Configure Initial Router Settings on Cisco 4000 Series ISRs

This chapter describes how to perform the initial configuration on Cisco 4000 Series Integrated Services Routers (ISRs). It contains the following sections:

Perform Initial Configuration on Cisco 4000 Series ISRs

You can perform initial configuration on Cisco 4000 Series ISRs by using either the setup command facility or the Cisco IOS command-line interface (CLI).

- Use Cisco Setup Command Facility
- Use Cisco IOS XE CLI—Manual Configuration

Use Cisco Setup Command Facility

The setup command facility prompts you to enter the information about your router and network. The facility steps guides you through the initial configuration, which includes LAN and WAN interfaces. For more general information about the setup command facility, see the following document:

Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4, Part 2: Cisco IOS User Interfaces: Using AutoInstall and Setup:
http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3s/products-installation-and-configuration-guides-list.html.

This section explains how to configure a hostname for the router, set passwords, and configure an interface to communicate with the management network.

Note The messages that are displayed will vary based on your router model, the installed interface modules, and the software image. The following example and the user entries (in **bold**) are shown only as examples.

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 in privileged EXEC mode (`Router#`)

To configure the initial router settings by using the setup command facility, follow these steps:

Step 1 From the Cisco IOS-XE CLI, enter the **setup** command in privileged EXEC mode:

```
Router> enable
Password: <password>
Router# setup

         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

You are now in the Setup Configuration Utility.

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

Note This setup command facility is also entered automatically if there is no configuration on the router when it is booted into Cisco IOS-XE.

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#). For more information on using the setup command facility, see *The Setup Command* chapter in *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2T, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2t/fun/command/reference/122tfr.html

Step 2 To proceed using the setup command facility, enter **yes**.

```
Continue with configuration dialog? [yes/no]:

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 '[]'.
```

Step 3 To enter the basic management setup, enter **yes**.

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

Step 4 Enter a hostname for the router (this example uses ‘myrouter’):

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

Step 5 Enter an enable secret password. This password is encrypted (for more security) 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: cisco
```

Step 6 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (and is 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: cisco123
```

Step 7 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: cisco
```

Step 8 Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [no]: yes
    Community string [public]:
```

A summary of the available interfaces is displayed.

Note The interface summary includes interface numbering, which is dependent on the router model and the installed modules and interface cards.

```
Current interface summary

Interface          IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1/0 10.10.10.12     YES DHCP   up                    up
GigabitEthernet0/2/0 unassigned      YES NVRAM  administratively down down
SSLVPN-VIF0                unassigned      NO  unset  up

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

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

```
Configuring interface GigabitEthernet0/1/0:
  Configure IP on this interface? [yes]: yes
    IP address for this interface [10.10.10.12]:
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

The following configuration command script was created:

```
hostname myrouter
enable secret 5 $1$t/Dj$yAeGKviLLZNOBX0b9eifO0 enable password cisco123 line vty 0 4
password cisco snmp-server community public !
no ip routing

!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface GigabitEthernet0/1/0
no shutdown
ip address 10.10.10.12 255.255.255.0
!
interface GigabitEthernet0/2/0
shutdown
```

```
no ip address
!
end
```

Step 10 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:

```
myrouter>
```

Complete the Configuration

When using the Cisco Setup, and after you have provided all the information requested by the facility, the final configuration appears. To complete your router configuration, follow these steps:

Step 1 Choose to save the configuration when the facility prompts you to save the configuration.

- If you answer 'no', the configuration information you entered is *not* saved, and you return to the router enable prompt (`Router#`). Enter **setup** to return to the System Configuration Dialog.
- If you answer 'yes', the configuration is saved, and you are returned to the user EXEC prompt (`Router>`).

```
Use this configuration? {yes/no} : yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.


Press RETURN to get started!

