Overview

This section contains the following:

- Introduction, on page 1
- Accessing the CLI Using a Router Console, on page 2
- Initial Bootup Security, on page 5
- Accessing the CLI from a Remote Console , on page 7
- CLI Session Management, on page 10

Introduction

The Cisco Catalyst IR1800 Rugged Series Router is a modular industrial router. The IR1800 series has four Base platforms with additional Pluggable Modules that can be added. The Pluggable Modules provides the flexibility of adding different interfaces to the base platform.

The IR1800 ISR series features a Base Platform with modularity that includes:

- Pluggable Interface Module (PIM)
- mSATA Module (SSDM)
- GPS Module (GNSS)
- Wi-Fi Interface Module (WIM)

The IR1800 series consists of four base platforms. They are:

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

The following table shows details of the differences:

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

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.

Accessing the CLI Using a Router Console

Cisco IR1800 routers have console port with only USB support.

The console port is a micro-B USB connector which is located on the front panel of the chassis. The default baud rate is 9600.

If your laptop or PC warns you that you do not have the proper drivers to communicate with the router, you can obtain them from your computers manufacturer, or go here:

https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

http://www.ftdichip.com/Support/Documents/InstallGuides/Mac_OS_X_Installation_Guide.pdf

Note The latest VCP Drivers do not work with MAC OS 10.14.x and beyond. If you require OS X 10.4 support, please install version 3.1 of the VCP driver.

On a device fresh from the factory, you are greeted with a System Configuration Dialog where you respond to basic configuration questions. 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:

```
         --- 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 '[]'.


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>

  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.
  Configure SNMP Network Management? [no]: <return>

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
```

Note Names and IP addresses in this next section are shown as examples.

```
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


[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! <return>


*Jul 27 21:35:24.369: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-3211716068
 has been generated or imported by crypto-engine
*Jul 27 21:35:24.372: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 27 21:35:24.448: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new IOS PKI configuration
*Jul 27 21:35:24.532: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named
TP-self-signed-3211716068.server has been generated or imported by crypto-engine
hostname>
```

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 basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: router-1

  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: ********

  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: **********

The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: *********
  Configure SNMP Network Management? [yes]: no

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [yes]: no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[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
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

The following is an example of what happens if you answer **no** to the initial configuration dialog:

```
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
```

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

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

There has been a change in the telnet and http boot configuration as of release 17.3.1. When the device is first booted after factory reset or fresh from the factory, the following takes place:

- Disable telnet
- Disable HTTP server. HTTP client works.
- Enable SSH
- Enable HTTPS server

Accessing the CLI from a Remote Console

The remote console of the IR1800 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 Router 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. For more information, see Related Topics below.

Procedure

	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** *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 4	**ip domain-name** *domain_name* **Example:** `router(config)# ip domain-name your_domain_name`	Configures a host domain for your device.

	Command or Action	Purpose
Step 5	**crypto key generate rsa** **Example:** `router(config)# crypto key generate rsa`	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 1024 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.
Step 6	**end** **Example:** `router(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `router# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Using Telnet to Access a Console Interface

Before you begin

Telnet is considered a security risk, and is disabled by defualt. If you need to enable it, see Configuring Telnet

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
```