



Cisco 910 Industrial Router Software Configuration Guide, Release 1.1

First Published: September 16, 2014

Last Updated: April 30, 2015

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax 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: www.cisco.com/go/trademarks. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



Preface

This document describes how to configure the Cisco 910 Industrial Router in your network.

This guide does not describe how to install the Cisco 910 Industrial Router. For information about how to install the Cisco 910 Industrial Router, see the hardware installation guide pertaining to your device.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Related Publications

- *Cisco 910 Industrial Router Hardware Installation Guide*
- *Release Notes for the Cisco 910 Industrial Router*
- *Mounting Kit Assembly Guide for the Cisco 910 Industrial Router*
- *Cisco 910 Industrial Router Quick Start Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



Overview

- [Cisco 910 Industrial Router Overview](#)
- [Powering On and Getting Started With the System](#)

Cisco 910 Industrial Router Overview

The Cisco 910 Industrial Router (IR910) belongs to the Cisco 900 Series Industrial Routers Family. IR910 is a gateway to connect an IP network and a wireless sensor network (WSN), offering an open platform on software and hardware. It can host partner application and sensor communication cards. IR910 is responsible for local WSN management, raw data collection, caching, processing, and forwarding to data centers in the cloud through a WAN IP interface.

With a modular and open-slot design, the Cisco IR910 provides a common gateway platform to quickly adapt to a variety of wireless sensor technologies for different use cases, with benefits including less development effort, quick time to market, and Cisco IP domain expertise. Offering a programmable environment and sufficient headroom of CPU horsepower, memory, and storage, the IR910 natively complies with Cisco Fog Computing architecture, executes distributed data processing at the edge of an IP network, and allows you to host partners' applications.

Features and Benefits

The Cisco 910 Industrial Router has the following features and benefits:

- Open slot for field-replaceable wireless sensor communication card adaptive to a variety of wireless sensor technologies.
- Programmable environment to allow hosting of partner applications.
- Sufficient headroom of compute and memory space to execute fog computing.
- Third-generation (3G) high-speed packet access plus (HSPA+) and Code Division Multiple Access (CDMA) Evolution-Data Optimized (EVDO), selective in single device (IR910G-K9 and IR910G-NA-K9 only).
- Pluggable 16-GB SSD for volume data storage.
- Smooth integration with ecosystem partners to build smart parking, smart metering, and other E2E solution for customer.
- Support for centralized device management.

Ease-of-Deployment and Ease-of-Use Features

- Express Setup for quickly configuring a router for the first time with basic network settings and SSH settings. For more information about Express Setup, see the [“Configuring Express Settings” section on page -9](#).
- An embedded device manager GUI for configuring and monitoring a single router through a web browser. For more information about the device manager, see [Chapter 21, “Using Device Manager”](#).

Powering On and Getting Started With the System

These sections describe how you power on the device and get started with the system:

- [Powering On the Device](#)
- [Connecting a PC or a Terminal to the Console Port](#)
- [Enabling Secret](#)
- [Configuring IPv4 Address on GE Port](#)
- [Enabling SSH Service](#)
- [Enabling SSH Service Port](#)
- [Enabling Web Admin](#)
- [Saving the Configuration](#)
- [Upgrading the Firmware](#)
- [Installing the Patch](#)

For detailed information on the configuration of the router, see the other chapters in this book.

Powering On the Device

The Cisco 910 Industrial Router support dual DC power inputs. The voltage range shall be 12 VDC to 24 VDC. When the device is installed in the environment requiring AC inputs, use the optional AC power adapter.

Connect one exit of the power to the shielded contact located in the upper right corner of the device, and the other exit to an electrical outlet. It takes about 60 seconds for the system to finish the first time booting up. The SYS LED on the left upper corner shows the system status:

- If the LED is off, it indicates that the bootloader is initializing hardware.
- If the LED is blinking, it indicates that the system is booting;
- If the LED is solid green, it indicates that the system is running;

Connecting a PC or a Terminal to the Console Port

You can access the command line interface (CLI) by connecting the console port to your PC or workstation and accessing the router through a terminal emulation program.

To connect a PC to the console port, use an RJ-45-to-DB-9 adapter cable. To connect a terminal to the console port, you need to provide an RJ-45-to-DB-25 female DTE adapter.

The PC or terminal must support VT100 terminal emulation. The terminal-emulation software—frequently a PC application such as HyperTerminal or Procomm Plus—makes communication between the router and your PC or terminal possible.

Follow these steps to connect the PC or terminal to the router:

1. Using an RJ-45-to-DB-9 adapter cable, insert the RJ-45 connector into the console port on the router front panel and connect the other exit to the PC or terminal port.
2. Start the terminal-emulation program on the PC or terminal.
3. Configure the baud rate and data format of the PC or terminal to match these console-port default characteristics:

- 115200 bits per second
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

After you get access to the router, you can change the port baud rate. See the router software configuration guide for instructions.

4. Connect the power of the router. The PC or terminal displays the bootloader sequence.
5. Press **Enter** to display the setup prompt of the command line interface (CLI) as following:

```
Router>
```

Enabling Secret

When you first use the device, there is no enable secret set. You can use the **enable** command to enter the privileged EXEC mode. However, this is not safe. You are recommended to set a secret before deployment. Moreover, you will not be allowed to enter privileged EXEC mode if enable secret is not set when connecting via SSH. To set the secret, use the following commands:

```
Router> enable
Router# configure terminal
Router(config)# enable secret MYSECRET
Router(config)# exit
```

Configuring IPv4 Address on GE Port

Before using any network service, you have to configure an IP address for the device. There are many network interfaces can be configured with IP address. This section only describes how to configure the IPv4 address to the Gigabit Ethernet (GE) port. In the factory default setting, VLAN 1 is already created and the GE port is added to VLAN 1.

To configure a dynamic IPv4 address:

```
Router(config)# interface vlan 1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

To configure a static IPv4 address:

```
Router(config)# interface vlan 1
Router(config-if)# ip address a.b.c.d netmask
Router(config-if)# exit
```

After the configuration, you can use ping command to verify the network is reachable:

```
Router(config)# ping ip x.x.x.x
```

Enabling SSH Service

The device has full SSH protocol support. In addition to the SSH service, the SFTP server and SCP command are also shipped with the firmware.

To enable the SSH service:

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

To disable the SSH service:

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

You can add accounts with the **username** command:

```
Router(config)# username USERNAME password PASSWORD
```

Enabling SSH Service Port

The Default port of SSH service is 22. To enable other SSH port:

```
Router (config)# ip ssh port  
    <1-65535> Service port number of SSH sessions
```

Enabling Web Admin

If you want to configure the device with a web admin interface, you can enable the HTTP service.

To enable the HTTP service:

```
Router(config)# ip http server
```

To enable the HTTPS service:

```
Router(config)# ip http secure-server
```

To enable the HTTP authentication:

```
Router(config)# ip http authentication local
```

Saving the Configuration

All configurations you have made in the previous sections only reside in memory. They have not been saved to the persistent storage and the configurations will be lost after next reboot.

To save the configurations you have made:

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

To restart the system: (If you haven't saved the configuration, it will prompt you)

```
Router# reload  
Running configuration has not been saved, save it now?[y/n] y  
Proceed with reload?[y/n] n  
Router#
```

Upgrading the Firmware

The firmware is distributed as a zip file which includes the kernel and root file system. There are several ways to upgrade the firmware:

- [Upgrading from TFTP Server](#)
- [Upgrading from FTP Server](#)
- [Upgrading from USB Disk](#)

Upgrading from TFTP Server

Follow these steps to upgrade the firmware from a TFTP server:

1. Install the TFTP server on another machine, make sure that
 - The machine is network reachable to the device.
 - You have put the firmware under the TFTP root directory.
2. Use the following command to upgrade the firmware:

```
Router# archive download-sw tftp://ip/firmware_XX.zip
```

Replace the ip with machine real ip address and firmware_XX.zip with real firmware name.

Upgrading from FTP Server

Follow these steps to upgrade the firmware from an FTP server:

1. Install the FTP server on another machine, make sure that
 - The machine is network reachable to the device.
 - You have put the firmware under the FTP root directory.
2. Use the following command to upgrade the firmware:

```
Router# archive download-sw ftp://user:pass@ip/firmware_XX.zip
```

Replace the user and pass with your real FTP username and password. Replace the ip with machine real ip address and firmware_XX.zip with real firmware name.

Upgrading from USB Disk

Follow these steps to upgrade the firmware from a USB disk:

1. Copy the firmware to the first partition of the USB disk, following these guidelines:
 - The partition should have been formatted in FAT/ext2/ext3/ext4. Other file system types are not supported.
 - You MUST copy the firmware to the first partition. For example, if you insert the USB disk to a PC and the device is recognized as /dev/sdb, you must copy the firmware to /dev/sdb1 partition.
2. Connect the USB disk to the router. You can view the contents from CLI to assure you have correctly prepared the USB disk:

```
Router# dir usb0:/
```

3. Use the following command to upgrade from the USB disk:

```
Router# archive download-sw usb0:/firmware_XX.zip
```

where firmware_XX.zip is the firmware name.

Installing the Patch

You can install a patch to the system by CLI or Linux shell.

From CLI:

```
Router# patch install
  /reload      Reload system (if no unsaved config changes) after successful sw upgrade
  /force-reload Unconditionally reload system after successful sw upgrade
  path         Get from remote or local address
```

From Linux shell:

```
# sh IR910_openssl-security_1.0.patch
```

Use the following commands to verify the patch information:

```
Router# show patch installed
Router# show patch info IR910_openssl-security_1.0.patch
```



Using the Command-Line Interface

This chapter describes the command-line interface (CLI) and how to use it to configure your Cisco 910 Industrial Router (*hereafter* referred to as the router).

It contains these sections:

- [Understanding Command Modes, page 1](#)
- [Understanding the Help System, page 2](#)
- [Understanding Abbreviated Commands, page 3](#)
- [Understanding No Forms of Commands, page 3](#)
- [Understanding CLI Error Messages, page 4](#)
- [Using Command History, page 4](#)
- [Using Command History, page 4](#)
- [Editing Commands through Keystrokes, page 5](#)
- [Searching and Filtering Output of show logging Commands, page 5](#)
- [Accessing the CLI, page 6](#)

Understanding Command Modes

The command line interface of the router is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the router, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status. The user EXEC commands are not saved when the router reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the router reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *router*.

Table 1 **Command Mode Summary**

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your router.	Router>	Enter exit .	Use this mode to ■ Change terminal settings. ■ Perform basic tests. ■ Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Router#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Router(config)#	To exit to privileged EXEC mode, enter exit or exit , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire router.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Router(config-if)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter exit .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line console command.	Router(config-line)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter exit .	Use this mode to configure parameters for the terminal line.

Understanding the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in [Table 2](#).

Table 2 Help Summary

Command	Purpose
help	Obtain a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Obtain a list of commands that begin with a particular character string. For example: Router# di? dir disable disconnect
<i>abbreviated-command-entry<Tab></i>	Complete a partial command name. For example: Router# sh st <tab> router# show startup-config
?	List all commands available for a particular command mode. For example: Router> ?
<i>command ?</i>	List the associated keywords for a command. For example: Router> show ?
<i>command keyword ?</i>	List the associated arguments for a keyword. For example: Router(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet

Understanding Abbreviated Commands

You need to enter only enough characters for the router to recognize the command as unique.

This example shows how to enter the **show startup-config** privileged EXEC command in an abbreviated form:

```
Router# show st
```

Understanding No Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Understanding CLI Error Messages

[Table 3](#) lists some error messages that you might encounter while using the CLI to configure your router.

Table 3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% The command is not completed.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Illegal parameter.	You entered the command incorrectly.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Using Command History

The software provides a record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in [Table 4](#). These actions are optional.

Table 4 Recalling Commands

Action ¹	Result
Press the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press the down arrow key.	Return to more recent commands in the history buffer after recalling commands with the up arrow key. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Commands through Keystrokes

Table 5 shows the keystrokes that you need to edit command lines. These keystrokes are optional.

Table 5 Editing Commands through Keystrokes

Capability	Keystroke ¹	Purpose
Move around the command line to make changes or corrections.	Press the left arrow key.	Move the cursor back one character.
	Press the right arrow key.	Move the cursor forward one character.
	Press Ctrl-A .	Move the cursor to the beginning of the command line.
	Press Ctrl-E .	Move the cursor to the exit of the command line.
Delete entries if you make a mistake or change your mind.	Press the Delete or Backspace key.	Erase the character to the left of the cursor.
	Press Ctrl-D .	Delete the character at the cursor.
	Press Ctrl-K .	Delete all characters from the cursor to the exit of the command line.
	Press Ctrl-U .	Delete all characters from the cursor to the beginning of the command line.
	Press Ctrl-W .	Delete the word to the left of the cursor.
Scroll down a line or screen on displays that are longer than the terminal screen can display. Note: The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.	Press the Return key or Space bar.	Scroll down one screen.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Searching and Filtering Output of show logging Commands

You can search and filter the output for **show logging** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

To use this functionality, enter a **show logging** command followed by the *pipe* character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

```
show logging | {begin | include | exclude} regular-expression
```

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Router# show logging | include protocol
```

Accessing the CLI

You can access the CLI through a console connection, through SSH, or by using the browser.

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or PC to the router console port and power on the router, as described in the getting started guide that shipped with your router. Then, to understand the boot process and the options available for assigning IP information, see [Chapter 4, “Assigning IP Address and Domain Name Server.”](#)

You can use one of these methods to establish a connection with the router:

- Connect the router console port to a management station or dial-up modem. For information about connecting to the console port, see the router quick start guide or hardware installation guide.
- Use any encrypted Secure Shell (SSH) package from a remote management station. The router must have network connectivity with the SSH client, and the router must have an enable secret password configured.

For information about configuring the router for SSH, see the [“Configuring the Router for Secure Shell”](#) section on [page -7](#).

After you connect through the console port or through an SSH session, the user EXEC prompt appears on the management station.



Configuring the Router Alarms

This chapter describes how to configure alarms for the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

- [Understanding Router Alarms, page 1](#)
- [Configuring Router Alarms, page 2](#)
- [Displaying Router Alarms Status, page 5](#)

For complete syntax and usage information for the commands used in this chapter, see the router command reference for this release.

Understanding Router Alarms

The router software monitors router conditions on a per port or a router basis. If the conditions present on the router or a port do not match the set parameters, the router software triggers an alarm or a system message. By default, the router software sends the system messages to a system message logging facility, or a *syslog* facility. You can also configure the router to send Simple Network Management Protocol (SNMP) traps to an SNMP server. For more information on how to configure the alarms, see the [“Configuring Router Alarms” section on page -2](#).

- [Global Status Monitoring Alarms, page 1](#)
- [Triggering Alarm Options, page 2](#)

Global Status Monitoring Alarms

The router processes alarms related to temperature and power supply conditions, referred to as global or facility alarms.

Table 6 Global Status Monitoring Alarms

Alarm	Description
Power supply alarm	The router monitors dual power supply levels. If there are two power supplies installed in the router, an alarm triggers if a power supply fails. The alarm is automatically cleared when both power supplies are working. For more information, see the “Configuring the Power Supply Alarms” section on page -2 .
Temperature alarms	The router contains two temperature sensors that monitor the environmental conditions inside the router. ■ The primary alarm is enabled automatically to trigger both at a low temperature, -4° F (-20° C) and a high temperature, 203° F (95° C). It cannot be disabled. ■ The secondary alarm triggers when the system temperature is higher or lower than the configured high and low temperature thresholds. The secondary alarm is disabled by default. For more information, see the “Configuring the Router Temperature Alarms” section on page -3.

Triggering Alarm Options

The router supports these methods for triggering alarms:

- **SNMP Traps**

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB).

The **snmp-server enable traps** command can be changed so that the user can send alarm traps to an SNMP server. You can use alarm profiles to set environmental or port status alarm conditions to send SNMP alarm traps. See the [“Enabling SNMP Traps” section on page -5](#) for more information.

- **Syslog Messages**

You can use alarm profiles to send system messages to a syslog server. See the [“Configuring Router Alarms” section on page -2](#) for more information.

Configuring Router Alarms

- [Default Router Alarm Configuration, page 2](#)
- [Configuring the Power Supply Alarms, page 2](#)
- [Configuring the Router Temperature Alarms, page 3](#)
- [Enabling SNMP Traps, page 5](#)

Default Router Alarm Configuration

Table 7 Default Router Alarm Configuration

Alarm	Default Setting
Power supply alarm	Enabled in router single power mode. No alarm. In dual-power supply mode, the default alarm notification is a system message to the console.
Primary temperature alarm	Enabled for router temperature range of 203°F (95°C) maximum to -4° F (-20°C) minimum.
Secondary temperature alarm	Disabled.

Configuring the Power Supply Alarms

The presence of power supplies is dynamically detected.

Use the **alarm facility power-supply** global configuration command to configure all alarms and traps associated with the power supply alarm to be sent to an SNMP server or to the rmon event log table.

Beginning in privileged EXEC mode, follow these steps to configure the power supply alarms:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	alarm facility power-supply notifies	send power supply alarm traps to an SNMP server.
3.	alarm facility power-supply snmplog	send power supply alarm log to the rmon event log table.
4.	exit	Return to privileged EXEC mode.
5.	show alarm settings	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable sending the power supply alarm to an SNMP server or to rmon event log table, use the **no alarm facility power-supply notifies**, or **no alarm facility power-supply snmplog** global configuration commands.

Before you can use the **notifies** command to send alarm traps to an SNMP server, you must first set up the SNMP server by using the **snmp-server enable traps** global configuration command. See the [“Enabling SNMP Traps” section on page -5](#).

Configuring the Router Temperature Alarms

You can change the temperature thresholds for both the primary and secondary temperature alarms.

- [Setting the Primary Temperature Threshold for the Router, page 3](#)
- [Setting a Secondary Temperature Threshold for the Router, page 4](#)
- [Associating the Temperature Alarms, page 4](#)

Setting the Primary Temperature Threshold for the Router

You can use the **alarm facility temperature primary** global configuration command to set low and high temperature thresholds for the primary temperature monitoring alarm.

Beginning in privileged EXEC mode, follow these steps to set the high temperature threshold:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	alarm facility temperature primary high threshold	Set the primary high temperature threshold value.
3.	alarm facility temperature primary low threshold	Set the primary low temperature threshold value.
4.	exit	Return to privileged EXEC mode.
5.	show alarm settings	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no alarm facility temperature primary high threshold** global configuration command to delete the temperature monitoring alarm configuration and return to the default setting.

This example shows how to delete the primary temperature monitoring alarm configuration and return to the default setting.

```
router(config) # no alarm facility temperature primary high 45
```

Setting a Secondary Temperature Threshold for the Router

You can use the **alarm facility temperature secondary** global configuration command to set the low and high temperature thresholds for the secondary temperature monitoring alarm.