%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down
%LINK-3-UPDOWN: Interface Serial0/2, changed state to down
%LINK-3-UPDOWN: Interface Serial1/0, changed state to up
%LINK-3-UPDOWN: Interface Serial1/1, changed state to down
%LINK-3-UPDOWN: Interface Serial1/2, changed state to down

<Additional messages omitted.>
```

Step 2 When the messages stop appearing on your screen, press **Return** to get the `Router>` prompt.

Step 3 Choose to modify the existing configuration or create another configuration. The `Router>` prompt indicates that you are now at the command-line interface (CLI) and you have just completed a initial router configuration. Nevertheless, this is *not* a complete configuration. At this point, you have two choices:

- Run the setup command facility again, and create another configuration.

```
Router> enable
```

```
Password: password
Router# setup
```

- Modify the existing configuration or configure additional features by using the CLI:

```
Router> enable
Password: password
Router# configure terminal
Router(config)#
```

Use Cisco IOS XE CLI—Manual Configuration

This section describes you how to access the command-line interface (CLI) to perform the initial configuration on the router.

Note To configure the initial router settings by using the Cisco IOS CLI, you must set up a console connection.

If the default configuration file is installed on the router prior to shipping, the system configuration dialog message does not appear, To configure the device, follow these steps:

Step 1 Enter the appropriate answer when the following system message appears on the router.

```
--- 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]: no
```

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

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

Several messages are displayed, ending with a line similar to the following:

```
...
Copyright (c) 1986-2012 by cisco Systems, Inc.
Compiled <date> <time> by <person>
```

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

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

Step 4 Type **enable** to enter privileged EXEC mode:

```
Router> enable
Router#
```

- Configure Cisco 4000 Series ISR Hostname, page 4-6 (Optional)
- Configure the Enable and Enable Secret Passwords, page 4-7 (Required)

Configure Cisco 4000 Series ISR Hostname

The hostname is used in CLI prompts and default configuration filenames. If you do not configure the router hostname, the router uses the factory-assigned default hostname "Router."

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. Verify that the router prompt displays your new hostname.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname myrouter`	Specifies or modifies the hostname for the network server.

	Command or Action	Purpose
Step 4	Verify that the router prompt displays your new hostname. **Example:** `myrouter(config)#`	—
Step 5	**end** **Example:** `myrouter# end`	(Optional) Returns to privileged EXEC mode.

Configure the Enable and Enable Secret Passwords

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** command or **enable secret** command. Both commands accomplish the same thing—they allow you to establish an encrypted password that users must enter to access privileged EXEC (enable) mode.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm. Use the **enable password** command only if you boot an older image of the Cisco IOS XE software.

For more information, see the "Configuring Passwords and Privileges" chapter in the *Cisco IOS Security Configuration Guide*. Also see the *Cisco IOS Password Encryption Facts* tech note and the *Improving Security on Cisco Routers* tech note.

Restrictions

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **enable secret** *password*
5. **end**
6. **enable**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**enable password** *password* **Example:** `Router(config)# enable password pswd2`	(Optional) Sets a local password to control access to various privilege levels. • We recommend that you perform this step only if you boot an older image of the Cisco IOS-XE software or if you boot older boot ROMs that do not recognize the **enable secret** command.
Step 4	**enable secret** *password* **Example:** `Router(config)# enable secret greentree`	Specifies an additional layer of security over the **enable password** command. • Do not use the same password that you entered in Step 3.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Verify that your new enable or enable secret password works.
Step 7	**end** **Example:** `Router(config)# end`	(Optional) Returns to privileged EXEC mode.

Configure the Console Idle Privileged EXEC Timeout

This section describes how to configure the console line's idle privileged EXEC timeout. By default, the privileged EXEC command interpreter waits 10 minutes to detect user input before timing out.

When you configure the console line, you can also set communication parameters, specify autobaud connections, and configure terminal operating parameters for the terminal that you are using. For more information on configuring the console line, see the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*. In particular, see the "Configuring Operating Characteristics for Terminals" and "Troubleshooting and Fault Management" chapters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **exec-timeout** *minutes* [*seconds*]
5. **end**
6. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**line console 0** **Example:** `Router(config)# line console 0`	Configures the console line and starts the line configuration command collection mode.
Step 4	**exec-timeout** *minutes* [*seconds*] **Example:** `Router(config-line)# exec-timeout 0 0`	Sets the idle privileged EXEC timeout, which is the interval that the privileged EXEC command interpreter waits until user input is detected. • The example shows how to specify no timeout. Setting the exec-timeout value to 0 will cause the router to never log out after it is logged in. This could have security implications if you leave the console without manually logging out using the disable command.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Router(config)# show running-config`	Displays the running configuration file. • Verify that you properly configured the idle privileged EXEC timeout.

Examples

The following example shows how to set the console idle privileged EXEC timeout to 2 minutes 30 seconds:

```
line console
 exec-timeout 2 30
```

The following example shows how to set the console idle privileged EXEC timeout to 30 seconds:

```
line console
 exec-timeout 0 30
```

Gigabit Ethernet Management Interface Overview

The router provides an Ethernet management port named GigabitEthernet0.

The purpose of this interface is to allow users to perform management tasks on the router. It is an interface that should not and often cannot forward network traffic. It ca, however, be used to access the router through Telnet and SSH to perform management tasks on the router. The interface is most useful before a router begins routing, or in troubleshooting scenarios when other forwarding interfaces are inactive.

Note he following aspects of the management ethernet interface:

- The router has one management ethernet interface named GigabitEthernet0.
- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The interface provides a way to access to the router even if forwarding interfaces are not functional, or the IOS process is down.
- The management ethernet interface is part of its own VRF. See the "Management Ethernet Interface VRF" section in the *Software Configuration Guide for Cisco 4000 Series ISRs* for more details.

Default Gigabit Ethernet Configuration

By default, a forwarding VRF is configured for the interface with a special group named "Mgmt-intf." This cannot be changed. This isolates the traffic on the management interface away from the forwarding plane. The basic configuration is like other interfaces; however, there are many forwarding features that are not supported on these interfaces. No forwarding features can be configured on the GigabitEthernet0 interface as it is only used for management.

For example, the default configuration is as follows:

```
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 172.18.77.212 255.255.255.240
negotiation auto
```

Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

The port can be accessed in configuration mode.

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

Configure Gigabit Ethernet Interfaces

This sections shows how to assign an IP address and interface description to an Ethernet interface on your router.

For comprehensive configuration information on Gigabit Ethernet interfaces, see the "Configuring LAN Interfaces" chapter of *Cisco IOS Interface and Hardware Component Configuration Guide*, http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflanin.html

For information on interface numbering, see the software configuration guide for your router.

SUMMARY STEPS

1. **enable**
2. **show ip interface brief**
3. **configure terminal**
4. **interface** {**fastethernet** | **gigabitethernet**} **0/0/***port*
5. **description** *string*
6. **ip address** *ip-address mask*
7. **no shutdown**
8. **end**
9. **show ip interface brief**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip interface brief** **Example:** `Router# show ip interface brief`	Displays a brief status of the interfaces that are configured for IP. • Learn which type of Ethernet interface is on your router.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**interface** {**fastethernet** | **gigabitethernet**} **0/***port* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies the Ethernet interface and enters interface configuration mode. **Note** For information on interface numbering, see Slots, Subslots (Bay), Ports, and Interfaces in Cisco 4000 Series ISRs, page 1-40.

	Command or Action	Purpose
Step 5	**description** *string* **Example:** `Router(config-if)# description GE int to 2nd floor south wing`	(Optional) Adds a description to an interface configuration. The description helps you remember what is attached to this interface. The description can be useful for troubleshooting.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.74.3 255.255.255.0`	Sets a primary IP address for an interface.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables an interface.
Step 8	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 9	**show ip interface brief** **Example:** `Router# show ip interface brief`	Displays a brief status of the interfaces that are configured for IP. Verify that the Ethernet interfaces are up and configured correctly.

Configuration Examples

Configuring the GigabitEthernet Interface: Example

```
!
interface GigabitEthernet0/0/0
 description GE int to HR group
 ip address 172.16.3.3 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
```

Sample Output for the show ip interface brief Command

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/1   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/3   unassigned      YES NVRAM  administratively down down
GigabitEthernet0       10.0.0.1        YES manual up                    up
```

Specify a Default Route or Gateway of Last Resort

This section describes how to specify a default route with IP routing enabled. For alternative methods of specifying a default route, see the *Configuring a Gateway of Last Resort Using IP Commands* Technical Specifications Note.

