

Overview

This document outlines the core characteristics and functional capabilities of the system to facilitate effective configuration and management.

- Cisco Catalyst IR8140 Heavy Duty Series routers, on page 1
- Access CLI using a router console, on page 2
- **Initial bootup security** , on page 4
- Remote console CLI access methods, on page 6
- CLI sessions, on page 9

Cisco Catalyst IR8140 Heavy Duty Series routers

A Cisco Catalyst IR8140 Heavy Duty Router (IR8140H) is a next-generation, modular, IP66/67-rated industrial router that:

- is designed for outdoor use,
- features four external module slots plus two onboard WAN ports, and
- is available in two models: IR8140H-P-K9 (supports Power over Ethernet) and IR8140H-K9 (does not support PoE).

Key points to consider

Consider these points before using this guide:

- The terms IR8140H , IR8100 , and router are used throughout this document in text and CLI examples to refer to the Cisco Catalyst IR8140 Heavy Duty Series Router, unless otherwise noted.
- The documentation set for this product strives to use bias-free language. For 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.

Supported modules

The IR8140H Series features four external module slots plus two onboard WAN ports and supports:

- 60W PSU,
- GNSS onboard transceiver,
- 900MHz WPAN – OFDM/FSK,
- 4G/LTE IRMH modules, mSATA module,
- 1x 1GbE SFP WAN and 1x 1GbE Cu WAN,
- PoE (15W) – Supported only on the IR8140H-P-K9 PID,
- 12VDC_OUT port (Only available when PoE is not in use),
- Battery Backup Units (BBUs) – Up to 3,
- 2x Alarm ports (Digital IO).

Access CLI using a router console

Cisco IR8140H routers have an RJ45 RS232 serial console port located on the CPU module. The default baud rate is 9600. You can use any RJ45 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.

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

Procedure

Step 1 Connect the RJ45 console cable to the router's RS232 serial console port on the CPU module.

Step 2 Open a terminal emulator on your computer and configure it to use 9600 baud rate.

Step 3 Power on the router and observe the console output. The System Configuration Dialog details are displayed as given in the example.

Example:

```
--- 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 17.6.1.
            *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 23:53:29.880: %PNP-6-HTTP_CONNECTED: PnP Discovery connected to PnP
server (https://devicehelper.cisco.com.:443/pnp/HELLO)
            *Jan 27 23:53:30.893: %PNP-6-PNP_SUDI_UPDATE: Device SUDI
[PID:IR8140H-P-K9,SN:FDO2438J8UN] identified
          *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#
```

Step 4 Press the **RETURN** key to get started and access the CLI prompt.

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

Access the router using the console interface

Use this task to access the router's console interface and enter privileged EXEC mode to manage and configure the device through the CLI.

Procedure

Step 1 Use the **enable** command to enable the router and enter privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 Enter your system password when prompted. Skip this step if the enable password has not been configured. Once your password is accepted, the privileged EXEC mode prompt is displayed.

Example:

```
Password: enablepass
```

Note 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 Use the **quit** command to exit the console session.

Example:

```
Router> quit
```

Initial bootup security

This reference provides guidance on enforcing default password changes and managing Telnet and HTTP access during initial device configuration.

- Enforce Changing Default Password
- Telnet and HTTP

Change the default password

When the router is first booted after a factory reset or when it is new, you will receive a prompt on the console to enter the initial configuration dialog. Cisco recommends using the enable secret command instead of the enable password command for improved encryption.

Procedure

Step 1 Enter your response to the initial configuration dialog prompt on the console. If you choose no, the router proceeds with auto-install attempts and then prompts you to set the enable secret password.

Example:

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

Step 2 Use the **enable secret** command to enter a new password when prompted to set the password.

Example:

```
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: **********
```

Note The initial dialog forces you to set a new enable password using the enable secret command. The password must be at least 10 characters, include upper and lower case letters, at least one digit, and must not contain the word "cisco". If a weak password is entered, you will be prompted again until a strong password is provided. You must enter the password twice for confirmation.

Step 3 Save the configuration and complete the setup process by selecting option 2 to save the configuration to NVRAM and exit.

Example:

```
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!
            Router> en
            Password:
            Router# sh run | inc sec
            enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
            Router#
```

Note After you save the configuration, you can access privileged EXEC mode using the new enable secret password. When you enter the password, it is masked, and the configuration will be encrypted and saved to NVRAM.

The router is now secured with a strong enable secret password, and the configuration is saved. You can proceed to further configure the router as needed.

Telnet and HTTP protocols

Telnet and HTTP protocols are remote access protocols that:

- have modified default boot configurations as of release 17.5.1,
- are automatically configured during factory reset or initial boot processes, and
- include changes to telnet, HTTP server, HTTP client, SSH, and HTTPS server settings.