Beginning in privileged EXEC mode, follow these steps to set the low temperature threshold:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	alarm facility temperature secondary high threshold	Set the secondary high temperature threshold value.
3.	alarm facility temperature secondary low threshold	Set the secondary low temperature threshold value.
4.	exit	Return to privileged EXEC mode.
5.	show alarm settings	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no alarm facility temperature secondary threshold** global configuration command to disable the secondary temperature threshold alarm.

This example disables the secondary temperature threshold alarm.

```
router(config) # no alarm facility temperature secondary 45
```

Associating the Temperature Alarms

You can use the **alarm facility temperature** global configuration command to associate the primary or secondary temperature alarm to an SNMP server, or the rmon event log table.

Beginning in privileged EXEC mode, follow these steps to associate the primary or secondary temperature alarms:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	alarm facility temperature {primary secondary} notifies	send primary or secondary temperature alarm traps to an SNMP server.
3.	alarm facility temperature {primary secondary} snmplog	send primary or secondary temperature alarm traps to the rmon event log table.
4.	exit	Return to privileged EXEC mode.
5.	show alarm settings	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Before you use the **notifies** command to send alarm traps to an SNMP server, you must first set up the SNMP server by using the **snmp-server enable traps** global configuration command. See the [“Enabling SNMP Traps” section on page -5](#).

Use the **no alarm facility temperature secondary** to disable the secondary temperature alarm.

This example sets the secondary temperature alarm with a high temperature threshold value of 113°F (45°C). All alarms and traps associated with this alarm are sent to a syslog server and an SNMP server.

```
router(config) # alarm facility temperature secondary high 45
router(config) # alarm facility temperature secondary snmplog
router(config) # alarm facility temperature secondary notifies
```

This example sets the first (primary) temperature alarm. All alarms and traps associated with this alarm are sent to a syslog server.

```
router(config) # alarm facility temperature primary snmplog
```

Enabling SNMP Traps

Use the **snmp-server enable traps** global configuration command to enable the router to send SNMP traps.

Before using alarm profiles to set the router to send SNMP alarm trap notifications to an SNMP server, you must first enable SNMP by using the **snmp-server enable traps** global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable the router to send *alarm* traps:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	snmp-server enable traps	Enable the router to send SNMP traps and specify the type of notifications to be sent. Default selects all snmp notification type..
3.	exit	Return to privileged EXEC mode.
4.	show alarm settings	Verify the configuration.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Displaying Router Alarms Status

To display the global and port alarm status, use one or more of the privileged EXEC commands in [Table 8](#):

Table 8 **Commands for Displaying Global and Port Alarm Status**

Command	Purpose
show alarm settings	Displays all global alarm settings on the router.



Assigning IP Address and Domain Name Server

This chapter describes how to create the initial router configuration (for example, assigning the IP address and default gateway information) for the Cisco 910 Industrial Routers (*hereafter* referred to as the router) by using a variety of automatic and manual methods.

This chapter consists of these sections:

- [Understanding the Boot Process, page 1](#)
- [Assigning Router Information, page 2](#)
- [Checking and Saving the Running Configuration, page 4](#)
- [Reload of the Software Image, page 4](#)

Information in this chapter about configuring IP addresses and DHCP is specific to IP Version 4 (IPv4). If you plan to enable IP Version 6 (IPv6) forwarding on your router, see [Chapter 15, “Configuring IPv6”](#) for information specific to IPv6 address format and configuration.

Understanding the Boot Process

To start your router, you need to follow the procedures in the Quick Start Guide or the hardware installation guide for installing and powering on the router and for setting up the initial router configuration (IP address, subnet mask, secret and Telnet passwords, and so forth).

The normal boot process involves the operation of the boot loader software, which performs these activities:

- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem. It tests the CPU DRAM and the portion of the flash device that makes up the flash file system.
- Initializes the compact flash file system on the system board.
- Loads a default operating system software image into memory and boots up the router.

The boot loader provides access to the flash file system before the operating system is loaded. Normally, the boot loader is used only to load, uncompress, and launch the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

Before you can assign router information, make sure you have connected a PC or terminal to the console port, and configured the PC or terminal-emulation software baud rate and character format to match these of the router console port:

- Baud rate default is 115200.
- Data bits default is 8.

Note: If the data bits option is set to 8, set the parity option to none.

- Stop bits default is 1.
- Parity settings default is none.

Assigning Router Information

You can assign IP information through a DHCP server or manually.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

These sections contain this configuration information:

- [Understanding DHCP, page 2](#)
- [Manually Assigning IP Information, page 4](#)

Understanding DHCP

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

DHCP client support is enabled on a per interface basis on the router for automatic IPv4 address assignment.

The DHCP server, which supplies the IP addresses to the router interfaces, does not need to be on the same subnet as the router. However, when the DHCP server and the router are on different subnets, DHCP relay must be active in the network. Generally, DHCP relay is configured on a router in the path between the router and the DHCP server.

Configuring DHCP

This section includes the following topics:

- [Enabling DHCP on Interfaces, page 2](#)
- [Configuring the DNS, page 3](#)

Enabling DHCP on Interfaces

To assign IP address by negotiation via DHCP, use the **ip address dhcp** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to enable DHCP on interfaces:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface_type</i> <i>interface_number</i>	Enter interface configuration mode.
3.	ip address dhcp	Enable DHCP client on the interface to allow automatic assignment of IP addresses to the specified interface.
4.	exit	Return to global configuration mode.
5.	show interfaces <i>interface_type</i> <i>interface_number</i>	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the DNS

This section includes the following topics:

- [DNS Client, page 3](#)
- [Name Servers, page 3](#)
- [DNS Operation, page 3](#)

DNS Client

When your network devices require connectivity with devices in networks for which you do not control the name assignment, you can assign device names that uniquely identify your devices within the entire internetwork using the domain name server (DNS). DNS uses a hierarchical scheme for establishing host names for network nodes, which allows local control of the segments of the network through a client-server scheme. The DNS system can locate a network device by translating the hostname of the device into its associated IP address.

On the Internet, a domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on the organization type or geography. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the Internet identifies by a com domain, so its domain name is cisco.com. A specific hostname in this domain, the File Transfer Protocol (FTP) system, for example, is identified as ftp.cisco.com.

Name Servers

Name servers keep track of domain names and know the parts of the domain tree for which they have complete information. A name server might also store information about other parts of the domain tree. To map domain names to IP addresses on the router, you must identify the hostnames, specify a name server, and enable the DNS service.

You can configure the router to use one or more domain name servers to find an IP address for a host name.

DNS Operation

A name server handles client-issued queries to the DNS server for locally defined hosts within a particular zone as follows:

An authoritative name server responds to DNS user queries for a domain name that is under its zone of authority by using the permanent and cached entries in its own host table. When the query is for a domain name that is under its zone of authority but for which it does not have any configuration information, the authoritative name server replies that no such information exists.

A name server that is not configured as the authoritative name server responds to DNS user queries by using information that it has cached from previously received query responses.

Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to multiple interfaces:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface vlan <i>vlan-id</i>	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The VLAN range is 1 to 4094.
3.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.
4.	exit	Return to global configuration mode.
5.	show interfaces vlan <i>vlan-id</i>	Verify the configured IP address.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the router IP address, use the **no ip address** interface configuration command. If you are removing the address through a Telnet session, your connection to the router will be lost.

For information on setting the router system name, protecting access to privileged EXEC commands, and setting time and calendar services, see [Chapter 5, “Administering the Router.”](#)

Checking and Saving the Running Configuration

You can check the configuration settings that you entered or changes that you made by entering this privileged EXEC command:

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

To store the configuration or changes you have made to your startup configuration in flash memory, enter this privileged EXEC command:

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

This command saves the configuration settings that you made. If you fail to do this, your configuration will be lost the next time you reload the system. To display information stored in the NVRAM section of flash memory, use the **show startup-config** privileged EXEC command.

Reload of the Software Image

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself. Use the **reload** command after you save the router configuration information to the startup configuration (**copy running-config startup-config**).

If your router is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the router from entering the boot loader mode and thereby taking it from the remote user’s control.

If you modify your configuration file, the router prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.



Administering the Router

This chapter describes how to perform one-time operations to administer the Cisco 910 Industrial Routers (*hereafter* referred to as the router). This chapter consists of these sections:

- [Managing the System Time and Date, page 1](#)
- [Configuring a System Name and Prompt, page 6](#)
- [Managing the MAC Address Table, page 9](#)

Managing the System Time and Date

You can manage the system time and date on your router using automatic configuration, such as the Network Time Protocol (NTP), or manual configuration methods.

These sections contain the following configuration information:

- [Understanding the System Clock, page 1](#)
- [Understanding Network Time Protocol, page 2](#)
- [NTP Version 4, page 2](#)
- [Configuring NTP, page 3](#)
- [Configuring Time and Date Manually, page 4](#)

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone so that the time appears correctly for the local time zone.

For configuration information, see the [“Configuring Time and Date Manually” section on page -4](#).

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Version 4

NTP version 4 is implemented on the router. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

Configuring NTP

These sections contain this configuration information:

- [Configuring NTP Server, page 3](#)
- [Configuring NTP Authentication, page 3](#)

Configuring NTP Server

This section describes how to configure the router to be synchronized by a time server.

Beginning in privileged EXEC mode, follow these steps to configure the NTP server:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ntp server {[ip ipv6 address] hostname} [prefer] [key keyid] [maxpoll number] [minpoll number] [burst] [iburst]	Defines the NTP server that provides the clocking source for the router. You can specify multiple server associations. ■ key— Configures a key to use while communicating with the NTP server. The range for the key-id argument is from 1 to 65534. Note: Only configure the key when you want the NTP server to provide authentication for the router. maxpoll, minpoll—Configures the maximum and minimum intervals in which to poll a server. The range for the max-poll and min-poll arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively. prefer —Assigns the NTP server as the preferred NTP server for the router. Note: When you configure a key for use in communicating with the NTP server, be sure that the key exists as a trusted key on the router. For more information on trusted keys, see the “Configuring NTP Authentication” section on page -3.
3.	exit	Return to privileged EXEC mode.
4.	show ntp status	(Optional) Show NTP status to verify the configuration.
5.	show ntp associations	(Optional) Show the NTP associations with upstream servers.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable the NTP service, use the **no ntp server** *hostname* global configuration command.

Configuring NTP Authentication

You can configure the router to authenticate the time sources to which the local clock synchronizes. When you enable NTP authentication, the router synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The router drops any packets that fail the authentication check and prevents them from updating the local clock.

By default, NTP authentication is disabled on the router.

This section describes how to configure NTP server(s) with the authentication keys configured on the router.

Beginning in privileged EXEC mode, follow these steps to configure NTP authentication:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ntp authentication-key <i>number</i> md5 <i>key</i>	Defines the authentication key. This key must match the value on the NTP server along with the ntp trusted-key <i>number</i> value of the router in 3. below. The router does not synchronize to the NTP server clocking source unless the ntp authentication-key and the ntp trusted-key values on the server and the router match. The range for authentication keys is from 1 to 65534. For the MD5 string, you can enter up to 16 alphanumeric characters.
3.	ntp trusted-key <i>number</i>	Specifies one or more keys (defined in 2.) that a time source (NTP server) must provide in its NTP packets in order for the router to synchronize to it. The range for trusted keys is from 1 to 65534. This command provides protection against accidentally synchronizing the router to a time source (NTP server) that is not trusted.
4.	exit	Return to privileged EXEC mode.
5.	show ntp status	(Optional) Show NTP status to verify the configuration.
6.	show ntp associations	(Optional) Show the NTP associations with upstream servers.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the authentication key for NTP, use the **no ntp authentication-key *number*** global configuration command.

To disable the authentication of the identity of the system, use the **ntp trusted-key *number*** global configuration command.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the router can synchronize, you do not need to manually set the system clock.

These sections contain this configuration information:

- [Setting the System Clock, page 5](#)
- [Displaying the Time and Date Configuration, page 5](#)
- [Configuring the Time Zone, page 6](#)

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
1.	clock set <i>hh:mm:ss month day year</i>	Manually set the system clock using one of these formats. ■ For <i>hh:mm:ss</i>, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. ■ For <i>day</i>, specify the day by date in the month. ■ For <i>month</i>, specify the month by name. ■ For <i>year</i>, specify the year (no abbreviation).

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
Router# clock set 13:32:00 July 23 2001
```

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock** privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *-Time is not authoritative.
- (blank)-Time is authoritative.
- .-Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	clock timezone <i>zone</i>	Set the time zone. The router keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. ■ For <i>zone</i> , enter the name of the time zone to be displayed when standard time is in effect. The default is UTC.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To set the time to UTC, use the **no clock timezone** global configuration command.

Configuring a System Name and Prompt

You configure the system name on the router to identify it. By default, the system name and prompt are *Router*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appended. The prompt is updated whenever the system name changes.

These sections contain the following configuration information:

- [Default System Name and Prompt Configuration, page 6](#)
- [Configuring a System Name, page 7](#)
- [Understanding DNS, page 7](#)

Default System Name and Prompt Configuration

The default router system name and prompt is *Router*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	hostname <i>name</i>	Manually configure a system name. The default setting is <i>router</i> . The name must follow the rules for ARPANET hostnames. They must start with a letter, exit with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your router, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

These sections contain this configuration information:

- [Default DNS Configuration, page 8](#)
- [Setting Up DNS, page 8](#)
- [Displaying the DNS Configuration, page 9](#)

Default DNS Configuration

Table 1 shows the default DNS configuration.

Table 1 Default DNS Configuration

Feature	Default Setting
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your router to use the DNS:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ip domain name <i>name</i>	Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot-up time, no domain name is configured; however, if the router configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
3.	ip name-server <i>dnsserver-address</i>	Defines up to three name servers. The address can be either an IPv4 address or an IPv6 address.
4.	ip domain list [<i>domain_name</i>]	(Optional) Define a list of default domain names to complete unqualified names.
5.	ip domain lookup	(Optional) Enable DNS-based hostname-to-address translation on your router. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
6.	exit	Return to privileged EXEC mode.
7.	show running-config	Verify your entries.
8.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If you use the router IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the software looks up the IP address without appending any default domain name to the hostname.

To remove a domain name, use the **no ip domain name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To delete a name from a list, use the **no ip domain list** [*domain_name*] global configuration command. To disable DNS on the router, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Managing the MAC Address Table

The MAC address table contains address information that the router 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 router learns and then ages when it is not in use.
- **Static address:** a manually entered unicast address that does not age and that is not lost when the router resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

These sections contain this configuration information:

- [Building the Address Table, page 9](#)
- [Default MAC Address Table Configuration, page 9](#)
- [Changing the Address Aging Time, page 10](#)
- [Displaying Address Table Entries, page 10](#)

Building the Address Table

With multiple MAC addresses supported on all ports, you can connect any port on the router to individual workstations, repeaters, routers, or other network devices. The router provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As stations are added or removed from the network, the router updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the router maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The router sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the router forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The router always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

Default MAC Address Table Configuration

[Table 2](#) shows the default MAC address table configuration.

Table 2 Default MAC Address Table Configuration

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the router learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the router receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact router performance.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	mac address-table aging-time [0 10-1000000]	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table.
3.	exit	Return to privileged EXEC mode.
4.	show mac address-table aging-time	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Displaying Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in [Table 3](#):

Table 3 Commands for Displaying the MAC Address Table

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.



Configuring Authentication

This chapter describes how to configure authentication on the Cisco 910 Industrial Routers (*hereafter* referred to as the router). This chapter consists of these sections:

- [Preventing Unauthorized Access to Your Router, page 1](#)
- [Protecting Access to Privileged EXEC Commands, page 1](#)
- [Controlling Router Access with RADIUS, page 2](#)
- [Configuring the Router for Local Authentication, page 7](#)
- [Configuring the Router for Secure Shell, page 7](#)
- [Configuring the Router for Secure Socket Layer HTTP, page 11](#)
- [Configuring the Router for Secure Copy Protocol, page 13](#)

Preventing Unauthorized Access to Your Router

You can prevent unauthorized users from reconfiguring your router and viewing configuration information. Typically, you want network administrators to have access to your router while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your router, you should configure username and password pairs, which are locally stored on the router. These pairs are assigned to lines or ports and authenticate each user before that user can access the router. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair. For more information, see the [“Configuring Username and Password for Local Authentication” section on page -2](#).

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

These sections contain this configuration information:

- [Configuring Enable Secret Passwords with Encryption, page 1](#)
- [Configuring Username and Password for Local Authentication, page 2](#)

Configuring Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use the **enable secret** global configuration commands. The command allows you to establish an encrypted password that users must enter to access privileged EXEC mode (the default).

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable secret passwords:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	enable secret [<i>password</i> 7]	Define a secret password for access to privileged EXEC mode. ■ For <i>password</i>, specify a string from 1 to 80 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. ■ (Optional) Specify 7 to indicate strong encryption.
3.	exit	Return to privileged EXEC mode.
4.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a password, use the **no enable secret** global configuration command.

Configuring Username and Password for Local Authentication

You can configure username and password pairs, which are locally stored on the router. These pairs are assigned to lines or ports and authenticate each user before that user can access the router.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	username <i>name</i> [password <i>password</i>] [description <i>description</i>]	Enter the username, privilege level, and password for each user. ■ For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. ■ For <i>password</i>, specify the password the user must enter to gain access to the router. If <i>password</i> is not specified, the user account will still be created but locked. ■ For <i>description</i>, specify detailed description of the user.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

Controlling Router Access with RADIUS

This section describes how to enable and configure the RADIUS, which provides detailed accounting information and flexible administrative control over authentication process. RADIUS is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

These sections contain this configuration information:

- [Understanding RADIUS, page 3](#)
- [RADIUS Operation, page 3](#)
- [Configuring RADIUS, page 3](#)
- [Displaying the RADIUS Configuration, page 7](#)

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

RADIUS Operation

When a user attempts to log in and authenticate to a router that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
 - a. ACCEPT—The user is authenticated.
 - b. REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
 - c. CHALLENGE—A challenge requires additional data from the user.
 - d. CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled. The additional data included with the ACCEPT or REJECT packets includes these items:

- Telnet, SSH, rlogin, or privileged EXEC services
- Connection parameters, including the host or client IP address, access list, and user timeouts

Configuring RADIUS

This section describes how to configure your router to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your router.

- [Default RADIUS Configuration, page 4](#)
- [Identifying the RADIUS Server Host, page 4](#) (required)
- [Configuring RADIUS Login Authentication, page 5](#) (required)
- [Defining AAA Server Groups, page 6](#) (optional)

Default RADIUS Configuration

When enabled, RADIUS can authenticate users accessing the router through the CLI.

Identifying the RADIUS Server Host

Router-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Key string

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

A RADIUS server and the router use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

You can configure the router to use AAA server groups to group existing server hosts for authentication. For more information, see the [“Defining AAA Server Groups” section on page -6](#).

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [key <i>string</i>]	Specify the IP address or hostname of the remote RADIUS server host. ■ (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. ■ (Optional) For key <i>string</i>, specify the authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. Note: The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the exit of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the router to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The router software searches for hosts in the order in which you specify them. Set the encryption key value to use with the specific RADIUS host.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname | ip-address* global configuration command.

This example shows how to configure a RADIUS server to be used for authentication:

```
Router(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
```

You also need to configure some settings on the RADIUS server. These settings include the IP address of the router and the key string to be shared by both the server and the router. For more information, see the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	aaa authentication login default [local group <i>group_name</i>]	Create a login authentication method list. ■ To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. ■ local—Use the local username database for authentication. You must enter username information in the database. Use the username name password global configuration command. ■ group group_name—Use server group authentication. Before you can use this authentication method, you must configure the group RADIUS server using the aaa group server radius command. You can use both the two methods as a failover. The server group authentication method is used prior than the local authentication. Note Default authentication method is local authentication only.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default value, which is local authentication only, use the **no login authentication default** command.

Defining AAA Server Groups

You can configure the router to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service, the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [key <i>string</i>]	Specify the IP address or hostname of the remote RADIUS server host. ■ (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. ■ (Optional) For key <i>string</i>, specify the authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. Note: The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the exit of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the router to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The router software searches for hosts in the order in which you specify them. Set the encryption key value to use with the specific RADIUS host.
3.	aaa group server radius <i>group-name</i>	Define the AAA server-group with a group name. This command puts the router in a server group configuration mode.
4.	server <i>hostname port-number</i>	Associate a particular RADIUS server with the defined server group. Each server in the group must be previously defined in 2..
5.	exit	Return to privileged EXEC mode.
6.	show running-config	Verify your entries.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.
8.		Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page -5 .

To remove the specified RADIUS server, use the **no radius-server host** global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius group-name** global configuration command. To remove the IP address of a RADIUS server, use the **no server hostname** server group configuration command.

The following example configures the login authentication with RADIUS server:

```
Router(config)# radius-server host 10.1.1.1 auth-port 1812 key Radius-Key
Router(config)# radius-server host 10.2.2.2 auth-port 1812 key Radius-Key
Router(config)# aaa group server radius MyServers
Router(config-sg-radius)# server 10.1.1.1 auth-port 1812
Router(config-sg-radius)# server 10.2.2.2 auth-port 1812
Router(config-sg-radius)# exit
Router(config)# aaa authentication login default group MyServers local
```

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Configuring the Router for Local Authentication

You can configure the router to operate without a server by setting the router to implement authentication in local mode.

Beginning in privileged EXEC mode, follow these steps to configure the router for local authentication:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	aaa authentication login default local	Set the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports.
3.	username name [password password] [description description]	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. ■ For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. ■ For <i>password</i>, specify the password the user must enter to gain access to the router.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example configures the login authentication with local authentication:

```
Router(config)# username abc password 123 description test_user
Router(config)# aaa authentication login default local
```

Configuring the Router for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

These sections contain this information:

- [Understanding SSH, page 8](#)
- [Configuring SSH, page 9](#)
- [Displaying the SSH Configuration and Status, page 11](#)

SSH in IPv6 functions the same and offers the same benefits as SSH in IPv4. IPv6 enhancements to SSH consist of support for IPv6 addresses that enable a Cisco router to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

Understanding SSH

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).

This section consists of these topics:

- [SSH Servers, Integrated Clients, and Supported Versions, page 8](#)
- [Limitations, page 8](#)

SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the router. You can use an SSH client to connect to a router running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The router supports an SSHv1 or an SSHv2 server.

The router supports an SSHv1 client.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

- RADIUS (for more information, see the [“Controlling Router Access with RADIUS”](#) section on page -2)
- Local authentication (for more information, see the [“Configuring the Router for Local Authentication”](#) section on page -7)

Limitations

These limitations apply to SSH:

- The router supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on DES (56-bit) and 3DES (168-bit) data encryption software.
- The router 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.

Configuring SSH

This section has this configuration information:

- [Configuration Guidelines, page 9](#)
- [Setting Up the Router to Run SSH, page 9](#) (required)
- [Configuring the SSH Server, page 10](#) (required only if you are configuring the router as an SSH server)

Configuration Guidelines

Follow these guidelines when configuring the router 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. For more information, see the [“Setting Up the Router to Run SSH” section on page -9](#).
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a 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.

Setting Up the Router to Run SSH

Follow these steps to set up your router to run SSH:

1. Configure a hostname and IP domain name for the router. Follow this procedure only if you are configuring the router as an SSH server.
2. Generate an RSA key pair for the router, which automatically enables SSH. Follow this procedure only if you are configuring the router as an SSH server.
3. Configure user authentication for local or remote access. This step is required. For more information, see the [“Configuring the Router for Local Authentication” section on page -7](#).

Beginning in privileged EXEC mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair. This procedure is required if you are configuring the router as an SSH server.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	hostname <i>hostname</i>	Configure a hostname for your router.
3.	ip domain name <i>domain_name</i>	Configure a host domain for your router.

	Command	Purpose
4.	crypto key generate rsa	Enable the SSH server for local and remote authentication on the router and generate an RSA key pair. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.
5.	exit	Return to privileged EXEC mode.
6.	show ip ssh or show ssh	Show the version and configuration information for your SSH server. Show the status of the SSH server on the router.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring the SSH Server

Beginning in privileged EXEC mode, follow these steps to configure the SSH server:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ip ssh version [1 2]	(Optional) Configure the router to run SSH Version 1 or SSH Version 2. ■ 1—Configure the router to run SSH Version 1. ■ 2—Configure the router to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
3.	ip ssh {timeout seconds authentication-retries number}	Configure the SSH control parameters: ■ Specify the time-out value in seconds; the default is 120 seconds. The range is 1 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the router uses the default time-out 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 time-out value returns to the default of 10 minutes. ■ Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 1 to 5. Repeat this step when configuring both parameters.

	Command	Purpose
4.	exit	Return to privileged EXEC mode.
5.	show ip ssh or show ssh	Show the version and configuration information for your SSH server. Show the status of the SSH server connections on the router.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default SSH control parameters, use the **no ip ssh {timeout | authentication-retries}** global configuration command.

The following example enables the SSH service:

```
Router# configure terminal
Router(config)# hostname test
Router(config)# ip domain name cisco.com
Router(config)# crypto key generate rsa
Router(config)# username cisco password cisco
Router(config)# ip ssh time-out 60
Router(config)# ip ssh authentication-retries 3
```

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in [Table 1](#):

Table 1 Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

Configuring the Router for Secure Socket Layer HTTP

This section describes how to configure Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and client. SSL provides server authentication, encryption, and message integrity, as well as HTTP client authentication, to allow secure HTTP communications.

These sections contain this information:

- [Understanding Secure HTTP Servers and Clients, page 11](#)
- [Configuring Secure HTTP Servers, page 12](#)
- [Displaying Secure HTTP Server Status, page 13](#)

Understanding Secure HTTP Servers and Clients

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a router from a Web browser. Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. HTTP over SSL is abbreviated as HTTPS; the URL of a secure connection begins with https:// instead of http://.

The primary role of the HTTP secure server (the router) is to listen for HTTPS requests on a designated port (the default HTTPS port is 443) and pass the request to the HTTP 1.1 Web server. The HTTP 1.1 server processes requests and passes responses (pages) back to the HTTP secure server, which, in turn, responds to the original request.

The primary role of the HTTP secure client (the web browser) is to respond to requests for HTTPS User Agent services, perform HTTPS User Agent services for the application, and pass the response back to the application.

Configuring Secure HTTP Servers

A self-signed certificate is generated the first time that you enable the secure HTTP server.

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

	Command	Purpose
1.	show ip http server status	(Optional) Display the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output: HTTP secure server capability: Present or HTTP secure server capability: Not present
2.	configure terminal	Enter global configuration mode.
3.	ip http secure-server	Enable the HTTPS server if it has been disabled. The HTTPS server is enabled by default.
4.	ip http secure-port <i>port-number</i>	(Optional) Specify the port number to be used for the HTTPS server. The default port number is 443. Valid options any number in the range 1 to 65535.
5.	ip http max-connections <i>value</i>	(Optional) Set the maximum number of concurrent connections that are allowed to the HTTP server. The range is 1 to 40; the default value is 16.
6.	exit	Return to privileged EXEC mode.
7.	show ip http server secure status	Display the status of the HTTP secure server to verify the configuration.
8.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no ip http server** global configuration command to disable the standard HTTP server. Use the **no ip http secure-server** global configuration command to disable the secure HTTP server. Use the **no ip http secure-port** global configuration commands to return to the default settings.

To verify the secure HTTP connection by using a Web browser, enter `https://URL`, where the URL is the IP address or hostname of the server router. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

```
https://209.165.129.1026
```

or

```
https://host.domain.com:1026
```

Displaying Secure HTTP Server Status

To display the SSL secure server status, use the privileged EXEC commands in [Table 2](#):

Table 2 **Commands for Displaying the SSL Secure Server Status**

Command	Purpose
show ip http server secure status	Shows the HTTP secure server configuration.
show running-config	Shows the generated self-signed certificate for secure HTTP connections.

Configuring the Router for Secure Copy Protocol

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

For SSH to work, the router needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Information About Secure Copy

To configure the Secure Copy feature, you should understand these concepts.

SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

When SSH service is enabled, the router allows secure network transfer with other hosts.



Configuring Interface Characteristics

This chapter defines the types of interfaces on the Cisco 910 Industrial Routers (*hereafter* referred to as the router) and describes how to configure them.

The chapter consists of these sections:

- [Understanding Interface Types, page 1](#)
- [Using Interface Configuration Mode, page 2](#)
- [Configuring Ethernet Interfaces, page 2](#)
- [Monitoring and Maintaining the Interfaces, page 7](#)

Understanding Interface Types

This section describes the different types of interfaces supported by the switch with references to chapters that contain more detailed information about configuring these interface types.

- [Switch Ports, page 1](#)
- [Dual-Purpose Uplink Ports, page 1](#)

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. A switch port can be an access port, a trunk port, or a tunnel port. You can configure a port as an access port or trunk port. Switch ports are used for managing the physical interface and associated Layer 2 protocols.

Configure switch ports by using the **switchport** interface configuration commands. Use the **switchport** command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

For detailed information about configuring access port and trunk port characteristics, see [Chapter 8, “Configuring 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.

Dual-Purpose Uplink Ports

The router supports a dual-purpose uplink ports. The uplink port is considered as a single interface with dual front exits—an RJ-45 connector and a small form-factor pluggable (SFP) module connector. The dual front exits are not redundant interfaces, and the router activates only one connector of the pair.

By default, the router dynamically selects the interface type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP module connector. For information about configuring speed and duplex settings for a dual-purpose uplink, see the [“Setting the Interface Speed and Duplex Parameters” section on page -5](#).

The uplink port has two LEDs: one shows the status of the RJ-45 port, and one shows the status of the SFP module port. The port LED is on for whichever connector is active. For more information about the LEDs, see the hardware installation guide.

Using Interface Configuration Mode

The switch supports these interface types:

- Physical ports—switch ports and routed ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

To configure a physical interface (port), specify the interface type, module number, and port number, and enter interface configuration mode.

Procedures for Configuring Interfaces

These general instructions apply to all interface configuration processes.

1. Enter the **configure terminal** command at the privileged EXEC prompt:

```
Router# configure terminal  
Router(config)#
```

2. Enter the **interface** global configuration command.

Identify the interface type and the interface number, Gigabit Ethernet port 0/1 in this example:

```
Router(config)# interface gigabitethernet 0/1  
Router(config-if)#
```

3. Follow each **interface** command with the configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter **exit** to return to privileged EXEC mode.
4. After you configure an interface, verify its status by using the **show** privileged EXEC commands listed in the [“Monitoring and Maintaining the Interfaces” section on page -7](#).

Enter the **show interfaces** privileged EXEC command to see a list of all interfaces on or configured for the router. A report is provided for each interface that the device supports or for the specified interface.

Configuring Ethernet Interfaces

These sections contain this configuration information:

- [Setting the Type of a Dual-Purpose Uplink Port, page 3](#)
- [Configuring Interface Speed and Duplex Mode, page 4](#)
- [Configuring Auto-MDIX on an Interface, page 5](#)
- [Adding a Description for an Interface, page 6](#)

Setting the Type of a Dual-Purpose Uplink Port

The router supports a dual-purpose uplink port. By default, the router dynamically selects the interface type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP module connector. For more information, see the [“Dual-Purpose Uplink Ports” section on page -1](#).

Beginning in privileged EXEC mode, follow these steps to select which dual-purpose uplink to activate so that you can set the speed and duplex. This procedure is optional.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the dual-purpose uplink port to be configured, and enter interface configuration mode.
3.	media-type { auto-select rj45 sfp }	Select the interface and type of a dual-purpose uplink port. The keywords have these meanings: ■ auto-select—The router dynamically selects the type. When link up is achieved, the router disables the other type until the active link goes down. When the active link goes down, the router enables both types until one of them links up. In auto-select mode, the router configures both types with autonegotiation of speed and duplex (the default). depending on the type of installed SFP module, the router might not be able to dynamically select it. For more information, see the information that follows this procedure. ■ rj45—The router disables the SFP module interface. If you connect an SFP module to this port, it cannot attain a link even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type. ■ sfp—The router disables the RJ-45 interface. If you connect a cable to the RJ-45 port, it cannot attain a link even if the SFP module side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type. For information about setting the speed and duplex, see the “Speed and Duplex Configuration Guidelines” section on page -4.
4.	exit	Return to privileged EXEC mode.
5.	show interfaces <i>interface-id</i>	Verify your setting.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **media-type auto interface** or the **no media-type** interface configuration commands.

The router configures both types to autonegotiate speed and duplex (the default). If you configure **auto-select**, you cannot configure the **speed** and **duplex** interface configuration commands.

When the router powers on or when you enable a dual-purpose uplink port through the **shutdown** and the **no shutdown** interface configuration commands, the router gives preference to the SFP module interface. In all other situations, the router selects the active link based on which type first links up.

The router operates with 100BASE-x (where -x is -BX, -FX-FE, -LX) SFP modules as follows:

- When the 100BASE-x SFP module is inserted into the module slot and there is no link on the RJ-45 side, the router disables the RJ-45 interface and selects the SFP module interface. This is the behavior even if there is no cable connected and if there is no link on the SFP module side.
- When the 100BASE-x SFP module is inserted and there is a link on the RJ-45 side, the router continues with that link. If the link goes down, the router disables the RJ-45 side and selects the SFP module interface.
- When the 100BASE-x SFP module is removed, the router again dynamically selects the type (**auto-select**) and re-enables the RJ-45 side.

The router does not have this behavior with 100BASE-FX-GE SFP modules.

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the router operate in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

These sections describe how to configure the interface speed and duplex mode:

- [Speed and Duplex Configuration Guidelines, page 4](#)
- [Setting the Interface Speed and Duplex Parameters, page 5](#)

Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Fast Ethernet (10/100-Mb/s) ports support all speed and duplex options.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
 - The 1000BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
 - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
 - The 100BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support only 100 Mb/s. These modules support full- and half- duplex options but do not support autonegotiation.

For information about which SFP modules are supported on your router, see the product release notes.

- If both exits of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other exit does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.

Caution: Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode.
3.	speed {10 100 1000 auto}	Enter the appropriate speed parameter for the interface: ■ Enter 10, 100, or 1000 to set a specific speed for the interface. The 1000 keyword is available only for 10/100/1000 Mb/s ports. ■ Enter auto to enable the interface to autonegotiate speed with the connected device. If you use the 10, 100, or the 1000 keywords with the auto keyword, the port autonegotiates only at the specified speeds. For more information about speed settings, see the “Speed and Duplex Configuration Guidelines” section on page -4 .
4.	duplex {auto full half}	Enter the duplex parameter for the interface. Enable half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s. For more information about duplex settings, see the “Speed and Duplex Configuration Guidelines” section on page -4 .
5.	exit	Return to privileged EXEC mode.
6.	show interfaces <i>interface-id</i>	Display the interface speed and duplex mode configuration.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no speed** and **no duplex** interface configuration commands to return the interface to the default speed and duplex settings (autonegotiate).

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# speed 100
```

Configuring Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately. With auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling.

Auto-MDIX is enabled by default. When you enable auto-MDIX, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

Auto-MDIX is not supported on 1000BASE-SX or -LX SFP module interfaces.

Table 1 shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 1 Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling
On	On	Link up	Link up
On	Off	Link up	Link up
Off	On	Link up	Link up
Off	Off	Link up	Link down

Beginning in privileged EXEC mode, follow these steps to configure auto-MDIX on an interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode.
3.	speed auto	Configure the interface to autonegotiate speed with the connected device.
4.	duplex auto	Configure the interface to autonegotiate duplex mode with the connected device.
5.	mdix auto	Enable auto-MDIX on the interface.
6.	exit	Return to privileged EXEC mode.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable auto-MDIX, use the **no mdix auto** interface configuration command.

This example shows how to enable auto-MDIX on a port:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# speed auto
Router(config-if)# duplex auto
Router(config-if)# mdix auto
Router(config-if)# exit
```

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: **show running-config** and **show interfaces**.

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the interface for which you are adding a description, and enter interface configuration mode.
3.	description <i>string</i>	Add a description (up to 18 characters) for an interface.
4.	exit	Return to privileged EXEC mode.
5.	show interfaces <i>interface-id</i> or show running-config	Verify your entry.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no description** interface configuration command to delete the description.

This example shows how to add a description on a port and how to verify the description:

```
Router# config terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# description ConnectstoMarketing
Router(config-if)# exit
Router# show interfaces gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is Combo Gigabit Ethernet and SFP Slot, address is 3C:CE:73:A5:5B:B0
  Description:ConnectstoMarketing
  MTU is 1500 bytes
  duplex full, speed 1000M, media type is Combo
  10079967 packets input, 479985141 bytes
  Received 2252279 broadcasts (2747874 multicasts)
  0 FCS errors, 0 under size, 0 over size, 0 pause input
  94789 packets output, 27415703 bytes
  Transmitted 325 broadcasts (30985 multicasts)
  0 FCS errors, 0 collisions, 0 deferred, 0 pause output
```

Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

- [Monitoring Interface Status, page 7](#)
- [Clearing and Resetting Interfaces and Counters, page 8](#)
- [Shutting Down and Restarting the Interface, page 8](#)

Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces. [Table 2](#) lists some of these interface monitoring commands. (You can display the full list of **show** commands by using the **show ?** command at the privileged EXEC prompt.)

Table 2 Show Commands for Interfaces

Command	Purpose
show interfaces [<i>interface-id</i>]	(Optional) Display the status and configuration of all interfaces or a specific interface.
show ip interface [<i>interface-id</i>]	(Optional) Display the usability status of all interfaces configured for IP routing or the specified interface.
show running-config interface [<i>interface-id</i>]	Display the running configuration in RAM for the interface.
show version	Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.

Clearing and Resetting Interfaces and Counters

To clear the interface counters shown by the **show interfaces** privileged EXEC command, use the **clear counters** privileged EXEC command. The **clear counters** command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.

The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface { <i>vlan vlan-id</i> } { GigabitEthernet <i>interface-id</i> }	Select the interface to be configured.
3.	shutdown	Shut down an interface.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entry.

Use the **no shutdown** interface configuration command to restart the interface.

To verify that an interface is disabled, enter the **show interfaces** privileged EXEC command. A disabled interface is shown as *administratively down* in the display.



Configuring VLANs

This chapter describes how to configure VLANs on the Cisco 910 Industrial Routers (*hereafter* referred to as the router). It includes information about VLAN membership modes, VLAN configuration modes, and VLAN trunks.

The chapter consists of these sections:

- [Understanding VLANs, page 1](#)
- [Configuring VLANs, page 1](#)
- [Assigning Static-Access Ports to a VLAN, page 2](#)
- [Displaying VLANs, page 3](#)
- [Configuring VLAN Trunks, page 3](#)

Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group exit stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to exit 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 switch supporting fallback bridging. VLANs are identified by a number from 1 to 4094.

Configuring VLANs

You configure VLANs in **vlan** global configuration command by entering a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. You can enter the **copy running-config startup-config** privileged EXEC command to save the configuration in the startup configuration file. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

Creating or Modifying a VLAN

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	vlan <i>vlan-id</i>	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.

	Command	Purpose
3.	exit	Return to privileged EXEC mode.
4.	show vlan	Verify your entries.
5.	copy running-config startup config	(Optional) This saves the configuration in the switch startup configuration file.

This example shows how to create VLAN 20:

```
Router# configure terminal
Router(config)# vlan 20
Router(config-vlan)# exit
```

Deleting a VLAN

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	no vlan <i>vlan-id</i>	Remove the VLAN by entering the VLAN ID.
3.	exit	Return to privileged EXEC mode.
4.	show vlan	Verify the VLAN removal.
5.	copy running-config startup config	(Optional) This saves the configuration in the switch startup configuration file.

Assigning Static-Access Ports to a VLAN

If you want to assign an interface to a VLAN that does not exist, create the new VLAN first. (See the [“Creating or Modifying a VLAN”](#) section on page -1.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN:

	Command	Purpose
1.	configure terminal	Enter global configuration mode
2.	interface <i>interface-id</i>	Enter the interface to be added to the VLAN.
3.	switchport mode access	Define the VLAN membership mode for the port (Layer 2 access port).
4.	switchport access vlan <i>vlan-id</i>	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
5.	exit	Return to privileged EXEC mode.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure a port as an access port in VLAN 2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the router. The display includes VLAN status, ports, and configuration information.

Configuring VLAN Trunks

These sections contain this information:

- [Trunking Overview, page 3](#)
- [Configuring an Ethernet Interface as a Trunk Port, page 3](#)

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The router supports IEEE 802.1Q encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle.

Ethernet trunk interfaces support different trunking modes (see [Table 3](#)). You can set an interface as trunking or nontrunking.

Table 3 **Interface Modes**

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

Configuring an Ethernet Interface as a Trunk Port

These sections contain this configuration information:

- [Configuring a Trunk Port, page 3](#)
- [Defining the Allowed VLANs on a Trunk, page 4](#)
- [Configuring the Native VLAN for Untagged Traffic, page 5](#)

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as a trunk port:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the port to be configured for trunking, and enter interface configuration mode.
3.	switchport mode trunk	Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
4.	switchport access vlan <i>vlan-id</i>	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
5.	switchport trunk native vlan <i>vlan-id</i>	Specify the native VLAN for IEEE 802.1Q trunks.
6.	exit	Return to privileged EXEC mode.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration command to configure the port as a static-access port.

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a trunk:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the port to be configured, and enter interface configuration mode.
3.	switchport mode trunk	Configure the interface as a VLAN trunk port.
4.	switchport trunk allowed vlan {all none <i>vlan-list</i> }	(Optional) Configure the list of VLANs allowed on the trunk. The <i>vlan-list</i> parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.
5.	exit	Return to privileged EXEC mode.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Define the interface that is configured as the IEEE 802.1Q trunk, and enter interface configuration mode.
3.	switchport trunk native vlan <i>vlan-id</i>	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For <i>vlan-id</i> , the range is 1 to 4094.
4.	exit	Return to privileged EXEC mode.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.



Configuring DHCP Server

This chapter describes how to configure DHCP server on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

- [Understanding DHCP, page 1](#)
- [Enabling DHCP Server, page 1](#)
- [Configuring DHCP Server, page 2](#)
- [Displaying DHCP Server Address Bindings, page 4](#)

Understanding DHCP

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

The DHCP server assigns IP addresses from specified address pools on a router or router to DHCP clients and manages them.

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

Enabling DHCP Server

Beginning in privileged EXEC mode, follow these steps to enable the DHCP server on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	service dhcp <i>interface-type number</i>	Enable the DHCP server on the interface.
3.	exit	Return to privileged EXEC mode.
4.	show running-config	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable the DHCP server, use the **no service dhcp** global configuration command.

Configuring DHCP Server

This section contains this configuration information:

- [Configuring DHCP Server, page 2](#)
- [Configuring Stateful DHCPv6 Server, page 3](#)
- [Configuring Stateless DHCPv6 Server, page 3](#)

Configuring DHCP Server

Beginning in privileged EXEC mode, follow these steps to configure DHCP server.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ip dhcp pool	Create a DHCP server address pool and enters DHCP pool configuration mode. Note: If you have changed the parameters of the DHCP server, you must perform a refresh using the no service dhcp interface-type number command and service dhcp interface-type number commands.
3.	network <i>network-number mask</i>	Specify the subnet network number and mask of the DHCP address pool.
4.	domain-name <i>domain</i>	Specify the domain name for the client.
5.	dns-server <i>address</i>	Specify the IP address of a DNS server that is available to a DHCP client.
6.	default-router <i>address</i>	Specify the IP address of the default router for a DHCP client.
7.	exit	Return to privileged EXEC mode.
8.	service dhcp <i>interface-type number</i>	Enable DHCP server on the interface.

The following example configures the DHCP server:

```
Router# configure terminal
Router(config)# ip dhcp included-address 192.168.1.101 192.168.1.150
Router(config)# ip dhcp pool
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# domain-name cisco.com
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# exit
Router(config)# service dhcp vlan1
```

Configuring Stateful DHCPv6 Server

Beginning in privileged EXEC mode, follow these steps to configure stateful DHCPv6 server.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ip dhcp pool	Create a DHCP server address pool and enters DHCP pool configuration mode. Note: If you have changed the parameters of the DHCP server, you must perform a refresh using the no service dhcp interface-type number command and service dhcp interface-type number commands.
3.	address prefix <i>ipv6-prefix</i>	Specify an address prefix for address assignment.
4.	domain-name <i>domain</i>	Specify the domain name for the DHCPv6 client.
5.	dns-server <i>ipv6-address</i>	Specify the DNS IPv6 servers available to a DHCPv6 client.
6.	exit	Return to privileged EXEC mode.
7.	ipv6 dhcp included-address <i>low-address high-address</i>	Specify the IP addresses that the DHCPv6 server should assign to DHCPv6 clients.
8.	interface <i>type number</i>	Specify an interface type and number, and enters the interface configuration mode.
9.	ipv6 dhcp server	Enable DHCPv6 on an interface.

The following example configures the stateful DHCPv6 server:

```
Router(config)# ipv6 dhcp pool
Router(config-dhcpv6)# address prefix 2001:DB8:1001::0/64
Router(config-dhcpv6)# domain-name cisco.com
Router(config-dhcpv6)# dns-server 2001:DB8:1001::1
Router(config-dhcpv6)# exit
Router(config)# ipv6 dhcp included-address 2001:DB8:1001::100 2001:DB8:1001::200
Router(config)# interface Vlan 1
Router(config-if)# ipv6 dhcp server
```

Configuring Stateless DHCPv6 Server

Beginning in privileged EXEC mode, follow these steps to configure stateless DHCPv6 server.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ipv6 nd managed-config-flag	Set the "managed address configuration flag" in IPv6 router advertisements.
3.	ipv6 nd prefix	Set the IPv6 prefix which is included in IPv6 Neighbor Discovery (ND) router advertisements.

The following example configures the stateless DHCPv6 server:

```
Router(config)# interface Vlan 1
```

```
Router(config-if)# ipv6 nd managed-config-flag
Router(config-if)# ipv6 nd prefix 2001:DB8:1001::0/64
```

Displaying DHCP Server Address Bindings

To display the DHCP server address binding information, use the privileged EXEC command in [Table 4](#):

Table 4 Commands for Displaying DHCP Address Bindings

Command	Purpose
show ip dhcp binding	Display address bindings on the DHCP server.

The following example is a sample output of the **show ip dhcp binding** command:

```
Router# show ip dhcp binding

IP address      Hardware address    Lease expiration
10.0.1.60       88:75:56:27:32:01   2000/01/01 17:37:12
```



Configuring LLDP

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) service on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

- [Understanding LLDP and LLDP-MED, page 1](#)
- [Configuring LLDP and LLDP-MED, page 1](#)
- [Monitoring and Maintaining LLDP and LLDP-MED, page 4](#)

Understanding LLDP and LLDP-MED

To support non-Cisco devices and to allow for interoperability between other devices, the router supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as routers. It specifically provides support for voice over IP (VoIP) applications, Power over Ethernet, inventory management, and location information. The Cisco 910 Industrial Router only supports the following location information for LLDP-MED.

- Civic location information—Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.
- ELIN location information—Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Configuring LLDP and LLDP-MED

- [Default LLDP Configuration, page 2](#)
- [Enabling LLDP, page 2](#)
- [Configuring LLDP-MED, page 2](#)

Default LLDP Configuration

Table 5 Default LLDP Configuration

Feature	Default Setting
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	1 second
LLDP receive	Disabled (When LLDP is globally enabled, LLDP receive is also enabled.)
LLDP transmit	Disabled (When LLDP is globally enabled, LLDP transmit is also enabled.)

Enabling LLDP

All LLDP configurations are under global configuration. The router does not support per-interface configuration for LLDP.

Beginning in privileged EXEC mode, follow these steps to enable LLDP:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	lldp run	Enable LLDP globally on the router.
3.	lldp timer rate	(Optional) Set the sending frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.
4.	exit	Return to privileged EXEC mode.
5.	show lldp	Verify the configuration.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable LLDP, use the **no lldp run** global configuration command.

This example shows how to globally enable LLDP.

```
Router# configure terminal
Router(config)# lldp run
Router(config)# exit
```

Configuring LLDP-MED

Beginning in privileged EXEC mode, follow these steps to configure location information for an endpoint and to apply it to an interface.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	location civic-location address interface <i>interface-id</i> or location elin-location address interface <i>interface-id</i>	Specify the location information for an endpoint. ■ civic-location—Specify civic location information. ■ elin-location—Specify emergency location information (ELIN). ■ address—Specify the site or location information in alphanumeric format. – The format of the civic-location is <i>2:County:6:Stree:3:City:19:House number</i>. The first digit is always 2. The next two letters are the country code. Then, arguments are paired to form the address. The first member of the pair is a digit indicating the type of the second member. The valid types are listed as following: 1—National subdivisions 2—County, parish, district 3—City, township 4—City division, borough, ward 5—Neighborhood, block 6—Street 16—Leading street direction 17—Trailing street suffix 18—Street suffix 19—House number 20—House number suffix 21—Landmark or vanity address 22—Additional location info 23—Name 24—Postal/ZIP code 25—Building 26—Unit 27—Floor 28—Room number 29—Place type 128—Script – The format of the elin-location is <i>3:ELIN_number</i>, where the first digit should be 3 and <i>ELIN_number</i> is a numerical string using for setting up emergency call. ■ interface-id—Specify the interface, which should only be GigabitEthernet 0/1 for the router.

	Command	Purpose
3.	exit	Return to privileged EXEC mode.
4.	show location civic-location interface <i>interface-id</i> or show location elin-location interface <i>interface-id</i>	Verify the configuration.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of each command to return to the default setting.

This example shows how to configure civic location information on the router:

```
Router# configure terminal
Router(config)# location civic-location 2:FR:6:CommercialRd:3:Roseville:19:4 interface GigabitEthernet
0/1
Router(config)# exit
```

This example shows how to configure ELIN location information on the router:

```
Router# configure terminal
Router(config)# location elin-location 3:000911 interface interface GigabitEthernet 0/1
Router(config)# exit
```

Monitoring and Maintaining LLDP and LLDP-MED

To monitor and maintain LLDP and LLDP-MED service on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

Command	Description
show lldp	Display global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface.
show lldp neighbors [<i>interface-id</i>]	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID.
show location civic-location identifier <i>id</i>	Display the location information for a specific global civic location.
show location elin-location identifier <i>id</i>	Display the location information for an emergency location.

The following example shows a sample output of the **show lldp** command:

```
Router# show lldp
-----
Global configuration:
-----
Configuration:
  Transmit delay: 30
  Hold time:      120
  Reinitialisation delay: 1
  Receive mode: no
  Pattern for management addresses: (none)
  Interface pattern: (none)
  Interface pattern for chassis ID: (none)
  Override description with: (none)
```

```
Override platform with: (none)
Advertise version: yes
Disable LLDP-MED inventory: no
```

The following example shows a sample output of the **show lldp neighbors** command:

```
Router# show lldp neighbors eth1
LLDP neighbors:
-----
Interface:      eth1, via: LLDP, RID: 3, Time: 0 day, 00:01:25
Chassis:
ChassisID: mac 00:64:40:f0:d2:80
SysName: C2960.hc.nsbg.efoxconn.com
SysDescr: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Dec-11 00:46 by prod_rel_team
MgmtIP:172.18.60.89
Capability: Bridge, on
Port:
  PortID: ifname Fa0/37
  PortDescr: FastEthernet0/37
  PMD autoneg: supported: yes, enabled: yes
  Adv: 10Base-T, HD: yes, FD: yes
  Adv: 100Base-T, HD: yes, FD: yes
  MAU oper type: 100BaseTXFD - 2 pair category 5 UTP, full duplex mode
VLAN: 1, pvid: yes
LLDP-MED:
  Device Type: unknown
  Capability: Capabilities
  Capability: Policy
  Capability: Location
  Capability: MDI/PSE
  Capability: Inventory
  LLDP-MED Network Policy for: AppType: 1, Defined: no
    : Voice
    Layer 2 Priority: 0
    DSCP Value: 0
  LLDP-MED Network Policy for: AppType: 2, Defined: no
    : Voice Signaling
    Layer 2 Priority: 0
    DSCP Value: 0
  LLDP-MED Location Identification: Type: address
    Country:
Extended Power-over-Ethernet:
  Power Type & Source: PSE Device
  Power Source: Primary Power Source
  Power Priority: low
  Power Value: 0
Inventory:
  Hardware Revision: WS-C2960-48PST-L (PowerPC405):B0
  Software Revision: 15.0(1)SE2
  Manufacturer: Cisco Systems, Inc.
  Model: WS-C2960-48PST-L
```

The following example shows the civic location configuration:

```
Router# show location civic-location eth1
Civic location information:
County: FR
Street: CommercialRd
City: Roseville
```

House number: 4
Floor: 2
Room number: 1

The following example shows the ELIN location configuration:

```
Router# show location elin-location eth1  
Elin location information:  
Elin: 00000911
```



Configuring RMON

This chapter describes how to configure Remote Network Monitoring (RMON) on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

This chapter consists of these sections:

- [Understanding RMON, page 1](#)
- [Configuring RMON, page 1](#)
- [Displaying RMON Status, page 4](#)

Understanding RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the router to monitor all the traffic flowing among routers on all connected LAN segments. The router supports the RMON probe function to provide basic traffic statistics information of Ethernet network on local environment.

The router supports these RMON groups (defined in RFC 1757):

- Statistics (RMON group 1)—Collects Ethernet statistics (including Fast Ethernet and Gigabit Ethernet statistics, depending on the router type and supported interfaces) on an interface.
- History (RMON group 2)—Collects a history group of statistics on Ethernet ports (including Fast Ethernet and Gigabit Ethernet statistics, depending on the router type and supported interfaces) for a specified polling interval.
- Alarm (RMON group 3)—Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Event (RMON group 9)—Specifies the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

Configuring RMON

These sections contain this configuration information:

- [Default RMON Configuration, page 2](#)
- [Configuring RMON Alarms and Events, page 2](#) (required)
- [Collecting Group History Statistics on an Interface, page 3](#) (optional)
- [Collecting Group Ethernet Statistics on an Interface, page 4](#) (optional)

Default RMON Configuration

RMON is disabled by default; no alarms or events are configured.

Configuring RMON Alarms and Events

You can configure your router for RMON by using the command-line interface (CLI). You must also configure SNMP on the router to access RMON MIB objects. For more information, see [Chapter 13, “Configuring SNMP.”](#)

Beginning in privileged EXEC mode, follow these steps to enable RMON alarms and events. This procedure is required.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	rmon alarm <i>number variable interval {absolute delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</i>	Set an alarm on a MIB object. ■ For <i>number</i>, specify the alarm number. The range is 1 to 65535. ■ For <i>variable</i>, specify the MIB object to monitor. ■ For <i>interval</i>, specify the time in seconds the alarm monitors the MIB variable. The range is 1 to 4294967295 seconds. ■ Specify the absolute keyword to test each MIB variable directly. Specify the delta keyword to test the change between samples of a MIB variable. ■ For <i>value</i>, specify a number at which the alarm is triggered and one for when the alarm is reset. The range for the rising threshold and falling threshold values is -2147483648 to 2147483647. ■ (Optional) For <i>event-number</i>, specify the event number to trigger when the rising or falling threshold exceeds its limit. ■ (Optional) For owner string, specify the owner of the alarm.
3.	rmon event <i>number [description string] [log] [owner string] [trap community]</i>	Add an event in the RMON event table that is associated with an RMON event number. ■ For <i>number</i>, assign an event number. The range is 1 to 65535. ■ (Optional) For description string, specify a description of the event. ■ (Optional) Use the log keyword to generate an RMON log entry when the event is triggered. ■ (Optional) For owner string, specify the owner of this event. ■ (Optional) For trap community, enter the SNMP community string used for this trap.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable an alarm, use the **no rmon alarm number** global configuration command on each alarm you configured. You cannot disable at once all the alarms that you configured. To disable an event, use the **no rmon event number** global configuration command. To learn more about alarms and events and how they interact with each other, see RFC 1757.

You can set an alarm on any MIB object. The following example configures RMON alarm number 10 by using the **rmon alarm** command. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events can include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0, the alarm is reset and can be triggered again.

```
Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner
jjohnson
```

The following example creates RMON event number 1 by using the **rmon event** command. The event is defined as *High ifOutErrors* and generates a log entry when the event is triggered by the alarm. The user *jjones* owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Router(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner jjones
```

Collecting Group History Statistics on an Interface

You must first configure RMON alarms and events to display collection information.

Beginning in privileged EXEC mode, follow these steps to collect group history statistics on an interface. This procedure is optional.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the interface on which to collect history, and enter interface configuration mode.
3.	rmon collection history <i>index</i> [buckets <i>bucket-number</i>] [interval <i>seconds</i>] [owner <i>ownername</i>]	Enable history collection for the specified number of buckets and time period. ■ For <i>index</i>, identify the RMON group of statistics. The range is 1 to 65535. ■ (Optional) For buckets <i>bucket-number</i>, specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1 to 65535. The default is 50 buckets. ■ (Optional) For interval <i>seconds</i>, specify the number of seconds in each polling cycle. The range is 1 to 3600. The default is 1800 seconds. ■ (Optional) For owner <i>ownername</i>, enter the name of the owner of the RMON group of statistics.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	show rmon history	Display the contents of the router history table.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable history collection, use the **no rmon collection history index** interface configuration command.

Collecting Group Ethernet Statistics on an Interface

Beginning in privileged EXEC mode, follow these steps to collect group Ethernet statistics on an interface. This procedure is optional.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Specify the interface on which to collect statistics, and enter interface configuration mode.
3.	rmon collection stats <i>index</i> [owner <i>ownername</i>]	Enable RMON statistic collection on the interface. ■ For <i>index</i>, specify the RMON group of statistics. The range is from 1 to 65535. ■ (Optional) For owner <i>ownername</i>, enter the name of the owner of the RMON group of statistics.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	show rmon statistics	Display the contents of the router statistics table.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable the collection of group Ethernet statistics, use the **no rmon collection stats** *index* interface configuration command.

This example shows how to collect RMON statistics for the owner *root*:

```
Router(config)# interface GigabitEthernet 0/1
Router(config-if)# rmon collection stats 2 owner root
```

Displaying RMON Status

To display the RMON status, use one or more of the privileged EXEC commands in [Table 6](#):

Table 6 Commands for Displaying RMON Status

Command	Purpose
show rmon alarms	Displays the RMON alarm table.
show rmon events	Displays the RMON event table.
show rmon history	Displays the RMON history table.
show rmon statistics	Displays the RMON statistics table.



Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

- [Understanding System Message Logging, page 1](#)
- [Configuring System Message Logging, page 1](#)
- [Displaying the Logging Configuration, page 6](#)

Understanding System Message Logging

By default, a router sends the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, console port, or a UNIX syslog server, depending on your configuration.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations.

You can access logged system messages by using the router command-line interface (CLI) or by saving them to a properly configured syslog server. The router software saves syslog messages in an internal buffer.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the router through Telnet or through the console port.

Configuring System Message Logging

These sections contain this configuration information:

- [System Log Message Format, page 1](#)
- [Default System Message Logging Configuration, page 2](#)
- [Enabling and Disabling Message Logging, page 2](#)
- [Setting the Message Display Destination Device, page 3](#)
- [Defining the Message Severity Level, page 4](#)

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

[Table 7](#) describes the elements of syslog messages.

Table 7 System Log Message Elements

Element	Description
<i>seq no:</i>	Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the “Defining the Message Severity Level” section on page -4.
<i>timestamp</i> formats: mm/dd hh:mm:ss	Date and time of the message or event.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 10 on page -6 .
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 9 on page -5 .
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

Default System Message Logging Configuration

[Table 8](#) shows the default system message logging configuration.

Table 8 Default System Message Logging Configuration

Feature	Default Setting
System message logging	Enabled.
System message logging to the console	Disabled.
Console severity	Debugging (and numerically lower levels; see Table 9 on page -5).
Logging file configuration	No filename specified.
Logging buffer size	256 KB.
Logging history size	1 message.
Time stamps	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7 (see Table 10 on page -6).
Server severity	Informational (and numerically lower levels; see Table 9 on page -5).

Enabling and Disabling Message Logging

Message logging is enabled by default, while message logging to the console is disabled by default.

Beginning in privileged EXEC mode, follow these steps to enable or disable message logging.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	logging on	Enable message logging.
3.	exit	Return to privileged EXEC mode.
4.	show running-config or show logging	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Disabling the logging process can slow down the router because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

To disable logging, use the **no logging on** global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable or disable message logging to the console.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	logging console <i>level</i>	Log messages that are not higher than required level to the console. See Table 9 on page -5 for the values and definitions of <i>level</i> .
3.	exit	Return to privileged EXEC mode.
4.	show running-config or show logging	Verify your entries.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable logging to the console, use the **no logging console** global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages. This procedure is optional.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	logging buffered size <i>[size]</i>	Log messages to an internal buffer on the router. The range is 4096 bytes (4 KB) to 10485760 bytes (10 MB). The default buffer size is 256 KB. Note: Do not make the buffer size too large because the router could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the router. However, this value is the maximum available, and the buffer size should <i>not</i> be set to this amount.
3.	logging host <i>host</i> [port port] [transport transport]	Log messages to a UNIX syslog server host. ■ <i>host</i>—Specify the name or IP address of the host to be used as the syslog server. ■ <i>port</i>—Specify the port of the syslog server. If this value is omitted, the default is 514. ■ <i>transport</i>—Specify tcp or udp to transmit the message. If this value is omitted, the default is udp. To build a list of syslog servers that receive logging messages, enter this command more than once. By default, message logging to a remote syslog server is disabled.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer.

To disable logging to the console, use the **no logging console** global configuration command.

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in [Table 9](#).

Beginning in privileged EXEC mode, follow these steps to define the message severity level. This procedure is optional.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	logging console <i>level</i>	Limit messages logged to the console. By default, logging to the console is disabled.
3.	logging trap <i>level</i>	Limit messages logged to the remote syslog servers. By default, remote syslog servers is disabled.
4.	exit	Return to privileged EXEC mode.
5.	show running-config or show logging	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Specifying a *level* causes messages at that level and numerically lower levels to appear at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

Table 9 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 9 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates the following categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the router is affected.
- Output from the **debug** commands, displayed at the **debugging** level. Debug commands are typically used only by the Technical Assistance Center.
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; router functionality is not affected.

Table 10 lists the system facilities supported by the software.

Table 10 Logging Facility Types

Facility Type	Description
LOG_KERN	kernel messages
LOG_USER	user-level messages
LOG_MAIL	mail system
LOG_DAEMON	system daemons
LOG_AUTH	security/authorization messages
LOG_SYSLOG	messages generated internally by syslogd
LOG_LPR	line printer subsystem
LOG_NEWS	network news subsystem
LOG_UUCP	UUCP subsystem
LOG_CRON	clock daemon
LOG_AUTHPRIV	security/authorization messages
LOG_FTP	FTP daemon
LOG_LOCAL0	local use 0
LOG_LOCAL1	local use 1
LOG_LOCAL2	local use 2
LOG_LOCAL3	local use 3
LOG_LOCAL4	local use 4
LOG_LOCAL5	local use 5
LOG_LOCAL6	local use 6
LOG_LOCAL7	local use 7

Displaying the Logging Configuration

To display the logging configuration and the contents of the log buffer, use one or more of the privileged EXEC commands in [Table 11](#):

Table 11 Commands for Displaying Logging Configuration

Command	Purpose
show logging	Displays the contents of the log buffer.
show debugging	Displays the state of each debugging option.
show crashinfo	Displays crash information.

To filter the contents of the log buffer, use the output modifiers in [Table 12](#):

Table 12 Output Modifiers of Show Logging Command

Command	Output Modifier	Purpose
show logging	 include string	Include lines that match.
	 exclude string	Exclude lines that match.
	 begin string	Begin with the line that matches.
	 redirect string	Copy the buffered logging to TFTP, FTP or A local file.

The following example shows the SNMP log:

```
Router# show logging | include snmpd
Jan 1 08:00:04 %snmpd-6-: NET-SNMP version 5.7.1
Jan 1 08:25:13 %snmpd-6-: Received TERM or STOP signal... shutting down...
..
```

The following example shows the state of each debugging option:

```
Router# show debugging
LLDP:
    LLDP packet info debugging is on.
    LLDP errors debugging is on.
```

The following example shows the crash information:

```
Router# show crashinfo

[ 138.520000] Unable to handle kernel NULL pointer dereference at virtual address 00000000
[ 138.520000] pgd = c0004000
[ 138.520000] [00000000] *pgd=00000000
[ 138.520000] Internal error: Oops: 817 [#1]
[ 138.520000] last sysfs file: /sys/devices/virtual/ubi/ubi0/mtd_num
[ 138.520000] Modules linked in: vfat fat
[ 138.520000] CPU: 0 Not tainted (2.6.35.14 #1)
[ 138.520000] PC is at mv_btms_handler+0x13c/0x26c
[ 138.520000] LR is at handle_IRQ_event+0x48/0x120
[ 138.520000] pc : [<c0175d3c>] lr : [<c01a5004>] psr: 60000093
[ 138.520000] sp : c04a7e98 ip : 00000000 fp : c04a7ef4
[ 138.520000] r10: 00021744 r9 : 56251311 r8 : c04aed04
[ 138.520000] r7 : 00000088 r6 : 00000004 r5 : c04d233c r4 : 00000022
[ 138.520000] r3 : c04d24d4 r2 : 00000000 r1 : 00000004 r0 : 00000000
[ 138.520000] Flags: nZCv IRQs off FIQs on Mode SVC_32 ISA ARM Segment kernel
[ 138.520000] Control: 0005397f Table: 1f11c000 DAC: 00000017
[ 138.520000] Process swapper (pid: 0, stack limit = 0xc04a6270)
[ 138.520000] Stack: (0xc04a7e98 to 0xc04a8000)
[ 138.520000] 7e80: c019be08 c04ab1c0
[ 138.520000] 7ea0: c04a7ea0 c04a7ea0 c019be20 00000001 00000004 c04d714c 60000093 00000000
[ 138.520000] 7ec0: 00000008 c04d7150 c04a7f1c dfc29680 00000000 00000000 00000062 00021778
[ 138.520000] 7ee0: 56251311 00021744 c04a7f14 c04a7ef8 c01a5004 c0175c10 c04b2d04 00000062
[ 138.520000] 7f00: 00000000 c04a9e58 c04a7f2c c04a7f18 c01a6994 c01a4fcc c04c0234 00000062
[ 138.520000] 7f20: c04a7f4c c04a7f30 c0026040 c01a6924 60000013 ffffffff 0000001f 00000004
[ 138.520000] 7f40: c04a7fb4 c04a7f50 c0028f70 c0026010 00000000 0005397f 0005297f 60000013
[ 138.520000] 7f60: c04a6000 c04d1b24 c04a6000 c04a9e58 00021778 56251311 00021744 c04a7fb4
[ 138.520000] 7f80: c04a7f98 c04a7f98 c012c214 c012c3bc 60000013 ffffffff c04d99f0 c0022ba4
[ 138.520000] 7fa0: c08f1140 c04a9e50 c04a7fc4 c04a7fb8 c002d338 c012c34c c04a7ff4 c04a7fc8
[ 138.520000] 7fc0: c0008904 c002d2e8 c0008374 00000000 00000000 c0022ba4 00000000 00053975
[ 138.520000] 7fe0: c04d1bd4 c0022ba0 00000000 c04a7ff8 00008034 c00086ec 00000000 00000000
[ 138.520000] Backtrace:
[ 138.520000] [<c0175c00>] (mv_btms_handler+0x0/0x26c) from [<c01a5004>] (handle_IRQ_event+0x48/0x120)
[ 138.520000] [<c01a4fbc>] (handle_IRQ_event+0x0/0x120) from [<c01a6994>]
(handle_level_irq+0x80/0x110)
```

```

[ 138.520000] r7:c04a9e58 r6:00000000 r5:00000062 r4:c04b2d04
[ 138.520000] [<c01a6914>] (handle_level_irq+0x0/0x110) from [<c0026040>] (asm_do_IRQ+0x40/0x90)
[ 138.520000] r5:00000062 r4:c04c0234
[ 138.520000] [<c0026000>] (asm_do_IRQ+0x0/0x90) from [<c0028f70>] (__irq_svc+0x30/0x180)
[ 138.520000] Exception stack(0xc04a7f50 to 0xc04a7f98)
[ 138.520000] 7f40: 00000000 0005397f 0005297f 60000013
[ 138.520000] 7f60: c04a6000 c04d1b24 c04a6000 c04a9e58 00021778 56251311 00021744 c04a7fb4
[ 138.520000] 7f80: c04a7f98 c04a7f98 c012c214 c012c3bc 60000013 ffffffff
[ 138.520000] r6:00000004 r5:0000001f r4:ffffffff r3:60000013
[ 138.520000] [<c012c33c>] (cpu_idle+0x0/0x9c) from [<c002d338>] (rest_init+0x60/0x78)
[ 138.520000] r7:c04a9e50 r6:c08f1140 r5:c0022ba4 r4:c04d99f0
[ 138.520000] [<c002d2d8>] (rest_init+0x0/0x78) from [<c0008904>] (start_kernel+0x228/0x270)
[ 138.520000] [<c00086dc>] (start_kernel+0x0/0x270) from [<00008034>] (0x8034)
[ 138.520000] Code: ea000011 e3a02000 e0843084 e0853103 (e5822000)
[ 138.530000] ---[ end trace 39f8e093c1b90767 ]---
```

Debugging the System

To debug the system, use one or more of the privileged EXEC commands in [Table 13](#):

Table 13 Commands for Debugging the System

Command	Purpose
debug charon	Enable debug charon information.
debug dhcloginet	Enable debug dhclient information.
debug dhcp	Enable debug dhcp information.
debug l2tp	Enable debug l2tp information.
debug lldp errors	Enable debug LLDP errors.
debug lldp packets	Enable debug LLDP packet-related information.
debug ntp	Enable debug ntp information.
debug ppp	Enable debug ppp information.
debug pptp	Enable debug pptp information.
debug snmp	Enable debug SNMP information.

To disable the debugging function, use the **no debug** global configuration command.

The following examples show the LLDP debugging logs:

Router# **debug lldp packets**

```

Jan  1 01:48:53: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:03: %lldpd-7-: LLDP advertisement packet TX'd on intf GigabitEthernet0/1
Jan  1 01:49:05: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:06: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:23: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:33: %lldpd-7-: LLDP advertisement packet TX'd on intf GigabitEthernet0/1
...
```

Router# **debug lldp errors**

```

Jan  1 01:48:35: %lldpd-7-: LLDP unknown tlv type 9 recd - ignoring it
Jan  1 01:48:35: %lldpd-7-: LLDP unknown tlv type 127 recd - ignoring it
...
```



Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

- [Understanding SNMP, page 1](#)
- [Configuring SNMP, page 3](#)
- [Displaying SNMP Status, page 10](#)

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the router. To configure SNMP on the router, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

These sections contain this conceptual information:

- [SNMP Versions, page 1](#)
- [SNMP Agent Functions, page 3](#)
- [SNMP Community Strings, page 3](#)
- [SNMP Notifications, page 3](#)

SNMP Versions

This software release supports these SNMP versions:

- **SNMPv1**—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- **SNMPv2C** replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
 - **SNMPv2**—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
 - **SNMPv2C**—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

- **SNMPv3**—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
 - **Message integrity**—ensuring that a packet was not tampered with in transit
 - **Authentication**—determining that the message is from a valid source
 - **Encryption**—mixing the contents of a package to prevent it from being read by an unauthorized source.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Table 14 identifies the characteristics of the different combinations of security models and levels.

Table 14 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: ■ DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. ■ 3DES 168-bit encryption ■ AES 128-bit, 192-bit, or 256-bit encryption

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- **Get a MIB variable**—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- **Set a MIB variable**—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the router, the community string definitions on the NMS must match at least one of the three community string definitions on the router.

A community string can have one of these attributes:

- **Read-only (RO)**—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- **Read-write (RW)**—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

SNMP Notifications

SNMP allows the router to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword *traps* refers to either traps or informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be re-sent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be re-sent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the router is a concern and notification is not required, use traps.

Configuring SNMP

- [Default SNMP Configuration, page 4](#)
- [Configuring Community Strings, page 4](#)
- [Configuring SNMP Groups and Users, page 5](#)

- [Configuring SNMP Notifications, page 7](#)
- [Setting the Agent Contact and Location Information, page 9](#)
- [SNMP Agent Configuration Example, page 9](#)

Default SNMP Configuration

Table 15 shows the default SNMP configuration.

Table 15 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Enabled.
SNMP trap receiver	None configured.
SNMP traps	Enabled.
SNMP version	If no version keyword is present, the default is Version 1.
SNMPv3 authentication	If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.
SNMP notification type	If no type is specified, all notifications are sent.

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. Optionally, you can specify one or more of these characteristics associated with the string:

- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Beginning in privileged EXEC mode, follow these steps to configure a community string on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	snmp-server community <i>string</i> [view <i>view-name</i>] [ro rw]	Configure the community string. ■ For <i>string</i>, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. ■ (Optional) For view, specify the view record accessible to the community. ■ (Optional) Specify either read-only (ro) if you want authorized management stations to retrieve MIB objects, or specify read-write (rw) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects.
3.	snmp-server view <i>view-name</i> <i>oid-tree</i> { included excluded }	Create or update an SNMP view entry. ■ For <i>view-name</i>, specify the name of the view. ■ For <i>oid-tree</i>, specify MIB view family name with: – OID. For example, .1.3.6.1. – Object name. For example, .internet. ■ Specify either included if MIB family name is included in the view, or excluded if MIB family name is excluded from the view.
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a specific community string, use the **no snmp-server community** *string* global configuration command.