The Cisco IOS-XE software uses the gateway (router) as a last resort if it does not have a better route for a packet and if the destination is not a connected network. This section describes how to select a network as a default route (a candidate route for computing the gateway of last resort). The way in which routing protocols propagate the default route information varies for each protocol.

Configure IP Routing and IP Protocols

For comprehensive configuration information about IP routing and IP routing protocols, see the *Configuring IP Routing Protocol-Independent Feature* at cisco.com.

IP Routing

IP routing is automatically enabled in the Cisco ISO- XE software. When IP routing is configured, the system will use a configured or learned route to forward packets, including a configured default route.

Note This task section does not apply when IP routing is disabled. To specify a default route when IP routing is disabled, refer to the *Configuring a Gateway of Last Resort Using IP Commands* Technical Specifications Note at cisco.com.

Default Routes

A router might not be able to determine the routes to all other networks. To provide complete routing capability, the common practice is to use some routers as smart routers and give the remaining routers default routes to the smart router. (Smart routers have routing table information for the entire internetwork.) These default routes can be passed along dynamically, or can be configured into the individual routers.

Most dynamic interior routing protocols include a mechanism for causing a smart router to generate dynamic default information that is then passed along to other routers.

Default Network

If a router has an interface that is directly connected to the specified default network, the dynamic routing protocols running on the router generates or sources a default route. In the case of RIP, the router will advertise the pseudonetwork 0.0.0.0. In the case of IGRP, the network itself is advertised and flagged as an exterior route.

A router that is generating the default for a network may also need a default of its own. One way a router can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.

Gateway of Last Resort

When default information is being passed along through a dynamic routing protocol, no further configuration is required. The system periodically scans its routing table to choose the optimal default network as its default route. In the case of RIP, there is only one choice, network 0.0.0.0. In the case of IGRP, there might be several networks that can be candidates for the system default. The Cisco IOS-XE software uses both administrative distance and metric information to determine the default route (gateway of last resort). The selected default route appears in the gateway of last resort display of the **show ip route** EXEC command.

If dynamic default information is not being passed to the software, candidates for the default route are specified with the **ip default-network** global configuration command. In this usage, the **ip default-network** command takes an unconnected network as an argument. If this network appears in the routing table from any source (dynamic or static), it is flagged as a candidate default route and is a possible choice for the default route.

If the router has no interface on the default network, but does have a route to it, it considers this network as a candidate default path. The route candidates are examined and based on administrative distance and metric, the best one is chosen. The gateway to the best default path becomes the gateway of last resort.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**]
4. **ip default-network** *network-number*
   or
   ip route *dest-prefix mask next-hop-ip-address*
5. **end**
6. **show ip route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip routing** **Example:** `Router(config)# ip routing`	Enables IP routing.

	Command or Action	Purpose
Step 4	**ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**] **Example:** `Router(config)# ip route 192.168.24.0 255.255.255.0 172.28.99.2`	Establishes a static route.

Step 5	**ip default-network** *network-number*
	or
	ip route *dest-prefix mask next-hop-ip-address*
	
	Example:
	`Router(config)# ip default-network 192.168.24.0`
	
	Example:
	`Router(config)# ip route 0.0.0.0 0.0.0.0 172.28.99.1`
		Selects a network as a candidate route for computing the gateway of last resort.
		Creates a static route to network 0.0.0.0 0.0.0.0 for computing the gateway of last resort.

Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	**show ip route** **Example:** `Router# show ip route`	Displays the current routing table information. Verify that the gateway of last resort is set.