Default configuration changes

For devices after a factory reset or when they are new from the factory, these events take place:

- Disable telnet.

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

Remote console CLI access methods

A remote console CLI access method is a network-based approach that:

- enables remote access to the IR8100H CLI via Telnet or SSH,
- provides Telnet functionality that is disabled by default for security reasons, and
- offers SSH as the preferred and more secure method for remote CLI access.

Router console connections

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

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.

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 .

Set up the IR8140H to run SSH

To set up your device to run SSH, follow this procedure.

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

Procedure

Step 1 Use the **enable** command to enable the router and enter the privileged EXEC mode.

Example:

```
Router> enable
```

Note Enter password if prompted.

Step 2 Use the **configure terminal** command to enter the global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 Use the **hostname** *hostname* command to configure a hostname for your device.

Example:

```
Router(config)# hostname your_hostname
```

Note You can follow this procedure only if you are configuring the device as an SSH server.

Step 4 Use the **ip domain-name** *domain_name* command to configure a host domain for your device.

Example:

```
Router(config)# ip domain-name your_domain_name
```

Step 5 Use the **crypto key generate rsa** command to enable the SSH server for local and remote authentication on the device and generate an RSA key pair.

Example:

```
Router(config)# crypto key generate rsa
```

Note You must follow this procedure only if you are configuring the device as an SSH server. Generating an RSA key pair for the device automatically enables SSH. A minimum modulus size of 1024 bits is recommended. 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.

Step 6 Use the **end** command to exit to privileged EXEC mode.

Example:

```
Router(config)# end
```

Step 7 Use the **show running-config** command to verify your entries.

Example:

```
Router# show running-config
```

Step 8 (Optional) Use the **copy running-config startup-config** command to save your entries in the configuration file.

Example:

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

Access a console interface using telnet

Use this task to access a device's console interface using Telnet for CLI management and configuration.

Procedure

Step 1 Use the **connect** *host* [*port*] [*keyword*] or **telnet** *host* [*port*] [*keyword*] command from your terminal or PC to connect to the router. 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.

Example:

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

Note For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

Step 2 Enter your login password at the prompt. If no password is configured, press Return.

Example:

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

Step 3 Use the **enable** command from user EXEC mode to enable the router and enter privileged EXEC mode.

Example:

```
Router> enable
```

Step 4 Enter your system password at the password prompt.

Example:

```
Password: enablepass
```

Step 5 The privileged EXEC mode prompt is displayed once the enable password is accepted.

Example:

```
Router#
```

Step 6 Enter the necessary commands to complete specific tasks using the CLI access in privileged EXEC mode.

Step 7 Use the **exit** or **logout** command to exit the Telnet session.

Example:

```
Router# logout
```

CLI sessions

A CLI session is a command-line interface connection that:

- enables user access to system configuration and management functions,
- provides mechanisms to control user access and protect system resources, and
- prevents conflicts during concurrent user interactions.

CLI session management features

CLI sessions include the following management features:

- **Inactivity timeout**: Can be configured and enforced to automatically end idle sessions.
- **Session locking**: Prevents two users from overwriting each other's changes.
- **Reserved capacity**: Spare capacity is reserved for CLI session access to ensure users can connect even when the system is under load.

Change CLI session timeout

Setting the CLI session timeout increases the security of a CLI session by automatically ending idle sessions after a specified period of inactivity.

Procedure

Step 1 Use the **configure terminal** command to enter the global configuration mode.

Example:

```
Router# configure terminal
```

Step 2 Use the **line console** *console-number* command to access the configuration mode for the console line of the router.

Example:

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

Step 3 Use the **session-timeout** [*minutes*] command to set the session timeout. The value of *minutes* sets the amount of time that the CLI waits before timing out. Specify a value of 0 for *minutes* to disable session timeout.

Example:

```
Router(config-line)# session-timeout 10
```

Step 4 Use the **show line console** *console-number* command to verify the value to which the session timeout has been set, which is shown as the value for idle session.

Example:

```
Router# show line console 0
```

Lock a CLI session

To configure a temporary password on a CLI session, use the lock command in EXEC mode. The line is first configured as lockable, and then the lock command is used to assign a temporary password.



Note Before you can use the lock command, you need to configure the line using the lockable command.

Procedure

Step 1 Use the **configure terminal** command to enter the global configuration mode.

Example:

```
Router# configure terminal
```

Step 2 Use the **line console** *line-number* command to enter the line upon which you want to be able to use the lock command.

Example:

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

Step 3 Use the **lockable** command to enable the line to be locked.

Example:

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

Step 4 Use the **exit** command to exit the configuration mode.

Example:

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

Step 5 Use the **lock** command to lock the CLI session. The system prompts you for a password, which you must enter twice.

Example:

```
Router# lock
Password: <password>
```

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