN connections
- Create firewalls

- Configure Virtual Private Network (VPN) connections
- Perform security audits

SDM also provides an advanced mode, through which you can configure advanced features, such as Firewall Policy, Network Address Translation (NAT), VPNs, routing protocols, and other options.

For More Information About SDM and About Your Router

For additional information about SDM features, refer to the SDM online help. Additional information about SDM is also available at this URL:

http://www.cisco.com/go/sdm

Here you can find detailed information about SDM, including an SDM FAQ, data sheet, customer presentation, Flash demo, and links to technical documentation and product updates.

Refer to the quick start guide for your router for other procedures, such as connecting a PC to the router console port so that you can use the CLI when you need to, and using the router LEDs to verify installation. The quick start guide may also contain important warranty information.

Obtaining the Latest Version of SDM

SDM is regularly enhanced to provide new features. If you are already running SDM on the router, you can update SDM automatically by clicking on the Tools menu and selecting **Update SDM**. SDM will determine whether there is a more recent version available and enables you to download and install it on the router.

If you have a supported router that does not have SDM installed, you can download the latest version of SDM free of charge. Instructions for installing it on your router can be found at this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

You should consult the SDM release notes to determine if SDM is supported for the router on which you want to install it.

If the following messages appear at the end of the startup sequence, Cisco Router and Security Device Manager (SDM) is installed on your router:

```
yourname con0 is now available

Press RETURN to get started.
```

Tip If these messages do not appear, SDM was not shipped with your router. If you want to use SDM, you can download the latest version of SDM and instructions for installing it on your router from the following URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

To obtain the SDM quick start guide, SDM release notes, and other SDM documentation, go to http://www.cisco.com/go/sdm and click the Technical Documentation link.

For instructions on configuring your router by using SDM, refer to the *Cisco Router and Security Device Manager (SDM) Quick Start Guide* that shipped with your router.

Initial Configuration Using the Setup Command Facility

This section shows how to use the setup command facility to configure a host name for the router, set passwords, and configure an interface for communication with the management network.

If the following messages appear at the end of the startup sequence, the setup command facility has been invoked automatically:

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

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

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

The setup command facility prompts you for basic information about your router and network, and it creates an initial configuration file. After the configuration file is created, you can use the CLI or Security Device Manager to perform additional configuration.

The prompts in the setup command facility vary, depending on your router model, the installed interface modules, and the software image. The following example and the user entries (in **bold**) are shown as examples only.

✎ **Note**   If you make a mistake while using the setup command facility, you can exit and run the setup command facility again. Press **Ctrl-C**, and enter the **setup** command at the privileged EXEC mode prompt (`Router#`).

Step 1   To proceed using the setup command facility, enter **yes**:

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

Step 2   When the following messages appear, enter **yes** to enter basic management setup:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

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

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

Step 3   Enter a host name for the router (this example uses Router):

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

Step 4   Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration:

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

Step 5   Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration:

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

Step 6   Enter the virtual terminal password, which prevents unauthenticated access to the router through ports other than the console port:

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

Step 7   Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [yes]:
    Community string [public]:
```

A summary of the available interfaces is displayed.

Note   The interface numbering that appears depends on the type of Cisco modular router platform and on the installed interface modules and cards.

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 0/0     24        23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface               IP-Address      OK? Method Status               Prol
FastEthernet0/0         unassigned      NO  unset  up                   up
FastEthernet0/1         unassigned      NO  unset  up                   dow
```

Step 8   Select one of the available interfaces for connecting the router to the management network:

```
Enter interface name used to connect to the
management network from the above interface summary: fastethernet0/0
```

Step 9   Respond to the following prompts as appropriate for your network:

```
Configuring interface FastEthernet0/0:
Use the 100 Base-TX (RJ-45) connector? [yes]: yes
Operate in full-duplex mode? [no]: no
Configure IP on this interface? [yes]: yes
    IP address for this interface: 172.1.2.3
    Subnet mask for this interface [255.255.0.0] : 255.255.0.0
    Class B network is 172.1.0.0, 26 subnet bits; mask is /16
```

Step 10   The configuration is displayed:

```
The following configuration command script was created:

hostname Router
enable secret 5 $1$D5P6$PYx41/lQIASK.HcSbfO5q1
enable password xxxxxx
line vty 0 4
password xxxxxx
snmp-server community public
!
no ip routing
!
interface FastEthernet0/0
no shutdown
```

```
speed 100
duplex half
ip address 172.1.2.3 255.255.0.0
!
interface FastEthernet0/1
shutdown
no ip address
end
```

Step 11 Respond to the following prompts. Select [**2**] to save the initial configuration.

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

Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started! RETURN

The user prompt is displayed.
Router>
```

Step 12 Verify the initial configuration. See the "Verifying the Initial Configuration" section on page 7 for verification procedures.

For more information, see the "Basic Software Configuration Using the Setup Command Facility" section, available at this URL:

http://www.cisco.com/en/US/docs/routers/access/1800/1841/software/configuration/guide/b_setup.html

http://www.cisco.com/en/US/docs/ios/12_3/featlist/cfun_vcg.html

Initial Configuration Using the Command-Line Interface

This section describes briefly how to display a command-line interface (CLI) prompt for configuration using the CLI.

You can use the CLI if the following messages appear at the end of the startup sequence:

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

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

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

If these messages do not appear, SDM and a default configuration file were installed on the router at the factory. To use SDM to configure the router, see the "Initial Configuration Using the Cisco Router and Security Device Manager" section on page 2.

Note Be sure to save your configuration changes occasionally so that they are not lost during resets, power cycles, or power outages. Use the **copy running-config startup-config** command at the privileged EXEC mode prompt (`Router#`) to save the configuration to NVRAM.

Step 1   To proceed with manual configuration using the CLI, enter **no** when the power-up messages end.

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

Step 2   Press **Return** to terminate autoinstall and continue with manual configuration.