Configuration Examples

Specifying a Default Route: Example

```
!
ip route 192.168.24.0 255.255.255.0 172.28.99.2
!
ip default-network 192.168.24.0
!
```

Sample Output for the show ip route Command

```
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS
       summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
       candidate default,
       U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP a - application route + - replicated route, % - next hop override

Gateway of last resort is not set 40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C
       40.0.0.0/24 is directly connected, Loopback1 L 40.0.0.1/32 is directly connected,
       Loopback1 Router#
```

Configure Virtual Terminal Lines for Remote Console Access

Virtual terminal (vty) lines are used to allow remote access to the router. This section shows you how to configure the virtual terminal lines with a password, so that only authorized users can remotely access the router.

By default, the router has five virtual terminal lines. However, you can create additional virtual terminal lines. See the Cisco IOS XE Dial Technologies Configuration Guide at http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/2_xe/dia_2_xe_book.html.

Line passwords and password encryption is described in the Cisco IOS XE Security Configuration Guide: Secure Connectivity document available at the following URL: http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/2_xe/sec_secure_connectivity_xe_book.html. See the Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices section. If you want to secure the virtual terminal lines (vty) with an access list, see the Access Control Lists: Overview and Guidelines.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**
6. **end**
7. **show running-config**
8. From another network device, attempt to open a Telnet session to the router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**line vty** *line-number* [*ending-line-number*] **Example:** `Router(config)# line vty 0 4`	Starts the line configuration command collection mode for the virtual terminal lines (vty) for remote console access. • Make sure that you configure all vty lines on your router. **Note** To verify the number of vty lines on your router, use the **line vty ?** command.

	Command or Action	Purpose
Step 4	**password** *password* **Example:** `Router(config-line)# password guessagain`	Specifies a password on a line.
Step 5	**login** **Example:** `Router(config-line)# login`	Enables password checking at login.
Step 6	**end** **Example:** `Router(config-line)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration file. Verify that you bave properly configured the virtual terminal lines for remote access.

Step 8	From another network device, attempt to open a Telnet session to the router.
	
	Example:
	`Router# 172.16.74.3`
	`Password:`
		Verifies that you can remotely access the router and that the virtual terminal line password is correctly configured.

Configuration Examples

The following example shows how to configure virtual terminal lines with a password:

```
!
line vty 0 4
 password guessagain
 login
!
```

What to Do Next

After you configure the vty lines, follow these steps:

- (Optional) To encrypt the virtual terminal line password, see the "Configuring Passwords and Privileges" chapter in the *Cisco IOS Security Configuration Guide*. Also see the *Cisco IOS Password Encryption Facts* tech note.
- (Optional) To secure the VTY lines with an access list, see the "Part 3: Traffic Filtering and Firewalls" in the *Cisco IOS Security Configuration Guide*.

Configure the Auxiliary Line

This section describes how to enter line configuration mode for the auxiliary line. How you configure the auxiliary line depends on your particular implementation of the auxiliary (AUX) port. See the following documents for information on configuring the auxiliary line:

- *Configuring a Modem on the AUX Port for EXEC Dialin Connectivity*, Technical Specifications Note

  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080094bbc.shtml
- *Configuring Dialout Using a Modem on the AUX Port*, sample configuration

  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a0080094579.shtml
- *Configuring AUX-to-AUX Port Async Backup with Dialer Watch*, sample configuration

  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a0080093d2b.shtml
- *Modem-Router Connection Guide*, Technical Specifications Note

  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a008009428b.shtml

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line aux 0**
4. See the Technical Specifications Note and sample configurations to configure the line for your particular implementation of the AUX port.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**line aux 0** **Example:** `Router(config)# line aux 0`	Starts the line configuration command collection mode for the auxiliary line.
Step 4	See the Technical Specifications Note and sample configurations to configure the line for your particular implementation of the AUX port.	—

Verify Network Connectivity

This section describes how to verify network connectivity for your router.

Prerequisites

- All configuration tasks describe in this chapter must be completed.
- The router must be connected to a properly configured network host.

SUMMARY STEPS

1. **enable**
2. **ping** [*ip-address* | *hostname*]
3. **telnet** {*ip-address* | *hostname*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**ping** [*ip-address* | *hostname*] **Example:** `Router# ping 172.16.74.5`	Diagnoses initial network connectivity. To verify connectivity, ping the next hop router or connected host for each configured interface to.
Step 3	**telnet** {*ip-address* | *hostname*} **Example:** `Router# telnet 10.20.30.40`	Logs in to a host that supports Telnet. If you want to test the vty line password, perform this step from a different network device, and use your router's IP address.

