THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
CHAPTER 1

Introduction

The Cisco Catalyst IR1101 Rugged Series Router is a next generation modular industrial router which has a Base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform.

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 IR1101 also has an Expansion Module that adds key capabilities such as dual LTE Pluggables, mSATA SSD FRU, SFP, and Digital GPIO connections.

The IR1101 is the first IoT platform to run the Cisco IOS-XE operating system. IOS-XE is a Linux based OS that comes with many enhancements and more features compared to the classic IOS version.

The following figure shows the front panel of the IR1101 and highlights some of its capabilities:
Table 1: Front Panel Descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SFP GigE WAN Port (Combo port of #3 below)</td>
</tr>
<tr>
<td>2</td>
<td>Type A USB 2.0 Host Port</td>
</tr>
<tr>
<td>3</td>
<td>RJ45 GigE WAN Port (Combo port of #1 above)</td>
</tr>
<tr>
<td>4</td>
<td>Asynchronous Serial Port (DTE only)</td>
</tr>
<tr>
<td>5</td>
<td>RJ45 Fast Ethernet LAN Ports</td>
</tr>
<tr>
<td>6</td>
<td>Grounding Point (On side of device)</td>
</tr>
<tr>
<td>7</td>
<td>DC Power and Alarm Input</td>
</tr>
<tr>
<td>8</td>
<td>Type B Mini-USB Console Port</td>
</tr>
<tr>
<td>9</td>
<td>Reset Button</td>
</tr>
<tr>
<td>10</td>
<td>Pluggable Module Slot (ex. 4G/LTE module)</td>
</tr>
</tbody>
</table>

Cisco IRM-1100-SP Expansion Module

The Expansion Module comes in two types:

- IRM-1100-SPMI
• IRM-1100-SP

The following figure shows the front panel of the IRM-1100-SPMI and highlights some of its capabilities:

**Figure 2: IR-1100-SPMI Expansion Module Details**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | 4 GPIO + 1 Return (Digital I/O)  
**Note** Functionality is available on Cisco IOS-XE release 16.12.1 and above. |
| 2    | SFP Connector |
| 3    | Pluggable Module |
| 4    | mSATA SSD Slot |
| 5    | Digital I/O LEDs |

The IR-1100-SP Expansion Module is the same as the IR-1100-SPMI module, without the Digital I/O and mSATA components.

More Expansion Module information can be found in this chapter *Expansion Module, on page 311.*

Complete details on the IR1101 can be found in the *product data sheet.*

This section of the guide also includes:

• *Accessing the CLI Using a Router Console, on page 4*
Accessing the CLI Using a Router Console

Cisco IR1101 routers have console port with only USB support. The console cable (Cisco P/N CAB-CONSOLE-USB, 6ft long) is not included and must be ordered.

The console port is a USB 2.0 mini USB Type B 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

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 UNENCRIPTED.

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

Current interface summary

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

```bash
hostname <your-hostname>
enable secret 9 $9$26f174fvoEdMgU5XYZS14phbqpxab4819bzCng3u4Bc2kh1STsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
nosnmp-server
!
!interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
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

**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
```

### Accessing the CLI from a Remote Console

The remote console of the IR1101 can be accessed through Telnet or the more secure SSH. Details on telnet access follow in this chapter. 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 Using Telnet


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.

Using Telnet to Access a Console Interface

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.

**Note** If you are using an access server, specify a valid port number, such as `telnet 172.20.52.40 2004`, in addition to the hostname or IP address.

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

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>Router(config)# line console 0</code></td>
</tr>
<tr>
<td></td>
<td>Enter the line upon which you want to be able to use the <code>lock</code> command.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>Router(config)# lockable</code></td>
</tr>
<tr>
<td></td>
<td>Enables the line to be locked.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>Router(config)# exit</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>Router# lock</code></td>
</tr>
<tr>
<td></td>
<td>The system prompts you for a password, which you must enter twice.</td>
</tr>
<tr>
<td></td>
<td><code>Password: &lt;password&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>Again: &lt;password&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>Locked</code></td>
</tr>
</tbody>
</table>
Locking a CLI Session
Understanding Command Modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. Use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, show commands show important status information, and clear commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode:
mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

The following table describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

**Table 2: Accessing and Exiting Command Modes**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Log in.</td>
<td>Router&gt;</td>
<td>Use the <strong>logout</strong> command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode,</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the <strong>disable</strong> command.</td>
</tr>
<tr>
<td></td>
<td>use the <strong>enable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the <strong>exit</strong> or <strong>end</strong> command.</td>
</tr>
<tr>
<td></td>
<td>mode, use the <strong>configure terminal</strong> command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an <strong>interface</strong> command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the <strong>exit</strong> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To return to privileged EXEC mode, use the <strong>end</strong> command.</td>
</tr>
</tbody>
</table>
If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode.

If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI.

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
</table>
| Diagnostic   | The router boots up or accesses diagnostic mode in the following scenarios:  
• In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload.  
• A user-configured access policy is configured using the transport-map command that directs a user into diagnostic mode.  
• A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) is entered and the router is configured to go to diagnostic mode when the break signal is received. | Router(diag)# | If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI. |
| ROM monitor  | From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting. | rommon#> | To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded. |

## Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

The following table lists the keyboard shortcuts for entering and editing commands.
Table 3: Keyboard Shortcuts

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or the Left Arrow key†</td>
<td>Move the cursor back one character.</td>
</tr>
<tr>
<td>Ctrl-F or the Right Arrow key†</td>
<td>Move the cursor forward one character.</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Move the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Move the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Esc B</td>
<td>Move the cursor back one word.</td>
</tr>
<tr>
<td>Esc F</td>
<td>Move the cursor forward one word.</td>
</tr>
</tbody>
</table>

Using the no and default Forms of Commands

Almost every configuration command has a no form. In general, use the no form to disable a function. Use the command without the no keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the no ip routing command; to re-enable IP routing, use the ip routing command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the no form of a command does.

Many CLI commands also have a default form. By issuing the <command> default command-name, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function from a default form of the command when the default form performs a different function than the plain and no forms of the command. To see what default commands are available on your system, enter default ? in the appropriate command mode.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retying them, by using special abbreviated commands.

The following table lists the history substitution commands.

Table 4: History Substitution Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or the Up Arrow key†</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or the Down Arrow key†</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.</td>
</tr>
</tbody>
</table>
### Managing Configuration Files

The startup configuration file is stored in the `nvr:mem` file system and the running configuration files are stored in the `system:mem` file system. This configuration file storage setup is also used on several other Cisco router platforms.


As a matter of routine maintenance on any Cisco router, users should back up the startup configuration file by copying the startup configuration file from NVRAM to one of the router’s other file systems and, additionally, to a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file if the startup configuration file in NVRAM becomes unusable for any reason.

The `copy` command can be used to back up startup configuration files.

For more detailed information on managing configuration files, see the “Managing Configuration Files” section in the [Cisco IOS XE Configuration Fundamentals Configuration Guide](https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html).

### Saving Configuration Changes

Use the `copy running-config startup-config` command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

```
[OK]
Router#
```

This task saves the configuration to the NVRAM.

### Filtering Output from the show and more Commands

You can search and filter the output of `show` and `more` commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a `show` or `more` command followed by the “pipe” character ( `|` ); one of the keywords `begin`, `include`, or `exclude`; and a regular expression on which you want to search or filter (the expression is case sensitive):

```
Router# show run | begin 10G
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show history</td>
<td>While in EXEC mode, lists the last few commands you entered.</td>
</tr>
</tbody>
</table>

1 The arrow keys function only on ANSI-compatible terminals such as VT100s.
show command | {append | begin | exclude | include | redirect | section | tee} regular-expression

The output matches certain lines of information in the configuration file.

Example

In this example, a modifier of the show interface command (include protocol) is used to provide only the output lines in which the expression protocol is displayed:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down (disabled)
  0 unknown protocol drops
FastEthernet0/0/1 is down, line protocol is down (notconnect)
  0 unknown protocol drops
FastEthernet0/0/2 is down, line protocol is down (notconnect)
  0 unknown protocol drops
FastEthernet0/0/3 is down, line protocol is down (notconnect)
  0 unknown protocol drops
FastEthernet0/0/4 is down, line protocol is down (notconnect)
  0 unknown protocol drops
GigabitEthernet0/0/5 is up, line protocol is up (connected)
  0 unknown protocol drops
Cellular0/1/0 is up, line protocol is up
  0 unknown protocol drops
Cellular0/1/1 is administratively down, line protocol is down
  0 unknown protocol drops
Cellular0/3/0 is up, line protocol is up
  0 unknown protocol drops
Cellular0/3/1 is administratively down, line protocol is down
  0 unknown protocol drops
Async0/2/0 is up, line protocol is down
  0 unknown protocol drops
Vlan1 is up, line protocol is up , Autostate Enabled
  0 unknown protocol drops
Vlan172 is up, line protocol is down , Autostate Enabled
  0 unknown protocol drops
Vlan175 is down, line protocol is down , Autostate Enabled
  0 unknown protocol drops
IR1101#
```

Finding Support Information for Platforms and Cisco Software Images

The Cisco IOS XE software is packaged in feature sets consisting of software images that support specific platforms.


The group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see the https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-16/products-release-notes-list.html.
Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator is a tool that enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To use the navigator tool, an account on Cisco.com is not required.

Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>help</code></td>
<td>Provides a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td><code>abbreviated-command-entry?</code></td>
<td>Provides a list of commands that begin with a particular character string.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> There is no space between the command and the question mark.</td>
</tr>
<tr>
<td><code>abbreviated-command-entry&lt;Tab&gt;</code></td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Lists all the commands that are available for a particular command mode.</td>
</tr>
<tr>
<td><code>command ?</code></td>
<td>Lists the keywords or arguments that you must enter next on the command line.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> There is a space between the command and the question mark.</td>
</tr>
</tbody>
</table>

Finding Command Options: Example

This section provides information about how to display the syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering a part of a command followed by a space. The Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the `arap` command, you should type `arap ?`.

The <cr> symbol in command help output stands for carriage return. On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press Enter to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by
itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

The following table shows examples of using the question mark (**) to assist you in entering commands.

**Table 5: Finding Command Options**

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; <strong>enable</strong></td>
<td>Enter the <strong>enable</strong> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “ # ” from the “ &gt; ”, for example, <strong>Router&gt; Io Router#</strong></td>
</tr>
<tr>
<td><strong>Router# configure terminal</strong></td>
<td>Enter the <strong>configure terminal</strong> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to <strong>Router (config)#</strong></td>
</tr>
<tr>
<td><strong>Router(config)# interface GigabitEthernet ?</strong></td>
<td>Enter interface configuration mode by specifying the interface that you want to configure, using the <strong>interface GigabitEthernet</strong> global configuration command.</td>
</tr>
<tr>
<td><strong>Router(config)# interface GigabitEthernet 0/?</strong></td>
<td>Enter ? to display what you must enter next on the command line. When the &lt;cr&gt; symbol is displayed, you can press <strong>Enter</strong> to complete the command.</td>
</tr>
<tr>
<td><strong>Router (config)# interface GigabitEthernet 0/0/? . &lt;0-71&gt;</strong></td>
<td>You are in interface configuration mode when the prompt changes to <strong>Router(config-if)#</strong></td>
</tr>
</tbody>
</table>

Using Cisco IOS XE Software

Finding Command Options: Example
Enter `?` to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ?</td>
<td></td>
</tr>
<tr>
<td>Interface configuration commands:</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>ip config commands</td>
<td>Interface Internet Protocol config commands</td>
</tr>
<tr>
<td>keepalive config commands</td>
<td>Enable keepalive</td>
</tr>
<tr>
<td>lan-name config commands</td>
<td>LAN Name command</td>
</tr>
<tr>
<td>llc2 Interface Subcommands</td>
<td></td>
</tr>
<tr>
<td>load-interval config commands</td>
<td>Specify interval for load calculation for an interface</td>
</tr>
<tr>
<td>locaddr-priority config commands</td>
<td>Assign a priority group for an interface</td>
</tr>
<tr>
<td>logging config commands</td>
<td>Configure logging for interface</td>
</tr>
<tr>
<td>loopback config commands</td>
<td>Configure internal</td>
</tr>
<tr>
<td>loopback on an interface</td>
<td></td>
</tr>
<tr>
<td>mac-address MPOA interface configuration commands</td>
<td>Manually set interface</td>
</tr>
<tr>
<td>mls mls router sub/interface</td>
<td></td>
</tr>
<tr>
<td>mtu (MTU) configuration commands</td>
<td>Set the interface Maximum Transmission Unit</td>
</tr>
<tr>
<td>netbios access list config commands</td>
<td>Use a defined NETBIOS or enable name-caching</td>
</tr>
<tr>
<td>no name-caching Negate a command or set</td>
<td></td>
</tr>
<tr>
<td>its defaults config commands</td>
<td>Enable use of NRZI</td>
</tr>
<tr>
<td>nrzi-encoding config commands</td>
<td></td>
</tr>
<tr>
<td>ntp config commands</td>
<td>Configure NTP</td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td></td>
</tr>
</tbody>
</table>
Enter the command that you want to configure for the interface. This example uses the `ip` command.

Enter `?` to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ip ?</td>
<td>Enter the command that you want to configure for the interface. This example uses the <code>ip</code> command. Enter <code>?</code> to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td>
</tr>
<tr>
<td>Interface IP configuration subcommands:</td>
<td></td>
</tr>
<tr>
<td>access-group Specify access control for packets</td>
<td></td>
</tr>
<tr>
<td>accounting Enable IP accounting on this interface</td>
<td></td>
</tr>
<tr>
<td>address Set the IP address of an interface authentication authentication subcommands</td>
<td></td>
</tr>
<tr>
<td>broadcast-address Set the broadcast address of an interface</td>
<td></td>
</tr>
<tr>
<td>cgmp Enable/disable CGMP</td>
<td></td>
</tr>
<tr>
<td>directed-broadcast Enable forwarding of directed broadcasts</td>
<td></td>
</tr>
<tr>
<td>dvmrp DVMRP interface commands</td>
<td></td>
</tr>
<tr>
<td>hello-interval Configures IP-EIGRP hello interval</td>
<td></td>
</tr>
<tr>
<td>helper-address Specify a destination address for UDP broadcasts</td>
<td></td>
</tr>
<tr>
<td>hold-time Configures IP-EIGRP hold time</td>
<td></td>
</tr>
<tr>
<td>. . .</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address A.B.C.D</td>
<td>Enter the keyword or argument that you want to use. This example uses the <code>ip address</code> command. Enter <code>?</code> to display what you must enter next on the command line. In this example, you must enter an IP address or the <code>negotiated</code> keyword. A carriage return ((&lt;cr&gt;)) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</td>
</tr>
<tr>
<td>negotiated IP Address negotiated over PPP</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 172.16.0.1</td>
<td>Enter the keyword or argument that you want to use. This example uses the <code>ip address</code> command. Enter <code>?</code> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. (&lt;cr&gt;) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</td>
</tr>
<tr>
<td>A.B.C.D IP subnet mask</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 172.16.0.1</td>
<td>Enter the keyword or argument that you want to use. This example uses the <code>ip address</code> command. Enter <code>?</code> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. (&lt;cr&gt;) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
</tbody>
</table>
Using Cisco IOS XE Software

Using Software Advisor

Cisco maintains the Software Advisor tool. See Tools and Resources. Use the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router. You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

See the release notes for information about the following:

- Memory recommendations
- Open and resolved severity 1 and 2 caveats

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ? secondary secondary address &lt;cr&gt;</td>
<td>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter ? to display what you must enter next on the command line. In this example, you can enter the secondary keyword, or you can press Enter. &lt;cr&gt; is displayed. Press Enter to complete the command, or enter another keyword.</td>
</tr>
<tr>
<td>Router(config-if)# ip address 172.16.0.1 255.255.255.0</td>
<td>Press Enter to complete the command.</td>
</tr>
</tbody>
</table>

Using Cisco IOS XE Software

Using Software Advisor

Cisco maintains the Software Advisor tool. See Tools and Resources. Use the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router. You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

See the release notes for information about the following:

- Memory recommendations
- Open and resolved severity 1 and 2 caveats

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.
Basic Router CLI Configuration

This chapter contains the following sections:

- IR1101 Interface Naming, on page 23
- Basic Configuration, on page 24
- Configuring Global Parameters, on page 28
- Configuring the Gigabit Ethernet Interface, on page 28
- Support for sub-interface on GigabitEthernet0/0/0, on page 30
- Configuring a Loopback Interface, on page 30
- Enabling Cisco Discovery Protocol, on page 31
- Configuring Command-Line Access, on page 31
- Configuring Static Routes, on page 33
- Configuring Dynamic Routes, on page 35
- Modular QoS (MQC), on page 36
- Configuring the Serial Interface, on page 36

IR1101 Interface Naming

The supported hardware interfaces and their naming conventions are in the following table:

<table>
<thead>
<tr>
<th>Hardware Interface</th>
<th>Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet combo port</td>
<td>gigabitethernet 0/0/0</td>
</tr>
<tr>
<td>Gigabit Ethernet SFP port on Expansion Module</td>
<td>gigabitethernet 0/0/5</td>
</tr>
<tr>
<td>Fast Ethernet ports</td>
<td>fastethernet0/0/1-0/0/4</td>
</tr>
<tr>
<td>Cellular Interface</td>
<td>cellular 0/1/0 and cellular 0/1/1</td>
</tr>
<tr>
<td>Cellular Interface on Expansion Module</td>
<td>cellular 0/3/0 and 0/3/1</td>
</tr>
<tr>
<td>Asynchronous Serial Interface</td>
<td>async 0/2/0</td>
</tr>
<tr>
<td>USB</td>
<td>usbflash0:</td>
</tr>
<tr>
<td>mSATA</td>
<td>msata</td>
</tr>
</tbody>
</table>
### Hardware Interface | Naming Convention
---|---
IR1101 Base Unit Alarm input | alarm contact 0
GPIO on Expansion Module | alarm contact 1-4

## Basic Configuration

The basic configuration is a result of the entries you made during the initial configuration dialog. This means the router has at least one interface set with an IP address to be reachable, either through WebUI or to allow the PnP process to work. Use the `show running-config` command to view the initial configuration, as shown in the following example:

```
Router# show running-config
Building configuration...

Current configuration : 8079 bytes

! Last configuration change at 17:33:19 GMT Tue Jun 25 2019

! version 16.12
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core

! hostname IR1101
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
no aaa new-model
!
!
Basic Router CLI Configuration
Basic Configuration

revocation-check crl
!
crypto pki trustpoint TP-self-signed-756885843
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-756885843
revocation-check none
rsakeypair TP-self-signed-756885843
!
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886
32310E30 0C060355 040A1305 43697363 6F312030 1E060355
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31
3834375A 170D3338 30353330 31393438 34375A30 32310E30
43697363 6F312030 1E060355 04031317 43697363 6F204C69
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE
D697DF7F 28
quit
crypto pki certificate chain TP-self-signed-756885843
certificate self-signed 01
3082032E 30820216 A0030201 02020101 300D0609 2A864886
30312E30 2C060355 04031325 494F532D 53656C66 2D536967
69666963 6174652D 37353638 38353834 33301E17 0D313930
385A170D 33303031 30313030 30303030 5A303031 2E302C06
532D5365 6C662D53 69676E65 642D4365 72746966 69636174
38343330 82012230 0D06092A 864886F7 0D010101 05000382
82010100 D2F61742 3B651909 95856431 9BC2CCB7 D4B04861
8BF2ABD9 5C3A597D 2EE0112C ECA615AA D0297F9E 071B6B5D
2352EEC9 EE70742E 46EFBAFC A03744D8 A22E4DA3 AAF919CC
C04DA5B9 028DD3EC 992493A6 EA864ED6 354CB3F4 094D3EBF
E458712D 841A43CD 709D4D9E 72A9DE3E F935A688 59B6F278
7B97582A 64E511A6 D81735FF 117CE399 4C2A2973 F5FD407D
882E0749 ACE5BD44 32634790 3607ADEA 9F319343 4CA76B0D
E38119E2 8B34F7AC 090C0450 03166B42 8C7C9EA7 5132687F
889F02BB 02030100 01A35330 51300F06 03551D13 0101FF04
0603551D 23041830 16801405 77954127 36509205 7025CF4E
1D060355 1D0E0416 04140577 95412736 50920570 25CF4E84
06092A86 4886F70D 01010505 00038201 01004147 49C6A0A9
22955E06 AF192FA6 868D5556 959ACF05 398F3907 DFE3148B
DC23E8D7 A47DB4AE D6CB6665 BCAE7F39 24D010F0 DB8F0E70
1346D540 47BB7E89 2BB1BE4D 16990318 A4612CC5 C7CC9376
4D950D99 3CC0C65B 0A98859A 3B81E324 BAB34EDF 64CA8C38
F71F8D5E D3B7A962 3D0FDE44 012AC034 D0E7F75A DB1BF12A
A588DCDA 8272CE33 36ABC57A BFF52980 5FFC7C34 4D4307BB

F70D0101
04031317
33303533
0C060355
63656E73
05000382
17222EA1
9CAE6388
700A8BF7
104FDC5F
C0BD23CF
539BA42B
5D5D5FB8
DF5F4368
0101FF04
0E041604
86F70D01
49631C78
9093D3B1
5575B146
11BA9CD2
C71E3B49
C37C1E69
B623CDBD
0275156F

0B050030
43697363
30313934
040A1305
696E6720
010F0030
F1EFF64D
8A38E520
D8F256EE
EA2956AC
58BD7188
42C68BB7
8F27D191
95135E44
04030201
1449DC85
010B0500
240DA905
6C9E3D8B
8DFC66A8
55A9232C
1765308B
39F08678
230E3AFB
719BB2F0

F70D0101
6E65642D
35333130
03550403
652D3735
010F0030
DD6E0924
9B831332
0A7929A7
5307CAA3
65B59EE0
BCEB62A6
B1DE6A1C
E1F7BF6E
05300301
84B5D4A2
B5D4A2A3
56F5BD4D
0E2CFC12
5E7C3F73
7DF1A1F4
184DC796
CF23E2F5
AC0C0F18

05050030
43657274
30303530
1325494F
36383835
82010A02
4C3E6A51
021E61F4
3BDB3B17
192B5759
6B72469E
FD7C6B08
AD144548
B065CD4E
01FF301F
A3D53730
D537300D
4892AEE0
20BEEA05
25AB1783
C09C0051
47DDD9DD
6A4FDA14
AA783B9D

Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide
25


quit
!
license udi pid IR1101-K9 sn FCW222700KS
diagnostic bootup level minimal
!
spanning-tree extend system-id
memory free low-watermark processor 50357
file prompt quiet
!
username cisco privilege 15 password 0 cisco
username lab password 0 lab123
!
redundancy
!
controller Cellular 0/1/0
  no lte firmware auto-sim
  lte modem link-recovery disable
!
controller Cellular 0/3/0
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/0/0
  no ip address
  shutdown
!
interface FastEthernet0/0/1
  switchport access vlan 192
  switchport mode access
!
interface FastEthernet0/0/2
  switchport access vlan 172
  switchport mode access
!
interface FastEthernet0/0/3
  switchport access vlan 172
!
interface FastEthernet0/0/4
  switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
  ip address negotiated
  load-interval 30
  dialer in-band
  dialer idle-timeout 0
  dialer watch-group 1
  ipv6 enable
  pulse-time 1
  ip virtual-reassembly
!
interface Cellular0/1/1
  no ip address
  shutdown
!
interface Cellular0/3/0
  ip address negotiated
  dialer in-band
dialer idle-timeout 0
dialer watch-group 2
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/3/1
no ip address
shutdown
!
interface Vlan1
ip address 192.168.10.15 255.255.255.0
!
interface Vlan172
ip address 172.27.167.121 255.255.255.128
!
interface Vlan175
ip address 175.1.1.1 255.255.255.0
!
interface Async0/2/0
no ip address
encapsulation acada
!
ip default-gateway 172.27.167.1
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.27.167.1
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 253
ip route 8.8.4.0 255.255.255.0 Cellular0/3/0
ip route 171.70.0.0 255.255.0.0 172.27.167.1
ip route 192.167.121.0 255.255.255.128 Cellular0/1/0
ip route 192.168.193.0 255.255.255.0 Cellular0/3/0 253
!
ip access-list standard 1
  10 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer watch-list 2 ip 5.6.7.8 255.255.255.255
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server host 171.70.127.43 version 2c public
snmp-server host 172.27.167.220 version 2c public
snmp-server manager
!
control-plane
!
line con 0
  exec-timeout 0 0
  stopbits 1
  speed 115200
line 0/0/0
line 0/2/0
line vty 0 4
exec-timeout 0 0
password cisco
login
transport input none
!
end
IR1101#

Configuring Global Parameters

To configure global parameters for your router, follow these steps.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal  | Enters global configuration mode when using the console port. |
| Example:
Router> enable  | Use the following to connect to the router with a remote terminal:
Router# configure terminal
Router(config)#
telnet router-name or address
Login: login-id
Password: **********
Router> enable |
| **Step 2**
hostname name | Specifies the name for the router. |
| Example:
Router(config)# hostname Router |
| **Step 3**
enable password password | Specifies a password to prevent unauthorized access to the router. |
| Example:
Router(config)# enable password cr1ny5ho |
| **Note** | In this form of the command, password is not encrypted. To encrypt the password use enable secret password as noted in the previously mentioned Device Hardening Guide. |

Configuring the Gigabit Ethernet Interface

The default configuration for the Gigabit Ethernet Interface (G10/0/0) on the IR1101 is Layer 3 (L3). It is possible to configure the interface as a Layer 2 (L2) interface. The Gigabit Ethernet Interface on the IR1101 is a combo port, which means it is a RJ45+SFP connector.
The Expansion Module also has an SFP port. The Gigabit Ethernet Interface (GI0/0/5) on the IRM-1100-SPMI is Layer 2 (L2) only. This means you can assign this port to any vlan (switchport acc vlan #) and use the SVI interface. You cannot assign an ip address directly under this port.

The correct connector must be selected, refer to the Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide.

To manually define the Gigabit Ethernet interface, follow these steps, beginning from global configuration mode.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>interface GigabitEthernet</td>
<td>Enters the configuration mode for an interface on the router.</td>
</tr>
<tr>
<td>slot/bay/port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ip address ip-address mask</td>
<td>Sets the IP address and subnet mask for the specified interface. Use</td>
</tr>
<tr>
<td>Example:</td>
<td>this Step if you are configuring an IPv4 address.</td>
</tr>
<tr>
<td>Router(config-if)# ip</td>
<td></td>
</tr>
<tr>
<td>address 192.168.12.2 255.255.255.0</td>
<td>Sets the IPv6 address and prefix for the specified interface. Use this</td>
</tr>
<tr>
<td>Step 3</td>
<td>Step 2, if you are configuring an IPv6 address. IPv6 unicast-routing</td>
</tr>
<tr>
<td>ipv6 address ipv6-address/prefix</td>
<td>needs to be set-up as well, see further information in the IPv6 Addressing</td>
</tr>
<tr>
<td>Example:</td>
<td>and Basic Connectivity Configuration Guide located here:</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enables forwarding of IPv6 unicast data packets.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ipv6</td>
<td></td>
</tr>
<tr>
<td>unicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enables the interface and changes its state from administratively down</td>
</tr>
<tr>
<td>Example:</td>
<td>to administratively up.</td>
</tr>
<tr>
<td>Router(config-if)# no</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the configuration mode of interface and returns to the global</td>
</tr>
<tr>
<td>Example:</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Support for sub-interface on GigabitEthernet0/0/0

Cisco IOS-XE release 16.11.1 and above supports sub-interfaces and dot1q configuration on the g0/0/0 interface. For example:

```
Router(config) # interface g0/0/0 ?
<1-4294967295> GigabitEthernet interface number
```

```
Router(config-subif) # encapsulation ?
  dot1q       IEEE 802.1Q Virtual LAN
```

Configuring a Loopback Interface

**Before you begin**

The loopback interface acts as a placeholder for the static IP address and provides default routing information. To configure a loopback interface, follow these steps.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>interface</strong> type number</td>
<td>Enters configuration mode on the loopback interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface Loopback 0</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>(Option 1) <strong>ip address</strong> ip-address mask</td>
<td>Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the <strong>ipv6 address</strong> command described below.)</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ip address 10.108.1.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Option 2) <strong>ipv6 address</strong> ipv6-address/prefix</td>
<td>Sets the IPv6 address and prefix on the loopback interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ipv6 address 2001:db8::ffff:1/128</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>exit</strong></td>
<td>Exits configuration mode for the loopback interface and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Verifying Loopback Interface Configuration
Enter the `show interface loopback` command. You should see an output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.0.2.0/16
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Alternatively, use the `ping` command to verify the loopback interface, as shown in the following example:

```
Router# ping 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

### Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router. It may be disabled if needed for security purposes.

For more information on using CDP, see Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S.

### Configuring Command-Line Access

To configure parameters to control access to the router, follow these steps.

**Note**

Transport input must be set as explained in the previous Telnet and SSH sections of the guide.
## Configuring Command-Line Access

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters line configuration mode, and specifies the type of line.</td>
</tr>
<tr>
<td>line [aux</td>
<td>console</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies a unique password for the console terminal line.</td>
</tr>
<tr>
<td>password password</td>
<td>Example: Router(config-line)# password 5dr4Hepw3</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables password checking at terminal session login.</td>
</tr>
<tr>
<td>login</td>
<td>Example: Router(config-line)# login</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.</td>
</tr>
<tr>
<td>exec-timeout minutes [seconds]</td>
<td>Example: Router(config-line)# exec-timeout 5 30</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits line configuration mode to re-enter global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Example: Router(config-line)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies a virtual terminal for remote console access.</td>
</tr>
<tr>
<td>line [aux</td>
<td>console</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies a unique password for the virtual terminal line.</td>
</tr>
<tr>
<td>password password</td>
<td>Example: Router(config-line)# password aldf2ad1</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Enables password checking at the virtual terminal session login.</td>
</tr>
<tr>
<td>login</td>
<td>Example: Router(config-line)# login</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Exits line configuration mode, and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td>Example:</td>
</tr>
</tbody>
</table>
Example

The following configuration shows the command-line access commands. Note that transport input none is the default, but if SSH is enabled this must be set to ssh.

You do not have to input the commands marked default. These commands appear automatically in the configuration file that is generated when you use the `show running-config` command.

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Configuring Static Routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the <code>ipv6 route</code> command described below.)</td>
</tr>
<tr>
<td>(Option 1) <strong>ip route</strong> prefix mask `{ip-address</td>
<td>interface-type interface-number [ip-address]}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2</code></td>
<td></td>
</tr>
<tr>
<td>(Option 2) <strong>ipv6 route</strong> prefix/mask `{ipv6-address</td>
<td>interface-type interface-number [ipv6-address]}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
</tbody>
</table>

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Gigabit Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not have to enter the command marked `default`. This command appears automatically in the configuration file generated when you use the `running-config` command.

```plaintext
! ip classless (default)
ip route 2001:db8:2::/64 2001:db8:3::0
```

### Verifying Configuration

To verify that you have configured static routing correctly, enter the `show ip route` command (or `show ipv6 route` command) and look for static routes marked with the letter S.

When you use an IPv4 address, you should see verification output similar to the following:

```plaintext
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2
  i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
  ia - IS-IS inter area, * - candidate default, U - per-user static route
  o - ODR, P - periodic downloaded static route
Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
 C    10.108.1.0 is directly connected, Loopback0
 S*   0.0.0.0/0 is directly connected, FastEthernet0
```

When you use an IPv6 address, you should see verification output similar to the following:

```plaintext
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
      EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
      Destination
      NDr - Redirect, O - OSPF Intra, DI - OSPF Inter, OE1 - OSPF ext 1
      OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      is - LISP site, ld - LISP dyn-EID, a - Application

C   2001:DB8:3::/64 [0/0] via GigabitEthernet0/0/2, directly connected
 S  2001:DB8:2::/64 [1/0] via 2001:DB8:3::1
```
Configuring Dynamic Routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.


Configuring Routing Information Protocol

To configure the RIP on a router, follow these steps.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>router rip</code></td>
<td>Enters router configuration mode, and enables RIP on the router.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config) # router rip</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`version {1</td>
<td>2}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-router) # version 2</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>network ip-address</code></td>
<td>Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-router) # network 192.168.1.1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-router) # network 10.10.7.1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no auto-summary</code></td>
<td>Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-router) # no auto-summary</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Exits router configuration mode, and enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-router) # end</code></td>
<td></td>
</tr>
</tbody>
</table>

Example

Verifying Configuration
To verify that you have configured RIP correctly, enter the `show ip route` command and look for RIP routes marked with the letter R. You should see an output similar to the one shown in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       *I - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, p - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
 C      10.108.1.0 is directly connected, Loopback0
 R  3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0/0
```

### Configuring Enhanced Interior Gateway Routing Protocol

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the Interior Gateway Routing Protocol (IGRP) developed by Cisco. The convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP, and IGRP is now obsolete.

The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations.


### Modular QoS (MQC)

This section provides an overview of Modular QoS CLI (MQC), which is how all QoS features are configured on the IoT Integrated Services Router. MQC is a standardized approach to enabling QoS on Cisco routing and switching platforms.

Follow the procedures that are in the QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE 17 guide.

### Configuring the Serial Interface

This section describes configuring serial interface management.

The IR1101 supports asynchronous serial interface protocols used for SCADA, Raw Socket, or reverse Telnet. It has a single serial interface, designated async 0/2/0. The serial interface is DTE only.
Specifying an Asynchronous Serial Interface

To specify an asynchronous serial interface and enter interface configuration mode, use one of the following commands in global configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# interface async 0/2/0</td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

Specifying Asynchronous Serial Encapsulation

The asynchronous serial interfaces support the following serial encapsulation methods:

- Raw-TCP
- Raw-UDP
- SCADA
- Encapsulation Relay

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# encapsulation {raw-tcp</td>
<td>raw-udp</td>
</tr>
</tbody>
</table>

Encapsulation methods are set according to the type of protocol or application you configure in the Cisco IOS software.

The remaining encapsulation methods are defined in their respective books and chapters describing the protocols or applications.

Configuring the Serial Port

To configure the serial port perform the steps in the following example:

```
IR1101#sh run int async 0/2/0
Building configuration...
Current configuration : 62 bytes
!
interface Async0/2/0
no ip address
encapsulation raw-tcp
end
IR1101#show line
Tty Line Typ   Tx/Rx  A Modem Roty AccO AccI Uses Noise Overruns  Int
*     0    0 CTY              -    -      -    -    -     0      0    0/0      -
0/2/0   50 TTY   9600/9600  -    -      -    -    -     0      0     0/0      -
74    74 VTY              -    -      -    -    -     3      0     0/0      -
75    75 VTY              -    -      -    -    -     0      0     0/0      -
```
Configuring the Serial Port

Line(s) not in async mode -or- with no hardware support:

1-49, 51-73, 79-726
Introduction to the Web User Interface

The Web user interface (Web UI) provides network administrators with a single solution for provisioning, monitoring, and optimizing devices. After you complete the hardware installation, you need to setup the device with a configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured. This is referred to as the Day 0 interface.

A Day 0 configuration is defined as a device that is fresh out of the box with no startup-configuration. After the initial Day 0 configuration, the WebUI can be used for day to day configuration.

Advanced Mode is needed in order to set up Cellular WAN, including public or private APN. This should be provided by your SIM's service provider.

The pluggable interface is not hot swappable. If you wish to change a SIM, power off the router. Instructions can be found in the IR1101 Hardware Installation Guide.

Effective with IOS-XE Release 17.3.1, the Day 0 Web User Interface (WebUI) will be supported on the IR1101. Day 0 WebUI is supported only on LAN ports. These are FastEthernet ports 0/0/1 – 0/0/4 on the...
IR1101. Connect a PC to one of the LAN ports of the IR1101 and boot the router on Day 0. The PC should be configured with a static IP address of 192.168.1.2/255.255.255.0.

Once the router boots up in Day 0, the PC can connect to the 192.168.1.x network and can access WebUI using the IP address of 192.168.1.1 with any browser. After the configuration is applied through the WebUI, the router will display the message "Day 0 config done. Stopping autoinstall".

### Configuration Notes

The following are important notes when using the WebUI:

- The WebUI is not supported on the 1G port because this interface is dedicated to PnP. It is only supported on the 100M ports 1-4. See the figure below:

- Plug and Play (PNP) cannot be used if router is being used to configure using Day 0 WebUI as PNP will be aborted once the configuration is applied through Day 0 WebUI.

- Starting from release 17.1.2, an explicit write memory is not needed once the configuration is applied through the WebUI.

---

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WAN port (GigabitEthernet 0/0/0 to IOS-XE)</td>
</tr>
<tr>
<td>2</td>
<td>LAN ports 1-4 (0/0/1 – 0/0/4 to IOS-XE)</td>
</tr>
</tbody>
</table>
Configuring Your Computer to Connect to the Router

The following section provides guidance for configuring your computer to properly interface with the IR1101. You can access the application from a client web browser. Ensure that the following web client requirements are met:

- **Hardware**—A Mac (OS version 10.9.5) or Windows (OS version 10) laptop or desktop compatible with one of the following tested and supported browsers:
  - Google Chrome 59 or later
  - Mozilla Firefox 54 or later
  - Apple Safari 10 or later
  - Microsoft Edge browser

- **Display resolution**—We recommend that you set the screen resolution to 1280 x 800 or higher.

Configuring Basic Mode WebUI through the Browser

The following steps guide you through the process of using the browser on your PC/laptop to configure the WebUI.

**Step 1**
Open your browser and enter 192.168.1.1 in the address bar. The Login Screen appears. Enter the Username **webui** and the Password **cisco**. Then click **Log In**.

*Figure 3: Login Screen*

**Step 2**
The Welcome Screen appears. Select Advanced Mode or Basic Mode. Basic Mode allows for configuring Basic settings, LAN, and a Primary WAN. Advanced Mode allows you to configure an additional Backup WAN, AVC, as well as additional settings. For the purposes of this section, Basic Mode is used. Select **Basic Mode**.
Step 3  Click **Go To Account Creation Page**. The Create New Account Screen appears. Create a new Login Name and Password to access the WebUI.

**Figure 5: Create New Account Screen**

Step 4  Click **CREATE & LAUNCH WIZARD**. The Basic Settings Screen appears. Provide a Router Name (hostname), Domain Name, Time Zone and Date & Time Mode.
Step 5

Click **LAN SETTINGS**. The LAN Configuration Screen appears. Enter the `webui_dhcp` Pool Name, VLAN interface IP address, and select the interface that is connected to your laptop from the list of available interfaces.

**Figure 7: LAN Configuration Screen**

Step 6

Click **PRIMARY WAN SETTINGS**. The PRIMARY WAN SETTINGS Screen appears. Configure the WAN interface by selecting the WAN Type and Interface from the available options. Next enter your DNS IP address information and select Enable/Disable NAT.
Step 7  Click Day 0 Config Summary. The Review Summary Screen appears. Verify your entries before applying the configuration.

Step 8  (Optional) You can click on CLI Preview to see the Configuration that is being applied to the router. Close the CLI Preview and if you are ready, Click Submit.
Step 9  
After clicking on Submit, a dialog box will appear which informs you that the configuration has been applied successfully. The new WebUI ip address is also presented.

Step 10  
If you have web connectivity, the device will try to connect. It is recommended that you close the browser session and move to the newly configured WebUI ip address.
Configuring Advanced Mode WebUI through the Browser

The following steps guide you through the process of using the browser on your PC to configure the WebUI. Make sure your laptop is configured to obtain an IP address through DHCP, or assign an IP address `n.n.n.n` matching our default subnet.

**Note** Advanced Mode is needed in order to set up Cellular WAN, including public or private APN.

**Step 1** Open your browser and enter 192.168.1.1 in the address bar. The Login Screen appears. Enter the Username `webui` and the Password `cisco`. Then click **Log In.**
Step 2  The WELCOME screen appears. Select Advanced Mode or Basic Mode. Basic Mode allows for configuring Basic settings, LAN, and a Primary WAN. Advanced Mode allows you to configure an additional Backup WAN, AVC, as well as additional settings. For the purposes of this section, Advanced Mode is used.

Figure 14: WELCOME Screen

Step 3  Select Advanced Mode, then click Go To Account Creation Page. The Create New Account screen appears. Create a new Login Name and Password to access the WebUI.
Step 4  Click **CREATE & LAUNCH WIZARD** The LAN Configuration screen appears. Provide a Pool Name, Network IP Address, Subnet, Access VLAN, and Device IP Address. A list of available interfaces is shown to select from. Only FastEthernet interfaces may be used.

**Figure 16: LAN Configuration Screen**

Step 5  Click **PRIMARY WAN SETTINGS**. The WAN Configuration screen appears. Select the WAN Type and Interface from the pull-downs. Provide an APN (Access Point Name) from your LTE Service Provider, and then select the DNS and IP Address settings for your network.
Step 6  Click **BACKUP WAN SETTINGS**. The **BACKUP WAN Configuration** screen appears. Select the button to Enable or Disable a backup WAN.

Figure 18: BACKUP WAN Configuration

Step 7  Click **Day 0 Config Summary**. The **SUMMARY** screen appears. Verify your entries before applying the configuration.

Figure 19: Summary Screen
Step 8  (Optional) You can click on CLI Preview to see the Configuration that is being applied to the router. Close the CLI Preview, and if you are ready, click Submit.

Note  A CLI Preview example is found at the end of this section.

Step 9  After clicking on Submit, a dialog box will appear which informs you that the configuration has been applied successfully. The new WebUI ip address is also presented.

Figure 20: Submit Dialog Box

Example

The following is an example of a CLI Preview:

```bash
ip domain name cisco.com
clock timezone GMT -6 00
ntp server pool.ntp.org

username admin privilege 15 secret 0 Mjc1N0dsb2NrIQ==

hostname "IR1101"
interface vlan 1
ip address 10.1.1.1 255.255.255.0
no shutdown
vlan 1
interface FastEthernet0/0/1
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/2
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/3
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/4
switchport access vlan 1
```
switchport trunk native vlan 1
switchport mode access
no shutdown
ip dhcp pool 10Net-Pool
dns-server 10.1.1.1
network 10.1.1.0 255.255.255.0
import all
default-router 10.1.1.1
lease 0 2

ip dhcp excluded-address 10.1.1.1

ip dns server
ip dns view default
default dns forwarder
default dns forwarding
default domain lookup
default domain name-server
interface Cellular0/1/0
description primary_wan
ip address negotiated
dialer in-band
dialer-group 1
pulse-time 1
shutdown
no shutdown
ip nat outside
exit
dialer-list 1 protocol ip permit

controller Cellular 0/1/0
lte sim data-profile 2 attach-profile 2 slot 0

ip route 0.0.0.0 0.0.0.0 Cellular0/1/0

ip nat inside source list 197 interface Cellular0/1/0 overload
access-list 197 permit ip any any

WebUI Dashboard

After completing the Day 0 setup, the WebUI can now be used for day to day administration. The WebUI opens up to an easy to use dashboard.

---

Note

WebUI feature support may vary based on the license and platform type of your device.

The following figure shows the dashboard:
The following table provides an overview of the dashboard.

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>View dashlets that give you a snapshot of CPU and memory utilization and system information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Monitor your network on a daily basis and perform other ad hoc operations related to network device inventory and configuration management.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configure your device.</td>
</tr>
<tr>
<td>Administration</td>
<td>Specify system configuration settings and user administration settings.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Troubleshoot connectivity problems and packet loss using Ping and Traceroute, and monitor device health and performance using web server logs and syslogs.</td>
</tr>
</tbody>
</table>
CHAPTER 5

Configuring Secure Shell

This chapter contains the following sections:

- Information About Secure Shell, on page 53
- How to Configure Secure Shell, on page 55
- Information about Secure Copy, on page 59
- Additional References, on page 61

Information About Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the device for secure shell (SSH):

- For SSH to work, the switch needs an RSA public/private key pair.

- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.

- Configure a hostname and host domain for your device by using the hostname and ip domain-name commands in global configuration mode. Use the hostname and ip domain-name commands in global configuration mode.

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the IR1101 for secure shell.

- The router supports RSA authentication.

- SSH supports only the execution-shell application.

- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
Cisco highly recommends the 3DES encryption as it is stronger.


- This software release supports IP Security (IPSec).
- The IR1101 supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2, which Cisco recommends due to its better security.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

**SSH And Router Access**

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2). SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

**SSH Servers, Integrated Clients, and Supported Versions**

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

- The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization
SSH Configuration Guidelines

Follow these guidelines when configuring the device as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command.
- When generating the RSA key pair, the message `No hostname specified` might appear. If it does, you must configure an IP hostname by using the `hostname` global configuration command.
- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Related Tasks

Setting Up the IR1101 to Run SSH, on page 55

#unique_60

How to Configure Secure Shell

Setting Up the IR1101 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>hostname hostname</code></td>
<td>Configures a hostname and IP domain name for</td>
<td>Follow this procedure only if you are configuring the device as an SSH server.</td>
</tr>
<tr>
<td>Example:</td>
<td>your device.</td>
<td></td>
</tr>
<tr>
<td>IR1101(config)# hostname</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the SSH Server

Follow these steps to configure the SSH server:

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Note**

This procedure is only required if you are configuring the device as an SSH server.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip domain-name domain_name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>IR1101(config)# ip domain-name your_domain_name</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>crypto key generate rsa</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>IR1101(config)# crypto key generate rsa</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>IR1101(config)# end</code></td>
</tr>
</tbody>
</table>

**Purpose**

- Configures a host domain for your device.
- 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.
- Returns to privileged EXEC mode.
Configuring Secure Shell

**Monitoring the SSH Configuration and Status**

This table displays the SSH server configuration and status.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td>show ssh</td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

---

**Configuring Secure Shell**

**Step 3**

Configures the SSH control parameters:

- Specifying the timeout value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the device uses the default timeout values of the CLI-based sessions.

By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session timeout value returns to the default of 10 minutes.

- Specifying the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.

Repeat this step when configuring both parameters.

**Example:**

IR1101(config)# ip ssh timeout 90
ip ssh authentication-retries 2

**Step 4**

(Optional) Configures the virtual terminal line settings.

- Enters line configuration mode to configure the virtual terminal line settings. For the `line_number` and `ending_line_number` arguments, the range is from 0 to 15.

- Specifies that the device prevents non-SSH Telnet connections, limiting the device to only SSH connections.

**Example:**

IR1101(config)# line vty 1 10
IR1101(config)# transport input ssh

**Step 5**

Exits line configuration mode and returns to privileged EXEC mode.

**Example:**

IR1101(config-line)# end
## Configuring the Router for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The router then handles authentication and authorization. No accounting is available in this configuration.

Follow these steps to configure AAA to operate without a server by setting the router to implement AAA in local mode:

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa new-model</td>
<td>Enables AAA</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101(config)# aaa new-model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authentication login default local</td>
<td>Sets the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101(config)# aaa authentication login default local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authorization exec local</td>
<td>Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101(config-line)# aaa authorization exec local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authorization network local</td>
<td>Configures user AAA authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR1101(config-line)# aaa authorization network local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:** To secure the router for HTTP access by using AAA methods, you must configure the router with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the router for HTTP access by using AAA methods.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6 username name privilege level password encryption-type password</td>
<td>Enters the local database, and establishes a username-based authentication system.</td>
</tr>
<tr>
<td><strong>Example:</strong> IR1101(config-line)# username your_user_name privilege 1 password 7 secret567</td>
<td>Repeat this command for each user.</td>
</tr>
<tr>
<td>a. For name, specify the user ID as one word. Spaces and quotation marks are not allowed.</td>
<td></td>
</tr>
<tr>
<td>b. (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</td>
<td></td>
</tr>
<tr>
<td>c. For encryption-type, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.</td>
<td></td>
</tr>
<tr>
<td>d. For password, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.</td>
<td></td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Exits line configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> IR1101(config-line)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Information about Secure Copy

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provide a secure replacement for the Berkeley r-tools.

### Prerequisites for Secure Copy

The following are the prerequisites for configuring the device for secure shell (SSH):

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an RSA key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the `copy` command. An authorized administrator can also do this from a workstation.
Restrictions for Configuring Secure Copy

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.
- When using SCP, you cannot enter the password into the `copy` command. You must enter the password when prompted.

Configuring Secure Copy

To configure the Cisco IR1101 for Secure Copy (SCP) server-side functionality, perform the following steps.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
**Example:**  
```bash
Device> enable
```
| | | - Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode.  
**Example:**  
```bash
Device# configure terminal
```
| Step 3 | aaa new-model | Sets AAA authentication at login.  
**Example:**  
```bash
Device(config)# aaa new-model
```
| | | |
| Step 4 | aaa authentication login \{default \[list-name\] method\} [ method2... ] | Enables the AAA access control system.  
**Example:**  
```bash
Device(config)# aaa authentication login default group tacacs+
```
| Step 5 | username name \{privilege level\} password encryption-type encrypted-password | Establishes a username-based authentication system.  
**Note** You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.  
**Example:**  
```bash
Device(config)# username superuser privilege 2 password 0 superpassword
```
| Step 6 | ip scp server enable | Enables SCP server-side functionality.  
**Example:**  
```bash
Device(config)# ip scp server enable
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>show running-config</td>
<td>(Optional) Displays the SCP server-side functionality.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show</td>
<td></td>
</tr>
<tr>
<td></td>
<td>running-config</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>debug ip scp</td>
<td>(Optional) Troubleshoots SCP authentication problems.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip scp</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
IR1101# copy scp <somefile> your_username@remotehost:/<some/remote/directory>
```

**Additional References**

The following sections provide references related to the SSH feature.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
CHAPTER 6

New Features for Cisco IOS-XE 17.1.1

The following are the new features available on the IR1101 for IOS-XE release 17.1.1:

- Support for the X25 over TCP (XOT), on page 63
- Support for YANG Data Models (Call-home), on page 63
- Yang Data Model Support for Scada, on page 64
- Support for Model Driven support for GNMI Telemetry Dial-In , on page 64
- Option to Enable or Disable USB Access, on page 64
- Day 0 Web User Interface, on page 64

Support for the X25 over TCP (XOT)

X.25 is an ITU standard for packet switching Wide Area Network (WAN). This is used in the Telecommunication industry over serial interfaces that are replaced by IP Network. An X25 connection can be established by using a PAD connection similar to Telnet/SSH. The IR1101 router has only one asynchronous serial interface where features of X25 are not supported. However, we can communicate to the X25 edge devices using by using feature TCP over X25 (XOT). With XOT, we can directly establish a PAD connection to X25 edge devices. Also, we can assign default or customized profiles to the access-groups by changing various parameters of X25 packets.

For additional information about XOT for IOS-XE, see the following:
Wide-Area Networking Configuration Guide: X.25 and LAPB, Cisco IOS XE

Support for YANG Data Models (Call-home)

The YANG models supported for the call-home feature are similar to the earlier releases of Cisco-IOS-XE, and the same is supported on 17.1 release of IOS-XE on IR1101. The following references are available for earlier YANG models:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1651

For additional information about call-home for IOS-XE, see the following:
Software Activation Configuration Guide, Cisco IOS XE Release 3S
Yang Data Model Support for Scada

The Cisco IOS XE 17.1.1 introduces support for the Cisco IOS XE YANG model for the Scada System. Previous releases already provided YANG models in other areas.

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711

Support for Model Driven support for GNMI Telemetry Dial-In

Similar to YANG models, there is support on IOS-XE for open source models defined by Google and is referred as Google Network Management Interface (GNMI). Configurations of GNMI can be verified either with Secure or Insecure Mode.

- Secure Mode

Secure Mode establishes secure connection using OpenSSL certificates between client and server. It sends GNMI telemetry updates using open source gnmi_cli tool.

- Insecure Mode

Insecure Mode sends GNMI telemetry updates between client and server using open source pygnmi tool.

For additional information about GNMI Telemetry see the following reference:

Programmability Configuration Guide, Cisco IOS XE

Option to Enable or Disable USB Access

Day 0 Web User Interface
New Features for Cisco IOS-XE 17.2.1

- Native docker support, on page 65
- Yang Data Model Support for Raw Socket Transport, on page 66
- Digital IO for IOx container applications, on page 67
- L2 Sticky Secure MAC Addresses, on page 68
- Signed Application Support, on page 69

Native docker support

Native Docker Support has been added to the 17.2.1 release. This feature enables users to deploy the docker applications on the IR1101. The application lifecycle process is similar to the procedure in the Installing and Uninstalling Apps section. For docker applications, entry point configuration is required as part of the application configuration. Please refer to the following example for the entry point configuration.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# app-hosting appid app3
Router(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)# guest-ipaddress 192.168.0.7 netmask 255.255.255.0
Router(config-app-hosting-gateway0)# app-default-gateway 192.168.0.1 guest-interface 0
Router(config-app-hosting)# app-resource docker
Router(config-app-hosting-docker)# run-opts 1 "--entrypoint '/bin/sleep 10000'"
Router(config-app-hosting-docker)# end
Router#
```

The output for docker applications is shown in the following example:

```
Router# show app-hosting detail
App id : app1
Owner : iox
State : RUNNING
Application
Type : docker
Name : aarch64/busybox
Version : latest
Description :
Path : bootflash:busybox.tar
Activated profile name : custom
Resource reservation
Memory : 431 MB
Disk : 10 MB
CPU : 577 units
```
Yang Data Model Support for Raw Socket Transport

Release 17.2.1 adds support for additional Yang Data Models. These additional models include Raw Socket Transport.

Yang Data Models can be found here:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1721

There are two feature modules available for raw socket that belong to the main Cisco-IOS-XE-native model. They are:

- Cisco-IOS-XE-rawsocket.yang

This module contains a collection of YANG definitions for Raw Socket Transport Configuration commands. This module has the following corresponding Cli commands:

```
# encapsulation raw-tcp
# encapsulation raw-udp
# raw-socket packet-length <length>
# raw-socket packet-timer <timer>
# raw-socket special-char <value>
# raw-socket tcp server <port> <ip>
# raw-socket tcp idle-timeout <value>
# raw-socket tcp client <dest-ip> <dest-port>
# raw-socket tcp idle-timeout <timeout>
# raw-socket tcp tcp-session
```
This module contains a collection of YANG definitions for Raw Socket Transport operational data.

This module has the following corresponding CLI commands:

```
# show raw udp statistics
# show raw tcp statistics
# show raw tcp session
# show raw udp session
# show raw tcp session local
# show raw udp session local
```

The following is a list of the Dependent Modules:

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (any revision)
- cisco-semver

---

### Digital IO for IOx container applications

Release 17.2.1 provides support for IOx container applications to be able to access the digital IO. There is a new CLI that has been added to the alarm contact command.

```
Router(config)# alarm contact ?
<0-4> Alarm contact number (0: Alarm port, 1-4: Digital I/O)
attach-to-iox Enable Digital IO Ports access from IOX
```

Enabling the `attach-to-iox` command will provide complete control of all Digital IO ports to IOx. The ports will be exposed as four character devices `/dev/dio-[1-4]` to IOX applications. You can use read/write functions to get/set values of the Digital IO ports.

If you wish to update the mode, you can write the mode value to the character device file. This is accomplished by IOCTL calls to read/write the state, change mode, and read the true analog voltage of the port. Following this method, you can attach analog sensors to the IR1101. All ports are initially set to Input mode with voltage pulled up to 3.3V.

The following are examples of IOCTL calls:

Read Digital IO Port:

```
cat /dev/dio-1
```

Write to Digital IO Port:
L2 Sticky Secure MAC Addresses

This is a new feature for the IR1101, however, it been present in IOS-XE for some time.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- **protect**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

  **Note:** If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

- **restrict**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown**—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command, or you can manually re-enable it by entering the shutdown and no shut down interface configuration commands. This is the default mode.

- **shutdown vlan**—Use to set the security violation mode per-VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs

### Command Line Interface

Under switch interface, add port-security cli.

```plaintext
Router(config-if)#switchport port-security ?
   aging       Port-security aging commands
   mac-address Secure mac address
   maximum     Max secure addresses
   violation   Security violation mode
   <cr>        <cr>
Router(config-if)#switchport port-security mac-address sticky
```

### Signed Application Support

Cisco Signed applications are now supported on the IR1101. In order to install a signed application, signed verification has to be enabled on the device. Signed verification can be enabled by following the following instructions.

```plaintext
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#app-hosting signed-verification
Router(config)#
Router(config)#exit
```

After enabling the signed verification, follow the instructions in the Installing and Uninstalling Apps section under IOx Application Hosting in order to install the application.
Signed Application Support
New Features for Cisco IOS-XE 17.3.1

The following are the new features available on the IR1101 for IOS-XE release 17.3.1:

- Yang Support for IO Ports, on page 71
- Support for Security-Enhanced Linux (SELinux), on page 72
- Support Added for the P-LTEAP18-GL Modem PID, on page 74
- Initial Bootup Security Improvements, on page 74
- Initial Bootup Security Improvements, on page 76

Yang Support for IO Ports

This feature increases the compatibility between the Command Line Interface and the Yang Model. Cisco IOS-XE Yang Data Models are found here:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.3.1 release is found under 1731. The two modules for Digital IO are Cisco-IOS-XE-digital-io-oper and Cisco-IOS-XE-digitalio.

The following are relevant IOS-XE CLI commands available:

Show Commands

- show run
- show alarm
- show led

Configuration Commands

- alarm contact attach-to-iox
- no alarm contact attach-to-iox
- alarm contact 1 enable enable
- no alarm contact <1-4> enable
- alarm contact <1-4> application <wet | dry>
- no alarm contact <1-4> application
- alarm contact <1-4> description <alarm description>
- no alarm contact <1-4> description
- alarm contact <1-4> severity <critical | major | minor | none>
Support for Security-Enhanced Linux (SELinux)

Security-Enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. SELinux provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

SELinux enforces mandatory access control policies that confine user programs and system servers to the minimum amount of privilege they require to do their jobs. This reduces or eliminates the ability of these programs and daemons to cause harm when compromised (for example, via buffer overflows or mis-configurations). This confinement mechanism operates independently of the traditional Linux access control mechanisms.

There are no additional requirements or configuration steps required to enable or operate the SELinux feature. The solution is enabled/operational by default as part of the base IOS-XE software on supported platforms.

The following are enhanced show commands that have been defined for viewing SELinux related audit logs.

**show platform software audit all**

**show platform software audit summary**

**show platform software audit switch <1-8> | active | standby> <FRU identifier from a drop-down list>**

**Command Examples**

The following is a sample output of the `show software platform software audit summary` command:

```
Device# show platform software audit summary
-----------------------------------
AUDIT LOG ON switch 1
-----------------------------------
AVC Denial count: 58
-----------------------------------
```

The following is a sample output of the `show software platform software audit all` command:

```
Device# show platform software audit all
-----------------------------------
AUDIT LOG ON switch 1
-----------------------------------
----------- START -----------
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
```
The following is a sample output of the `show software platform software audit switch` command:

```
Device# show platform software audit switch active R0

--- START ---
```

```
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filter" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0
tclass=lnk_file permissive=1
```

```
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028
comm="mcp_trace_filter" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0
tclass=dir permissive=1
```

```
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028
comm="ls" path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0
tclass=dir permissive=1
```

```
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_server" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_server" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0
tclass=tcp_socket permissive=1
```

```
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_server" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438732.973:126): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0
tclass=tcp_socket permissive=1
```

```
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_server" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
```

(output omitted for brevity)
Syslog Message Reference

Facility-Severity-Mnemonic

• %SELINUX-3-MISMATCH

Severity-Meaning

• ERROR LEVEL Log

Message Explanation

• A resource access was made by the process for which a resource access policy is not defined. The operation was flagged but not denied.
• The operation continued successfully and was not disrupted. A system log has been generated about the missing policy for resource access by the process as denied operation.

