

Prerequisites

This section contains the following:

- Cisco Catalyst IR1800 Rugged Series routers, on page 1
- Initial bootup security and configuration guidelines, on page 2
- Accessing the CLI on Cisco IR1800 routers, on page 5
- Access the CLI via console port, on page 6
- Accessing the CLI from a remote console, on page 7
- CLI session management, on page 10

Cisco Catalyst IR1800 Rugged Series routers

Cisco Catalyst IR1800 Rugged Series Routers are modular industrial routers that:

- Features four base platforms with modularity for additional pluggable modules.
- Provides flexibility to add different interfaces to the base platform.
- Supports industrial-grade performance for harsh environments.

The series includes four base platforms:

- IR1821: Lite
- IR1831: Base B
- IR1833: Base M
- IR1835: Pro

Each platform supports pluggable modules, enabling customization for specific use cases.

It provides modular design with pluggable modules such as PIM, mSATA, GNSS, and Wi-Fi Interface Modules.

The table displays the features of the base platforms:

Features	IR1821	IR1831	IR1833	IR1835
Processor	600MHz	600MHz	600MHz	1200MHz
Memory	4GB	4GB	4GB	8GB

Features	IR1821	IR1831	IR1833	IR1835
PIM Slot(s)	1	2	2	2
WiFi Pluggable Module Slot	Yes	Yes	Yes	Yes
PoE	No	No	Yes	Yes
mSATA Pluggable Module	No	No	Yes	Yes
GNSS Pluggable Module	No	No	Yes	Yes
GPIO	No	No	No	Yes
Ignition Management	Yes	Yes	Yes	Yes
CAN Bus	Yes	Yes	Yes	Yes
Serial Interface	RS232 (1)	RS232 (2)	RS232 (2)	RS232 (1) RS232/RS485 (1)
Advanced Security	No	No	No	Yes, Cisco Umbrella Integration

Initial bootup security and configuration guidelines

This document outlines the initial security and configuration measures for a Cisco device during the first boot or after a factory reset.

When a Cisco device is first booted after a factory reset or new from the factory, these security measures and configurations are enforced:

- Enforce changing default password:

  In the initial configuration dialog, set a new enable password and enter the **enable secret** command for stronger encryption. Weak passwords are rejected until a strong password is entered, adhering to the standard mix of upper/lower case characters, special characters, and numbers.

- Password management:

  The **enable secret** command is recommended over the **enable secret** command due to its stronger encryption algorithm. The **service password-encryption** command can be used to encrypt passwords in the configuration file, but it is not designed to protect against sophisticated attacks.

- Telnet and HTTP configuration changes:

  Release 17.3.1 implements the following changes:

  - Telnet is disabled.
  - The HTTP server is disabled, but the HTTP client remains functional.

- SSH is enabled for secure access.
- The HTTPS server is enabled.

Configure initial bootup security on a Cisco router

To setup management information, security passwords, and network management settings, while also recognizing conditions that cause the dialog to be skipped, such as Cisco PnP centralized provisioning.

Follow the prompts to set up basic parameters such as hostname, passwords, and IP addresses.

Procedure

Step 1 Start the initial configuration dialog.

Example:

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

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

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 2 Set global parameters.

Enter the hostname and configure the enable secret password.

```
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: <your-host-name>

  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: <your-password>

  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: <your-password>
```

Step 3 Configure virtual terminal password.

Set a password to secure network access.

Example:

```
The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: <your-password>
Setup account for accessing HTTP server? [yes]: <return>
    Username  [admin]: <your-username>
```

```
    Password  [cisco]: <your-password>
    Password is UNENCRYPTED.
```

Step 4 Configure hostname and IP addresses.

Example:

Displays interface summary:

```
Current interface summary

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

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      NO  unset  up                    up
GigabitEthernet0/1/0   unassigned      YES unset  down                  down
GigabitEthernet0/1/1   unassigned      YES unset  down                  down
GigabitEthernet0/1/2   unassigned      YES unset  down                  down
GigabitEthernet0/1/3   unassigned      YES unset  up                    up
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  up                    up
```

Displays example names and IP addresses:

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 192.168.1.1
    Subnet mask for this interface [255.255.255.0] : <return>
    Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Would you like to configure DHCP? [yes/no]: yes
 Enter DHCP pool name: wDHCPool
 Enter DHCP network: 192.168.1.0
 Enter DHCP netmask: 255.255.255.0
 Enter Default router: 192.168.1.1

The following configuration command script was created:

hostname <your-hostname>
enable secret 9 $9$Z6fl74fvoEdMgU$XZYs8l4phbqpXsb48l9bzCng3u4Bc2kh1STsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
no snmp-server
!
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface Vlan1
no shutdown
ip address 192.168.1.1 255.255.255.0
```

```
no mop enabled
ip dhcp pool wDHCPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
end
```

Step 5 Save the configuration.

Example:

```
[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.
```

Step 6 Verify the configuration.

Example:

```
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

Step 7 Review the initial configuration dialog.

If you answer **no** to the initial configuration dialog:

Example:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
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: ********
  Confirm enable secret: ********
Would you like to terminate autoinstall? [yes]: yes

.
```

Accessing the CLI on Cisco IR1800 routers

There are two methods to access the router's CLI:

- Accessing the CLI using a router console
- Accessing the CLI from a remote console

Accessing the CLI using a router console

The Cisco IR1800 router has a micro-B USB console port located on the front panel of the chassis. This port only supports USB connectivity. The default baud rate for the console connection is 9600 bps.

For detailed steps, see *Access the CLI via console port*.

Accessing the CLI from a remote console

The CLI of the Cisco IR1800 routers can also be accessed remotely using Telnet or SSH. By default, Telnet is disabled, and the more secure SSH protocol is recommended for use.

For detailed steps, see *Access the CLI via remote console*.

Access the CLI via console port

The purpose of this task is to enable access to the CLI in privileged EXEC mode, allowing the you to execute necessary commands for device configuration and management.

Before you begin

- Install the required drivers from the manufacturer or download them from Silicon Labs or FTDI.
- The latest VCP drivers may not support macOS 10.14.x and beyond. For older macOS versions, use driver version 3.1.
- Follow the prompts to set up basic parameters such as hostname, passwords, and IP addresses. See *Configure initial bootup security on a Cisco router*. If the router is pre-configured for Cisco PnP services, the initial dialog may be skipped.

Procedure

Step 1 Enter the enable command.

Example:

```
Router > enable
```

Step 2 Enter the system password (if configured).

At the password prompt, type your system password.

Example:

```
Password: enablepass
```

Step 3 Once accepted, the privileged EXEC mode prompt is displayed.

Example:

```
Router#
```

You now have access to the CLI in privileged EXEC mode and can execute necessary commands.

Step 4 Exit the console session.

Example:

```
Router# quit
```

Accessing the CLI from a remote console

This topic provides an overview of accessing the IR1800 router's CLI remotely via Telnet or SSH. By following the outlined procedures, you can securely and effectively manage the router remotely.

There are two methods to access the router's CLI remotely:

- Telnet:

  An older protocol that transmits data in plaintext, making it less secure. Telnet is disabled by default on the Cisco IR1800 router.

- SSH (Secure Shell):

  A more secure protocol that encrypts data during transmission. SSH should be used for remote access whenever possible. For detailed SSH configuration instructions, refer to the SSH chapter.

Here are the necessary steps to establish a remote CLI session with the IR1800 router:

1. Prepare to connect to the router console.
2. Set up the router to run SSH.
3. Use Telnet to access a console interface.

Prepare to connect to the router console

To prepare the router console remotely using Telnet from a TCP/IP network:.

Before you begin

- Ensure the router has a valid hostname and an IP address configured.
- For SSH access, configure user authentication for local or remote access.
- Refer to the Cisco IOS-XE Device Hardening Guide for additional security configurations.

Procedure

Step 1 Configure the router to support virtual terminal lines.

Use the **line vty** global configuration command.

Step 2 Set up login requirements and specify a password.

Use the **password** and **login** commands.

Step 3 If using AAA, configure the `login authentication` command and ensure the AAA authentication list is properly set up.

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.

Step 4 Optionally, configure diagnostic and wait banners to provide status indicators for Telnet or SSH attempts.

Set up the router to run SSH

SSH provides secure remote access to network devices. This configuration enables encrypted communication and helps protect against unauthorized access attempts.

Note Ensure that you configure user authentication for local or remote access.

Follow these steps to set up the router to run SSH.

Procedure

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

Example:

```
Router> enable
```

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

Example:

```
Router# configure terminal
```

Step 3 Use the **hostname** *your_hostname* and **ip domain-name** *your_domain_name* commands to configure a hostname and domain name for the device.

Example:

```
Router(config)# hostname <your_hostname>
Router(config)# ip domain-name <your_domain_name>
```

Step 4 Use the **crypto key generate rsa** command to generate an RSA key pair to enable SSH.

Example:

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

Note Use a modulus size of at least 1024 bits for security.

Step 5 Use the **end** command to exit global configuration mode.

Example:

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

Step 6 Use the **show running-config** command to verify the configuration.

Example:

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

Step 7 (Optional) Use the **copy running-config startup-config** command to save the configuration.

Example:

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

The router is now configured to accept SSH connections. You can connect remotely using an SSH client with the configured hostname and the appropriate user credentials.

Use Telnet to access a console interface

To access the console interface using Telnet.

Before you begin

Since Telnet is disabled by default, enable it only if necessary, and understand its security limitations. Use Telnet for initial testing or in trusted network environments. For detailed steps, see Configuring Telnet

Procedure

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

Example:

```
connect host [port] [keyword]
```

```
telnet host [port] [keyword]
```

- **<host>**: Router's hostname or IP address.
- **[port]**: Port number (default is 23).

Example:

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 when prompted.

Example:

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

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

Step 3 Access the privileged EXEC mode.

Use the **enable** command and provide the system password.

Example:

```
Router> enable
```

```
Password: enablepass
```

Privileged EXEC mode prompt is displayed. You now have access to the CLI in privileged EXEC mode and can execute necessary commands.

```
Router#
```

Step 4 Exit the Telnet session.

Use the **exit** or **logout** command.

Example:

```
Router# logout
```

CLI session management

A CLI session is a management interface that allows configuration of inactivity timeouts. It provides session locking to prevent overwriting of changes by multiple users and reserves spare capacity to ensure CLI access even under high system load.

Two methods of CLI session management

- Change the CLI session timeout
- Lock a CLI session

Change the CLI session timeout

To manage a CLI session.

Procedure

Step 1 Enter global configuration mode

Example:

```
Router# configure terminal
```

Step 2 Specify the console line.

Example:

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

Step 3 Set the session timeout value in minutes.

Example:

```
Router(config)# session-timeout <minutes>
```

Use **0** to disable the timeout.

The **minutes** value determines the CLI duration. Increasing the CLI session timeout enhances session security.

Step 4 Verify the session timeout configuration.

Example:

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

Lock a CLI session

To lock a CLI session.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Router# configure terminal
```

Step 2 Specify the console line to be locked.

Example:

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

Step 3 Enable the line to be lockable.

Example:

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

Step 4 Exit the configuration mode:

Example:

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

Step 5 Lock the session and set a temporary password.

Example:

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