Examples

The following display shows sample output for the ping command when you ping the IP address 192.168.7.27:

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

The following display shows sample output for the ping command when you ping the IP hostname donald:

```
Router# ping donald

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

Save Your Device Configuration

This section describes how to avoid losing your configuration at the next system reload or power cycle by saving the running configuration to the startup configuration in NVRAM. The NVRAM provides 256KB of storage on the router.

SUMMARY STEPS

1. **enable**
2. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Save Backup Copies of Configuration and System Image

To aid file recovery and minimize downtime in case of file corruption, we recommend that you save backup copies of the startup configuration file and the Cisco IOS-XE software system image file on a server.

SUMMARY STEPS

1. **enable**
2. **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**}
3. **show bootflash:**
4. **copy {bootflash}:** {**ftp:** | **rcp:** | **tftp:**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} **Example:** `Router# copy nvram:startup-config ftp:`	Copies the startup configuration file to a server. The configuration file copy can serve as a backup copy.Enter the destination URL when prompted.
Step 3	**show {bootflash0|bootflash1}:** **Example:** `Router# show {bootflash0|bootflash1}:`	Displays the layout and contents of a flash memory file system. Learn the name of the system image file.
Step 4	**copy {bootflash0|bootflash1}:** {**ftp:** | **rcp:** | **tftp:**} **Example:** `Router# copy {bootflash0|bootflash1}: ftp:`	Copies a file from flash memory to a server. • Copy the system image file to a server to serve as a backup copy. • Enter the filename and destination URL when prompted.

Configuration Examples

Copying the Startup Configuration to a TFTP Server: Example

The following example shows the startup configuration being copied to a TFTP server:

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Copying from Flash Memory to a TFTP Server: Example

The following example shows the use of the **show {flash0|flash1}:** command in privileged EXEC to learn the name of the system image file and the use of the **copy {flash0|flash1}: tftp:** privileged EXEC command to copy the system image to a TFTP server. The router uses the default username and password.

```
Router#Directory of bootflash:
```

```
11 drwx 16384 Jun 12 2012 17:31:45 +00:00 lost+found 64897 drwx 634880 Sep 6 2012 14:33:26
+00:00 core 340705 drwx 4096 Oct 11 2012 19:28:27 +00:00 .prst_sync 81121 drwx 4096 Jun 12
2012 17:32:39 +00:00 .rollback_timer 12 -rw- 0 Jun 12 2012 17:32:50 +00:00 tracelogs.336
713857 drwx 1347584 Oct 11 2012 20:24:26 +00:00 tracelogs 162241 drwx 4096 Jun 12 2012
17:32:51 +00:00 .installer 48673 drwx 4096 Jul 2 2012 17:14:51 +00:00 vman_fdb 13 -rw-
420654048 Aug 28 2012 15:01:31 +00:00
crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120826_083012.SSA.bin 14 -rw- 727035 Aug 29
2012 21:03:25 +00:00 uut2_2000_ikev1.cfg 15 -rw- 420944032 Aug 29 2012 19:40:28 +00:00
crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120829_033026.SSA.bin 16 -rw- 1528 Aug 30 2012
14:24:38 +00:00 base.cfg 17 -rw- 360900 Aug 31 2012 19:10:02 +00:00 uut2_1000_ikev1.cfg 18
-rw- 421304160 Aug 31 2012 16:34:19 +00:00
crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120821_193221.SSA.bin 19 -rw- 421072064 Aug 31
2012 18:31:57 +00:00 crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120830_110615.SSA.bin 20
-rw- 453652 Sep 1 2012 01:48:15 +00:00 uut2_1000_ikev1_v2.cfg 21 -rw- 16452768 Sep 11 2012
20:36:20 +00:00 upgrade_stage_1_of_1.bin.2012-09-05-Delta 22 -rw- 417375456 Sep 12 2012
20:28:23 +00:00 crankshaft-universalk9.2012-09-12_00.45_cveerapa.SSA.bin 23 -rw- 360879
Oct 8 2012 19:43:36 +00:00 old-config.conf 24 -rw- 390804800 Oct 11 2012 15:34:08 +00:00
_1010t.bin 7451738112 bytes total (4525948928 bytes free)