Recommended Action

• Please contact CISCO TAC with the following relevant information as attachments:
  • The message exactly as it appears on the console or in the system log.
  • Output of "show tech-support" (text file)
  • Archive of Btrace files from the box using the following command ("request platform software trace archive target <URL>") For Example: Device# request platform software trace archive target flash:selinux_btrace_logs

Support Added for the P-LTEAP18-GL Modem PID

The P-LTEAP18-GL PID uses the Telit modem LM960 modem. Details about all of the IR1101 modems are found here:

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_01.html#con_1161147

Initial Bootup Security Improvements

This section contains the following:
Enforce Changing Default Password

Previous software versions allowed the user to bypass setting a new enable password. When the device was 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]:

Previous software versions allowed answering no and the device would drop to the Router> prompt with a blank enable password. At this point, the router could be configured and brought into service with a blank enable password.

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

Starting with 17.3.1, the initial dialog has been changed to force 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.

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 $9$emUzIshVXwJ1UaE$5nTzhgJ19STd2ZKzQcVJ0kEac9afjUNdCD7Jf37SY9qq
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

Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwJ1UaE$5nTzhgJ19STd2ZKzQcVJ0kEac9afjUNdCD7Jf37SY9qq
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$nTzhgi19STdZKzQc4VJ0kEaCqafjUNdCD72UF37SY9qq

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. 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

**Note:** This only applies to the IR1101, other IoT routers configuration remains the same.

Initial Bootup Security Improvements

This section contains the following:

Enforce Changing Default Password

Previous software versions allowed the user to bypass setting a new enable password. When the device was 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]:

Previous software versions allowed answering no and the device would drop to the **Router>** prompt with a blank enable password. At this point, the router could be configured and brought into service with a blank enable password.

In previous documentation, Cisco recommended using the **enable secret** command instead of the **enable password** command because this offers an improved encryption algorithm.
Starting with 17.3.1, the initial dialog has been changed to force 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 $9$emUzIshVXw1uAe5nTzhgi9STdZkQc4VJ0kEaCqafjUNdCD7UIf37SYqg
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 $9$emUzIshVXw1uAe5nTzhgi9STdZkQc4VJ0kEaCqafjUNdCD7UIf37SYqg
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:
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.
CHAPTER 9

New Features for Cisco IOS-XE 17.4.1

The following are the new features available on the IR1101 for IOS-XE release 17.4.1:

- Features for Cisco IOS-XE 17.4.1, on page 79
- Cyber Vision Support, on page 79
- Deployment of Cyber Vision Center (CVC) on IOS-XE platform, on page 79
- Installing CVC Sensor using LM GUI, on page 86

Features for Cisco IOS-XE 17.4.1

The following features are introduced for IoT Routing.

Cisco Cyber Vision Support feature is found further below in this chapter.


DSL capability by using a Small Form-factor Pluggable (SFP) network interface module is found here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/m_configuring.dsl.html

Cyber Vision Support

Cisco Cyber Vision Center (CVC) gives more visibility into Industrial IoT networks across Industrial Control Systems (ICS) with real-time monitoring of control and data networks. On IoT IOS-XE platforms beginning with release 17.4, integration of CVC is supported by deploying IOX Cyber Vision sensor. With this sensor deployed on IoT Routers, the platform can forward the traffic from IOX applications to Cyber Vision Center for real-time monitoring and we can forward any captured PCAP files to Vision center from IOX application.

Deployment of Cyber Vision Center (CVC) on IOS-XE platform

Step 1  Download Cisco supported Cyber Vision IOX application from the following location:
https://software.cisco.com/download/home/286325414/type/286325316/release/3.1.1?catid=268438162
Select Cisco Cyber Vision Sensor IOx Application 3.1.1 for IE3400 and IR1101.

**Step 2**
Install CVC version 3.1.1 on Virtual Machine or on any Hypervisor. The following location is the download link for different versions of CVC:

https://software.cisco.com/download/home/286325414/type

Release Notes for Cisco Cyber Vision Release 3.1.1:

**Step 3**
The CVC sensor requires two VirtualPort Group interfaces. One on the platform where one interface is used for IOX traffic, and the other for mirror traffic which is forwarded to physical, SVI or Tunnel interface which ERSPAN source. Refer to the following illustration:

*Figure 22: CVC over L3 interface*

**Step 4**
The CVC Sensor deployment can be installed from either the LMGUI or CLI.

---

**Example Configuration for ERSPAN over L3 configuration along with Virtual Port Groups:**

Physical and Virtual Port Configuration:

```bash
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
interface virtualportgroup 1
ip nat inside
ip address 169.254.0.1 255.255.255.252
interface gi0/0/0
ip address 101.0.0.151 255.255.255.0
ip nat outside
no shut
```

ERSPAN Configuration:

```bash
monitor session 1 type erspan-source
```
source interface Gi0/0/0
no shutdown
destination
erspan-id 1
mtu 1464
ip address 169.254.1.2
origin ip address 169.254.1.1

NAT Configuration with Access-list:

ip nat inside source list NAT_ACL interface Gi0/0/0 overload
ip access-list standard NAT_ACL
 10 permit 169.254.0.0 0.0.0.3

**CLI Installation**

To install the app through the CLI, copy the CVC sensor to bootflash, USB or mSATA. Then install the app using the app-hosting CLI, and provide the docker options before activating the app. For example:

Router(config-if)#iox
Router# app-hosting install app-id <app-id> package {bootflash://|usbflash0:|msata:}
app-hosting applid <app-id>
  app-vnic gateway0 virtualportgroup 0 guest-interface 0
  mtu.1464 ipaddress 169.254.1.2 netmask 255.255.255.252
  app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 169.254.0.2 netmask 255.255.255.252
  app-default-gateway 169.254.0.1 guest-interface 1
  app-resource docker
    run-opts 1 "-rm --tmpfs /tmp:rw,size=128m"
Router# app-hosting {activate|start|stop|deactivate|uninstall} app-id <app-id>

**LMGUI Installation**

Configure the following to reach the LMGUI:

iox
ip http server
ip http secure-server
ip http authentication local
Username cisco privilege 15 password cisco
Login URL: http://<Mgmt_IP>/iox/login

Additional details can be found in Installing CVC Sensor using LM GUI, on page 86

**Register the Router Details**

**Step 1**

Register the IOS-XE Router details on CVC by logging in and navigating to:

**Admin > Sensors > Install Sensor Manually**

Then click on Cisco IOX Application. Refer to the following:
Step 2  Provide the serial number of the Router. It should be an exact match from the output of `show inventory`, and then click on **Create Sensor**. Refer to the following:
Step 3  Generate the Provisioning file from CVC by clicking on Get Provisioning File. Refer to the following:

*Figure 25: Generate Provisioning File*

Step 4  Download the provisioning file to a local directory. The file comes as a zip file with a file name like the following:

**Example:**

`sbs-sensor-config-<S/N of Router>.zip`

Step 5  Import the Provisioning file to Router through the LM GUI. From the LM GUI Applications, navigate to:

**Applications > CVC App (Application Name) > Manage > App-DataDir**

Refer to the following:
Step 6  Click **Upload**. The Upload Configuration window appears. Upload the downloaded provisioned file from CVC with the same name. Refer to the following:

*Figure 27: Upload Configuration*

Step 7  Verify the Authentication on CVC. Validate if the installed sensor Status changed to **Connected** or **Waiting for Data**. Refer to the following:
Capture Live Traffic

Step 1  Sync the date and time between CVC and Router. To capture the live traffic there should be exact clock sync between Router and CVC.

Step 2  Simulate IOx Traffic or play captured PCAP files. The CVC Sensor installed on the Router is a docker app. To login to the console of the App, perform the following command:

Example:
```
app-hosting connect app-id <app-name> session
```

Step 3  Upload the PCAP Files to the App from LM-GUI. Navigate to:

Applications > CVC App (Application Name) > Manage > App-Dir

The following commands show how to play the PCAP file:

Example:
```
Router# show app-hosting list
App id | State
-------------------------
CVC Sensor | RUNNING

Router# app-hosting connect appid CVCSensor session
```
Step 4  Monitor the traffic on CVC. Navigate to Explore > Essential Data > Activity List

Refer to the following:

*Figure 29: Activity List*

---

**Installing CVC Sensor using LM GUI**

**Step 1**  Login using user account and password.
**Step 2**  
Install the sensor virtual application. Once you are logged in, the following menu will appear:
Step 3  Click on **Add New**. Navigate to the app file, for example, CiscoCyberVision-IOx-aarch64-xxx.tar. Add the name of the app, for example, **CCVSensor**.

Configure the sensor virtual application. Refer to the following:
Step 4  
Click on **Activate** to launch the configuration of the sensor application. Click on the **CCVSensor** Tab, and click on **Resources**. Refer to the following:
Change the disk size to 128MB.

**Note**  
Do not use more space than that.

**Step 5**  
Navigate to **Advanced Settings**. In advanced options, configure the tmpfs by adding the following in the text area beside Docker Options:

```bash
--tmpfs /tmp:rw,size=128m
```
Figure 34: Advanced Settings

Resource Profile
- Profile: exclusive
- CPU: 1155 cpu-units
- Memory: 862 MB
- Disk: 128 MB

Available CPU: 1155
Available Memory: 862
Available Disk: 438

Advanced Settings

Specify "docker run" options to be used while spawning the container. These will override activation settings above.

Docker Options:
- --rm --tmpfs /tmp:rw.size=128m

Auto delete container instance

Step 6
Bind interfaces in the container to an interface on the host in the Network Configuration section.

What to do next
Move to the next sections Binding eth0 and Binding eth1.

Binding eth0

to configure eth0:

Step 1
Select interface eth0, and then click on edit.
Figure 35: eth0

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Config</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>VPG0</td>
<td>none</td>
</tr>
<tr>
<td>eth1</td>
<td>Not Configured</td>
<td>none</td>
</tr>
</tbody>
</table>

Add App Network Interface

Step 2
Select the Interface VPG1.

Figure 36: VPG1

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>VPG0</td>
</tr>
<tr>
<td>eth1</td>
<td>Not Configured</td>
</tr>
</tbody>
</table>

eth0: VPG1 VirtualPortGroup via intser
Description (optional): VPG0 VirtualPortGroup via intsvc0

Step 3
Click on Interface Setting.
Step 4  
Apply the following configuration:
- Choose the Static option
- IP/Mask add 169.254.0.2 / 30
- Default Gateway IP is 169.254.0.1

Then click on OK.

Step 5  
Click on OK again.
Step 6

The **Activate** window appears. Click on **OK**.

*Figure 39: Activate Window*

---

**Binding eth1**

To configure the eth1 interface:

**Step 1**
Select VPG0.
Step 2  
Click **Interface Setting** and apply the following configuration:

- Choose the **Static** option
- IP/Mask add **169.254.1.2 / 30**
Activate the Application

Now the sensor application should be activated.

**Step 1**
Click on **Activate App**. Refer to the following:

*Figure 42: Activate the Application*

**Network Configuration**

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Config</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>VPG1</td>
<td>none</td>
</tr>
<tr>
<td>eth1</td>
<td>VPG0</td>
<td>none</td>
</tr>
</tbody>
</table>

[Add App Network Interface]

**Peripheral Configuration**

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Name</th>
<th>Label</th>
<th>Status</th>
</tr>
</thead>
</table>

[Add Peripheral]

**Step 2**
The progress window appears. This may take several seconds to finish.

*Figure 43: Activation Progress*

**Step 3**
Click on **Applications** to display the app status. Refer to the following:
Figure 44: Applications Resources

Starting the Application

Step 1  Click on Start. Refer to the following:

Step 4  The application is activated and needs to be started.
Step 2  The progress window appears. This may take several seconds to finish.

Step 3  After some time, the app status will change to running.
Figure 47: Application Running

CCVSensor
Cisco Cyber Vision sensor for aarch64

<table>
<thead>
<tr>
<th>TYPE</th>
<th>VERSION</th>
<th>PROFIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>docker</td>
<td>3.1.0+202004150638</td>
<td>exclusive</td>
</tr>
</tbody>
</table>

| Memory * | 100.0% |
| CPU *    | 100.0% |

- Stop
- Manage

Starting the Application
New Features for Cisco IOS-XE 17.5.1

The following are the new features available on the IR1101 for IOS-XE release 17.5.1:

• DSL SFP Annex J support, on page 101
• VXLAN, on page 102
• Dying-Gasp SMS Notification for EM74XX Modems, on page 103
• SNMP MIB for Digital I/O, on page 104
• GPS access to IOx Apps, on page 104
• Yang model for mSATA, on page 105
• Guest shell as IOx container app, on page 106
• SNMP MIB supports the show power CLI, on page 107
• ERSPAN support cellular interface as source interface, on page 108
• Yang model for DSL, on page 108
• DNP3 Enhancement, on page 109

DSL SFP Annex J support

IOS-XE release 17.5.1 adds in support for Annex-J configuration in the controller interface.

Note

ADSL2+ J is supported, ADSL2 J is not yet supported in 17.5.1.

To enable Annex-J, perform the following:

```
router#config term
router(config)#controller vdsl 0/0/0
router(config-if)#capability annex-j
router(config-if)#exit
router#
```

To remove Annex-J, perform the following:

```
To remove Annex-J:
router#config term
router(config)#controller vdsl 0/0/0
router(config-if)#no capability annex-j
router(config-if)#exit
router#
```
17.5.1 adds in a new command **rx-padding**. This command is used for packets with an MTU less than 64 bytes.

---

**Important**

If frames less than 64mtu are expected downstream from the service provider, the Vlan configuration must be vlan 96.

---

The command example is as follows:

```
router(config)
```

```
router#config term
router#controller vds 0/0/0
router(conf-if)#rx-padding
router(conf-if)#end
```

Execute **write mem** to save the configuration.

---

**VXLAN**

VXLAN is a MAC in IP/UDP (MAC-in-UDP) encapsulation technique with a 24-bit segment identifier in the form of a VXLAN ID. The larger VXLAN ID allows LAN segments to scale to 16 million in a cloud network. In addition, the IP/UDP encapsulation allows each LAN segment to be extended across existing Layer 3 networks, making use of Layer 3 Equal-Cost Multi-Path (ECMP).

The configuration for the two devices is shown in the following table:
<table>
<thead>
<tr>
<th>Router-1</th>
<th>Router-2</th>
</tr>
</thead>
</table>
| bridge-domain 1  
member vni 6001  
member Vlan100 service-instance 1  |
| interface Loopback1  
ip address 200.200.200.200 255.255.255.255  |
| interface GigabitEthernet0/0/0  
ip address 192.168.1.2 255.255.255.0  
media-type rj45  |
| interface FastEthernet0/0/1  
switchport access vlan 100  |
| interface Vlan100  
no ip address  
service instance 1 ethernet  
encapsulation dot1q 100 //untag  |
| interface nve1  
no ip address  
source-interface Loopback1  
member vni 6001  
ingress-replication 100.100.100.100  |
| ip forward-protocol nd  
ip pim rp-address 200.200.200.200  
ip http server  
ip http secure-server  
ip route 0.0.0.0 0.0.0.0 192.168.1.3  |
| bridge-domain 1  
member vni 6001  
member Vlan100 service-instance 1  |
| interface Loopback1  
ip address 100.100.100.100 255.255.255.255  |
| interface GigabitEthernet0/0/0  
ip address 192.168.1.3 255.255.255.0  
media-type rj45  |
| interface FastEthernet0/0/1  
switchport access vlan 100  |
| interface Vlan100  
no ip address  
service instance 1 ethernet  
encapsulation dot1q 100 //untag  |
| interface nve1  
no ip address  
source-interface Loopback1  
member vni 6001  
ingress-replication 200.200.200.200  |
| ip forward-protocol nd  
ip pim rp-address 100.100.100.100  
no ip http server  
ip http secure-server  
ip route 0.0.0.0 0.0.0.0 192.168.1.2  |

**Dying-Gasp SMS Notification for EM74XX Modems**

**Prerequisites:**

- Hardware Peripheral: P-LTEA-EA, P-LTEA-LA
- Initial Release: IOS-XE 17.5.1
- License: Cisco Network-advantage

Pluggable Interface Modules (PIMs) using the EM7430 or EM7455 modem have extra capacitors to supply power to the modem in case of loss of power to the module. This allows a graceful power off of the modem. When loss of power is detected, the modem is expected to send out dying gasp SMS when configured.

The following is an example of configuring dying gasp with a phone number and SMS message:

```
#controller Cellular 0/1/0
#lte dyinggasp sms send 9119110911 “Losing Power”
```

Warning: Enabling Dying Gasp SMS configuration completed successfully. Please reset Modem for the changes to take effect
## Configuration Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>controller Cellular &lt;slot&gt;</td>
<td>Enters the interface command mode for the cellular module controller slot.</td>
</tr>
<tr>
<td>3</td>
<td>lte dyinggasp detach enable</td>
<td>Enable dying-gasp feature with send detach request</td>
</tr>
<tr>
<td>4</td>
<td>lte dyinggasp sms send &lt;phone number&gt; &lt;SMS message&gt;</td>
<td>Configure the phone number to receive SMS text message and the content of text message to be sent by the modem when platform or module powered down.</td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Exit configuration</td>
</tr>
<tr>
<td>6</td>
<td>write mem</td>
<td>Save changes to the router configuration</td>
</tr>
</tbody>
</table>

## Configuration Example

The following example shows how to enable dying-gasp feature on cellular module in slot 0/1/0, specify phone number receiving the SMS, and the specific SMS text message to be sent by modem upon power failure.

```
router# configure terminal
router(config)# controller cellular 0/1/0
router (config-controller)# lte dyinggasp detach enable
router (config-controller)# lte dyinggasp sms send 4081112222
```

## SNMP MIB for Digital I/O

Digital I/O is similar to the ALARM IN and ALARM OUT supported in other IR devices. On other devices, ALARM IN is a dedicated input and the ALARM OUT is a dedicated output. With Digital I/O it can be input or output. There are 4 Digital I/O available on the IR1101 with an Expansion Module.

MIB support will reflect the show alarm output for digital I/O only.

CISCO-DIGITAL-IO-MIB.my will have 4 digital I/O nodes. Each digital I/O node will have corresponding attributes like description, enable, severity, application, output, threshold, trigger leaf nodes for each digital I/O nodes.

## GPS access to IOx Apps

Previously, when a modem has GPS enabled, the NMEA stream was not forwarded to IOx. This release allows the NMEA stream to be forwarded to IOx from the ngiolite module. There are two steps to enable this.

- Create a tunnel between Linux and IOx
- Forward all NMEA messages over the tunnel to IOx.
The system code checks for the presence of the tunnel, and if it is not present, data cannot be sent to IOx.

To support this feature there will be two new tunnels created for two cellular modems on the IR1101 and IR1800. Two tunnels are created by default and whichever modem has the GPS/NMEA enabled, the NMEA stream will be sent over the corresponding tunnel as follows:

Modem0:

[Linux] /dev/ttyTun5 and /dev/ttyTun6 [IOx]. Soft link to /dev/ttyTun5 will be created named /dev/ttyTunNMEA0, soft link to /dev/ttyTun6 will be created named /dev/ttyNMEA0 which can be accessed from IOx.

Modem1:

[Linux] /dev/ttyTun7 and /dev/ttyTun8 [IOx]. Soft link to /dev/ttyTun7 will be created named /dev/ttyTunNMEA1, soft link to /dev/ttyTun8 will be created named /dev/ttyNMEA1 which can be accessed from IOx.

The following command shows the state of the GPS:

IR1101# show app-hosting list
App id State
-------------------------------
gps RUNNING

Yang model for mSATA

YANG is a popular data modeling language to represent data sent over network management protocols such as NETCONF and RESTCONF. The Cisco-IOS-XE-device-hardware-oper YANG model has been modified to show mSATA information. mSATA has two CLIs to display associated data.

These two CLIs are:

show platform hardware msata status

• The CLI gives information on whether the SSD is present or not.
• If the SSD is present, a message "SSD is present" is displayed.
• If the SSD is not present, a message "SSD is not present" is displayed.

show platform hardware msata lifetime

• If SSD is present an output representing the SSD lifetime in % is displayed: "SSD lifetime remaining (%): 99"
• If SSD is not present, a message "SSD is not present" is displayed.

A typical YANG response for mSATA in device-inventory is as shown below:

<device-inventory>
   <hw-type>hw-type-ssd</hw-type>
   <hw-dev-index>5</hw-dev-index>
   <version>V00</version>
   <part-number>IR-SSD-MSATA-100G</part-number>
   <serial-number>FOC21520XFV</serial-number>
   <hw-description>mSATA Module</hw-description>
   <dev-name>Expansion module 2 - mSATA Module</dev-name>
   <field-replaceable>true</field-replaceable>
   <hw-class>hw-class-virtual</hw-class>
Guest shell as IOx container app

The Guest Shell is a virtualized Linux-based environment, designed to run custom Linux applications, including Python for automated control and management of Cisco devices. Using the Guest Shell, the user can also install, update, and operate third-party Linux applications and access the IOS CLI.

The Guest Shell environment is intended for tools, Linux utilities, and manageability rather than networking. Guest Shell shares the kernel with the host (router) system. Users can access the Linux shell of Guest Shell and update scripts and software packages in the container rootfs. However, users within the Guest Shell cannot modify the host file system and processes.

The Guest Shell container is managed using IOx. IOx is Cisco's Application Hosting Infrastructure for Cisco IOS XE devices. IOx enables hosting of applications and services developed by Cisco, partners, and third-party developers in network edge devices, seamlessly across diverse and disparate hardware platforms.

The Guest Shell is typically bundled with the system image and can be installed using the `guestshell enable` Cisco IOS command. However, this approach leads to an increase of roughly 75MB in the size of the image. This is a problem for some users who have limited bandwidth, or download images through LTE.

With these users in mind, guestshell will be made available as a single tar file which can then be downloaded and installed on the system like any other IOX application. As a result, there won't be any increase in the size of the universal release image.

---

**Note**

Day 0 guestshell provisioning will not work with this approach.

By default, Guest Shell allows applications to access the management network via the management interface. For platforms like the IR1101, which don't have a dedicated management port, a VirtualPortGroup can be associated with Guest Shell in the IOS configuration.

Sample guestshell configuration can be found on this page:

To install guestshell on the device, copy the tar file to the router and run the following command:

```
app-hosting install appid guestshell package <path to tar file>
```

Use the following command to check the status:

```
show app-hosting list
```

Once guestshell has been deployed successfully, standard guestshell commands such as `guestshell enable`, `guestshell run bash`, and `guestshell run python3` should work.

The following resource talks about running python scripts using guestshell:

---

Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide
Only python3 is supported in 17.5.1.

**Important - Before You Install**

Before attempting to install Guest shell on your device, please verify that the device has IOx container keys programmed on it by running the following command:

```
Router#show software authenticity keys | i Name
```

The output should contain one or more lines with the Product Name “Cisco Services Containers”. If the device doesn’t have container keys programmed on it, then you won’t be able to install guest shell.

You will see an error like the following:

```
*Aug 26 15:47:21.484: %IOSXE-3-PLATFORM: R0/0: IOx: App signature verification failed with non-zero exit code
```

There is no software based mechanism to install container keys on the device. The keys have to be programmed at the manufacturing facility. IR1100 devices shipped after January 1, 2020, should have the container keys programmed.

The guest shell tar file is published along with the IOS-XE image for a given release. More information can be found here: [https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads](https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads)

---

**SNMP MIB supports the show power CLI**

SNMP MIB support for the `show power` CLI is available through a new mib file: CISCO-ENTITY-SENSOR-MIB.my

The following is an example of the `show power` CLI:

```
#show power
Main PSU:
    Total Power Consumed: 8.77 Watts
    Configured Mode : N/A
    Current runtime state same : N/A
    PowerSupplySource : External PS
```

The following is an example of the CISCO-ENTITY-SENSOR-MIB.my MIB:

```
SensorDataType (INTEGER) watts(6)
SensorDataScale (INTEGER) milli(8)
SensorValue(INTEGER) 8770
```
Use the following commands to configure:

```bash
Router(config)#snmp-server community public RW
Router(config)#end
```

**ERSPAN support cellular interface as source interface**

Encapsulated Remote Switched Port Analyzer (ERSPAN) allows traffic from Cellular interfaces to be monitored. ERSPAN sends monitored traffic to a network analyzer.

The following is a sample configuration:

```bash
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#no shut
Router(config-mon-erspan-src)#source interface Cellular0/1/0
Router(config-mon-erspan-src)#destination
Router(config-mon-erspan-src-dst)#erspan-id 1
Router(config-mon-erspan-src-dst)#mtu 146
Router(config-mon-erspan-src-dst)#ip address 169.254.1.2
Router(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
Router(config-mon-erspan-src-dst)#show monitor session erspan-source
```

For detailed information on configuring ERSPAN, see the following guide:


**Yang model for DSL**

YANG is a popular data modeling language to represent data sent over network management protocols such as NETCONF and RESTCONF.

The `Cisco-IOS-XE-controller-vdsl-oper` has been introduced to edit the Controller vdsl configurations which gives the yang support for the DSL.

An example of a typical yang response for edit config of the dsl controller follows:

```xml
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
  <controller>
    <VDSL xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
      <name>0/0/0</name>
      <adsl-pvc xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-adsl">
        <vpi-vci>255/65535</vpi-vci>
        <bridge-dot1q>21</bridge-dot1q>
        <encapsulation>vcmux</encapsulation>
      </adsl-pvc>
    </VDSL>
  </controller>
</native>
```
The Controller configurations can be retrieved using `get` and `get-config` operations with the Cisco-IOS-XE-native yang model.

Cisco IOS-XE Yang Data Models are found here:
https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.5.1 release is found under 1751.

**DNP3 Enhancement**

In some cases, older RTUs were previously used in peer-to-peer mode. These RTUs dynamically swapped the roles of DNP3 Serial subordinate and primary by setting the bit DIR=1 in the message header. ASE’s SCADA stack used in Cisco routers are always configured to be DNP3 Serial primary. In this case, all the packets received from DNP3 serial with DIR=1 were ignored causing many messages from RTU to be discarded. To handle these scenarios, a new SCADA configuration CLI has been added:

```plaintext
scada-gw protocol ignore direction
```

Enabling this CLI will allow the router to accept incoming packets from RTU even when DIR=1. The new CLI will also be added to the Cisco-IOS-XE-scada-gw.yang config model.

The following is an example usage:

```plaintext
Router# config term
Router(config)# scada-gw protocol ignore direction
```

**Configuration**

Configuration example with scada-gw protocol ignore direction on T101/T104

```plaintext
scada-gw protocol t101
channel rt-chan
link-addr-size two
bind-to-interface Async0/2/0
session rt-sess
attach-to-channel rt-chan
common-addr-size one
cot-size two
info-obj-addr-size three
link-addr 31
sector rt-sec
attach-to-session rt-sess
asdu-addr 100
scada-gw protocol t104
channel mt-chan
t3-timeout 20
tcp-connection 0 local-port 8001 remote-ip 192.168.1.0/24
session mt-sess
```
attach-to-channel mt-chan
sector mt-sec
attach-to-session mt-sess
asdu-addr 101
map-to-sector rt-sec
scada-gw protocol ignore direction
scada-gw enable
New Features for Cisco IOS-XE 17.6.1

The following are the new features available for the IR1101 on release 17.6.1:

- Per Port DHCP Address Allocation, on page 111
- Custom Controlled LED, on page 112
- Support DSL SFP Firmware signing and signature validation, on page 112
- DSL SFP Annex M support, on page 113
- Support Four ADSL MIB Objects, on page 113
- Digital IO Enhancement, on page 113

Per Port DHCP Address Allocation

No new CLI added. The device on interface FA0/0/1 should get 192.0.2.90.

The minimum configuration looks like the following example:

```conf
conf t
ip dhcp excluded-address 192.0.2.1 192.0.2.80
ip dhcp excluded-address 192.0.2.100 192.0.2.255
ip dhcp use subscriber-id client-id
end

conf t
ip dhcp pool 16
  network 192.0.2.0 255.255.255.0
  address 192.0.2.90 client-id Fa0/0/1 ascii
end
```

The show output CLI appears like the following:

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type State Interface
Hardware address/
User name
192.0.2.90 0046.6130.2f30.2f31 Infinite Manual Active Unknown
```

The client-id has to be the short-name of the interface. Use "Fa" for FastEthernet interface. Use "Gi" for GigabitEthernet interface.
Custom Controlled LED

The IR-1101 has a non-blinking tri-color custom LED, which can be controlled with the following executive privilege CLI.

```
router# set platform hardware custom-led <0-7>
```

The numbers 0-7 are as follows:

- 0: Off
- 1: Blue
- 2: Green
- 3: Red
- 4: Blue/Green
- 5: Blue/Red
- 6: Green Red
- 7: Blue/Green/Red

Support DSL SFP Firmware signing and signature validation

An optional IOS filepath has been added to the end of the existing upgrade command. The file must be signed with SFP-VADSL2-I key. The file could be in bootflash/flash:, usbflash0 or msata:. It cannot be from any remote file system.

Command Line Interface

The command line interface for upgrading the module follows:

```
router# upgrade hw-module subslot 0/0 sfp 0 <IOS filepath>
```

Options to the command are:

```
Router#upgrade hw-module subslot 0/0 sfp 0 ?
  bootflash: Firmware filename on local driver
  crashinfo: Firmware filename on local driver
  flash: Firmware filename on local driver
  usbflash0: Firmware filename on local driver
```

The following is an example of the command usage:

```
Router#upgrade hw-module subslot 0/0 sfp 0 bootflash:sfp8455_rel.bin
Digital signature successfully verified in file bootflash:sfp8455_rel.bin
Upgrade SFP firmware on interface GigabitEthernet0/0/0 from 1_62_8463 to 1_62_8455
Connection will be disrupted, Continue(Y/N)?y
Start ebm upgrade!!
..........................................................................................................................
..........................................................................................................................
..........................................................................................................................
..........................................................................................................................
..........................................................................................................................
firmware update success!!
```
DSL SFP Annex M support

Support is the same as it was for Annex-J in 17.5.1

Support Four ADSL MIB Objects

MIB support has been added to obtain the DSL line speed and attainable rate on the IR1101.

The new MIBS are shown below:

1.3.6.1.2.1.10.94.1.1.4.1.2 ADSL-LINE MIB:adslAtucChanCurrTxRate
1.3.6.1.2.1.10.94.1.1.5.1.2 ADSL-LINE MIB:adslAturChanCurrTxRate
1.3.6.1.2.1.10.94.1.1.2.1.8 ADSL-LINE MIB:adslAtucCurrAttainableRate
1.3.6.1.2.1.10.94.1.1.3.1.8 ADSL-LINE MIB:adslAturCurrAttainableRate

Command Line Interface

On a router with a DSL SFP connected to ADSL DSLAM, the following existing SNMP CLIs can be used to verify support for the above OIDs:

```
!configure SNMP Server
!---------------------
snmp-server community public RO
snmp-server manager
!
!verify MIB OIDs
!---------------------
snmp get-next v2c 33.33.33.102 public oid 1.3.6.1.2.1.10.94.1.1.4.1.2
!
```

The following command can also be used to gather the MIB values from another SNMP Client (for example, a linux device):

```
$ snmpwalk -v 2c -c public 33.33.33.102 1.3.6.1.2.1.10.94.1.1.4.1.2
```

Digital IO Enhancement

Support has been added to allow some digital I/O ports to be managed by IOSd, and some other digital IO ports to be managed by IOx container apps. An updated CLI has been added and the YANG model for Digital IO Enhancement has been updated.

The 17.5.1 version of the CLI is:

```
Router(config)# alarm contact attach-to-iox
```

Note

With release 17.5.1, `alarm contact attach-to-iox` gave IOX control for ALL digital IO ports (1 thru 4).
The 17.6.1 version of the CLI is:

Router(config)#alarm contact 1 ?
  application Set the alarm application
  attach-port-to-iox Enable selected Digital IO Ports access from IOX
  description Set alarm description
  enable Enable the alarm/digital IO port
  output Set mode as output
  severity Set the severity level reported
  threshold Set the digital IO threshold
  trigger Set the alarm trigger

Router(config)#alarm contact 1 attach-port-to-iox

Router#show alarm
  Alarm contact 0:
  Not enabled.
  Digital I/O 1:
  Attached to IOX.
  Digital I/O 2:
  Not enabled.
  Digital I/O 3:
  Not enabled.
  Digital I/O 4:
  Not enabled.

In the updated CLI, <1-4> are the number of digital I/O ports to assign to IOX for container apps.

**Note**

With release 17.6.1, each digital IO port can be assigned to IOX individually.
New Features for Cisco IOX XE 17.7.1

This chapter contains the following sections:

• IRM-1100 Expansion Module on the Compute Side, on page 115
• Support ADSL MIB Objects, on page 115
• Support VDSL MIB Objects, on page 116
• Support 1G SFPs, on page 117

IRM-1100 Expansion Module on the Compute Side

The IR1101 has two attachment points for expansion modules. The top side of the router is referred to as the Expansion side. The bottom side of the router is referred to as the Compute side.

Prior to IOS XE release 17.7.1, support was only on the Expansion side.

Starting with the 17.7.1 release, additional modules can be connected on the Compute side.

Features and Limitations

The following apply to the IRM-1100 with release 17.7.1:

• Switchports will not work if anything is connected on the Compute side
• MSATA and GPIO Pins for IRM-1100-SPMI are not supported when it is connected to the Compute side (bottom) for 17.7.1
• The IR1101 can only support a maximum of two LTE interfaces. Connecting an IRM-1100 on both sides is not supported. If connected in this configuration, only the Expansion side will be active.
• LTE interfaces when connected on Compute side, are enumerated cellular 0/4/0 and cellular 0/4/1
• CAT18 LTE module is not supported on the Compute side.
• Only the LTE interface functions when the IRM-1100-SP or IRM-1100-SPMI is connected on the Compute side.

Support ADSL MIB Objects

The following ADSL MIB OID will be supported on the IR1101:
Support VDSL MIB Objects

The following VDSL MIB OID will be supported on the IR1101:

1.3.6.1.2.1.10.251.1.4.1.1.1.2 ADSL-LINE-MIB xdsl2PMLCurr15MValidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.3 ADSL-LINE-MIB xdsl2PMLCurr15MInvalidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.4 ADSL-LINE-MIB xdsl2PMLCurr15MTimeElapsed
1.3.6.1.2.1.10.251.1.4.1.1.1.5 ADSL-LINE-MIB xdsl2PMLCurr15MCodingViolations
1.3.6.1.2.1.10.251.1.4.1.1.1.6 ADSL-LINE-MIB xdsl2PMLCurr15MCorrectedBlocks
1.3.6.1.2.1.10.251.1.4.1.1.1.7 ADSL-LINE-MIB xdsl2PMChHist15MMonitoredTime
1.3.6.1.2.1.10.251.1.4.1.1.1.8 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.9 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.10 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.11 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.12 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.13 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.14 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.15 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.16 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.17 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.18 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.19 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.20 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.21 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.22 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.23 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.24 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.25 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.26 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.27 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.28 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.29 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.30 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.31 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.32 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.33 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.34 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.35 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.36 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.37 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.38 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.39 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.40 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.41 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.42 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.43 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.44 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.45 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.46 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.47 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.48 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.49 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.50 ADSL-LINE-MIB xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.1.1.51 ADSL-LINE-MIB xdsl2PMChHist15MInvalidInterval
Support 1G SFPs

Release 17.7.1 will add support for the following SFPs:

- GLC-T-RGD
- CWDM-SFP-1470=
- CWDM-SFP-1610=
- CWDM-SFP-1530=
- DWDM-SFP-3033=
- DWDM-SFP-3112=
- GLC-BX-D-I=
- GLC-BX-U-I=
- GLC-TE
New Features for Cisco IOX XE 17.7.1

Support 1G SFPs
Installing the Software

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

These are the two main methods to install the software:

- Managing and Configuring a Router to Run Using Consolidated Packages — This method allows for individual upgrade of subpackages and generally has reduced boot times compared to the method below. Use this method if you want to individually upgrade a module's software.

- Managing and Configuring a Router to Run Using Individual Packages — This simple method is similar to a typical Cisco router image installation and management that is supported across Cisco routers.

It is better to upgrade software in a planned period of maintenance when an interruption in service is acceptable. The router needs to be rebooted for a software upgrade to take effect.

Licensing

This section contains the following:

Cisco Software Licensing

Cisco software licensing consists of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
You can enable licensed features and store license files in the bootflash of your router. Licenses pertain to consolidated packages, technology packages, or individual features.

The IR1101 uses Smart Licensing, which is discussed in detail in the next chapter.

The IR1101 does not support the Right to Use licenses, and supports only the Specific License Reservation (SLR)

### Consolidated Packages

To obtain software images for the router, go to: [https://software.cisco.com/download/home/286319772/type/282046477/release/Gibraltar-16.11.1](https://software.cisco.com/download/home/286319772/type/282046477/release/Gibraltar-16.11.1)

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>All of the IOS-XE feature set may not apply to the IR1101. Some features may not have been implemented yet, or are not appropriate for this platform.</td>
</tr>
</tbody>
</table>

An image-based license is used to help bring up all the subsystems that correspond to a license. This license is enforced only at boot time.

One of the following image-based licenses can be pre-installed on the IR1101 router:

- Network-Essentials
- Network-Advantage

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details of the Network-Essentials and Network-Advantage contents can be found in the product data sheet located here:</td>
</tr>
</tbody>
</table>


### Network-Essentials

The **Network-Essentials** technology package includes the baseline features. It also supports security features.

The **Network-Essentials_npe** technology package (**npe = No Payload Encryption**) includes all the features in the Network-Essentials technology package without the payload encryption functionality. This is to fulfill export restriction requirements. The Network-Essentials_npe is available only in the Network-Essentials_npe image. The difference in features between the Network-Essentials package and the Network-Essentials_npe package is therefore the set of payload encryption features such as IPsec and Secure VPN.

### Network-Advantage

The **Network-Advantage** technology package includes all crypto features.

The **Network-Advantage_npe** package (**npe = No Payload Encryption**) includes all the features in the **Network-Advantage** technology package without the payload-encryption functionality. This is to fulfill export restriction requirements. The **Network-Advantage_npe** package is available only in the **Network-Advantage_npe** image. The difference in features between the **Network-Advantage** package and the **Network-Advantage_npe** package is therefore the set of payload-encryption-enabling features such as IPsec and Secure VPN.
Related Documentation

For further information on software licenses, see the Smart Licensing chapter.

How to Install the Software for Cisco IOS XE

To install the software, use one of the following methods to use the software from a consolidated package or an individual package. Also see Overview section.

- Managing and Configuring a Router to Run Using a Consolidated Package section
- Managing and Configuring a Router to Run Using Individual Packages section
- Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example section

Installing the Cisco IOS XE Release

When the device boots up with Cisco IOS XE image for the first time, the device checks the installed version of the ROMMON, and upgrades if the system is running an older version. During the upgrade, do not power cycle the device. The system automatically power cycles the device after the new ROMMON is installed. After the installation, the system will boot up with the Cisco IOS XE image as normal.

Note

When the device boots up for first time and if the device requires an upgrade, the entire boot process may take several minutes. This process will be longer than a normal boot due to the ROMMON upgrade.

The following example illustrates the boot process of a consolidated package:

Router# configure terminal
Router(config)#boot sys bootflash:/ir1101-universalk9.16.10.01.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router#*
Nov 7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
Router# show run | inc license
license udi pid IR1101-K9 sn FCW2150THOF
license boot level network-advantage
Router# reload
/noverify Don't verify file signature before reload.
/verify Verify file signature before reload.
at Reload at a specific time/date
cancel Cancel pending reload
in Reload after a time interval
pause Pause during reload
reason Reload reason
<cr>
<cr>
Router# reload /verify
System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
Nov 7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Verifying file integrity of bootflash:/ir1101-universalk9.16.10.01.SPA.bin.........

-----------------------------
ROMMON Images

A ROMMON image is a software package used by ROM Monitor (ROMMON) software on a router. The software package is separate from the consolidated package normally used to boot the router.

An independent ROMMON image (software package) may occasionally be released and the router can be upgraded with the new ROMMON software. For detailed instructions, see the documentation that accompanies the ROMMON image.

Note

A new version of the ROMMON image is not necessarily released at the same time as a consolidated package for a router.

File Systems

The following table provides a list of file systems that can be seen on the Cisco IR1101 router.

Table 7: Router File Systems

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Boot flash memory file system.</td>
</tr>
</tbody>
</table>
File System | Description
---|---
flash: | Alias to the boot flash memory file system above.
cns: | Cisco Networking Services file directory.
nvram: | Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl: | File system for Onboard Failure Logging (OBFL) files.
system: | System memory file system, which includes the running configuration.
tar: | Archive file system.
tmpsys: | Temporary system files file system.
usbflash0: | The Universal Serial Bus (USB) flash drive file systems.

**Note** The USB flash drive file system is visible only if a USB drive is installed in the usb port.

Use the ? help option if you find a file system that is not listed in the table above.

### Option to Enable or Disable USB Access

USB flash drives offer inexpensive and easy storage space for the routers to store the images, configuration files and other files.

**Note**: The IR1101 supports ext2 and vfat file systems for USB flash drives.

The IR1101 supports hot plug/unplug of USB flash drives. To access the USB flash drive, insert the device into Router's USB interface. Once the USB is recognized, an alert message is seen on the console:

```
Aug  1 11:08:53.198 PDT: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
```

After this message is seen, the USB flash drive is accessible. Users can access the USB contents using the `dir usbflash0:` command:

```
Device# dir usbflash0:
Directory of usbflash0:/
  5 drwx  Aug 23 2019 10:42:18 -07:00  System Volume Information
  6 -rwx  Aug 27 2019 17:40:38 -07:00  test.txt
206472192 bytes total (206470144 bytes free)
Device#
```

Contents can be copied to and from the USB flash drive using the copy command. Once the copy is complete, a log message showing number of bytes copied is displayed.

```
Device# copy flash:test.txt usbflash0:
Destination filename [test.txt]? <Enter>
Copy in progress...C
35 bytes copied in 0.020 secs (1750 bytes/sec)
Device#
```
While hot plug/unplug of a USB flash drive is supported, the functionality comes with security vulnerabilities. To prevent users from copying sensitive information to the USB flash drive, USB enable/disable functionality has been added.

By default, the USB flash drive is enabled. If a user wishes to disable USB, they can do so using the disable command:

```
Device# config terminal
Device(config)# platform usb disable
Device(config)# end
```

Once the USB flash drive has been disabled, the file system is not shown on the Device and syslog messages will not be displayed when the USB is inserted. Users will not be able to access the contents of the USB.

For example:

```
Device# dir usbflash0:
dir usbflash0: ^
% Invalid input detected at '^' marker.
Device#
```

The USB is enabled by issuing a `no` with the disable command:

```
Device# config terminal
Device(config)# no platform usb disable
Device(config)# end
```

The USB status can be displayed using the following command:

```
Device# show platform usb status
USB enabled
Device#
```

The USB port could be considered a potential security risk. If you wish to disable the USB port, use these steps:

```
Configure terminal
platform usb disable
exit
show platform usb
```

**Autogenerated File Directories and Files**

This section discusses the autogenerated files and directories that can be created, and how the files in these directories can be managed.
Table 8: Autogenerated Files

<table>
<thead>
<tr>
<th>File or Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo files</td>
<td>Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.</td>
</tr>
<tr>
<td>core directory</td>
<td>The storage area for .core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.</td>
</tr>
<tr>
<td>managed directory</td>
<td>This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.</td>
</tr>
<tr>
<td>tracelogs directory</td>
<td>The storage area for trace files. Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure. Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.</td>
</tr>
</tbody>
</table>

Important Notes About Autogenerated Directories

Important information about autogenerated directories include:

- Autogenerated files on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by Cisco customer support.

  Note: Altering autogenerating files on the bootflash: may have unpredictable consequences for system performance.

- Crashinfo files and files in the core and tracelogs directory can be deleted.

Flash Storage

Subpackages are installed to local media storage, such as flash. For flash storage, use the `dir bootflash:` command to list the file names.

Note: Flash storage is required for successful operation of a router.
LED Indicators

For information on LEDs on the router, see "LED Indicators" in the "Product Overview" section of the Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide.

To monitor the LED status of the system, the alarm and interface ports, the show LED command line is supported in IOS mode.

Router# show LED
SYSTEM LED : Green
Custom LED : Off
VPN LED : Off
ALARM LED : Off
GigabitEthernet0/0/0 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off
GigabitEthernet0/0/5 LED : On
EM Module digital I/O 1 LED : Off
EM Module digital I/O 2 LED : Off
EM Module digital I/O 3 LED : Off
EM Module digital I/O 4 LED : Off
*System LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On
*EM Module LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On
Router#

Related Documentation

For further information on software licenses, see the Smart Licensing Chapter.

For further information on obtaining and installing feature licenses, see Configuring the Cisco IOS Software Activation Feature.
Prerequisites for Cisco Network Plug and Play Agent

- Cisco Network Plug and Play (PnP) deployment method depends on the type of discovery process as required by the customer.
- Deploy the discovery mechanism, either a DHCP server discovery process or a Domain Name Server (DNS) discovery process, before launching the PnP.
- Configure the DHCP server or the DNS server before deploying the PnP.
- Ensure that the PnP server talks to the PnP agent.
- Ensure that the Cisco Network PnP Agent has connectivity with the PnP Server. The Cisco Network PnP Agent should be able to PING server.
- The PnP agent enforces the PnP server to send user credentials for every request. Cisco recommends the usage of HTTP secure (HTTPS) protocol.
Restrictions for Cisco Network Plug and Play Agent

- Cisco Network Plug and Play (PnP) agent facilitates HTTP and HTTP secure (HTTPS) transport based communication with the server.
- HTTPS cannot be used on platforms where crypto-enabled images are not supported (also, do not use Secure Sockets Layer [SSL] or Transport Layer Security [TLS] protocols if crypto-enabled images are used).
- Non-VLAN 1 configuration-Cisco Network Plug and Play supports devices using VLAN 1 by default. To use a VLAN other than 1, adjacent upstream devices must use supported releases and configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: \texttt{pnp startup vlan x}. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, all the active interfaces on the upcoming Plug and Play device are changed to the specified VLAN. This guideline applies to both routers and switches.

Information About Cisco Network Plug and Play Agent

Cisco Network Plug and Play Deployment Solution

The Cisco Network PnP Agent is a part of Cisco Network Plug and Play solution. The Cisco initiated Network Plug and Play (PnP) deployment solution supports the concept of redirection and includes a PnP agent, a PnP server, and other components. Simplified deployment process of any Cisco device automates the following deployment related operational tasks:

- Establishing initial network connectivity for the device
- Delivering device configuration
- Delivering software and firmware images
- Delivering licenses
- Delivering deployment script files
- Provisioning local credentials
- Notifying other management systems about deployment related events
Simplified deployment reduces the cost and complexity and increases the speed and security of deployments. Cisco Network Plug and Play (PnP) agent is a software application that is running on a Cisco IOS or IOS-XE device. The PnP agent together with the PnP deployment server provides effortless deployment services. When a device is powered on for the first time, the PnP agent process wakes up in the absence of the startup config, user input on the device's console, and attempts to discover the address of the PnP server. The PnP agent uses methods like DHCP, Domain Name System (DNS), and others to acquire the desired IP address of the PnP server. When the PnP agent successfully acquires the IP address, it initiates a long lived, bidirectional layer 3 connection with the server and waits for a message from the server. The PnP server application sends messages to the agent requesting for information and services to be performed on the device.

The PnP agent converges existing solutions into a unified agent and adds functionality to enhance the current solutions. The main objectives of PnP agent are:

- Provide consistent day 1 deployment solution for all the deployment scenarios.
- Add new features to improve existing solutions.
- Provide day 2 management framework mainly in the context of configuration and image upgrades.

### Cisco Network Plug and Play Features

Some of the features that the Cisco Network Plug and Play agent provides:

- **Day 0 boot strapping**—Configuration, image, licenses, and other files
- **Day 2 management**—Configuration and image upgrades and on-going monitoring of Simple Network Management Protocol (SNMP) and syslog messages.
- **Open communication protocol**—Enables customers and partners to write applications
- **XML based payload over HTTP between the server and the agent.**
- **Security**—Authentication and encrypted communication channel between the management app and the agent
- **Deployment and management of devices behind firewall and Network Address Translation (NAT).**
- **Support for one-to-one and one-to-many communication**
- **Support for policy based deployment (product ID or location of the device)**
- **Deployment based on unique ID (Unique Device Identifier [UDI] or MAC)**
- **Unified solution across Cisco platforms (including IOS classic)**
- **Support for various deployment scenarios and use cases**
- **Zero-touch when possible, low-touch when needed**

### Cisco Network Plug and Play Agent Services and Capabilities

The services and capabilities of the Cisco Network Plug and Play agent are as follows:

1. **Backoff**
2. **CLI execution**
3. **Configuration upgrade**
4. Device information
5. File transfer
6. Image install
7. License install
8. PnP tagging
9. Script execution
10. Topology information

---

**Note**

The PnP server provides an optional checksum tag to be used in the image installation and config upgrade service requests by the PnP agent. When the checksum is provided in the request, the image install process compares the checksum against the current running image checksum.

If the checksums are same, the image being installed or upgraded is the same as the current image running on the device. The image install process will not perform any other operation in this scenario.

If the checksums are not same, then the new image will be copied to the local file system, and checksum will again be calculated and compared against the checksum provided in the request. If same, the process will continue to install the new image or upgrade the device to new image. If now, the checksums are not same, the process will exit with error.

---

**Backoff**

A Cisco IOS device that supports PnP protocol (that uses HTTP transport), requires the PnP agent to send the work request to the PnP server continuously. In case the PnP server does not have any scheduled or outstanding PnP service for the PnP agent to execute, the continuous no operation work requests exhausts both network bandwidth and device resource. This PnP backoff service allows the PnP server to inform the PnP agent to rest for the specified time and call back later.

---

**CLI Execution**

Cisco IOS supports two modes of command execution—EXEC mode and global configuration mode. Most of the EXEC commands are one-time commands, such as `show` commands, which show the current configuration status, and `clear` commands, which clear counters or interfaces. The EXEC commands are not saved when a device reboots. Configuration modes allow user to make changes to the running configuration. If you save the configuration, these commands are saved when a device reboots.

---

**Note**

For `show` command request and response details and for all PnP configuration commands, see *Cisco Network Plug and Play Agent Command Reference*.

---

**Configuration Upgrade**

There are two types of configuration upgrades that can happen in a Cisco device—copying a new configuration files to startup configuration and copying new configuration files to running configuration.
Copying a new configuration files to startup configuration— The new configuration file is copied from the file server to the device through `copy` command and file check is performed to check the validity of the file. If the file is valid, then the file is copied to startup configuration. Backing up the previous configuration file will be done if there is enough disk space available. The new configuration is seen when the device reloads again.

Copying new configuration files to running configuration— The new configuration file is copied from the file server to the device through `copy` command or `configure replace` command. Configuration file replace and rollback may leave the system in an unstable state if rollback is performed efficiently. So configuration upgrade by copying the files is preferred.

**Device Information**

The PnP agent provides capability to extract device inventory and other important information to the PnP server on request. The following five types of device-profile requests are supported:

1. `all`—returns complete inventory information, which includes unique device identifier (UDI), image, hardware and file system inventory data.
2. `filesystem`—returns file system inventory information, which includes file system name and type, local size in bytes, free size in bytes, read flag, and write flag.
3. `hardware`—returns hardware inventory information, which includes hostname, vendor string, platform name, processor type, hardware revision, main memory size, I/O memory size, board ID, board rework ID, processor revision, midplane revision, and location.
4. `image`—returns image inventory information, which includes version string, image name, boot variable, return to rommon reason, bootloader variable, configuration register, configuration register on next boot, and configuration variable.
5. `UDI`—returns device UDI.

**File Transfer**

The PnP file server hosts files that can be copied over by the deploying devices in the network. The file server can be a dedicated server hosting files or a part of the device hosting the PnP server. The PnP agent uses standard file transfer protocols to copy files from the remote file server to the device. If the device is running a crypto image then secured file transfer protocols such as SFTP, SCP, HTTPS are supported. For devices running non-crypto images, the PnP agent supports unsecured copy protocols such as FTP, TFTP, HTTP.

**Image Install**

Image installation service enables a PnP-enabled device to perform image upgrade on receiving a request from the PnP server.

**Standalone Devices**

When the PnP agent on a standalone device receives a request from the PnP server, the agent parses the XML payload and identifies the request as an Image Upgrade request. The agent then creates an ImageInstall process, which identifies the request as a standalone image install request. The PnP agent populates the data structure defined by the ImageInstall service and passes it to the ImageInstall service.

The Image Install service then performs the following operations to successfully load the device with the new image:
1. Copies the image from the file server to a local disk (the file server information is provided by the PnP server in the request).
2. Configures the device to load the new image on next reload by executing the `boot system` command.
3. Reloads the device and sends a message to the PnP server.

**PnP Tagging**

Cisco IOS provides capability to assign tags to the devices for better grouping and tracking of all Cisco devices. The PnP agent provides XML service for configuring the tag information on the device and for propagating the tag information within the network using Cisco Discovery Protocol (CDP). The purpose of this service is for the PnP agents to get to know their tag information and to pass on this information to the PnP server upon request.

**Topology Information**

By default, every Cisco device on the network runs Cisco Discovery Protocol (CDP). Through CDP, devices in the network discover their immediate neighbors and populate their databases with the attributes learnt or derived through the protocol. This neighbor information is stored in the database and is available on demand by the device to the PNP server. Typical neighbor information comprises neighboring device ID, software version, hardware platform, interface ip, and the port on which CDP messages are sent or received.

**Software Maintenance Upgrade**

The software maintenance upgrade (SMU) is a package that contains fixes for a specific defect or security resolution to a released image. SMUs are created to respond to immediate issues and do not include new features. SMUs do not have a large impact on router operations. SMU versions are synchronized to the package major, minor, and maintenance versions they upgrade.

To install and activate a software maintenance upgrade package:

---

**Step 1**

Use the `install add <filename>` command to unpack the package software file and copy it to the boot device (usually disk0). If the file is on a remote source, use the tftp/ftp option to copy the file to the device.

After the file is copied to the device, information within the package is used to verify compatibility with the target cards and with the other active software. Actual activation is performed only after the package compatibility and application program interface (API) compatibility checks are passed.

**Step 2**

To activate a package, use the `install activate <filename>` command. The activate operation will run the compatibility checks and install the software maintenance upgrade package. If it is a reload software maintenance upgrade, it will automatically initiate a reload.

**Step 3**

Use the `install commit` command to commit the changes.

**Step 4**

To deactivate the package, use the `install deactivate <filename>` command.

**Step 5**

If you find that you prefer a previous package set over the currently active package set, you can use the `install rollback to committed` command to make a previously active package set active again.

**Step 6**

To remove the installed version, use the `install remove <filename>` command.

This example shows how to install and remove the software maintenance upgrade package on a device.

```
install add <filename>
install activate <filename>
install commit
```

---
Cisco Network Plug and Play Agent

The Cisco Network Plug and Play agent is an embedded software component that is present in all Cisco network devices that support simplified deployment architecture. The PnP agent understands and interacts only with a PnP server. The PnP agent first tries to discover a PnP server, with which it can communicate. Once a server is found and connection established, the agent performs deployment related activities like configuration, image, license, and file updates by communicating with the server. It also notifies the server of all interesting deployment related events like out-of-band configuration changes and a new device connection on an interface.

Cisco Network Plug and Play Server

The Cisco Network Plug and Play server is a central server that encodes the logic of managing and distributing deployment information (images, configurations, files, and licenses) for the devices being deployed. The server communicates with the agent on the device that supports the simplified deployment process using a specific deployment protocol.

![Simplified Deployment Server Diagram]

The PnP server also communicates with proxy servers like deployment applications on smart phones and PCs, or other PnP agents acting as Neighbor Assisted Provisioning Protocol (NAPP) servers, and other types of proxy deployment servers like VPN gateways.

The PnP server can redirect the agent to another deployment server. A common example of redirection is a PnP server redirecting a device to communicate with it directly after sending the bootstrap configuration through a NAPP server. A PnP server can be hosted by an enterprise. This solution allows for a cloud based...
deployment service provided by Cisco. In this case, a device discovers and communicates with Cisco’s cloud based deployment service for initial deployment. After that, it can be redirected to the customer’s deployment server.

In addition to communicating with the devices, the server interfaces with a variety of external systems like Authentication, Authorizing, and Accounting (AAA) systems, provisioning systems, and other management applications.

Cisco Network Plug and Play Agent Deployment

The following steps indicate the Cisco Network Plug and Play agent deployment on Cisco devices:

1. The Cisco device, having PnP agent contacts the PnP server requesting for a task, that is, the PnP Agent sends its unique device identifier (UDI) along with a request for work.

2. The PnP server if it has any task for the device, sends a work request. For example, image install, config upgrade, and so on.

3. When the PnP agent receives the work request, executes the task and sends back a reply to the PnP server about the task status, whether it is a success or error, and the corresponding information requested.

Cisco Network Plug and Play Agent Network Topology

*Figure 49: Network Topology of Cisco Network Plug and Play Agent Deployment*
Cisco Network Plug and Play Agent Initialization

The Cisco Network Plug and Play agent software is currently available on all Cisco IOS XE platforms, and is enabled by default. The PnP agent can be initiated on a device by the following ways:

Absence of Startup Configuration

New Cisco devices are shipped to customers with no startup configuration file in the NVRAM of the devices. When a new device is connected to a network and powered on, the absence of a startup configuration and the user input file on the device, it will automatically trigger the Cisco Network Plug and Play agent to discover the PnP server IP address.

Figure 50: State Diagram for PnP Trigger with no Startup Configuration

CLI Configuration for Open Plug-n-Play Agent

Network administrators may use CLI configuration mode to initiate the Open Plug-n-Play (PnP) agent process at any time. By configuring a PnP profile through CLI, a network administrator can start and stop the PnP agent on a device. When the PnP profile is configured with CLI, the device starts the PnP agent process which, in turn, initiates a connection with the PnP server using the IP address in the PnP profile.

Figure 51: State Diagram for PnP Trigger with CLI Configured PnP Profile

Cisco Network Plug and Play Agent Deployment Solutions

This section discusses the functionality of the Cisco Network Plug and Play agent, exposed to the PnP server, for device deployment and management. The PnP agent deployment solution comprises the discovery process initiated by the agent, communication between the device, agent, and the server, and the PnP agent services. The PnP solution is described in detail in the following sections:

Cisco Network Plug and Play Agent Discovery Process

When the device boots up, the absence of any startup config on the NVRAM triggers the PnP discovery agent to acquire the IP address of the PnP server. In order to acquire the IP address of the PnP server, the PnP agent goes through one of the following discovery mechanisms:

1. PnP discovery through DHCP server
2. PnP discovery through DHCP snooping
3. PnP discovery through DNS lookup
4. PnP proxy for layer 2 and layer 3 devices
5. PnP deployment application

Cisco Network Plug and Play Discovery through DHCP Server

Device with no startup configuration in the NVRAM triggers the Cisco Network Plug and Play agent to initiate a DHCP discovery process which acquires the IPv4 configuration from the DHCP server required for the device. The DHCP server can be configured to insert additional information using vendor specific option 43 upon receiving option 60 from the device with the string 'cisco pnp', to pass on the IPv4 address or hostname of the PnP server to the requesting device. When the DHCP response is received by the device, the PnP agent extracts the option 43 from the response to get the IP address or the hostname of the PnP server. PnP agent then uses this IPv4 address or hostname to communicate with the PnP server.

Assumptions:
- New devices can reach DHCP server
- Customer is willing to configure DHCP server for network devices

Plug-n-Play Discovery through DHCP Snooping

If a third party DHCP server cannot be configured to insert any vendor specific options, an existing Cisco Open Plug-n-Play (PnP) enabled device can be configured to snoop in to the DHCP response and insert PnP specific option 43 with the PnP server IP address.
Before inserting the option 43, the snooping agent verifies if the DHCP message is from a Cisco device in the network. The remaining DHCP discovery process is same as described in the previous section.

**Assumptions:**
- New devices can reach DHCP server
- New devices can reach DNS server
- Customer is not willing to configure DHCP server for network devices
- Upstream switch (SW) is configured to snoop DHCP and insert PnP server IP

**Cisco Network Plug and Play Discovery through DNS Lookup**

When the DHCP discovery fails to get the IP address of the Cisco Network Plug and Play server, the agent falls back on Domain Name System (DNS) lookup method. PnP agent then uses a preset deployment server name. The agent obtains the domain name of the customer network from the DHCP response and constructs the fully qualified domain name (FQDN). The following FQDN is constructed by the PnP agent using a preset deployment server name and the domain name information for the DHCP response, `deployment.customer.com`. The agent then looks up the local name server and tries to resolve the IP address for the above FQDN.
Figure 54: DNS Lookup for deployment.customer.com

Assumptions:

- New devices can reach DHCP server
- Customer deployed PnP server in the network with the name “pnpserver”

Cisco Network Plug and Play Proxy Server for Layer 3 and Layer 2 Devices

This device listens to a specific port for any incoming PnP messages. The Cisco device which is trying to come up as a PnP device sends a UDP broadcast message to its network every 30 min for ten times. Hence, if the device does not receive a response, the broadcasts stop after 300 min.
Figure 55: DNS Lookup for Layer 3 and Layer 2 Devices
When the device hosting the proxy server process receives the incoming broadcasts, it verifies the version field in the request and forwards the request to the PnP server if version validation is successful. The proxy server process also caches the unique device identifier (UDI) of the requesting client coming in via incoming datagram before forwarding the request to PnP server.

Upon receiving the configlet datagram from PnP server, the proxy server validates UDI in the incoming datagram with the entries in the UDI cache. If validation is successful, proxy server process broadcasts the datagram to a specific port number reserved for the proxy client processes to receive datagrams.

Upon receiving the datagrams, devices running proxy client processes, parse the incoming datagram for the target UDI. If the target UDI in the datagram matches the UDI of the device, proxy client process proceeds with framing, error control and configuring the configlet.

If the target UDI in the datagram fails to match UDI of the device, the packet is dropped.

**Plug-n-Play Agent Deployment Application**

A Cisco device can alternatively be manually configured by the network administrator using a deployment application running on their PC or on a smart phone. The PC or the smart phone can be connected to the device using an USB or an Ethernet cable.

*Figure 56: Manually Configured PnP Agent*

---

**Plug-n-Play Agent Deployment Protocol**

Deployment can be run over different transports. These transports include Ethernet and IP with Transport Layer Security (TLS). Layer 2 transport is typically used between a deployment agent and a proxy deployment server like a deployment application or as a deployment agent acting as a proxy. Transport between an agent and a server is over an IP connection with TLS for security. Transport between a proxy deployment server and a deployment server is also over IP with TLS.
Plug-n-Play Agent Application Protocol

The Cisco Open Plug-n-Play (PnP) agent application protocol is an XML-based protocol that defines a mechanism that allows network devices to be monitored and controlled by a remote application. The PnP agent is a software module running on a Cisco device. The PnP server is an application running as the network manager that remotely manages the network devices. The main features of the PnP protocol are as follows:

1. Supports HTTP protocols
2. Supports Transport Level Security (TLS) based encryption for HTTP
3. Uses HTTP secure (HTTPS) certificate for TLS handshake

Plug-n-Play Transport over Ethernet

Cisco Open Plug-n-Play (PnP) agent uses the Ethernet based transport in the following two scenarios:

- **Deployment agent communicating with a deployment application on a PC**: In this case, the PC is connected to the device being deployed using an Ethernet cable. The deployment application advertises itself as a deployment server supporting Ethernet transport.

- **Deployment agent communicating with an already deployed device acting as a proxy deployment server**: In this case, the new device being deployed has an Ethernet connection to an already deployed device. The deployment agent on the deployed device responds to the discovery requests and acts as a proxy deployment server for the new device.

Once discovery is complete, the deployment agent starts an unsecured XML stream with the deployment server over Ethernet. This protocol reserves an Ethertype (0xXX TBD) for this purpose. The deployment agent and the server then negotiate to use Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) to protect the communication and complete the EAP-TLS session establishment. The deployment server then authenticates the device with the HTTP secure (HTTPS) certificate or some other supported mechanism.

Plug-n-Play Transport over IP

In Cisco Network Plug-n-Play (PnP) agent, the deployment agent opens TCP connection to the deployment server and starts an XML stream of messages. The server can request the use of Transport Layer Security (TLS) at this time. The agent closes the existing XML stream, initiates a TLS connection to the server, and then restarts the XML stream. The server can request agent authentication over the TLS connection.

Plug-n-Play Agent Security

Security to all Cisco Open Plug-n-Play (PnP) devices is provided at both transport level as well as the application level. The following sections describe the security mechanisms in detail:

Plug-n-Play Transport Layer 3 Security

For non-crypto or non-crypto-enabled images, TLS security choice is not possible. One alternative minimum security is to have the PnP agent initiate the connection to the specified trusted PnP server on port 5222.

Authentication and Authorization between Plug-n-Play Agent and Server

Once the Cisco Open Plug-n-Play (PnP) deployment agent discovers the PnP server, the agent engages the server in a Transport Layer Security (TLS) handshake. In order to authenticate itself to the server, the agent presents its HTTP secure (HTTPS) certificate. The administrator for the PnP server sets device authentication mechanisms which are acceptable for a particular deployment.
The deployment server presents its certificate to the deployment agent so that the agent can authenticate the server. Irrespective of whether the agent is able to verify the server certificate, the agent engages the deployment server in a post-TLS authorization exchange. In this exchange the agent requests the server to present its server authorization token. In response to this request the server presents the authorization token it had obtained from Cisco. The agent verifies the signature on the authorization token. If the authorization token is specific to a Unique Device Identifier (UDI), the agent also ensures its UDI is listed in the authorization-token. At the end of this step, a secure communication channel is established between the deployment agent and the server. This secure communication channel is leveraged by the server to send deployment information to the agent.

Security Methods for the PnP Discovery Process

This section describes the methods that are used to secure the PnP agent-server communication in various scenarios. The security options are used by the PnP agent during the zero-touch PnP server discovery. This section includes the following topics:

- Self-Signed Certificate Based Authentication, on page 142
- Mobile Device Based Secured Installation, on page 143
- CA-Signed Certificate based Authentication, on page 143
- DHCP Option based Discovery over an IPv4 Network, on page 143

Self-Signed Certificate Based Authentication

The PnP server has an option to use a self-signed SSL certificate for server side authentication. When the PnP server uses a self-signed certificate, the PnP discovery cannot be used for automatically initiating secured communication from the agent to the server. The device goes through usual PnP discovery mechanisms and when it finds the server, the agent sends a work-request over HTTP. The server should use the PnP certificate-install service to instruct the agent to install the server self-signed certificate, and then automatically reconnect back to the server over HTTPS.

To keep the solution secured, it is recommended that you use the unsecured port 80 of server to deliver the one-time certificate installation to the devices. All other services should be sent over the secured port.

The following figure shows the end-to-end secured PnP workflow using a self-signed server SSL certificate.

Figure 57: PnP Deployment with Self-Signed Certificate
Mobile Device Based Secured Installation

As part of this solution, an application for mobile devices is available to configure the bootstrap on the devices. The mobile application can be used to install the server certificate directly on each device along with other bootstrap configuration and then allow the PnP agent initiate secured communication with the server. In this method, the server does not open up any unsecured port for certificate-install.

The following figure shows the end-to-end secured PnP workflow using the application on the mobile devices.

Figure 58: Secured PnP Deployment with the Mobile Application

CA-Signed Certificate based Authentication

Cisco distributes certificates signed by a signing authorities in a tar file format and signs the bundle with Cisco Certificate Authority (CA) signature. This certificate bundle is provided by Cisco infoSec for public downloads on cisco.com.

The certificates from this bundle can be installed on the Cisco IOS device for server side validation during SSL handshake. It is assumed that the server uses a certificate, which is signed by one of the CA that is available in the bundle.

The PnP agent uses the built-in PKI capability to validate the certificate bundle. As the bundle is signed by Cisco CA, the agent is capable of identifying the bundle that is tampered before installing the certificates on the device. After the integrity of the bundle is ensured by the agent, the agent installs the certificates on the device. After the certificates are installed on the device, the PnP agent initiates an HTTPs connection to the server without any additional steps from the server. The following mechanisms helps the PnP agent to initiate a zero-touch secured communication.

DHCP Option based Discovery over an IPv4 Network

The DHCP option 43 and option 60 is a vendor specific identifier which is used by the PnP agent to locate and connect to the PnP server. To support multiple vendors, the PnP agent in Cisco device sends out a case-sensitive “ciscopnp” as the option 60 string during the DHCP discovery. The DHCP server can be configured with multiple classes matching with a different option 60 string that comes from each network device. After the option 60 string matches, the DHCP server sends out the corresponding option 43 string back to the device. The following is the format for defining the option 43 for PnP deployments:

```
option 43 ascii "5A;K5;B2;110.30.30.10;J443;Tftp://10.30.30.10/ios.p7b;Z10.30.30.1
```
The field ‘T’ in the PnP string provides an option for the network administrator to specify the location of the certificate bundle, which can be hosted on a local or remote file server.

If the certificate bundle is available at the specified location, then the agent:

1. Downloads the bundle from the file server to the device.
2. Checks the signature of the downloaded bundle to ensure it has a genuine Cisco signature.
3. Installs the certificates on the device.

If the ‘T’ option is not specified and the transport mechanism is specified in the option 43 string as HTTPs, the PnP agent looks for the Cisco signed certificate bundle in the default folder of the same server http://10.30.30.10:443/certificates/default/cert.p7b.

If the certificates are available at the default location then the agent performs the steps mentioned above to install the certificates.

After the certificates are installed and the server discovery is complete, the agent initiates the HTTPs connection with the server without any additional configuration. During the HTTPs handshake, the device uses the certificates installed from the bundle to validate the server certificate.

The following figure shows the end-to-end secured PnP workflow using the CA bundle-based certificate.

Figure 59: Secured PnP Deployment with Trustpool

This flow works only if the server is using a certificate signed by one of the known signing authorities that is available in the bundle. If the server uses a certificate that is not a part of the bundle then the HTTPS handshake will fail. When you specify the option 43 string with HTTPs as a transport option and if the bundle download fails, the agent will not fall back to any of the unsecured communication protocol even if the server is reachable. If the transport option is specified as HTTP with a parameter ‘T’ pointing to a valid certificate bundle location, the agent overrides the transport option HTTP and changes it to HTTPs for secured communication. Generally, the agent will choose the most secured communication from the available options.

The path specified in the DHCP option 43 to locate the certificate bundle file can be an absolute URL or a relative URL. If you specify a relative URL, the agent forms a full URL with the server IP address or hostname as specified in the option 43 string and uses HTTP as the file transfer protocol.

Also, to install the certificates, the agent expects the device to have an updated system clock. Because, you configure the DHCP server first, you cannot specify the current time in the DHCP server. In such a scenario, an IP address or a URL can be specified as an alternative parameter in the option 43 with the prefix ‘Z’, which
can point the device to a NTP server. The agent synchronizes the clock on the device with the NTP server and then installs the certificates.

**DHCP Option based Discovery over an IPv6 Network**

Cisco Network PnP uses the DHCP Option 16 and Option 17 for an IPv6 DHCP discovery process. The Option 16 and Option 17 are vendor specific identifiers. These are used by the Cisco Network PnP agent to locate and connect to the Cisco Network PnP server. The DHCP server can be configured to insert an additional information using the vendor specific Option 17. When the DHCP server receives an Option 16 from the device with the string `cisco pnp`, and if it matches the Option 17 string, the server passes the IP address or the hostname of the Cisco PnP server to the requesting device. When the device receives the DHCPv6 response, the Cisco Network PnP agent extracts the option from the response and identifies the IPv6 address of the Cisco PnP server. Cisco PnP agent uses this IPv6 address to communicate with the Cisco PnP server. To obtain and install the certificate, use the same process explained in the DHCP Option based Discovery over an IPv4 Network section.

The following example shows how to configure a pool (DHCPv6-pool) with the vendor-specific options:

```
ipv6 dhcp pool dhcpv6-pool
address prefix 2003::/64 lifetime infinite infinite
vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5a1d:k4:b3;ife80::2e0:81ff:fe2d:3799;j6088"
```

**DNS-based Discovery**

In DNS-based discovery, a DHCP server receives the domain name of the customer network. The domain name is used to create a PnP-specific, fully qualified domain name (FQDN) such as `pnpserver.<domain_name>`. In this method, the customer network resolves this URL to a valid PnP server IP address. Because, there is no mechanism to specify the certificate location, the agent locates the server certificate to initiate the HTTPS connection without manual intervention.

During the system boot up, the device acquires IP network information from a DHCP server along with the domain name. With the customer specific domain name, the Cisco PnP agent creates the following URL `pnpserver.<domain_name>` and looks for the Cisco signed certificate bundle in a default folder of the server `<domain_name>/ca/trustpool/cabundle.p7b`.

If the certificate bundle is available at the specified location, then the agent:

1. Downloads the bundle from the file server to the device.
2. Checks the signature of the downloaded bundle to ensure it has genuine Cisco signature.
3. Installs the certificates on the device.

If the certificate bundle is not available at the specified location, the PnP agent use a predefined URL `pnpcertserver.<domain_name>` and looks for the Cisco signed certificate bundle in the default folder of the server, `<domain_name>/ca/trustpool/cabundle.p7b`.

If the certificates are available at the specified location, then the agent performs the steps specified above to install the certificates.

After the certificates are installed and the server discovery is complete, the agent initiates the HTTPS connection with the server at the URL `pnpserver.<domain_name>` without any additional configuration. During the HTTPS handshake, the device uses the certificates that are installed from the bundle to validate the server certificate.
Also, to install the certificates, the agent expects the device to have an updated system clock. Because, you configure the DHCP server first, you cannot specify the current time in the DHCP server. In such a scenario, the agent uses a predefined URL, `pnpntpserver <domain_name>` which needs to be mapped to a NTP sever to synchronize the clock on the device, and then installs the certificates.

However, if the certificate is not present at either URL, the Cisco PnP agent will fall back and establish the HTTP connection to the server using the created FQDN `pnpserver.<domain_name>`. With this workflow, the agent expects the server to use the certificate-install service to install the self-signed certificates first and then start the provisioning steps.

**DNS-based Discovery over an IPv6 Network**

To enable DNS-based discovery over an IPv6 network:

### Step 1
Configure the DNS server with an IPv6 option. To enable the Cisco Network PnP DNS discovery, configure the DNS server as shown in this example:

```plaintext
ip host pnpntpserver.domain.com 2001::1
ip host pnptrustpool.domain.com 2001::2
ip host pnpserver.domain.com 2001::3
```

### Step 2
DHCPv6 server is discovered through DHCP bootstrap process. The following example shows how to configure the DHCP server:

```plaintext
ipv6 unicast routing
ipv6 cef
ipv6 dhcp pool test
dns-server 2001::4
domain-name example.com
```

The device sends the DHCPv6 packets to the server over an IPv6 network. After receiving the DHCPv6 packets, the DNS server information and the domain-name are returned to the device as Option 23 and Option 24 respectively.

### Step 3
Configure the NTP server. The following example shows how to configure the NTP server:

```plaintext
ntp master 1
```

**Note** Similarly, the device NTP configuration should use the NTPv4 option.

### Step 4
Host the trustpool server on an IPv6 network. Trustpool is supported only on DHCP Options T and Z. If the Option T is configured, specify the URL of the trustpool CA bundle. If the Option Z is configured, specify the NTP server IP address.

**Note** When the Cisco Network PnP agent attempts to download the trustpool bundle over HTTP by using an IPv6 option, the trustpool server should support HTTP over an IPv6 network. Also, the clock must be synchronized before configuring the trustpool.

### Step 5
Host the Cisco Network PnP server on an IPv6 network.

---

**Cisco Cloud Redirection over an IPv4 and IPv6 Network**

Cisco Cloud Redirection service supports Cisco Network PnP zero-touch discovery. It is supported on both IPv4 and IPv6 based Cisco Cloud discovery.
Some of the Cisco PnP devices may have root certificate embedded in the devices. These devices will communicate with the CCO server using HTTPS from the beginning. If the device does not have the embedded certificate then the legacy behavior is initiated.

When the device boots up without any start-up configuration or authentication certificates, and if the DHCP and DNS discovery fails, the device tries to contact the Cisco Cloud server at devicehelper.cisco.com.

If the devicehelper.cisco.com is reachable, the Cisco Network PnP agent downloads the trustpool bundle and establishes a secure HTTP connection with the Cisco Cloud Redirection service. When the device tries the Cisco cloud discovery for the first time, Cisco Network PnP agent downloads the trustpool from this location devicehelper.cisco.com/ca/trustpool and saves it to the local flash memory. This location is shared with a Public Key Infrastructure for a trustpool installation. If the Cisco cloud discovery fails, trustpool bundle is retained in the flash memory and Cisco Network PnP checks for a copy of the trustpool bundle in the local device flash memory. If the copy is not available in the local flash memory, it retries to download the trustpool bundle from this location devicehelper.cisco.com/ca/trustpool download.

Cisco Network PnP agent sends a HTTPS hello message to the Cisco cloud. The Cisco Network PnP redirection service running at Cisco cloud server replies to the HTTP request. A Cisco cloud server PnP profile is created on the device as shown in this example.

```
pnp profile pnp_cco_profile
transport https host devicehelper.cisco.com port 443
```

After the Cisco cloud profile is created, the device sends a work-information message with its unique device identifier information to the Cisco cloud server. Cisco Cloud Redirection service sends a redirection non-backoff PnP request with the Cisco Network PnP server information. It can be an IPv4 address, IPv6 address, or a hostname. When the redirection is successful, the following redirection profile is configured on the device.

```
pnp profile pnp_redirection_profile
transport https ipv4 172.19.153.133 port 443
```

If the non-backoff PnP request is not received within default wait time, Cisco Network PnP discovery process continues with the next discovery mechanism.

**Cisco Network PnP Discovery Over 4G Interface**

Cisco Network PnP over 4G interface is available on platforms that have 4G NIMs and running Cisco IOS XE. When a device with an activated SIM card boots up, the 4G interface is activated and used for the Cisco Network PnP cloud discovery process. When a device without an activated SIM card boots up, the non-4G interfaces are preferred for the discovery process. Cisco Network PnP cloud discovery over 4G interfaces is attempted when the non-4G interfaces are not available or if the Cisco Network PnP discovery does not succeed on the non-4G interfaces. When the device has multiple 4G interfaces with active SIM cards, the Cisco Network PnP tries the cloud discovery on all the 4G interfaces one after the other until one of them succeeds.

To use the 4G interface for the Cisco Network PnP discovery, the 4G NIMs should have an activated SIM card on it.

Cisco Network PnP Cloud discovery over 4G interfaces works when all the 4G interfaces are activated during the device bootup by default. In the absence of a startup configuration, the device attempts to bring up the 4G
inutrafec by default and attempts Cisco PnP over cloud. After the device is redirected, the device connects to the Cisco Network PnP server and downloads the appropriate image and configuration to the device.

Note
The DNS server is available as part of the 4G network and the cloud portal should be programmed to redirect the calling device to an appropriate Cisco Network PnP server for provisioning the device. Currently, Cisco Network PnP support over 4G interface uses only the IPv4 network.

Ensure that the configuration pushed through the Cisco Network PnP server contains a route to Cisco Network PnP server over the 4G interface. This can be a default route and should retain the Cisco Network PnP agent and server communication to continue to work over the 4G interface, after the provisioning is completed.

Cisco Network PnP Discovery over a Management Interface

Cisco Network PnP Agent supports discovery and four-way handshake over a management interface with a default VPN Routing/Forwarding (VRF). To send and receive the DHCP traffic over an VRF interface, you have to configure the IOS DHCP server. This feature helps the new devices to access the Cisco Network PnP features when only the management interface is active.

When the device boots up, the management interface under the default VRF is assigned an IP address through DHCP. This interface establishes a connection to a Cisco Network PnP server and the Cisco Network PnP agent on the device records this information (VRF name and source interface). This information is used for future PnP communication with the Cisco Network PnP server. In this case, the Cisco PnP profile that is created on the device will have an extra keyword `VRF` attached to it.

Cisco PnP over an EtherChannel

When you deploy an access switch by using the Cisco Network Plug and Play, the existence of LACP EtherChannels on the provisioned switch (which acts as trunk) does not allow you to configure the device. When the access device tries to connect through the provisioned switch over an L2 EtherChannel using LACP, it breaks the connectivity. Since the configuration does not exist on the access device, the access device cannot bring up the EtherChannel with the switch. This results in keeping the EtherChannel ports in suspended state and breaks the L2 connectivity. Cisco Network PnP Agent detects the presence of EtherChannels and auto-configures the EtherChannel on the device to bring up the Layer 2 connectivity automatically for the day-zero configuration.

Security Methods for Post-PnP Discovery Process

This section explains the methods provided by the Cisco PnP agent which can be, used by the Cisco PnP server to secure the client-server communication after completing the discovery process. This section includes the following topic:

- Certificate Install Service, on page 148

Certificate Install Service

The Cisco PnP agent provides a mechanism to manage SSL certificates on the device by providing the certificate-install service to the Cisco PnP server. The certificate-install service provides a simple XML to install the server’s self-signed certificates or certificates signed by standard CA certificates on the device,
before initiating an HTTPs connection. The certificate-install service also provides an option to install the client SSL certificate and instruct the device to use the same SSL certificate during the next device authentication process.

**SUDI-based PnP Application Level Authentication**

The SSL communication ensures encryption of the data packets exchanged between the server and the device, but does not provide a solution to authenticate the device.

To ensure that the server is talking to a genuine Cisco device, the agent uses the built-in Secure Unique Device Identifier (SUDI) certificate support on the device. SUDI is a X.509 compliant device certificate burnt into the device's secured chip (ACT2) during the manufacture time. The SUDI certificate contains the device's serial number, private-public keys, and the Cisco CA signature. The agent provides the following mechanisms that can be used by the server to authenticate the device as a genuine Cisco device:

- SUDI-based Client Certificate Validation, on page 149
- SUDI-based Serial Number, on page 149

**SUDI-based Client Certificate Validation**

Before the agent initiates an HTTPs connection with the server, the agent checks whether the device has a built-in SUDI certificate. If the device has a certificate, then the agent sends the SUDI certificate to the client during the SSL handshake for validating. Optionally, the HTTPs server may choose to validate the device using the SUDI certificate during the SSL handshake. After validating, the HTTPs server allows the device to connect to the server. To validate the device's SUDI certificate, the server should use Cisco CA to complete the validation.

**SUDI-based Serial Number**

If the device is loaded with SUDI certificate, the PnP agent reads the serial number from the SUDI certificate and presents the same information as an additional tag in the work-request body for all communication with the server. To achieve this, the following optional tag is added in the work-info message, which goes out from the device in every work-request. This field is optional and does not show up for devices that does not have SUDI certificate.

There is no change in the existing UDI mechanism that is read from the chassis inventory. The agent continues to be backwards compatible by sending the chassis UDI as the primary identifier. The server can use the additionally provided SUDI-based serial number to authenticate the device and then continue to use the primary UDI. For the devices without a SUDI certificate, the agent does not send this additional SUDI-based serial number. Therefore, the server should continue with the primary UDI for authentication and further communication.

There is no mechanism available to read the SUDI-based serial number from member hardware and there is no change in how UDI is read from other members on a stack or HA unit. The agent will continue to read the UDI from all the hardware units as it does presently.

**SUDI-Based Device Authentication**

In SUDI-based device authentication, the agent checks whether the device has a built-in SUDI certificate at the boot-up time. If the device is loaded with the SUDI certificate, the agent provides a new PnP service, which allows the server to help the device to identify itself. The availability of this new service depends on the presence of the SUDI certificate and is listed in the agent's capability service.
Along with the above change in the capability-service, the agent adds an additional field under the hardware-info section of the device-info response, to specify and check whether the SUDI certificate is built into the device.

After, the agent initiates an HTTPS connection with the server and sends a work-request, the server should be able to use the device authentication service for a challenge request-response. The device authentication service requires a minimum of one field to generate a string by the server. Optionally, the server can send a list of encryptions and hashing methods that it can support. The agent checks whether it has the capability to use any of the listed encryption methods specified by the server, uses the encryption method and sends a notification to the server. If the agent does not have the capability to use any of the methods specified by the server, then the agent responds with an error message.

When the server sends a device authentication service request to the agent, the agent does the following:

1. Uses one of the specified encryption and hashing methods.
2. If the agent does not have capability to use one of the specified encryption and hashing methods, the agent responds with an error message.
3. Encrypts the challenge string provided by the server using the private key using the PKI APIs.
4. Sends a response back with the following:
   a. Cipher text
   b. Methods used to cipher
   c. Certificate (SUDI or client installed certificate)

After, the server receives the above response from the device, the server does the following:

1. Verifies the SUDI or the client certificate against the Cisco or customer CA.
2. Decrypts the cipher-string using the public key that is available in the SUDI or client certificate.
3. Verifies whether the deciphered string matches the original version.
4. Generates a session key (string) and sends it back to the device as an acknowledgment.

After the agent receives the final acknowledgment from the server with the session-key, it associates the corresponding profile with the provided session-key and sends it to the server as an attribute in the root PnP section of all the subsequent messages that the agent sends.

The server validates the session-key before sending any message from the device. Optionally, the server maintains a timer for the session-keys and moves to invalid status when the timer expires. If the agent sends a message with an expired session-key, the server repeats the device authentication process and generates a new session-key before sending to the same device again. If the device sends a request without any session-key, then the server performs the device authentication process and generates a new session-key before sending to the same device.

The following figure displays the message sequence between the agent and the server to accomplish the device authentication using the SUDI certificate.
How to Configure Cisco Network Plug and Play Agent

Configuring Cisco Network Plug and Play Agent Profile

Perform the following task to create a Cisco Network Plug and Play agent profile:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>pnp profile <em>profile-name</em></td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# pnp profile test-profile-1</td>
<td>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Exits the PnP profile initialization mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-pnp-init)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Network Plug and Play Agent Device

Perform the following task to create a Cisco Network Plug and Play agent device:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 <code>pnp profile profile-name</code></td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated.</td>
</tr>
<tr>
<td><code>Device(config)# pnp profile test-profile-1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4 `device {username username} {password {0</td>
<td>7} password}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Establishes a username and password based authentication system.</td>
</tr>
<tr>
<td><code>Device(config-pnp-init)# device username sjohn password 0 Tan123</code></td>
<td></td>
</tr>
<tr>
<td><code>• username</code>—User ID</td>
<td></td>
</tr>
<tr>
<td><code>• password</code>—Password that a user enters</td>
<td></td>
</tr>
<tr>
<td><code>• 0</code>—Specifies that an unencrypted password or secret (depending on the configuration) follows.</td>
<td></td>
</tr>
<tr>
<td><code>• 7</code>—Specifies that an encrypted (hidden) password follows.</td>
<td></td>
</tr>
<tr>
<td>Step 5 <code>end</code></td>
<td>Exits the PnP profile initialization mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-pnp-init)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring Cisco Network Plug and Play Reconnect Factor

Perform the following task to configure the time to wait before attempting to reconnect a session in either fixed-interval-backoff, exponential-backoff, or random-exponential-backoff mode:
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> pnp profile profile-name</td>
<td>Creates a PnP agent profile and enters the PnP profile</td>
</tr>
<tr>
<td>Example:</td>
<td>initialization mode.</td>
</tr>
<tr>
<td>Device(config)# pnp profile test-profile-1</td>
<td>• String of alphanumeric characters that specify a name</td>
</tr>
<tr>
<td></td>
<td>for the PnP agent profile. Profile names cannot be</td>
</tr>
<tr>
<td></td>
<td>duplicated.</td>
</tr>
<tr>
<td><strong>Step 4</strong> reconnect [pause-time [exponential-backoff-factor [random] ] ]</td>
<td>Specifies the time for the PnP agent initiator profile to</td>
</tr>
<tr>
<td>Example:</td>
<td>wait before attempting to reconnect a session.</td>
</tr>
<tr>
<td>Device(config-pnp-init)# reconnect 100 2 random</td>
<td>• The pause-time value is the time to wait, in seconds,</td>
</tr>
<tr>
<td></td>
<td>before attempting to reconnect after a connection is</td>
</tr>
<tr>
<td></td>
<td>lost. The range is from 1 to 2000000. The default is</td>
</tr>
<tr>
<td></td>
<td>60.</td>
</tr>
<tr>
<td></td>
<td>• Exponential backoff factor value is the value that</td>
</tr>
<tr>
<td></td>
<td>triggers the reconnect attempt exponentially. The range is</td>
</tr>
<tr>
<td></td>
<td>from 2 to 9.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits the PnP profile initialization mode and returns to</td>
</tr>
<tr>
<td>Example:</td>
<td>privileged EXEC mode.</td>
</tr>
<tr>
<td>Device(config-pnp-init)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Cisco Network Plug and Play HTTP Transport Profile

Perform the following task to create a HTTP transport profile of the Cisco Plug and Play agent manually on a device.

Both IPv4 and IPv6 addresses can be used for PnP server IP configuration. Alternately, a hostname can also be used in the configuration to connect to the PnP server.

Every profile can have one primary server and a backup server configuration. The Cisco PnP agent attempts to initiate a connection with the primary server first and if it fails, it will try the backup server. If the backup server fails, the Cisco PnP agent will attempt to connect to the primary server again. This will continue until a connection is established with one of the servers.
### Cisco Network Plug and Play HTTP Transport Profile

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>enable</strong></td>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td><strong>Example:</strong> Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>pnp profile profile-name</strong></td>
<td><strong>Example:</strong> Device(config)# pnp profile test-profile-1</td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>transport http host host-name [port port-number] [source interface-type]</strong></td>
<td><strong>Example:</strong> Device(config-pnp-init)# transport http host hostname-1 port 1 source gigabitEthernet 0/0/0</td>
<td>Creates a HTTP transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>transport http ipv4 ipv4-address [port port-number] [source interface-type]</strong></td>
<td><strong>Example:</strong> Device(config-pnp-init)# transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0</td>
<td>Creates a HTTP transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>transport http ipv6 ipv6-address [port port-number] [source interface-type interface-number]</strong></td>
<td><strong>Example:</strong> Device(config-pnp-init)# transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1</td>
<td>Creates a HTTP transport configuration for the PnP agent profile based on the IPv6 address of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>end</strong></td>
<td><strong>Example:</strong></td>
<td>Exits the PnP profile initialization mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring Cisco Network Plug and Play HTTPS Transport Profile

Perform the following task to create a HTTP Secure (HTTPS) transport profile of the Cisco Network Plug and Play agent manually on a device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-pnp-init)# end</td>
<td>Purpose: Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> pnp profile profile-name</td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td>Example: Device(config)# pnp profile test-profile-1</td>
<td>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated.</td>
</tr>
<tr>
<td><strong>Step 4</strong> transport https host host-name [port port-number ][source interface-type ][localcert trustpoint-name ][remotecert trustpoint-name ]</td>
<td>Creates a HTTPS transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td>Example: Device(config-pnp-init)# transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz</td>
<td>• The value of localcert specifies the trustpoint used for client-side authentication during the transport layer security (TLS) handshake.</td>
</tr>
<tr>
<td></td>
<td>• The value of remotecert specifies the trustpoint used for server certificate validation.</td>
</tr>
<tr>
<td><strong>Note</strong> Configure the trustpoint-name using the crypto pki trustpoint command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> transport https ipv4 ipv4-address [port port-number ] [source interface-type ][localcert trustpoint-name ][remotecert trustpoint-name ]</td>
<td>Creates a HTTPS transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td>Example: Device(config-pnp-init)# transport https ipv4</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Backup Cisco Network Plug and Play Device

Perform the following task to create a backup profile and to enable or disable Cisco Network Plug and Play agent manually on a device:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 configure terminal | Enters global configuration mode. |
| Example:                  |                                       |
| Device# configure terminal|                                       |

| Step 3 pnp profile profile-name | Creates a PnP agent profile and enters the PnP profile initialization mode. |
| Example:                        | • String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| Device(config)# pnp profile test-profile-1 | |

| Step 4 backup device {username username } {password [0 | 7] password} | Configures the PnP agent backup profile on the device. |
| Example: | • Establishes a username and password based authentication system. |
| Device(config-pnp-init)# backup device username sjohn password 0 Tan123 | • username-User ID |
### Configuring Backup Cisco Network Plug and Play Reconnect Factor

Perform the following task to configure backup reconnection of the Cisco Network Plug and Play (PnP) agent to the server in either fixed-interval-backoff, exponential-backoff, or random-exponential-backoff manner:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> pnp profile <em>profile-name</em></td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated.</td>
</tr>
<tr>
<td>Device(config)# pnp profile test-profile-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> backup reconnect [<em>pause-time</em> [<em>exponential-backoff-factor</em> [<em>random</em>]] ]</td>
<td>Specifies the time for the PnP agent initiator profile to wait before attempting to reconnect a session.</td>
</tr>
<tr>
<td>Example:</td>
<td>- The pause-time value is the time to wait, in seconds, before attempting to reconnect after a connection is lost. The range is from 1 to 2000000. The default is 60.</td>
</tr>
<tr>
<td>Device(config-pnp-init)# backup reconnect 100 2 random</td>
<td>- Exponential backoff factor value is the value that triggers the reconnect attempt exponentially. The range is from 2 to 9.</td>
</tr>
</tbody>
</table>
### Configuring Backup Cisco Network Plug and Play HTTP Transport Profile

Perform the following task to create a backup HTTP transport profile of the Cisco Network Plug and Play agent manually on a device.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> pnp profile profile-name</td>
<td>Creates a PnP agent profile and enters the PnP profile initialization mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# pnp profile test-profile-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> backup transport http host host-name [port port-number ] [source interface-type]</td>
<td>Creates a backup HTTP transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-pnp-init)# backup transport http host hostname-1 port 1 source gigabitEthernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> backup transport http ipv4 ipv4-address [port port-number ] [source interface-type]</td>
<td>Creates a backup HTTP transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>backup transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0</code></td>
<td>Creates a backup HTTP transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed.</td>
</tr>
</tbody>
</table>

**Step 6**

`backup transport http ipv6 ipv6-address [port port-number ] [source interface-type interface-number ]`

**Example:**

```
Device(config-pnp-init)# backup transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1
```

**Step 7**

`end`

**Example:**

```
Device(config-pnp-init)# end
```

Exits the PnP profile initialization mode and returns to privileged EXEC mode.

---

**Configuring Backup Cisco Network Plug and Play HTTPS Transport Profile**

Perform the following task to create a backup HTTPS transport profile of the Cisco Network Plug and Play agent manually on a device.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`
| Example:
| `Device>` enable |
| Enables privileged EXEC mode. |
| • Enter your password if prompted. |
| **Step 2**
| `configure terminal`
| Example:
| `Device# configure terminal`
| Enters global configuration mode. |
| **Step 3**
| `pnp profile profile-name`
| Example:
| `Device(config)# pnp profile test-profile-1`
| Creates a PnP agent profile and enters the PnP profile initialization mode. |
| • String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4**
| `backup transport https host host-name [port port-number ] [source interface-type ] [localcert trustpoint-name ] [remotecert trustpoint-name ]`
| Example:
| `Device(config-pnp-init)# backup transport https`
| Creates a HTTPS backup transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed. |
| • The value of `localcert` specifies the trustpoint used for client-side authentication during the transport layer security (TLS) handshake. |
## Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz</td>
<td>The value of remotecert specifies the trustpoint used for server certificate validation.</td>
</tr>
</tbody>
</table>

### Step 5

**backup transport https ipv4 ipv4-address [port port-number | [source interface-type interface-number | [localcert trustpoint-name ] [remotecert trustpoint-name ]

**Example:**

Device(config-pnp-init)# backup transport https ipv4 10.0.0.1 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz

### Step 6

**backup transport https ipv6 ipv6-address [port port-number | [source interface-type interface-number | [localcert trustpoint-name ] [remotecert trustpoint-name ]

**Example:**

Device(config-pnp-init)# backup transport https ipv6 2001:DB8::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz

### Step 7

**end

**Example:**

Device(config-pnp-init)# end

## Configuring Cisco Network Plug and Play Agent Tag

Perform the following task to create a Cisco Network Plug and Play agent tag information:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<p>| <strong>Step 2</strong> configure terminal | Enters global configuration mode.                                                          |
| <strong>Example:</strong>               |                                                                                             |
| Device# configure terminal |                                                                                             |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3**  
**pnp tag** *tag-name*  
**Example:**  
Device(config)# pnp tag xyz | Use the `pnp tag` command to configure the tag for the device. The neighboring Cisco devices will receive this tag information through Cisco Discovery Protocol (CDP).  
**Note**  
If there is an existing tag for the device, the tag name can be only changed when the xml schema is sent by the PnP server to change the tag name. The tag name cannot be overwritten.  
- String of alphanumeric characters that specify a name for the PnP agent tag. |
| **Step 4**  
**end**  
**Example:**  
Device(config)# end | Exits the global configuration mode and returns to privileged EXEC mode. |

## Troubleshooting and Debugging

To run the debugging on the Cisco Network Plug and Play (server, start the server, configure the PnP profile and PnP transport. For example, start the service interaction between PnP agent and PnP server.

You can capture the debugs by executing the `debug pnp service` command. When you report a problem, collect all the pnp* files in the PnP agent flash” to the guide.

**Note**

To collect Cisco Plug and Play server log, see the [Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide](#).

To troubleshoot the device, server and Cisco PnP Agent, use the following commands:

### Table 9: Troubleshooting the Device, Server, and Cisco PnP Agent

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir nvram</code></td>
<td>Use this command to ensure that the device does not have left over certificates.</td>
</tr>
<tr>
<td><code>ping vrf interface-name &lt;controller_ip&gt;</code></td>
<td>Use this command to ensure that the device can ping the controller.</td>
</tr>
<tr>
<td><code>show auto install trace</code></td>
<td>Use this command to view auto install trace log.</td>
</tr>
<tr>
<td><code>show boot</code></td>
<td>Use the show boot command to display the current value for the BOOTLDR variable.</td>
</tr>
<tr>
<td><code>show cdp neighbor</code></td>
<td>Use this command to display all CDP neighbors.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show crypto pki trustpoint</td>
<td>Use this command to view the PKI trustpoint.</td>
</tr>
<tr>
<td>show crypto pki trustful</td>
<td>Use this command to view the PKI trustful.</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Use this command to view a summary of the router interfaces.</td>
</tr>
<tr>
<td>show ipv6 interface brief</td>
<td>Use this command to display the IPv6 interfaces.</td>
</tr>
<tr>
<td>show run</td>
<td>inc pnp</td>
</tr>
<tr>
<td>show pnp trace</td>
<td>Use this command to ensure that the device does not have start-up configuration.</td>
</tr>
<tr>
<td>show pnp tech</td>
<td>Use this command to view active connections for the Cisco Plug and Play IOS Agent.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Use this command to view the VLAN information.</td>
</tr>
<tr>
<td>show ntp status</td>
<td>Use this command to view the NTP status.</td>
</tr>
<tr>
<td>show version</td>
<td>Use this command to ensure that the device is running the latest CCO image</td>
</tr>
</tbody>
</table>

**Glossary**

**PnP Agent:** An embedded agent on the device to automate deployment process

**PnP Helper Applications:** Applications on smart phones and personal computers that facilitate deployment. PnP helper applications are not specific to a customer or device and can be used in any deployment scenario. May be needed in limited scenarios

**PnP Protocol:** Protocol between the PnP agent and PnP server. This is an open protocol allowing third-party development of PnP servers

**PnP Server:** A central server that manages and distributes deployment information (images, configurations, files, and licenses) for the devices being deployed. Cisco Network Plug and Play server provides a north bound interface for management applications and communicates with the PnP agents on the devices using the PnP protocol.

**Additional References for Open Plug-n-Play Agent**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PnP commands: Complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS PnP Command Reference</td>
</tr>
<tr>
<td>How to use the Cisco Network Plug and Play in the APIC-EM to configure Cisco network devices.</td>
<td>Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM.</td>
</tr>
<tr>
<td>How to deploy the APIC-EM.</td>
<td>Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide.</td>
</tr>
<tr>
<td>Getting started with the APIC-EM.</td>
<td>Cisco APIC-EM Quick Start Guide.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-BULK-FILE-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td>• CISCO-DATA-COLLECTION-MIB</td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-PROCESS-MIB</td>
<td></td>
</tr>
<tr>
<td>• Expression-MIB</td>
<td></td>
</tr>
</tbody>
</table>
Additional References for Open Plug-n-Play Agent

Cisco Network Plug and Play Agent

Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide
Software Maintenance Upgrade (SMU) Overview

The Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or security resolution to a released image for a specific defect in order to respond to immediate issues. It does not contain new features.

Some of the caveats of the SMU are:

- Provided on a per release, per component basis and is specific to the platform. SMU versions are synchronized to the package major, minor, and maintenance versions they upgrade.
- SMUs are not an alternative to maintenance releases. All defects fixed by SMUs are then automatically integrated into the upcoming maintenance releases.
- The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install non-compatible SMUs. This is based on rules/limitations for a SMU change-set.
- An SMU provides a significant benefit over classic IOS software as it allows you to address the network issue quickly while reducing the time and scope of the testing required.
- SMU is a method to fix bugs in an existing release, and allows the application of a PSIRT fix in an existing release
- SMU is NOT an upgrade path from release X to maintenance release X.1
- SMU is NOT an upgrade path from release X to release Y

The device only supports “Hot Patching”. This means:

- The running image is modified in-place or in-service
- This avoids downtime and interruption of service
- The updated code to fix the defect is written in a different location, and where the patch redirects the program run
SMU Work-flow and Basic Requirements

The work-flow for the patch requires that you complete the following sequence of operation in exec mode:

1. Addition of the SMU to the file system
2. Activation of the SMU onto the system
3. Committing the SMU change
4. Removal and Uninstallation of the SMU

The basic requirements for SMU are:

- The image where the defect was discovered
- The patch file that contains the fix for the defect must be formatted as
  ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin

SMU Example

This section shows an example of a patch for the CDET CSCvk58743.

Command example:

Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface g0/0/0
Router(config-if)# ipv6 nd cache expire 770
Router(config-if)# end
Router#
*Sep 25 12:00:29.978: %SYS-5-CONFIG_I: Configured from console by console

As the following CDET states, the ND Cache expire timer did not appear in the command output of show ipv6 neighbors g0/0/0

- CSCvk58743

Summary: Show ipv6 interface does not display "ND Cache expire timer"

Component: ipv6

Defective Image: ir1101-universalk9.16.11.01.SPA.bin

Patch Image: ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin

The following is what the required configuration output should look like:

Interface GigabitEthernet0/0/0
   no switchport
   no ip address
   ipv6 address FE80::1 link-local
   ipv6 address 2001::1/64
   ipv6 nd na glean
   ipv6 nd cache expire 770

end
In the above output, the blue text configures the length of time before an IPv6 neighbor discovery cache entry expires. The range is from 1 to 65536 seconds.

## Installing a Patch Image

Perform the following steps to install the patch image:

### Step 1
Add the image.

```
Router# install add file flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
install_add: START Mon Dec 17 21:11:23 UTC 2018
install_add: Adding SMU
*Dec 17 21:11:26.241: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install add
flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin--- Starting SMU Add operation ---
Performing SMU_ADD on Active/Standby
 [R0] SMU_ADD package(s) on R0
 [R0] Finished SMU_ADD on R0
Checking status of SMU_ADD on [R0]
SMU_ADD: Passed on [R0]
Finished SMU Add operation
SUCCESS: install_add Mon Dec 17 21:11:39 UTC 2018
```

### Step 2
Activate the patch image.

```
Router# install activate file flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
install_activate: START Mon Dec 17 21:11:57 UTC 2018
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK] Modified configuration has been saved
*Dec 17 21:12:02.086: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config
fileinstall_activate: Activating SMU
*Dec 17 21:12:05.339: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install activate
flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on Active/Standby
 [R0] SMU_ACTIVATE package(s) on R0
 [R0] Finished SMU_ACTIVATE on R0
Checking status of SMU_ACTIVATE on [R0]
SMU_ACTIVATE: Passed on [R0]
Finished SMU Activate operation
SUCCESS: install_activate /flash1/ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin Mon Dec 17 21:12:26 UTC 2018
*Dec 17 21:12:25.463: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install auto abort timer will expire in 7200 seconds
*Dec 17 21:12:27.358: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install activate SMU flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
```

### Step 3
Commit the installation.

```
Router# install commit
install_commit: START Mon Dec 17 21:13:28 UTC 2018
install_commit: Committing SMU
```
Step 4
Show the status summary of the installation procedure.

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted, C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU  C    /flash1/ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
IMG  C    16.11.1.0.4
--------------------------------------------------------------------------------
Auto abort timer: inactive

Uninstalling the Patch Image

There are two methods to remove or uninstall the patch image.

• Restoring the image to its original version by using the following command:
  • install rollback to base

• Specific removal of a patch by using the following commands in sequence:
  • install deactivate file flash:ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin
  • install commit
  • install remove file flash:ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin

Uninstalling the Patch Image Using Rollback

This section shows an example of using the rollback method.

Show what patches are installed:

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted, 
C - Activated & Committed, D - Deactivated & Uncommitted

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMU</td>
<td>C</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.12.02.0.6</td>
</tr>
</tbody>
</table>

The following commands are available:

Router# install ?
abort             Abort the current install operation
activate          Activate an installed package
add               Install a package file to the system
auto-abort-timer  Install auto-abort-timer
commit            Commit the changes to the loadpath
deactivate        Deactivate an install package
label             Add a label name to any installation point
prepare           Prepare package for operation
remove            Remove installed packages
rollback          Rollback to a previous installation point

Router# install rollback to ?
base       Rollback to the base image
committed  Rollback to the last committed installation point
id         Rollback to a specific install point id
label      Rollback to a specific install point label

The install rollback to base command removes the entire patch and returns to the base image version with the found defect.

Router# install rollback to base
install_rollback: START Fri Apr 24 22:58:25 UTC 2020

*Apr 24 22:58:28.375: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install rollbackinstall_rollback: Rolling back SMU
Executing pre scripts....
Executing pre scripts done.

--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on Active/Standby
[R0] SMU_ROLLBACK package(s) on R0
[R0] Finished SMU_ROLLBACK on R0
Checking status of SMU_ROLLBACK on [R0]
SMU_ROLLBACK: Passed on [R0]
Finished SMU Rollback operation


*Apr 24 22:58:55.368: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install rollback

Show what patches are installed:

Router# show install summary

[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted, 
C - Activated & Committed, D - Deactivated & Uncommitted

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.12.02.0.6</td>
</tr>
</tbody>
</table>
Uninstalling the Patch Image Using Deactivate, Commit, and Remove

In the following sequence, there are two patches installed on the device. Only one will be removed.

Show what patches are installed.

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMU</td>
<td>C</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin</td>
</tr>
<tr>
<td>SMU</td>
<td>D</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.12.02.0.6</td>
</tr>
</tbody>
</table>

Step 1  Deactivate the patch.

Router# install deactivate file flash:/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
install_deactivate: START Fri Apr 24 22:54:10 UTC 2020
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre scripts done.

--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
 [R0] SMU_DEACTIVATE package(s) on R0
 [R0] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation

SUCCESS: install_deactivate /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin Fri Apr 24
22:54:49 UTC 2020

Show what patches are installed:

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMU</td>
<td>C</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin</td>
</tr>
<tr>
<td>SMU</td>
<td>D</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.12.02.0.6</td>
</tr>
</tbody>
</table>

Step 2  Commit the action.
Router# install commit
install_commit: START Fri Apr 24 22:56:11 UTC 2020
install_commit: Committing SMU

*Apr 24 22:56:15.169: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install commit
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on Active/Standby
[R0] SMU_COMMIT package(s) on R0
[R0] Finished SMU_COMMIT on R0
Checking status of SMU_COMMIT on [R0]
SMU_COMMIT: Passed on [R0]
Finished SMU Commit operation


*Apr 24 22:56:33.342: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install commit SMU

Show what patches are installed:

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
SMU   I    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
IMG   C    16.12.02.0.6
--------------------------------------------------------------------------------

Step 3
Remove the patch.

Router# install remove file flash:ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
install_remove: START Fri Apr 24 22:57:17 UTC 2020

*Apr 24 22:57:20.775: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install remove
flash:ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bininstall_remove: Removing SMU
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Remove operation ---
Performing SMU_REMOVE on Active/Standby
[R0] SMU_REMOVE package(s) on R0
[R0] Finished SMU_REMOVE on R0
Checking status of SMU_REMOVE on [R0]
SMU_REMOVE: Passed on [R0]
Finished SMU Remove operation


*Apr 24 22:57:34.902: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install remove flash:ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin

Show what patches are installed:

Router# show install summary
Uninstalling the Patch Image Using Deactivate, Commit, and Remove

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMU</td>
<td>C</td>
<td>/flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.12.02.0.6</td>
</tr>
</tbody>
</table>

Note in the above command output the patch for CDET CSCvt63576 has been removed, while the patch for CDET CSCvq74407 remains.
Smart Licensing Using Policy (SLP)

This chapter contains the following sections:

- SLP Overview, on page 173
- Customer Topologies, on page 175
- License Installation Procedure - Full Offline Access Topology, on page 176
- License Installation Procedure - CSLU has No Access to CSSM, on page 181
- Removing the Device from CSSM, on page 192

SLP Overview

Smart Licensing Using Policy (SLP), was previously referred to as Smart Licensing Enhanced (SLE), and is the default mode starting with IOS-XE release 17.3.2. SLE replaced Smart Software Licensing. The IR1101 only supports SLP. Some of the feature differences are:

- An Authorization Code is required only for export control requirement
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.
- Throughput is defaulted and capped at 250MB.

Important

Examples used throughout the rest of this section show the ESR6300 Router. The IR1101 functions in the same manner, with the exception of not supporting the higher throughput license.

License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced
The vast majority of licenses belong to this enforcement type. Unenforced licenses do not require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

- **Enforced**
  Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

  An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Industrial Ethernet Switches.

- **Export-Controlled**
  Licenses that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

  An example of an export-controlled license is the High Security (HSEC) license, which is available on certain Cisco Routers.

### SLP Architecture

This section explains the various components that can be part of your SLP implementation.

#### Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. The RUM reports and usage data are also stored securely in the product instance.

#### Cisco Smart Software Manager (CSSM)

CSSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access CSSM at [https://software.cisco.com](https://software.cisco.com). Under the License tab, click the Smart Software Licensing link.

In CSSM you can:

- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.


Click on the View Video button.
Cisco Smart Licensing Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing work-flows. It helps you administer all your licenses and their associated product instances from your premises instead of having to connect to CSSM.

This utility performs the following key functions:

• Provides the options relating to how work-flows are triggered. The work-flows can be triggered by CSLU or by the product instance

• Collects usage reports from the product instance and upload these usage reports to the corresponding smart account or virtual account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and provided back to the product instance.

• Sends authorization code requests to CSSM and receives authorization codes from CSSM.

CSLU can be part of your SLP topology in the following ways:

• Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.

• Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.

• Embed it in a controller such as Cisco DNA Center.

Customer Topologies

IoT Routing platforms use two different topologies.

• Full Offline Access

• CSLU has No Access to CSSM

The following figure illustrates the Full Offline Access:

In this topology, devices do not have connectivity to CSSM (software.cisco.com). The user must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

The following figure illustrates the CSLU having No Access to CSSM:
In this topology the devices are connected to the CSLU controller, but there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com).

Cisco devices will send usage information to a locally installed CSLU. The user must copy and paste information between the CSLU and CSSM to manually check-in and check-out licenses.

**License Installation Procedure - Full Offline Access Topology**

This procedure requires a manual exchange of required information between the router and CSSM.

Refer to the following graphic for the flow of information:

1. Generate a License Usage Data file or AuthCode Request.
2. Export to CSSM.
3. Upload License Usage Data or AuthCode Request.
4. Export ACK/AuthRequest file to Router.
5. Upload ACK file or AuthRequestAuthCode

**Procedure to Register Product Instance in CSSM**

**Step 1**
Generate a license usage file from the Router.

In exec mode, perform the following:

**Example:**

```
Router# license smart save usage all file flash:slp
```

**Step 2**
Export the license usage file (slp) to your host laptop/PC.

**Step 3**
Importing the license usage file to CSSM on Cloud. Click on the Usage Data Files tab.
Step 4  The **Upload Usage Data** window appears. Click **Browse**, and navigate to where the file is.

Step 5  Click on **Upload Data**.

Step 6  Select the Virtual Account.
Step 7

From the pull-down, select your respective virtual account.

Step 8

Click Ok.

Step 9

Observe the Smart Software Licensing window. Initially, the Reporting Status state will be Pending. Wait until the window reflects No Errors before continuing.

Figure 63: Select Account

Figure 64: Select Your Account

Figure 65: Reporting Status
Step 10 Click **Download** to download the ACK file.

Step 11 Check under the **Product Instances** tab to verify your device is listed.

*Figure 66: Product Instances*

![Image of Product Instances]

Step 12 Import the ACK file from CSSM to your device using the command line interface.

## Importing the ACK file from CSSM to your Device

### Step 1
Copy the ACK file from CSSM to your host laptop or usbflash device. In exec mode on the device:

**Example:**

```
Router# license smart import <flash: | usbflash0:> ACK_slp
Import Data Successful
```

### Step 2
Verify Product Instance has imported the data

**Example:**

```
Router# show license usage
License Authorization:
    Status: Not Applicable
network-advantage_250M (ESR6300_P_250M_A):
    Description: network-advantage_250M
    Count: 1
    Version: 1.0
    Status: IN USE
    Export status: NOT RESTRICTED
    Feature Name: network-advantage_250M
    Feature Description: network-advantage_250M
    Enforcement type: NOT ENFORCED
```

### Step 3
Verify the license is in use.

**Example:**

```
Router# show license summary
```
Removing the Device from CSSM

Step 1

Navigate back to the product instances tab. Locate your device.

Figure 67: Product Instances

Step 2

Click on Actions beside your device, and from those options click Remove.

The Confirm Remove Product Instance window appears.

Figure 68: Confirm Remove Product Instance
Step 3: Click Remove Product Instance.

License Installation Procedure - CSLU has No Access to CSSM

This procedure performs an online exchange of required information between the Router and CSLU. Refer to the following graphic for the flow of information:

---

Procedure when devices are connected to the CSLU

First, perform these steps on the router using the CLI to get a license UDI:

```bash
Router#show license summary
License Reservation is ENABLED License Usage:
License Entitlement tag Count Status
coreadvantage_250M (ESR6300 _P_250M_A) 1 IN USE

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!

Router(config)#end
Router#sh license udi
UDI: PID:ESR-6300-CON-K9,SN:FOC23032UVB
```

---

Step 1: Open the Cisco Smart License Utility (CSLU).
Step 2: Navigate to the **Product Instances** tab, then click on the UDI.
Procedure when devices are connected to the CSLU

**Step 3** The Edit Single Product Instance window appears.

**Step 4** The Edit Multiple Devices window appears. Supply your account password and click Save.
Step 5  In the Product Instances window, click on the Actions for Selected Devices Tab.


Step 7  The Authorization Request Information window appears. Read the contents and then click Accept.
Figure 73: Authorization Request Information

Authorization Request Information

This operation will download an authorization request file for the devices that have been selected. Once this file is downloaded please:
1. Upload the file to CSSM.
2. After uploading to CSSM you will be able to download the file containing the authorization codes for devices you selected.
3. Please upload this file using the “Upload From CSSM” menu option to apply the authorization codes for the devices.

Accept  Cancel

Step 8  The CSLU downloads a Authorization Request file to your laptop. Click Save.

Figure 74: Authorization Request File

Exporting the AuthRequest File to CSSM

The next step is to take the Authorization Request file you just saved, and export it into Cisco Smart Software Manager (CSSM).

Launch CSSM.

Click on the Inventory Tab, select your Virtual Account.
**Step 1**  
Click on the **Product Instances** Tab.

**Step 2**  
Click on **Authorize License-Enforced Features**.

*Figure 75: Authorize License-Enforced Features*

The **Authorize License-Enforced Features** window appears.

*Figure 76: Authorize License-Enforced Features*

**Step 3**  
Choose **Multiple** or **Single** devices from the pull-down.

**Step 4**  
The window changes to an option to select a device file. Click on **Choose File**.
Step 5  
A popup window opens to navigate to where you saved your Authorization Request file on your laptop.

*Figure 77: Open File Navigation Window*

Step 6  
Select your file, and then click **Open**.

Step 7  
The authorization file loads, and the window changes to present your devices.
Step 8 When successful, click **Next**.

Step 9 The **Select Licenses** Tab opens.

Step 10 Under **Quantity per Device**, enter the number you wish.
Step 11  If CSSM cannot identify your device from the identifying information, you can select it manually.

Step 12  Click **Continue**, and the window changes to **Review and Confirm**.
Step 13  Click on Reserve Licenses, and CSSM generates feature authorization codes.

Step 14  Click Download Authorization Codes, and a window opens to navigate to where you wish to save the codes.
Step 15 Click Ok.

Uploading the Authorization Request Code file into CSLU

Step 1 Open the Cisco Smart License Utility (CSLU).
Step 2 Navigate to Product Instances, and then select Upload From Cisco.
Step 3  There are two options to load your file. Drag and Drop, or Browse to where you saved your file. This example shows Browse.

Figure 86: Browse to File

Step 4  Select your authorization code file, and then click Open. The system uploads the authorization code file, then a successful upload message appears.

Figure 87: Successful Upload

License Installation Process in the Router

Perform the following from the command line interface.

Router#show license summary
License Reservation is ENABLED
License Usage:
  License Entitlement tag Count Status
Removing the Device from CSSM

Step 1  Navigate back to the product instances tab. Locate your device.

Figure 88: Product Instances
Step 2  Click on **Actions** beside your device, and from those options click **Remove**.

The Confirm Remove Product Instance window appears.

*Figure 89: Confirm Remove Product Instance*

Step 3  Click **Remove Product Instance**.
Removing the Device from CSSM
Configuring VLANs

A VLAN is a switched network that is logically segmented by function or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs. However, you can group end-stations even if they are not physically located on the same LAN segment. Any device port can belong to a VLAN, unicast, broadcast, and multicast packets are forwarded and flooded only to end-stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a device supporting fallback bridging. In a device stack, VLANs can be formed with ports across the stack. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the device is assigned manually on an interface-by-interface basis. When you assign device interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

The device can route traffic between VLANs by using device virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

Trunk Ports
A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. These trunk port types are supported:

- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

For more information on VLANs, see VLAN Configuration Guide, Cisco IOS XE Gibraltar 16.10.x.

### VLAN Trunking Protocol (VTP)

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.


### Configuring IEEE 802.1X Port-Based Authentication

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built-in switch ports or a plug-in module with switch ports. This feature supports both access ports and trunk ports. For more information on 802.1X port-based authentication, see the Configuring IEEE 802.1X Port-Based Authentication Guide.
Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- **Root**—A forwarding port elected for the spanning-tree topology
- **Designated**—A forwarding port elected for every switched LAN segment
- **Alternate**—A blocked port providing an alternate path to the root bridge in the spanning tree
- **Backup**—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch. Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

For detailed configuration information on STP see the following link:


Example: Spanning Tree Protocol Configuration

The following example shows configuring spanning-tree port priority of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses the port priority when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

The following example shows how to change the spanning-tree port cost of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state.

Configuring MAC Address Table Manipulation

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use. You can use the aging time setting to define how long the switch retains unseen addresses in the table.

- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port associated with the address and the type (static or dynamic).

See the “Example: MAC Address Table Manipulation” for sample configurations for enabling secure MAC address, creating a static entry, set the maximum number of secure MAC addresses and set the aging time.

For detailed configuration information on MAC address table manipulation see the following link:
Example: MAC Address Table Manipulation
The following example shows creating a static entry in the MAC address table.

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface FastEthernet 0/0/1 vlan 3
Router(config)# end
```

The following example shows setting the aging timer.

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

---

**Configuring Switch Port Analyzer**

The Cisco IR1101 supports local SPAN only, and up to one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source can be monitored by using SPAN; traffic routed to a source cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another source cannot be monitored; however, traffic that is received on the source and routed to another can be monitored.

For detailed information on how to configure a switched port analyzer (SPAN) session, see the following web link:


Example: SPAN Configuration
The following example shows how to configure a SPAN session to monitor bidirectional traffic from a Gigabit Ethernet source interface:

```
Router# configure terminal
Router(config)# monitor session 1 source FastEthernet 0/0/1
Router(config)# end
```

The following example shows how to configure a gigabit ethernet interface as the destination for a SPAN session:

```
Router# configure terminal
Router(config)# monitor session 1 destination FastEthernet 0/0/1
Router(config)# end
```

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:
IGMP Snooping for IPv4

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients. For more information on this feature, see https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/snooigmp.html.
Cisco Fourth-Generation LTE Advanced on the Cisco Catalyst IR1101 Rugged Series Router


The IR1101 offers LTE support through the use of Pluggable Modules. You can find a list of the supported Pluggable Modules in the Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide.

Cisco LTE Pluggable Module support the following 4G/3G modes:

- **4G LTE**—4G LTE mobile specification provides multi-megabit bandwidth, more efficient radio network, latency reduction, and improved mobility. LTE solutions target new cellular networks. These networks
initially support up to 100 Mb/s peak rates in the downlink and up to 50 Mb/s peak rates in the uplink. The throughput of these networks is higher than the existing 3G networks.

- **3G Evolution High-Speed Packet Access (HSPA/HSPA+)**—HSPA is a UMTS-based 3G network. It supports High-Speed Downlink Packet Access (HSDPA) and High-Speed Uplink Packet Access (HSUPA) data for improved download and upload speeds. Evolution High-Speed Packet Access (HSPA+) supports Multiple Input/Multiple Output (MIMO) antenna capability.

- **3G Evolution-Data Optimized (EVDO or DOReA) Mode**—EVDO is a 3G telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. DOReA refers to EVDO Rev-A. EVDO uses multiplexing techniques including Code Division Multiple Access (CDMA), as well as Time Division Multiple Access (TDMA), to maximize both individual users' throughput and the overall system throughput.

It is important to understand the architecture of the IR1101 series and the relationship between Modems, SIMs, Interface and Controller. The following table helps to illustrate these relationships.

<table>
<thead>
<tr>
<th>Router</th>
<th>Controller</th>
<th>SIM</th>
<th>Modem SubSlot</th>
<th>PDN Interface</th>
<th>Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101</td>
<td>0/1/0</td>
<td>0/1</td>
<td>0/1</td>
<td>Cellular 0/1/0</td>
<td>N/A</td>
</tr>
<tr>
<td>IR1101 with Expansion Module</td>
<td>0/3/0</td>
<td>0/1</td>
<td>0/3</td>
<td>Cellular 0/3/0</td>
<td>N/A</td>
</tr>
</tbody>
</table>


### Prerequisites for Configuring Cisco 4G LTE Advanced

- If the signal is not good at the router, use the Cisco offered antenna accessories and extension cables to place the antenna away from router in a better coverage area. Please refer to the RSSI/SNT values as displayed through `show cellular 0/1/0 all` or the LED of the pluggable modem.

- You must have 4G LTE network coverage where your router is physically placed. For a complete list of supported carriers.

- You must subscribe to a service plan with a wireless service provider and obtain a Subscriber Identity Module (SIM) card. Only micro SIM is supported.

- You must install the SIM card before configuring the 4G LTE or router.

- The standalone antenna that supports GPS capabilities must be installed for the GPS feature to work.

### Restrictions for Configuring Cisco 4G LTE Advanced

- Currently, cellular networks support only user initiated bearer establishment.
• Due to the shared nature of wireless communications, the experienced throughput varies depending on
the number of active users or congestion in a given network.

• Cellular bandwidth is asymmetric with the downlink data rate being greater than the uplink data rate.

• Cellular networks have higher latency compared to wired networks. Latency rates depend on the
technology and carrier. Latency also depends on the signal conditions and can be higher because of
network congestion.

• CDMA-EVDO, CDMA-1xRTT, and GPRS technology modes are not supported.

• Any restrictions that are part of the terms of service from your carrier.

• SMS—Only one text message up to 160 characters to one recipient at a time is supported. Larger texts
are automatically truncated to the proper size before being sent.

• It is strongly recommended that you configure SNMP V3 with authentication/privacy.

**Features not Supported in 4G LTE Advanced**

The following features are not supported on Cisco 4G LTE Advanced on the IR1101, when compared to
Classic IOS:

• TTY support or Line

• Chat script/dialer string

• DM log output to USB flash is not supported.

**4G LTE-Advanced LEDs**

LED status can be obtained through the show led CLI, or visually on the pluggable modem card. The following
is an example of the show led CLI:

IR1101#show led
SYSTEM LED : Green
Custom LED : Off
VPN LED : Off
ALARM LED : Off
GigabitEthernet0/0/0 LED : Off
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off
GigabitEthernet0/0/5 LED : On
EM Module digital I/O 1 LED : Off
EM Module digital I/O 2 LED : Off
EM Module digital I/O 3 LED : Off
EM Module digital I/O 4 LED : Off

*System LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On

*EM Module LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On

The following table describes the LED behavior in 4G LTE-Advanced.

<table>
<thead>
<tr>
<th>LED</th>
<th>Color/Bar and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTE SIM(0) &amp; SIM(1)</td>
<td>Green (Solid) Modem up, SIM installed and active</td>
</tr>
<tr>
<td></td>
<td>Off No SIM is present</td>
</tr>
<tr>
<td></td>
<td>Amber (Solid) Modem up, SIM installed but not active</td>
</tr>
<tr>
<td>EN</td>
<td>Off Pluggable is powered off.</td>
</tr>
<tr>
<td></td>
<td>Amber (Solid) Module power is on, but the module is not functioning correctly.</td>
</tr>
<tr>
<td></td>
<td>Green (Solid) Module power is on</td>
</tr>
<tr>
<td>RSSI - Uses Bars for LED Indication</td>
<td>Four Bar High RSSI &gt;= -69dBm</td>
</tr>
<tr>
<td></td>
<td>Three Bar Medium RSSI, -89dBm &lt;= -70dBm</td>
</tr>
<tr>
<td></td>
<td>Two Bar Low RSSI, -99dBm &lt;= -90dBm</td>
</tr>
<tr>
<td></td>
<td>One Bar RSSI &lt;= -100dBm</td>
</tr>
<tr>
<td></td>
<td>0 or No Bar No Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Green (Solid) GPS coordinates are obtained.</td>
</tr>
<tr>
<td></td>
<td>Off GPS is disabled, GPS is enabled without GPS mode and NMEA configuration, or GPS is acquiring</td>
</tr>
</tbody>
</table>
Cisco 4G LTE-Advanced Features

Cisco 4G LTE-Advanced supports the following major features:

- Global Navigation Satellite System (GNSS) (requires a GNSS compliant antenna) and National Marine Electronics Association (NMEA) streaming.
- Short Message Service (SMS)
- 3G/4G Simple Network Management Protocol (SNMP) MIB
- SIM lock and unlock capabilities
- Dual SIM (Only SIM slot 0 is functional on the P-LTE-VZ pluggable)
- Auto SIM
- NeMo
- Mobile Network IPv6
- Public Land Mobile Network (PLMN) selection
- IPv6
- Multiple PDN
- LTE Link Recovery

4G GNSS and NMEA

Active GNSS is supported on the SubMiniature version A (SMA) port. Active GNSS antenna is supported only in the standalone mode. An Active GNSS antenna includes a built-in Low-Noise Amplifier that provides sufficient gain to overcome coaxial cable losses while providing the proper signal level to the GNSS receiver. Active GNSS antennae require power from the GNSS receiver SMA port to operate.

National Marine Electronics Association (NMEA) streams GNSS data either from a 4G LTE through a virtual COM port and a TCP/IP Ethernet connection to any marine device (such as a Windows-based PC) that runs a commercially available GNSS-based application.

The following GNSS and NMEA features are supported on the Cisco 4G LTE-Advanced:

- GNSS standalone mode (satellite-based GNSS)
- Cisco IOS-XE CLI display coordinates.
- External application displays router map location
- Objects in the CISCO-WAN-3G-MIB supports GNSS and NMEA features
- The Cisco 4G LTE-Advanced only support NMEA over IP and uses show commands in the platform

Note

Assisted GNSS mode is not supported.
Example: Connecting to a Server Hosting a GPS Application

You can feed the NMEA data to a remote server that hosts the GPS application. The server can be connected to the router either directly using an Ethernet cable or through a LAN or WAN network. If the application supports serial port, run a serial port emulation program to create a virtual serial port over the LAN or WAN connection.

**Note**
Microsoft Streets & Trips is a licensed software that you can download from the Microsoft website.

To connect a Cisco 4G LTE-Advanced through IP to a PC running Microsoft Streets & Trips, perform the following steps:

1. Connect the PC to the router using an Ethernet cable.
2. Ensure that the PC and router can ping.
3. Launch the serial port redirector on the PC.
4. Create a virtual serial port that connects to the NMEA port on the router.
5. Launch **Microsoft Streets & Trips** on your PC.
6. Select the GPS Menu.
7. Click Start Tracking.
8. If you have acquired a location fix from the `show cellular 0/1/0 gps` command output on the router, the current location is plotted on the graph, and a reddish brown dotted cursor with a circle around it is seen on the map.

**Note**
If you have not acquired a location fix, the Microsoft application times out and disconnects.

### Dual SIM Card

**Note**
The P-LTE-VZ pluggable which supports Verizon is a single SIM.

SIM card primary slot is selected when router boots up or when NIM reloads. The default slot is 0. If SIM card is not present in the primary slot, select the alternative slot if SIM card is present.

```
controller cellular 0/1/0
lte sim primary slot <slot#>
```

If the active SIM card loses connectivity to the network a failover to the alternative SIM card slot occurs. By default the failover timer is 3 minutes. The failover timer can be set from 3 to 7 minutes.

```
controller cellular 0/1/0
lte failovertimer <3-7>
```
You can also manually switch the SIM slot via the command line interface.

```
cellular 0/1/0 lte sim activate slot <0-1>
```

### Auto SIM

The Auto SIM feature detects the SIM and loads the corresponding firmware. For example, if an AT&T SIM is detected, the modem loads the AT&T firmware.

When Auto-SIM is enabled, it is said to be in Auto-SIM mode and when disabled, it is known as Manual mode. In Auto-SIM mode, the modem selects the right carrier firmware from the list of firmware's available. When in manual mode, you can select the firmware manually. Modem resets every time you make a config change from Auto-SIM enabled to disabled or vice-versa.

The P-LTE-US and P-LTE-GB pluggable modules on the IR1101 support Auto SIM.

---

**Note**

Auto SIM is always enabled by default.

### Enable Auto SIM

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  configure terminal
  **Example:**
  `Router# configure terminal`
| Enters configuration mode. |
| **Step 2**
  cellular slots/sub-slots/interface lte firmware-activate firmware-index
  **Example:**
  `Router(config)# cellular 0/1/0 lte firmware-activate 1`
| Activates the firmware index.  
**Note** For the 4G LTE Advanced, the *unit* argument identifies the slot, subslot, and the interface separated by slashes (0/1/0). |

### Example: List the firmware when Auto-SIM is Enabled

```
Device# show cellular 0/1/0

<table>
<thead>
<tr>
<th>firmware</th>
<th>Idx Carrier</th>
<th>FwVersion</th>
<th>PriVersion</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATT</td>
<td>02.28.00.00</td>
<td>002.035_000</td>
<td>002.035_000</td>
<td>Inactive</td>
</tr>
<tr>
<td>GENERIC</td>
<td>02.28.00.00</td>
<td>002.035_000</td>
<td>001.012_000</td>
<td>Active</td>
</tr>
<tr>
<td>ROGERS</td>
<td>02.28.00.00</td>
<td>001.012_000</td>
<td>002.012_000</td>
<td>Inactive</td>
</tr>
<tr>
<td>SPRINT</td>
<td>02.14.03.02</td>
<td>002.012_000</td>
<td>002.012_000</td>
<td>Inactive</td>
</tr>
<tr>
<td>VERIZON</td>
<td>02.28.00.00</td>
<td>002.042_000</td>
<td>002.042_000</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

Firmware Activation mode = AUTO
```
## Disable Auto SIM

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>controller cellular</code> <em>slots/sub-slots/interface</em></td>
<td>Specifies the controller interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# controller cellular 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>no lte firmware auto-sim</code></td>
<td>Disable auto SIM.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# no lte firmware auto-sim</code></td>
<td></td>
</tr>
</tbody>
</table>

### Example: List the firmware when Auto-SIM is Disabled

```plaintext
Device# show cellular 0/1/0 firmware
Idx Carrier      FWVersion    PriVersion   Status
1   ATT          02.28.00.00  002.035_000  Active
2   GENERIC      02.28.00.00  002.035_000  Inactive
3   ROGERS       02.28.00.00  001.012_000  Inactive
4   SPRINT       02.14.03.02  002.012_000  Inactive
5   VERIZON      02.28.00.00  002.042_000  Inactive
```

Firmware Activation mode = Manual

## Using a SIM Card

Cisco 4G LTE-Advanced needs an active SIM card provided by a service provider. The SIM cards are usually provided in an unlocked state so that it can be used without a Personal Identification Number (PIN). If the SIM is unlocked, it can be inserted into a 4G LTE-Advanced and used without an authorization code.

The SIM can be initially locked with a PIN code (4 to 8 digits long) defined by the service provider. Contact your service provider for the PIN code.

The SIM-Lock feature allows a SIM to be locked or unlocked with a PIN code so that it is used only in an authorized device. Perform the SIM lock and unlock procedures using the Cisco IOS CLI through a console or Telnet/SSH to the Router.

After the SIM is locked, it cannot initiate a call unless authentication is done using the same PIN. Authentication is done automatically by Cisco IOS through configuration of the PIN. This mandatory configuration for automatic SIM authentication is done using the Cisco IOS CLI as part of the router startup configuration.
After the Cisco IOS configuration is in place, the Router can initiate an LTE connection. The Router uses the configured PIN to authenticate prior to the LTE connection. If the Cisco IOS PIN configuration is missing or if the PIN is incorrect, the SIM authentication will fail and the connection will not be initiated.

If the locked SIM is moved to a different Router or to another device, or if the 4G LTE-Advanced in which the locked SIM resides is moved to a different 4G LTE-Advanced slot in the same Router, the Router configuration should be changed. The configuration is associated with the cellular controller that is specific to an Router 4G LTE-Advanced slot number. This will ensure that the SIM card will not be used in any unauthorized device, or, if there are multiple 4G LTE-Advanced in a single Router, that the appropriate PIN is applied to each 4G LTE-Advanced SIM. An authentication command (with the same PIN used to lock the SIM) must be defined on the new device or on the new cellular controller slot to successfully initiate the LTE connection.

The following procedures are used to configure a SIM:

⚠️ Caution

It is very important to use the correct PIN after it is configured. The SIM card will be blocked if the wrong PIN is entered three consecutive times on a locked SIM during authentication or when trying to unlock a locked SIM. You can unblock a blocked SIM card using the PUK code. Contact your service provider for the PUK code. Use the `cellular <slot> lte sim unblock <PUK code> <new PIN code>` command to unblock the SIM.

### Changing the PIN

Ensure to enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> cellular interface lte sim change-pin current-pin new-pin</td>
<td>Locks or unlocks the SIM card using a PIN code.</td>
</tr>
<tr>
<td><strong>Example</strong>: Router# cellular 0/1/0 lte sim lock 1111 1234</td>
<td><strong>Note</strong>: Locks or unlocks the SIM card using a PIN code. <em>pin</em>—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card.</td>
</tr>
<tr>
<td><strong>Note</strong>: SIM should be in locked state when the PIN is being changed.</td>
<td></td>
</tr>
</tbody>
</table>

### Locking and Unlocking a SIM Card Using a PIN

Perform this task to lock or unlock a SIM card given by your service provider. Make sure you enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> cellular unit lte sim {lock</td>
<td>unlock} pin</td>
</tr>
</tbody>
</table>
Configure CHV1 for Unencrypted Levels

Use either of these commands:

```plaintext
lte sim authenticate 0 pin
```
or

```plaintext
lte sim authenticate 0 pin slot {0 | 1}
```

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller cellular interface</td>
<td>Enters the cellular controller configuration mode or</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router# controller cellular 0/1/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lte sim authenticate 7 1111 slot 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure CHV1 for Unencrypted Level7

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode. When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command.

**Note**

After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration. A SIM should be locked for SIM authentication to work.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service password-encryption</td>
<td>Enables password encryption.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router (config)# service password-encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Username privilege var password pin</td>
<td>Creates username and password.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>name - specifies the username. pin — A 4 to 8 digits PIN code.</td>
<td></td>
</tr>
<tr>
<td>Router (config)# username SIM privilege 0 password 1111</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;do show run</td>
<td>i name&lt;br&gt;Example: Router(config)# do show run</td>
<td>i SIM</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;<strong>username privilege 0 password pin</strong>&lt;br&gt;Example: Router(config)# controller cellular 0/1/0</td>
<td>Enters the cellular controller configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;lte sim authenticate 7 pin OR lte sim authenticate 7 pin slot {0</td>
<td>1}&lt;br&gt;Example: Device(config-controller)# lte sim authenticate 7 055A575E70</td>
<td>Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. <strong>Note</strong> The slot keyword and its options are available only on platforms that supports Dual-SIM feature.</td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;exit&lt;br&gt;Example: Router(config-controller)# exit</td>
<td>(Optional) Exits the cellular controller configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong>&lt;br&gt;no usernamename&lt;br&gt;Example: Router(config-controller)# no username SIM</td>
<td>(Optional) Removes the username and password created in Step 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong>&lt;br&gt;no service password-encryptionname&lt;br&gt;Example: Router(config-controller)# no service password-encryption</td>
<td>(Optional) Removes the username and password created in Step 3</td>
<td></td>
</tr>
</tbody>
</table>

## Short Message Service (SMS) Capabilities

Cisco 4G LTE-Advanced support receiving, transmitting, archiving, and deleting of SMS messages. This support includes the ability to view up to 25 received texts, and archive more messages in a custom file location. SMS is supported on multiple carriers. Cisco 4G LTE-Advanced also have the capability to revert from LTE SMS to 3G technology if necessary.

A sending device behind a Cisco 4G LTE-Advanced transmits an SMS text message over the 4G cellular link through cellular towers until it the message reaches the recipient’s router, which then notifies the recipient device, such as a cell phone. The receiving device uses the same process to return a reply to the sending device. The following figure describes the flow from a mobile device to a sending device. For SMS transmission to work, end users must have a text-capable device, and optionally, a text plan. If end users do not have a text plan, standard SMS rates apply to their text transmissions.
Data Account Provisioning

One or more modem data profiles can be created to provision a modem on a 4G LTE SKU. An active wireless account with a service provider with one or more (dual) SIM cards must be installed. The modem data profile is pre-configured on the modem.

The following tasks are used to verify the signal strength and service availability of the modem and to create, modify, and delete modem data profiles:

IP Multimedia Subsystem Profiles

IP Multimedia Subsystem (IMS) profiles establish a session, and are a part of the modem configuration and are stored in the modem's NVRAM. An IMS network is an access-independent and standard-based IP connectivity service that enables different types of multimedia services to end users using common Internet-based protocols.
Configuring Cisco 4G LTE Advanced

For 4G-LTE-Advanced, the numbering on the IR1101 for slot 0, module 0, and port 0 is 0/1/0 for all commands on the base unit. On the Expansion Module, the numbering for slot 0, module 0, and port 0 is 0/3/0 for all commands.

4G modems in the Expansion Module will support the same feature set, including GPS, as supported by the same modem in the Base Module.

Verifying Modem Signal Strength and Service Availability

For the 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** show cellular *unit* network  
Example:  
Router# show cellular 0/1/0 network | Displays information about the carrier network, cell site, and available service. |
| **Step 2** show cellular *unit* radio  
Example:  
Router# show cellular 0/1/0 radio | Shows the radio signal strength.  
**Note** The RSSI should be better than –90 dBm for steady and reliable connection. |
| **Step 3** show cellular *unit* profile  
Example:  
Router# show cellular 0/1/0 profile | Shows information about the modem data profiles created. |
| **Step 4** show cellular *unit* security  
Example:  
Router# show cellular 0/1/0 security | Shows the security information for the modem, such as SIM and modem lock status. |
| **Step 5** show cellular *unit* all  
Example:  
Router# show cellular 0/1/0 all | Shows consolidated information about the modem, profiles created, radio signal strength, network security, and so on. |

Guidelines for Creating, Modifying, or Deleting Modem Data Profiles

Customized profiles (Access Point Name(APN) in mobile networks) can be created and used on Cisco 4G LTE Advanced SKU’s. Maximum number of profiles that can be created are 16.
Cisco SKU's shipping with specific carrier provisioning file (Can be found in Carrier label under "show cellular <slot> hardware"), default profiles are already populated and can be deployed readily.

In all other cases where profile configurations are not available, separate profiles should be created with required parameters.

You can create multiple profiles on Cisco 4G LTE Advanced. The following are the default internet profile numbers for the modems:

<table>
<thead>
<tr>
<th>Modem</th>
<th>Profile Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP7607 (Global)</td>
<td>Profile 1</td>
</tr>
<tr>
<td>WP7601 (Verizon)</td>
<td>Both Profile 1 and Profile 3</td>
</tr>
<tr>
<td>WP7603 (AT&amp;T or other SPs)</td>
<td>Profile 1</td>
</tr>
</tbody>
</table>

Follow these guidelines when you configure a data profile using EXEC mode or Config mode:

- You do not have to make any profile-related changes if your modem comes with a data profile, for instance, AT&T, Sprint and Verizon.
- If any profile parameter changes are required for a connection type, the changes will likely be carried out in the default profiles.
- To configure different profile types and use them for a different connection, you can create separate profiles with different parameters (for instance, APN names). Note that only one profile is active at a given time.
- Use the `show cellular <unit> profile` command to view the data profile. An asterisk(*) symbol is displayed against the data profile. Double asterisk(**) symbol is displayed against the attach profile.
- The data profile is used to set up a data call. If you want to use a different profile, that profile needs to be made the default one. Use the `lte sim data-profile number` command to change the default profile under `controller cellular 0/1/0`.

### Creating, Modifying, or Deleting Data Profiles Using EXEC Mode

Customized profiles (Access Point Name(APN) in mobile networks) can be created and used on Cisco 4G LTE Advanced SKU's. Maximum number of profiles that can be created are 16.

Cisco SKU's shipping with specific carrier provisioning file (can be found in carrier label under `show cellular slot hardware`), default profiles are already populated and can be deployed readily.

---

**Note**

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

---

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cellular unit lte profile [create</td>
<td>delete] profile-number [apn [authentication [username password [bearer-type]]]]`</td>
</tr>
</tbody>
</table>

- The `profile-number` argument specifies the profile number created for the modem.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router# cellular 0/1/0 lte profile create 2 apn.com pap username pwd ipv4 | • (Optional) The apn argument specifies an Access Point Name (APN). An APN is provided by your service provider. Only a single APN can be specified for a single profile.  
  • (Optional) The authentication parameter specifies the authentication type used. Acceptable parameters are chap, none (no authentication), pap, and pap_chap (PAP or CHAP authentication).  
  • (Optional) The username and password arguments are given by a service provider. These are mandatory when an authentication type other than none is used.  
  • (Optional) The PDN type parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: ipv4 ipv6 and ipv4v6 (IPv4 and IPv6). |

The show cellular slot profile displays configured profile list.

**Note**  
Single asterisk(*) displayed against data profile.  
Double asterisk(**) displayed against attached profile.

### Example

```
router# show cellular 0/1/0 profile  
Profile 1 = INACTIVE **  
--------  
PDP Type = IPv4v6  
Access Point Name (APN) = vzwims  
Authentication = None  

Profile 2 = INACTIVE  
--------  
PDP Type = IPv4v6  
Access Point Name (APN) = vzwadmin  
Authentication = None  

Profile 3 = ACTIVE*  
--------  
PDP Type = IPv4v6  
PDP address = 100.119.136.44  
PDP IPv6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64 Scope: Global  
Access Point Name (APN) = VZWINTERNET  
Authentication = None  
Primary DNS address = 198.224.173.135  
Secondary DNS address = 198.224.174.135  
Primary DNS IPv6 address = 2001:4888:68:FF00:608:D:0:0  
Secondary DNS IPv6 address = 2001:4888:61:FF00:604:D:0:0  

Profile 4 = INACTIVE  
--------  
PDP Type = IPv4v6  
Access Point Name (APN) = vzwapp  
```
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzw800
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = CISCO.GW4.VZWENTP
Authentication = None

* - Default profile
** - LTE attach profile

#show cellular 0/3/0 profile
Profile 1 = INACTIVE **
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None

Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
--------
PDP Type = IPv4v6
PDP address = 100.86.69.19
Access Point Name (APN) = VZWINTERNET
Authentication = None
Primary DNS address = 198.224.173.135
Secondary DNS address = 198.224.174.135
Primary DNS IPV6 address = 2001:4888:68:FF00:608:D:0:0
Secondary DNS IPV6 address = 2001:4888:61:FF00:604:D:0:0

Profile 4 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwclass6
Authentication = None

* - Default profile
** - LTE attach profile

Configured default profile for active SIM 0 is profile 3.
If data and attach profile bindings need modification, use the controller cellular slot.

```
router(config-controller)# lte sim data-profile 3 attach-profile 2 slot unit
```

```
Device# show cellular 0/1/0 profile
Profile 1 = INACTIVE
--------------
PDP Type = IPv4v6
Access Point Name (APN) = test
Authentication = None

Profile 2 = INACTIVE **
-------
PDP Type = IPv4
Access Point Name (APN) = internet
Authentication = PAP or CHAP
Username = user@solution.com
Password = cisco

Profile 3 = INACTIVE*
-------
PDP Type = IPv4v6
Access Point Name (APN) = basic
Authentication = None

* - Default profile
** - LTE attach profile
Configured default profile for active SIM 0 is profile 2.
```

**Configuration Examples**

The following example shows how to change a default profile on 4G LTE Advanced:

```
router(config-controller)# lte sim data-profile 2 attach-profile 1 slot unit
```

The following example shows the output of the `show cellular` command for Verizon network service:

```
router# show cellular 0/1/0 profile
Profile 1 = INACTIVE **
-------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None

Profile 2 = INACTIVE
-------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
-------
PDP Type = IPv4v6
PDP address = 100.119.136.44
PDP IPv6 address = 2600:1010:800E:1E11:192D:3E20:199B:3A70/64 Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
Primary DNS address = 198.224.173.135
```
Secondary DNS address = 198.224.174.135
Primary DNS IPv6 address = 2001:4888:68::FF00:608:D:0:0
Secondary DNS IPv6 address = 2001:4888:61::FF00:604:D:0:0

Profile 4 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzw800
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = CISCO.GW4.VZWENTP
Authentication = None

* - Default profile
** - LTE attach profile

### Configuring a SIM for Data Calls

#### Locking and Unlocking a SIM Card Using a PIN Code

Perform this task to lock or unlock a SIM card given by your service provider.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code. Using the PUK code, you can unblock the SIM card.

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>`cellular unit lte sim {lock</td>
<td>unlock} pin`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# cellular 0/1/0 lte sim lock 1111</code></td>
<td>* <code>pin</code>—A code (4 to 8 digits long) provided by your carrier to lock or unlock the SIM card.</td>
</tr>
</tbody>
</table>

#### Changing the PIN Code

Perform this task to change the PIN code of a SIM.

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).
Verifying the Security Information of a Modem

Perform this task to verify the security information of a modem.

![Note]
For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>show cellular unit security</code></td>
<td>Shows the security information of the modem, including the SIM lock status.</td>
</tr>
</tbody>
</table>

Example:
```
Router# show cellular 0/1/0 security
```

Configuring Automatic Authentication for a Locked SIM

An unencrypted PIN can be configured to activate the Card Holder Verification (CHV1) code that authenticates a modem.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code.

Follow these procedures when using an unencrypted Level 0 PIN to configure CHV1. For instructions on how to configure CHV1 using an encrypted Level 7 PIN, see the Configuring an Encrypted PIN for a SIM, on page 220.

A SIM should be locked for SIM authentication to work. To verify the SIM’s status, use the `show cellular unit security` command.

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

Router# configure terminal

**Step 2**

**controller cellular unit**

**Example:**

Router(config)# controller cellular 0/1/0

**Purpose**

Enters the cellular controller configuration mode.

**Step 3**

**lte sim authenticate 0 pin**

**Example:**

Router(config)# lte sim authenticate 0 pin

**Purpose**

Authenticates the SIM CHV1 code by using an unencrypted (0) keyword and PIN. This PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.

**Note**

This command is valid only when an unencrypted PIN is used. To configure CHV1 code using an encrypted PIN, see the Configuring an Encrypted PIN for a SIM, on page 220.

### Configuring an Encrypted PIN for a SIM

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode.

**Note**

When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command. After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration.

**Note**

A SIM should be locked for SIM authentication to work. To verify the SIM’s status, use the show cellular <unit> security command.

**Note**

For the 4G LTE SKU, the unit argument identifies the router slot, module slot, and port separated by slashes (0/1/0).
<table>
<thead>
<tr>
<th><strong>Procedure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Applying a Modem Profile in a SIM Configuration

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# no service password-encryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>controller cellular unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# controller cellular 0/1/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>lte sim data-profile number attach-profile number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies the configured profile number to the SIM and its slot number. The default (primary) slot is 0. The attach profile is the profile used by the modem to attach to the LTE network. The data profile is the profile used to send and receive data over the cellular network.</td>
<td></td>
</tr>
</tbody>
</table>

Data Call Setup

To set up a data call, use the following procedures:

Configuring the Cellular Interface

To configure the cellular interface, enter the following commands starting in EXEC mode.

For the 4G LTE Advanced, the unit argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

If a tunnel interface is configured with ip unnumbered cellular 0/1/0, it is necessary to configure the actual static IP address under the cellular interface, in place of ip address negotiated.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
### Configure Cellular Interface with dialer watch-group

To configure the cellular interface with dialer watch-group, enter the following commands starting in EXEC mode.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>interface cellular unit</td>
<td>Specifies the cellular interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ip address negotiated</td>
<td>Specifies that the IP address for a particular interface is dynamically obtained.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ip address negotiated</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dialer in-band</td>
<td>Enables DDR and configures the specified serial interface to use in-band dialing.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# dialer in-band</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>dialer watch-group group-number</td>
<td>Specifies the number of the dialer access group to which the specific interface belongs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# dialer watch-group 1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ip route network-number network-mask {ip-address</td>
<td>interface} [administrative distance] [name name]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# ip route 209.165.200.225 255.255.255.224 cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>dialer-list dialer-group protocol protocol-name {permit</td>
<td>deny</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# dialer-list 1 protocol ip list 1</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `configure terminal`  
**Example:** Router# configure terminal | Enters global configuration mode. |
| 2    | `interface cellular unit`  
**Example:** Router(config)# interface cellular 0/1/0 | Specifies the cellular interface. |
| 3    | `ip address negotiated`  
**Example:** Router(config-if)# ip address negotiated | Specifies that the IP address for a particular interface is dynamically obtained. |
| 4    | `dialer in-band`  
**Example:** Router(config-if)# dialer in-band | Enables DDR and configures the specified serial interface to use in-band dialing. |
| 5    | `ip address negotiated`  
**Example:** Router(config-if)# ip address negotiated | Specifies that the IP address for a particular interface is dynamically obtained. |
| 6    | `dialer idle-timeout seconds`  
**Example:** Router(config-if)# dialer idle-timeout 30 | Specifies the duration of idle time, in seconds, after which a line has no outbound traffic. “0” second means no idle timeout. The default idle timeout is 120 seconds if there is no idle timer specified. |
| 7    | `dialer watch-group group-number`  
**Example:** Router(config-if)# dialer watch-group 1 | Enables Dialer Watch on the specific interface. |
| 8    | `exit`  
**Example:** Router(config-if)# exit | Enters the global configuration mode. |
| 9    | `dialer-list dialer-group protocol protocol-name [permit | deny] list access-list-number group-number`  
**Example:** Router(config)# dialer-list 1 protocol ip list 1 | Creates a dialer list for traffic of interest and permits access to an entire protocol. |
### Enabling 4G GPS and NMEA Data Streaming

GPS NMEA data streaming to external NMEA 2.0-compliant GPS plotter applications can be enabled on Cisco 4G LTE Advanced.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller cellular unit</td>
<td>Enters the controller cellular configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling 4G GPS and NMEA Data Streaming

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>lte gps enable</code></td>
<td>(Optional) GPS is enabled by default. Use this command to enable the GPS feature if GPS has been disabled for any reason.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# lte gps enable</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>lte gps mode standalone</code></td>
<td>Enables the standalone GPS mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# lte gps mode standalone</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`lte gps nmea {ip</td>
<td>udp [source address][destination address][destination port] }`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# lte gps nmea ip or Router(config-controller)# lte gps nmea</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Exits the controller configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# end</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>test cellular unit modem-power-cycle</code></td>
<td>GPS can take effect only after modem power cycle.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# test cellular 0/1/0 modem-power-cycle</td>
<td></td>
</tr>
</tbody>
</table>
| 8    | `show cellular unit gps` | Displays a summary of the following GPS data:  
- GPS state information (GPS disabled, GPS acquiring, GPS enabled)  
- GPS mode configured (standalone)  
- GPS location and timestamp information  
- GPS satellite information  
- GPS feature (enabled or disabled)  
- GPS port selected (Dedicated GPS and GPS port with voltage-no-bias) |
|      | **Example:**      |         |
|      | Router# show cellular 0/1/0 gps |         |
|      | GPS Feature = enabled |
|      | GPS Mode Configured = standalone |
|      | GPS Port Selected = Dedicated GPS port |
|      | GPS Status = GPS coordinates acquired |
|      | Last Location Fix Error = Offline [0x0] |
|      | Latitude = 37 Deg 25 Min 4.8915 Sec North |
|      | Longitude = 121 Deg 55 Min 8.5627 Sec West |
|      | Timestamp (GMT) = Wed Nov 7 21:54:18 2018 |
|      | Fix type index = 0, Height = 8 m |
|      | Satellite Info |
|      | ----------------- |
|      | Satellite #1, elevation 45, azimuth 303, SNR 20 * |
|      | Satellite #3, elevation 15, azimuth 296, SNR 21 |
|      | Satellite #8, elevation 9, azimuth 227, SNR 27 * |
|      | Satellite #11, elevation 41, azimuth 270, SNR 27 * |
|      | Satellite #18, elevation 64, azimuth 258, SNR 29 * |
|      | Satellite #22, elevation 35, azimuth 303, SNR 22 * |
|      | Satellite #31, elevation 51, azimuth 140, SNR 24 * |
|      | Satellite #32, elevation 46, azimuth 43, SNR 22 * |
### Command or Action
- Satellite #10, elevation 25, azimuth 97, SNR 0
- Satellite #14, elevation 68, azimuth 26, SNR 0
- Satellite #18, elevation 64, azimuth 258, SNR 33
- Satellite #22, elevation 35, azimuth 303, SNR 26
- Satellite #31, elevation 51, azimuth 140, SNR 27
- Satellite #32, elevation 46, azimuth 43, SNR 22
- Satellite #1, elevation 45, azimuth 303, SNR 0
- Satellite #3, elevation 14, azimuth 296, SNR 0

### Step 9
**show cellular unit gps detail**

**Example:**
```
Router# show cellular 0/1/0 gps detail
GPS Feature = enabled
GPS Mode Configured = standalone
GPS Port Selected = Dedicated GPS port
GPS Status = GPS coordinates acquired
Last Location Fix Error = Offline [0x0]
Latitude = 37 Deg 25 Min 4.9282 Sec North
Longitude = 121 Deg 55 Min 8.5209 Sec West
Timestamp (GMT) = Wed Nov 7 21:53:52 2018
Fix type index = 0, Height = 7 m
HDOP = 1.5, GPS Mode Used = standalone
```

### Satellite Info
```
Satellite #8, elevation 9, azimuth 227, SNR 31 *
Satellite #11, elevation 41, azimuth 270, SNR 32 *
Satellite #18, elevation 64, azimuth 258, SNR 33 *
Satellite #22, elevation 35, azimuth 303, SNR 26 *
Satellite #31, elevation 51, azimuth 140, SNR 27 *
Satellite #32, elevation 46, azimuth 43, SNR 22
Satellite #1, elevation 45, azimuth 303, SNR 0
Satellite #3, elevation 14, azimuth 296, SNR 0
```

### Configuring 4G SMS Messaging

**Note**

For an 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router# configure terminal
```
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>controller cellular unit</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# controller cellular 0/1/0</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>lte sms archive path FTP-URL</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-controller)# lte sms archive path ftp://username:password@172.25.211.175/SMS-LTE</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**cellular unit lte sms view { all</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show cellular unit sms</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# show cellular 0/1/0 sms&lt;br&gt;Incoming Message Information&lt;br&gt;-----------------------------&lt;br&gt;SMS stored in modem = 20&lt;br&gt;SMS archived since booting up = 0&lt;br&gt;Total SMS deleted since booting up = 0&lt;br&gt;Storage records allocated = 25&lt;br&gt;Storage records used = 20&lt;br&gt;Number of callbacks triggered by SMS = 0&lt;br&gt;Number of successful archive since booting up = 0&lt;br&gt;Number of failed archive since booting up = 0&lt;br&gt;Outgoing Message Information&lt;br&gt;-----------------------------&lt;br&gt;Total SMS sent successfully = 0&lt;br&gt;Total SMS send failure = 0&lt;br&gt;Number of outgoing SMS pending = 0&lt;br&gt;Number of successful archive since booting up = 0&lt;br&gt;Number of failed archive since booting up = 0&lt;br&gt;Last Outgoing SMS Status = SUCCESS&lt;br&gt;Copy-to-SIM Status = 0x0&lt;br&gt;Send-to-Network Status = 0x0&lt;br&gt;Report-Outgoing-Message-Number:&lt;br&gt;Reference Number = 0</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result Code = 0x0</td>
<td>Enables a user to send a 4G LTE band SMS message to other valid recipients, provided they have a text message plan. The number argument is the telephone number of the SMS message recipient.</td>
</tr>
<tr>
<td>Diag Code = 0x0 0x0 0x0 0x0 0x0</td>
<td></td>
</tr>
<tr>
<td>SMS Archive URL = ftp://lab:lab@1.3.150.1/outbox</td>
<td></td>
</tr>
</tbody>
</table>

### Step 7

**cellular unit lte sms send number**

**Example:**

Router# cellular 0/1/0 lte sms send 15554443333

<sms text>

### Step 8

**cellular unit lte sms delete [ all | id ]**

**Example:**

Router# cellular 0/1/0 lte sms delete [ all | id ]

(Optional) Deletes one message ID or all of the stored messages from memory.

### Configuring Modem DM Log Collection

Diagnostic Monitor (DM) Log is a modem’s feature that captures data transactions between the modem and the network over the radio frequency interface. This feature is a useful tool for troubleshooting 3G and 4G data connectivity or performance issues.

Once a DM log file is captured, diagnostic software tools, such as Sierra Wireless SwiLog and Qualcomm QXDM, can be used to decode the DM log file to understand the issues. A member of Cisco TAC can help with decoding the DM log files.

To configure DM log collection, enter the following commands, starting in privileged EXEC mode.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 controller cellular slot</td>
<td>Enters cellular controller configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>• autoshop—Automatically stops DM log capturing based on:</td>
<td></td>
</tr>
<tr>
<td>link-down—cellular interface link down event</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Modem DM Log Collection

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router(config-controller)# lte modem dm-log enable | Purpose Command or Action
| timer\(t\)imer\)—amount of time in minutes |
| enable—Starts DM log capturing. |
| filesize \(s\)ize—Specifies the maximum log file size, in MB for each DM log file before creating another DM log file. Range is from 1 to 64. Default is 20. |
| filter location:filename—Specifies the DM log filter to use from the following locations: |
| —bootflash:file |
| —flash:file |
| Note Bootflash and flash are the only valid locations to store the DM log filter file. |
| Note If the DM log filter file is not specified, the generic filter file, which comes with the router will be used. |
| Note The DM log filter file needs to be in .sqf format. |
| rotation—Enables continuous DM log capturing by replacing the oldest DM log files with the latest. |
| size \(l\)og-\(s\)ize—Specifies the maximum total size in MB of all DM log files that can be allowed in the bootflash or flash before modem stops capturing DM log files. If rotation is enabled, the oldest DM files is replaced with the latest DM file to meet this size configuration. |
| Returns to privileged EXEC mode. |

Step 4 end

Example:

Router(config-controller)# end

Step 5 show cellular unit logs dm-log

Example:

Router# show cellular 0/1/0 logs dm-log
Integrated DM logging is on
output path = Utility Flash
filter = MC74xx generic - v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf
maximum log size = 0
maximum file size = 0
log rotation = disabled

33 packets sent to the modem, 4663 bytes, 0 errors
28521 packets received from the modem, 13500758 bytes, 0 input drops

(Optional) Displays DM log configuration and statistics.
Example

The following example shows how to:

- Specifies the maximum size of all DM log files that can be stored in bootflash or flash to 512 MB
- Specifies the maximum size of each DM log file to 32 MB
- Uses MC7xxx_GPS_Log.sqf DM log filter in the flash
- Enable rotation
- Enables DM log capturing

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log filesize 512
Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log filesize 32

The following example shows how to specify the filter file for LTE:

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf

The following example shows how to enable DM log rotation for LTE:

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log rotation

The following example shows how to specify the maximum log size for LTE:

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log enable

The following example shows how to enable DM log rotation for LTE:

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# end

The following example shows how to specify the maximum log size for LTE:

Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log size 1024

The following example shows what was configured on the router for DM log feature:

Router# show running-config | section controller
cellular 0/1/0
lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf
lte modem dm-log size 512
lte modem dm-log filesize 32
lte modem dm-log rotation
lte modem dm-log enable
lte modem dm-log size 1024
Enabling Modem Crashdump Collection

Modem crashdump collection is useful in debugging firmware crash. To collect crash data, the modem has to be pre-configured so that it will stay in memdump mode after a crash. Memdump mode is a special boot-and-hold mode for the memdump utility to collect crash data.

To enable modem crashdump collection, perform the following steps.

Note

The integrated modem crashdump collection feature is supported only on 3G HSPA and 4G LTE Advanced based SKUs.

Before you begin

The device will need to be in boot-and-hold mode.

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#controller cel 0/1/0
Router(config-controller)#lte modem crash-action?
boot-and-hold Remain in crash state
Router(config-controller)#lte modem crash-action boot-and-hold

This ensures that whenever the router crashes, it will stay in that state and will not try to recover. By default the crash-action is reset which means the modem will reset and try to recover itself whenever it crashes. The above boot-and-hold command is used to keep the modem in a crashed state so that you can capture crashdump using the following command:

Router#test cell-cwan 0/1/0 modem-crashdump ?
off Disable Modem firmware crash dump
on Enable Modem firmware crash dump

Router#test cell-cwan 0/1/0 modem-crashdump on

This will capture the crashdump and store it in flash.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables or disables modem crashdump collection.</td>
</tr>
<tr>
<td>test { cell-cwan } unit modem-crashdump { on location</td>
<td>Enables crashdump log collection.</td>
</tr>
<tr>
<td></td>
<td>off }</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• cell-host</td>
</tr>
<tr>
<td>Router# test cell-host 0/1/0 modem-crashdump on local_uf</td>
<td>—Keyword for fixed platform.</td>
</tr>
<tr>
<td></td>
<td>• cell-cwan</td>
</tr>
<tr>
<td></td>
<td>— Keyword for LTE on a modular inside platform.</td>
</tr>
<tr>
<td></td>
<td>• unit</td>
</tr>
<tr>
<td></td>
<td>—For LTE module, this is the router slot, module slot, and port separated by slashes (for example, 0/1/0). For fixed platform, this is the number 0.</td>
</tr>
<tr>
<td></td>
<td>• on</td>
</tr>
<tr>
<td></td>
<td>Enables crashdump log collection.</td>
</tr>
<tr>
<td></td>
<td>• location</td>
</tr>
<tr>
<td></td>
<td>—Specifies the destination URL where the modem crashdump logs will be stored.</td>
</tr>
<tr>
<td></td>
<td>• off</td>
</tr>
<tr>
<td></td>
<td>—Disables crashdump log collection.</td>
</tr>
</tbody>
</table>

### Displaying Modem Log Error and Dump Information

As part of the 3G serviceability enhancement, commands strings (**at!err** and **at!gcdump**) can be sent to the modem using Cisco IOS CLI rather than setting up a reverse telnet session to the cellular modem to obtain log error and dump information.

To obtain log error and dump information, perform the following steps.
The modem log error and dump collection feature is supported only on 3G SKUs.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show cellular <em>unit</em> log error</td>
<td>Shows modem log error and dump information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show cellular 0/1/0 log error</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> test cellular <em>unit</em> modem-error-clear</td>
<td>(Optional) Clears out the error and dump registers. By default, error and dump registers are not cleared out after a read. This command changes the operation so that registers are cleared once they are read. As a result, the AT command strings are changed to &quot;at!errclr=-1&quot; for CDMA and &quot;at!err=0&quot; for GSM modems.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# test cellular 0/1/0 modem-error-clear</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the 4G LTE Advanced Router Information

You can verify the configuration by using the following show commands:

```
show version

Router# show version
Cisco IOS XE Software, Version BLD_V1612_THROTTLE_LATEST_20190604_050228_V16_12_0_134
Cisco IOS Software (Gibraltar), ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version 16.12.190604:055159
[v1612_throttle-/nobackup/mcpre/BLD-BLD_V1612_THROTTLE_LATEST_20190604_050228 226]
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 04-Jun-19 16:24 by mcpree

Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON
IR1101 uptime is 5 minutes
Uptime for this control processor is 6 minutes
System returned to ROM by Power-on at 17:11:39 GMT Tue Jun 25 2019
System image file is
"usbflash0:ir1101-universalk9.BLD_V1612_THROTTLE_LATEST_20190604_050228_V16_12_0_134.SSA.bin"
Last reload reason: Power-on
```
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

<table>
<thead>
<tr>
<th>Current</th>
<th>Type</th>
<th>Next reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-essentials</td>
<td>Smart License</td>
<td>network-essentials</td>
</tr>
</tbody>
</table>

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 708327K/6147K bytes of memory.
Processor board ID FCW222700KS
3 Virtual Ethernet interfaces
4 FastEthernet interfaces
2 Gigabit Ethernet interfaces
1 Serial interface
1 terminal line
4 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
---More---
2766848K bytes of Bootflash at bootflash:.
15350496K bytes of USB Flash at usbflash0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x1820

show platform

router# sh platform
Chassis type: IR1101-K9

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Insert time (ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IR1101-K9</td>
<td>ok</td>
<td>1w1d</td>
</tr>
<tr>
<td>0/0</td>
<td>IR1101-ES-5</td>
<td>ok</td>
<td>1w1d</td>
</tr>
<tr>
<td>0/1</td>
<td>P-LTE-GB</td>
<td>ok</td>
<td>1w1d</td>
</tr>
<tr>
<td>R0</td>
<td>IR1101-K9</td>
<td>ok, active</td>
<td>1w1d</td>
</tr>
<tr>
<td>F0</td>
<td>IR1101-K9</td>
<td>init, active</td>
<td>1w1d</td>
</tr>
</tbody>
</table>

show interfaces

router#sh interface cellular 0/1/0
Cellular0/1/0 is up, line protocol is up
Hardware is LTE Adv CAT6 - Europe/North America Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/
Internet address is 10.14.162.11/32
MTU 1500 bytes, BW 50000 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive not supported
DTR is pulsed for 1 seconds on reset
Last input never, output 00:00:42, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
5 packets input, 460 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
21 packets output, 1692 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions

show inventory

router# show inventory
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ 
NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V00 , SN: FCW222700KS

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: V00 , SN: FOC22224U22

NAME: "module subslot 0/0", DESCR: "IR1101-ES-6S"
PID: IR1101-ES-6S , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 5", DESCR: "100BASE FX-GE"
PID: GLC-FE-100FX-RGD , VID: V02 , SN: FNS153304G4

NAME: "module subslot 0/1", DESCR: "P-LTEA-LA Module"
PID: P-LTEA-LA , VID: V01 , SN: FOC22287JNR

NAME: "Modem on Cellular0/1/0", DESCR: "Sierra Wireless EM7430"
PID: EM7430 , VID: 1.0 , SN: 355813070162356

NAME: "module subslot 0/3", DESCR: "P-LTEA-EA Module"
PID: P-LTEA-EA , VID: V01 , SN: FOC22170JA9

NAME: "Modem on Cellular0/3/0", DESCR: "Sierra Wireless EM7455"
PID: EM7455 , VID: 1.0 , SN: 356129070235970

NAME: "Module 2 - Expansion Module", DESCR: "IR1100 expansion module with Pluggable slot and SFP"
PID: IRM-1100-SP , VID: V00 , SN: FCW23050014

NAME: "Module 3 - FP F0", DESCR: "Cisco IR1101 Forwarding Processor"
PID: IR1101-K9 , VID: V00 , SN: FOC22224U22
Configuring Cellular Modem Link Recovery

The cellular modem link recovery feature is disabled by default and it is recommended to enable the link recovery feature.

**Note**

No manual operations or automated scripts interacting with 4G modems may be possible until and unless the modems have come fully in-service. Modems may take approximately 4 minutes after platform bootup and CLI available to be able to allow full interaction and establish IP connectivity. A typical modem power-cycle may also take approximately 4 minutes before any interaction is possible. Modems are in-service after the console displays “%CELLWAN-2-MODEM_RADIO: Cellular0/x/0 Modem radio has been turned on” – where x is the modem slot number.

To enable or disable the cellular modem link recovery feature, if required, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** controller cellular unit | Enters cellular controller configuration mode. |
| **Example:** | |
| Router(config)# controller cellular 0/1/0 | |

| **Step 3** {lte modem link-recovery disable | no lte | modem link-recovery disable} | Enables or disables the cellular modem link recovery feature. |
| **Example:** | Enables or disables the cellular modem link recovery feature. |
| Router(config-controller)# lte modem link-recovery disable | Once we enable link-recovery, the default Cisco recommended values for link-recovery parameters are populated. |
| Router(config-controller)# no lte modem link-recovery disable | We can change the values of link-recovery parameters from the default Cisco recommended values, by using cli for each parameter like in example. |
| Device#show run | sec controller Cellular 0/1/0 controller Cellular 0/1/0 lte modem link-recovery rssi onset-threshold -110 lte modem link-recovery monitor-timer 20 lte modem link-recovery wait-timer 10 lte modem link-recovery debounce-count 6 | |
| **Example:** | Changing the default recommended cisco values is not advised as it will impact ideal performance of link-recovery feature. |
| Device#configure terminal | |
| Device(config)#controller Cellular 0/1/0 | |
| Device(config-controller)#lte modem link-recovery | |
### Cellular Modem Link Recovery Parameters

There are four configurable parameters to adjust the behavior of cellular link recovery. The default values optimized for the best performance of the feature and changing it is not recommended unless advised by Cisco.

The following table explains the link recovery parameters:

**Table 11: Link Recovery Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rssi onset-threshold</td>
<td>This parameter defines the RSSI value below which the link recovery feature triggers additional scrutiny to look for potential issues and take action if needed. The range of this parameter can be set from -90 dBm to -125 dBm. The recommended and default value is -110 dBm.</td>
</tr>
<tr>
<td>monitor-timer</td>
<td>This parameter determines how often link recovery looks for potential issues. The default value for this parameter is 20 seconds meaning that link recovery feature will be triggered every 20 seconds and look at certain parameters to determine if there is a potential issue. You can configure the monitor-timer range between 20 to 60 seconds. Increasing the monitor timer value above 20 seconds will increase the response time of the feature.</td>
</tr>
</tbody>
</table>
### Parameter: wait-timer and debounce-count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wait-timer and debounce-count</td>
<td>The wait-timer parameter is used in conjunction with the debounce-count parameter to perform more frequent, additional checks, once the link recovery feature has identified a potential issue that needs to be recovered from, with a modem power-cycle. The default value for wait-timer is 10 seconds and the default value for debounce-count is 6. With this setting, once link recovery has identified an inoperative modem state, it performs additional checks every 10 seconds, up to 6 times, to determine if the issue has been resolved without a modem power-cycle. Reducing the debounce-count and the wait-timer makes faster link recovery, while reducing them may increase the time for recovery. The configurable range for wait-timer is 5-60 seconds. The configurable range for debounce-count is 6-20 seconds.</td>
</tr>
</tbody>
</table>

---

### Verifying the Cellular Modem Link Recovery Configuration

To determine if the cellular modem link recovery is enabled, use the `show controller cellularunit` command. In this example, the cellular modem link recovery feature related information is highlighted.

Router# show controller cellular 0/1/0 Interface Cellular0/1/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

**Cellular Modem Configuration**

- Modem is recognized as valid
- Power save mode is OFF
- manufacture id = 0x00001199    product id = 0x000068C0
- Sierra Wireless unknown modem
- Modem Uplink Speed = 50000 kbit.
- Modem Downlink Speed = 300000 kbit.

- GPS Feature = enabled
- GPS Status = NMEA Disabled
- GPS Mode = not configured

**Cellular Dual SIM details:**

- SIM 0 is present
- SIM 1 is not present
- SIM 0 is active SIM

**Module Reload Statistics**

- Soft OIR reloads = 0
- Hard OIR reloads = 0

**Modem Management Statistics**

- Modem resets = 1
- Modem timeouts = 0
Link recovery is ON
Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6

Link recovery count is 0

When the cellular modem link recovery occurs and modem is power cycled, you can see the %CELLWAN-2-MODEM_DOWN message on the console logs and additionally there is a %CELLWAN-2-LINK_RECOVERY message which indicates that action has been taken by the cellular modem link recovery feature.

Whenever the cellular modem link recovery has occurred, it updates the Modem timeouts counter under the Modem Management Statistics section of the show controller cellular unit command output. Modem parameters at the last timeout section has information that helps to identify the cause of the issue that triggered link recovery.

In the following example log, the messages, modem time out counter, and modem parameters at the last time out are highlighted.

*Jul 19 17:15:18.980 PDT: %CELLWAN-2-LINK_RECOVERY: Cellular0/1/0: Cellular Modem has been power cycled

Device#show controller Cellular 0/1/0
Interface Cellular0/1/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
-----------------------------------
Modem is recognized as valid
Power save mode is OFF
manufacture id = 0x00001199    product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status = NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0

Modem Management Statistics
---------------------------
Modem resets = 1
Modem user initiated resets = 0
Modem user initiated power-cycles = 0

Modem timeouts = 1
Modem parameters at the last timeout:
  LTE first time attach State was No
  Radio Interface Technology Mode was AUTO
Configuration Examples for 3G and 4G Serviceability Enhancement

Example: Sample Output for the show cellular logs dm-log Command

The following shows a sample output of the `show cellular logs dm-log` command:

```
Router# show cellular 0/1/0 logs dm-log
Integrated DM logging is on
filter = generic
maximum log size = 67108864
maximum file size = 20971520
log rotation = disabled
7 packets sent to the modem, 3232 bytes, 0 errors
75 packets received from the modem, 57123 bytes, 0 input drops
75 packets stored in file system, 57123 bytes, 0 errors, 0 aborts
2 max rcv queue size
current file size = 57123
current log size = 57123
total log size = 57123
DM log files: (1 files)
```

Example: Sample Output for the show cellular logs modem-crashdump Command

The following shows a sample output of the `show cellular logs modem-crashdump` command:

```
Router# show cellular 0/1/0 logs modem-crashdump
Modem crashdump logging: off
Progress = 100%
Last known State = Getting memory chunks
Total consecutive NAKs = 0
Number of retries = 0
Memory Region Info:
1: Full SDRAM [Base:0x0, Length:0x2000000]
2: MDSP RAM A region [Base:0x9100000, Length:0x8000]
3: MDSP RAM B region [Base:0x9120000, Length:0x8000]
4: MDSP RAM C region [Base:0x9140000, Length:0xC000]
5: MDSP Register region [Base:0x91C0000, Length:0x28]
6: ADSP RAM A region [Base:0x7000000, Length:0x10000]
7: ADSP RAM B region [Base:0x7020000, Length:0x10000]
```
Configuration Examples for 4G LTE Advanced

Configuration examples follow based upon the following hardware shown in the two examples.

Router# show inventory

NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V00 , SN: FCW222700KS

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: V00 , SN: FOC22224U22

NAME: "module subslot 0/0", DESCR: "IR1101-ES-6S"
PID: IR1101-ES-6S , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 5", DESCR: "100BASE FX-GE"
PID: GLC-FE-100FX-RGD , VID: V02 , SN: FNS153304G4

NAME: "module subslot 0/1", DESCR: "P-LTEA-LA Module"
PID: P-LTEA-LA , VID: V01 , SN: FOC22287JNR

NAME: "Modem on Cellular0/1/0", DESCR: "Sierra Wireless EM7430"
PID: EM7430 , VID: 1.0 , SN: 355813070162356

NAME: "module subslot 0/3", DESCR: "P-LTEA-EA Module"
PID: P-LTEA-EA , VID: V01 , SN: FOC22170JA9

NAME: "Modem on Cellular0/3/0", DESCR: "Sierra Wireless EM7455"
PID: EM7455 , VID: 1.0 , SN: 356129070235970

NAME: "Module 2 - Expansion Module", DESCR: "IR1100 expansion module with Pluggable slot and SFP"
PID: IRM-1100-SP , VID: V00 , SN: FCW23050014

NAME: "Module 3 - FP F0", DESCR: "Cisco IR1101 Forwarding Processor"
PID: IR1101-K9 , VID: V00 , SN: FOC22224U22

Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM administratively down down
FastEthernet0/0/1 unassigned YES unset down down
FastEthernet0/0/2 unassigned YES unset down down
FastEthernet0/0/3 unassigned YES unset down down
FastEthernet0/0/4 unassigned YES unset down down
GigabitEthernet0/0/5 unassigned YES unset up up
Cellular0/1/1 unassigned YES NVRAM administratively down down
Cellular0/3/0 100.86.69.19 YES IPCP up up
Cellular0/3/1 unassigned YES unset administratively down down
Async0/2/0 unassigned YES unset up down
Vlan1 192.168.10.15 YES NVRAM up up
Vlan172 172.27.167.121 YES NVRAM up up
Example: Basic Cellular Interface Configuration: Cisco 4G LTE Advanced

The following example shows a dual LTE scenario configuration showing working cellular configuration for both 0/1/0 and 0/3/0 with appropriate routes and dialer watch-group.

```
show run
Building configuration...

Current configuration : 8079 bytes
!
! Last configuration change at 17:33:19 GMT Tue Jun 25 2019
!
version 16.12
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname IR1101
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone GMT 0 0
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
! address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
!
ip name-server 171.70.168.183 198.224.173.135 8.8.8.8
no ip domain lookup
ip domain name cisco.com
!
login on-success log
ipv6 unicast-routing
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
chat-script hspa-R7 "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki trustpoint TP-self-signed-756885843
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-756885843
  revocation-check none
  rsakeypair TP-self-signed-756885843
!
Example: Basic Cellular Interface Configuration: Cisco 4G LTE Advanced

```plaintext
! crypto pki certificate chain SLA-TrustPoint
certificate ca 01
   30820292 30820216 A0030201 02020101 300D0609 2A868486 F700D101 0B050030
   30312030 C060355 040A1305 43679363 6F312030 1E060355 04031317 43679363
   6F204C69 63656763 69666720 5266F6F4 20434130 1E17D313 33035333 30313934
   3834375A 170D3338 30353330 33934384 34375A30 32310E30 C060355 040A1305
   43679363 6F312030 1E060355 04031317 43679363 6F204C69 63656763 69666720
   5266F6F4 20434130 82012230 00D6092A 684686F7 F0000101 00050308 01F0F003
   82010A02 82010100 6ABCD96 13E05F7 145E7A2C 2C6D6E66 1722E2A1 F1EFFF64
   CB48C798 212A1A47 C655D0BD 971413BD 8711441E 1AA0F701A 9CAEE3688 A38E6520
   1C1394DE 462E23C9 659F71B 9B8CA0A9 5BBB5CB5 C0F3EBA3 700A8BFF D8F256EE
   4A4BBD9F DB6FD1C9 60B1FD18 FF6C9C6 6FA68697 A2616D7E 10456C5F E2A956AC
   7390AA3E 2BF435AD C847A2C5 DAB553EB 69A5A535 58BF9E33 CB0B23CF 5BF8D71B8
   68654941 20F320E7 948E71D7 AE38CC84 F10684C7 4BCE800F 539B4A2B 42C66BB7
   C79C0976 C48CB2D2 E2AF505D CB062A4A 681D9598 E2850F4C 5D056BF8 F2B7D191
   C55F0D76 61F94ACD 3D9D2327 ABBB03BD 46ED6709 7CBADF88 DF5F3468 95135E44
   DFC7C6D9 C48CB2D2 E2AF505D CB062A4A 681D9598 E2850F4C 5D056BF8 F2B7D191
   06300F6F 035531D3 011FF0F4 03005301 01F031D0 063531D1 E041604 E449DC85
   4B3D31E5 1B3E6A17 606A3333 3083C87C 83B06D0E 92A86848 867FD001 010B0500
   03821005 00570F24 D3932A66 86025DF9 B8EAE5C 6DD6F860 96436178 2409DA05
   604E6DCE FF4FED28 77FC6E6D C6D36FDB D4D648E1 3A567A3B 6C9E3D8B D9897BFF
   C4E0C09D B2E1CA0C2B 21D9B85C 8FAB856E CD986B46 5575B146 BDFC668A
   467A30F4 4D565700 6ADF0FD0 CP835015 3C04FF7C 21B87A8C 11B94C92 55A98232
   7C7A7BE8 C1AF74FE 15E299B7 B1F3FP9B E973DE7F 5BDEDE86 C713EB49 176S30B8
   5FBDA0E6 B92AFE7F 494E88A0 E7B85737 F3A5BB61 1AA4A229 C37C6E69 3F098678
   80DCCD16 D6BACCEA EBBCE7CF 8428787B 35202C0C 60E4616A B623CDBD 230E3AFB
   418616A9 4093E0A9 4D10AB75 27E86F73 932E35B5 886FDA6E 0275156F 719BB2F0
   D697DF7F 28
quit
```

```
cisco 4G LTE-Advanced Configuration
```

```
Example: Basic Cellular Interface Configuration: Cisco 4G LTE Advanced

```
memory free low-watermark processor 50357
file prompt quiet
!
username cisco privilege 15 password 0 cisco
username lab password 0 lab123
!
redundancy
!
controller Cellular 0/1/0
no lte firmware auto-sim
lte modem link-recovery disable
!
controller Cellular 0/3/0
!
vlan internal allocation policy ascending

interface GigabitEthernet0/0/0
no ip address
shutdown
!
interface FastEthernet0/0/1
switchport access vlan 192
switchport mode access
!
interface FastEthernet0/0/2
switchport access vlan 172
switchport mode access
!
interface FastEthernet0/0/3
switchport access vlan 172
!
interface FastEthernet0/0/4
switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/1/1
no ip address
shutdown
!
interface Cellular0/3/0
ip address negotiated
dialer in-band
dialer idle-timeout 0
dialer watch-group 2
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/3/1
no ip address
shutdown
!
interface Vlan1
  ip address 192.168.10.15 255.255.255.0
!
interface Vlan172
  ip address 172.27.167.121 255.255.255.128
!
interface Vlan175
  ip address 175.1.1.1 255.255.255.0
!
interface Async0/2/0
  no ip address
  encapsulation scada
  ip default-gateway 172.27.167.1
  ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.27.167.1
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 253
ip route 8.8.4.0 255.255.255.0 Cellular0/3/0
ip route 171.70.0.0 255.255.255.0 172.27.167.1
ip route 192.1.1.0 255.255.255.0 Cellular0/1/0
ip route 192.168.193.0 255.255.255.0 Cellular0/1/0
!
!
ip access-list standard 1
  10 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer watch-list 2 ip 5.6.7.8 255.255.255.255
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server host 171.70.127.43 version 2c public
snmp-server host 172.27.167.220 version 2c public
snmp-server manager
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
  speed 115200
  line 0/0/0
  line 0/2/0
  line vty 0 4
  exec-timeout 0 0
  password cisco
  login
  transport input none
!
The following example shows how to configure Cisco 4G LTE Advanced:

```plaintext
! Last configuration change at 19:14:26 UTC Fri Oct 19 2018
!
version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
no platform punt-keepalive settings
!
hostname IR1101
!
boot-start-marker
boot system flash ir1101-universalk9.16.10.SSA.bin
boot-end-marker
!
!
no aaa new-model
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
```
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
!

ip admission watch-list expiry-time 0
!
login on-success log
!

crypto pki trustpoint TP-self-signed-2240381033
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2240381033
revocation-check none
rsakeypair TP-self-signed-2240381033
!

crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!

crypto pki certificate chain TP-self-signed-2240381033
certificate self-signed 01
30820300 30820218 A0030201 02020101 30000609 2A864886 F700D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D5369676E65642D 43657274
69666963 6174652D 33383130 3333301E 170D3138 30733131 32323035
35315A17 0D333030 30303030 30A50301 32323430 33383130 2939341CF 77FE4E28
31BB1356 29E3121 371AB009
BEAF6DD7 47E425B2 F5922BDD 8CD4F7F2 390FE87E C8EC2023 0E6A879F E91B796C
36032BB8 20688D62 774D131C 907A93AC 530A88BB 5BABBD06 5F5959E1 61386E4E
EC6E8F11 9E2D43A8 3C306FBA 7C620F5 2BA3FE66 F049C40F 29B98755 ADBB9896
CDF197C6 6BC27BDE CEA29350 35A520B9 70D8436C 20408476 6716680C 1FCD2B1B
90067B65 E398BC80 1D20EFE7 62995271 88D12026 1879F9D8 FDC9F201 8379598F
109B52A7 5C8C71C9 C5706526 44044193 1CC86D69 66AF7CD5 D6404B55 50C2B6C2
8222C80A 52570945 CAFAAA96 88728572 05F45E80 7A9F2E9D 4185D0A4 939EDC5B
D4770CB7 C3630203 010001A3 53305130 0F060355 1D310011 FF040530 30101FF
301F0603 551D2004 18301680 14287B4A B9BEF6E1 3ECC2015 830EFE12 0CD474C6
E130106E 0355100C 04100414 2B78CA9B B8EF613E C2301583 0E0E120C 474C6E1
300D0609 2A864886 F700D0101 05050030 82010100 9F1269A8 349CFE9D E2801B79
4F82F1ED 4498F4A3 E62A4632 F02B9779 F6B885D0 994E0F88 FFC2F43C A0FA7A08
EOE0F5218 BF97A7EA 51563627 7085417E CBBDE865F 9C7B3E76 54D2AB69 046DFD4E
3406AB3F 6CCAFCDBB AC583F3C 49CA95C9 5E5E09E9 6A92122D 886441D0 997F8F9B
218188E7 E1EA44D6 525216A CAA2EE76 9B68C116 0932EFE4 9A86FAD2 F394C361
A7DA9E98 94942B80 52CAD033 7636DCC8 E6F687C2 2B0518F 38D3E17D A8854BE9
FA2F167E 00C08853 EC0BB86 B1342ACF 20046280 F90883D0 51EF66A1 719D19E9
110ACDE3 D872A6B0 B04A57F1 7D3D364A 592426E9 3EC92AD2 2D34DE52 9F7588E8
E060B27E 01BC2E1C 7375F6B3 5584E704 B2A54DE
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 30000609 2A864886 F700D0101 0B050030
31301E03 C060355 040A1305 34397363 6F312030 0E060355 04031317 43697363
6F204CC9 63656E73 69666720 526F6F74 20434130 16170D31 33303533 30313934
3834375A 170D3330 30353330 31393438 34375A30 32310E30 C060355 040A1305
43697363 6F312030 0E060355 04031317 43697363 6F204CC9 63656E73 69666720
526F6F74 20434130 82012220 0D06092A 864886F7 9D010101 05000382 010F0030
82010A02 82010100 A6BC0D96 131E05F7 145E7A2C 2D686E67 17222EAA 1FEFF64D
CB84C798 212AA147 C655DB07 9471380D 8711441E 1A0F701A 9CAB6388 8A38E520
!!!
license udi pid IR1101-K9 sn FCW22270XXX
license boot level network-advantage
license smart transport callhome
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 50290
!
redundancy
!
controller Cellular 0/1/0
  lte sim data-profile 3 attach-profile 1 slot 0
  no lte firmware auto-sim
  lte gps mode standalone
  lte modem link-recovery disable
!
controller Cellular 0/3/0
  no lte firmware auto-sim
  lte gps mode standalone
  lte modem link-recovery disable
!
!
vlan internal allocation policy ascending
!
!
! interface GigabitEthernet0/0/0
  ip address 175.1.1.1 255.255.255.0
!
interface FastEthernet0/0/1
  shutdown
!
interface FastEthernet0/0/2
  shutdown
!
interface FastEthernet0/0/3
  shutdown
!
interface FastEthernet0/0/4
  switchport access vlan 168
  switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
  ip address negotiated
  load-interval 30
  dialer in-band
  dialer idle-timeout 0
  dialer watch-group 1
  ipv6 enable
  pulse-time 1
  ip virtual-reassembly
!
interface Cellular0/1/1
  no ip address
  shutdown
!
interface Vlan1
  no ip address
!
interface Vlan168
  ip address 192.168.10.22 255.255.255.0
!
interface Async0/2/0
  no ip address
  encapsulation slip
!
  ip default-gateway 172.27.138.129
  ip forward-protocol nd
!
  ip http server
  ip http authentication local
  ip http secure-server
  ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
  ip route 172.27.0.0 255.255.0.0 172.27.138.129
!
  access-list 1 permit any
  access-list 2 permit any
  dialer watch-list 1 ip 5.6.7.8 255.255.255.255
  dialer watch-list 1 delay route-check initial 60
  dialer watch-list 1 delay connect 1
  dialer-list 1 protocol ip permit
  dialer-list 1 protocol ipv6 permit
  dialer-list 2 protocol ip permit
  dialer-list 2 protocol ipv6 permit
  ipv6 route ::/0 Cellular0/1/0
!
  control-plane
!
  line con 0
  exec-timeout 0 0
  transport input none
  stopbits 1
  speed 115200
  line 0/2/0
  line vty 0 4
  password cisco
  login
  transport input all
  transport output all
!
end
Cellular Back-off

Cellular Back-off is a feature introduced in IOS which addresses the concerns about Cisco LTE router not performing backoff in error handling. When PDP Context activation is failing, modems may receive from a cellular service provider. As a result, when some specific error codes (for example: 29, 33) are received by the modem from a cellular network, the router’s IOS incrementally adds interval in sending PDP Context Activation requests and any IP traffic such as not to load service provider network with requests that are known to IOS as failing. Once PDP Context is established and IP traffic is successful, the Cellular Backoff is removed for normal operation.

This back-off implementation will be a generic design and will NOT be specific to a particular service provider. There will be NO IOS CLI command to disable this new feature either.

Example: GRE Tunnel over Cellular Interface Configuration

The following example shows how to configure the static IP address when a GRE tunnel interface is configured with `ip address unnumbered cellular interface`:

```plaintext
interface Tunnel2
ip unnumbered <internal LAN interface GE0/0 etc.>
tunnel source Cellular0/1/0
tunnel destination a.b.c.d
interface Cellular0/1/0
ip address negotiated
no ip mroute-cache
dialer in-band
dialer-group 1
```

Example: 4G LTE Advanced as Backup with NAT and IPSec

The following example shows how to configure the 4G LTE Advanced on the router as backup with NAT and IPsec:

The receive and transmit speeds cannot be configured. The actual throughput depends on the cellular network service.

For service providers using a private IP address, use the `crypto ipsec transform-set esp` command (that is, esp-aes esp-sha256-hmac...).

```plaintext
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lan-pool
   network 10.4.0.0 255.255.0.0
```
Example: 4G LTE Advanced as Backup with NAT and IPSec

dns-server 10.4.0.254
default-router 10.4.0.254
!
crypto isakmp policy 1
encri 3des
authentication pre-share
crypto isakmp key address a.b.c.d
!
crypto ipsec transform-set ah-sha-hmac esp-3des
!
crypto map gsm1 10 ipsec-isakmp
  set peer a.b.c.d
  set transform-set
  match address 103
!
interface interface Gi 0/0/0
  no ip address
  ip virtual-reassembly
  load-interval 30
  no atm ilmi-keepalive
dsl operating-mode auto
!
backup interface Cellular0/1/0
  ip address negotiated
  ip mtu 1492
  ip nat outside
  ip virtual-reassembly
  encapsulation ppp
  load-interval 30
dialer pool 2
dialer-group 2
  ppp authentication chap callin
  ppp chap hostname cisco@dsl.com
  ppp chap password 0 cisco
  ppp ipcp dns request

crypto map gsm1
  ip nat outside
  ip virtual-reassembly
  no snmp trap link-status
  pvc 0/35
  pppoe-client dial-pool-number 2
!
interface Cellular0/1/0
  ip address negotiated
  ip nat outside
  ip virtual-reassembly
  no ip mroute-cache
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
  crypto map gsm1
!
interface Vlan1
  description used as default gateway address for DHCP clients
  ip address 10.4.0.254 255.255.0.0
  ip nat inside
  ip virtual-reassembly
!
  ip local policy route-map track-primary-if
  ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
ip nat inside source route-map nat2cell interface Cellular0/1/0 overload
ip nat inside source route-map nat2dsl overload
!
ip sla 1
   icmp-echo 2.2.2.2 source
   timeout 1000
   frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 101 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 2.2.2.2
access-list 103 permit ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
route-map track-primary-if permit 10
   match ip address 102
!
route-map nat2dsl permit 10
   match ip address 101
!
route-map nat2cell permit 10
   match ip address 101
   match interface Cellular0/1/0
!
exec-timeout 0 0
login
modem InOut

Example: SIM Configuration

This section provides the following examples:

Locking the SIM Card

The following example shows how to lock the SIM. The italicized text in this configuration example is used to indicate comments and are not be seen when a normal console output is viewed.

Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
Router# cellular 0/1/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router# Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
Unlocking the SIM Card

The following example shows how to unlock the SIM. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```bash
Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state.!
```

```
Router# cellular 0/1/0 lte sim unlock 1111
!!!WARNING: SIM will be unlocked with pin=1111(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
```

```
Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
```

Automatic SIM Authentication

The following example shows how to configure automatic SIM authentication. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```bash
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller cellular 0/1/0
Router(config-controller)# lte sim authenticate 0 1111
```

```
CHV1 configured and sent to modem for verification
```

```
Router(config-controller)# end
```
Changing the PIN Code

The following example shows how to change the assigned PIN code. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router!! SIM is in unlocked state.!

Router# cellular 0/1/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]

Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router!! SIM is in locked state. SIM needs to be in locked state to change its PIN.!

Router# cellular 0/1/0 lte sim change-pin 1111 0000
!!!WARNING: SIM PIN will be changed from:1111(4) to:0000(4)
Call will be disconnected. If old PIN is entered incorrectly in 3 attempt(s), SIM will be blocked!!!
Are you sure you want to proceed?[confirm]
Resetting modem, please wait...
CHV1 code change has been completed. Please enter the new PIN in controller configuration for verification

Router# sh cellular 0/1/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router!! SIM stays in locked state, as expected, but with new PIN.!

Router# lte sim unlock 0000
!!!WARNING: SIM will be unlocked with pin=0000(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Configuring an Encrypted PIN

The following example shows how to configure automatic SIM authentication using an encrypted PIN. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do sh run | i SIM
username SIM privilege 0 password 7 055A575E70.!! Copy the encrypted level 7 PIN. Use this scrambled PIN in the SIM authentication ! command.!!

Router(config)# controller cellular 0/1/0
Router(config-controller)# lte sim authenticate 7 055A575E70
CHV1 configured and sent to modem for verification
Router(config-controller)# exit
Router(config)# no username SIM
Router(config)# end
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console

Upgrading the Modem Firmware

The IR1101 uses Sierra Wireless modems that are supported on Cisco 4G LTE Advanced. The firmware for the modem is upgradable using Cisco IOS commands. The firmware is typically a Crossword Express (cwe) file and can be downloaded from the wireless software download page on Cisco.com. For some modems, such as the EM74XX series, the file type is an *.spk file.

Prior to performing the cellular modem firmware upgrade, make sure of the following:

- The "microcode reload ..." command is issued only from router's base directory.
- The modem firmware directory must contain the following:
  
  Only the *.spk file
  Only the *.cwe file
  Only the *.nvu file
  Only a matching pair of *.cwe and *.nvu files for the exact same version

- The modem firmware directory MUST NOT contain any other files

Note
Firmware upgrade is supported on utility flash.
Use only Cisco certified firmware. Using a firmware version not certified by Cisco may impact the wireless service provider network adversely.

**Caution**

Do not disconnect power or switch the router off during the firmware upgrade process. This may result in permanent modem failure.

**Note**

Firmware downgrade is not supported.

**Note**

Not all IR1101 cellular interfaces can support 2G (only P-LTE-GB), and may not support 3G (P-LTE-VZ).

Details about supported cellular pluggable module SKUs and modems can be found in the IR1101 Hardware Installation Guide here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst/pview.html#72641

You can determine which radio bands are supported by using the following command:

```
IR1101#show cellu 0/1/0 radio band
```

LTE bands supported by modem:
- Bands 1 3 7 8 20 28.

LTE band Preference settings for the active sim(slot 0):
- Bands 1 3 7 8 20 28.

Non-LTE bands supported by modem:
Index:
72 - GSM DCS band (1800)
73 - GSM Extended GSM (E-GSM) band (900)
87 - WCDMA (Europe, Japan, and China) 2100 band
114 - WCDMA Europe and Japan 900 band

Non-LTE band Preference settings for the active sim(slot 0):
Index:
72 - GSM DCS band (1800)
73 - GSM Extended GSM (E-GSM) band (900)
87 - WCDMA (Europe, Japan, and China) 2100 band
114 - WCDMA Europe and Japan 900 band

Band index reference list:
Indices 1-64 correspond to LTE bands 1-64.
Indices 65-128 correspond to Non-LTE bands.

```
IR1101#
```
# Upgrading the Modem Firmware Manually With CLI

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Go to the Cisco Wireless WAN software download website at: <a href="http://software.cisco.com/download/navigator.html">http://software.cisco.com/download/navigator.html</a></td>
<td>Provides access to Cisco Wireless WAN software downloads page to select the firmware for Cisco 4G. <strong>Note</strong> This website is only available to registered Cisco.com users.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the Cisco Wireless WAN software page, go to <strong>Products</strong> -&gt; <strong>Cisco Interfaces and Modules</strong> -&gt; <strong>Cisco High-Speed WAN interface Cards</strong> and select your product from the list of available cards.</td>
<td>Select your product for firmware upgrade.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select and download the appropriate firmware.</td>
<td>Download the modem firmware file to flash memory on the router.</td>
</tr>
</tbody>
</table>
| **Step 4** | terminal monitor  
*Example:*  
Router# terminal monitor | Enables the logging console in privileged EXEC mode. |
| **Step 5** | **microcode reload cellular** pa-bay slot **modem-provision** [flash:<firmware_directory_name>]  
*Example:*  
Router# microcode reload cellular 0 slot modem-provision bootflash:/<firmware_directory> | Initiates the firmware upgrade process.  
For the IR1101 Base, the firmware upgrade would use `microcode reload cellular 0 1 ...`.  
For the IR1101 Expansion Module, the firmware upgrade would use `microcode reload cellular 0 3 ...`. **Note** Modem firmware upgrade may take 10-15 mins from issuing the `microcode reload` command to the modem coming up. The router console will display 'FW_UPGRADE: Firmware upgrade success.....' message to indicate the firmware upgrade completed. The modem will reset itself and may take an additional 5 minutes to be up in-service.  
- *pa-bay*—Use 0 for 4G LTE Advanced.  
- *slot*—For 4G LTE Advanced, slot number, 0 to 3, where the 4G LTE Advanced is plugged in.  
- For remote download, you can transfer this using the wireless link from Cisco.com onto flash. |
| **Step 6** | show cellular 0/1/0 hardware | Verifies the cellular modem type, model, carrier, firmware, PRI, SKU, IMEI and other modem details. |
Manual Modem Firmware Upgrade: Example

Router#  sh cellu 0/1/0 hardware
Modem Firmware Version = SWI9X30C_02.20.03.00
Modem Firmware built = 2016/06/30 10:54:05
Hardware Version = 1.0
Device Model ID: EM7455
International Mobile Subscriber Identity (IMSI) = <imsi>
International Mobile Equipment Identity (IMEI) = <imei>
Integrated Circuit Card ID (ICCID) = <iccid>
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Modem Online
Current Modem Temperature = 44 deg C
PRI SKU ID = 1102526, PRI version = 002.020_000, Carrier = AT&T
OEM PRI version = 006
Router#cd fw_22_vzw
Router#dir
Directory of bootflash:/fw_22_vzw/
227586  -rw-  64389490  Jun 30 2000 10:21:29 +00:00  74XX_02.20.03.22.cwe
227587  -rw-  16951  Jun 30 2000 10:22:10 +00:00
7455_02.20.03.22_Verizon_002.026_000.nvu
6816092160 bytes total (5965422592 bytes free)
Router#cd
Router#microcode reload cellular 0 2 modem-provision bootflash:/fw_22_vzw/
Reload microcode? [confirm]
Log status of firmware download in router flash?[confirm]
Firmware download status will be logged in bootflash:fwlogfile
Microcode Reload Process launched for cwan slot/bay =0/2; hw type=0x102download option = 0

Router#Success !! send FW Upgrade command to card

********************************************************************
The interface will be Shut Down for Firmware Upgrade
This will terminate any active data connections.
********************************************************************

*************************************************************************
Modem will be upgraded!
Upgrade process will take up to 15 minutes. During this time the modem will be unusable.
Please do not remove power or reload the router during the upgrade process.
*************************************************************************
*Jul  6 10:19:34.701: %LINK-5-CHANGED: Interface Cellular0/1/0, changed state to administratively down
*Jul  6 10:19:34.701: %LINK-5-CHANGED: Interface Cellular0/2/1, changed state to administratively down

FIRMWARE INFO BEFORE UPGRADE:
Modem Device ID: EM7455      MODEM F/W Boot Version: SWI9X30C_02.20.03.00
Modem F/W App Version: SWI9X30C_02.20.03.00      Modem SKU ID: 1102526
Modem Package Identifier:      Modem Carrier String: 4
Modem PRI Ver: 000.006      Modem Carrier Name: ATT
Modem Carrier Revision: 002.020_000

FIRMWARE INFO AFTER UPGRADE:
Modem Device ID: EM7455      MODEM F/W Boot Version: SWI9X30C_02.20.03.00
Modem F/W App Version: SWI9X30C_02.20.03.00      Modem SKU ID: 1102526
Modem Package Identifier:      Modem Carrier String: 4
Modem PRI Ver: 000.006      Modem Carrier Name: ATT
Modem Carrier Revision: 002.020_000

FW_UPGRADE: Modem needs CWE, PRI
*Jul  6 10:19:57.978: %CELL02-5-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
FW_UPGRADE: Upgrade begin at Thu Jul  6 10:20:01 2000
FW_UPGRADE: Firmware upgrade success.....
FW_UPGRADE: Waiting for modem to become online
FIRMWARE INFO AFTER UPGRADE:
Modem Device ID: EM7455
Modem F/W Boot Version: SWI9X30C_02.20.03.22
Modem F/W App Version: SWI9X30C_02.20.03.22
Modem Package Identifier: Modem Carrier String: 5
Modem PRI Ver: 000.006
Modem Carrier Name: VERIZON
Modem Carrier Revision: 002.026_000

F/W Upgrade: Firmware Upgrade has Completed Successfully

*Jul  6 10:21:55.275: %CELLWAN-2-MODEM_RADIO: Cellular0/1/0 Modem radio has been turned on
*Jul  6 10:21:57.276: %LINK-3-UPDOWN: Interface Cellular0/1/0, changed state to down
*Jul  6 10:21:57.277: %LINK-3-UPDOWN: Interface Cellular0/2/1, changed state to down

Router# sh cellu 0/1/0 hardware
Modem Firmware Version = SWI9X30C_02.20.03.22
Hardware Version = 1.0
Device Model ID: EM7455
International Mobile Subscriber Identity (IMSI) =<imsi>
International Mobile Equipment Identity (IMEI) = <imei>
Integrated Circuit Card ID (ICCID) = <iccid>
Digital Network-Number (MSISDN) = <msisdn>
Modem Status = Modem Online
Current Modem Temperature = 0 deg C
PRI SKU ID = 1102526, PRI version = 002.026_000, Carrier = Verizon
OEM PRI version = 006

Configuring dm-log to Utility Flash: Example

Router(config)#controller cellular 0/1/0
Router(config-controller)#lte modem dm-log enable
Router(config-controller)#

*May 8 17:57:09.905: %SYS-5-CONFIG_I: Configured from console by console

Router# show cellular 0/1/0 log dm-log
Integrated DM logging is off
Output path = bootflash:
Filter Type = Default
Filter Name = v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf
Maximum log size = 0 MB
Maximum file size = 0 MB
Log rotation = Disabled

IR1101#show cellular 0/1/0 log dm-log details
Integrated DM logging is off
Output path = bootflash:
Filter Type = Default
Filter Name = v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf
Maximum log size = 0 MB
Maximum file size = 0 MB
Log rotation = Disabled

0 Packets sent to the modem, 0 Bytes, 0 Errors
0 Packets received from the modem, 0 Bytes, 0 Input drops
0 Packets stored in file system, 0 Bytes, 0 Errors, 0 Aborts
0 Max rcv queue size

Current file size = 0 MB
Current log size = 0 MB
Total log size = 0 MB
IR1101#
SNMP MIBs

A MIB (Management Information Base) is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces.

You can find complete information on MIBS and the MIB locator here: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

It is recommended that you configure SNMP V3 with authentication/privacy when implementing SNMP SET operation.


The following Simple Management Network Protocol (SNMP) MIBs are supported on Cisco 4G LTE Advanced:

- IF-MIB
- ENTITY-MIB
- CISCO-WAN-3G-MIB
- CISCO-WAN-CELL-EXT-MIB

For the CISCO-WAN-3G-MIB, the following tables and sub-tables are supported for 3G and LTE technologies:

- ciscoWan3gMIB(661)
- ciscoWan3gMIBNotifs(0)
- ciscoWan3gMIBObjects(1)
- c3gWanCommonTable(1)
- c3gWanGsm(3)
- c3gGsmIdentityTable(1)
- c3gGsmNetworkTable(2)
- c3gGsmPdpProfile(3)
- c3gGsmPdpProfileTable(1)
- c3gGsmPacketSessionTable(2)
- c3gGsmRadio(4)
- c3gGsmRadioTable(1)
- c3gGsmSecurity(5)
- c3gGsmSecurityTable(1)
For the CISCO-WAN-CELL-EXT-MIB, the following tables and sub-tables are supported for LTE technology only:

- ciscoWanCellExtMIB(817)
- ciscoWanCellExtMIBNotifs(0)
- ciscoWanCellExtMIBObjects(1)
- ciscoWanCellExtLte(1)
- cwceLteRadio(1)
- cwceLteProfile(2)

You can download the MIBs from the Cisco MIB Locator at http://www.cisco.com/go/mibs.

### SNMP 4G LTE Advanced Configuration: Example

The following example describes how to configure 3G 4G MIB trap on the router:

```plaintext
controller Cellular 0/1/0
lte event rssi onset mib-trap All-lte
lte event rssi onset threshold -100
lte event rssi abate mib-trap All-lte
lte event rssi abate threshold -90
lte event temperature onset mib-trap
lte event temperature abate mib-trap
lte event temperature abate threshold 55
lte event modem-state mib-trap all
lte event service mib-trap
lte event network mib-trap
lte event connection-status mib-trap All-lte
lte event rsrp onset mib-trap All-lte
lte event rsrp abate mib-trap All-lte
lte event rsrp abate threshold -85
lte event rsrq onset mib-trap All-lte
lte event rsrq onset threshold -80
lte event rsrq abate mib-trap All-lte
lte event rsrq abate threshold -6
```

The following example describes how to configure SNMP capability on the router:

```plaintext
snmp-server group neomobilityTeam v3 auth notify 3gView
snmp-server view 3gView ciscoWan3gMIB included
snmp-server community neomobility-test RW
snmp-server community public RW
snmp-server enable traps c3g
snmp server enable traps LTE
snmp-server host 172.19.153.53 neomobility c3g
snmp-server host 172.19.152.77 public c3g
snmp-server host 172.19.152.77 public udp-port 6059
```

The following example describes how to configure an external host device to communicate with the router through SNMP:

```plaintext
setenv SR_MGR_CONF_DIR /users/<userid>/mibtest
setenv SR_UTIL_COMMUNITY neomobility-test
setenv SR_UTIL_SNMP_VERSION -v2c
setenv SR_TRAP_TEST_PORT 6059
```
Troubleshooting

This section provides the essential information and resources available for troubleshooting the Cisco 4G LTE Advanced feature.

Verifying Data Call Setup

To verify the data call setup, follow these steps:

1. After you create a modem data profile using the cellular profile create command and configuring DDR on the cellular interface, send a ping from the router to a host across the wireless network.

2. If the ping fails, debug the failure by using the following debug and show commands:

   3. debug chat
   4. debug modem
   5. debug dialer
   6. show cellular all
   7. show controller cell0/1/0
   8. show interface cellular
   9. show running-config
   10. show ip route
   11. show platform
   12. Save the output from these commands and contact your system administrator.

Checking Signal Strength

If the Received Signal Strength Indication (RSSI) level is very low (for example, if it is less than –110 dBm), follow these steps:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ensure at least one antenna is connected to the 'MAIN' RF port on the 4G module. Preferably both MAIN and DIV RF ports should be connected to antenna for better RF signal. Check to ensure the antenna are threaded and tightened.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact your wireless service provider to verify if there is service availability in your area.</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Service Availability

The following is a sample output for the `show cellular all` command for a scenario where the antenna is disconnected and a modem data profile has not been created.

```
Router# show cellular 0/1/0 all
Hardware Information
--------------------
Modem Firmware Version = SWI9X07Y_02.18.05.00
Device Model ID = WP7603
International Mobile Subscriber Identity (IMSI) = 001012345678901
Integrated Circuit Card ID (ICCID) = 898600000502000180722
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Factory Serial Number (FSN) = U3734285450506
Modem Status = Modem Online
Current Modem Temperature = 49 deg C
PRI SKU ID = 1103507, PRI version = 002.041_002, Carrier = GENERIC
OEM PRI version = 002.000

Profile Information
-------------------
Profile 1 = ACTIVE* **
--------
PDP Type = IPv4v6
PDP address = 192.1.1.21
PDP IPV6 address = FC01:ABAB:CDCD:EFE0:7DC4:256:B64F:22F8/64 Scope: Global
Access Point Name (APN) = broadband
Authentication = None
Primary DNS address = 192.1.1.2
Primary DNS IPV6 address = FC01:CAFE:0:0:0:0:1
Secondary DNS IPV6 address = 0:0:0:0:0:0:0:0
* - Default profile
** - LTE attach profile

Configured default profile for active SIM 0 is profile 1.

Data Connection Information
-----------------------------
Profile 1, Packet Session Status = ACTIVE
Cellular0/1/0:
Data Packets Transmitted = 31546, Received = 57008
Data Transmitted = 5049096 bytes, Received = 7702570 bytes
IP address = 192.1.1.21
IPV6 address = FC01:ABAB:CDCD:EFE0:7DC4:256:B64F:22F8/64 Scope: Global
Primary DNS address = 192.1.1.2
Primary DNS IPV6 address = FC01:CAFE:0:0:0:0:1
Secondary DNS IPV6 address = 0:0:0:0:0:0:0:0
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
Profile 6, Packet Session Status = INACTIVE
Profile 7, Packet Session Status = INACTIVE
Profile 8, Packet Session Status = INACTIVE
Profile 9, Packet Session Status = INACTIVE
Profile 10, Packet Session Status = INACTIVE
```
Profile 11, Packet Session Status = INACTIVE
Profile 12, Packet Session Status = INACTIVE
Profile 13, Packet Session Status = INACTIVE
Profile 14, Packet Session Status = INACTIVE
Profile 15, Packet Session Status = INACTIVE
Profile 16, Packet Session Status = INACTIVE

Network Information
-------------------
Current System Time = Thu Jan 10 8:31:28 1980
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = Test PLMN 1-1
Mobile Country Code (MCC) = 1
Mobile Network Code (MNC) = 1
Packet switch domain (PS) state = Attached
Registration state (EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1
Cell ID = 256
Negotiated network MTU = 1500

Radio Information
------------------
Radio power mode = online
LTE Rx Channel Number = 2175
LTE Tx Channel Number = 20175
LTE Band = 4
LTE Bandwidth = 20 MHz
Current RSSI = -68 dBm
Current RSRP = -102 dBm
Current RSRQ = -13 dB
Current SNR = 19.4 dB
Physical Cell Id = 0
Number of nearby cells = 1
Idx PCI (Physical Cell Id)

1 0
Radio Access Technology (RAT) Preference = AUTO
Radio Access Technology (RAT) Selected = LTE

LTE bands supported by modem:
- Bands 2 4 5 12.

LTE band Preference settings for the active sim (slot 0):
- Bands 2 4 5 12.

Non-LTE bands supported by modem:
Index:
88 - WCDMA US PCS 1900 band
90 - WCDMA US 1700 band
91 - WCDMA US 850 band

Non-LTE band Preference settings for the active sim (slot 0):
Index:
88 - WCDMA US PCS 1900 band
90 - WCDMA US 1700 band
91 - WCDMA US 850 band

Band index reference list:
Indices 1-64 correspond to LTE bands 1-64.
Indices 65-128 correspond to Non-LTE bands.

Modem Security Information
-------------------------------
Active SIM = 0
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

Cellular Firmware List
------------------------
<table>
<thead>
<tr>
<th>Idx</th>
<th>Carrier</th>
<th>FwVersion</th>
<th>PriVersion</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ATT</td>
<td>02.18.04.00</td>
<td>002.039_000</td>
<td>Inactive</td>
</tr>
<tr>
<td>2</td>
<td>GENERIC</td>
<td>02.18.05.00</td>
<td>002.041_002</td>
<td>Active</td>
</tr>
<tr>
<td>3</td>
<td>VERIZON</td>
<td>02.17.01.00</td>
<td>002.036_000</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

Firmware Activation mode = MANUAL

FOTA Information
-----------------
FOTA server poll timer (mins) = Disable
FOTA server connection retry value = 0
FOTA status = Please re-configure FOTA poll timer

GPS Information
-----------------
GPS Feature = enabled
GPS Mode Configured = not configured
GPS Status = NMEA Disabled

SMS Information
-----------------
Incoming Message Information
-------------------------------
SMS stored in modem = 7
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 7
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0

Outgoing Message Information
-------------------------------
Total SMS sent successfully = 0
Total SMS send failure = 0
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status = 0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
  Reference Number = 0
  Result Code = 0x0
  Diag Code = 0x0 0x0 0x0 0x0 0x0 0x0

SMS Archive URL =
Modem Crashdump Information
---------------------------------
Modem crashdump logging = off

Successful Call Setup

The following is a sample output when a call is set up. It shows a received IP address from the network. Call setup is successful and data path is open.

default cellular 0/1/0 messages callcontrol

Modem Troubleshooting Using Integrated Modem DM Logging

As part of the 3G and 4G serviceability enhancement in Cisco IOS, DM log collection has been integrated into Cisco IOS, eliminating the need for an external PC and simplifying the DM log collection process. The lte modem dm-log command can be used in controller cellular configuration mode to configure integrated DM logging to monitor traffic on the modem. See the Cisco 3G and 4G Serviceability Enhancement User Guide for more information on configuring Integrated DM Logging parameters.

Modem Settings for North America and Carriers Operating on 700 MHz Band

For LTE-EA deployments in North America and for carriers operating in the 700 MHz band, the following changes to the modem settings are required to prevent long network attach times.

The output of show cellular 0/1/0 all command shows the following:
- Current RSSI is –125 dBM
- LTE Technology Preference = No preference specified (AUTO)

The following sections explain useful commands for changing modem settings:

Changing Modem Settings

To change the modem settings to force the modem to scan different technologies, use the following Cisco IOS command:

```
Router# cellular 0/1/0 lte technology ?
auto Automatic LTE Technology Selection
lte LTE
umts UMTS
```

Electronic Serial Number (ESN)

The ESN number is located directly on the modem label in hexadecimal notation. It can also be retrieved using the Cisco IOS CLI using the show cellular slot/port/module hardware command.

The sample output below shows the ESN number:

```
Hardware Information
----------------------
Electronic Serial Number (ESN) = 0x603c9854 [09603971156]
Electronic Serial Number (ESN) = <specific ESN in hexadecimal> [specific ESN in decimal]
CHAPTER 19

Configuring Cellular IPv6 Address

• Cellular IPv6 Address, on page 269
• Configuring a Deterministic IPv6 Host Address, on page 273

Cellular IPv6 Address

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of the same IPv6 address:

- 2001:CDBA::3257:9652 (zeros can be omitted)

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats.

An IPv6 address prefix, in the format ipv6-prefix/prefix-length, can be used to represent bit-wise contiguous blocks of the entire address space. The ipv6-prefix must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:cdba::3257:9652 /64 is a valid IPv6 prefix.

IPv6 Unicast Routing

An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

The IR1101 supports the following address types:

Link-Local Address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. An link-local address is automatically configured on the cellular interface when an IPv6 address is enabled.

After the data call is established, the link-local address on the cellular interface is updated with the host generated link-local address that consists of the link-local prefix FF80::/10 (1111 1110 10) and the
Global Address

Configuring Cellular IPv6 Address

To configure the cellular IPv6 address, perform these steps:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ipv6 unicast-routing</td>
<td>Enable IPv6 routing globally on the router.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface cellular <code>&lt;slot/port/interface&gt;</code></td>
<td>Specifies the cellular interface. The IR1101 has the primary Cellular interface as 0/1/0.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>description <code>&lt;text&gt;</code></td>
<td>Provides a description for the cellular interface, if desired.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ipv6 address <code>&lt;options&gt;</code></td>
<td>Specifies that the IP address for a particular interface is dynamically obtained.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>load-interval <code>&lt;seconds&gt;</code></td>
<td>Specifies the length of time for which data is used to compute load statistics.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>dialer in-band</td>
<td>Enables DDR and configures the specified serial interface to use in-band dialing.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>dialer idle-timeout <code>&lt;seconds&gt;</code></td>
<td>Specifies the dialer idle timeout period.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>dialer watch-group <code>&lt;group number&gt;</code></td>
<td>Specifies the number of the dialer access group to which the specific interface belongs.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# dialer watch-group 1</code></td>
<td>Enables IPv6.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 10** ipv6 enable  
  Example:  
  `Router(config-if)# ipv6 enable` | Enables IPv6. |
| **Step 11** pulse time `<seconds>`  
  Example:  
  `Router(config-if)# pulse-time 1` | Define pulse time |
| **Step 12** ip virtual-reassembly  
  Example:  
  `Router(config-if)# ip virtual-reassembly` | Enable Virtual Fragment Reassembly (default is ‘in’ only). |
| **Step 13** no shutdown  
  Example:  
  `Router(config-if)# no shutdown` | No shutdown the interface |
| **Step 14** exit  
  Example:  
  `Router(config-if)# exit` | Exit from the interface configuration. |
| **Step 15** access-list 1 permit any  
  Example:  
  `Router(config)#access-list 1 permit any` | Defines traffic of interest. |
| **Step 16** dialer watch-list 1 `<ipaddress>` `<mask>`  
  Example:  
  `Router(config)#dialer watch-list 1 ip 5.6.7.8 255.255.255.255` | Defines IP and mask for a watch list. |
| **Step 17** dialer watch-list 1 delay route-check initial 60  
  Example:  
  `Router(config)#dialer watch-list 1 delay route-check initial 60` | Defines delay for a route check. |
| **Step 18** dialer watch-list 1 delay connect 1  
  Example:  
  `Router(config)#dialer watch-list 1 delay connect 1` | Defines delay for connect. |
| **Step 19** dialer-list 1 protocol ip permit  
  Example:  
  `Router(config)#dialer-list 1 protocol ip permit` | Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 20</strong></td>
<td></td>
</tr>
<tr>
<td>dialer-list 1 protocol ipv6 permit</td>
<td>Permits IPv6 on the dialer list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)#dialer-list 1 protocol ipv6 permit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 route &lt;destination ipv6 prefix&gt;/ &lt;destination mask&gt; [forwarding router address</td>
<td>Defines the route.</td>
</tr>
<tr>
<td>interface</td>
<td>other options]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)#ipv6 route ::/0 Cellular0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exits to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)#end</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the Cellular IPv6 configuration:

```
ltc sim data-profile 1 attach-profile 1 slot 0
ltc sim data-profile 1 attach-profile 1 slot 1
ltc interface 0 64 1111:2222:3333:0001
ltc gps mode standalone
ltc modem dm-log size 2
ltc modem dm-log filesize 1
ltc modem dm-log rotation
ltc modem link-recovery disable

interface Loopback0
   ip address 1.1.1.1 255.255.255.255

interface Cellular0/1/0
   description Cell-to-CMW
   ip address negotiated
   load-interval 30
   dialer in-band
   dialer idle-timeout 0
   dialer watch-group 1
   ipv6 enable
   pulse-time 1
   ip virtual-reassembly

interface Cellular0/1/1
   no ip address
   shutdown
   ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
   ipv6 route ::/0 Cellular0/1/0
```

```
access-list 1 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
```
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit

Configuring a Deterministic IPv6 Host Address

Deterministic IPv6 addresses allow a user to configure a static, user-specified IPv6 address host portion for the interface. While IPv6 address network and subnet parts may be assigned by the ISP, the host part remains unchanged using this configuration. This allows devices to have known, pre-determined IPv6 addresses in their network.

To configure the a deterministic IPv6 host address, perform these steps:

**SUMMARY STEPS**

1. config terminal
2. ipv6 unicast-routing
3. interface Cellular <slot/port/interface>
4. enable ipv6
5. ipv6 address autoconfig
6. no shut
7. controller cellular <controller slot/port adapter/port>
8. lte interface <interface number> <address length 48-80> <deterministic address suffix>
9. end
10. clear int cellular 0/1/0

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Enable IPv6 routing. |
| **Example:** | | 
| Router(config)# ipv6 unicast-routing | |

| **Step 3** | Specifies the cellular interface. |
| **Example:** | | 
| Router(config)# interface Cellular 0/1/0 | |

<p>| <strong>Step 4</strong> | Enables IPv6. |
| <strong>Example:</strong> | |
| Router(config-if)# enable ipv6 | |</p>
<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>ipv6 address autoconfig</td>
<td>Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 address autoconfig</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>no shut</td>
<td>Shutdown Interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# no shut</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>controller cellular</td>
<td>Configure the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td>lte interface</td>
<td>Specify in controller config the deterministic IPv6 address for cellular interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# lte interface 0 64 1111:2222:3333:1234</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td>clear int cellular 0/1/0</td>
<td>Clears the cellular interface and forces the cellular interface to reacquire IP address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# clear int cellular 0/1/0</td>
<td></td>
</tr>
</tbody>
</table>

**Example**
The following example shows the configuration:

```plaintext
controller Cellular 0/1/0
lte sim data-profile 1 attach-profile 1 slot 0
lte sim data-profile 1 attach-profile 1 slot 1
no lte firmware auto-sim
lte interface 0 64 1111:2222:3333:00001
lte gps mode standalone
lte modem dm-log size 2
lte modem dm-log filesize 1
lte modem dm-log rotation
lte modem link-recovery disable
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.255
!
interface Cellular0/1/0
description Cell-to-CMW
```
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
dialer-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/1/1
 no ip address
 shutdown
!
   ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
 ipv6 route ::/0 Cellular0/1/0
   !
   access-list 1 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
 !
   ...
CHAPTER 20

Information About SCADA

This chapter contains the following sections:

- SCADA Overview, on page 277
- Role of the IR1101, on page 278
- Key Terms, on page 278
- Protocol Translation Application, on page 278
- Prerequisites, on page 279
- Guidelines and Limitations, on page 280
- Default Settings, on page 280
- Configuring Protocol Translation, on page 280
- Configuring the T101 Protocol Stack, on page 281
- Configuring the T104 Protocol Stack, on page 284
- Configuration Example, on page 287
- Yang Data Model Support for Scada, on page 288
- Configuring the DNP3 Protocol Stacks, on page 291
- Starting and Stopping the Protocol Translation Engine, on page 294
- Verifying Configuration, on page 295
- Debug Commands, on page 295

SCADA Overview

SCADA refers to a control and management system employed in industries such as water management, electric power, and manufacturing. A SCADA system collects data from various types of equipment within the system and forwards that information back to a Control Center for analysis. Generally, individuals located at the Control Center monitor the activity on the SCADA system and intervene when necessary.

The Remote Terminal Unit (RTU) acts as the primary control system within a SCADA system. RTUs are configured to control specific functions within the SCADA system, which can be modified as necessary through a user interface.

On the IR1101, line is 0/2/0 same as the Async interface.
Role of the IR1101

In the network, the Control Center always serves as the master in the network when communicating with the IR1101. The IR1101 serves as a proxy master station for the Control Center when it communicates with the RTU.

The IR1101 provides protocol translation to serve as a SCADA gateway to do the following:

- Receive data from RTUs and relay configuration commands from the Control Center to RTUs.
- Receive configuration commands from the Control Center and relay RTU data to the Control Center
- Terminate incoming requests from the Control Center, when an RTU is offline.

The IR1101 performs Protocol Translation for the following protocols:

- IEC 60870 T101 to/from IEC 60870 T104.
- DNP3 serial to DNP3 IP

Key Terms

The following terms are relevant when you configure the T101 and T104 protocol stacks on the IR1101:

- Channel–A channel is configured on each IR1101 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single T101 (RTU) or T104 (Control Center) protocol stack.
- Link Address–Refers to the device or station address.
- Link Mode (Balanced and Unbalanced)–Refers to the modes of data transfer.
  - An Unbalanced setting refers to a data transfer initiated from the master.
  - A Balanced setting can refer to either a master or slave initiated data transfer.
- Sector–Refers to a single RTU within a remote site.
- Sessions–Represents a single connection to a remote site.

The following terms are relevant when you configure the DNP3 protocol stacks on the on the IR1101:

- Channel–A channel is configured on the IR1101 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single DNP3 serial (RTU) or DNP3 IP (Control Center) protocol stack.
- Link Address–Refers to the device or station address.
- Sessions–Represents a single connection to a remote site.

Protocol Translation Application

In Figure 91: Routers Within a SCADA System, on page 279 the IR1101 (installed within a secondary substation of the Utility Network) employs Protocol Translation to provide secure, end-to-end connectivity between Control Centers and RTUs within a SCADA System.

The IR1101 connects to the RTU (slave) through a RS232 connection. To protect the traffic when forwarded over public infrastructures (for example, cellular), the IR1101 forwards SCADA data from the RTU to the Control Center in the SCADA system through an IPSec tunnel (FlexVPN site-to-site or hub and spoke). The
IPSec tunnel protects all traffic between the IR1101 and the Head-end aggregation router. SCADA traffic can be inspected through an IPS device positioned in the path of the SCADA traffic before it is forwarded to the proper Control Center.

Prerequisites

RTUs must be configured and operating in the network.

For each RTU that connects to the IR1101, you will need the following information for T101/T104:

- Channel information
  - Channel name
  - Connection type: serial
  - Link transmission procedure setting: unbalanced or balanced
  - Address field of the link (number expressed in octets)

- Session information
  - Session name
  - Size of common address of Application Service Data Unit (ASDU) (number expressed in octets)
  - Cause of transmission (COT) size (number expressed in octets)
  - Information object address (IOA) size (number expressed in octets)

- Sector information
  - Sector name
  - ASDU address, (number expressed in octets)

For each RTU that connects to the IR1101, you will need the following information for DNP3:
Guidelines and Limitations

Each channel supports only one session.

Each session supports only one sector.

Default Settings

<table>
<thead>
<tr>
<th>T101/T104 Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role for T101</td>
<td>Master</td>
</tr>
<tr>
<td>Role for T104</td>
<td>Slave</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNP3 Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsolicited Response (DNP3-serial)</td>
<td>Not Enabled</td>
</tr>
<tr>
<td>Send Unsolicited Message (DNP3-IP)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Configuring Protocol Translation

This section includes the following topics:

Note

Before making any configuration changes to a IR1101 operating with Protocol Translation, please review the section on Starting and Stopping the Protocol Translation Engine, on page 294.

Enabling the IR1101 Serial Port and SCADA Encapsulation

Before you can enable and configure Protocol Translation on the IR1101, you must first enable the serial port on the IR1101 and enable SCADA encapsulation on that port.
Before you begin

Determine availability of serial port on the IR1101.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface async slot/port/interface</td>
<td>Enters the interface command mode for the async slot/port/interface.</td>
</tr>
<tr>
<td>slot –value of 0</td>
<td></td>
</tr>
<tr>
<td>port –value of 2</td>
<td></td>
</tr>
<tr>
<td>interface –value of 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no shutdown</td>
<td>Brings up the port, administratively.</td>
</tr>
<tr>
<td><strong>Step 4</strong> encapsulation scada</td>
<td>Enables encapsulation on the serial port for protocol translation and other SCADA protocols.</td>
</tr>
</tbody>
</table>

### EXAMPLE

This example shows how to enable serial port 0/2/0 and how to enable encapsulation on that interface to support SCADA protocols.

```
router# configure terminal
router(config)# interface async 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
```

### Configuring T101 and T104 Protocol Stacks

You can configure T101 and T104 protocol stacks, which allow end-to-end communication between Control Centers (T104) and RTUs (T101) within a SCADA system.

- Configuring the T101 Protocol Stack, on page 281
- Configuring the T104 Protocol Stack, on page 284
- Starting and Stopping the Protocol Translation Engine, on page 294

### Prerequisites

Ensure that you have gathered all the required configuration information.

Enable the serial port and SCADA encapsulation.

### Configuring the T101 Protocol Stack

Configure the channel, session, and sector parameters for the T101 protocol stack.
### Configuring the T101 Protocol Stack

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>scada-gw protocol t101</code></td>
<td>Enters the configuration mode for the T101 protocol.</td>
</tr>
</tbody>
</table>
| 3    | `channel channel_name` | Enters the channel configuration mode for the T101 protocol.  
*channel_name* – Identifies the channel on which the serial port of the IR1101 communicates to the RTU.  
*Note* When the entered channel name does not already exist, the router creates a new channel.  
Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel. |
| 4    | `role master` | Assigns the master role to the T101 protocol channel (default). |
| 5    | `link-mode {balanced | unbalanced}` | Configures the link-mode as either balanced or unbalanced.  
unbalanced – Refers to a data transfer initiated from the master.  
balanced – Refers to either a master or slave data transfer. |
| 6    | `link-addr-size {none | one | two}` | Defines the link address size in octets. |
| 7    | `bind-to-interface async slot/port/interface` | Defines the IR1101 serial interface on which the system sends its T101 protocol traffic.  
*slot* – Value of 0  
*port* – Value of 2  
*interface* – Value of 0 |
| 8    | `exit` | Ends configuration of the channel and exits the channel configuration mode. Saves all settings. |
| 9    | `session session_name` | Enters the session configuration mode and assigns a name to the session. |
| 10   | `attach-to-channel channel_name` | Attaches the session to the channel. Enter the same channel name that you entered in Step 3.  
*channel_name* – Identifies the channel. |
<p>| 11   | <code>common-addr-size {one | two | three}</code> | Defines the common address size in octets. |
| 12   | <code>cot size {one | two | three}</code> | Defines the cause of transmission such as spontaneous or cyclic data schemes in octets. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 13</td>
<td>info-obj-addr-size {one</td>
</tr>
<tr>
<td>Step 14</td>
<td>link-addr-size {one</td>
</tr>
<tr>
<td>Step 15</td>
<td>link-addr link_address Refers to the link address of the RTU.</td>
</tr>
<tr>
<td></td>
<td>Note The link address entered here must match the value set on the RTU to which the serial port connects.</td>
</tr>
<tr>
<td></td>
<td>link_address –Range of 0-65535.</td>
</tr>
<tr>
<td>Step 16</td>
<td>exit Exits the session configuration mode.</td>
</tr>
<tr>
<td>Step 17</td>
<td>sector sector_name Enters the sector configuration mode and assigns a name to the sector for the RTU.</td>
</tr>
<tr>
<td></td>
<td>sector_name –Identifies the sector.</td>
</tr>
<tr>
<td>Step 18</td>
<td>attach-to-session session_name Attaches the RTU sector to the session.</td>
</tr>
<tr>
<td></td>
<td>Enter the same session name that you entered in Step 9.</td>
</tr>
<tr>
<td></td>
<td>session_name- Identifies the session.</td>
</tr>
<tr>
<td>Step 19</td>
<td>asdu-addr asdu_address Refers to the ASDU structure address of the RTU.</td>
</tr>
<tr>
<td>Step 20</td>
<td>exit Exits the sector configuration mode.</td>
</tr>
<tr>
<td>Step 21</td>
<td>exit Exits the protocol configuration mode.</td>
</tr>
</tbody>
</table>

**EXAMPLE**

This example shows how to configure the parameters for the T101 protocol stack for RTU_10.

```
router# configure terminal
router(config)# scada-gw protocol t101
router(config-t101)# channel rtu_channel
router(config-t101-channel)# role master
router(config-t101-channel)# link-mode unbalanced
router(config-t101-channel)# link-addr-size one
router(config-t101-channel)# bind-to-interface async 0/2/0
router(config-t101-channel)# exit
router(config-t101)# session rtu_session
router(config-t101-session)# attach-to-channel rtu_channel
router(config-t101-session)# common-addr-size two
router(config-t101-session)# cot-size one
router(config-t101-session)# info-obj-addr-size two
router(config-t101-session)# link-addr 3
router(config-t101-session)# exit
router(config-t101)# sector rtu_sector
router(config-t101-sector)# attach-to-session rtu_session
router(config-t101-sector)# asdu-addr 3
router(config-t101-sector)# exit
```
Configuring the T104 Protocol Stack

Follow the steps below for each Control Center that you want to connect to over a T104 protocol.

**Before you begin**

Ensure that you have gathered all the required configuration information. (See Prerequisites, on page 279)

Enable the serial port and SCADA encapsulation. (See Enabling the IR1101 Serial Port and SCADA Encapsulation, on page 280)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>scada-gw protocol t104</td>
<td>Enters the configuration mode for the T104 protocol.</td>
</tr>
</tbody>
</table>
| Step 3 | channel channel_name | Enters the channel configuration mode for the T104 protocol.  
channel_name – Identifies the channel on which the router communicates with the Control Center.  
**Note**  
When the entered channel name does not already exist, the router creates a new channel.  
Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel. |
| Step 4 | k-value value | Sets the maximum number of outstanding Application Protocol Data Units (APDUs) for the channel.  
**Note** An APDU incorporates the ASDU and a control header.  
value – Range of values from 1 to 32767. Default value is 12 APDUs. |
| Step 5 | w-value value | Sets the maximum number of APDUs for the channel.  
value – Range of values from 1 to 32767. Default value is 8 APDUs. |
<p>| Step 6 | t0-timeout value | Defines the t0-timeout value for connection establishment of the T104 channel. |
| Step 7 | t1-timeout value | Defines the t1-timeout value for send or test APDUs on the T104 channel. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> t2-timeout value</td>
<td>Defines the t2-timeout value for acknowledgements when the router receives no data message.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The t2 value must always be set to a lower value than the t1 value on the T104 channel.</td>
</tr>
<tr>
<td><strong>Step 9</strong> t3-timeout value</td>
<td>Defines the t3-timeout value for sending s-frames in case of a long idle state on the T104 channel.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The t3 value must always be set to a higher value than the t1 value on the T104 channel.</td>
</tr>
<tr>
<td><strong>Step 10</strong> tcp-connection {0</td>
<td>1} local-port {port_number</td>
</tr>
<tr>
<td></td>
<td>port-number –value between 2000 and 65535.</td>
</tr>
<tr>
<td></td>
<td>default–value of 2404.</td>
</tr>
<tr>
<td></td>
<td>A.B.C.D –single host.</td>
</tr>
<tr>
<td></td>
<td>A.B.C.D/nn –subnet A.B.C.D/LEN.</td>
</tr>
<tr>
<td></td>
<td>any–any remote hosts 0.0.0.0/0.</td>
</tr>
<tr>
<td></td>
<td>WORD–VRF name.</td>
</tr>
<tr>
<td><strong>Step 11</strong> exit</td>
<td>Exits the channel configuration mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong> session session_name</td>
<td>Enters the session configuration mode and assigns a name to the session.</td>
</tr>
<tr>
<td></td>
<td>session_name –Use the same name that you assigned to the channel in Step 3.</td>
</tr>
<tr>
<td><strong>Step 13</strong> attach-to-channel channel_name</td>
<td>Defines the name of the channel that transports the session traffic.</td>
</tr>
<tr>
<td><strong>Step 14</strong> cot size {one</td>
<td>two</td>
</tr>
<tr>
<td><strong>Step 15</strong> exit</td>
<td>Exits the session configuration mode.</td>
</tr>
<tr>
<td><strong>Step 16</strong> sector sector_name</td>
<td>Enters the sector configuration mode and assigns a name to the sector for the Control Center.</td>
</tr>
<tr>
<td><strong>Step 17</strong> attach-to-session session_name</td>
<td>Attaches the Control Center sector to the channel.</td>
</tr>
<tr>
<td></td>
<td>session_name –Use the same name that you assigned to the channel in Step 3.</td>
</tr>
<tr>
<td><strong>Step 18</strong> asdu-addr asdu_address</td>
<td>Refers to the ASDU structure address. Value entered here must match the ASDU value on the RTU.</td>
</tr>
<tr>
<td></td>
<td>asdu_address –asdu_address –Value of 1 or 2.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>step 19 map-to-sector sector_name</td>
<td>Maps the Control Center (T104) sector to the RTU (T101) sector.</td>
</tr>
<tr>
<td>Start 20</td>
<td>Return to Step 1.</td>
</tr>
<tr>
<td>Return to Step 1</td>
<td>Repeat all steps in this section for each Control Center active in the network.</td>
</tr>
</tbody>
</table>

**EXAMPLE**

This example shows how to configure the parameters for the T104 protocol stack on Control Center 1 and Control Center 2, both of which are configured as masters, and how to map the T104 sector to the T101 sector.

To configure Control Center 1 (cc_master1), enter the following commands.

```
router# configure terminal
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master1
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2050 remote-ip 209.165.200.225
router(config-t104-channel)# tcp-connection 1 local-port 2051 remote-ip 209.165.201.25
router(config-t104-channel)# exit
router(config-t104)# session cc_master1
router(config-t104-session)# attach-to-channel cc_master1
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master1-sector
router(config-t104-sector)# attach-to-session cc_master1
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104)# exit
router(config)#
```

To configure Control Center 2 (cc_master2), enter the following commands.

```
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master2
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2060 remote-ip 209.165.201.237
router(config-t104-channel)# tcp-connection 1 local-port 2061 remote-ip 209.165.200.27
router(config-t104-channel)# exit
router(config-t104)# session cc_master2
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
```
Configuration Example

The following example shows how to configure the serial port interface for T101 connection, configure T101 and T104 protocol stacks, and starts the Protocol Translation Engine on the IR1101.

```plaintext
router# configure terminal
router (config)# interface async 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
router (config-if)# exit
router (config)# scada-gw protocol t101
router (config-t101)# channel rtu_channel
router (config-t101-channel)# role master
router (config-t101-channel)# link-mode unbalanced
router (config-t101-channel)# link-addr-size one
router (config-t101-channel)# bind-to-interface async 0/2/0
router (config-t101-channel)# exit
router (config-t101)# session rtu_session
router (config-t101-session)# attach-to-channel rtu_channel
router (config-t101-session)# common-addr-size two
router (config-t101-session)# cot-size one
router (config-t101-session)# info-obj-addr-size two
router (config-t101-session)# link-addr 3
router (config-t101-session)# exit
router (config-t101)# sector rtu_sector
router (config-t101-sector)# attach-to-session rtu_session
router (config-t101-sector)# asdu-adr 3
router (config-t101-sector)# map-to-sector rtu_sector
router (config-t101)# exit
router (config-t101)# session cc_master1
router (config-t101-session)# attach-to-channel cc_master1
router (config-t101-session)# cot-size two
router (config-t101-session)# exit
router (config-t101)# sector cc_master1-sector
router (config-t101-sector)# attach-to-session cc_master1
router (config-t101-sector)# asdu-adr 3
router (config-t101-sector)# map-to-sector rtu_sector
router (config-t101)# exit
router (config-t101)# session cc_master2
```
This example configures end-to-end communication between Control Centers and RTUs within a SCADA system using the DNP3 protocol stacks and starts the Protocol Translation Engine on the IR1101:

```plaintext
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit
router(config-t104)# exit
router(config)# scada-gw enable
```

IOA addresses obtained from T101 side are sent to T104 side without any modification by the SCADA Gateway.

---

**Yang Data Model Support for Scada**

The Cisco IOS XE 17.1.1 introduces support for the Cisco IOS XE YANG model for the Scada System. Previous releases already provided Yang models in other areas.

[https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17111](https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17111)
Scada Yang Models

There are two feature modules available for Scada that belong to the main Cisco-IOS-XE-native model:

- Cisco-IOS-XE-scada-gw.yang

This module contains a collection of YANG definitions for Scada Gateway Configuration commands.

- Cisco-IOS-XE-scada-gw-oper.yang

This module contains a collection of YANG definitions for Scada Gateway operational data.

There are 8 dependent modules (also belonging to the main Cisco-IOS-XE-native model), that should be imported for the Scada models to work. The following section shows the Scada Yang Models list, configuration CLI commands, and the dependent modules that each feature module covers.

Cisco-IOS-XE-scada-gw

This module has the following corresponding Cli commands:

```
(config)# scada-gw protocol t101
(config-t101)# channel <channel-name>
(config-t101)# bind-to-interface <interface-name>
(config-t101)# link-mode <link-mode>
(config-t101)# link-addr-size <size>
(config-t101)# day-of-week <enable>
(config-t101)# session <session_name>
(config-t101)# attach-to-channel <channel-name>
(config-t101)# cot-size <size>
(config-t101)# common-addr-size <size>
(config-t101)# info-obj-addr-size <size>
(config-t101)# link-addr <addr>
(config-t101)# request
(config-t101)# sector <sector_name>
(config-t101)# attach-to-session <session-name>
(config-t101)# asdu-addr <addr>
(config-t101)# request
(config-t101)# scada-gw protocol t104
(config-t104)# channel <channel-name>
(config-t104)# tcp connection

(config-t104)# to-timeout <value>
(config-t104)# t1-timeout <value>
(config-t104)# t2-timeout <value>
```
The Cisco-IOS-XE-scada-gw module has the following dependent modules:

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (any revision)
- cisco-semver

Cisco-IOS-XE-scada-gw-oper

This module has the following corresponding CLI commands:

```
# show scada statistics
# show scada tcp
```

The Cisco-IOS-XE-scada-gw-oper module has the following dependent modules:

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (any revision)
- cisco-semver
Configuring the DNP3 Protocol Stacks

You can configure the DNP3 serial and DNP3 IP protocol stacks, which allow end-to-end communication between Control Centers and RTUs within a SCADA system.

Configuring DNP3 Serial

Configure the channel and session parameters for the DNP serial communication with an RTU.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> scada-gw protocol dnp3-serial</td>
<td>Enters configuration mode for the DNP3 serial protocol.</td>
</tr>
<tr>
<td><strong>Step 3</strong> channel channel_name</td>
<td>Enters channel configuration mode for the DNP3 serial protocol.</td>
</tr>
<tr>
<td></td>
<td>channel_name –Identifies the channel on which the router serial port communicates to the RTU.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered channel name does not already exist, the router creates a new channel.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</td>
</tr>
<tr>
<td><strong>Step 4</strong> bind-to-interface async0/2/0</td>
<td>Defines the router async interface on which the system sends its DNP3 protocol traffic.</td>
</tr>
<tr>
<td><strong>Step 5</strong> link-addr source source_address</td>
<td>Refers to the link address of the master.</td>
</tr>
<tr>
<td></td>
<td>source_address –Range of values from 1 to 65535.</td>
</tr>
<tr>
<td><strong>Step 6</strong> unsolicited-response enable</td>
<td>(Optional) Allows unsolicited responses.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command disables unsolicited responses.</td>
</tr>
<tr>
<td></td>
<td>The default is disabled.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Ends configuration of the channel and exits channel configuration mode. Saves all settings.</td>
</tr>
<tr>
<td><strong>Step 8</strong> session session_name</td>
<td>Enters session configuration mode and assigns a name to the session.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered session name does not already exist, the router creates a new session.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command deletes an existing session.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td><em>attach-to-channel channel_name</em></td>
</tr>
<tr>
<td></td>
<td>Attaches the session to the channel.</td>
</tr>
<tr>
<td></td>
<td>Note: Enter the same channel name that you entered in Step 3 above</td>
</tr>
<tr>
<td></td>
<td><em>channel_name</em> – Identifies the channel.</td>
</tr>
<tr>
<td>Step 10</td>
<td><em>link-addr dest destination_address</em></td>
</tr>
<tr>
<td></td>
<td>Refers to the link address of the slave.</td>
</tr>
<tr>
<td></td>
<td><em>destination_address</em> – Range of values from 1 to 65535.</td>
</tr>
<tr>
<td>Step 11</td>
<td><em>exit</em></td>
</tr>
<tr>
<td></td>
<td>Exits session configuration mode.</td>
</tr>
<tr>
<td>Step 12</td>
<td><em>exit</em></td>
</tr>
<tr>
<td></td>
<td>Exits protocol configuration mode.</td>
</tr>
</tbody>
</table>

### EXAMPLE

This example shows how to configure the parameters for the DPN3-serial protocol stack:

```
router# configure terminal
router(config)# scada-gw protocol dnp3-serial
router(config-dnp3s)# channel rtu_channel
router(config-dnp3s-channel)# bind-to-interface async 0/2/0
router(config-dnp3s-channel)# link-addr source 3
router(config-dnp3s-channel)# unsolicited-response enable
router(config-dnp3s-channel)# exit
router(config-dnp3s)# session rtu_session
router(config-dnp3s-session)# attach-to-channel rtu_channel
router(config-dnp3s-session)# link-addr dest 3
router(config-dnp3s-session)# exit
router(config-dnp3s)# exit
```

### Configuring DNP3 IP

Follow the steps below for the Control Center that you want to connect to over DNP3 IP. For redundancy, you can create multiple connections that share the same session configuration under the same session.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><em>configure terminal</em></td>
</tr>
<tr>
<td></td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><em>scada-gw protocol dnp3-ip</em></td>
</tr>
<tr>
<td></td>
<td>Enters configuration mode for the DNP-IP protocol.</td>
</tr>
<tr>
<td>Step 3</td>
<td><em>channel channel_name</em></td>
</tr>
<tr>
<td></td>
<td>Enters channel configuration mode for the DNP-IP protocol.</td>
</tr>
<tr>
<td></td>
<td><em>channel_name</em> – Identifies the channel on which the router communicates with the Control Center.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered channel name does not already exist, the router creates a new channel.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>link-addr dest destination_address</td>
</tr>
<tr>
<td></td>
<td>Refers to the link address of the master.</td>
</tr>
<tr>
<td></td>
<td><em>destination_address</em> – Range of values from 1 to 65535.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>send-unsolicited-msg enable</td>
</tr>
<tr>
<td></td>
<td>(Optional) Allow unsolicited messages.</td>
</tr>
<tr>
<td></td>
<td>The default is enabled.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>tcp-connection local-port [default</td>
</tr>
<tr>
<td></td>
<td>remote-ip [any</td>
</tr>
<tr>
<td></td>
<td>Configures the local port number and remote IP address for the TCP connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>default</strong> – 20000.</td>
</tr>
<tr>
<td></td>
<td>• <strong>local_port</strong> – Range of values from 2000 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• <strong>any</strong> – Any remote hosts 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>remote_ip</strong> – Single host: A.B.C.D</td>
</tr>
<tr>
<td></td>
<td>• <strong>remote_subnet</strong> – Subnet: A.B.C.D/LEN</td>
</tr>
<tr>
<td></td>
<td>If remote_subnet is specified, when two channels have the same local ports, the remote subnets cannot overlap each other.</td>
</tr>
<tr>
<td></td>
<td>Note: Every &lt;local-port, remote-ip&gt; must be unique per channel. If remote_subnet is specified, when two channels have the same local ports, the remote subnets cannot overlap each other.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Exits channel configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>session session_name</td>
</tr>
<tr>
<td></td>
<td>Enters session configuration mode and assigns a name to the session.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered session name does not already exist, the router creates a new session.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command deletes an existing session.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>attach-to-channel channel_name</td>
</tr>
<tr>
<td></td>
<td>Attaches the session to the channel.</td>
</tr>
<tr>
<td></td>
<td>Enter the same channel name that you entered in <strong>Step 3</strong>.</td>
</tr>
<tr>
<td></td>
<td><em>channel_name</em> – Identifies the channel.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>link-addr source source_address</td>
</tr>
<tr>
<td></td>
<td>Refers to the link address of the slave.</td>
</tr>
<tr>
<td></td>
<td><em>source_address</em> – Value of 1-65535.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>map-to-session session_name</td>
</tr>
<tr>
<td></td>
<td>Maps the dnp3-ip session to an existing dnp3-serial session.</td>
</tr>
<tr>
<td></td>
<td>Note: One dnp3-ip session can be mapped to only one dnp3-serial session.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Exits session configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 13</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Exits protocol configuration mode.</td>
</tr>
</tbody>
</table>

### EXAMPLE

This example shows how to configure the DNP3 IP parameters:

```
router# configure terminal
router(config)# scada-gw protocol dnp3-ip
router(config-dnp3n)# channel cc_channel
router(config-dnp3n-channel)# link-addr dest 3
router(config-dnp3n-channel)# tcp-connection local-port default remote-ip any
router(config-dnp3n-channel)# exit
router(config-dnp3n)# session cc_session
router(config-dnp3n-session)# attach-to-channel cc_channel
router(config-dnp3n-session)# link-addr source 4
router(config-dnp3n-session)# map-to-session rtu_session
router(config-dnp3n)# exit
router(config)# exit
```

### Starting and Stopping the Protocol Translation Engine

You must start the Protocol Translation Engine to use Protocol Translation on the IR1101.

**Starting**—After enabling SCADA encapsulation on the IR1101 serial port and configuring the T101 and T104 protocols on the IR1101, you can start the Protocol Translation Engine.

**Stopping**—Before you can make any configuration changes to Protocol Translation on the IR1101 with an active Protocol Translation Engine, you must stop the engine.

**Before you begin**

Before starting the Protocol Translation Engine on the router for the first time, make sure you complete the following items:

- Enabling the IR1101 Serial Port and SCADA Encapsulation, on page 280
- Configuring T101 and T104 Protocol Stacks, on page 281

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 [no] scada-gw enable</td>
<td>Starts (scada-gw enable) or stops (no scada-gw enable) the Protocol Translation Engine on the IR1101.</td>
</tr>
</tbody>
</table>

### EXAMPLE

To start the protocol translation engine on the router, enter the following commands:
To stop the protocol translation engine on the router, enter the following commands:

```
routerr# configure terminal
router(config)# no scada-gw enable
```

### Verifying Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the configuration of the router including active features and their settings.</td>
</tr>
<tr>
<td>show scada database</td>
<td>Displays details on the SCADA database.</td>
</tr>
<tr>
<td>show scada statistics</td>
<td>Shows statistics for the SCADA gateway, including the number of messages sent and received, timeouts, and errors.</td>
</tr>
<tr>
<td>show scada tcp</td>
<td>Displays TCP connections associated with the SCADA gateway.</td>
</tr>
</tbody>
</table>

This example shows the output from the `show scada tcp` and `show scada statistics` commands:

```
routerr# show scada tcp
DNP3 network channel [test]: 4 max simultaneous connections
conn: local-ip: 3.3.3.21 local-port 20000 remote-ip 3.3.3.15 data-socket 1
Total:
  1 current client connections
  0 total closed connections
routerr# show scada statistics
DNP3 network Channel [test]:
  5 messages sent, 2 messages received
  0 timeouts, 0 aborts, 0 rejections
  2 protocol errors, 2 link errors, 0 address errors
DNP3 serial Channel [test]:
  152 messages sent, 152 messages received
  1 timeouts, 0 aborts, 0 rejections
  0 protocol errors, 0 link errors, 0 address errors
```

### Debug Commands

This section lists some debug commands that are helpful when troubleshooting.

**Table 12: SCADA Function Level Debug Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada function config</td>
<td>Configuration trace</td>
</tr>
<tr>
<td>debug scada function control</td>
<td>Control trace</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>debug scada function file</td>
<td>File trace</td>
</tr>
<tr>
<td>debug scada function freeze</td>
<td>Freeze trace</td>
</tr>
<tr>
<td>debug scada function physical</td>
<td>Physical trace</td>
</tr>
<tr>
<td>debug scada function poll</td>
<td>Poll trace</td>
</tr>
<tr>
<td>debug scada function stack</td>
<td>Stack trace</td>
</tr>
<tr>
<td>debug scada function umode</td>
<td>Umode trace</td>
</tr>
</tbody>
</table>
This chapter contains the following sections:

- Raw Socket Transport, on page 297
- Information About Raw Socket Transport, on page 297
- Prerequisites, on page 299
- Guidelines and Limitations, on page 300
- Default Settings, on page 300
- Configuring Raw Socket Transport, on page 300
- Verifying Configuration, on page 306
- Configuration Example, on page 306

Raw Socket Transport

Raw Socket Transport transports streams of characters from one serial interface to another over an IP network for utility applications.

This document describes Raw Socket Transport for the IR1101 and provides a reference section describing the Raw Socket Transport commands.

This document includes the following sections:

Information About Raw Socket Transport

Raw Socket is a method for transporting serial data through an IP network. The feature can be used to transport Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). This method is an alternative to the Block Serial Tunnel (BSTUN) protocol.

Raw Socket Transport supports TCP or UDP as the transport protocol. An interface can be configured to use either protocol but not both at the same time. TCP transport is suitable for applications such as control applications that require acknowledged and sequenced delivery of data. For latency-sensitive applications such as line SEL relays, UDP transport provides faster transport of serial data than TCP.

Raw Socket Transport supports the following for the asynchronous serial interface:

- TCP as the transport protocol, with built-in auto TCP connection retry mechanism.
- Up to 32 TCP sessions.
- Interface configuration as a server, client, or a combination of both.
TCP Transport

TCP Raw Socket transport uses a client-server model. At most one server and multiple clients can be configured on a single asynchronous serial line. In client mode, the IR1101 can initiate up to 32 TCP sessions to Raw Socket servers, which can be other IR1101 routers or third-party devices.

Figure 1 shows a sample Raw Socket TCP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes several IR1101 routers. One IR1101 router (Router 1) acts as a Raw Socket server, listening for TCP connection requests from the other IR1101 routers (Router 2 and Router 3), which are configured as Raw Socket clients.

A Raw Socket client receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket client initiates a TCP connection with the Raw Socket server and sends the packetized data across the IP network to the Raw Socket server, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

Note

When you configure the serial link interface on the router as a server, the interface’s peer is the serial link interface on the client router and vice versa.

UDP Transport

UDP transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line.
Figure 2 shows a sample Raw Socket UDP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes two routers (Router 1 which is an IR1101 and Router 2 which is an IR807) that are configured as Raw Socket UDP peers.

In this example, the Raw Socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket UDP peer sends the packetized data across the IP network to the Raw Socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

Serial Data Processing

When the default serial protocol, Asynchronous Communication Protocol, is used, the streams of serial data received by a Raw Socket peer can be packetized based on the following criteria:

- **Packet length**—You can specify a packet length that triggers the IR1101 to transmit the serial data to the peer. Once the IR1101 collects this much data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.
- **Packet-timer value**—The packet timer specifies the amount of time the IR1101 waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the IR1101 has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.
- **Special character**—You can specify a character that will trigger the IR1101 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR1101 packetizes the accumulated data and sends it to the Raw Socket peer.

See the “Configuring Common Raw Socket Line Options” procedure on page 6 for information about configuring the processing options.

VRF-Aware Raw Socket

The VRF-aware Raw Socket Transport feature enables you to isolate Raw Socket traffic using a VRF for efficient management and control of serial data. After configuring a VRF, you can associate the serial interface configured for Raw Socket Transport with the VRF. See the Raw Socket VRF, on page 308 for a configuration example.

Prerequisites

Determine how you want Raw Socket traffic transported in your network, including the network devices and interfaces to use, how the router packetizes the serial data, and whether to use VRF.
Guidelines and Limitations

Typically, UDP traffic is blocked by firewalls in the network. If the network has such firewalls, make sure to configure pinholes to allow the raw socket UDP traffic.

Default Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Socket Transport</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Packet length</td>
<td>No packet length is configured.</td>
</tr>
<tr>
<td>Serial Protocol</td>
<td>Asynchronous Communication Protocol</td>
</tr>
<tr>
<td>Packet timeout</td>
<td>15 ms.</td>
</tr>
<tr>
<td>Special character</td>
<td>No special character is configured.</td>
</tr>
<tr>
<td>Raw Socket mode</td>
<td>Best-effort mode is off, not supported on the IR1101.</td>
</tr>
<tr>
<td>TCP idle timeout</td>
<td>5 minutes.</td>
</tr>
</tbody>
</table>

Configuring Raw Socket Transport

This section includes the following topics:

Enabling Raw Socket Transport on the Serial Interface

To enable Raw Socket Transport on the IR1101 router, you must first enable an asynchronous serial port and enable Raw Socket TCP or UDP encapsulation for that port.

**Before you begin**

Determine availability of the serial port on the IR1101.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface async0/slot/port</td>
<td>Enters the interface command mode for the async slot/port.</td>
</tr>
<tr>
<td>Step 3 no ip address</td>
<td>Disables IP processing on the interface.</td>
</tr>
<tr>
<td>Step 4 Do one of the following:</td>
<td>Enables Raw Socket TCP encapsulation or UDP encapsulation for the serial port.</td>
</tr>
<tr>
<td>• encapsulation raw-tcp</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td></td>
</tr>
<tr>
<td>• encapsulation raw-udp</td>
<td></td>
</tr>
</tbody>
</table>

### EXAMPLE

This example shows how to enable serial port 0/2/0 and how to enable Raw Socket TCP encapsulation on that port.

```
router# configure terminal
router(config)# interface async0/2/0
router(config-if)# no ip address
router(config-if)# encapsulation raw-tcp
router(config-if)# exit
```

### Configuring Common Raw Socket Line Options

You can configure options common to all connections on a line. The common options apply to both TCP and UDP.

#### Before you begin

Enable Raw Socket Transport as described in Enabling Raw Socket Transport on the Serial Interface, on page 300.

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

| Step 2   | line 0[slot /]port         | Enters line command mode for the serial slot/port. |

| Step 3   | raw-socket packet-length length | Specifies the packet size that triggers the IR1101 to transmit the data to the peer. When the IR1101 accumulates this much data in its buffer, it packetizes the data and forwards it to the Raw Socket peer. |

- length—2 to 1400 bytes.
  - By default, the packet-length trigger is disabled.

| Step 4   | raw-socket packet-timer timeout | Specifies the maximum time in milliseconds the IR1101 waits to receive the next character in a stream. If a character is not received by the time the packet-timer expires, the accumulated data is packetized and forwarded to the Raw Socket peer. |

- timeout—3 to 1000 ms.
  - The default is 15 ms.
### Purpose

Command or Action | Purpose
--- | ---
**Step 5** | raw-socket spec-char *ascii_char*

Specifies a character that will trigger the IR1101 to packetize the data accumulated in its buffer and send it to the Raw Socket peer.

*ascii_char*— 0 to 255.

By default, the special character trigger is disabled.

### What to do next

Use the **no** form of these commands to return to the default values.

### EXAMPLE

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket packet-length 32
router(config-line)# raw-socket packet-timer 500
router(config-line)# raw-socket special-char 3
```

### Configuring Raw Socket TCP

After enabling Raw Socket TCP encapsulation, you configure the TCP server and/or clients.

### Configuring the Raw Socket TCP Server

**Before you begin**

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 300.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>line 0/1/slot/port</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>raw-socket tcp server <em>port</em> [ <em>ip_address</em> ]</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>raw-socket tcp idle-timeout <em>session_timeout</em></td>
</tr>
</tbody>
</table>

Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session
## Purpose

Command or Action | Purpose
--- | ---
 | closes. The client then automatically attempts to reestablish the TCP session with the server. This timeout setting applies to all Raw Socket Transport TCP sessions under this particular line.

### session_timeout

#### Currently configured session idle timeout in minutes. The default is 5 minutes.

## What to do next

To remove a Raw Socket TCP server, use the **no raw-socket tcp server** command.

### EXAMPLE

This example shows how to configure a Raw Socket TCP server for an asynchronous serial line. The TCP server listens for TCP client connection requests on local port 4000 and local IP address 10.0.0.1. If no data is exchanged between the Raw Socket TCP server and one of the TCP clients for 10 minutes, then the TCP session closes, and the Raw Socket client attempts to reestablish the session with the Raw Socket server.

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket tcp server 4000 10.0.0.1
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
router(config)#
```

## Configuring the Raw Socket TCP Client

### Before you begin

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 300.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>line 0/slot/port</td>
<td>Enters line command mode for the serial slot/port.</td>
</tr>
</tbody>
</table>
| 3 | raw-socket tcp client dest_ip_address dest_port [local_ip_address ] [local_port ] | Specifies settings for Raw Socket Transport TCP client sessions. 

*dest_ip_address* –Destination IP address of the remote Raw Socket server.

*dest_port* –Destination port number to use for the TCP connection to the remote server.

*local_ip_address* –(Optional) Local IP address that the client can also bind to.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>local_port</em> — (Optional) Local port number that the client can also bind to.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session is closed. The client then automatically attempts to reestablish the TCP session with the server.</td>
</tr>
<tr>
<td><strong>raw-socket tcp idle-timeout</strong></td>
<td>This timeout setting applies to all Raw Socket Transport TCP sessions under this particular line.</td>
</tr>
<tr>
<td><strong>session_timeout</strong></td>
<td><em>session_timeout</em> — Currently configured session idle timeout in minutes. The default is 5 minutes.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Sets the Raw Socket Transport TCP session keepalive interval for the asynchronous line interface. The router sends keepalive messages based on the configured interval. You may need to configure this interval, for example, when sending raw TCP traffic over a cellular interface.</td>
</tr>
<tr>
<td><strong>raw-socket tcp keepalive</strong></td>
<td><em>interval</em> — Currently configured keepalive interval in seconds. Range is 1-864000 seconds. The default is 1 second.</td>
</tr>
</tbody>
</table>

### What to do next

To remove a Raw Socket TCP client, use the `no raw-socket tcp client` command.

### EXAMPLE

This example shows how to configure a Raw Socket TCP client for an asynchronous serial line. The IR1101 (router), serving as a Raw Socket client, initiates TCP sessions with a Raw Socket server and forwards packetized serial data to it. The router collects streams of serial data in its buffer; when it accumulates 827 bytes in its buffer, the router packetizes the data and forwards it to the Raw Socket server. If the router and the Raw Socket server do not exchange any data for 10 minutes, then the TCP session with the Raw Socket server closes, and the router attempts to reestablish the session with the Raw Socket server.

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket tcp client 10.0.0.1 4000
router(config-line)# raw-socket packet-length 827
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
```

### Configuring a Raw Socket UDP Peer-to-Peer Connection

After enabling Raw Socket UDP encapsulation and the common line options, you configure the Raw Socket UDP peer-to-peer connection. The local port on one end of the connection should be the destination port on the other end.
Before you begin
Enable a serial port and Raw Socket UDP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 300.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> line 0/slot/port</td>
<td>Enters line command mode for the serial slot/port.</td>
</tr>
<tr>
<td><strong>Step 3</strong> raw-socket udp connection</td>
<td>Specifies settings for Raw Socket Transport UDP connections.</td>
</tr>
<tr>
<td>dest_ip_address dest_port local_port</td>
<td>- Destination IP address to use for the UDP connection.</td>
</tr>
<tr>
<td>local_ip_address</td>
<td>- Destination port number to use for the UDP connection.</td>
</tr>
<tr>
<td></td>
<td>- Local port number for the UDP connection.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Local IP address for the UDP connection.</td>
</tr>
</tbody>
</table>

**What to do next**
To remove a Raw Socket UDP connection, use the `no raw-socket udp connection` command.

**EXAMPLE**

This example shows how to configure a Raw Socket UDP connection between router A (local IP address 192.168.0.8) and router B (local IP address 192.168.0.2).

**Router A**

```
routing# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.2 5000 7000
router(config-line)# exit
router(config)#
```

**Router B**

```
routing# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.8 7000 5000
router(config-line)# exit
router(config)#
```
### Verifying Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show running-config</strong></td>
<td>Shows the configuration of the IR1101, including those features that are active and their settings.</td>
</tr>
<tr>
<td><strong>show raw-socket tcp detail</strong></td>
<td>Displays information about Raw Socket Transport TCP activity.</td>
</tr>
<tr>
<td><strong>show raw-socket tcp sessions</strong></td>
<td>Displays information about Raw Socket Transport TCP sessions.</td>
</tr>
<tr>
<td><strong>show raw-socket tcp statistics</strong></td>
<td>Displays Raw Socket Transport TCP statistics for each asynchronous serial line.</td>
</tr>
<tr>
<td><strong>show raw-socket udp detail</strong></td>
<td>Displays information about Raw Socket Transport UDP activity.</td>
</tr>
<tr>
<td><strong>show raw-socket udp sessions</strong></td>
<td>Displays information about Raw Socket Transport UDP sessions.</td>
</tr>
<tr>
<td><strong>show raw-socket udp statistics</strong></td>
<td>Displays Raw Socket Transport UDP statistics for each asynchronous serial line.</td>
</tr>
<tr>
<td><strong>clear raw-socket statistics</strong></td>
<td>Clears Raw Socket Transport statistics for a specific TTY interface or for all asynchronous serial lines.</td>
</tr>
</tbody>
</table>

### Configuration Example

The following sections include Raw Socket Transport configuration examples:

#### Raw Socket TCP

The following example shows a Raw Socket Transport configuration in which an IR1101 router (Router 1) acts as the server, and another IR809 (Router 2) acts as the client.

The following table displays the configuration of the server and client IR1101s highlighted in Figure 3:
IR1101 Server Configuration | IR807 Client Configuration
---|---
... interface async0/2/0 no ip address encapsulation raw-tcp ! ... line 0/2/0 raw-socket tcp server 5000 10.0.0.1 raw-socket packet-timer 3 raw-socket tcp idle-timeout 5 ... | ... interface async0 no ip address encapsulation raw-tcp ! interface async1 no ip address encapsulation raw-tcp ! ... line 0 raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9000 raw-socket packet-length 32 raw-socket tcp idle-timeout 5 line 2 raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9001 raw-socket packet-length 32 raw-socket tcp idle-timeout 5

**Raw Socket UDP**

This example shows the configuration for a Raw Socket UDP connection between two IR1101 routers:

**From Router1**

interface GigabitEthernet0/1
ip address 192.168.0.8 255.255.255.0
duplex auto
speed auto
interface async0/2/0
no ip address
encapsulation raw-udp
line 0/2/0
raw-socket udp connection 192.168.0.2 2 2

**From Router2**

interface GigabitEthernet0/1
ip address 192.168.0.2 255.255.255.0
load-interval 60
duplex auto
speed auto
no keepalive
interface async0/2/0
no ip address
encapsulation raw-udp
line 0/2/0
raw-socket udp connection 192.168.0.8 2 2
The following example shows a Raw Socket VRF configuration in which two routers, configured for Raw Socket Transport, connect through a VRF. Router1 is an IR1101, serves as the Raw Socket TCP server, and Router2 is an IR807 serves as the Raw Socket TCP client.

Following are the configurations of Router1 and Router2 as shown in Figure 4:

**Router1 Configuration**

Defining VRF on the router:

```
vrf definition router1
  rd 100:1
  route-target export 100:3
  route-target import 100:3
!
address-family ipv4
exit-address-family
```

Applying VRF configuration on the interface:

```
interface GigabitEthernet0/0
  vrf forwarding router1
  ip address 100.100.100.2 255.255.255.0
  duplex auto
  speed auto
```

Applying raw-tcp on the serial interface:

```
interface async0/2/0
  vrf forwarding router1
  no ip address
  encapsulation raw-tcp
```

Applying raw-tcp on the line:

```
line 0/2/0
  raw-socket tcp server 5000 4.4.4.4
```
Router2 Configuration

Defining VRF on the router:

definition router1
 rd 100:1
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family

Applying VRF configuration on the interface:

interface GigabitEthernet0/0
 vrf forwarding router1
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto

Applying raw-tcp on the serial interface:

interface async0
 vrf forwarding router1
 no ip address
 encapsulation raw-tcp

Applying raw-tcp on line:

line 1
 raw-socket tcp client 4.4.4.4 5000
Expansion Module Overview

The IR1101 Router has an Expansion Module that adds key capabilities such as dual LTE Pluggables, mSATA SSD FRU, SFP, and Digital GPIO connections.

The Expansion Module comes in two types:

• IRM-1100-SPMI
• IRM-1100-SP

Warning

It is important to note that just like the Base IR1101, Online Insertion and Removal (OIR) is not supported on The Expansion Module. If the 4G module (or mSATA) is inserted or pulled out while the device is powered up, it may damage the module.

The following figure shows the front panel of the IRM-1100-SPMI and highlights some of its capabilities:
**mSATA Overview**

IOx/Guest-OS legacy systems on which end users can host applications, typically came with a disk storage of 4GB to store user data. Functionality has been added allowing for a Cisco supported Pluggable mSATA SSD PID to add 50 GB of available storage. Support for a 100 GB mSATA SSD has the following limitations:

- There is no support for the `show inventory` command.

- Supports 55GB (IOx allocation for applications and packages alike), 32B (IOS allocation for storage can be viewed in ‘dir msata’ on IOS).

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4 GPIO + 1 Return (Digital I/O)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Functionality is available on Cisco IOS-XE release 16.12.1 and above.</td>
</tr>
<tr>
<td>2</td>
<td>SFP Connector</td>
</tr>
<tr>
<td>3</td>
<td>Pluggable Module</td>
</tr>
<tr>
<td>4</td>
<td>mSATA SSD Slot</td>
</tr>
<tr>
<td>5</td>
<td>Digital I/O LEDs</td>
</tr>
</tbody>
</table>

---

*Figure 92: IR-1100-SPMI Expansion Module Details*
It is important to note that Online Insertion and Removal (OIR) is not supported. If the mSATA SSD is inserted or pulled out while the device is powered up, it may damage the module.

Warning

As with any IoT platform, for IOx, use the Fog Director, Local Manager, or app-hosting CLI's to install applications and access the new mSATA disk storage provided.

Note

50 GB mSATA Partitioning

IOS-XE divides the mSATA SSD into 2 partitions. One for IOS-XE and the other for IOx. The percentage of usage is:

- IOS: 33.33 %
- IOx: 66.66 %

Using these percentages, the space allocation breaks down as follows:

50GB mSATA:

- IOS: 16.51 GB
- IOx: 31.43 GB

Using the mSATA SSD

Functionality-wise, there are no configuration and troubleshooting differences to the end-user in IOS or IOx, with or without mSATA. The system simply recognizes the additional storage. There are some CLI commands that will show information that pertains to the mSATA storage. Examples are show inventory, and show platform msata.

Router# show inventory

+++
INFO: Please use "show license UDI" to get serial number for licensing.
+++

Router# show platform hardware msata lifetime

SSD Lifetime Remaining: 99% -> 99% of the net disk read/write lifetime is remaining

Router# show platform hardware msata status

SSD is present

Router# show platform hardware msata

SSD Lifetime remaining(%): 99

Display the mSATA Partitioning:

Display mSATA partition 1 in IOS-XE:

Router# dir msata:

Directory of msata:/
11 drwx 16384 Jun 4 2019 17:59:45 +00:00 lost+found
33820622848 bytes total (32052379648 bytes free)
Copy contents to and from mSATA partition:

Router#copy bootflash: msata:
Source filename [?] ir1101-uefi-rommon.SSA
Destination filename [ir1101-uefi-rommon.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
2097152 bytes copied in 0.164 secs (12787512 bytes/sec)

Display disk space allocated by mSATA to IOx:

Router#show app-hosting resource
CPU:
Quota: 1000(Units)
Available: 1000(Units)
Memory:
Quota: 862(MB)
Available: 862(MB)
Storage space:
Total: 58313(MB)
Available: 58313(MB)

Displaying the Wear Leveling Data for the mSATA SSD

IOx Local Manager/ Fog Director can now display the wear leveling data for the mSATA SSD on the IR1101. In the IOx Local Manager, it is observed by selecting System > Storage.

From the IOS command line, you can monitor the lifetime using the show platform hardware msata command.

Router#show platform hardware msata lifetime
SSD Lifetime remaining(%) : 98

After a router reload, it will take a few minutes (approximately 5) before this data will be populated again. When the SSD lifetime reduces to 15% and 5% of the lifetime limit, errors start getting reported in syslog. For example:

*Jan 30 19:03:00.257: %IOX-4-IOX_SSD_LIFETIME_WARN: SSD Lifetime remaining in module:15

MIB support for mSATA Wear Ratio and Usage

mSATA functionality was added to the router to add extra storage for IOx apps. The following table shows the router with the OID:

<table>
<thead>
<tr>
<th>SKU</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1100-SSD-100G</td>
<td>1.3.6.1.4.1.9.12.3.1.9.96.176</td>
</tr>
</tbody>
</table>

As part of this enhancement, SNMP support has been added for the following mSATA parameters on the router:

- lifetime remaining (wear leveling)
- memory usage for the mSATA SSD
The `show platform hardware msata` command gives information about this MIB.

Related documentation:
https://developer.cisco.com/docs/iox/

**Example: Actual OID and output of SNMP get/walk on OID**

```bash
_OID> = STRING: "Lifetime Remaining: 99%, Usage: 30%"
```

### Feature Details

The following conditions must be met before performing SNMP requests on the Router:

- An active mSATA module must be configured in the router.
- The Integrator must have incorporated the supported pluggable mSATA into their design.
- Verify this using the `show platform hardware msata` CLI.

### Feature Assumptions

- After a router reload it will take approximately 5 minutes before mSATA data will be populated again. Only SNMP get is allowed on the OID and is marked as read-only. Setting its value will not be allowed.
- Configurations to enable SNMP on the router are necessary for fetching MIB value.

### Digital IO

The IR1101 has two different Expansion Modules, the IRM-1100-SP and IRM-1100-SPMI. The IRM-1100-SPMI comes with a Digital I/O connector which has 4 GPIO connections plus 1 Return connection. Both Dry and Wet contacts up to 60Volts.

- Dry contact is isolated from a voltage source (or “No Volt”), with an embedded relay function (NPN transistor), usually used to indicate an event. For example: open/close, alarm.
- Wet contact is a contact with external power (+3.3V to +60V, max 150mA of current allowed at high voltage) applied, usually used to energize something. For example: solenoid, light.

Digital IO is similar to the ALARM IN and ALARM OUT supported on the IR800 series routers. The differences are that on the IR800 series, ALARM IN is a dedicated input, the ALARM OUT is a dedicated output. With Digital IO, it can be input or output. ALARM OUT includes a relay to provide the Normally Open (NO) or Normally Close (NC) terminals. Digital IO does not include a relay.

There are no traps for alarms on the GPIO.

More information on the Digital IO hardware capabilities can be found in the Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide.

### Configuration Commands

You can set the alarm severity to critical, major, minor, or none. The severity is included in the alarm message when the alarm is triggered.
To configure and show alarms on the IR1101, use the Command Line Interface (CLI).

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>alarm contact</td>
<td>Enables the alarm contact number. The contact-number value is from</td>
</tr>
<tr>
<td>contact-number</td>
<td>0 to 4. &lt;0-4&gt; Alarm contact number (0: Alarm port, 1-4: Digital I/O).</td>
</tr>
<tr>
<td>enable</td>
<td>Alarm contact 0 is located in the base unit (pins 3 and 4) and always in</td>
</tr>
<tr>
<td></td>
<td>Output Mode. Additional configurations for Alarm 0 include severity,</td>
</tr>
<tr>
<td></td>
<td>threshold and trigger.</td>
</tr>
<tr>
<td>alarm contact</td>
<td>Alarm contact 1-4 (pins 1-4) are located in the IRM-1100 Expansion</td>
</tr>
<tr>
<td>contact-number</td>
<td>Module and can be in Input or Output Mode. Pin 5 is for ground.</td>
</tr>
<tr>
<td></td>
<td>Additional configurations for Alarms 1-4 include application, output,</td>
</tr>
<tr>
<td></td>
<td>severity, threshold and trigger.</td>
</tr>
<tr>
<td></td>
<td>• Enter a contact number (0-4) that you are configuring.</td>
</tr>
<tr>
<td></td>
<td>• The description string is up to 80 alphanumeric characters in length</td>
</tr>
<tr>
<td></td>
<td>and is included in any generated system messages.</td>
</tr>
<tr>
<td></td>
<td>• For application, select dry (default) or wet. Only applicable for</td>
</tr>
<tr>
<td></td>
<td>Digital I/O ports 1-4.</td>
</tr>
<tr>
<td></td>
<td>• enable is for enabling the alarm port. A no alarm contact</td>
</tr>
<tr>
<td></td>
<td>contact-number x will disable the alarm port.</td>
</tr>
<tr>
<td></td>
<td>• The output is either 1 for High or 0 for Low. Only application for</td>
</tr>
<tr>
<td></td>
<td>Digital I/O ports 1-4.</td>
</tr>
<tr>
<td></td>
<td>• For severity, enter critical, major, minor or none. If you do not</td>
</tr>
<tr>
<td></td>
<td>configure a severity, the default is minor.</td>
</tr>
<tr>
<td></td>
<td>• For threshold, select a value between 1600-2700. The default value</td>
</tr>
<tr>
<td></td>
<td>is 1600 mv.</td>
</tr>
<tr>
<td></td>
<td>• For trigger, enter open or closed. If you do not configure a trigger,</td>
</tr>
<tr>
<td></td>
<td>the alarm is triggered when the circuit is closed.</td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>show alarm</td>
<td>Shows the configured alarm contacts.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Verify alarm contacts using the CLI:

Router(config)# alarm contact ?
<0-4> Alarm contact number (0: Alarm port, 1-4: Digital I/O)

Configuration Examples

Configure an alarm.

ir1101# conf term
Enter configuration commands, one per line. End with CNTL/Z.
ir1101(config)# alarm contact 1 description
Your Descriptive Text Here
ir1101(config)#alarm contact 1 severity critical

ir1101(config)#alarm contact 1 trigger closed

ir1101#

To show the alarm status:

ir1101#show alarm
Alarm contact 0:
Enabled: Yes
Status: Not Asserted
Application: Dry
Description: test
Severity: Critical
Trigger: Open
Threshold: 2000

Example of an alarm being generated:

ir1101! *
*Nov 27 14:54:52.573: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External alarm asserted, Severity: Critical

To show the alarm status during an event:

ir1101#show alarm
ALARM CONTACT
Enabled: Yes
Status: Asserted
Application: Dry
Description: test
Severity: Critical
Trigger: Open
Threshold: 2000
Digital I/O 1:
Enabled: No
Status: Not Asserted
Application: Dry
Description: External digital I/O port 1
Severity: Minor
Trigger: Closed
Threshold: 1600
Digital I/O 2:
Enabled: No
Status: Not Asserted
Application: Dry
Description: External digital I/O port 2
Severity: Minor
Trigger: Closed
Threshold: 1600
Digital I/O 3:
Enabled: No
Status: Not Asserted
Application: Dry
Description: External digital I/O port 3
Severity: Minor
Trigger: Closed
Threshold: 1600  
Digital I/O 4:  
Enabled: Yes  
Status: Not Asserted  
Description: External digital I/O port 4  
Mode: Output  
Router#

Example of an alarm being cleared:

ir1101# !
*Nov 27 14:55:02.573: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External alarm cleared
ir1101#

New Cellular Pluggable Modules

Release 16.12.1 supports new pluggable modules/modems. The IR1101 with an Expansion Module supports DUAL LTE (Active/Active), DUAL SIM and DUAL Radio.

- Dual LTE (active/active or active/backup) is supported on the IR1101 equipped with an expansion module and two LTE pluggable interfaces. One on the base unit, the other on the expansion module.
- With DUAL SIM, the two SIMs operate in active/backup mode on the single LTE pluggable module. With DUAL Radio the two LTE pluggable modules operate in active/active mode with each of the two SIMs assigned to a specific cellular radio on the DUAL Radio.

See the following table for details on the new SKUs.

<table>
<thead>
<tr>
<th>SKU ID</th>
<th>Modem Used</th>
<th>Description</th>
<th>Technology Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-LTE-GB</td>
<td>WP7607-G</td>
<td>Europe Dual Micro SIM</td>
<td>LTE CAT4: B3, B5, B8, B20, B28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HSPA+: B1, B5, B8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EDGE: 900/1800</td>
</tr>
<tr>
<td>SKU ID</td>
<td>Modem Used</td>
<td>Description</td>
<td>Technology Supported</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>P-LTEA-LA</td>
<td>EM7430</td>
<td>APAC</td>
<td>LTE Bands: B1, B3, B5, B7, B8, B18, B19, B21, B28, B38, B39, B40, B41.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Non-LTE Bands: B87 - WCDMA (Europe, Japan, and China) 2100 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B91 - WCDMA US 850 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B92 - WCDMA Japan 800 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B114 - WCDMA Europe and Japan 900 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B115 - WCDMA Japan 1700 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B125 - WCDMA Japan 850 band</td>
</tr>
<tr>
<td>P-LTEA-EA</td>
<td>EM7455</td>
<td>USA, Canada, Europe, Latin America</td>
<td>LTE bands: Bands B2, B4, B5, B13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Non-LTE bands: B87 - WCDMA (Europe, Japan, and China) 2100 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B88 - WCDMA US PCS 1900 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B89 - WCDMA (Europe and China) DCS 1800 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B90 - WCDMA US 1700 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B91 - WCDMA US 850 band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B114 - WCDMA Europe and Japan 900 band</td>
</tr>
</tbody>
</table>

**SFP Support**

The SFP interface on the Expansion Module operates differently than on the Base unit. The SFP interface on the IR1101 base module is part of the combo port (SFP/RJ45) for GigabitEthernet0/0/0. It may be configured as Layer-3 (default) or Layer-2 interface.

The SFP interface on the Expansion Module is only an SFP interface. It is named GigabitEthernet0/0/5, and is a Layer-2 interface. For Layer-3 feature set, it must be assigned to a VLAN interface.

Details about the SFP Interface can be displayed using the `show interfaces transceiver detail` CLI, for example:

```
Router#show interfaces transceiver detail
IDPROM for transceiver Gigabitethernet0/0/0:
  Description = SFP or SFP+ optics (type 3)
  Transceiver Type: = GE T (26)
  Product Identifier (PID) = ABCU-5710RZ-CS4
  Vendor Revision =
  Serial Number (SN) = AGM151124J4
  Vendor Name = CISCO-AVAGO
  Vendor OUI (IEEE company ID) = 00.17.6A (5994)
  CLEI code =
  Cisco part number =
  Device State = Enabled.
  Date code (yy/mm/dd) = 11/03/21
```
Connector type = Unknown.
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified

Socket Verification

SFP IDPROM Page 0xA0:
000: 03 04 00 08 00 00 00 00 00 00
010: 00 01 0D 00 00 00 00 00 64 00
020: 43 4F 53 4C 4F 2D 4C 4F 62 4C
030: 4C 4F 62 4C 4F 62 4C 4F 62 4C
040: 4C 4F 62 4L 4F 62 4C 4F 62 4C
050: 02 03 04 00 00 00 00 00 00 00
060: 02 03 04 00 00 00 00 00 00 00
070: 03 04 00 00 00 00 00 00 00 00
080: 03 04 00 00 00 00 00 00 00 00
090: 03 04 00 00 00 00 00 00 00 00
0A0: 03 04 00 00 00 00 00 00 00 00
0B0: 03 04 00 00 00 00 00 00 00 00
0C0: 03 04 00 00 00 00 00 00 00 00
0D0: 03 04 00 00 00 00 00 00 00 00
0E0: 03 04 00 00 00 00 00 00 00 00
0F0: 03 04 00 00 00 00 00 00 00 00
100: 03 04 00 00 00 00 00 00 00 00
110: 03 04 00 00 00 00 00 00 00 00
120: 03 04 00 00 00 00 00 00 00 00
130: 03 04 00 00 00 00 00 00 00 00
140: 03 04 00 00 00 00 00 00 00 00
150: 03 04 00 00 00 00 00 00 00 00
160: 03 04 00 00 00 00 00 00 00 00
170: 03 04 00 00 00 00 00 00 00 00
180: 03 04 00 00 00 00 00 00 00 00
190: 03 04 00 00 00 00 00 00 00 00
1A0: 03 04 00 00 00 00 00 00 00 00
1B0: 03 04 00 00 00 00 00 00 00 00
1C0: 03 04 00 00 00 00 00 00 00 00
1D0: 03 04 00 00 00 00 00 00 00 00
1E0: 03 04 00 00 00 00 00 00 00 00
1F0: 03 04 00 00 00 00 00 00 00 00
200: 03 04 00 00 00 00 00 00 00 00
210: 03 04 00 00 00 00 00 00 00 00
220: 03 04 00 00 00 00 00 00 00 00
230: 03 04 00 00 00 00 00 00 00 00
240: 03 04 00 00 00 00 00 00 00 00
250: 03 04 00 00 00 00 00 00 00 00

SFP IDPROM Page 0xA2:
000: 00 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 00 00
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 00 00
070: 00 00 00 00 00 00 00 00 00 00
080: 00 00 00 00 00 00 00 00 00 00
090: 00 00 00 00 00 00 00 00 00 00
0A0: 00 00 00 00 00 00 00 00 00 00
0B0: 00 00 00 00 00 00 00 00 00 00
0C0: 00 00 00 00 00 00 00 00 00 00
0D0: 00 00 00 00 00 00 00 00 00 00
0E0: 00 00 00 00 00 00 00 00 00 00
0F0: 00 00 00 00 00 00 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 00 00 00
130: 00 00 00 00 00 00 00 00 00 00
140: 00 00 00 00 00 00 00 00 00 00
150: 00 00 00 00 00 00 00 00 00 00
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: 00 00 00 00 00 00 00 00 00 00
1A0: 00 00 00 00 00 00 00 00 00 00
1B0: 00 00 00 00 00 00 00 00 00 00
1C0: 00 00 00 00 00 00 00 00 00 00
1D0: 00 00 00 00 00 00 00 00 00 00
1E0: 00 00 00 00 00 00 00 00 00 00
1F0: 00 00 00 00 00 00 00 00 00 00
200: 00 00 00 00 00 00 00 00 00 00
210: 00 00 00 00 00 00 00 00 00 00
220: 00 00 00 00 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 00 00
250: 00 00 00 00 00 00 00 00 00 00

Link reach for 9u fiber (km)
= SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
### Link reach for 9μ fiber (m)
- SX (550/270m) (0)
- 1xFC-MM (500/300m) (0)
- 2xFC-MM (300/150m) (0)
- ESCON-MM (2km) (0)

### Link reach for 50μ fiber (m)
- SR (2km) (0)
- IR-1 (15km) (0)
- IR-2 (40km) (0)
- LR-1 (40km) (0)
- LR-2 (80km) (0)
- LR-3 (80km) (0)
- DX (40km) (0)
- HX (40km) (0)
- ZX (80km) (0)
- VX (100km) (0)
- 1xFC, 2xFC-SM (10km) (0)
- ESCON-SM (20km) (0)

### Link reach for 62.5μ fiber (m)
- SR (2km) (0)
- IR-1 (15km) (0)
- IR-2 (40km) (0)
- LR-1 (40km) (0)
- LR-2 (80km) (0)
- LR-3 (80km) (0)
- DX (40km) (0)
- HX (40km) (0)
- ZX (80km) (0)
- VX (100km) (0)
- 1xFC, 2xFC-SM (10km) (0)
- ESCON-SM (20km) (0)

---

**Nominal laser wavelength**
- 16652 nm.

**DWDM wavelength fraction**
- 16652.193 nm.

**Supported options**
- Tx disable

---

Assigning L3 SVI with IP address to Extended Module GE 0/0/5 SFP interface:

```bash
IR1101#config t
IR1101(config)#interface g0/0/5
IR1101(config-if)#switchport access vlan 2
IR1101(config-if)#no shut
IR1101(config-if)#interface vlan2
IR1101(config-if)#ip address 192.168.1.2 255.255.255.0
IR1101(config-if)#no shut
```

You can find all of the supported SFP Interfaces in the **Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide**
CHAPTER 23

System Messages

This chapter contains the following sections:

- Information About Process Management, on page 323
- How to Find Error Message Details, on page 323

Information About Process Management

You can access system messages by logging in to the console through Telnet protocol and monitoring your system components remotely from any workstation that supports the Telnet protocol.

Starting and monitoring software is referred to as process management. The process management infrastructure for a router is platform independent, and error messages are consistent across platforms running on Cisco IOS XE. You do not have to be directly involved in process management, but we recommend that you read the system messages that refer to process failures and other issues.

How to Find Error Message Details

To show further details about a process management or a syslog error message, enter the error message into the Error Message Decoder tool at: https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi.

For example, enter the message %PMAN-0-PROCESS_NOTIFICATION into the tool to view an explanation of the error message and the recommended action to be taken.

The following are examples of the description and the recommended action displayed by the Error Message Decoder tool for some of the error messages.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The process lifecycle notification component failed, preventing proper detection of a process start and stop. This problem is likely the result of a software defect in the software subpackage.

Note the time of the message and investigate the kernel error message logs to learn more about the problem and see if it is correctable. If the problem cannot be corrected or the logs are not helpful, copy the error message exactly as it appears on the console along with the output of the `show tech-support` command and provide the gathered information to a Cisco technical support representative.

**Error Message:** `%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A process important to the functioning of the router has failed.</td>
<td>Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a>. If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the <code>show logging</code> and <code>show tech-support</code> commands and your pertinent troubleshooting logs.</td>
</tr>
</tbody>
</table>

**Error Message:** `%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A process important to the functioning of the router has failed.</td>
<td>Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a>. If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the <code>show logging</code> and <code>show tech-support</code> commands and your pertinent troubleshooting logs.</td>
</tr>
</tbody>
</table>
A process that does not affect the forwarding of traffic has failed.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])</td>
<td>The process has failed as the result of an error.</td>
<td>This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a>. If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the show logging and show tech-support commands and your pertinent troubleshooting logs.</td>
</tr>
</tbody>
</table>
### Error Message: %PMAN-3-PROCFAIL_IGNORE

**Explanation:** A process failure is being ignored due to the user-configured debug settings.

**Recommended Action:** If this behavior is desired and the debug settings are set according to a user's preference, no action is needed. If the appearance of this message is viewed as a problem, change the debug settings. The router is not expected to behave normally with this debug setting. Functionalities such as SSO switchover, router reloads, FRU resets, and so on will be affected. This setting should only be used in a debug scenario. It is not normal to run the router with this setting.

### Error Message: %PMAN-3-PROCHOLDDOWN

**Explanation:** The process has been heldown (rc)

**Recommended Action:** This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: [http://www.cisco.com/tac](http://www.cisco.com/tac). With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: [http://www.cisco.com/cisco/psn/bssprt/bss](http://www.cisco.com/cisco/psn/bssprt/bss). If you still require assistance, open a case with the Technical Assistance Center at: [http://tools.cisco.com/ServiceRequestTool/create/](http://tools.cisco.com/ServiceRequestTool/create/), or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the `show logging` and `show tech-support` commands and your pertinent troubleshooting logs.

### Error Message: %PMAN-3-RELOAD_RP_SB_NOT_READY

**Explanation:** The route processor is being reloaded because there is no ready standby instance.

**Recommended Action:** Ensure that the reload is not due to an error condition.

### Error Message: %PMAN-3-RELOAD_RP

**Explanation:** Reloading: [chars]
The RP is being reloaded.

**Error Message:** %PMAN-3-RELOAD_SYSTEM : Reloading: [chars]

**Explanation**
The system is being reloaded.

**Recommended Action**
Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

---

**Error Message:** %PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]

**Explanation**
The executable file used for the process is bad or has permission problem.

**Recommended Action**
Ensure that the named executable is replaced with the correct executable.

---

**Error Message:** %PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>

**Explanation**
The executable file used for the process is missing, or a dependent library is bad.

**Recommended Action**
Ensure that the named executable is present and the dependent libraries are good.

---

**Error Message:** %PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]

**Explanation**
The executable file used for the process is empty.

**Recommended Action**
Ensure that the named executable is non-zero in size.

---

**Error Message:** %PMAN-5-EXITACTION : Process manager is exiting: [chars]

**Explanation**
The process manager is exiting.

**Recommended Action**
Ensure that the process manager is not exiting due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

---

**Error Message:** %PMAN-6-PROCSHUT : The process [chars] has shutdown

**Explanation**
The process has gracefully shut down.

**Recommended Action**
No user action is necessary. This message is provided for informational purposes only.

---

**Error Message:** %PMAN-6-PROCSTART : The process [chars] has started
The process has launched and is operating properly. | No user action is necessary. This message is provided for informational purposes only.

