Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a terminal or PC to the router by using the light-blue console port. With a connected terminal or PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface (Ethernet, ADSL, or telephone) by using Telnet. The Telnet option assumes that the interface is up and running.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number

- Maintenance agreement or warranty information

- Type of software and version number

- Date you received the hardware

- Brief description of the problem

- Brief description of the steps you have taken to isolate the problem

ADSL Troubleshooting

If you experience trouble with the ADSL connection, verify the following:

- The ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, see the hardware guide for your router.
- The ADSL CD LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the ADSL LEDs, see the hardware installation guide specific for your router.
- The correct Asynchronous Transfer Mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports discrete multi-tone (DMT) Issue 2.
- The ADSL cable that you connect to the Cisco router must be 10BASE-T Category 5, unshielded twisted-pair (UTP) cable. Using regular telephone cable can introduce line errors.

SHDSL Troubleshooting

Symmetrical high-data-rate digital subscriber line (SHDSL) is available on the Cisco 1000 Integrated Services Routes. If you experience trouble with the SHDSL connection, verify the following:

- The SHDSL line is connected and using pins 3 and 4. For more information on the G.SHDSL connection, see the hardware guide for your router.
- The G.SHDSL LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the G.SHDSL LED, see the hardware installation guide specific for your router.
- The correct asynchronous transfer mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports the G.SHDSL signaling protocol.

Use the **show controllers dsl 0** command in EXEC mode to view an SHDSL configuration.

VDSL2 Troubleshooting

Very-high-data-rate digital subscriber line 2 (VDSL2) is available on the Cisco 1000 Series Integrated Services Routers. If you experience trouble with the VDSL2 connection, verify the following:

- The VDSL2 line is connected and using pins 3 and 4. For more information on the VDSL2 connection, see the hardware guide for your router.
- The VDSL2 LED CD light is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the VDSL2 LED, see the hardware installation guide specific for your router.
- The DSLAM supports the VDSL2 signaling protocol.

Use the **show controllers vdsl 0** command in EXEC mode to view a VDSL2 configuration. The debug vdsl 0 daemon state command can be used to enable the debug messages that print the state transition of VDSL2 training.

If there is trouble with the VDSL firmware file, you can reload or upgrade it without upgrading your Cisco IOS image. Use the command:

controller vdsl 0 firmware *flash:<firmware file name>*

to load the firmware file into the VDSL modem chipset. Then enter shutdown/no shutdown commands on the controller vdsl 0 interface. After this, the new firmware will be downloaded and the VDSL2 line starts training up.

Note Cisco 1000 series ISRs require that the router be reloaded (IOS reload) before the new VDSL firmware will be loaded.

If the command is not present or the named firmware file is corrupt or not available, the default firmware file *flash:vdsl.bin* is checked to be present and not corrupt. The firmware in this file is then downloaded to the modem chipset.

Note Cisco 1000 series ISRs will state the reason of failure during bootup if the new VDSL firmware fails to load after IOS reload.

show interfaces Troubleshooting Command

Use the **show interface**s command to display the status of all physical ports (Ethernet, Fast Ethernet, and ATM) and logical interfaces on the router. describes messages in the command output.

The following example shows how to view the status of Ethernet or Fast Ethernet Interfaces:

```
Router# show interfaces ethernet 0 **similar output for show interfaces fastethernet 0
command **
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.Oc13.a4db
(bia0010.9181.1281)
Internet address is 170.1.4.101/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255., txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
```

The following example shows how to view the status of ATM Interfaces:

```
Router# show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 14.0.0.16/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
```

```
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        512 packets input, 59780 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        426 packets output, 46282 bytes, 0 underruns
        0 output errors, 0 collisions, 2 interface resets
        0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to view the status of Dialer Interfaces:

```
Router# show interfaces dialer 1
Dialer 1 is up, line protocol is up
 Hardware is Dialer interface
 Internet address is 1.1.1.1/24
 MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
  255/255. txload 1/255, rxload 1/255
 Encapsulation PPP, loopback not set
 Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

The table below describes possible command output for the **show interfaces** command.

Table 1: show interfaces Command Output Description

Output	Cause
For ATM Interfaces	
ATM 0 is up, line protocol is up	The ATM line is up and operating correctly.
ATM 0 is down, line protocol is down	• The ATM interface has been disabled with the shutdown command. or • The ATM line is down, possibly because the ADSL cable is disconnected or because the wrong type of cable is connected to the ATM port.
ATM 0.*n* is up, line protocol is up	The specified ATM subinterface is up and operating correctly.
ATM 0.*n* is administratively down, line protocol is down	The specified ATM subinterface has been disabled with the shutdown command.
ATM 0.*n* is down, line protocol is down	The specified ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider).
For Ethernet/Fast Ethernet Interfaces	
Ethernet/Fast Ethernet *n* is up, line protocol is up	The specified Ethernet/Fast Ethernet interface is connected to the network and operating correctly.
Ethernet/Fast Ethernet *n* is up, line protocol is down	The specified Ethernet/Fast Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN.

Output	Cause
Ethernet/Fast Ethernet *n* is administratively down, line protocol is down	The specified Ethernet/Fast Ethernet interface has been disabled with the **shutdown** command, and the interface is disconnected.
For Dialer Interfaces	
Dialer *n* is up, line protocol is up	The specified dialer interface is up and operating correctly.
Dialer *n* is down, line protocol is down	• This is a standard message and may not indicate anything is actually wrong with the configuration. or • If you are having problems with the specified dialer interface, this can mean it is not operating, possibly because the interface has been brought down with the **shutdown** command, or the ADSL cable is disconnected.

ATM Troubleshooting Commands

Use the following commands to troubleshoot your ATM interface:

ping atm interface Command

Use the **ping atm interface** command to determine whether a particular PVC is in use. The PVC does not need to be configured on the router to use this command. The below example shows the use of this command to determine whether PVC 8/35 is in use.

The following example shows how to determine if a PVC is in use:

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

This command sends five OAM F5 loopback packets to the DSLAM (segment OAM packets). If the PVC is configured at the DSLAM, the ping is successful.

To test whether the PVC is being used at the aggregator, enter the following command:

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

This command sends end-to-end OAM F5 packets, which are echoed back by the aggregator.

show atm interface Command

To display ATM-specific information about an ATM interface, use the **show atm interface atm 0 command from** privileged EXEC mode.

The following example shows how to view information about an ATM interface:

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0
Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
Avail bw = 640
Config. is ACTIVE
```

The table below describes some of the fields shown in the command output.

Table 2: show atm interface Command Output Description

Field	Description
ATM interface	Interface number. Always 0 for the Cisco 860 and Cisco 880 series access routers.
AAL enabled	Type of AAL enabled. The Cisco 860 and Cisco 880 series access routers support AAL5.
Maximum VCs	Maximum number of virtual connections this interface supports.
Current VCCs	Number of active virtual channel connections (VCCs).
Maximum Transmit Channels	Maximum number of transmit channels.
Max Datagram Size	Configured maximum number of bytes in the largest datagram.
PLIM Type	Physical layer interface module (PLIM) type.

debug atm Commands

Use the **debug** commands to troubleshoot configuration problems that you might be having on your network. The **debug** commands provide extensive, informative displays to help you interpret any possible problems.

Guidelines for Using Debug Commands

Read the following guidelines before using debug commands to ensure appropriate results.

- All debug commands are entered in privileged EXEC mode.
- To view debugging messages on a console, enter the **logging console debug** command.
- Most **debug** commands take no arguments.
- To disable debugging, enter the **undebug all** command.
- To use **debug** commands during a Telnet session on your router, enter the **terminal monitor** command.

⚠

Caution   Debugging is assigned a high priority in your router CPU process, and it can render your router unusable. For this reason, use **debug** commands only to troubleshoot specific problems. The best time to use debug commands is during periods of low network traffic so that other activity on the network is not adversely affected.

You can find additional information and documentation about the **debug** commands in the Cisco IOS Debug Command Reference.

debug atm errors Command

Use the **debug atm errors** command to display ATM errors. The **no** form of this command disables debugging output.

The following example shows how to view the ATM errors:

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

debug atm events Command

Use the **debug atm events** command to display events that occur on the ATM interface processor and to diagnose problems in an ATM network. This command provides an overall picture of the stability of the network. The **no** form of this command disables debugging output.

If the interface is successfully communicating with the Digital Subscriber Line Access Multiplexer (DSLAM) at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8. Note that the modem state does not transition to 0x10.

The following example shows how to view the ATM interface processor events-success:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
```

```
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

The following example shows how to view the ATM interface processor events—failure:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

debug atm packet Command

Use the **debug atm packet** command to display all process-level ATM packets for both outbound and inbound packets. The output reports information online when a packet is received or a transmission is attempted. The **no** form of this command disables debugging output.

⚠️

Caution Because the **debug atm packet** command generates a significant amount of output for every packet processed, use it only when network traffic is low, so that other system activities are not adversely affected.

The command syntax is:

debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

no debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

where the keywords are defined as follows:

interface atm *number* (Optional) ATM interface or subinterface number.

vcd *vcd-number* (Optional) Number of the virtual circuit designator (VCD).

vc *vpi/vci number* VPI/VCI value of the ATM PVC.

The below example shows sample output for the **debug atm packet** command.

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
```

```
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

The table below describes some of the fields shown in the **debug atm packet** command output.

Table 3: debug atm packet Command Output Description

Field	Description
ATM0	Interface that is generating the packet.
(O)	Output packet. (I) would mean receive packet.
VCD: 0xn	Virtual circuit associated with this packet, where n is some value.
VPI: 0xn	Virtual path identifier for this packet, where n is some value.
DM: 0xn	Descriptor mode bits, where n is some value.
Length: n	Total length of the packet (in bytes) including the ATM headers.

Software Upgrade Methods

Several methods are available for upgrading software on the Cisco 860 and Cisco 880 series Integrated Services Routers, including:

- Copy the new software image to flash memory over LAN or WAN when the existing Cisco IOS software image is in use.

- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.
- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.

Recovering a Lost Password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register

2. Reset the Router

3. Reset the Password and Save your Changes (for lost enable secret passwords only)

4. Reset the Configuration Register Value.

Note Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Tip See the "Hot Tips" section on Cisco.com for additional information on replacing enable secret passwords.

Change the Configuration Register

To change a configuration register, follow these steps:

Procedure

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the Fthe router.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 At the privileged EXEC prompt (r*outer_name* #), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

Example:

```
Router# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
 16.6.2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 01-Nov-17 03:00 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON

Router uptime is 6 minutes
Uptime for this control processor is 8 minutes
System returned to ROM by Reload Command
System image file is "usb0:c1100-universalk9_ias.16.06.02.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
```

```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current          Type          Suite Next reboot
--------------------------------------------------------------------------------
FoundationSuiteK9     None                   None          None
securityk9
appxk9


Technology Package License Information:

------------------------------------------------------------------
Technology     Technology-package           Technology-package
               Current        Type          Next reboot
------------------------------------------------------------------
appxk9         None           None          None
securityk9     None           None          None
ipbase         ipbasek9       None          ipbasek9

cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.
Processor board ID FGL212392WT
8 Virtual Ethernet interfaces
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6762495K bytes of flash memory at bootflash:.
7855044K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2100

Router#
```

Step 4   Record the setting of the configuration register.

Step 5   To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Reset the Router

To reset the router, follow these steps:

Procedure

Step 1 If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

> **Note** Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press break. The terminal displays the following prompt:

Example:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

Example:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

Example:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

Example:

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

Step 5 Enter **no** in response to the prompts until the following message is displayed:

Example:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

Example:

```
Router>
```

Step 7 Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

Example:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

Example:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

Example:

```
Router# show startup-config
```

What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

Reset the Router

To reset the router, follow these steps:

Procedure

Step 1 If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

Note Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press break. The terminal displays the following prompt:

Example:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

Example:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

Example:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

Example:

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

Step 5 Enter **no** in response to the prompts until the following message is displayed:

Example:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

Example:

```
Router>
```

Step 7 Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

Example:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

Example:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

Example:

```
Router# show startup-config
```

What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

Reset the Password and Save Your Changes

To reset your password and save the changes, follow these steps:

Procedure

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **enable secret** command to reset the enable secret password in the router:

Example:

```
Router(config)# enable secret
password
```

Step 3 Enter **exit** to exit global configuration mode:

Example:

```
Router(config)# exit
```

Step 4 Save your configuration changes:

Example:

```
Router# copy running-config startup-config
```

Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

Procedure

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

Example:

```
Router(config)# config-reg
value
```

Step 3 Enter **exit** to exit configuration mode:

Example:

```
Router(config)# exit
```

Note To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

Step 4 Reboot the router, and enter the recovered password.

References

Refer to the following troubleshooting scenarios from the Cisco ISR guides:

- Monitor CPU Usage - http://www.cisco.com/c/en/us/support/docs/routers/ 4000-series-integrated-services-routers/210760-Monitor-CPU-Usage-On-ISR4300-Series.html

- Memory Troubleshooting Guide for Cisco 4000 Series ISRs - http://www.cisco.com/c/en/us/td/docs/ routers/access/4400/troubleshooting/memorytroubleshooting/isr4000_mem.html

- Stuck in ROMMON Trouble Shooting - http://www.cisco.com/c/en/us/support/docs/routers/ 4000-series-integrated-services-routers/200678-Troubleshoot-Cisco-4000-Series-ISR-Stuck.html

- Monitoring Control Plane Resource & Hardware Alarms Trouble Shooting - https://www.cisco.com/c/ en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/bm_isr_4400_sw_config_ guide_chapter_01000.html#concept_5A8508E657FA48E7B9563BE9073D4884

- SFP Modules Maintenance and Troubleshooting - http://www.cisco.com/c/en/us/support/docs/ interfaces-modules/cwdm-gbic-sfp/72370-sfp-trcvr-mods.html

- How to Find Error Message Details - https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/ configuration/guide/isr4400swcfg/bm_isr_4400_sw_config_guide_chapter_01001.html#concept_ AD47EC93DC3D4557B99BC155B8BB68FA

- IOS XE Syslog Messages - http://www.cisco.com/c/en/us/td/docs/ios/system/messages/guide/xemsg01.html

- Debugging AppNav/AppNav-XE and ISR-WAAS - http://www.cisco.com/c/en/us/td/docs/routers/access/ 4400/appnav/isr/isr_appnav/isr_trblshoot.html

- Troubleshooting for Cisco Smart Licensing Client - https://www.cisco.com/c/en/us/td/docs/routers/access/ 4400/software/configuration/guide/isr4400swcfg/isr4400swcfg_chapter_010011.html#reference_ C0E7BB9ED86D4FA18202EE72E87EB3A9

- Retrieving the License and Configuration Files - http://www.cisco.com/c/en/us/td/docs/routers/access/ 4400/flashmemory/isr4000_flashmem.html#72593

- Power and Cooling System Trouble Shooting - http://www.cisco.com/c/en/us/td/docs/routers/access/ 4400/troubleshooting/guide/isr4400trbl.html

- T1/E1 Data Clocking Trouble Shooting and Configuration - http://www.cisco.com/c/en/us/td/docs/routers/ access/4400/feature/guide/isr4400netclock.html#54707

- Troubleshooting Layer 2/3 Switch SW - http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/ eesm/software/configuration/guide/4451_config.html#pgfId-1000127

- Best Practices for Implementing WAN MACsec and MKA - http://www.cisco.com/c/en/us/td/docs/ ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/ wan-macsec-mka-support-enhance.html#reference_66BBEB1DDF3147DB8B89B6BB6CEBB7DC

- QoS FAQ - http://www.cisco.com/c/en/us/products/collateral/routers/ asr-1000-series-aggregation-services-routers/q-and-a-c67-731655.html

- SNMB Notification - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/technical_references/ 4400_mib_guide/isr4400_MIB/4400mib_04.html#42335

- Monitoring router interface through MIB - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/ technical_references/4400_mib_guide/isr4400_MIB/4400mib_05.html#96205