Router#show bootflash: -#- --length-- ---------date/time--------- path 1 4096 Oct 11 2012
20:22:19 +00:00 /bootflash/ 2 16384 Jun 12 2012 17:31:45 +00:00 /bootflash/lost+found 3
634880 Sep 06 2012 14:33:26 +00:00 /bootflash/core 4 1028176 Sep 06 2012 14:31:17 +00:00
/bootflash/core/UUT2_RP_0_iomd_17360.core.gz 5 1023738 Sep 06 2012 14:31:24 +00:00
/bootflash/core/UUT2_RP_0_iomd_23385.core.gz 6 1023942 Sep 06 2012 14:31:30 +00:00
/bootflash/core/UUT2_RP_0_iomd_24973.core.gz 7 1023757 Sep 06 2012 14:31:37 +00:00
/bootflash/core/UUT2_RP_0_iomd_26241.core.gz 8 1023726 Sep 06 2012 14:31:43 +00:00
/bootflash/core/UUT2_RP_0_iomd_27507.core.gz 9 1023979 Sep 06 2012 14:31:50 +00:00
/bootflash/core/UUT2_RP_0_iomd_28774.core.gz 10 1023680 Sep 06 2012 14:31:56 +00:00
/bootflash/core/UUT2_RP_0_iomd_30045.core.gz 11 1023950 Sep 06 2012 14:32:02 +00:00
/bootflash/core/UUT2_RP_0_iomd_31332.core.gz 12 1023722 Sep 06 2012 14:32:09 +00:00
/bootflash/core/UUT2_RP_0_iomd_5528.core.gz 13 1023852 Sep 06 2012 14:32:15 +00:00
/bootflash/core/UUT2_RP_0_iomd_7950.core.gz 14 1023916 Sep 06 2012 14:32:22 +00:00
/bootflash/core/UUT2_RP_0_iomd_9217.core.gz 15 1023875 Sep 06 2012 14:32:28 +00:00
/bootflash/core/UUT2_RP_0_iomd_10484.core.gz 16 1023907 Sep 06 2012 14:32:35 +00:00
/bootflash/core/UUT2_RP_0_iomd_11766.core.gz 17 1023707 Sep 06 2012 14:32:41 +00:00
/bootflash/core/UUT2_RP_0_iomd_13052.core.gz 18 1023963 Sep 06 2012 14:32:48 +00:00
/bootflash/core/UUT2_RP_0_iomd_14351.core.gz 19 1023915 Sep 06 2012 14:32:54 +00:00
/bootflash/core/UUT2_RP_0_iomd_15644.core.gz 20 1023866 Sep 06 2012 14:33:00 +00:00
/bootflash/core/UUT2_RP_0_iomd_17171.core.gz 21 1023518 Sep 06 2012 14:33:07 +00:00
/bootflash/core/UUT2_RP_0_iomd_18454.core.gz 22 1023938 Sep 06 2012 14:33:13 +00:00
/bootflash/core/UUT2_RP_0_iomd_19741.core.gz 23 1024017 Sep 06 2012 14:33:20 +00:00
/bootflash/core/UUT2_RP_0_iomd_21039.core.gz 24 1023701 Sep 06 2012 14:33:26 +00:00
/bootflash/core/UUT2_RP_0_iomd_22323.core.gz 25 4096 Oct 11 2012 19:28:27 +00:00
/bootflash/.prst_sync 26 4096 Jun 12 2012 17:32:39 +00:00 /bootflash/.rollback_timer 27 0
Jun 12 2012 17:32:50 +00:00 /bootflash/tracelogs.336 28 1347584 Oct 11 2012 20:24:26
+00:00 /bootflash/tracelogs 29 392 Oct 11 2012 20:22:19 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.gz 30 308 Oct 11 2012 18:39:43 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011183943.gz 31 308 Oct 11 2012
18:49:44 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011184944.gz 32 42853
Oct 04 2012 07:35:39 +00:00 /bootflash/tracelogs/hman_R0-0.log.0498.20121004073539.gz 33
307 Oct 11 2012 18:59:45 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011185945.gz 34 308 Oct 11 2012
19:19:47 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011191947.gz 35 307
Oct 11 2012 19:37:14 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011193714.gz 36 308 Oct 11 2012
19:47:15 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011194715.gz 37 308
Oct 11 2012 19:57:16 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011195716.gz 38 308 Oct 11 2012
20:07:17 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011200717.gz 39 307
Oct 11 2012 20:12:18 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011201218.gz 40 306 Oct 11 2012
20:17:18 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011201718.gz 41 44220
Oct 10 2012 11:47:42 +00:00 /bootflash/tracelogs/hman_R0-0.log.32016.20121010114742.gz 42
64241 Oct 09 2012 20:47:59 +00:00
```

