Basic Software Configuration Using the Cisco IOS Command-Line Interface

This document describes how to use the Cisco IOS command-line interface (CLI) to perform a basic software configuration for your router.

Contents

Platforms Supported by This Document

Use this document with the following platforms:

- Cisco 1800 series routers
- Cisco 2800 series routers
- Cisco 3800 series routers

CISCO SYSTEMS

Prerequisites for Basic Software Configuration Using the Cisco IOS CLI

Follow the instructions in the quick start guide that shipped with your router to install the chassis, connect cables, and power up the router.

Timesaver Before powering up the router, disconnect all WAN cables from the router to keep it from trying to run the AutoInstall process. The router may try to run AutoInstall if you power it on while there is a WAN connection on both ends and the router does not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote TCP/IP host.

Restrictions for Basic Software Configuration Using the Cisco IOS CLI

If Cisco Router and Security Device Manager (SDM) is installed on your router, we recommend that you use Cisco SDM instead of the Cisco IOS CLI to perform the initial software configuration. To access SDM, see the quick start guide that shipped with your router.

How to Perform a Basic Software Configuration Using the Cisco IOS CLI

This section contains the following procedures:

Configuring the Router 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."

Do not expect capitalization and lowercasing to be preserved in the hostname. Uppercase and lowercase characters are treated as identical by many Internet software applications. It may seem appropriate to capitalize a name as you would ordinarily do, but conventions dictate that computer names appear in all lowercase characters. For more information, see RFC 1178, *Choosing a Name for Your Computer*.

The name must also follow the rules for Advanced Research Projects Agency Network (ARPANET) hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. For more information, see RFC 1035, *Domain Names—Implementation and Specification*.

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.
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.

What to Do Next

Proceed to the "Configuring the Enable and Enable Secret Passwords" section on page 4.

Configuring 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 software or if you boot older boot ROMs that do not recognize the **enable secret** command.

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.

	Command or Action	Purpose
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 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.

Troubleshooting Tips

If you forget the password that you configured, or if you cannot access privileged EXEC (enable) mode, see the Password Recovery Procedures for your router, available at http://www.cisco.com/warp/public/474.

What to Do Next

If you want to set the console interface privileged EXEC timeout to a value other than 10 minutes (the default), proceed to the "Configuring the Console Idle Privileged EXEC Timeout" section on page 5.

If you do not wish to change the privildged EXEC timeout, proceed to the "Specifying a Default Route or Gateway of Last Resort" section on page 9.

Configuring 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.
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 10 seconds:

```
line console
 exec-timeout 0 10
```

What to Do Next

Proceed to the "Configuring Fast Ethernet and Gigabit Ethernet Interfaces" section on page 7.

Configuring Fast Ethernet and 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 Fast Ethernet and Gigabit Ethernet interfaces, see the "Configuring LAN Interfaces" chapter of the *Cisco IOS Interface and Hardware Component Configuration Guide*.

For information on interface numbering, see the quick start guide that shipped with your router.

> **Note** Cisco 1841 and Cisco 2801 routers have a hardware limitation on the Fast Ethernet ports FE0/0 and FE0/1. In half-duplex mode, when traffic reaches or exceeds 100% capacity (equal to or greater than 5 Mbps in each direction), the interface will experience excessive collisions and reset once per second. To avoid this problem, traffic must be limited to less than 100% of capacity.

SUMMARY STEPS

1. **enable**

2. **show ip interface brief**

3. **configure terminal**

4. **interface** {**fastethernet** | **gigabitethernet**} **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: Fast Ethernet or Gigabit Ethernet.
Step 3	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 4	**interface** {**fastethernet** | **gigabitethernet**} **0/**_port_ **Example:** Router(config)# interface fastethernet 0/1 **Example:** Router(config)# interface gigabitethernet 0/0	Specifies the Ethernet interface and enters interface configuration mode. **Note** For information on interface numbering, see the quick start guide that shipped with your router.
Step 5	**description** _string_ **Example:** Router(config-if)# description FE 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.

Examples

Configuring the Fast Ethernet Interface: Example

```
!
interface FastEthernet0/0
 description FE 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
FastEthernet0/0        172.16.3.3      YES NVRAM  up                      up
FastEthernet0/1        unassigned      YES NVRAM  administratively down   down
Router#
```

What to Do Next

Proceed to the .

Specifying 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* tech note.

The Cisco IOS software uses the gateway (router) of 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.

For comprehensive configuration information about IP routing and IP routing protocols, see the *Cisco IOS IP Configuration Guide*. In particular, see the "Configuring IP Addressing" chapter and all "Part 2: IP Routing Protocols" chapters.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **ip routing**

4. **ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**]

5. **ip default-network** *network-number*
   or
   ip route *dest-prefix mask next-hop-ip-address*

6. **end**

7. **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.
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.

Examples

Specifying a Default Route: Example

```
!
ip routing
!
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: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is 172.28.99.2 to network 192.168.24.0

     172.24.0.0 255.255.255.0 is subnetted, 1 subnets
C       172.24.192.0 is directly connected, FastEthernet0
S       172.24.0.0 255.255.0.0 [1/0] via 172.28.99.0
S*   192.168.24.0 [1/0] via 172.28.99.2
     172.16.0.0 255.255.255.0 is subnetted, 1 subnets
C       172.16.99.0 is directly connected, FastEthernet1
Router#
```

What to Do Next

Proceed to the "Configuring Virtual Terminal Lines for Remote Console Access" section on page 11.

Configuring 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.

The router has five virtual terminal lines by default. However, you can create additional virtual terminal lines as described in the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide*.

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

If you want to secure the vty lines with an access list, see "Part 3: Traffic Filtering and Firewalls" in the *Cisco IOS Security Configuration Guide*.

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.
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.

	Command or Action	Purpose

Step 7	`show running-config`
	
	Example:
	`Router# show running-config`
		Displays the running configuration file.
		
		• Verify that you 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.

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 "Part 3: Traffic Filtering and Firewalls" in the *Cisco IOS Security Configuration Guide*.

• To continue with the basic software configuration for your router, proceed to the "Configuring the Auxiliary Line" section on page 13.

Configuring 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, tech note

http://www.cisco.com/warp/public/471/mod-aux-exec.html

Configuring Dialout Using a Modem on the AUX Port, sample configuration

http://www.cisco.com/warp/public/471/mod-aux-dialout.html

Connecting a SLIP/PPP Device to a Router's AUX Port, tech note

http://www.cisco.com/warp/public/701/6.html

Configuring AUX-to-AUX Port Async Backup with Dialer Watch, sample configuration

http://www.cisco.com/warp/public/471/aux-aux-watch.html

Modem-Router Connection Guide, tech note

http://www.cisco.com/warp/public/76/9.html

SUMMARY STEPS

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

What to Do Next

Proceed to the .

Verifying Network Connectivity

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

Prerequisites

- Complete all previous configuration tasks in this document.
- 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 basic 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
```

What to Do Next

Proceed to the "Saving Your Router Configuration" section on page 16.

Saving Your Router 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.

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.

What to Do Next

Proceed to the "Saving Backup Copies of Your Configuration and System Image" section on page 16.

Saving Backup Copies of Your 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 software system image file on a server.

For more detailed information, see the "Managing Configuration Files" chapter and the "Loading and Maintaining System Images" chapter of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **copy nvram:startup-config {ftp: | rcp: | tftp:}**
3. **show flash:**
4. **copy flash: {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 flash:`
	
	Example:
	`Router# show flash:`
		Displays the layout and contents of a flash memory file system.
		
		• Learn the name of the system image file.

Step 4	`copy flash: {ftp: | rcp: | tftp:}`
	
	Example:
	`Router# copy flash: 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.

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 flash:** command in privileged EXEC to learn the name of the system image file and the use of the **copy flash: tftp:** privileged EXEC command to copy the system image (c3640-2is-mz) to a TFTP server. The router uses the default username and password.

```
Router# show flash:

System flash directory:
File Length Name/status
1 4137888 c3640-c2is-mz
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\

Router# copy flash: tftp:

IP address of remote host [255.255.255.255]? 172.16.13.110
filename to write on tftp host? c3600-c2is-mz
writing c3640-c2is-mz !!!!...
successful ftp write.
```

Where to Go Next

- When you complete the basic software configuration, consider implementing routing protocols or access lists and other security-improving methods to protect your router. See the documents listed in the "Related Documents—Additional Configuration" section on page 19.

- To configure features on your router, see Finding Feature Documentation.

Additional References

The following sections provide references related to basic software configuration using the Cisco IOS CLI.

Related Documents—Basic Software Configuration

Topic	Related Document Title or Link
Chassis installation, cable connections, power-up procedures, and interface numbering	Quick start guide for your router
Cisco Security Device Manager (SDM)	http://www.cisco.com/go/sdm
Guidelines for assigning the router hostname	RFC 1035, *Domain Names—Implementation and Specification* RFC 1178, *Choosing a Name for Your Computer*
Access lists, passwords, and privileges	*Cisco IOS Security Configuration Guide*
Passwords and password encryption	*Cisco IOS Password Encryption Facts* tech note
Password recovery procedures for Cisco products	Password Recovery Procedures
Configuring the console line, managing configuration files, and loading and maintaining system images	*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*
Configuring interfaces	*Cisco IOS Interface and Hardware Component Configuration Guide*
IP routing and IP routing protocols	*Cisco IOS IP Configuration Guide*
Configuring default routes or a gateway of last resort	*Configuring a Gateway of Last Resort Using IP Commands* tech note

Topic	Related Document Title or Link
Configuring virtual terminal lines	*Cisco IOS Terminal Services Configuration Guide*
Configuring the auxiliary (AUX) port	*Configuring a Modem on the AUX Port for EXEC Dialin Connectivity*, tech note
	Configuring Dialout Using a Modem on the AUX Port, sample configuration
	Connecting a SLIP/PPP Device to a Router's AUX Port, tech note
	Configuring AUX-to-AUX Port Async Backup with Dialer Watch, sample configuration
	Modem-Router Connection Guide, tech note

Related Documents—Additional Configuration

Topic	Related Document Title or Link
Cisco configuration settings that network administrators should consider changing on their routers, especially on their border routers, to improve security	*Improving Security on Cisco Routers* tech note
	Note To view this document, you must have an account on Cisco.com. 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 that appear.
IP routing and IP routing protocols	*Cisco IOS IP Configuration Guide*
Access lists	*Cisco IOS Security Configuration Guide*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Basic Software Configuration Using the Cisco IOS Command-Line Interface