**Error Message:** %PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process has requested a stateless restart.</td>
<td>No user action is necessary. This message is provided for informational purposes only.</td>
</tr>
</tbody>
</table>
Environmental Monitoring

The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. The following are some of the key functions of the environmental monitoring system:

- Monitoring temperature of CPUs and Motherboard
- Recording abnormal events and generating notifications
- Monitoring Simple Network Management Protocol (SNMP) traps
- Generating and collecting Onboard Failure Logging (OBFL) data
- Sending call home event notifications
- Logging system error messages
- Displaying present settings and status

Environmental Monitoring and Reporting Functions

Monitoring and reporting functions allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

- Environmental Monitoring Functions, on page 330
- Environmental Reporting Functions, on page 331
Environmental Monitoring Functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

The router is expected to meet the following environmental operating conditions:

- Non-operating Temperature: -40°F to 158°F (-40°C to 70°C)
- Non-operating Humidity: 5 to 95% relative humidity (non-condensing)
- Operating Temperature:
  - -40° to 140°F (-40° to 60°C) in a sealed NEMA cabinet with no airflow
  - -40° to 158°F (-40° to 70°C) in a vented cabinet with 40 lfm of air
  - -40° to 167°F (-40° to 75°C) in a forced air enclosure with 200 lfm of air
- Operating Humidity: 10% to 95% relative humidity (non-condensing)
- Operating Altitude: -500 to 5,000 feet. Derate max operating temperature 1.5°C per 1000 feet.

The following table displays the levels of status conditions used by the environmental monitoring system.

**Table 14: Levels of Status Conditions Used by the Environmental Monitoring System**

<table>
<thead>
<tr>
<th>Status Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>All monitored parameters are within normal tolerance.</td>
</tr>
<tr>
<td>Warning</td>
<td>The system has exceeded a specified threshold. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>Critical</td>
<td>An out-of-tolerance temperature or voltage condition exists. Although the system continues to operate, it is approaching shutdown. Immediate operator action is required.</td>
</tr>
</tbody>
</table>

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

**Temperature and Voltage Exceed Max/Min Thresholds**

The following example shows the warning messages indicating the maximum and minimum thresholds of the temperature or voltage:

**Warnings:**

---

For all the temperature sensors (name starting with "Temp:"), above,
the critical warning threshold is 100°C (100°C and higher)
the warning threshold is 80°C (range from 80°C to 99°C)
the low warning threshold is 1°C (range from -inf to 1°C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
Environmental Reporting Functions

You can retrieve and display environmental status reports using the following commands:

- show diag all eeprom
- show environment
- show environment all
- show inventory
- show platform
- show platform diag
- show platform software status control-processor
- show diag slot R0 eeprom detail
- show version
- show power

These commands show the current values of parameters such as temperature and voltage.

The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are shown below:

**show diag all eeprom: Example**

```
Router# show diag all eeprom
MIDPLANE EEPROM data:
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
Asset ID :
CLEI Code : UNASSIGNED
Power/Fan Module P0 EEPROM data is not initialized

Power/Fan Module P1 EEPROM data is not initialized

Slot R0 EEPROM data:
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
Slot F0 EEPROM data:
```
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED

Slot 0 EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED

SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : IR1101-ES-5
Version Identifier (VID) : V01
Top Assy. Part Number : 68-2236-01
Top Assy. Revision : A0
Hardware Revision : 2.2
CLEI Code : CNUIAHSAAA

SPA EEPROM data for subslot 0/1 is not available
SPA EEPROM data for subslot 0/2 is not available
SPA EEPROM data for subslot 0/3 is not available
SPA EEPROM data for subslot 0/4 is not available
SPA EEPROM data for subslot 0/5 is not available

Router#

**show environment: Example**

Router# show environment
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0

Slot Sensor Current State Reading Threshold(Minor,Major,Critical,Shutdown)

<table>
<thead>
<tr>
<th>Sensor</th>
<th>State</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>R0 Temp</td>
<td>LM75BXXX</td>
<td>Normal 43 Celsius (75,80,90,na) (Celsius)</td>
</tr>
</tbody>
</table>

Router#

**show environment all: Example**

Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: LM75BXXX R0 Normal 48 Celsius

show inventory: Example

Router# show inventory
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V00 , SN: FCW2132TH02

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: , SN:

NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"
PID: IR1101-ES-5 , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 0", DESCR: "GE SX"
PID: GLC-SX-MM-RGD , VID: V01 , SN: FNS16370HL4

NAME: "module subslot 0/1", DESCR: "P-LTE-US Module"
PID: P-LTE-US , VID: V01 , SN: FOC21333R92

NAME: "Modem 0 on Cellular0/1/0", DESCR: "Sierra Wireless WP7603"
PID: WP7603 , VID: 10000, SN: 359528080000794

show platform: Example

Router# show platform
Chassis type: IR1101-K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 IR1101-K9 ok 01:52:41
0/0 IR1101-ES-5 ok 01:51:35
R0 IR1101-K9 ok, active 01:52:41
F0 IR1101-K9 init, active 01:52:41

show platform diag: Example

Router# show platform diag
Chassis type: IR1101-K9

Slot: 0, IR1101-K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:25 (5d02h ago)
Software declared up time : 00:01:07 (5d02h ago)
CPLD version :
Firmware version : 1.3

Sub-slot: 0/0, IR1101-ES-5
Operational status: ok
Internal state: inserted
Physical insert detect time: 00:02:21 (5d02h ago)
Logical insert detect time: 00:02:21 (5d02h ago)

Sub-slot: 0/1, P-LTE-US
Operational status: ok
Internal state: inserted
Physical insert detect time: 00:02:21 (5d02h ago)
Logical insert detect time: 00:02:21 (5d02h ago)

Slot: R0, IR1101-K9
Running state: ok, active
Internal state: online
Internal operational state: ok
Physical insert detect time: 00:00:25 (5d02h ago)
Software declared up time: 00:00:25 (5d02h ago)
CPLD version: 00000000
Firmware version: 1.2

Slot: F0, IR1101-K9
Running state: init, active
Internal state: online
Internal operational state: ok
Physical insert detect time: 00:00:25 (5d02h ago)
Software declared up time: 00:01:10 (5d02h ago)
Hardware ready signal time: 00:00:00 (never ago)
Packet ready signal time: 00:00:00 (never ago)
CPLD version: 00000000
Firmware version: 1.2

Router#

show platform software status control-processor: Example

Router# show platform software status control-processor
RP0: online, statistics updated 9 seconds ago
Load Average: healthy
1-Min: 0.32, status: healthy, under 5.00
5-Min: 0.33, status: healthy, under 5.00
15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
Total: 3959840
Used: 2894588 (73%), status: healthy
Free: 1065252 (27%)
Committed: 2435656 (62%), under 90%

Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 0.50, System: 0.91, Nice: 0.00, Idle: 98.07
IRQ: 0.40, SIRQ: 0.10, IOWait: 0.00

CPU1: CPU Utilization (percentage of time spent)
User: 0.81, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.20, SIRQ: 0.20, IOWait: 0.00

CPU2: CPU Utilization (percentage of time spent)
User: 0.81, System: 2.65, Nice: 0.00, Idle: 95.41
IRQ: 1.12, SIRQ: 0.00, IOWait: 0.00

CPU3: CPU Utilization (percentage of time spent)
User: 7.66, System: 17.05, Nice: 0.00, Idle: 70.58
IRQ: 4.50, SIRQ: 0.10, IOWait: 0.00
show diag slot R0 eeprom detail: Example

Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:

  EEPROM version : 4
  Compatible Type : 0xFF
  Controller Type : 3457
  Hardware Revision : 0.2
  PCB Part Number : 73-18820-03
  Board Revision : 02
  Deviation Number : 0
  Fab Version : 02
  PCB Serial Number : FOC22106KKH
  Top Assy. Part Number : 68-6479-03
  Top Assy. Revision : 04
  Chassis Serial Number : FCW2213TH07
  Deviation Number : 0
  RMA Test History : 00
  RMA Number : 0-0-0-0
  RMA History : 00
  Product Identifier (PID) : IR1101-K9
  Version Identifier (VID) : V00
  CLEI Code : UNASSIGNED
  Manufacturing Test Data : 00 00 00 00 00 00 00 00
  Field Diagnostics Data : 00 00 00 00 00 00 00 00
  Chassis MAC Address : 682c.7b4d.7880
  MAC Address block size : 128
  Asset ID :
  Asset Alias :
  PCB Part Number : 73-18821-03
  Board Revision : 03
  Deviation Number : 0
  Fab Version : 02
  PCB Serial Number : FOC22106KHD
  PCB Part Number : 73-19117-02
  Board Revision : 02
  Deviation Number : 0
  Fab Version : 01
  PCB Serial Number : FOC22106KJ9
  Asset ID :
  Router#

show version: Example

Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1prd7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 31-Oct-18 23:27 by mcpre
Environmental Reporting Functions

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License (“GPL”) Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON

Router uptime is 1 hour, 53 minutes
Uptime for this control processor is 1 hour, 54 minutes
System returned to ROM by reload
System image file is "usb0:ir1101-universalk9.16.10.01prd7.SPA.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

------------------------------------------------------------------------------------------------------------------
Technology-package Technology-package
Current Type Next reboot
------------------------------------------------------------------------------------------------------------------
network-advantage Smart License network-advantage

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711867K/6147K bytes of memory.
Processor board ID FC2150TH0F
1 Virtual Ethernet interface
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.
30670832K bytes of USB Flash at usbflash0:.

Configuration register is 0x0 (will be 0x2102 at next reload)

Router#
**show power: Example**

Router# `show power`
Main PSU :
Total Power Consumed: 8.16 Watts
Router#

---

**Additional References**

The following sections provide references related to the power efficiency management feature.

**MIBs**

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-ENTITY-FRU-CONTROL-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator at: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>.</td>
</tr>
</tbody>
</table>

---

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 25

IOx Application Hosting

This chapter contains the following sections:

- Application Hosting, on page 339
- Information About Application Hosting, on page 339
- Application Hosting on the IR1101 Router, on page 340
- How to Configure Application Hosting, on page 343
- Installing and Uninstalling Apps, on page 347
- Overriding the App Resource Configuration, on page 348
- Verifying the Application Hosting Configuration, on page 349
- Configuration Examples for Application Hosting, on page 350

Application Hosting

A hosted application is a software as a service solution, and it can be run remotely using commands. Application hosting gives administrators a platform for leveraging their own tools and utilities.

This module describes the Application Hosting feature and how to enable it.

Information About Application Hosting

Need for Application Hosting

The move to virtual environments has given rise to the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes. This ranges from automation, configuration management monitoring, and integration with existing tool chains.

Cisco devices support third-party off-the-shelf applications built using Linux tool chains. Users can run custom applications cross-compiled with the software development kit that Cisco provides.

IOx Overview

IOx is a Cisco-developed end-to-end application framework that provides application hosting capabilities for different application types on Cisco network platforms.
IOx architecture for the IR1101 is different compared to other Cisco platforms that use the hypervisor approach. In other platforms, IOx runs as a virtual machine. IOx is running as a process on the IR1101.

Cisco Application Hosting Overview

The IR1101 enables the user to deploy the application using the app-hosting CLIs. These app-hosting CLIs are not available on the other older platforms. There are additional ways to deploy the applications using the Local Manager and Fog Director.

Application hosting provides the following services:

- Launches designated applications in containers.
- Checks available resources (memory, CPU, and storage), and allocates and manages them.
- Provides support for console logging.
- Provides access to services via REST APIs.
- Provides a CLI endpoint.
- Provides an application hosting infrastructure referred to as Cisco Application Framework (CAF).
- Helps in the setup of platform-specific networking (packet-path) via VirtualPortGroup and management interfaces.

The container is referred to as the virtualization environment provided to run the guest application on the host operating system. The Cisco IOS-XE virtualization services provide manageability and networking models for running guest applications. The virtualization infrastructure allows the administrator to define a logical interface that specifies the connectivity between the host and the guest. IOx maps the logical interface into the Virtual Network Interface Card (vNIC) that the guest application uses.

Applications to be deployed in the containers are packaged as TAR files. The configuration that is specific to these applications is also packaged as part of the TAR file.

The management interface on the device connects the application hosting network to the IOS management interface. The Layer 3 interface of the application receives the Layer 2 bridged traffic from the IOS management interface. The management interface connects through the management bridge to the container/application interface. The IP address of the application must be on the same subnet as the management interface IP address.

IOXMAN

IOXMAN is a process that establishes a tracing infrastructure to provide logging or tracing services for guest applications, except Libvirt, that emulates serial devices. IOXMAN is based on the lifecycle of the guest application to enable and disable the tracing service, to send logging data to IOS syslog, to save tracing data to IOx tracelog, and to maintain IOx tracelog for each guest application.

Application Hosting on the IR1101 Router

This section describes the application-hosting characteristics specific to the IR1101 Industrial Router.

Note

The IR1101 CPU is not based on x86 architecture like other Routers. Therefore, this requires the application to comply with the ARM 64-bits architecture.
Application hosting can be achieved using the app-hosting cli's as well using the Local Manager and Fog Director. Application hosting using Local Manager is done through the WebUI. In order to deploy the applications using Local Manager, WebUI should be enabled and then login to the Local Manager.

**Figure 93: Local Manager**

1. From the WebUI, click on **Configuration > Services > IOx**
2. Login using the username and password configured.
3. Follow the steps for the application lifecycle in the **Cisco IOx Local Manager Reference Guide** using this link: [https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-7/b_iox_lm_ref_guide_1_7/b_iox_lm_ref_guide_1_7_chapter_011.html](https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-7/b_iox_lm_ref_guide_1_7/b_iox_lm_ref_guide_1_7_chapter_011.html)

The next section explains the deployment of an application using the app-hosting cli's.

**VirtualPortGroup**

The VirtualPortGroup is a software construct on Cisco IOS that maps to a Linux bridge IP address. As such, the VirtualPortGroup represents the switch virtual interface (SVI) of the Linux container. Each bridge can contain multiple interfaces; each mapping to a different container. Each container can also have multiple interfaces.

VirtualPortGroup interfaces are configured by using the interface virtualportgroup command. Once these interfaces are created, IP address and other resources are allocated.

The VirtualPortGroup interface connects the application hosting network to the IOS routing domain. The Layer 3 interface of the application receives routed traffic from IOS. The VirtualPortGroup interface connects through the SVC Bridge to the container/application interface.

The following graphic helps to understand the relationship between the VirtualPortGroup and other interfaces, as it is different than the IR8x9 routers.
For the container life cycle management, the Layer 3 routing model that supports one container per internal logical interface is used. This means that a virtual Ethernet pair is created for each application; and one interface of this pair, called vNIC is part of the application container. The other interface, called vpgX is part of the host system.

NIC is the standard Ethernet interface inside the container that connects to the platform dataplane for the sending and receiving of packets. IOx is responsible for the gateway (VirtualPortGroup interface), IP address, and unique MAC address assignment for each vNIC in the container.

The vNIC inside the container/application are considered as standard Ethernet interfaces.
How to Configure Application Hosting

Enabling IOx

Perform this task to enable access to the IOx Local Manager. The IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities.

Note

In the steps that follow, IP HTTP commands do not enable IOX, but allow the user to access the WebUI to connect the IOX Local Manager.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Steps</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device&gt;enable</td>
</tr>
<tr>
<td>2.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device#configure terminal</td>
</tr>
<tr>
<td>3.</td>
<td>iox</td>
<td>Enables IOX</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config)#iox</td>
</tr>
<tr>
<td>4.</td>
<td>ip http server</td>
<td>Enables the HTTP server on your IP or IPv6 system.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config)#ip http server</td>
</tr>
<tr>
<td>5.</td>
<td>ip http secure-server</td>
<td>Enables a secure HTTP (HTTPS) server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config)#ip http secure-server</td>
</tr>
</tbody>
</table>
### Purpose

Command

Establishes a username-based authentication system and privilege level for the user.

The username privilege level must be configured as 15.

**username name privilege level password {0 | 7 | user-password | encrypted-password}

Example:

```
Device(config)#username cisco privilege 15 password 0 cisco
```  

### Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>username name privilege level password {0</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#username cisco privilege 15 password 0 cisco</code></td>
</tr>
<tr>
<td>7.</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)#end</code></td>
</tr>
</tbody>
</table>

### Configuring a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. VirtualPortGroups and Layer 3 data ports must be on different subnets.

Enable the `ip routing` command to allow external routing on the Layer 3 data-port.

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device&gt;enable</td>
</tr>
<tr>
<td>2.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device&gt;configure terminal</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 3.   | `ip routing`  
Example: 
Device(config)#ip routing | Enables IP routing.  
The **ip routing** command must be enabled to allow external routing on Layer 3 data ports. |
| 4.   | `interface type number`  
Example: 
Device(config)#interface gigabitethernet 0/0/0 | Configures an interface and enters interface configuration mode |
| 5.   | `no switchport`  
Example: 
Device(config-if)#no switchport | Places the interface in Layer 3 mode, and makes it operate more like a router interface rather than a switch port. |
| 6.   | `ip address ip-address mask`  
Example: 
Device(config-if)#ip address 10.1.1.1 255.255.255.0 | Configures an IP address for the interface. |
| 7.   | `exit`  
Example: 
Device(config-if)#exit | Exits interface configuration mode and returns to global configuration mode. |
| 8.   | `interface type number`  
Example: 
Device(config)#interface virtualportgroup 0 | Configures an interface and enters interface configuration mode. |
| 9.   | `ip address ip-address mask`  
Example: 
Device(config-if)#ip address 192.168.0.1 255.255.255.0 | Configures an IP address for the interface. |
| 10.  | `end`  
Example: 
Device(config-if)#end | Exits interface configuration mode and returns to privileged EXEC mode. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 11.  | `configure terminal`  
Enter configuration commands, one per line. End with CNTL/Z.  
Example:  
Device# configure terminal | Enters global configuration mode. |
| 12.  | `app-hosting appid app1`  
Example:  
Device(config)# app-hosting appid app1 | Configures the application and enters the application configuration mode. |
| 13.  | `app-vnic gateway0 virtualportgroup 0 guest-interface 0`  
Example:  
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0 | Configures the application interface and the gateway of the application. |
| 14.  | `guest-ipaddress 192.168.0.2 netmask 255.255.255.0`  
Example:  
Device(config-app-hosting-gateway0)# guest-ipaddress 192.168.0.2 netmask 255.255.255.0 | Configures the application Ethernet interface ip address. |
| 15.  | `app-default-gateway 192.168.0.1 guest-interface 0`  
Example:  
Device(config-app-hosting-gateway0)# app-default-gateway 192.168.0.1 guest-interface 0 | Configures the default gateway for the application. |
| 16.  | `end`  
Example:  
Device# end | Exits global configuration mode and returns to privileged EXEC configuration mode. |
## Installing and Uninstalling Apps

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enable</code>&lt;br&gt;Example: <code>Device&gt;enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>2.</td>
<td><code>app-hosting install appid application-name package package-path</code>&lt;br&gt;Example: <code>Device#app-hosting install appid lxc_app package flash:my_iox_app.tar</code></td>
<td>Installs an app from the specified location. The app can be installed from any local storage location such as, flash, bootflash, and usbflash0.</td>
</tr>
<tr>
<td>3.</td>
<td><code>app-hosting activate appid application-name</code>&lt;br&gt;Example: <code>Device#app-hosting activate appid app1</code></td>
<td>Activates the application. This command validates all application resource requests, and if all resources are available the application is activated; if not, the activation fails.</td>
</tr>
<tr>
<td>4.</td>
<td><code>app-hosting start appid application-name</code>&lt;br&gt;Example: <code>Device#app-hosting start appid app1</code></td>
<td>Starts the application. Application start-up scripts are activated.</td>
</tr>
<tr>
<td>5.</td>
<td><code>app-hosting stop appid application-name</code>&lt;br&gt;Example: <code>Device#app-hosting stop appid app1</code></td>
<td>Stops the application.</td>
</tr>
<tr>
<td>6.</td>
<td><code>app-hosting deactivate appid application-name</code>&lt;br&gt;Example: <code>Device#app-hosting deactivate appid app1</code></td>
<td>Deactivates all resources allocated for the application.</td>
</tr>
</tbody>
</table>
Overriding the App Resource Configuration

Resource changes will take effect only after the app-hosting activate command is configured.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>app-hosting uninstall appid application-name</td>
<td>Uninstalls the application. Uninstalls all packaging and images stored. All changes and updates to the application are also removed.</td>
</tr>
</tbody>
</table>

Example:

```
Device#app-hosting uninstall appid appl
```
### Verifying the Application Hosting Configuration

#### DETAILED STEPS

1. **enable**

   Enables privileged EXEC mode. Enter your password if prompted.

   **Example:**

   Device> enable

2. **show iox-service**

   Displays the status of all IOx services

   **Example:**

   Device# show iox-service
   IOx Infrastructure Summary:
   ----------------------------
   IOx service (CAF) 1.8.0.2 : Running
   IOx service (HA) : Not Supported
   IOx service (IOxman) : Running
   Libvirtd 1.3.4 : Running
   Device#

3. **show app-hosting detail**

   Displays detailed information about the application.

   **Example:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><code>memory memory</code>&lt;br&gt;Example:&lt;br&gt;Device(config-app-resource-profile-custom)#&lt;br&gt;memory 512</td>
<td>Changes the default memory allocation.</td>
</tr>
<tr>
<td>7.</td>
<td><code>vcpu number</code>&lt;br&gt;Example:&lt;br&gt;Device(config-app-resource-profile-custom)#&lt;br&gt;vcpu 2</td>
<td>Changes the virtual CPU (vCPU) allocation for the application.</td>
</tr>
<tr>
<td>8.</td>
<td><code>end</code>&lt;br&gt;Example:&lt;br&gt;Device(config-app-resource-profile-custom)#&lt;br&gt;end</td>
<td>Exits custom application resource profile configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Device# show app-hosting detail
App id : app1
Owner : iox
State : RUNNING
Application
Type : lxc
Name : nt08-stress
Version : 0.1
Description : Stress Testing Application
Path : usbflash0: my_iox_app.tar
Activated profile name : custom
Resource reservation
Memory : 64 MB
Disk : 2 MB
CPU : 500 units
Attached devices
<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>serial/shell</td>
<td>iox_console_shell</td>
<td>serial0</td>
</tr>
<tr>
<td>serial/aux</td>
<td>iox_console_aux</td>
<td>serial1</td>
</tr>
<tr>
<td>serial/syslog</td>
<td>iox_syslog</td>
<td>serial2</td>
</tr>
<tr>
<td>serial/trace</td>
<td>iox_trace</td>
<td>serial3</td>
</tr>
</tbody>
</table>

Network interfaces
eth0:
MAC address : 52:54:dd:fa:25:ee

4. show app-hosting list
Displays the list of applications and their status.
Example:

Device# show app-hosting list
App id State
----------------------------------------
app1 RUNNING

Configuration Examples for Application Hosting

See the following examples:

Example: Enabling IOx

Device> enable
Device# configure terminal
Device(config)# iox
Device(config)# ip http server
Device(config)# ip http secure-server
Device(config)# username cisco privilege 15 password 0 cisco
Device(config)# end
Example: Configuring a VirtualPortGroup to a Layer 3 Data Port

Device> enable
Device# configure terminal
Device(config)# ip routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface virtualportgroup 0
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# end

Example: Installing and Uninstalling Apps

Device> enable
Device# app-hosting install appid app1 package flash:my_iox_app.tar
Device# app-hosting activate appid app1
Device# app-hosting start appid app1
Device# app-hosting stop appid app1
Device# app-hosting deactivate appid app1
Device# app-hosting uninstall appid app1

Example: Overriding the App Resource Configuration

Device# configure terminal
Device(config)# app-hosting appid app1
Device(config-app-hosting)# app-resource profile custom
Device(config-app-resource-profile-custom)# cpu 800
Device(config-app-resource-profile-custom)# memory 512
Device(config-app-resource-profile-custom)# vcpu 2
Device(config-app-resource-profile-custom)# end
Serial Relay Service

Serial Relay service on the IR1101 enables IOx apps to communicate with the Async Serial port (/dev/ttyS1 under IOS-XE). The configuration of Serial Relay service is similar to that of the IR800.

Data Paths

On the IR1101, IOS-XE has complete control over the data path and control path of the Async Serial port. This aspect is essential to other encapsulations supported on the Aysnc port such as PPP, raw-socket, SCADA, etc. The IOx app is never allowed to exercise full control over the device. All data and configurations are passed through IOS-XE before going to the device. Instead of exposing the actual Serial port to IOx apps, the Serial relay service creates a software emulated serial tty device enumerated as /dev/ttyTun0 (shown below). The pair of devices /dev/ttyTun0 and /dev/ttyTun1 represent a data tunnel whose primary function is to act as a pass-through gateway during any data transfer. /dev/ttyTun1 is open by IOS-XE and all the ingress/egress data from IOS to the app uses this device during data transfer. Line 0/0/0 is used to communicated with /dev/ttyTun1. Serial relay service should be configured beforehand to allow the connection between two lines.
Data Paths:

1. When the IOx app sends a character to /dev/ttyTun0, the tunnel driver automatically pushes the data to /dev/ttyTun1.
2. IOS reads the data which it then passes to the Serial relay service.
3. The Serial relay service retrieves information about the other end of the relay service (Line 0/2/0 in this case) and forwards the data to the Line's buffer.
4. The line driver actively pushes the data into the actual serial device (/dev/ttyS1) based on buffer availability.
5. The reverse path functions the same with the roles of /dev/ttyS1 and /dev/tun0 reversed.

Control Path:

1. When the IOx app performs TCGETS ioctl call on /dev/ttyTun0, the tunnel driver uses /dev/cttyTun to send request to the CTTY handler service running in IOS.
2. CTTY handler service and the kernel driver use a client-server architecture to communicate configuration objects.
3. Upon receiving the request about TCGETS from /dev/cttyTun, the CTTY handler examines the request and requests Line driver to populate the required data into control data structures.
4. Upon receiving the control data structures, CTTY handler sends out a response to /dev/cttyTun which eventually goes back to /dev/ttyTun0.
5. /dev/ttyTun0 passes the control data to IOx app as requested.
6. Similar path can be extrapolated for TCSETS where the CTTY handler requests the Line driver to update the settings of the underneath /dev/ttyS1 driver.
7. Line driver of Line 0/2/0 and driver config on /dev/ttyTun0 are always in sync with each other. Any configuration changes such as baud rate modification is transparently propagated to the Line driver without any additional configuration overhead. This emulates the propagation feature of Serial relay on the IR800 series where the virtual serial port can configure the parameters of the real serial port.
Configuration Commands

IR1101#configure terminal
IR1101(config)#interface async 0/2/0
IR1101(config-if)#encapsulation relay-line
IR1101(config-if)#exit
IR1101(config)#relay line 0/2/0 0/0/0
IR1101(config)#exit
IR1101#
Cisco SD-WAN Support

This chapter contains the following sections:

- Cisco SD-WAN Overview, on page 357
- Related Documentation, on page 358

Cisco SD-WAN Overview

Cisco SD-WAN is a cloud-first architecture that separates data and control planes, managed through the Cisco vManage console. You can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and co-location facilities to improve network speed, security, and efficiency.

Cisco SDWAN adopts a cloud based solution, it consists of vOrchestrator, vManage, vSmart and vEdge.

- vOrchestrator is responsible for launching all controllers VMs in the cloud.
- vManage is the management plane for the overall SDWAN solution. It uses netconf/YANG to talk to vEdge devices.
- vSmart is the control plane for the overall SDWAN solution. It talks to the vEdge device, acts as the route reflector, key reflector, and policy engine.
- vEdge is the data plane of the overall SDWAN solution. The IR1101 platform talks to vSmart, vManage, as part of the SDWAN network.

The follow diagram shows the high level architecture of SDWAN:
While Cisco SD-WAN is a cloud-first architecture, some of the components can be deployed on-premises. Refer to the Cisco SD-WAN landing page for further information on the capabilities of SD-WAN.

Starting with IOS XE release 17.3.2, the IOS XE image can be configured as controller mode to run SD-WAN. A single universalk9 image is used to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality. This universalk9 image supports two modes - Autonomous mode (for Cisco IOS XE features) and Controller mode (for Cisco SD-WAN features).

Access the Cisco IOS XE and Cisco IOS XE SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the router and includes the Cisco IOS XE functionality. To access Cisco IOS XE SD-WAN functionality, switch to the Controller mode. You can use the existing Plug and Play Workflow to determine the mode of the device.

Note

The PnP process works on either Gi0/0/0 or Cellular.

See the Cisco SD-WAN Getting Started Guide for further information.

Related Documentation

Cisco SDWAN documentation is available from the following sources:

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features

All of the technical documentation for Cisco SD-WAN can be found here:

ROM Monitor Overview

This chapter contains the following sections:

- ROM Monitor Overview, on page 359
- Access ROM Monitor Mode, on page 360
- Displaying the Configuration Register Setting, on page 362
- Environment Variable Settings, on page 363
- Exiting ROM Monitor Mode, on page 364

ROM Monitor Overview

The ROM Monitor is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a router. When you connect a terminal to the router that is in ROM Monitor mode, the ROM Monitor (rommon 1>) prompt is displayed.

During normal operation, users do not use ROM Monitor mode. ROM Monitor mode is used only in special circumstances, such as reinstalling the entire software set, resetting the router password, or specifying a configuration file to use at startup.

The ROM Monitor software is known by many names. It is sometimes called ROMMON because of the CLI prompt in ROM Monitor mode. The ROM Monitor software is also called the boot software, boot image, or boot helper. Although it is distributed with routers that use the Cisco IOS XE software, ROM Monitor is a separate program from the Cisco IOS XE software. During normal startup, the ROM Monitor initializes the router, and then control passes to the Cisco IOS XE software. After the Cisco IOS XE software takes over, the ROM Monitor is no longer in use.

Environmental Variables and the Configuration Register

Two primary connections exist between ROM Monitor and the Cisco IOS XE software: the ROM Monitor environment variables and the configuration register.

The ROM Monitor environment variables define the location of the Cisco IOS XE software and describe how to load it. After the ROM Monitor has initialized the router, it uses the environment variables to locate and load the Cisco IOS XE software.

The configuration register is a software setting that controls how a router starts up. One of the primary uses of the configuration register is to control whether the router starts in ROM Monitor mode or Administration EXEC mode. The configuration register is set in either ROM Monitor mode or Administration EXEC mode as needed. Typically, you set the configuration register using the Cisco IOS XE software prompt when you
need to use ROM Monitor mode. When the maintenance in ROM Monitor mode is complete, you change the configuration register so the router reboots with the Cisco IOS XE software.

**Accessing ROM Monitor Mode with a Terminal Connection**

When the router is in ROM Monitor mode, you can access the ROM Monitor software only from a terminal connected directly to the console port of the card. Because the Cisco IOS XE software (EXEC mode) is not operating, nonmanagement interfaces are not accessible. Basically, all Cisco IOS XE software resources are unavailable. The hardware is available, but no configuration exists to make use of the hardware.

**Network Management Access and ROM Monitor Mode**

It is important to remember that ROM Monitor mode is a router mode, not a mode within the Cisco IOS XE software. It is best to remember that ROM Monitor software and the Cisco IOS XE software are two separate programs that run on the same router. At any given time, the router runs only one of these programs.

One area that can be confusing when using ROM Monitor and the Cisco IOS XE software is the area that defines the IP configuration for the Management Ethernet interface. Most users are comfortable with configuring the Management Ethernet interface in the Cisco IOS XE software. When the router is in ROM Monitor mode, however, the router does not run the Cisco IOS XE software, so that Management Ethernet interface configuration is not available.

When you want to access other devices, such as a TFTP server, while in ROM Monitor mode on the router, you must configure the ROM Monitor variables with IP access information.

---

**Note**

TFTP access variables are currently not supported on the IR1101 platform.

---

**Access ROM Monitor Mode**

The following sections describe how to enter the ROMMON mode, and contains the following sections:

**Checking the Current ROMMON Version**

To display the version of ROMmon running on a router, use the `show rom-monitor` command. To show all variables that are set in ROMmon, use `show romvar`.

```
Router# show rom-monitor r0
System Bootstrap, Version 1.2, RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Router# show romvar
ROMMON variables:
PS1 = rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
LICENSE_SUITE =
RET_2_RTS =
Diagnostic = 1
THRPUT =
USER_BOOT_PARAM = DEBUG_CONF=/bootflash/debug.conf
EULA_ACCEPTED = TRUE
BOOT_WDOG = DISABLE
```
License Boot Level =
BOOT = bootflash:ir1101_crashkernel.bin,1;
CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 1662155698

Router# reload

If your configuration register was set to hex value 0x0 or 0x1820, reload operation will bring you to the
ROMmon mode command prompt (rommon 1>). Invoking the set command at the prompt (rommon 1> set)
will display the same information as "show romvar" above in IOS/XE exec mode.

```
rommon 1 > set
PS1=rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
LICENSE_SUITE =
RET_2_RTS =
Diagnostic = 1
THRPRT =
USER_BOOT_PARAM = DEBUG_CONF=/bootflash/debug.conf
EULA_ACCEPTED = TRUE
BOOT_WDOG = DISABLE
LICENSE_BOOT_LEVEL =
BOOT = bootflash:ir1101_crashkernel.bin,1;
CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 1662155698
```

Commonly Used ROM Monitor Commands

The following table summarizes the commands commonly used in ROM Monitor. For specific instructions
on using these commands, refer to the relevant procedure in this document.

<table>
<thead>
<tr>
<th>ROMMON Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot image</td>
<td>Manually boots a Cisco IOS XE software image.</td>
</tr>
<tr>
<td>boot image –o config-file-path</td>
<td>Manually boots the Cisco IOS XE software with a temporary alternative administration configuration file.</td>
</tr>
<tr>
<td>confreg</td>
<td>Changes the config-register setting.</td>
</tr>
<tr>
<td>dev</td>
<td>Displays the available local storage devices.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays the files on a storage device.</td>
</tr>
<tr>
<td>reset</td>
<td>Resets the node.</td>
</tr>
<tr>
<td>set</td>
<td>Displays the currently set ROM Monitor environmental settings.</td>
</tr>
<tr>
<td>sync</td>
<td>Saves the new ROM Monitor environmental settings.</td>
</tr>
<tr>
<td>unset</td>
<td>Removes an environmental variable setting.</td>
</tr>
</tbody>
</table>
Examples

The following example shows what appears when you enter the `?` command on a router:

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
dev                 list the device table
dir                 list files in file system
help                monitor built-in command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
showmon             display currently selected ROM monitor
sync                write monitor environment to NVRAM
token               display board's unique token identifier
unalias             unset an alias
unset               unset a monitor variable
```

Changing the ROM Monitor Prompt

You can change the prompt in ROM Monitor mode by using the `PS1=` command as shown in the following example:

```
rommon 8 > PS1="IR1101 rommon ! > ">
IR1101 rommon 9 >
```

Changing the prompt is useful if you are working with multiple routers in ROM Monitor at the same time. This example specifies that the prompt should be “IR1101 rommon ”, followed by the line number, and then followed by “ > “ by the line number.

Displaying the Configuration Register Setting

To display the current configuration register setting, enter the `confreg` command without parameters as follows:

```
rommon > confreg
```

```
Configuration Summary
   (Virtual Configuration Register: )
enabled are:
   [ 0 ] break/abort has effect
   [ 1 ] console baud: 9600
   boot:...... the ROM Monitor
do you wish to change the configuration? y/n [n]:
```

The configuration register setting is labeled `Virtual Configuration Register`. Enter the `no` command to avoid changing the configuration register setting.
Environment Variable Settings

The ROM Monitor environment variables define the attributes of the ROM Monitor. Environmental variables are entered like commands and are always followed by the equal sign (=). Environment variable settings are entered in capital letters, followed by a definition. For example:

```
IP_ADDRESS=10.0.0.2
```

Under normal operating conditions, you do not need to modify these variables. They are cleared or set only when you need to make changes to the way ROM Monitor operates.

This section includes the following topics:

Frequently Used Environmental Variables

The following table shows the main ROM Monitor environmental variables. For instructions on how to use these variables, see the relevant instructions in this document. The IR1101 boot loader does not support netboot, so any setting like environment variables IP_ADDRESS, IP_SUBNET_MASK, DEFAULT_GATEWAY, TFTP_SERVER, TFTP_FILE are not used.

<table>
<thead>
<tr>
<th>Environmental variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT= path/file</td>
<td>Identifies the boot software for a node. This variable is usually set automatically when the router boots.</td>
</tr>
</tbody>
</table>

Displaying Environment Variable Settings

To display the current environment variable settings, enter the set command:

```
rommon 1 > showmon
```

```
System Bootstrap, Version 1.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
IR1101-K9 platform with 4188160 Kbytes of main memory
MCU Version - Bootloader: 4, App: 4
MCU is in application mode.
```

Entering Environment Variable Settings

Environment variable settings are entered in capital letters, followed by a definition. The following example shows the environmental variables that can be configured in ROMmon mode:

```
rommon 1 > confreg 0x0
rommon 1> BOOT_WDOG = DISABLE
rommon 1> BOOT = IR1101-K9_image_name
```
Saving Environment Variable Settings

To save the current environment variable settings, enter the `sync` command:

```
rommon > sync
```

**Note**

Environmental values that are not saved with the `sync` command are discarded whenever the system is reset or booted.

Exiting ROM Monitor Mode

To exit ROM Monitor mode, you must change the configuration register and reset the router.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> confreg</td>
<td>Initiates the configuration register configuration prompts.</td>
</tr>
<tr>
<td>Example: <code>rommon 1&gt; confreg</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> reset</td>
<td>Resets and initializes the router.</td>
</tr>
<tr>
<td>Example: <code>rommon 2&gt; reset</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Example**

```
rommon 3 > confreg
Configuration Summary
(Virtual Configuration Register: 0x0)
enabled are:
[ 0 ] break/abort has effect
[ 1 ] console baud: 9600
boot: ...... the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
enable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
disable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]:
change the boot characteristics? y/n [n]:
Configuration Summary
```
Upgrading the ROMmon for a Router

ROMmon upgrade on the IR1101-K9 router is automatically done when the image is booted. The latest version of the ROMmon is bundled with the IOSXE image. An algorithm detects if the current running version is older than the bundled version, if so, it is automatically upgraded. If the current running version is equal to the bundled version no upgrade is executed. For every successful upgrade, the router is automatically rebooted in order for the new version to get loaded and executed:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>(Optional) Run the <code>show rom-monitor slot</code> command on the router to see the current release numbers of ROMmon on the hardware. See the Checking the Current ROMMON Version, on page 360 for information about interpreting the output of the command that you run.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>If autoboot has not been enabled by using the <code>config-register 0x2102</code> command, run the <code>boot filesystem:/file-location</code> command at the ROMmon prompt to boot the Cisco IOS XE image, where <code>filesystem:/file-location</code> is the path to the consolidated package file. The ROMmon upgrade is not permanent for any piece of hardware until the Cisco IOS XE image is booted.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Run the <code>enable</code> command at the user prompt to enter the privileged EXEC mode after the boot is complete.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Run the <code>show rom-monitor slot</code> command to verify whether the ROMmon has been upgraded.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 29

WAN Monitoring

This chapter contains the following sections:

• Information About WANMon, on page 367
• Prerequisites, on page 368
• Guidelines and Limitations, on page 368
• Configuring WANMon, on page 368
• Verifying WANMon Configuration, on page 370
• Configuration Examples, on page 371

Information About WANMon

WANMon is a flexible solution to address the WAN link recovery requirements for the following products and interfaces:

• Physical networks: 4G LTE and Ethernet (WAN port)
• Virtual links: Non-crypto map based IPSec tunnels (either legacy or FlexVPN); that is, any IPSec tunnel you configure as an interface.

You enable WANMon to monitor your WAN links and initiate link recovery actions on receipt of link failure triggers.

Built-in Recovery Actions

The following are the three levels of built-in recovery processes specific to the link type:

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Recovery Actions</th>
<th>Level 1 (Active)</th>
<th>Level 2 (Last-Resort)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4G LTE</td>
<td>Clear interface, and then shut/no-shut</td>
<td>Module reload</td>
<td>System reload</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Clear interface, and then shut/no-shut</td>
<td>No action taken</td>
<td>System reload</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Shut/no-shut</td>
<td>No action taken</td>
<td>System reload</td>
</tr>
</tbody>
</table>
Each level has two time-based thresholds based on which built-in recovery actions are taken. The following are the default settings for each level:

- **threshold** is the wait time in minutes after receipt of a link failure trigger to initiate the recovery action as set in the specified level.
- **mintime** is the frequency to perform the recovery action if the link remains down.

The built-in values are:

<table>
<thead>
<tr>
<th>Level</th>
<th>threshold</th>
<th>mintime</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>10 min</td>
<td>10 min</td>
<td>Triggers Level 0 actions 10 minutes after the link went down. Repeat no more than every 10 minutes.</td>
</tr>
<tr>
<td>Level 1</td>
<td>60 min</td>
<td>60 min</td>
<td>Triggers Level 1 actions 10 minutes after the link went down. Repeat no more than every 60 minutes.</td>
</tr>
<tr>
<td>Level 2</td>
<td>480 min</td>
<td>60 min</td>
<td>Triggers Level 2 actions 480 minutes after the link went down. Repeat no more than every 60 minutes.</td>
</tr>
</tbody>
</table>

If threshold values are specified as 0, no recovery actions are taken for that level. You can use this to avoid system reload (the built-in Level 2 recovery action) on receipt of a link failure trigger where other WAN links may be operational.

---

**Prerequisites**

Ensure that the WANMon module is available. The WANMon module is included in the IOS-XE image as the `tm_wanmon.tcl` policy file.

**Guidelines and Limitations**

- WANMon automatically performs IP address checking (no user configuration) as required for cellular interfaces.
- For all other interfaces, WANMon never performs IP address checking.
- WANMon indirectly triggers user-specified actions by generating an application event that link resetter applets monitor.
- If your network is live, ensure that you understand the potential impact of any command.

**Configuring WANMon**

You can enable WANMon on the router and assign WANMon support to specific interfaces. Optionally, you can override the built-in recovery actions, define custom recovery links, and define an event manager.
environment policy to set the track object value and disable IP address checking. WANMon is disabled by
default.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>event manager policy <em>im_wanmon.tcl</em> authorization bypass</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Enables the WANMon link recovery module. Use authorization bypass to avoid authorization for CLIs invoked by this policy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>event manager environment wanmon_if_list &lt;instance&gt; (interface name {ipsla &lt;instance&gt; })</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Configures WANMon for the interfaces in your WAN, and indicates that this is an interface configuration command.</td>
</tr>
</tbody>
</table>

**Note** Any environment variable with the prefix wanmon_if_list constitutes an interface configuration. Multiple interfaces are allowed by specifying an instance. Be sure to specify the full interface name (for example, cellular0/1/0 or cellular0/3/0). You can set the IP SLA icmp-echo trigger, if desired. Multiple IP SLA triggers are allowed by specifying an instance. **Note** WANMon only looks at the status of the SLA ID. Even though icmp-echo is most common, if needed any other type of SLA probe (for example, udp-echo) can be used instead.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>event manager environment wanmon_if_listsx (interface name {recovery Level0 {Level1 Level2}})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>(Optional) Overrides the built-in thresholds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>publish-event sub-system 798 type 2000 arg1 &lt;interface name&gt; arg2 &lt;level&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>(Optional) Configures custom recovery actions using link resetter applets. <code>&lt;interface&gt;</code> is the full interface name (for example, cellular0/1/0 or cellular0/3/0). <code>&lt;level&gt;</code> is 0, 1, or 2 to match the desired link recovery action.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>{stub &lt;track-stub-id&gt;}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>(Optional) Allows an event manager environment policy to set the track object value. WANMon can set a track-stub-object value to reflect the link state so that an external applet can track the stub object.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>event manager environment wanmon_if_listsx (interface name {checkip &lt;instance&gt; })</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>(Optional) Disables IP address checking.</td>
</tr>
</tbody>
</table>

**What to do next**

**EXAMPLES**
event manager policy tm_wanmon.tcl authorization bypass

The following examples are Event Manager commands to configure cellular and Ethernet interfaces:

event manager environment wanmon_if_list1 {cellular0/1/0 {ipsla 1}}
event manager environment wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}

This example sets custom recovery thresholds:

event manager environment wanmon_if_list {cellular0/1/0 {recovery 20 (90 75) 600}}

where:

- The Level 0 threshold is set to 20 minutes after the link failure trigger. Level 0 recovery actions are performed for the cellular interface. Repeats indefinitely, no more than every 10 minutes (default).
- Level 1 threshold is set to 90 minutes. Level 1 recovery actions are performed for the cellular interface. Repeats no more frequently than every 75 minutes.
- The Level 2 threshold is set to 600 minutes (10 hours).

The following sets the track-stub-object value to 21:

```conf
t
track 21 stub-object
```
event manager environment wanmon_if_list {cellular0/1/0 {ipsla 1} {stub 21}}

**Verifying WANMon Configuration**

Use the following steps to verify your WANMon configuration.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show event manager policy registered</td>
<td>Displays the WAN monitoring policy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show event manager environment</td>
<td>Displays the interface environment variables set during interface configuration.</td>
</tr>
</tbody>
</table>

**What to do next**

**EXAMPLE**

```
show event manager policy registered
1 script system multiple Off Thu Jan 16 18:44:29 2014 tm_wanmon.tcl
show event manager environment
1 wanmon_if_list {cellular0/1/0 {ipsla 1}}
```
Configuration Examples

The following examples are provided:

**WANMon Cellular Interface Configuration Example**

```plaintext
track 1 ip sla 1
ip sla 1
  icmp-echo 172.27.166.250
  timeout 6000
  frequency 300
ip sla schedule 1 life forever start-time now
event manager environment wanmon_if_list {cellular0/1/0 {ipsla 1}}
event manager policy tm_wanmon.tcl authorization bypass
```

**Multiple WAN Link Monitoring Example**

```plaintext
track 1 ip sla 1
track 21 stub-object
ip sla 1
  icmp-echo 172.27.166.250
  timeout 6000
  frequency 300
ip sla schedule 1 life forever start-time now
track 2 ip sla 2
track 22 stub-object
ip sla 2
  icmp-echo 10.27.16.25
  timeout 6000
  frequency 300
ip sla schedule 2 life forever start-time now
event manager environment wanmon_if_list1 {cellular0/1/0 {ipsla 1} {stub 21}}
event manager policy tm_wanmon.tcl authorization bypass
```
Overview

The router adds DSL capability by using a Small Form-factor Pluggable (SFP) network interface module. The DSL solution supports the following Annex:

ADSL2 (A), ADSL2+(A,J, where J only supported by the 17.5.1 release). VDSL2 supports Annex A,B. All in compliance with TR100, TR105, TR114, TR115.

IOS-XE release 17.5.1 adds in support for Annex-J configuration in the controller interface.

Note

ADSL2+ J is supported, ADSL2 J is not yet supported in 17.5.1.

To enable Annex-J, perform the following:

```
router#config term
router(conf)#controller vdsl 0/0/0
router(conf-if)#capability annex-j
router(conf-if)#exit
router#
```
To remove Annex-J, perform the following:

```
router#config term
router(config)#controller vdsl 0/0/0
router(config-if)#no capability annex-j
router(config-if)#exit
router#
```

17.5.1 adds in a new command `rx-padding`. This command is used for packets with an MTU less than 64 bytes.

---

**Note**

If frames less than 64mtu are expected downstream from the service provider, the Vlan configuration must be vlan 96. If frames less than 64mtu are expected downstream from the service provider, only a Single VLAN is supported in a single-PVC, i.e. Vlan96. In future releases, there is plan to extend the range of vlan support to range from Vlan44 to 1024, single-vlan in single-pvc option.

The command example is as follows:

```
router#config term
router#controller vdsl 0/0/0
router(config-if)#rx-padding
router(config-if)#end
router#write mem
```

**Feature Caveats**

This section provides a list of what features are supported and unsupported.

- The DSL SFP operates only when inserted in the IR1101 base unit. It is NOT supported in the IRM-1100 expansion unit. The IR1101 can support only a single DSL SFP on GI0/0/0
- VDSL2 only supports profiles 8a through 17a, 30a is not supported.
- The SFP currently does not have Yang support. This will be provided in a future release.
- Supports Radius and AAA when authenticating and configuring DSL users.
- The DSL interface requires a minimum configuration dependent of the DSL services, therefore Plug and Play (PnP) features are not available on the DSL interface.
- Zero-Touch-Deployment (ZTD) is only supported through IIoT Field Network Director. From FND, use cgna wsma based ZTD only, PnP based ZTD is not supported over the DSL interface. For ZTD, stage with basic minimum configuration and parameters depending on the service provider requirements.
- The show controller vdsl 0/0/0 command is used to display all DSL [VDSL2/ADSL2/ADSL2+] controller information, similar to the c111x platforms. Although the controller command is vdsl, is actually means dsl and is used for adsl and vdsl alike.
- For ADSL2/2+ configurations, there is no ATM interface as with c111x platforms. All configurations are on the DSL SFP WAN g0/0/0 interface, its sub-interface options, and controller vdsl0/0/0 itself. ATM packets are handled by the DSL SFP and re-assembled as Ethernet packets. Annex A, L is supported.
- Using the WebUI, interface g0/0/0 can be configured/monitored as normal. No specific options to monitor/configuration option for Controller vdsl 0/0/0 on release 17.4.1.
• VDSL2 and ADSL2+ various MIBS support only trickle in 17.5.1 and beyond releases. MIB information is available later in this section.

• For ADSL2/2+ ATM configuration, if your scenario expects frames <64 byte MTU downstream from Service Provider, please ensure following steps:
  1. rx-padding cli is enabled
  2. Vlan96 value is used in interface configuration
  3. There is no multi-VLAN support in single-PVC in this specific scenario

### DSL Feature Specifications

#### Table 17: DSL Feature Specifications

<table>
<thead>
<tr>
<th>Multimode DSL (VDSL2 and ADSL2/2+)</th>
<th>Provided through a DSL SFP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFP has a single RJ-45 interface</td>
</tr>
<tr>
<td></td>
<td>Support for double-ended line testing (DELT) diagnostics mode (VDSL2 Only)</td>
</tr>
</tbody>
</table>

#### Table 18: VDSL2 Feature Specifications

<table>
<thead>
<tr>
<th>VDSL2</th>
<th>VDSL2 993.2 Annex A and Annex B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>997 and 998 band plans</td>
</tr>
<tr>
<td></td>
<td>G.994.1 ITU G.hs</td>
</tr>
<tr>
<td></td>
<td>VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, and 17a</td>
</tr>
<tr>
<td></td>
<td>Vectoring</td>
</tr>
<tr>
<td></td>
<td>U0 band support (25 to 276 kHz)</td>
</tr>
<tr>
<td></td>
<td>Ethernet packet transfer mode (PTM) based only on IEEE 802.3ah 64/65 octet encapsulation</td>
</tr>
<tr>
<td></td>
<td>Dying gasp</td>
</tr>
</tbody>
</table>
### Installing the DSL SFP

Instructions for inserting the DSL SFP are found in your products Hardware Installation Guide.

**Warning**

It is critical that the installer read these instructions and be familiar with the correct method of inserting and removing the SFP. Failure to do so may result in damage to the SFP.

The minimum IOS-XE release for DSL SFP support is 17.4.1 on the IR1101.

---

Table 19: ADSL2/2+ Feature Specifications

<table>
<thead>
<tr>
<th>ADSL2/2+</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Annex A and L for ADSL2</td>
<td></td>
</tr>
<tr>
<td>• Annex A for ADSL2+</td>
<td></td>
</tr>
<tr>
<td>• Annex J for ADSL2+ (available in 17.5.1)</td>
<td></td>
</tr>
<tr>
<td>• G.994.1 ITU G.hs</td>
<td></td>
</tr>
<tr>
<td>• Reach-extended ADSL2 (G.922.3) Annex L for increased performance on loop lengths greater than 16,000 feet from central office</td>
<td></td>
</tr>
<tr>
<td>• T1.413 ANSI ADSL2/2+ DMT issue 2 compliance</td>
<td></td>
</tr>
<tr>
<td>• DSL Forum TR-067, and TR-100 conformity</td>
<td></td>
</tr>
<tr>
<td>• Impulse noise protection (INP) and extended INP</td>
<td></td>
</tr>
<tr>
<td>• Downstream power backoff (DPBO)</td>
<td></td>
</tr>
<tr>
<td>• Dying gasp</td>
<td></td>
</tr>
</tbody>
</table>

Dying gasp is when the router is using some residual power on capacity to send outage messages to the DSLAM. You can verify your router is ready to send out dying gasp messages by using the `show controller vdsl 0/0/0 local` command:

```
Router#show controllers vdsl 0/0/0 local
SFP Vendor PID: SFPV5311TR
SFP Vendor SN: V021932028C
Firmware embedded in IOS-XE: 1_62_8463
Running Firmware Version: 1_62_8455
Management Link: up
DSL Status: showtime
Dying Gasp: armed
Dumping internal info: idle
Dying Gasp: armed
Dumping DELT info: idle
```

If Dying Gasp is disabled, the output will show **Dying gasp: disarmed**.

There is no configuration for Dying Gasp. The Software takes care internally for the implementation. Once an SFP shut/no shut has been triggered, 1-2 notifications are sent within 50ns.
Basic Configuration

Once the SFP is installed, it requires a basic configuration to bring it up. Follow these steps:

```
configure t
Router(conf)#interface g0/0/0
Router(conf-if)#media-type sfp
Router(conf-if)#no shut
Router(conf-if)#exit
```

At this point, SFP insertion SYSLOG messages will appear.

SFP Verification

After safely installing the SFP, you can check its status with the `show inventory` command:

```
Router#show inventory
```

```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++  

NAME: "Chassi", DESCR: "IR1101 Base Chassi"  
PID: IR1101-K9 , VID: V03 , SN: FCW23500H5X  

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"  
PID: IR1101-K9 , VID: V03 , SN: FCC23473SRK  

NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"  
PID: IR1101-ES-5 , VID: V01 , SN:  

NAME: "subslot 0/0 transceiver 0", DESCR: "GE T"  
PID: SFP-VADSL2+-I , VID: V01 , SN: MET2023000A  

Ignore the description, it will always reflect GE T for all IR1101 SFPs  
PID and S/N are what matter  

In the below output, ignore the Description and bitrate. The PID/Serial number information are true to the SFP.

```
Router#show interfaces transceiver detail
IDPROM for transceiver Gigabitethernet0/0/0:  
Description = SFP or SFP+ optics (type 3)  
Transceiver Type: = GE T (26)  
Product Identifier (PID) = SFP-VADSL2+-I  
Vendor Revision = V5.1  
Serial Number (SN) = MET2023000A  
Vendor Name = CISCO-METANOIA  
Vendor OUI (IEEE company ID) = 00.00.00 (0)  
CLEI code =  
Cisco part number = 74-124941  
Device State = Enabled.  
Date code (yy/mm/dd) = 20/23/  
Connector type = .  
Encoding = SB10B (1)  
Nominal bitrate = GE (1300 Mbits/s)  
Minimum bit rate as % of nominal bit rate = not specified  
Maximum bit rate as % of nominal bit rate = not specified  
```

Socket Verification

```
SFP IDPROM Page 0xA0:  
000: 03 04 22 08 00 00 00 00 00 00 00 00 00 00
010: 00 01 0D 00 00 00 00 00 FF 00
020: 43 49 53 43 4F 2D 4D 45 54 41
```
Installing the DSL SFP

Link reach for 9u fiber (km) = SX(550/270m) (0)
1xFc-MM(500/300m) (0)
ESCON-MM(2km) (0)

Link reach for 9u fiber (m) = SX(550/270m) (0)
1xFc-MM(500/300m) (0)
ESCON-MM(2km) (0)

Link reach for 50u fiber (km) = SR(2km) (0)
IR-1(15km) (0)
IR-2(40km) (0)
LR-1(40km) (0)
LR-2(80km) (0)
LR-3(80km) (0)
DX(40km) (0)
HX(40km) (0)
LED Indications on the SFP

The DSL SFP has two LED indicators built into it. This LED operates independent of any LED that is on the panel of the Router.

There is no show platform led support for the SFP LED. Use the show controller vdsl 0/0/0 local command for DSL link status.

LED Indications

The following table describes the SFP LED indications:

<table>
<thead>
<tr>
<th>Indicator LED</th>
<th>LED Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED 1</td>
<td>Orange</td>
<td>On</td>
<td>CPE side (expected to be ON when used on an IR router)</td>
</tr>
<tr>
<td>LED 1</td>
<td>Orange</td>
<td>Off</td>
<td>Central office side (not supported)</td>
</tr>
<tr>
<td>xDSL Status LED</td>
<td>Green</td>
<td>Slow Flash</td>
<td>Idle</td>
</tr>
<tr>
<td>xDSL Status LED</td>
<td>Green</td>
<td>Fast Flash</td>
<td>Training</td>
</tr>
<tr>
<td>xDSL Status LED</td>
<td>Green</td>
<td>Steady</td>
<td>Showtime</td>
</tr>
<tr>
<td>xDSL Status LED</td>
<td>Green</td>
<td>Extremely Rapid Flash</td>
<td>Packet Transmit</td>
</tr>
</tbody>
</table>

SFP LED Workflow

The following table describes the SFP LED indications during a bootup:
### Auto-Negotiation

You can tell the status of auto-negotiation based on the LED on the SFP. On shut/no shut or during auto-negotiation, the following sequence should be observed:

<table>
<thead>
<tr>
<th>Status</th>
<th>LED Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>Slow Flashing Green</td>
</tr>
<tr>
<td>Training</td>
<td>Fast Flashing Green</td>
</tr>
<tr>
<td>Handshake success, Showtime</td>
<td>Solid Green</td>
</tr>
</tbody>
</table>

If the SFP LED is toggling between slow flashing green and fast flashing green, it usually means it is in auto-negotiation mode. If this continues for a long time, the DSLAM and Router DSL SFP parameters need to be rechecked. The following chapters cover more details on Router xDSL configuration.

### DSL SFP Firmware Upgrade

The DSL SFP has firmware loaded on it. You should check the version loaded on the SFP and compare it to what is available in the router image. The customer should make their decision to upgrade according to their own agreement with their ISP.

The SFP must have a minimum configuration in order to upgrade it:

```
configure t
Router(config)#interface g0/0/0
Router(config-if)#media-type sfp
Router(config-if)#no shut
Router(config-if)#exit
```

Check your firmware levels by executing `show controllers vdsl 0/0/0 local` command.

```
Router#show controllers vdsl 0/0/0 local
SFP Vendor PID: SFPV5311TR
SFP Vendor SN: V021932028C
Firmware embedded in IOS-XE: 1_62_8463
Running Firmware Version: 1_62_8455
Management Link: up
DSL Status: showtime
Dumping internal info: idle
Dying Gasp: armed
Dumping DELT info: idle
```

Use the following command to upgrade the SFP:
Router\texttt{# upgrade hw-module subslot 0/0 sfp 0}
Upgrade SFP firmware on interface GigabitEthernet0/0/0 from 1_62_8455 to 1_62_8463
Connection will be disrupted, Continue\(\text{\texttt{Y/N}}\)\text{\texttt{?y}}
Start ebm upgrade!!
........................................................
........................................................
..................
firmware update success!!

The command loads the new firmware, and then performs a shut/no shut on the interface to reset the SFP.

---

\textbf{Note}

In 17.5.1 and beyond, the capability exists to upgrade standalone SFP Firmware, in addition to the SFP Firmware bundled with IOS image. For example:

\texttt{Router# upgrade hw-module subslot 0/0 sfp 0 \{flash|usbflash0|msata\}:sfp-fw_image}

\textbf{MTU Limitation}

As per the SFP Data sheet specification, the following are MTU limitations:

- For VDSL, the MTU range on the DSL SFP interface is between 64 - 1800 Bytes
- For ADSL2/2+, the MTU range on the DSL SFP interface is between 64 - 1700 Bytes

---

\textbf{ADSL2/2+}

\textbf{ADSL2/2+ Overview}

This section provides an overview for ADSL2/2+

---

\textbf{Important}

The Router SFP based DSL support differs in configuration and troubleshooting in comparison to other ISR DSL platforms. There is no ATM interface, ethernet to ATM packet translation is handled internally via Adaption Layer5 (AAL5). All configurations are on the controller vdsl 0/0/0 and g0/0/0 interface/sub-interface. UBR is recommended over AAL5.

All details are listed in the chapters that follow.

ADSL2/2+ works in auto mode (configuration on DSLAM auto-negotiation automatically with the DSL controller). Annex A is supported on ADSL2+. Annex A and reach-extended Annex L mode-1 is supported on ADSL2. This is in compliance with TR-100/TR-105

- For Auto-negotiation handshake procedure, the SFP is compliant with ITU-T G.994.1 DSL TRx and for Physical Layer Management compliant with ITU-T G.997.1 for DSL TRx.
- The DSL SFP complies with ITU-T G.99x standard with supporting AVD2 CPE mode only.
- Supports LLC/SNAP and VCMux ethernet bridged encapsulation option.
- All PPPoX encapsulation is configured via PPPoE only. Internally, packet translation is handled via ATM. There is no PPPoA configuration like there is with the c1111x ISR.
• ADSL-PVC is configurable in the Controller VDSL 0/0/0: Each SFP supports 8 PVCs.
• Each PVC supports mapping to/from 802.1q Vlan tagging.
• VPI range is 0-255, VCI range is 32-65535.

The ‘mode’ reflected in `show controller vdsl 0/0/0` will always be PTM (Packet transfer mode). Internally packet translation to ATM is handled (AAL5).

## Configuring ADSL2/2+

The Router supports Asymmetric Digital Subscriber Line (ADSL) 2/2+.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> controller vdsl &lt;port&gt;</td>
<td>Enters configuration mode for the ADSL2/2+ controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config)# controller vdsl 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> adsl-pvc &lt;vpi/vci&gt;</td>
<td>Configures the PVC's VPI and VCI parameters. Refer to ADSL2/2+ PVC Sub Mode, on page 384 for detailed sub-commands.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller)#adsl-pvc 0/35</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> bridge-dot1q &lt;1-4094&gt;</td>
<td>Configures the PVC's bridge-dot1q parameter.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller-adsl-pvc)#bridge-dot1q 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation llcsnap</td>
<td>vcmux</td>
</tr>
<tr>
<td>Example:</td>
<td>Disabled by default. Can be either llcsnap or vcmux. This example shows the PVC encapsulation as LLCSNAP.</td>
</tr>
<tr>
<td>router(config-controller-adsl-pvc)#encapsulation llcsnap</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Enables new configuration to take effect.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller-adsl-pvc)#exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
**ADSL2/2+ Controller Configuration Commands**

This section describes some of the CLI commands specific to controller configuration.

<table>
<thead>
<tr>
<th>Brief</th>
<th>Format</th>
<th>Command Default</th>
<th>Description</th>
<th>Differences From Other IOS-XE ISRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>adsl-pvc</td>
<td><code>adsl-pvc [name]</code> <code>{&lt;vpi&gt;/&lt;vci&gt;}</code></td>
<td>None</td>
<td>ADSL2/2+ PVC Submode VPI/VCI value 0-255 VCI Value 32-65535 For additional details on the ADSL2/2+ submode, refer to ADSL2/2+ PVC Sub Mode, on page 384</td>
<td>VPI: 0-31 VCI: 1-1023</td>
</tr>
<tr>
<td>bitswap</td>
<td></td>
<td>Default is Enabled</td>
<td>Bitswap</td>
<td></td>
</tr>
<tr>
<td>carrier-set</td>
<td><code>carrier-set [a43 a43c b43]</code></td>
<td>a43 a43c b43</td>
<td>DSL SFP Carrier Set</td>
<td>c111x defines these tones under the modem vdsl option. For example, v43 has to be disabled via cli. In the Router, tone v43 is disabled by default.</td>
</tr>
<tr>
<td>default</td>
<td></td>
<td></td>
<td>Set a command to its defaults</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td></td>
<td></td>
<td>Controller specific description</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
<td>Exit from controller configuration mode. This is mandatory in order to make the configuration take effect.</td>
<td></td>
</tr>
</tbody>
</table>
### ADSL2+/PVC Sub Mode

The following table lists related commands.

<table>
<thead>
<tr>
<th>Brief</th>
<th>Format</th>
<th>Default</th>
<th>Description</th>
<th>Differences From Other IOS-XE ISRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>adsl-pvc</td>
<td>adsl-pvc vpi/vci</td>
<td>None</td>
<td>A maximum of 8 PVCs can be supported on a DSL interface.</td>
<td>VPI/VCI value 0-31</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vci range 32 - 65535</td>
<td>VCI value 1-1023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vpi range 0-255</td>
<td></td>
</tr>
<tr>
<td>bridge-dot1q</td>
<td><strong>bridge-dot1q</strong>&lt;1-4094&gt;</td>
<td>None</td>
<td>802.1Q VLAN ID to PVC mapping</td>
<td></td>
</tr>
<tr>
<td>Brief</td>
<td>Format</td>
<td>Default</td>
<td>Description</td>
<td>Differences From Other IOS-XE ISRs</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>
| cbr     | **cbr <peak cell rate>**  
cbr pcr range is 0 to 5500 | No      | Configure Constant Bit Rate (CBR) Service        | 48-1408 in Kbps.                   |
| default-pvc | **default-pvc** | First PVC Created | Set PVC as default PVC                             |                                     |
|         |                 |         | The default-pvc command under adsl-pvc is an option available with the DSL SFP. It selects which PVC the DSL SFP will treat as the default when there are 2 or more active PVCs. |                                     |
| encapsulation | **encapsulation**  
<llcsnap|vcmux> | None   | Configure ADSL2/2+ PVC Encapsulation               |                                     |
| exit    |                 |         | Exit adsl-pvc sub commands                        |                                     |
| ubr     | **ubr <peak cell rate>**  
ubr peak cell rate range is 0 to 5500 | Yes     | Configure Unspecified Bit Rate (UBR) Service      | 48-1408 in Kbps.                   |
| vbr-nrt | **vbr-nrt <peak cell rate> <sustainable cell rate>**  
pcr range is 0 to 5500  
scr range is 0 to 5500 | No      | Configure Non Real-time Variable Bit Rate Service 
UBR is recommended over AAL5.                     | 48-1408 in Kbps.                   |
<table>
<thead>
<tr>
<th>Brief</th>
<th>Format</th>
<th>Default</th>
<th>Description</th>
<th>Differences From Other IOS-XE ISRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>vbr-rt</td>
<td>vbr-rt (&lt;peak cell rate&gt; &lt;sustainable cell rate&gt;)</td>
<td>No</td>
<td>Configure Real-time Variable Bit Rate Service</td>
<td>48-1408 in Kbps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UBR is recommended over AAL5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>pcr range is 0 to 5500</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scr range is 0 to 5500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vbr-rt</td>
<td></td>
<td>vbr-rt &lt;peak cell rate&gt; &lt;sustainable cell rate&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>pcr range is 0 to 5500</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scr range is 0 to 5500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlanid-rx (&lt;1-4094&gt;)</td>
<td>Depends on bridge-dot1q</td>
<td>Configure the DSL SFP to set the VLAN ID of the Ethernet packet received by the DSL SFP to be sent to the router. Used in conjunction with the DSL SFP VLAN operation vlanop-rx to either remove or replace the VLAN ID from the Ethernet packet.</td>
<td>Only on IoT Routers</td>
</tr>
<tr>
<td></td>
<td>vlanid-rx (&lt;1-4094&gt;)</td>
<td></td>
<td>vlanid-rx (&lt;1-4094&gt;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vlanid-rx (&lt;1-4094&gt;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlanid-tx (&lt;1-4094&gt;)</td>
<td></td>
<td>Configure the DSL SFP to set VLAN ID of the Ethernet packet for transmission to the network. Used in conjunction with the DSL SFP VLAN operation vlanop-tx to either remove or replace the VLAN ID from the Ethernet packet before transmitting the packet to the network.</td>
<td>Only on IoT Routers</td>
</tr>
<tr>
<td></td>
<td>vlanid-tx (&lt;1-4094&gt;)</td>
<td></td>
<td>vlanid-tx (&lt;1-4094&gt;)</td>
<td></td>
</tr>
</tbody>
</table>
### Differences From Other IOS-XE ISRs

<table>
<thead>
<tr>
<th>Brief</th>
<th>Format</th>
<th>Default</th>
<th>Description</th>
<th>Differences From Other IOS-XE ISRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlanop-rx</td>
<td><strong>vlanop-rx</strong> &lt;pass-through</td>
<td>remove</td>
<td>replace&gt;</td>
<td>Configure the VLAN ID operation of the DSL SFP to the Ethernet packet received by the DSL SFP to be sent to the router. Remove or replace VLAN operations are used in conjunction with the vlanid-rx. Pass-through option preserves the existing VLAN ID of the Ethernet packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlanop-tx</td>
<td><strong>vlanop-tx</strong> &lt;pass-through</td>
<td>remove</td>
<td>replace&gt;</td>
<td>Configure the VLAN ID operation of the DSL SFP to the Ethernet packet for transmission to the network. Remove or replace VLAN operation are used in conjunction with the vlanid-tx. Pass-through option preserves the existing VLAN ID of the Ethernet packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replace</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ADSL2+ Example

The following example is from an ADSL2+ configuration:

**Note**

For an explanation of some of the key output messages, see Controller Status Messages, on page 403.

```
Router#show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP

Daemon Status: UP
```
XTU-R (DS) XTU-C (US)
Chip Vendor ID: 'META' 'BDCM'
Chip Vendor Specific: 0x0000 0x0762
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' '
Modem Vendor Specific: 0x0000 0x0000
Modem Vendor Country: 0xB500 0x0000
Serial Number Near: MET2023000A V5311TR 1_62_8463
Serial Number Far:
Modem Version Near: 1_62_8463 MT5311.
Modem Version Far: <value>
Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.3 (ADSL2) Annex A

TC Mode: PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running
Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version:
Modem PHY Version:
Modem PHY Source: System

Line 0:
XTU-R (DS) XTU-C (US)
Trellis: ON ON
SRA: enabled enabled.
SRA count: 0 0.
Bit swap: enabled enabled.
Bit swap count: 0 0
Line Attenuation: 2.4 dB dB
Signal Attenuation: 5.0 dB 0.0 dB
Noise Margin: 8.2 dB 6.5 dB
Attainable Rate: 12491 kbits/s 1153 kbits/s
Actual Power: 0.0 dBm 10.2 dBm
Total FECC: 0 0
Total ES: 0 399
Total SES: 0 188
Total LOSS: 0 177
Total UAS: 103 6325
Total LPRS: 0 0
Total LOFS: 0 0
Total LOLS: 0 0

DS Channel1 DS Channel0 US Channel1 US Channel0
Speed (kbps): NA 12491 NA 1093
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 12583 NA 1097
Reed-Solomon EC: NA 0 NA 0
CRC Errors: NA 209 NA 0
Header Errors: NA 0 NA 0
Interleave (ms): NA 1.00 NA 1.00
Actual INP: NA 0.00 NA 0.00
ADSL2 Annex A Example

The following example is from an ADSL2 Annex A configuration:

For an explanation of some of the key output messages, see Controller Status Messages, on page 403.

```
show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)
  Chip Vendor ID: 'META' 'BDCM'
  Chip Vendor Specific: 0x0000 0x0762
  Chip Vendor Country: 0xB500 0xB500
  Modem Vendor ID: 'META' '
  Modem Vendor Specific: 0x0000 0x0000
  Modem Vendor Country: 0xB500 0x0000
  Serial Number Near: MET2023000A V5311TR 1_62_8463
  Serial Number Far:

  Modem Version Near: 1_62_8463 MT5311
  Modem Version Far:
  Modem Status: TC Sync (Showtime!)
  DSL Config Mode: AUTO
  Trained Mode: G.992.5 (ADSL2+) Annex A
  TC Mode: PTM
  Selftest Result: 0x00
  DELT configuration: disabled
  DELT state: not running

  Failed full inits: 0
  Short inits: 0
  Failed short inits: 0

  Modem FW Version:
  Modem PHY Version:
  Modem PHY Source: System

  Line 0:
  XTU-R (DS) XTU-C (US)

  Trellis: ON ON
  SRA: enabled enabled
  SRA count: 0 0
  Bit swap: enabled enabled
  Bit swap count: 0 0
  Line Attenuation: 1.4 dB dB
  Signal Attenuation: 2.4 dB 0.0 dB
  Noise Margin: 9.5 dB 6.3 dB
  Attainable Rate: 23550 kbits/s 1105 kbits/s
  Actual Power: 0.0 dBm 12.2 dBm
  Total FECC: 1 0
  Total ES: 1 396
  Total SES: 0 317
  Total LOSS: 0 287
  Total UAS: 57 3344
  Total LPRS: 0 0
  Total LOPS: 0 0
  Total LOLS: 0 0
  DS Channel1 DS Channel0 US Channel1 US Channel0
```
ADSL2 Annex L Example

The following example is from an ADSL2 Annex L configuration:

```
show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)

Chip Vendor ID: 'META' 'BDCM'
Chip Vendor Specific: 0x0000 0x0762
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' '
Modem Vendor Specific: 0x0000 0x0000
Modem Vendor Country: 0xB500 0x0000
Serial Number Near: V0219320270 V5311TR 1_62_8463
Serial Number Far:

Modem Version Near: 1_62_8463 MT5311
Modem Version Far:
Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.3 (ADSL2) Annex L
TC Mode: PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running
Failed full inits: 0
Short inits: 0
Failed short inits: 0
Modem FW Version:
Modem PHY Version:
Modem PHY Source: System
Line 0:
XTU-R (DS) XTU-C (US)

Trellis: ON ON
SRA: enabled enabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 0 0
Line Attenuation: 2.5 dB dB
Signal Attenuation: 5.7 dB 0.0 dB
Noise Margin: 7.0 dB 6.2 dB
Attainable Rate: 10164 kbits/s 288 kbits/s
```

Note

For an explanation of some of the key output messages, see Controller Status Messages, on page 403.
VDSL2

VDSL2 Overview

This section provides an overview for VDSL2.

The Router DSL SFP-VADSL2+-I provides VDSL2 Annex A, B support in conformance to ITU-T standards G.993.2 (VDSL2). This xDSL SFP is also in compliance with TR-114 (VDSL2 Annex A and B performance) and TR-115 (VDSL2 Feature validation tests by University of New Hampshire). The SFP complies with ITU-T G.99x standard with supporting AVD2 CPE mode only.

- Supports all VDSL2 profiles (8a/b/c/d, 12a/b, 17a, 30a).
- Supports EU type Upstream Band 0 (US0).
- Complies with ITU-T G.994.1 Handshake Procedure for DSL TRx.
- Complies with ITU-T G.997.1 Physical Layer Management for DSL TRx
- Complies with ITU-T G.993.5 Self-FEXT Cancellation (Vectoring) for CPE mode
- Supports Robust Overhead Channel (ROC)
- Supports Online Reconfiguration (OLR) including Seamless Rate Adaptation (SRA) with D/L change and Bit Swapping
- Supports Upstream/Downstream Power Back Off (UPBO/DPBO)
- Supports DELT
- Supported maximum MTU size on VDSL2 is 1800 Bytes
- Standard compliance VDSL2 mode is PTM (Packet transfer mode)
• Supports VDSL2 Vectoring

For configuration and display commands, see the detailed sections below. The `show controller vdsl 0/0/0` is the fundamental command for validation.

## Configuring VDSL2

The Router supports Very-high-bit-rate Digital Subscriber Line (VDSL2).

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> controller vdsl 0/0/0</td>
<td>Enters configuration mode for the VDSL2 controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller)# controller vdsl 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> carrier-set a43 a43c b43</td>
<td>Configures the carrier set. Multiple choice. Default is a43 a43c b43. v43 is disabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller)# carrier-set a43</td>
<td>a43c</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>router(config-controller)# end</td>
<td></td>
</tr>
</tbody>
</table>

### VDSL2 Controller Configuration Commands

This section describes some of the CLI commands specific to controller configuration.

<table>
<thead>
<tr>
<th>Brief</th>
<th>Format</th>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bitswap</td>
<td></td>
<td>Default is Enabled</td>
<td>Bitswap</td>
</tr>
<tr>
<td>capability</td>
<td>capability [annex-j]</td>
<td>None</td>
<td>Set the DSL SFP Capability</td>
</tr>
<tr>
<td>carrier-set</td>
<td>carrier-set [a43 b43 a43c]</td>
<td>a43 b43 a43c</td>
<td>DSL SFP Carrier Set</td>
</tr>
</tbody>
</table>
### VDSL Example

The following example is from a VDSL configuration:

```plaintext
show controllers vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)

Chip Vendor ID: 'META' 'IKNS'
Chip Vendor Specific: 0x0000 0x0101
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' '
Modem Vendor Specific: 0x0000 0x2AB0
Modem Vendor Country: 0xB500 0x37A0
Serial Number Near: E80462D1B001 SFP-V5311-T-R 8431
Serial Number Far: ^A5u
Modem Version Near: 1_62_8431 MT5311
Modem Version Far: 6.7.0.15IK005010

Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.993.2 (VDSL2) Profile 17a

TC Mode: PTM
```
Troubleshooting and L1 Training Logs

Troubleshooting

This section provides information for troubleshooting and debugging if the DSL control and/or datapath is not up.

For an explanation of some of the key output messages, see Controller Status Messages, on page 403.
**Problem:** If WAN interface g0/0/0 is DOWN:

**Solution:** Try the following:

- Check L1 cabling, networking, and with different SFP
- Capture output for `show int g0/0/0`, `show run all`, and `show version`
- Check if g0/0/0 has **media-type sfp** configuration set and the interface is unshut.
- Try another SFP to see if that is detected.
- Check SFP's LED status. Refer to **LED Indications on the SFP**, on page 379

---

**Problem:** If controller state is DOWN:

For example:

```
Router#show controllers vdsl 0/0/0
Controller VDSL 0/0/0 is DOWN
```

**Solution:** Try the following:

- Check L1 cabling.
- Try inserting RJ11 cable into an RJ11 male to RJ45 female connector to see if it helps align.
- Ensure Running FW is the same as System FW. If not, upgrade the SFP FW. Refer to **DSL SFP Firmware Upgrade**, on page 380.
- Gather output for all L1 Training logs. Ensure L1 debug logs in folder are sent to Cisco TAC, as well as the output of service internal command `test vdsl option 0x0 6`, and the output from `show controller 0/0/0 local`. Refer to **L1 Training Logs**, on page 404.
- Possible workaround: After gathering the above logs, try to reboot the router to see if it recovers. If it still does not work, try to hot remove/insert the SFP again.

---

**Problem:** If the controller is UP, but `show controller vdsl 0/0/0` shows the DSL Link Idle.

**Solution:** Try the following:

- Ensure `show controller vdsl 0/0/0 local` shows Running FW = System FW. If not, upgrade FW and shut/no shut g0/0/0. Refer to **DSL SFP Firmware Upgrade**, on page 380
- Ensure carrier-set match (in controller vdsl 0/0/0) configuration with DSLAM
- Restart DSLAM interface if any config changes have been made
- Fine-tune the Power Spectrum Density, Freq Bandplan, profile, operating mode, vlan, etc... on the DSLAM end. On the Router DSL controller end, auto mode is the default and no configuration is required except possibly carrier-set. For example: If DSLAM only supports POTS, recommended to set carrier-set to a43. By default, Cisco allows a43, a43c, b43.
• Ensure the DSLAM profile ONLY includes supported Profiles, bands, etc as per VDSL2/ADSL2/2+. Refer to the tables in DSL Feature Specifications, on page 375.

• When using the service internal command test vdsl rawcli "basic show summary 1" consecutively, do you see the status move from Idle/Handshake/Training back to Idle, or stuck in Idle? If former case, recheck DSLAM profile configs. If latter, share L1 debug logs.

• If the DSLAM has the same configuration that used to work, and then after an image upgrade, or new SFP change the controller is UP but no negotiation, then please provide following to Cisco:
  • SFP LED status
  • Capture show version, show running-config, show run all | sec controller, show interface gigabitethernet 0/0/0, and show controller vdsl 0/0/0 local.

• Possible workaround: After providing logs to Cisco, attempt to write erase and reload the router. Also, shut/no shut the DSLAM interface tied to this device, and unplug/plug SFP and cables again.

**Problem:** If the controller is Up, but the daemon is Down.

**Solution:** Try the following:
- Enable debug vdsl for debug, share with Cisco TAC
- Provide last known working configs and software version
- Possible workaround: After providing logs to Cisco, attempt to write erase and reload the router. Also, shut/no shut the DSLAM interface tied to this device, and unplug/plug SFP and cables again.
- Check if the appropriate datak9, securityk9, and network-advantage licenses are enabled on both Peer and Client.

**Problem:** If Controller is up, profile with DSLAM up in show controller vdsl 0/0/0, but Dialer did not acquire IP

**Solution:** Try the following:
- Check routes
- Check the output of debug dialer to see if it offers any information. If dialer idle time is resetting too soon, modify dialer idle-timeout (default is 120s, which ideally should be enough).
  - Ensure there are SW Licenses (datak9, securityk9, and network-advantage) on both PPPoE server and the PPPoE Client/CPE.
  - The following is a basic Dialer configuration that works:

    ```
    interface Dialer1
    ip address negotiated
    no ip redirects
    encapsulation ppp
dialer pool 1
dialer-group 1
    ```
no cdp enable
ppp authentication chap callin
ppp chap hostname WORD
ppp chap password 0 WORD
ppp ipcp route default
ip route 0.0.0.0 0.0.0.0 Dialer1 (or any route that works in user environment)

• Ensure PPPoE Server authentication credentials match PPPoE client
• If using DHCP, ensure the Server has enough addresses to lease out
• Enable debug ppp session and debug ip dhcp server packet detail on the headend/Peer router to debug if we receive any packets. Enable debug ppp session on router.
• If the above steps did not resolve the issue, provide all of the above debug information to Cisco TAC, along with the following:
  • Output of show version, show running, show run all | sec controller, show controller vdsl 0/0/0 and show controller vdsl 0/0/0 local.
  • Output of service internal commands test vdsl rawcli "basic show summary 1", basic show summary 1, and test vdsl option 0x0 6.
  • Configuration of the DSLAM.
  • L1 training logs. Refer to L1 Training Logs, on page 404.

• Possible workaround: After gathering the above logs in sequence for Cisco, you can try to write erase and reload Peer and Router. Specifically removing the Dialer interface with PPP configurations and reapplying. As a last resort, try to shut/no shut DSLAM interface attached to this Router DSL SFP interface. Additionally, to isolate behavior, validate this SFP on another Router if available. If it works, then validate multiple SFPs on same Router (to narrow down if it is an SFP or Router issue).

Problem: If controller is Up, Dialer is Up, but Dialer did not acquire IP. Authentication works only with PAP and does not work with CHAP.

Solution: Suppose there is a scenario where:

show controller vdsl 0/0/0 shows showtime
show pppoe session shows PPP session established.

Then we see Virtual Access bound with Dialer successfully, but still Dialer didn't acquire an IP with PAP config in dialer all as well, but CHAP would not work On PPPoE Server end, it showed CHAP authentication passed and device ack too, but still IP not acquiring on PPPoE Client/device end.

debug ppp packet showed everything was okay, but still IP not acquiring. In such cases, enable following to monitor: debug ppp authentication enabled, we may notice that after successful chap handshake, there was another attempt by our device/client to validate based on local hostname set on Router CLI required to disable, if there is default local hostname set for chap in Router client (or any IOS router):

config t
service internal
Int Dialer1
no ppp chap ignoreus
**Problem** If controller is up, Dialer acquired an IP, but cannot self-ping Dialer or ping PPPoE Server

**Solution:** Try the following:

- Ensure the appropriate SW licenses (datak9, securityk9, and network-advantage) are enabled on both the PPPoe Server and Client
- Verify if icmp is enabled on PPPoE client session (enable via access list)
- Ensure pap/chap authentication match is seen in `debug pppoe session`
- `show pppoe session` should reflect session (virtual-access binding with Dialer)
- For PPPoE session debugging, this section is common to all IOS platforms: [https://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_0/configuration/guide/ir910scg/swpppoe.pdf](https://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_0/configuration/guide/ir910scg/swpppoe.pdf)
- Apply Static IP on g0/0/0 DSL interface and check if you can ping the DSLAM and Peer (to isolate DSL SFP issues)
- The following is a Basic PPPoE Server and PPPoE client configuration that works, presuming PPPoE Server is a Cisco IOS device as well:

  **PPPoE Server**

  ```
  ip dhcp excluded-address 41.41.41.1 41.41.41.9
  !
  ip dhcp pool 41-41-41-pool
  network 41.41.41.0 255.255.255.0
  default-router 41.41.41.1
  lease 2
  !
  username dslpeer password 0 dslpeerpass
  !
  bba-group pppoe global
  virtual-template 1
  !
  interface GigabitEthernet0/0/0
  no ip address
  media-type sfp
  !
  interface GigabitEthernet0/0/0.1
  encapsulation dot1Q 1 native
  ip address 41.41.41.1 255.255.255.255.0
  pppoe enable group global
  !
  interface Virtual-Template1
  ip unnumbered GigabitEthernet0/0/0.1
  peer default ip address dhcp-pool 41-41-41-pool
  ppp authentication pap chap
  !
  >>>>>> Add routes as relevant, next hop being the IP that Router Dialer acquires
  !
  ip route 10.0.0.0 255.255.255.0 41.41.41.3 >> dialer ip, change as necessary
  ```

PPPoE Client:
controller VDSL 0/0/0
Carrier-set a43 >>> Can set to whichever [a43, b43, a43c, v43 depending on DSLAM support]
interface GigabitEthernet0/0/0
no ip address
media-type sfp

interface GigabitEthernet0/0/0.1
encapsulation dot1Q 1 native
pppoe enable group global
pppoe-client dial-pool-number 1

interface Dialer1
ip address negotiated
no ip redirects
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname dslpeer
ppp chap password 0 dslpeerpass
ppp ipcp route default

ip route 0.0.0.0 0.0.0.0 Dialer1

Problem: If DSL traffic has been going through for a while, however bandwidth drops in time:

Solution: Try the following:

• Ensure DSLAM profile PSD, Freq band plan configurations are fine-tuned (in such cases, ideally unrelated to Router DSL SFP).

• Ensure ip arp timeout is increased in the Cisco Router DSL interface, Dialer interface - this may specially help in bursty traffic or during congestion.

Note: The following commands may be helpful for troubleshooting:

Interface Status:

Router# show ip interface brief
Use this command to validate if Dialer acquired an IP address

Inventory Status:

Router# show inventory

+---------------------------------------------------------------------------+
| INFO: Please use "show license UDI" to get serial number for licensing. | +---------------------------------------------------------------------------+
NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V03 , SN: FCW23500H5X

Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide

399
Commands to display the running software details:

Router# show running-config all
Router# dir flash:
Router# dir nvram:
Router# show version

There are some debugging commands that will also reflect the status of auto-negotiation:

Router# configure terminal
Router# service internal
Router# exit

The following test command will reflect auto-negotiation status:

Router# test vdsl rawcli "basic show summary 1"

<table>
<thead>
<tr>
<th>Link time</th>
<th>Rate US/DS Mode Status Annex TxPkts/RxPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1097/12491 ADSL2 Showtime AnnexA 0/0</td>
</tr>
</tbody>
</table>

Frequently Asked Questions

This section provides answers to some common questions.

**Question**: How can I set VDSL2 or ADSL2/2+ to a specific Annex and profile in Controller?

**Answer**: The Router DSL SFP operates in auto mode only. There are no options to configure on the SFP controller end. You can only make changes on the DSLAM side.

**Question**: There is no Controller ADSL option to configure.

**Answer**: Controller vdsl 0/0/0 is common nomenclature across Cisco IOS-XE products. The same cli is valid for ALL DSL protocols - VDSL2, ADSL2, ADSL2+.

**Question**: There is no ATM interface to configure.

**Answer**: There is no ATM interface for user configuration. On all configuration options on controller vdsl 0/0/0 and DSL SFP WAN interface g0/0/0 and its sub-interface options, ATM packets are handled by the DSL SFP and re-assembled as Ethernet packets. Annex A, L is supported.
**Question:** The training log in show controller vdsl 0/0/0 is not working. There is no option to start/stop.

**Answer:** This option is only specific to the c111x platform and not the Router DSL SFP. For Router platform L1 debugging, refer to: L1 Training Logs, on page 404

**Question:** Where can I download DSL SFP Firmware?

**Answer:**

In 17.5.1 and beyond, standalone FW is available to upgrade via Flash:, mSATA and usbflash0: in IOS To upgrade DSL Firmware, refer to: DSL SFP Firmware Upgrade, on page 380

**Question:** ADSL2 Annex L is not working.

**Answer:** Ensure the DSLAM profile configuration has the right bit rate allowed. Since the Router DSL SFP is auto-mode, it will negotiate with the profile with the highest bit rate (so this is predominantly determined by DSLAM config fine-tuning).

**Question:** Annex-L Mode1 is supported, but not Mode2.

**Answer:** Ensure that unsupported modes/profiles/bands in DSLAM configuration are disabled. Refer to DSL Feature Specifications, on page 375 for supported specifications.

**Question:** In ADSL2/2+ if burst size (peak cell rate and sustainable cell rate ) are configured to the maximum 5500, dialer keeps flapping.

**Answer:** If Dialer is flapping, could be receiving Peer upstream and was unable to handle high rate of downstream traffic. Either disable `ip keepalive` in dialer configuration, or increase default keepalive to the maximum.

**Question:** How many PVCs are allowed?

**Answer:** 8

**Question:** Controller configurations are not taking effect.
**Answer:** Ensure you exit out of controller configuration mode for the configuration to take effect. As a workaround, shut/no shut the controller interface. Ideally this should reflect the moment you 'exit' out of controller config mode. Check the DSLAM for matching profile criteria, unsupported bands/profiles should be removed as they may delay the Handshake.

**Question:** In ADSL2/2+ controller configuration, Maximum Burst Size configuration is not taking affect.
**Answer:** When configuring either nrt-VBR or rt-VBR, only the configuration of Peak Cell Rate (PCR) and Sustainable Cell Rate (SCR) are supported. The optional Maximum Burst Size (MBS) is not supported.

**Question:** System hangs during L1 Debug Logs capture, taking very long. show commands are not working.
**Answer:** When `debug vdsl controller 0/0/0 dump internal folder_name` is executed, it drains most of the system resources. A warning syslog to that effect is displayed as well. This takes approximately 10 minutes to complete depending on state of controller. Multiple times during the process the controller is shut/no shut, during this activity do NOT intervene. Once complete, you should observe 'DONE' in syslog and prompted to shut/no shut g0/0/0.

**Question:** Are there any new SNMP MIBS added?
**Answer:** Release 17.5.1 introduced the following ADSL2+ MIBS:
- 1.3.6.1.2.1.10.94.1.1.4.1.2 ADSL-LINE MIB:adslAtucChanCurrTxRate
- 1.3.6.1.2.1.10.94.1.1.5.1.2 ADSL-LINE MIB:adslAturChanCurrTxRate
- 1.3.6.1.2.1.10.94.1.1.2.1.8 ADSL-LINE MIB:adslAtucCurrAttainableRate
- 1.3.6.1.2.1.10.94.1.1.3.1.8 ADSL-LINE MIB:adslAturCurrAttainableRate

**Question:** SFP is stuck in the Router.
**Answer:** This can occur on older models of the IR1101. There was a faceplate rework.

Follow these steps to ensure the SFP Latch is handled cautiously (as with all SFPs). When doing a hot removal of SFP:
- Remove the latch (hear the click) and tilt to ~ 45deg - 90deg, without pressuring it or forcing it to snap.
- Remove the cable.
- Remove the SFP
When inserting the SFP, make sure you hear it lock in. Insert the cable and then close the latch. You should hear the click again. If you force the latch and it breaks, the SFP will be stuck in the Router. Workaround is to remove the faceplate and remove the SFP.

**Controller Status Messages**

This section explains some of the key output messages from the `show controller vdsl 0/0/0` command.

Refer to the following table:

<table>
<thead>
<tr>
<th>Output message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller VDSL 0/0/0 is UP</td>
<td>State of the controller</td>
</tr>
<tr>
<td>Daemon Status: UP</td>
<td>State of internal IOS DSL Daemon</td>
</tr>
<tr>
<td>Chip Vendor ID: 'META' 'BDCM'</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Chip Vendor Specific: 0x0000 0x0762</td>
<td>SFP Metanoia Chip Information burnt in EEPROM programming</td>
</tr>
<tr>
<td>Chip Vendor Country: 0xB500 0xB500</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Modem Vendor ID: 'META'</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Modem Vendor Specific: 0x0000 0x0000</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Modem Vendor Country: 0xB500 0x0000</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Serial Number Near: MET2023000A V5311TR 1_62_8463</td>
<td>SFP Metanoia Chip information</td>
</tr>
<tr>
<td>Serial Number Far:</td>
<td>SFP Metanoia Chip information, ignore if empty, Serial Number Near is the value required</td>
</tr>
<tr>
<td>Modem Version Near: 1_62_8463 MT5311.</td>
<td>Modem Firmware information</td>
</tr>
<tr>
<td>Modem Version Far: &lt;value&gt;</td>
<td>Ignore if empty, the above Near version is what is important</td>
</tr>
<tr>
<td>Modem Status: TC Sync (Showtime!)</td>
<td>Shows L1 SFP auto-negotiation status. When SFP is shut/no shut, you see following auto-negotiation sequence: Idle, Handshake, Training, Showtime! Showtime implies auto-neg complete</td>
</tr>
<tr>
<td>DSL Config Mode: AUTO</td>
<td>Always in AUTO mode, no specific CLI to configure for ADSL2/2+, VDSL2</td>
</tr>
<tr>
<td>Trained Mode: G.992.3 (ADSL2) Annex A</td>
<td>Specifies ITU and Annex type</td>
</tr>
</tbody>
</table>
### L1 Training Logs

To configure the device perform the following:

```bash
Router#configure terminal
Router#service internal
Router#logging console
Router#exit
```

To configure debug, perform the following:

```bash
Router#debug vdsl sfp debug | error | event | info | packet For SFP level debugging
Router#debug vdsl controller 0/0/0 dump internal {dir} For L1 debugging
```

When the L1 debug dump starts you should see the following:

```
$VDSL_SFP_MGR-5-DUMP_START: Dump internal info started on interface GigabitEthernet0/0/0
```

**Important**

At this point, the device is unusable. Wait approximately 10 minutes until it completes.

At that point you should see the following:

```
$VDSL_SFP_MGR-4-DUMP_DONE: Dump internal info done, please shut/no shut on interface GigabitEthernet0/0/0 to recover
```

To recover the device into normal operational mode, preform the following:

```bash
Router#configure terminal
Router#interface g0/0/0
Router#shut
Router#no shut
Router#exit
```

Provide directory logs saved in bootflash: to Cisco.

**Note**

Cisco recommends that each time you start a new log or debug, save it to a new directory rather than append to the existing information.

To enable Metanoia SFP debug commands, perform the following:

```bash
Router#configure terminal
Router#service internal
Router#exit
Router#test vdsl rawcli "basic show summary 1" This command shows the L1 auto-negotiation
```
status
Link time Rate US/DS Mode Status Annex TxPkts/RxPkts
773 1089/23628 ADSL2+ Showtime AnnexA 470/338

Router#test vdl option 6 0x0 If functional, State = 2 should display. This command shows basic L1 bringup of DSL SFP and it's states. Provide to Cisco for L1 troubleshooting.
Debug flags: 0x8000
Seq 0: slot=0 slot_port=0 bay=0 port=0 Name:MetaMgr0_0_0
MetanoiaPort=0 SFP type: 1 State: 2 cnt=855
MAC:00:00:00:00:00:00 Choice:0
hw interface:GigabitEthernet0/0/0 sw interface:GigabitEthernet0/0/0
Firmware file: /etc/SFP_V5311-T-R_CSP.b, size=491520, version=1_62_8463
SFP version: 1_62_8463
Notification Seq: 0x1 cnt: 0xB3 Stat Cycle:255
VDSL State: 5
EBM Tx: 21039 Rx: 21031
EBM Wait Timeout: 8 Rx Loss: 0
G994 vid CO: BDCM CPE: META
Serial No CO: CPE: MET2023000A V5311TR 1_62_8463
Version CO: CPE: 1_62_8463 MT5311
Capability CO: 0000000000100000 CPE: 0000000000100000
Line Attn: UP: 65535 DOWN: 13

Tips for resetting the SFP:

- Ideally g0/0/0 shut/no shut will work in most cases (for example: after firmware upgrade, hot OIR, etc).

For hard reload of SFP, perform the following:

Router#hw-module subslot 0/0 reload

This option will force the entire subslot to reload, including the software module. So if connectivity is via telnet/ssh you might lose access for 1-2 minutes, and then all messages/syslogs buffered will print out.
Out Of Band Management (OOB)

This chapter contains the following sections:

- Out Of Band Management (OOB), on page 407
- OOB Topology, on page 407
- Feature Caveats, on page 408
- OOB Configuration, on page 408

Out Of Band Management (OOB)

OOB offers a method for connecting two routers together with a USB cable for extra redundancy in case of 4G failure. This allows you to retain out-of-band connectivity by connecting the USB port for Router A to the USB console of Router B, as well as the ability to access Router B console port from Router A.

This feature will need to be implemented with IOS CLI. The user should be able to do a reverse telnet via tty line (/dev/ttyUSB) to another router's USB console.

OOB Topology

The following graphic illustrates the physical connection between two IR1101 routers:
Feature Caveats

Prior to configuring each router, ensure that both routers have a basic serial configuration:

```
line con 0
stopbits 1
speed 9600
```

Note

Depending on how old the IR1101 is, the default baud rate is 9600 or 115200.

- Plug and Play is not supported. Cable must be installed prior to configuration.
- OOB only works for async0/2/1, which is the USB port. Async0/2/0 is the serial interface on the IR1101
- To exit from the feature, press “Ctrl-Shift-6”, then “x”, then “disconnect”.

OOB Configuration

Refer to the previous figure for examples of Router A and Router B. To access Router B console from Router A:

Power on Router A and configure the following:

```
interface Async0/2/1
ip address 20.0.0.1 255.0.0.0
encapsulation relay-line
!
line 0/2/1
transport input all
transport output all
```
Make sure that the speed of line 51 is the same speed as the console on Router B:

IR1101-A# show line

<table>
<thead>
<tr>
<th>Try</th>
<th>Line</th>
<th>Typ</th>
<th>Tx/Rx</th>
<th>A Modem</th>
<th>Roty</th>
<th>AccO</th>
<th>AccI</th>
<th>Uses</th>
<th>Noise</th>
<th>Overruns</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>0</td>
<td>CTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/0/0</td>
<td>2</td>
<td>TTY</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/2/0</td>
<td>50</td>
<td>TTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>0/2/1</td>
<td>51</td>
<td>TTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>74</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>75</td>
<td>75</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>76</td>
<td>76</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>77</td>
<td>77</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>78</td>
<td>78</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>79</td>
<td>79</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>80</td>
<td>80</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>81</td>
<td>81</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>82</td>
<td>82</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>83</td>
<td>83</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>84</td>
<td>84</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>85</td>
<td>85</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>86</td>
<td>86</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>87</td>
<td>87</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>88</td>
<td>88</td>
<td>VTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Line(s) not in async mode -or- with no hardware support:
1, 3-49, 52-73, 89-735

Configure line 0/2/1 on Router A:

IR1101-A# configure term
Enter configuration commands, one per line. End with CNTL/Z.

IR1101-A(config)# line 0/2/1
IR1101-A(config-line)# speed 9600
IR1101-A(config-line)#

Telnet to Router B via Router A IP, port 2051:

IR1101-A# telnet 20.0.0.1 2051
Trying 20.0.0.1, 2051 ... Open

IR1101-B#

IR1101-B# <= to exit, press “Ctrl-Shift-6”, then “x”, then “disconnect”

IR1101-A# disconnect
Closing connection to 20.0.0.1 [confirm]
Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

- Monitoring Control Plane Resources, on page 411
- Monitoring Hardware Using Alarms, on page 416

Monitoring Control Plane Resources

The following sections explain the details of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

- Avoiding Problems Through Regular Monitoring, on page 411
- Cisco IOS Process Resources, on page 411
- Overall Control Plane Resources, on page 414

Avoiding Problems Through Regular Monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. It also establishes a baseline for a normal system load. You can use this information as a basis for comparison, when you upgrade hardware or software to see if the upgrade has affected resource usage.

Cisco IOS Process Resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the `show memory` command and the `show process cpu` command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do not include information for resources on the entire platform. When the `show memory` command is used in a system with 4 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

```
Router# show memory
Tracekey : 1#33e0077971693714bd2b0bc347d77489
```
### Processor memory

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>what Alloc</th>
<th>PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>7F68ECD010</td>
<td>0000000568</td>
<td>00000000</td>
<td>7F68ECD2A0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60E37C4</td>
<td>:400000+60D12A8</td>
</tr>
<tr>
<td>7F68ED5300</td>
<td>0000000056</td>
<td>7F68ECD2A0</td>
<td>7F68ED5390</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+3B0C610</td>
<td></td>
</tr>
<tr>
<td>7F68ED5390</td>
<td>00001280</td>
<td>7F68ED5300</td>
<td>7F68ED85F0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+B8A5D64</td>
<td></td>
</tr>
<tr>
<td>7F68ED85F0</td>
<td>000032776</td>
<td>7F68ED5390</td>
<td>7F68EE0650</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>List Elements</td>
<td>:400000+60AA49C</td>
</tr>
<tr>
<td>7F68EE0650</td>
<td>000032776</td>
<td>7F68ED85F0</td>
<td>7F68EE86B0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>IOSXE Process S</td>
<td>:400000+11924CC</td>
</tr>
<tr>
<td>7F68EE86B0</td>
<td>0000036872</td>
<td>7F68EE0650</td>
<td>7F68EE86F0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>IOSXE Queue Pro</td>
<td>:400000+1192510</td>
</tr>
<tr>
<td>7F68EE86F0</td>
<td>0000032776</td>
<td>7F68EE86B0</td>
<td>7F68EEF770</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>IOSXE Queue Bal</td>
<td>:400000+1192554</td>
</tr>
<tr>
<td>7F68EEF770</td>
<td>0000065544</td>
<td>7F68EE86F0</td>
<td>7F68EF07D0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Process Events</td>
<td>:400000+60F9CD4</td>
</tr>
<tr>
<td>7F68EF07D0</td>
<td>00000328</td>
<td>7F68EEF770</td>
<td>7F68F08970</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>SDB String :400000+605991C</td>
<td></td>
</tr>
<tr>
<td>7F68F08970</td>
<td>0000036872</td>
<td>7F68F08970</td>
<td>7F68F0B810</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Init :400000+60599E4</td>
<td></td>
</tr>
<tr>
<td>7F68F0B810</td>
<td>00000328</td>
<td>7F68F08970</td>
<td>7F68F0E70</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Process Events</td>
<td></td>
</tr>
<tr>
<td>7F68F0E70</td>
<td>0000032776</td>
<td>7F68F0B810</td>
<td>7F68F12008</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+11891E8</td>
<td>:400000+11AD244</td>
</tr>
<tr>
<td>7F68F12008</td>
<td>000010008</td>
<td>7F68F0E70</td>
<td>7F68F14778</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Platform VM Pag</td>
<td></td>
</tr>
<tr>
<td>7F68F14778</td>
<td>000002008</td>
<td>7F68F12008</td>
<td>7F68F14FA8</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em></td>
<td></td>
</tr>
<tr>
<td>7F68F14FA8</td>
<td>0000000056</td>
<td>7F68F14778</td>
<td>7F68F46008</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Interrupt Stack</td>
<td>:400000+11891E8</td>
</tr>
<tr>
<td>7F68F46008</td>
<td>000003008</td>
<td>7F68F14FA8</td>
<td>7F68F46C20</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Watched Semapho</td>
<td>:400000+60FE4A8</td>
</tr>
<tr>
<td>7F68F46C20</td>
<td>00000328</td>
<td>7F68F46008</td>
<td>7F68F46DC0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Process Array</td>
<td>:400000+60FE4D8</td>
</tr>
<tr>
<td>7F68F46DC0</td>
<td>0000000096</td>
<td>7F68F46C20</td>
<td>7F68F46E78</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Watched Message</td>
<td>:400000+60FE4D8</td>
</tr>
<tr>
<td>7F68F46E78</td>
<td>00000216</td>
<td>7F68F46DC0</td>
<td>7F68F46FA8</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Watched Message</td>
<td></td>
</tr>
<tr>
<td>7F68F46FA8</td>
<td>0000036872</td>
<td>7F68F46E78</td>
<td>7F68F50008</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+11891E8</td>
<td></td>
</tr>
<tr>
<td>7F68F50008</td>
<td>000002008</td>
<td>7F68F50008</td>
<td>7F68F50C10</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Watcher Message</td>
<td></td>
</tr>
<tr>
<td>7F68F50C10</td>
<td>0000000360</td>
<td>7F68F50008</td>
<td>7F68F50DD0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Process Events</td>
<td></td>
</tr>
<tr>
<td>7F68F50DD0</td>
<td>000000184</td>
<td>7F68F50C10</td>
<td>7F68F50EE0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60ED918</td>
<td>:400000+60F9CD4</td>
</tr>
<tr>
<td>7F68F50EE0</td>
<td>00000112</td>
<td>7F68F50DD0</td>
<td>7F68F50FA8</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60B57CC</td>
<td></td>
</tr>
<tr>
<td>7F68F50FA8</td>
<td>0000036872</td>
<td>7F68F50EE0</td>
<td>7F68F5A008</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+11891E8</td>
<td></td>
</tr>
<tr>
<td>7F68F5A008</td>
<td>000002336</td>
<td>7F68F50FA8</td>
<td>7F68F5A980</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>Process Array</td>
<td>:400000+60FE4A8</td>
</tr>
<tr>
<td>7F68F5A980</td>
<td>00000184</td>
<td>7F68F5A008</td>
<td>7F68F5A90</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60ED918</td>
<td></td>
</tr>
<tr>
<td>7F68F5A90</td>
<td>00000184</td>
<td>7F68F5A980</td>
<td>7F68F5ABA0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60ED918</td>
<td></td>
</tr>
<tr>
<td>7F68F5ABA0</td>
<td>00000184</td>
<td>7F68F5A90</td>
<td>7F68F5ACB0</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td><em>Init</em> :400000+60ED918</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide

### Cisco IOS Process Resources

**Process Health Monitoring**
The `show process cpu` command displays Cisco IOS CPU utilization average:

```
Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 0 0 0.00% 0.00% 0.00% 0 Chunk Manager
2 552 1205 458 0.00% 0.00% 0.00% 0 Load Meter
3 0 1 0.00% 0.00% 0.00% 0 PKI Trustpool
4 0 1 0.00% 0.00% 0.00% 0 Retransmission o
5 0 1 0.00% 0.00% 0.00% 0 IPC ISSU Dispact
6 36 13 2769 0.00% 0.00% 0.00% 0 RF Slave Main Th
7 0 1 0.00% 0.00% 0.00% 0 EDDRI_MAIN
8 0 1 0.00% 0.00% 0.00% 0 RO Notify Timers
9 4052 920 4404 0.23% 0.09% 0.06% 0 Check heaps
10 12 101 118 0.00% 0.00% 0.00% 0 Pool Manager
11 0 1 0.00% 0.00% 0.00% 0 DiscardQ Backgro
12 0 2 0.00% 0.00% 0.00% 0 Timers
13 0 163 0.00% 0.00% 0.00% 0 WATCH_AFS
14 0 2 0.00% 0.00% 0.00% 0 ATM AutoVC Perio
15 0 2 0.00% 0.00% 0.00% 0 ATM VC Auto Crea
16 76 3024 25 0.00% 0.00% 0.00% 0 IOSXE heartbeat
17 0 13 0.00% 0.00% 0.00% 0 DB Lock Manager
18 0 1 0.00% 0.00% 0.00% 0 DB Notification
19 0 1 0.00% 0.00% 0.00% 0 IPC Apps Task
20 0 101 0.00% 0.00% 0.00% 0 ifIndex Receive
21 36 1210 29 0.00% 0.00% 0.00% 0 IPC Event Notifi
22 72 5904 12 0.00% 0.00% 0.00% 0 IPC Mcast Pendin
23 0 1 0.00% 0.00% 0.00% 0 Platform appsess
24 0 101 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
25 16 1210 13 0.00% 0.00% 0.00% 0 IPC Service NonC
26 0 1 0.00% 0.00% 0.00% 0 IPC Zone Manager
27 64 5904 10 0.00% 0.00% 0.00% 0 IPC Periodic Tim
28 76 5904 12 0.00% 0.00% 0.00% 0 IPC Deferred Por
29 0 1 0.00% 0.00% 0.00% 0 IPC Process leve
30 0 1 0.00% 0.00% 0.00% 0 IPC Seat Manager
31 8 346 23 0.00% 0.00% 0.00% 0 IPC Check Queue
32 0 1 0.00% 0.00% 0.00% 0 IPC Seat RX Cont
33 0 1 0.00% 0.00% 0.00% 0 IPC Seat TX Cont
34 48 606 79 0.00% 0.00% 0.00% 0 IPC Keep Alive M
35 28 1210 23 0.00% 0.00% 0.00% 0 IPC Loadometer
36 0 1 0.00% 0.00% 0.00% 0 IPC Session Deta
37 0 1 0.00% 0.00% 0.00% 0 SENSOR-MGR event
38 4 606 6 0.00% 0.00% 0.00% 0 Compute SRP rate
39 0 1 0.00% 0.00% 0.00% 0 MEMLEAK PROCESS
40 0 1 0.00% 0.00% 0.00% 0 ARP Input
41 112 6331 17 0.00% 0.00% 0.00% 0 ARP Background
42 0 2 0.00% 0.00% 0.00% 0 ATM Idle Timer
43 0 1 0.00% 0.00% 0.00% 0 ATM ASYNC PROC
44 0 1 0.00% 0.00% 0.00% 0 CEF MIB API
```

CPU utilization for five seconds: 11%, one minute: 12%, five minutes: 12%
Core 0: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 1: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Overall Control Plane Resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the `show platform software status control-processor brief` command.
(summary view) or the `show platform software status control-processor` command (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational, but that the operating level should be reviewed. Critical implies that the router is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

The following sections describe the fields in the `show platform software status control-processor` command output.

**Load Average**

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

**Memory Utilization**

Memory utilization is represented by the following fields:

- **Total**—Total system memory
- **Used**—Consumed memory
- **Free**—Available memory
- **Committed**—Virtual memory committed to processes

**CPU Utilization**

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- **CPU**—Allocated processor
- **User**—Non-Linux kernel processes
- **System**—Linux kernel process
- **Nice**—Low-priority processes
- **Idle**—Percentage of time the CPU was inactive
- **IRQ**—Interrupts
- **SIRQ**—System Interrupts
- **IOWait**—Percentage of time CPU was waiting for I/O
Monitoring Hardware Using Alarms

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use show commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.
BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

Oct 6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded [free space is 1429020 kB] - Please clean up files on bootflash.

Approaches for Monitoring Hardware Alarms

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

Enabling the logging alarm Command

The `logging alarm` command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC4133 (required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)
Process Health Monitoring

Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP
Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a PC to the router via the console port. With a connected PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface by using Telnet. The Telnet option assumes that the interface is up and running.

- Understanding Diagnostic Mode, on page 419
- Before Contacting Cisco or Your Reseller, on page 420
- show interfaces Troubleshooting Command, on page 420
- Software Upgrade Methods, on page 420
- Change the Configuration Register, on page 421
- Recovering a Lost Password, on page 424

Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the transport-map command that directs the user into the diagnostic mode.
- A send break signal (Ctrl-C or Ctrl-Shift-6) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.
- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.
The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

show interfaces Troubleshooting Command

Use the `show interfaces` command to display the status of all physical ports and logical interfaces on the router. The IR1101 supports the following interfaces:

- GigabitEthernet 0/0/0
- Cellular 0/1/0
- FastEthernet 0/0/1 to 0/0/4
- Async 0/2/0

Software Upgrade Methods

Several methods are available for upgrading software on the Cisco IR1101 Routers, including:

- Copy the new software image to flash memory over LAN or WAN when the existing Cisco IOS software image is in use.
- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.
- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.
Change the Configuration Register

To change a configuration register, follow these steps:

**Step 1**
Connect a PC to the CONSOLE port on the router.

**Step 2**
At the privileged EXEC prompt, enter the `show version` command to display the existing configuration register value (shown in bold at the bottom of this output example):

**Example:**

```
Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 18:08 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

Router uptime is 14 hours, 36 minutes
Uptime for this control processor is 14 hours, 37 minutes
System returned to ROM by reload
System restarted at 08:47:04 GMT Mon Nov 12 2018
System image file is "bootflash:ir1101-universalk9.16.10.01.SPA.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

If you require further assistance please contact us by sending email to
export@cisco.com.

Technology Package License Information:
```
Step 3  Record the setting of the configuration register.

Step 4  To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the `config-register 0x01` command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

---

Configuring the Configuration Register for Autoboot

**Note**  Altering the configuration register is only for advanced troubleshooting and should only be done with guidance from Cisco support.

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the `config-reg 0x0` command.
- From the ROMMON prompt, use the `confreg 0x0` command.

**Note**  Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.
## Reset the Router

To reset the router, follow these steps:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (I) again. Within 60 seconds, press the <strong>Break</strong> key. The terminal displays the ROM monitor prompt.</td>
<td><strong>Note</strong> Some terminal keyboards have a key labeled <strong>Break</strong>. If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Press break. The terminal displays the following prompt:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>rommon 2&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter <strong>confreg 0x142</strong> to reset the configuration register:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>rommon 2&gt; <strong>confreg 0x142</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Initialize the router by entering the <strong>reset</strong> command:</td>
<td>The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>rommon 2&gt; <strong>reset</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>--- System Configuration Dialog ---</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enter <strong>no</strong> in response to the prompts until the following message is displayed:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Press RETURN to get started!</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Press <strong>Return</strong>. The following prompt appears:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:</td>
<td>The prompt changes to the privileged EXEC prompt:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; <strong>enable</strong></td>
<td></td>
</tr>
</tbody>
</table>
Recovering a Lost Password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value.
5. If you have performed a **write erase**, or used the reset button, you will need to add the license.

```
IR1101#config term
IR1101#license smart reservation
```

**Note**
Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

**Tip**
See the “Hot Tips” section on Cisco.com for additional information on replacing enable secret passwords.

Reset the Password and Save Your Changes

To reset your password and save the changes, follow these steps:

---

**Command or Action** | **Purpose**
--- | ---

**Step 8** Enter the `show startup-config` command to display an enable password in the configuration file:

**Example:**

```
Router# show startup-config
```

**What to do next**

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the `show startup-config` command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Enter the <code>configure terminal</code> command to enter global configuration mode:</td>
<td></td>
</tr>
<tr>
<td>Example: <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Enter the <code>enable secret</code> command to reset the enable secret password in the router:</td>
<td></td>
</tr>
<tr>
<td>Example: <code>Router(config)# enable secret password</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Enter <code>exit</code> to exit global configuration mode:</td>
<td></td>
</tr>
<tr>
<td>Example: <code>Router(config)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Save your configuration changes:</td>
<td></td>
</tr>
<tr>
<td>Example: <code>Router# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Password Recovery Disable

The No Service Password-Recovery is a Cisco IOS Platform independent feature/CLI which is available in Cisco IOS-XE devices. When the No Service Password-Recovery security feature is enabled, it prevents anyone with console access from using a break sequence (Control+C) during bootup to enter into rommon.

**Note**

Ensure a valid Cisco IOS image is present in flash before enabling this feature. Failure to do so will result in the router going into a boot loop. Hard power reset button is disabled if system has **no service password recovery**.

The following events will cause the router to go into rommon mode as standard IOS-XE behavior:

- config-reg setting is manual boot
- User opts to reset to factory default option

Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Enter the <code>configure terminal</code> command to enter global configuration mode:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Enter the <code>configure register</code> command and the original configuration register value that you recorded.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>config-reg value</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Enter <code>exit</code> to exit configuration mode:</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.</td>
</tr>
<tr>
<td>Router(config)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Reboot the router, and enter the recovered password.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>transport-map type console transport-map-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Creates and names a transport map for handling console connections, and enters transport map configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config)# transport-map type console consolehandler</td>
<td>Specifies how a console connection will be handled using this transport map.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>connection wait [allow [interruptible]</td>
<td>none [disconnect]]</td>
</tr>
<tr>
<td>Router(config-tmap)# connection wait none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) banner [diagnostic</td>
<td>wait] banner-message</td>
</tr>
<tr>
<td>Router(config-tmap)# banner diagnostic X</td>
<td>- Welcome to Diagnostic Mode--</td>
</tr>
<tr>
<td><a href="X">Enter TEXT message. End with the character 'X'.</a></td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>transport type console console-line-number input transport-map-name</td>
<td>Applies the settings defined in the transport map to the console interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# transport type console 0 input consolehandler</td>
<td>The transport-map-name for this command must match the transport-map-name defined in the transport-map type console command.</td>
</tr>
</tbody>
</table>
Examples
The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```bash
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- `show transport-map`
- `show platform software configuration access policy`

Use the `show transport-map` command to view transport map configurations.

```
show transport-map [all | name transport-map-name | type [console ]]
```

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: console port (consolehandler):

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport
Connection:
Wait option: Wait Allow Interruptable Wait banner:
Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type console
Transport Map:
Name: consolehandler
```

REVIEW DRAFT - CISCO CONFIDENTIAL
Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode

Use the show platform software configuration access policy command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the show transport-map command, the show platform software configuration access policy command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the show platform software configuration access policy command.

Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :

Using the factory reset Commands

The factory reset commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The factory-reset all command erases the bootflash, nvram, rommon variables, licenses, and logs.

Router# factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm] *Enter*
Using the factory reset Commands


***Return to ROMMON Prompt