```
/bootflash/tracelogs/fman-fp_F0-0.log.12268.20121009204757.gz 43 177 Oct 11 2012 19:27:03
+00:00 /bootflash/tracelogs/inst_compmatrix_R0-0.log.gz 44 307 Oct 11 2012 18:24:41 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011182441.gz 45 309 Oct 11 2012
18:29:42 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011182942.gz 46 43748
Oct 06 2012 13:49:19 +00:00 /bootflash/tracelogs/hman_R0-0.log.0498.20121006134919.gz 47
309 Oct 11 2012 18:44:43 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011184443.gz 48 309 Oct 11 2012
19:04:46 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011190446.gz 49 2729
Oct 09 2012 21:21:49 +00:00 /bootflash/tracelogs/IOSRP_R0-0.log.20011.20121009212149 50
116 Oct 08 2012 21:06:44 +00:00
/bootflash/tracelogs/binos_log_R0-0.log.20013.20121008210644
```

Note To avoid losing work you have completed, be sure to save your configuration occasionally as you proceed. Use the **copy running-config startup-config** command to save the configuration to NVRAM.

Verify Initial Configuration on Cisco 4000 Series ISRs

Enter the following commands at Cisco IOS-XE to verify the initial configuration on the router:

- **show version**—Displays the system hardware version; the installed software version; the names and sources of configuration files; the boot images; and the amount of installed DRAM, NVRAM, and flash memory.
- **show diag**—Lists and displays diagnostic information about the installed controllers, interface processors, and port adapters.
- **show interfaces**— Shows interfaces are operating correctly and that the interfaces and line protocol are in the correct state; either up or down.
- **show ip interface brief—** Displays a summary status of the interfaces configured for IP protocol.
- **show configuration—** Verifies that you have configured the correct hostname and password.
- **show platform—** Displays the software/rommon version, and so on.

When you have completed and verified the initial configuration, specific features and functions are ready to be configured. See the *Software Configuration Guide for the Cisco 4400 and Cisco 4300 Series ISRs.*

ROM Monitor Overview and Basic Procedures

The *ROM Monitor* is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a router. When you connect a terminal to the router that is in ROM Monitor mode, the ROM Monitor command-line interface (CLI) prompt is displayed.

During normal operation, users do not use ROM Monitor mode. ROM Monitor mode is used only in special circumstances, such as reinstalling the entire software set, resetting the router password, or specifying a configuration file to use at startup.

The *ROM Monitor software* is known by different names. It is sometimes called *ROMMON* because of the CLI prompt in ROM Monitor mode. It is also called the *boot software*, *boot image*, or *boot helper*. Although it is distributed with the routers that use the Cisco IOS XE software, the ROM Monitor software is a program that is separate from the Cisco IOS XE software. During normal startup, the ROM Monitor initializes the router, and then control passes to the Cisco IOS XE software. After the

Cisco IOS XE software takes over, the ROM Monitor is no longer in use. For more information, see the ROMMON Overview section of the *Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs*