Overview

Introduction

The Cisco Catalyst IR8340 Rugged Series Router is Cisco's first industrial-grade fully integrated routing and switching platform. IR8340 is designed to provide outstanding flexibility and adaptability to address the latest needs of the network evolution.

Note The terms *IR8340* and *router* are used throughout this document in text and CLI examples to refer to the Cisco Catalyst IR8340 Rugged Series Router, unless otherwise noted.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

The IR8340 Router features 2 Pluggable Interface Module (PIM) slots, 2 single-wide IRM-NIM slots, 1 timing module slot, plus 12 onboard LAN ports and 2 WAN ports, and supports the following:

- 150W/250W PSU, Low Voltage DC and High Voltage AC/DC options
- Timing and SyncE support–IRIG-B (Analog & Digital), GNSS, and PTP

Note For more information about timing related configuration, see *Timing and Synchronization Configuration Guide, Cisco IOS XE 17 (Cisco Catalyst IR8340 Rugged Series Router)*.

- LTE PIM modules
- Network Interface Modules (NIMs)
- mSATA module
- 2 x 1G Combo WAN ports
- 4 x 1G Copper LAN Ports
- 4 x 1G Combo LAN ports
- 4 x 1G SFP LAN Ports
- PoE/PoE+/UPoE (up to 120w) support on LAN port 1-4
- 2 x IN and 1 x OUT Alarm ports (RJ45)

Accessing the CLI Using a Router Console

Cisco IR8340 routers have an RJ45 RS232 serial console port located on the router front panel. The default baud rate is 9600. You can use an RJ45 Roll Over console cable that is available in the market.

On a device fresh from the factory, you are greeted with a System Configuration Dialog. If the router was ordered for the use of Cisco PnP connect services, in the case of centralized provisioning, the router skips the initial dialog. The following is an example, and names and IP addresses are shown as examples.

Note Autoinstall will terminate if any input is detected on console.

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

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

WARNING: ** NOTICE ** This is the final IOS XE release to provide support for the H.323
protocol. Consider switching to SIP for multimedia applications before upgrading to 17.7.1.
*Jan 27 23:51:55.579: %TAMPER_ALARM-0-TAMPER_ALARM_ASSERT: Tamper alarm slot (Tamper alarm
 slot 2) asserted

*Jan 27 23:51:55.579: %TAMPER_ALARM-0-TAMPER_ALARM_ASSERT: Tamper alarm slot (Tamper alarm
 slot 3) asserted

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0,GigabitEthernet0/0/1

Autoinstall trying DHCPv4 on GigabitEthernet0/0/0,GigabitEthernet0/0/1

AUTO IP is starting!!!!

start Autoip process
```

```
Acquired IPv4 address 192.168.0.202 on Interface GigabitEthernet0/0/0
Received following DHCPv4 options:
dns-server-ip : 192.168.0.2
si-addr : 192.168.0.2
hostname : Router

stop Autoip process


Press RETURN to get started!


*Jan 27 23:53:08.903: %SYS-5-USERLOG_NOTICE: Message from tty0(user id: ): Device in day0
workflow, some non user-configured options may be enabled by default
*Jan 27 23:53:08.920: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

*Jan 27 23:53:08.921: %PNP-6-HTTP_CONNECTING: PnP Discovery trying to connect to PnP server
 (https://devicehelper.cisco.com.:443/pnp/HELLO)
*Jan 27 23:53:09.788: AUTOINSTALL: Obtain siaddr 192.168.0.2 (as config server)
*Jan 27 23:53:09.788: AUTOINSTALL: Setting hostname Router from DHCP reply
*Jan 27 23:53:10.899: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
administratively down
*Jan 27 23:53:11.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
 changed state to down
*Jan 27 23:53:29.880: %PNP-6-HTTP_CONNECTED: PnP Discovery connected to PnP server
(https://devicehelper.cisco.com.:443/pnp/HELLO)
*Jan 27 23:53:29.883: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(1/3) by (pid=656, pname=PnP Agent Discovery, time=23:53:29 UTC Wed Jan 27 2021)
*Jan 27 23:53:30.893: %PNP-6-PNP_SUDI_UPDATE: Device SUDI [PID:IR8340-K9,SN:FDO2523J7GF]
identified
*Jan 27 23:53:30.893: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (1/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:53:30.894: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:53:35.635: %PNP-6-PNP_RELOAD_INFO_STOPPED: Reload reason (PnP Service Info
2408-Unknown reason) stopped by (profile=pnp_cco_profile, host=devicehelper.cisco.com.,
port=443)
*Jan 27 23:53:56.755: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(1/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
*Jan 27 23:54:07.900: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (1/10) by (pid=656, pname=PnP Agent Discovery, time=23:54:07
 UTC Wed Jan 27 2021)
*Jan 27 23:54:07.900: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(1/3) by (pid=656, pname=PnP Agent Discovery, time=23:54:07 UTC Wed Jan 27 2021)
*Jan 27 23:54:07.901: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:54:07.909: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:54:13.907: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (4/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:13 UTC Wed Jan
27 2021)
*Jan 27 23:54:13.907: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (5/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:13 UTC Wed Jan 27 2021)
*Jan 27 23:54:29.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (6/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:29 UTC Wed Jan
27 2021)
*Jan 27 23:54:29.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (7/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:29 UTC Wed Jan 27 2021)
```

```
*Jan 27 23:54:37.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (8/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:37 UTC Wed Jan
27 2021)
*Jan 27 23:54:37.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (9/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:37 UTC Wed Jan 27 2021)
*Jan 27 23:54:53.914: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (10/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:53 UTC Wed Jan
27 2021)
*Jan 27 23:55:20.100: %PNP-6-PNP_CCO_SERVER_IP_RESOLVED: CCO server (devicehelper.cisco.com.)
 resolved to ip (18.205.166.131) by (pid=656, pname=PnP Agent Discovery, time=23:55:20 UTC
 Wed Jan 27 2021)
*Jan 27 23:55:20.100: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(2/3) by (pid=656, pname=PnP Agent Discovery, time=23:55:20 UTC Wed Jan 27 2021)
*Jan 27 23:55:21.107: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (2/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:55:21.108: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:55:32.751: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(2/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:55:43.108: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (2/10) by (pid=656, pname=PnP Agent Discovery, time=23:55:43
 UTC Wed Jan 27 2021)
*Jan 27 23:55:43.108: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(2/3) by (pid=656, pname=PnP Agent Discovery, time=23:55:43 UTC Wed Jan 27 2021)
*Jan 27 23:55:43.109: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:55:43.113: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:56:55.316: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(3/3) by (pid=656, pname=PnP Agent Discovery, time=23:56:55 UTC Wed Jan 27 2021)
*Jan 27 23:56:56.323: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (3/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:56:56.324: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:57:09.810: AUTOINSTALL: script execution not successful for Gi0/0/0.
*Jan 27 23:57:10.829: %SYS-5-CONFIG_P: Configured programmatically by process DHCP Autoinstall
 from console as vty0
*Jan 27 23:58:10.003: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(3/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
*Jan 27 23:58:21.323: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (3/10) by (pid=656, pname=PnP Agent Discovery, time=23:58:21
 UTC Wed Jan 27 2021)
*Jan 27 23:58:21.323: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(3/3) by (pid=656, pname=PnP Agent Discovery, time=23:58:21 UTC Wed Jan 27 2021)
*Jan 27 23:58:21.324: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:58:21.327: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:59:34.507: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
```

```
*Jan 27 23:59:59.507: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (4/10) by (pid=656, pname=PnP Agent Discovery, time=23:59:59
 UTC Wed Jan 27 2021)
*Jan 27 23:59:59.508: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:59:59.511: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:01:12.715: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:22.715: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (5/10) by (pid=656, pname=PnP Agent Discovery, time=00:02:22
 UTC Thu Jan 28 2021)
*Jan 28 00:02:22.716: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:22.719: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Router>en
Router#sh ip in
*Jan 28 00:02:42.724: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as console
*Jan 28 00:02:42.724: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary
(/pnp-tech/pnp-tech-discovery-summary)... Please wait. Do not interrupt.t b
*Jan 28 00:02:42.877: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:42.924: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:43.394: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:43.494: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary
(/pnp-tech/pnp-tech-discovery-summary) saved successfully (elapsed time: 1 seconds).
*Jan 28 00:02:43.494: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config Wizard)
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.0.202 YES DHCP up up
GigabitEthernet0/0/1 unassigned YES unset administratively down down
WPAN0/1/0 unassigned YES unset up up
Router#
```

The device now has a basic configuration that you can build upon.

Using the Console Interface

Procedure

Step 1 Enter the following command:

```
Router > enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 3 To exit the console session, enter the **quit** command:

```
Router# quit
```

Initial Bootup Security

This section contains the following:

Enforce Changing Default Password

When the device is first booted after factory reset or fresh from the factory, the following prompt is received on the console:

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

In previous documentation, Cisco recommended using the **enable secret** command instead of the **enable password** command because this offers an improved encryption algorithm.

The initial dialog forces setting a new enable password, and also using the **enable secret** command instead. The following is an example:

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

Autoinstall trying DHCP on GigabitEthernet0/0/0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

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.
-------------------------------------------------
secret should be of minimum 10 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-------------------------------------------------
Enter enable secret: **********
Confirm enable secret: **********

The following configuration command script was created:

enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
!
end


[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...
[OK]
Use the enabled mode 'configure' command to modify this configuration.




Press RETURN to get started!
*Feb 12 00:14:14.305: %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to
```

```
administratively down
*Feb 12 00:14:14.308: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
administratively down
*Feb 12 00:14:15.306: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to down
Router>
*Feb 12 00:14:15.653: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: SLA-TrustPoint created succesfully
*Feb 12 00:14:15.657: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM[OK]
Router>
Router>en
Password:
*Feb 12 00:14:18.878: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
 file
*Feb 12 00:14:18.910: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
Router#sh run | inc sec
*Feb 12 00:14:26.299: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0ret
enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
Router#
```

After the enable secret is prompted during the first login, and the admin enters a password, the admin entered password will be always masked. If the admin enters a weak password, they will be prompted again to enter strong password (i.e. the standard mix of upper/lower case characters, special characters, numbers etc.). The prompting will continue until the admin enters a strong password. The admin will be prompted to enter the strong secret password twice for confirming that admin is sure that it is the secret that they want to configure.

Telnet and HTTP

When the device is first booted after factory reset or fresh from the factory, by default the following takes place:

- Disable telnet
- Disable http server. HTTP client works.
- Enable SSH
- Enable https server

Examples

From a freshly booted device, below configurations for HTTPS and SSH are enabled.

```
ip http server
ip http authentication local
ip http secure-server
.
.

line vty 0 4
login
transport input ssh
line vty 5 14
login
transport input ssh
```

To enable Telnet, use the **line vty** command.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#line vty 0
R1(config-line)#password Pass123
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 40
R1(config-line)#motd-banner
R1(config-line)#exit
R1(config)#
R1(config)#enable password Password
R1(config)#exit
```

To test the Telnet connectivity, from a client PC, type **telnet 192.168.10.1** and press **Enter**, then enter the telnet password. Execute the **enable** command and press **Enter**, then type the router password.

```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.10.1
Trying 192.168.10.1 …Open
User Access Verification
Password:
R1>enable
Password:
R1#
```

Now you are remotely connected to router R1 and you can execute all router commands through Telnet command line interface.

Accessing the CLI from a Remote Console

The remote console of the IR8340 can be accessed through Telnet or SSH. Telnet is disabled by default, and the more secure SSH should be used. For details on SSH access see the SSH chapter.

The following topics describe the procedure to access the CLI from a remote console:

Preparing to Connect to the Router Console

See the Cisco IOS-XE Device hardening guide at https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html for details.

Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

To access the router remotely using Telnet from a TCP/IP network, configure the router to support virtual terminal lines using the **line vty** global configuration command. Configure the virtual terminal lines to require users to log in and specify a password.

See the Cisco IOS Terminal Services Command Reference document for more information about the line **vty global** configuration command.

To prevent disabling login on a line, specify a password with the **password** command when you configure the **login** command.

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a line for AAA authentication when you configure a list with the login authentication command, you must also configure that list using the **aaa authentication login** global configuration command.

For more information about AAA services, see the Cisco IOS XE Security Configuration Guide: Secure Connectivity and the Cisco IOS Security Command Reference documents. For more information about the **login line-configuration** command, see the Cisco IOS Terminal Services Command Reference document.

In addition, before you make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about the requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the Cisco IOS Configuration Fundamentals Configuration Guide.

Setting Up the IR8340 to Run SSH

Follow the procedure given below to set up your device to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Router(config)# hostname your_hostname`	Configures a hostname and IP domain name for your device. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 3	**ip domain-name** *domain_name* **Example:** `Router(config)# ip domain-name your_domain_name`	Configures a host domain for your device.
Step 4	**crypto key generate rsa modulus** *size* **Example:** `Router(config)# crypto key generate rsa modulus 2048`	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 2048 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the device as an SSH server.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Using Telnet to Access a Console Interface

Procedure

Step 1 From your terminal or PC, enter one of the following commands:

- **connect host** [*port*] [*keyword*]
- **telnet host** [*port*] [*keyword*]

Here, *host* is the router hostname or IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

The following example shows how to use the **telnet** command to connect to a router named **router**:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

Step 2 Enter your login password:

```
User Access Verification
Password: mypassword
```

Note If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command:

```
Router> enable
```

Step 4 At the password prompt, enter your system password:

```
Password: enablepass
```

Step 5 When the **enable** password is accepted, the privileged EXEC mode prompt is displayed:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command.

```
Router# logout
```

CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

Information About CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that each other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access the router.

Changing the CLI Session Timeout

Procedure

Step 1 `configure terminal`

Enters global configuration mode

Step 2 `line console 0`

Step 3 `session-timeout` *`minutes`*

The value of *`minutes`* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *`minutes`* to disable session timeout.

Step 4 `show line console 0`
Verifies the value to which the session timeout has been set, which is shown as the value for `"Idle Session"`.

Locking a CLI Session

Before you begin

To configure a temporary password on a CLI session, use the **lock** command in EXEC mode. Before you can use the **lock** command, you need to configure the line using the **lockable** command. In this example the line is configured as **lockable**, and then the **lock** command is used and a temporary password is assigned.

Procedure

Step 1 `Router# configure terminal`

Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the **lock** command.

```
Router(config)# line console 0
```

Step 3

```
Router(config)# lockable
```

Enables the line to be locked.

Step 4

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

Step 5

```
Router# lock
```

The system prompts you for a password, which you must enter twice.

```
Password: <password>
Again: <password>
Locked
```

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.