```
Would you like to terminate autoinstall? [yes] Return

Several messages appear, ending with a line similar to the following:
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled <date> <time> by <person>
```

Step 3   Press **Return** to display the `Router>` prompt.

```
...
flashfs[4]: Initialization complete.
Router>
```

Step 4   Enter privileged EXEC mode.

```
Router> enable
Router#
```

Step 5   Verify the initial configuration. See the "Verifying the Initial Configuration" section on page 7 for verification procedures.

For more information on using the CLI for router configuration, see "Basic Software Configuration Using the Cisco IOS Command-Line Interface" section, available at this URL:

http://www.cisco.com/en/US/docs/routers/access/1800/1841/software/configuration/guide/b_setup.html

Verifying the Initial Configuration

To verify that the new interfaces are operating correctly, perform the following tests:

- To verify that the interfaces are operating correctly and that the interfaces and line protocol are in the correct state—up or down—enter the **show interfaces** command.
- To display a summary status of the interfaces configured for IP, enter the **show ip interface brief** command.
- To verify that you configured the correct host name and password, enter the **show configuration** command.

When you have completed and verified the initial configuration, your Cisco router is ready to configure for specific functions.

Using the Cisco IOS Startup Sequence

This section explains how to use the IOS Startup sequence to configure your router, as an alternative to using SDM.

✎

Note Because SDM uses a default configuration file, if you have used SDM to configure your router, it *does not execute the standard Cisco IOS startup sequence*.

Using the Cisco IOS setup utility enables you to use TFTP or BOOTP configuration download, or use other features available through the standard Cisco IOS startup sequence.

The configuration file shipped with your router does the following:

- Provides an IP address for your Fast Ethernet interface, enabling an interface to your LAN
- Enables your router's HTTP/HTTPS server, allowing HTTP access from your LAN
- Creates a default username (**cisco**) and password (**cisco**) with privilege level 15
- Enables Telnet/SSM access to the router from your LAN

To erase the existing configuration and use the Cisco IOS startup sequence, perform the following steps.

✎

Note SDM remains installed on the router. See the "Enabling SDM on a Router Configured to Use the IOS Startup Sequence" section on page 9 for instructions to reenable it.

Step 1 Connect the light blue console cable, included with your router, from the blue console port on your router to a serial port on your PC. Refer to the hardware installation guide that came with your router for instructions.

Step 2 Connect the power supply to your router, plug the power supply into a power outlet, and turn on your router. Refer to the quick start guide that came with your router for instructions.

Step 3 Use Hyperterminal or a similar terminal emulation program on your PC, with the terminal emulation settings of 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to your router.

Step 4 At the prompt, enter the **enable** command. The default configuration file does not configure an enable password.

```
yourname> enable

yourname#
```

Step 5 Enter the **erase startup-config** command.

```
yourname# erase startup-config
```

Step 6 Confirm the command by pressing **Enter**.

Step 7 Enter the **reload** command.

```
yourname# reload
```

Step 8 Confirm the command by pressing **Enter**.

The router begins executing the standard startup sequence. If you want to use SDM to perform subsequent configurations for the router, you must reconfigure the router manually to support web-based applications and the Telnet and Secure Shell (SSH) protocols. You must also create a user account with a privilege level of 15. See the "Enabling SDM on a Router Configured to Use the IOS Startup Sequence" section on page 9 for information.

Enabling SDM on a Router Configured to Use the IOS Startup Sequence

If you erased the factory startup configuration to use the IOS startup sequence, you can still use SDM. To do so, you must configure the router to support web-based applications, configure it with a user account defined with privilege level 15, and then configure it to support the Telnet and SSH protocols. These changes can be made using a telnet session or using a console connection.

Configuring the Router to Support Web-Based Applications, a User with Priv 15, and Telnet/SSH

Step 1 Enable the HTTP/HTTPS server on the router, using the following Cisco IOS commands in the global configuration mode:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

If the router uses an IPSec IOS image, the HTTPS server is enabled. Otherwise only the HTTP server is enabled.

Step 2 Create a user account with privilege level 15 (enable privileges, if necessary).

```
Router(config)# username <username> privilege 15 password 0 <password>
```

Replace *<username>* and *<password>* with the username and password of your choosing.

Step 3 Configure SSH and Telnet for local login and privilege level 15:

```
line vty 0 4
 privilege level 15
 login local
 transport input telnet
 transport input telnet ssh
```

Step 4 (Optional) Enable local logging to support the log monitoring function:

```
Router(config)# logging buffered 51200 warning
```

Starting SDM on a Manually Configured Router

SDM is a web-based application that must be run from a PC that is connected to the router over a LAN. If the router is configured as a DHCP server, the PC must be configured to receive an IP address automatically. If the router is not configured as a DHCP server, you must configure the PC with a static IP address on the same subnet as the router interface to which you are connecting the PC. For example, if the router has the IP address 172.16.30.1, and the subnet mask is 255.255.255.248, you must configure the PC to use a network address in the range 172.16.30.2 through 172.16.30.6, and use the same subnet mask as the router.

Step 1 Open a web browser on the PC, and enter the IP address for the router:

https://*IP-address*

The https://... specifies that the Secure Socket Layer (SSL) protocol will be used for a secure connection. You can use **http://... if SSL is not available.**

Step 2   Enter the username and password that you specified in Step 2 of "Configuring the Router to Support Web-Based Applications, a User with Priv 15, and Telnet/SSH."

To continue configuring your router, see the "Initial Configuration Using the Cisco Router and Security Device Manager" section on page 2.