This example shows how to assign the string *public* to SNMP, to allow read-only access:

```
Router(config)# snmp-server community public ro
```

Configuring SNMP Groups and Users

You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	snmp-server group <i>groupname</i> { v1 / v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>]	Configure a new SNMP group on the remote device. ■ For <i>groupname</i>, specify the name of the group. ■ Specify a security model: – v1 is the least secure of the possible security models. – v2c is the second least secure model. It allows transmission of informs and integers twice the normal width. – v3, the most secure, requires you to select an authentication level: auth—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication. noauth—Enables the noAuthNoPriv security level. This is the default if no keyword is specified. priv—Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>). ■ (Optional) Enter read <i>readview</i> with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent. Default read view is v1default. ■ (Optional) Enter write <i>writeview</i> with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent. Default write view is none.
3.	snmp-server user <i>username</i> <i>groupname</i> { v1 / v2c v3 { auth { md5 sha } <i>auth-password</i> }} [<i>priv</i> { des aes } <i>priv-password</i>]	Add a new user for an SNMP group. ■ The <i>username</i> is the name of the user on the host that connects to the agent. ■ The <i>groupname</i> is the name of the group to which the user is associated. ■ Enter the SNMP version number (v1, v2c, or v3). If you enter v3, you have an additional option: – auth—An authentication level setting session that can be either the HMAC-MD5-96 (md5) or the HMAC-SHA-96 (sha) authentication level and requires a password string <i>auth-password</i> (not to exceed 64 characters). ■ If you enter v3, you can also configure a private (priv) encryption algorithm and password string <i>priv-password</i> (not less than 8 alphanumeric characters and not to exceed 64 characters). – <i>priv</i> specifies the User-based Security Model (USM). – des specifies the use of the 56-bit DES algorithm. – aes specifies the use of the AES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.

	Command	Purpose
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries. Note: To display SNMPv3 information about auth noauth priv mode configuration, you must enter the show snmp user privileged EXEC command.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure an snmp group with the name *grp1*:

```
Router(config) # snmp-server group grp1 v3 priv read view1 write view1
```

This example shows how to configure an snmp user *user1*:

```
Router(config) # snmp-server user user1 grp1 v3 auth md5 12345678 priv des 12345678
```

Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the router generates when certain events occur. The following notification types are supported on the router:

- snmp authentication
- snmp linkdown
- snmp linkup

By default, no trap manager is defined, and no traps are sent.

You can enable any or all of these traps and configure a trap manager to receive them. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host host-addr informs** global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure the router to send traps or informs to a host:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	snmp-server user <i>username</i> <i>groupname</i> { v1 v2c v3 [auth { md5 sha } <i>auth-password</i>]} [priv { des aes } <i>priv-password</i>]	Configure an SNMP user.
3.	snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>]	Configure an SNMP group.

	Command	Purpose
4.	snmp-server host <i>host-addr</i> [informs traps] [version { 1 / 2c 3 { auth noauth priv }}] <i>community-string</i> [udp-port <i>port</i>]	Specify the recipient of an SNMP trap operation. ■ For <i>host-addr</i>, specify the name or Internet address of the host (the targeted recipient). ■ (Optional) Enter informs to send SNMP informs to the host. ■ (Optional) Enter traps (the default) to send SNMP traps to the host. ■ (Optional) Specify the SNMP version (1, 2c, or 3). Default is version 1. SNMPv1 does not support informs. ■ (Optional) For Version 3, select authentication level auth, noauth, or priv. Note: The priv keyword is available only when the cryptographic software image is installed. ■ For <i>community-string</i>, when version 1 or version 2c is specified, enter the password-like community string sent with the notification operation. When version 3 is specified, enter the SNMPv3 username. ■ (Optional) For <i>port</i>, specify the UDP port of the notification host. Default is port 162.
5.	snmp-server inform [retries <i>retries</i>] [timeout <i>timeout</i>]	(Optional) Specify SNMP inform request options. For <i>retries</i> , specify the retry count for informs. Default is 3. Valid range is from 0 to 100. For <i>timeout</i> , specify the timeout for informs in seconds. Default is 15 seconds. Valid range is from 0 to 4294967 seconds.
6.	snmp-server enable traps [<i>notification-types</i>]	Enable the router to send traps or informs and specify the type of notifications to be sent. The following notification types are supported on the router: ■ snmp authentication ■ snmp linkdown ■ snmp linkup By default, all supported notification types are enabled.
7.	exit	Return to privileged EXEC mode.
8.	show running-config	Verify your entries. Note To display SNMPv3 information about auth noauth priv mode configuration, you must enter the show snmp user privileged EXEC command.
9.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The **snmp-server host** command specifies which hosts receive the notifications. The **snmp-server enable trap** command globally enables the mechanism for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an **snmp-server host informs** command for the host and globally enable informs by using the **snmp-server enable traps** command.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

This example shows how to enable the router to send all SNMP notification types:

```
Router(config)# snmp-server enable traps snmp
```

This example shows how to configure the host 192.168.1.0 to receive SNMPv2c traps:

```
Router(config)# snmp-server host 192.168.1.0 traps version 2c public
```

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	snmp-server contact <i>text</i>	Set the system contact string. For example: snmp-server contact SystemOperator
3.	snmp-server location <i>text</i>	Set the system location string. For example: snmp-server location Building3
4.	exit	Return to privileged EXEC mode.
5.	show running-config	Verify your entries.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

SNMP Agent Configuration Example

The following example shows how to configure the SNMP agent:

```
Router# configure terminal
Router(config)# snmp-server community public ro
Router(config)# snmp-server community private rw
Router(config)# snmp-server contact SystemOperator
Router(config)# snmp-server location Building3
Router(config)#
Router(config)# snmp-server view view1 .1.3.6.1 included
Router(config)# snmp-server view view1 .1.3.6.1.6.3.15 excluded
Router(config)# snmp-server view view1 .1.3.6.1.6.3.16 excluded
Router(config)# snmp-server group grp1 v3 priv read view1 write view1
Router(config)# snmp-server user user1 grp1 v3 auth md5 12345678 priv des 12345678
Router(config)#
Router(config)# snmp-server enable traps snmp authentication
Router(config)# snmp-server host 192.168.1.0 traps version 2c public
Router(config)# snmp-server host 192.168.1.1 traps version 3 priv user1
Router(config)# exit
```

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. You also can use the other privileged EXEC commands in [Table 16](#) to display SNMP information.

Table 16 Commands for Displaying SNMP Information

Feature	Default Setting
show snmp	Displays SNMP statistics.
show snmp community	Displays all SNMP community access strings.
show snmp contact	Displays SNMP contact information.
show snmp group	Displays SNMP group information.
show snmp host	Displays information configured for SNMP notification operation.
show snmp location	Displays SNMP location information.
show snmp mib	Display a list of the MIB module OIDs registered on the system.
show snmp user	Displays information on each SNMP user name in the SNMP users table. Note: You must use this command to display SNMPv3 configuration information for auth noauth priv mode. This information is not displayed in the show running-config output.
show snmp view	Displays the SNMP view configuration.

You can use the following commands in user mode as well to display SNMP status:

- **show snmp**
- **show snmp contact**
- **show snmp location**

This example shows the SNMP server statistics:

```
Router# show snmp
1 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  11 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  15 Get-next PDUs
  0 Set-request PDUs
1 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  25 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled
SNMP informs: disabled

SNMP agent enabled
```

This example shows the SNMP community:

```
Router# show snmp community
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile      active

Community name: private
Community Index: private
Community SecurityName: private
storage-type: nonvolatile      active
```

This example shows the SNMP group:

Router# show snmp group

```
groupname: kp_grp                security model:v3 auth
readview : kp_view              writeview: kp_view
row status: active
```

This example shows the SNMP host:

Router# show snmp host

```
Notification host: 172.18.60.61 udp-port: 162   type: inform
user: public      security model: v2c

Notification host: 172.18.60.61 udp-port: 150   type: trap
user: kpuser      security model: v3 priv
```

This example shows the SNMP user:

Router# show snmp user

```
User name: kp_user
Engine ID: 800000090300006440F0D281
storage-type: nonvolatile      active
Authentication Protocol: None
Privacy Protocol: None
Group-name: kp_grp
```

This example shows the SNMP views:

Router# show snmp views

```
vldefault .iso - included permanent active
vldefault .iso.org.dod.internet - included permanent active
vldefault .iso.org.dod.internet.snmpV2.snmpModules.snmpUsmMIB - excluded permanent active
vldefault .iso.org.dod.internet.snmpV2.snmpModules.snmpVacmMIB - excluded permanent active
view1 .1.3.6 - included permanent active
```




Configuring IPv4

This chapter describes how to configure IPv4 information on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

- [About IPv4, page 1](#)
- [Configuring IPv4 Address, page 2](#)
- [Configuring IPv4 Static and Default Route, page 4](#)
- [Diagnosing IPv4 Connectivity, page 5](#)
- [Monitoring and Maintaining IPv4 Host Information, page 6](#)

Information in this chapter about configuring IP addresses is specific to IP Version 4 (IPv4). If you plan to enable IP Version 6 (IPv6) forwarding on your router, see [Chapter 15, “Configuring IPv6”](#) for information specific to IPv6 address format and configuration.

About IPv4

You can configure IP on the router to assign IP addresses to network interfaces. When you assign IP addresses, you enable the interfaces and allow communication with the hosts on those interfaces. The router supports the following interfaces: cellular (3G), Wi-Fi, and Gigabit Ethernet.

You can use a subnet to mask the IP addresses. A mask determines to which subnet an IP address belongs. An IP address contains the network address and the host address. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. Subnet masks are 32-bit values that allow the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address.

This section includes the following topics:

- [Address Resolution Protocol](#)
- [ICMP](#)

Address Resolution Protocol

Networking devices and Layer 3 switches and routers use Address Resolution Protocol (ARP) to map IP (network layer) addresses to (Media Access Control [MAC]-layer) addresses which enables IP packets to be sent across networks. Before a device sends a packet to another device, it looks in its own ARP cache to see if there is a MAC address and corresponding IP address for the destination device. If there is no entry, then the source device sends a broadcast message to every device on the network.

Each device compares the IP address to its own. Only the device with the matching IP address replies to the device that sends the data with a packet that contains the MAC address for the device. The source device adds the destination device MAC address to its ARP table for future reference, creates a data-link header and trailer that encapsulates the packet, and proceeds to transfer the data.

When the destination device lies on a remote network that is beyond another device, the process is the same except that the device that sends the data sends an ARP request for the MAC address of the default gateway. After the address is resolved and the default gateway receives the packet, the default gateway broadcasts the destination IP address over the networks connected to it. The device on the destination device network uses ARP to obtain the MAC address of the destination device and delivers the packet. ARP is enabled by default.

To display the ARP table on the router, use the **show ip arp** EXEC command.

This is an example to show IPv4 arp table discovered by the router.

```
Router# show ip arp
Protocol  Address          Hardware Addr    Interface        state
Internet  172.18.60.254     9c:4e:20:bf:a1:d1 GibitEthernet0/1 REACHABLE
Internet  172.18.60.128     00:22:bd:d8:1e:28 GibitEthernet0/1 REACHABLE
```

ICMP

You can use the Internet Control Message Protocol (ICMP) to provide message packets that report errors and other information that is relevant to IP processing. ICMP generates error messages, such as ICMP destination unreachable messages, ICMP Echo Requests (which send a packet on a round trip between two hosts), and Echo Reply messages. ICMP also provides many diagnostic functions and can send and redirect error packets to the host. By default, ICMP is enabled on the router.

Some of the ICMP message types are as follows:

- Network error messages
- Network congestion messages
- Troubleshooting information
- Timeout announcements

Configuring IPv4 Address

This section includes the following topics:

- [Assigning IP Address to a VLAN Interface](#)
- [Assigning IP Address to the GE Interface](#)
- [Assigning IP Address to the Dot11Radio Interface](#)

Assigning IP Address to a VLAN Interface

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to a VLAN interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface vlan <i>vlan-id</i>	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The VLAN range is 1 to 4094.
3.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.
4.	exit	Return to global configuration mode.
5.	show interfaces <i>vlan vlan-id</i>	Verify the configured IP address.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the router IP address, use the **no ip address** interface configuration command. If you are removing the address through a Telnet session, your connection to the router will be lost.

The following example shows a VLAN interface status and configuration:

```
Router# show ip interface vlan 1
vlan1 is up, line protocol is up
Internet address is 172.18.60.209
Mask is 255.255.0.0
Broadcast address is 172.18.255.255
MTU is 1500 bytes
ICMP redirects are enabled
Proxy ARP is disabled
```

Assigning IP Address to the GE Interface

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to the Gigabit Ethernet interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface GigabitEthernet <i>interface_number</i>	Enter GE interface configuration mode, and enter interface number.
3.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.
4.	exit	Return to global configuration mode.
5.	show ip interfaces GigabitEthernet <i>interface_number</i>	Verify the configured IP address.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the router IP address, use the **no ip address** interface configuration command.

The following example shows a Gigabit Ethernet interface status and configuration:

```
Router# show ip interface GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
Internet address is 172.18.60.202
Mask is 255.255.0.0
Broadcast address is 172.18.255.255
MTU is 1500 bytes
ICMP redirects are enabled
Proxy ARP is disabled
```

Assigning IP Address to the Dot11Radio Interface

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to a dot11radio interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface dot11radio <i>interface_number</i>	Enter dot11radio interface configuration mode, and enter interface number.
3.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.

	Command	Purpose
4.	exit	Return to global configuration mode.
5.	show ip interfaces dot11radio <i>interface_number</i>	Verify the configured IP address.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the router IP address, use the **no ip address** interface configuration command.

The following example shows a dot11radio interface status and configuration:

```
Router# show ip interface dot11radio 0
line protocol is up
Internet address is 172.18.60.204
Mask is 255.255.0.0
Broadcast address is 172.18.255.255
MTU is 1500 bytes
ICMP redirects are enabled
Proxy ARP is disabled
```

Configuring IPv4 Static and Default Route

This chapter includes the following sections:

- [Information About Static Routing](#)
- [Configuring Default Static Route](#)

Information About Static Routing

Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Static routes, which define explicit paths between two routers, cannot be automatically updated. Static routes must be manually configured when network changes occur. Static routes use less bandwidth than dynamic routes. Additionally, the router uses no CPU cycles when calculating and analyzing routing updates.

Configuring Default Static Route

A default route identifies the gateway IP address to which the router sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.

Beginning in privileged EXEC mode, follow these steps to configure an IPv4 default router for an interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ip route 0.0.0.0 0.0.0.0 <i>interface_type</i> <i>interface_number</i> [<i>gateway_ip</i>] [Metric <i>metric_value</i>]	Configures a default static route and the interface for this route. You can optionally configure the default gateway address. ■ For <i>interface_type interface_number</i>, choose the default route interface. ■ For <i>gateway_ip</i>, specify default gateway. ■ For <i>metric_value</i>, specify the default route metric. Default value is 1. The metric value can be from 1 to 254.
3.	exit	Return to global configuration mode.
4.	show ip route	Verify the configuration.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the default router, use the **no ip route** privileged EXEC command.

The following example configures a default route for the GigabitEthernet interface 0/1 when the IP address of the interface is static IP address:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 172.18.60.254 Metric 1
```

The following example configures a default route for the GigabitEthernet interface 0/1 when the IP address of the interface is obtained by DHCP:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 Metric 1
```

The following example deletes a default route from the GigabitEthernet interface 0/1:

```
Router(config)# no ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1
```

The following example sets the cellular interface as a backup route and VLAN interface as a primary route:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 cellular 0 Metric 2
Router(config)# ip route 0.0.0.0 0.0.0.0 Vlan 1 172.18.60.254 Metric 1
```

Diagnosing IPv4 Connectivity

Table 17 shows the privileged EXEC commands for diagnosing IPv4 network connectivity on the router.

Table 17 Commands for Monitoring IPv4

Command	Purpose
ping [ip] [hostname ip_address] [repeat repeat-count size datagram-size source [interface-name source-address]]	Ping a remote host through IPv4. ■ (Optional) Specify repeat count. Default is 5 times. ■ (Optional) Specify datagram size. Default is 56 bytes. ■ (Optional) Specify source address. Default is none.
tracert [ip] [hostname ip_address]	Traceroute a remote host through IPv4.

Monitoring and Maintaining IPv4 Host Information

You can display specific statistics, such as the contents of IP routing tables, caches, and databases; the reachability of nodes; and the routing path that packets are taking through the network. [Table 18](#) lists the privileged EXEC commands for displaying IPv4 statistics.

Table 18 Commands to Monitor IPv4 Host Information

Command	Purpose
show hosts	Display the default domain name, style of lookup service, name server hosts, and the cached list of hostnames and addresses.
show ip arp	Display the IP ARP cache.
show ip interface <i>interface-type interface-id</i>	Display the IP status of interfaces.
show ip route [<i>address [mask]</i>] [<i>protocol</i>]	Display the current state of the routing table.
show ip traffic	Display IP traffic statistics.
show interfaces	Display interface status and configuration.

The following example shows the output of the **show interfaces** command:

```
Router# show interfaces
Vlan is administratively down, line protocol is down
  Hardware address is , Internet address is
  MTU is 1500 bytes
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
dot11radio0 line protocol is down
  Hardware address is 00:22:58:2E:CE:74 , Internet address is
  MTU is 1500 bytes
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
GigabitEthernet0/1 is up, line protocol is up
  Hardware is Combo Gigabit Ethernet and SFP Slot, address is 3C:CE:73:A4:E6:00
  MTU is 1500 bytes
  duplex 1000M, speed full, media type is Combo
  RX packets:4314 errors:0 dropped:0 overruns:0 frame:0
  TX packets:2814 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:532
  RX bytes:672661 (656.8 KiB) TX bytes:2894793 (2.7 MiB)
```

The following example shows the output of the **show ip traffic** command:

```
Router# show ip traffic
IP statistics:
  Rcvd: 75586 total, 0 format errors,
        0 bad hop count 1639 unknown protocol
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 couldn't fragment
  Sent: 2929 generated, 0 forwarded

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors
        211 unreachable
        0 echo request, 288 echo reply
  Sent: 0 redirects, 0 unreachable
        0 echo request, 25 echo reply
```

```
0 mask requests, 0 mask replies
0 quench,288 timestamp
548 time exceeded,0 parameter problem
```

```
TCP statistics:
  Rcvd:  6 total
  Sent: 111 total
```

```
UDP statistics:
  Rcvd: 1495 input, 0 errors
        212 no port
  Sent: 1749 output
```

The following example shows the output of the **show hosts** command:

```
Router# show hosts
Host Address
nameserver 172.18.32.5
nameserver 172.18.32.219
...
```




Configuring IPv6

This chapter describes how to configure IPv6 information on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

For information about configuring IPv4 on the router, see [Chapter 14, “Configuring IPv4.”](#)

This chapter consists of these sections:

- [Understanding IPv6, page 1](#)
- [Configuring IPv6, page 5](#)
- [Diagnosing IPv6 Connectivity, page 8](#)
- [Displaying and Monitoring IPv6, page 9](#)

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as exit-to-exit security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.

This section describes IPv6 implementation on the router. These sections are included:

- [IPv6 Addresses, page 1](#)
- [Supported IPv6 Unicast Routing Features, page 1](#)

IPv6 Addresses

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

```
2031:0000:130F:0000:0000:09C0:080F:130B
```

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

```
2031:0:130F:0:0:9C0:80F:130B
```

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

```
2031:0:130F::09C0:080F:130B
```

Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the router:

- [128-Bit Wide Unicast Addresses, page 2](#)
- [DNS for IPv6, page 2](#)

- [ICMPv6, page 2](#)
- [Neighbor Discovery, page 3](#)
- [Default Router Preference, page 3](#)
- [IPv6 Stateless Autoconfiguration and Duplicate Address Detection, page 3](#)
- [IPv6 Applications, page 3](#)
- [Static Routes for IPv6, page 3](#)
- [Dual IPv4 and IPv6 Protocol Stacks, page 3](#)
- [DHCP for IPv6 Address Assignment, page 4](#)
- [SNMP and Syslog Over IPv6, page 4](#)
- [HTTP\(S\) Over IPv6, page 4](#)

128-Bit Wide Unicast Addresses

The router supports aggregatable global unicast addresses, link-local unicast addresses, and Unique Local Address (ULA). It does not support site-local unicast addresses. ULA will replace it.

- Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider. These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.
- Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless auto-configuration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.
- Unique Local Address (ULA) is an IPv6 unicast address that is globally unique and is intended for local communications. They are not expected to be routable on the global Internet and are routable inside of a limited area, such as a site. They may also be routed between a limited set of sites. It addresses with a prefix of FC00::/7.

DNS for IPv6

IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an address record in IPv4. The router supports DNS resolution for IPv4 and IPv6.

The statically assigned DNS address has the highest priority than others dynamically assigned DNS address. The priority order in the system is static, IPsec, PPP0-PPP255 (L2TP, PPTP), PPPoE, DHCP, and DHCPv6.

ICMPv6

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.

Neighbor Discovery

The router supports NDP for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that do not support NDP. The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), to verify the reachability of the neighbor, and to keep track of neighboring routers.

The router supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for host routes or for summarized routes with mask lengths greater than 64 bits.

Default Router Preference

The router supports IPv6 default router preference (DRP), an extension in router advertisement messages. DRP improves the ability of a host to select an appropriate router, especially when the host is multihomed and the routers are on different links. The router does not support the Route Information Option in RFC 4191.

An IPv6 host maintains a default router list from which it selects a router for traffic to offlink destinations. The selected router for a destination is then cached in the destination cache. NDP for IPv6 specifies that routers that are reachable or probably reachable are preferred over routers whose reachability is unknown or suspect. For reachable or probably reachable routers, NDP can either select the same router every time or cycle through the router list. By using DRP, you can configure an IPv6 host to prefer one router over another, provided both are reachable or probably reachable.

IPv6 Stateless Autoconfiguration and Duplicate Address Detection

The router uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send router solicitations to request router advertisements for configuring interfaces.

IPv6 Applications

The router has IPv6 support for these applications:

- Ping, traceroute, Telnet, and TFTP
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA over IPv4 transport
- SNMP support for IPv6

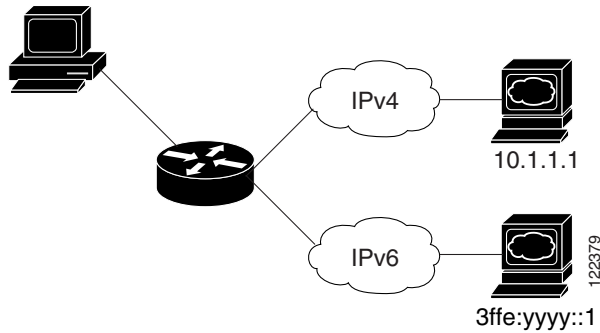
Static Routes for IPv6

Static routes are manually configured and define an explicit route between two networking devices. Static routes are useful for smaller networks with only one path to an outside network or to provide security for certain types of traffic in a larger network.

Dual IPv4 and IPv6 Protocol Stacks

When a device has dual stack capabilities, it can use both IPv4 and IPv6 technologies to connect to remote servers and destinations in parallel.

Figure 1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.

Figure 1 Dual IPv4 and IPv6 Support on an Interface

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

SNMP and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6
- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
- SNMP- and syslog-related MIBs to support IPv6 addressing
- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings
- Provides a new transport mechanism called *SR_IPV6_TRANSPORT*
- sends SNMP notifications over IPv6 transport
- Supports SNMP-named access lists for IPv6 transport
- Supports SNMP proxy forwarding using IPv6 transport
- Verifies SNMP Manager feature works with IPv6 transport

HTTP(S) Over IPv6

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.

The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.

The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (**ping**) must exist between the client and the server hosts before HTTP connections can be made.

Configuring IPv6

These sections contain this IPv6 forwarding configuration information:

- [Configuring IPv6 Addressing and Enabling IPv6 Routing](#)
- [Configuring DHCP for IPv6 Address Assignment](#)
- [Configuring Default Static Routes for IPv6](#)

Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the router.

In the **ipv6 address** interface configuration command, you must enter the *ipv6-address* and *ipv6-prefix* variables with the address specified in hexadecimal using 16-bit values between colons. The *prefix-length* variable (preceded by a slash [/]) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02:0:0:0:0:1:ff00::/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)
- all-nodes link-local multicast group FF02::1
- all-routers link-local multicast group FF02::2

Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Enter interface configuration mode, and specify the Layer 3 interface to configure. The interface can be a physical interface, a router virtual interface (SVI), or a Layer 3 EtherChannel.
3.	ipv6 address eui-64 <i>ipv6-prefix/prefix length</i> or ipv6 address link-local <i>ipv6-address</i> or ipv6 address autoconf	Specify a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the router MAC address. Specify a link-local address on the interface to be used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. Specify automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
4.	exit	Return to global configuration mode.
5.	exit	Return to privileged EXEC mode.
6.	show ipv6 interface <i>interface-id</i>	Verify your entries.
7.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove an IPv6 address from an interface, use the **no ipv6 address** *ipv6-prefix/prefix length eui-64* or **no ipv6 address link-local** *ipv6-address* interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** interface configuration command without arguments.

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8:c18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the **show ipv6 interface** EXEC command shows how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Router(config)# interface GigabitEthernet 0/1
Router(config-if)# ipv6 address eui-64 2001:0DB8:c18:1::/64
Router(config-if)# exit
Router# show ipv6 interface GigabitEthernet 0/1
GigabitEthernet 0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
Joined group address(es):
FF02::1
FF02::2
FF02::1:FE2F:D940
MTU is 1500 bytes
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
Hosts use stateless autoconfig for addresses.
```

Configuring DHCP for IPv6 Address Assignment

These sections describe how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address assignment:

- [Enabling DHCPv6 Server Function](#)
- [Enabling DHCPv6 Client Function](#)

Enabling DHCPv6 Server Function

See the [“Configuring Stateful DHCPv6 Server” section on page -3](#) and [“Configuring Stateless DHCPv6 Server” section on page -3](#) for detailed information about enabling DHCPv6 server function.

Enabling DHCPv6 Client Function

Beginning in privileged EXEC mode, follow these steps to enable DHCPv6 client function on an interface.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to configure.
3.	ipv6 address dhcp	Enable the interface to acquire an IPv6 address from the DHCPv6 server.
4.	exit	Return to privileged EXEC mode.
5.	show ipv6 dhcp interface	Verify that the DHCPv6 client is enabled on an interface.

To disable the DHCPv6 client function, use the **no ipv6 address dhcp** interface configuration command.

This example shows how to acquire an IPv6 address:

```
Router(config)# interface gigabitethernet 0/1  
Router(config-if)# ipv6 address dhcp
```

Configuring Default Static Routes for IPv6

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 static route:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	ipv6 route ::/0 {interface-type / interface-id [ipv6_next_hop_address]} [administrative_distance]	Configure a static IPv6 route. ■ <i>interface-type</i>—Specify the interface type. ■ <i>ipv6_next_hop_address</i>—The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be specified in hexadecimal using 16-bit values between colons. ■ <i>interface-id</i>—Specify direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent. Note: You must specify an <i>interface-id</i> when using a link-local address as the next hop (the link-local next hop must also be an adjacent router). ■ <i>administrative_distance</i>—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over any other type of route except connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.
3.	exit	Return to privileged EXEC mode.
4.	show ipv6 route	Verify your entries by displaying the contents of the IPv6 routing table.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a configured static route, use the **no ipv6 route** global configuration command.

This example shows how to configure a default static route with an administrative distance of 130 to an interface:

```
Router(config)# ipv6 route ::/0 gigabitethernet 0/1 130
```

Diagnosing IPv6 Connectivity

Table 20 shows the privileged EXEC commands for diagnosing IPv6 network connectivity on the router.

Table 19 Commands for Monitoring IPv6

Command	Purpose
ping ipv6 [<i>hostname</i> <i>ip_address</i>] [repeat <i>repeat-count</i> size <i>datagram-size</i> source [<i>interface-name</i> <i>source-address</i>]	Ping a remote host through IPv6. ■ (Optional) Specify repeat count. Default is 5 times. ■ (Optional) Specify datagram size. Default is 56 bytes. ■ (Optional) Specify source address. Default is none. Note If you ping IPv6 link-local at first time, the source option is required.
traceroute ipv6 [<i>hostname</i> <i>ip_address</i>]	Traceroute a remote host through IPv6.

The following example shows a sample output of the **ping ipv6** command:

```
Router# ping ipv6 2001:db8:2::1234 source 2001:db8:2:0:8a75:56ff:fe27:4d01
PING 2001:db8:2::1234 (2001:db8:2::1234) from 2001:db8:2:0:8a75:56ff:fe27:4d01: 56 data bytes
64 bytes from 2001:db8:2::1234: seq=0 ttl=64 time=0.825 ms
64 bytes from 2001:db8:2::1234: seq=1 ttl=64 time=0.714 ms
64 bytes from 2001:db8:2::1234: seq=2 ttl=64 time=0.682 ms
64 bytes from 2001:db8:2::1234: seq=3 ttl=64 time=0.652 ms
64 bytes from 2001:db8:2::1234: seq=4 ttl=64 time=0.687 ms
```

Displaying and Monitoring IPv6

Table 20 shows the privileged EXEC commands for monitoring IPv6 on the router.

Table 20 Commands for Monitoring IPv6

Command	Purpose
show hosts	Display IPv4/IPv6 DNS server.
show ipv6 interface <i>interface-id</i>	Display IPv6 interface status and configuration.
show ipv6 neighbors	Display IPv6 neighbor cache entries.
show ipv6 prefix-list	Display a list of IPv6 prefix lists.
show ipv6 route	Display the IPv6 route table entries.
show ipv6 traffic	Display IPv6 traffic statistics.
show ip http server connection	Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.

This is an example of the output from the **show ipv6 interface** privileged EXEC command:

```
Router# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF2F:D940
MTU is 1500 bytes
```

```
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
<output truncated>
```

This is an example of the output from the **show ipv6 neighbor** privileged EXEC command:

```
Router# show ipv6 neighbors
IPv6 Address Interface Link-layer-Addr Device State
fe80::20c:29ff:fe8c:27da gigabitethernet0/1 00:0c:29:8c:27:da router STALE
```

This is an example of the output from the **show ipv6 traffic** privileged EXEC command.

```
Router# show ipv6 traffic
IPv6 statistics:
  Rcvd:  7 total
         0 truncated
         0 bad header, 0 bad source
         0 unknown protocol, 0 not a router
         0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  8 generated, 0 forwarded
         0 no route,
Mcast:  7 received, 14 sent

ICMP statistics:
  Rcvd:  7 input, 0 input error
         0 unreachable
         0 parameter problems
         0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         7 router solicit, 0 router advert, 0 redirects
         0 neighbor solicit, 0 neighbor advert
  Sent:  8 output
         0 unreachable
         0 parameter problems
         0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 0 router advert, 0 redirects
         2 neighbor solicit, 0 neighbor advert
```



Configuring NAT

This chapter provides conceptual information about network address translation (NAT) configuration and management of NAT on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

- [Understanding Network Address Translation, page 1](#)
- [Configuring NAT, page 2](#)
- [Configuring Port Forwarding, page 3](#)
- [Monitoring NAT Information, page 3](#)

Understanding Network Address Translation

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. As part of the process, the device also records the substitution in a translation database; these records are known as “xlate” entries. The appropriate xlate entry must exist to allow address translation on return packets—the substitution of the original real address for the mapped address; this procedure is sometimes referred to as “untranslation.” Thus, network address translation (NAT) actually consists of two steps: the translation of a real address into a mapped address, and the reverse translation for returning traffic.

One of the main functions of NAT is to enable private IP networks to connect to the Internet. Network address translation replaces a private IP address with a public IP address, translating the private addresses in the internal network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses; for example, NAT rules can be configured to utilize only one public address for the entire network in communications with the outside world.

In the deployment of Cisco 910 Industrial Routers, multiple slave IR910 routers can be connected to the LAN behind the master IR910 router. Before the traffic from these slave routers is sent to Internet, it can be encrypted and filtered.

Configuring NAT

Beginning in privileged EXEC mode, follow these steps to configure NAT on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>type number</i>	Enter interface configuration mode. For <i>type</i> , choose one of the following interfaces as an outside interface: ■ dot11radio (only available for Wi-Fi model IR910W-K9) ■ cellular (only available for 3G models IR910G-K9 and IR910G-NA-K9) ■ Dialer ■ GigabitEthernet For <i>number</i> , enter the interface number.
3.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.
4.	ip nat outside	Identify the specified interface as the NAT outside interface.
5.	exit	Return to global configuration mode.
6.	interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
7.	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.
8.	ip nat inside	Identify the VLAN interface as the NAT inside interface.
9.	exit	Return to global configuration mode.
10.	ip nat inside source <i>inside-network inside-network mask outside-interface-name interface-number overload</i>	Enable dynamic translation of addresses on the inside interface. Outside interface should be dot11radio, cellular, dialer, or Gigabit Ethernet. Dot11radio interface is only available for Wi-Fi model IR910W-K9 and cellular interface is only available for 3G models IR910G-K9 and IR910G-NA-K9.
11.	exit	Return to global configuration mode.
12.	show ip nat translation	Verify the configuration.
13.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure NAT on a IR910W-K9 router:

```
Router# configure terminal
Router(config)# interface dot11radio 0
Router(config-if)# ip address 200.1.1.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface vlan 1
Router(config-if)# ip address 192.168.3.254 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip nat inside source 192.168.3.0 255.255.255.0 dot11radio 0 overload
Router(config)# exit
```

Configuring Port Forwarding

Port forwarding is a NAT function that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway.

Use the following command to configure port forwarding:

```
ip nat inside { static { tcp | udp | sctp } inside_network_address | source inside_network_address }
```

Syntax Description

static	Port Forwarding Configuration.
source	Source address translation.

Monitoring NAT Information

You can display specific statistics and the translation table of NAT. [Table 21](#) lists the privileged EXEC commands for displaying NAT information.

Table 21 Commands to Monitor NAT Information

Command	Purpose
show ip nat statistics	Display the statistics information of NAT configuration.
show ip nat translation	Display the translation table.

The following example shows the output of the **show ip nat statistics** command:

```
Router# show ip nat statistics
Total Active Translations: 0
Inside Interface: vlan 1
Inside Source: 192.168.0.1/24
Outside Interface: dot11radio 0
```

The following example shows the output of the **show ip nat translation** command:

```
Router# show ip nat translation
Proto NATed Address NAT-host Address Destination Address
icmp 10.0.1.220 192.168.3.168 192.168.3.254
tcp 10.0.1.220 192.168.3.168 192.168.3.254
```




Configuring PPPoE

This section describes how to configure the Point-to-Point over Ethernet (PPPoE) client on the Cisco 910 Industrial Routers (*hereafter* referred to as the router). It includes the following topics:

- [PPPoE Client Overview, page 1](#)
- [Configuring PPPoE, page 1](#)
- [Monitoring the PPPoE Client, page 3](#)

PPPoE Client Overview

The Point-to-Point over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frame. PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems.

The Cisco 910 Industrial Router can be configured as a PPPoE client, so that a tunnel can be established for the router to access the WAN.

At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Configuring PPPoE

This section contains the following information:

- [Configuring VPDN Group, page 2](#)
- [Configuring Ethernet WAN Interface, page 2](#)
- [Configuring the Dialer Interface, page 2](#)
- [Connecting to the PPPoE Service, page 3](#)

Configuring VPDN Group

Beginning in privileged EXEC mode, follow these steps to configure the VPDN group:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	vpdn-group <i>number</i>	Create and associate a Virtual Private Dialup Network (VPDN) group with a customer or VPDN profile. For <i>number</i> , enter the group number.
3.	request dialin	Create a request dial-in VPDN subgroup that configures the router to request the establishment of a dial-in tunnel to a tunnel server, and enters VPDN request-dialin group configuration mode.
4.	protocol pppoe	Specify the PPPoE tunneling protocol that a VPDN subgroup will use.
5.	exit	Return to global configuration mode.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring Ethernet WAN Interface

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet WAN interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface <i>type number</i>	Enter interface configuration mode for the WAN interface.
3.	pppoe-client dial-pool-number <i>number</i>	Configure the PPPoE client and specifies the dialer interface to use for cloning
4.	exit	Return to global configuration mode.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the Dialer Interface

Beginning in privileged EXEC mode, follow these steps to configure the dialer interface:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface dialer <i>number</i>	Enter interface configuration mode for the dialer interface.
3.	ip address negotiated	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.
4.	dialer-pool <i>number</i>	Specify the dialer pool to use to connect to a specific destination subnetwork.
5.	dialer-group <i>number</i>	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
6.	ppp authentication chap	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP)
7.	ppp chap hostname <i>username</i>	Define an interface-specific CHAP hostname.

	Command	Purpose
8.	ppp chap password <i>password</i>	Define an interface-specific CHAP password.
9.	exit	Return to global configuration mode.
10.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Connecting to the PPPoE Service

Beginning in privileged EXEC mode, follow these steps to connect to the PPPoE service:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	pppoe <i>profile_name</i>	Connect to the PPPoE service. For <i>profile_name</i> , specify the target tunnel profile.
3.	exit	Return to global configuration mode.
4.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disconnect from the PPPoE service, use the **no pppoe** privileged EXEC command.

Monitoring the PPPoE Client

Use the **show interface Dialer** global configuration command to display the dialer interface statistics. The following example shows a sample output of the **show interface Dialer** command:

```
Router# show interface Dialer 0
Link encap:Point-to-Point Protocol
inet addr:10.100.11.16 P-t-P:10.100.11.10 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
RX packets:10 errors:0 dropped:0 overruns:0 frame:0
TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:125 (125.0 B) TX bytes:113 (113.0 B)
```




Configuring VPN

This chapter provides conceptual information about Virtual Private Networks (VPN) configuration and management on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

- [Understanding VPN Connection Types, page 1](#)
- [Configuring PPTP, page 2](#)
- [Configuring IPsec, page 4](#)
- [Configuring L2TP, page 6](#)

Understanding VPN Connection Types

As a machine-to-machine (M2M) gateway, the router collects the information reported by every sensor. The reported information should be protected when it is transferred through Internet. In a typical deployment scenario of the router, the main purpose of VPN is to provide a security path for transporting sensor data to admin.

The following VPN connection types are supported on the router:

- [PPTP, page 1](#)
- [IPsec, page 1](#)
- [L2TP, page 2](#)

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol which allows a remote client to use a public IP network in order to communicate securely with servers at a private corporate network. PPTP tunnels the IP.

IPsec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (site-to-site), or between a security gateway and a host (remote-access).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffics over an IP network. Applications can be automatically secured by its IPsec at the IP layer. Without IPsec, the protocols of TLS/SSL must be inserted under each of applications for protection.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

L2TP with IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. By using L2TP with IPsec, L2TP packets between the endpoints are encapsulated by IPsec.

The configuration of L2TP with IPsec supports certificates using the preshared keys or RSA signature methods.

Configuring PPTP

Beginning in privileged EXEC mode, follow these steps to configure PPTP on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	crypto vpn {l2tp ipsec pptp l2tp_ipsec} <i>profile-name</i>	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For <i>profile-name</i> : enter the target tunnel profile or name. Note: The command should be activated again if the profile configuration is changed. Note: Use “no crypto vpn” to disconnect from a VPN tunnel.
3.	vpdn-group <i>name</i>	Associates a VPDN group with a customer or VPDN profile.
4.	request dialin	Create a request dial-in VPDN subgroup that configures the router to request the establishment of a dial-in tunnel to a tunnel server, and enters VPDN request-dialin group configuration mode.
5.	protocol pptp	Specifies the tunneling protocol that a VPDN subgroup will use.
6.	initiate-to <i>ip-address</i>	Specifies the IP address (VPN server) that will be tunneled to.
7.	interface dialer <i>number</i>	Create a Dialer interface. The interface number will fall within the scope of 0~255
8.	ip address negotiated	Specify that the IP address for a particular interface is obtained via PPP/PCP address negotiation.
9.	dialer-group <i>number</i>	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
10.	ppp authentication chap	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP)
11.	ppp chap hostname <i>username</i>	Define an interface-specific CHAP hostname.
12.	ppp chap password <i>password</i>	Define an interface-specific CHAP password.
13.	ppp encrypt mppe auto	Enable Microsoft Point-to-Point Encryption (MPPE) on the virtual template.
14.	exit	Return to global configuration mode.
15.	show interface Dialer <i>interface-number</i>	(Optional) Show interface statistics.

	Command	Purpose
16.	show vpdn tunnel pptp	(Optional) Display details about PPTP active VPDN tunnel.
17.	show vpdn session pptp	(Optional) Display details about PPTP active VPDN session.
18.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure PPTP client on the router:

```
Router# configure terminal
Router(config)# vpdn-group 2
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol pptp
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to 172.19.66.181
Router(config-vpdn)# exit
Router(config)# interface Dialer 2
Router(config-if)# ip address negotiated
Router(config-if)# dialer-group 2
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp authentication ms-chap-v2
Router(config-if)# ppp chap hostname vpn
Router(config-if)# ppp chap password cisco123
Router(config-if)# exit
```

The following example shows a sample output of the **show interface Dialer** command:

```
Router# show interface dialer 2
Dialer2 Link encap:Point-to-Point Protocol
    inet addr:192.168.3.148 P-t-P:192.168.3.148 Mask:255.255.255.255
    UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1396 Metric:1
    RX packets:12 errors:0 dropped:0 overruns:0 frame:0
    TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:3
    RX bytes:210 (210.0 B) TX bytes:102 (102.0 B)
```

The following example shows a sample output of the **show vpdn tunnel pptp** command:

```
Router# show vpdn tunnel pptp
PPTP Tunnel Information Total tunnels 1 Sessions 1
  Remote Address      Port      Sessions  State
  192.168.1.2         1723      1         established
```

The following example shows a sample output of the **show vpdn session pptp** command:

```
Router# show vpdn session pptp
PPTP Tunnel Information Total tunnels 1 Sessions 1
  Interface  Local Address  Username  State
  Dialer20   192.168.1.6    cisco_client  established
```

Configuring IPsec

Beginning in privileged EXEC mode, follow these steps to configure IPsec on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	crypto vpn {l2tp ipsec pptp l2tp_ipsec} profile-name	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For <i>profile-name</i>: enter the target tunnel profile or name. Note: The command should be activated again if the profile configuration is changed. Note: Use “no crypto vpn” to disconnect from a VPN tunnel.
3.	crypto isakmp profile name	Set IPsec VPN profile.
4.	set peer {address ip-address host fqdn-hostname}	Set peer VPN ip address.
5.	self-identity {address ip-address user-fqdn fqdn-hostname}	(Optional) To define the ISAKMP identity used by the router when participating in the Internet Key Exchange (IKE) protocol. Default value is the WAN IP address of the router. For <i>ip-address</i>: set the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations. For <i>fqdn-hostname</i>: set the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com). Note: Self-identity is not supported in main mode.
6.	match identity {address ip-address user-fqdn fqdn-hostname}	(Optional) To define the ISAKMP identity used by the peer server when participating in the Internet Key Exchange (IKE) protocol. Default value is the WAN IP address of the peer server. For <i>ip-address</i>: set the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations. For <i>fqdn-hostname</i>: set the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com). Note: Self-identity is not supported in main mode.
7.	match address {remote-access site-to-site local-subnet local-netmask peer-subnet peer-netmask}	(Optional) Define the VPN type. If the option is not set, default value is host-to-host.
8.	initiate mode {aggressive main}	(Optional) Define the ISAKMP operation mode. Default value is main mode.
9.	keepalive seconds	(Optional) Set the number of seconds between DPD messages. The range is from 10 to 3600 seconds. The connection would be dropped after 5 messages. Default value is 30s.

	Command	Purpose
10.	xauth-identity <i>name</i> xauth-password <i>password</i>	(Optional) Set Xauth identity name and password. If the option is set, xauth would be enabled. Note: Xauth is not supported for site-to-site type.
11.	policy authentication { pre-share rsa-sig }	Set authentication for ISAKMP to pre-shared key or certificate authentication. Note: Certificate is not supported for aggressive mode. It works only for the main mode.
12.	passphrase <i>password-phrase</i>	(Optional) Set rsa-sig private key pass phrase.
13.	pre-share-key <i>keystring</i>	(Optional) Set pre-share key value.
14.	exit	Return to global configuration mode.
15.	show crypto isakmp sa	(Optional) Display details about ISAKMP SA.
16.	show crypto ipsec sa	(Optional) Display details about IPsec SA.
17.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Table 22 shows the limitations of the IPsec configuration.

Table 22 Limitations of the IPsec Configuration

	main	aggressive	main and Xauth	aggressive and Xauth
remote-access-psk	No	Yes	Yes	Yes
remote-access-rsa	No	No	Yes	No
site-to-site-psk	Yes	Yes	No	No
site-to-site-rsa	Yes	No	No	No

The following example shows how to configure IPsec remote-access type with RSA authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile remote-access-cert
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address remote-access
Router(config-ipsec-pf)# xauth-identity justin xauth-password cisco123
Router(config-ipsec-pf)# policy authentication rsa-sig
Router(config-ipsec-pf)# passphrase 123456
Router(config-ipsec-pf)# exit
Router(config)#
```

The following example shows how to configure IPsec remote-access type with PSK authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile remote-access-psk
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# self-identity user-fqdn access
Router(config-ipsec-pf)# initiate mode aggressive
Router(config-ipsec-pf)# match address remote-access
Router(config-ipsec-pf)# policy authentication pre-share
Router(config-ipsec-pf)# pre-share-key cisco123
Router(config-ipsec-pf)# xauth-identity justin xauth-password cisco123
Router(config-ipsec-pf)# exit
Router(config)#
```

The following example shows how to configure IPsec site-to-site type with RSA authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile site2site-cert
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address site-to-site 192.168.30.0 255.255.255.0 192.168.20.0
255.255.255.0
Router(config-ipsec-pf)# initiate mode main
Router(config-ipsec-pf)# policy authentication rsa-sig
Router(config-ipsec-pf)# passphrase 123456
Router(config-ipsec-pf)# exit
Router(config)#
```

The following example shows how to configure IPsec site-to-site type with PSK authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile site2site-psk
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address site-to-site 192.168.30.0 255.255.255.0 192.168.20.0
255.255.255.0
Router(config-ipsec-pf)# initiate mode main
Router(config-ipsec-pf)# policy authentication pre-share
Router(config-ipsec-pf)# pre-share-key cisco123
Router(config-ipsec-pf)# exit
Router(config)#
```

Configuring L2TP

Beginning in privileged EXEC mode, follow these steps to configure L2TP on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	crypto vpn {l2tp ipsec pptp l2tp_ipsec} profile-name	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For <i>profile-name</i> : enter the target tunnel profile or name. Note: The command should be activated again if the profile configuration is changed. Note: Use “no crypto vpn” to disconnect from a VPN tunnel.
3.	vpdn-group name	Associates a VPDN group with a customer or VPDN profile.
4.	request dialin	Create a request dial-in VPDN subgroup that configures the router to request the establishment of a dial-in tunnel to a tunnel server, and enters VPDN request-dialin group configuration mode.
5.	protocol l2tp	Specifies the tunneling protocol that a VPDN subgroup will use.
6.	initiate-to ip-address	Specify the IP address (VPN server) that will be tunneled to.
7.	l2tp security crypto-profile profile-name	Configure IP Security (IPsec) protection of Layer 2 Tunnel Protocol (L2TP). For <i>profile-name</i> , specify the name of the crypto profile to be used for IPsec protection of tunneled PPP sessions.
8.	interface dialer number	Create a Dialer interface. The interface number will fall within the scope of 0-255
9.	ip address negotiated	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.

	Command	Purpose
10.	dialer-group <i>number</i>	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
11.	ppp authentication chap	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP)
12.	ppp chap hostname <i>username</i>	Define an interface-specific CHAP hostname.
13.	ppp chap password <i>password</i>	Define an interface-specific CHAP password.
14.	exit	Return to global configuration mode.
15.	show interface <i>Dialer interface-number</i>	(Optional) Show interface statistics.
16.	show vpdn tunnel l2tp	(Optional) Display details about L2TP active VPDN tunnel.
17.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure L2TP with IPsec on the router:

```
Router# configure terminal
Router(config)# vpdn-group 2
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to 172.19.66.213
Router(config-vpdn)# l2tp security crypto-profile ipsec1
Router(config-vpdn)# exit
Router(config)# interface Dialer 2
Router(config-if)# ip address negotiated
Router(config-if)# dialer-group 1
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp authentication ms-chap-v2
Router(config-if)# ppp chap hostname test
Router(config-if)# ppp chap password test
Router(config-if)# exit
```

The following example shows a sample output of the **show interface Dialer** command:

```
Router# show interface dialer 0
Link encap:Point-to-Point Protocol
inet addr:192.168.1.128 P-t-P:192.168.1.99 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1410 Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:234 (234.0 b) TX bytes:240 (240.0 b)
```

The following example shows a sample output of the **show vpdn tunnel l2tp** command:

```
Router# show vpdn tunnel l2tp
L2TP Tunnel Information Total tunnels 1
  Remote Address    Port    State
  192.168.1.99      1701    established
```




Configuring the Wi-Fi Interface

This chapter provides details on how to configure the Wi-Fi interface on the Cisco 910 Industrial Routers (*hereafter* referred to as the router). The Wi-Fi interface helps to provide remote wireless connectivity to a router.

The Wi-Fi interface can be configured only on the IR910W-K9 model of Cisco 910 Industrial Routers.

This chapter includes the following sections:

- [Information About the Wi-Fi Interface, page 1](#)
- [Configuring the Wi-Fi Interface, page 3](#)
- [Monitoring Wi-Fi Information, page 8](#)

Information About the Wi-Fi Interface

This section includes the following information:

- [Wi-Fi Modes, page 1](#)
- [Wi-Fi Settings, page 1](#)
- [SSID, page 2](#)
- [Security, page 2](#)

Wi-Fi Modes

- [Wi-Fi Access Point, page 1](#)
- [Wi-Fi Station, page 1](#)

The Wi-Fi interface can only be set up to perform as a Wi-Fi access point or Wi-Fi client at any one time—it cannot perform both roles simultaneously.

Wi-Fi Access Point

The router's 2.4GHz Wi-Fi radio interface can function as an access point (AP) that provides connectivity to 802.11 b/g/n devices. This Wi-Fi connectivity allows remote access and diagnostics of the router in the field.

Wi-Fi Station

The Wi-Fi interface can be configured as a Wi-Fi station. This configuration allows the Wi-Fi interface to act as a Wi-Fi client to another access point or repeater. Layer-3 routing is supported over the radio interface. SSIDs are required to be configured on the dot11 interface operating as a Wi-Fi station.

Wi-Fi Settings

The Wi-Fi interface is identified as *dot11Radio 0* on the router.

The essential configuration elements are:

- Wi-Fi interface IP address.
- Service set identifier (SSID).
- Authentication type for enabling the router's Wi-Fi functionality.
- Configuring a passphrase if WPA/WPA2 authentication is selected.

For more information, see the [“SSID” section on page -2](#), the [“Security” section on page -2](#), and the [“Configuring the Wi-Fi Interface” section on page -3](#).

SSID

The WLAN associates a service set identifier (SSID) to the Wi-Fi interface. An SSID must be assigned to the Wi-Fi interface for it to be active in the network.

The SSID can be suppressed such that it is not advertised in the 802.11 beacons. Multiple SSIDs can be configured but the Wi-Fi interface supports only one SSID—only one active SSID can be assigned at a time to the Wi-Fi Interface.

Security

The Wi-Fi interface supports none, Wired Equivalent Privacy (WEP), WPA2, and WPA1WPA2 mode.

This section contains information about:

- [WEP, page 2](#)
- [WPA2, page 2](#)
- [WPA1WPA2, page 2](#)

WEP

WEP is the encryption algorithm built into the 802.11 (Wi-Fi) standard. WEP encryption uses the Ron's Code 4 (RC4) Stream Cipher with 40- or 104-bit keys and a 24-bit initialization vector (IV).

As the standard specifies, WEP uses the RC4 algorithm with a 40-bit or 104-bit key and a 24-bit IV. RC4 is a symmetric algorithm because it uses the same key for the encryption and the decryption of data. When WEP is enabled, each radio station has a key. The key is used to scramble the data before transmission of the data through the airwaves. If a station receives a packet that is not scrambled with the appropriate key, the packet is discarded and never delivered to the host.

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

WPA2

WPA2 provides full implementation of the IEEE 802.11i standard for WLANs and supports the enhanced AES-CCMP encryption algorithm.

WPA1WPA2

WPA1WPA2 mode allows support of WPA/TKIP and WPA2/AES-CCMP clients on a common SSID. The access point advertises the available encryption methods (TKIP, AES-CCMP) on the network, and the Wi-Fi client then selects which security method it wants to employ.

Configuring the Wi-Fi Interface

You can configure the Wi-Fi interface to AP mode or station mode.

This section includes:

- [Configuring Wireless Mode, page 3](#)
- [Configuring the Wi-Fi Interface for AP Mode, page 3](#)
- [Configuring the Wi-Fi Interface for Station Mode, page 6](#)

Configuring Wireless Mode

Beginning in privileged EXEC mode, follow these steps to choose AP mode or station mode for the radio interface.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface dot11radio 0	Enter 802.11 radio interface configuration mode, and enter the interface number.
3.	dot11mode {ap sta auto-connect {on off}}	Choose AP or station mode for the 802.11 radio interface.
4.	exit	Return to global configuration mode.
5.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the Wi-Fi Interface for AP Mode

- [Creating an SSID and Binding an AP Profile, page 3](#)
- [Configuring AP Settings, page 4](#)
- [Configuring AP Profiles, page 6](#)

Creating an SSID and Binding an AP Profile

The service set identifier (SSID) is a unique identifier of the wireless network that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSID. An SSID name is case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID name.

You must define an SSID for the Wi-Fi interface to activate the interface within the network.

Only one active SSID can be associated with the interface.

Beginning in privileged EXEC mode, follow these steps to create an AP profile and associate the radio interface to the profile.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	dot11ap ssid <i>ssid-name</i>	Create 802.11 AP profile.
3.	interface dot11radio 0	Enter 802.11 radio interface configuration mode, and enter the interface number.
4.	ssid <i>ssid-name</i>	Create an SSID.
5.	exit	Return to global configuration mode.
6.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to associate an SSID to the Wi-Fi interface.

```
Router(config)# configure terminal
Router(config)# dot11ap ssid test-ap
Router(config)# interface dot11radio 0
Router(config-if)# ssid test-ap
```

Configuring AP Settings

Beginning in privileged EXEC mode, follow these steps to configure the AP settings:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	interface dot11radio 0	Enter 802.11 radio interface configuration mode, and enter the interface number.
3.	bandwidth {ht20 ht40}	Configure the bandwidth of the AP. The bandwidth value includes ht20 and ht40. ■ ht20—High-throughput 20 MHz. ■ ht40—High-throughput 40 MHz.
4.	speed 2.4g <i>speed-string</i>	Specify the radio data rates. The <i>speed-string</i> value can be one of the following: ■ 36.0 ■ 48.0 ■ 54.0 ■ 36.0 48.0 ■ 48.0 54.0 ■ 36.0 54.0 ■ 36.0 48.0 54.0
5.	short-gi {enable disable}	Enable or disable the short guard interval which is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device.
6.	ssid-hidden {enable disable}	Enable or disable hiding the SSID when scanning the WLAN.

	Command	Purpose
7.	ampdu {0 1/4 1/2 1 2 4 8 16}	Configure aggregate MAC Protocol Data Unit (A-MPDU), which joins multiple MPDU sub frames with a single leading PHY header.
8.	ap-isolation {enable disable}	Enable or disable AP Isolation. AP Isolation effectively creates a virtual network among wireless clients, where each device is an individual entity that cannot communicate with other wireless devices on the same Wi-Fi access point.
9.	power local <i>value</i>	Set the transmit power for the AP. The value could be 8-17 or maximum.
10.	band {5a 5an 2.4bg 2.4bgn} channel <i>channel_number</i>	Specify radio band and channel as following. The country code for United States is US, China is CN, and Japan is JP. ■ 2.4bg supports 802.11b, 802.11g ■ 2.4bgn supports 802.11b, 802.11g, and 802.11n ■ 5a supports 802.11a ■ 5an supports 802.11a, 802.11n ■ All of 2.4bg 2.4bgn are supported to use in China. ■ All of 5a, 5an, 2.4bg, 2.4bgn are supported to use in US and JP. ■ US 5a and 5an supports the channels: auto, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, and 165. ■ JP 5a and 5an supports channels: auto, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140. ■ CN does not support 5a and 5an Channel ■ US 2.4bg and 2.4bgn support Channel1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11. ■ JP 2.4bgand 2.4bgn support Channel 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14. ■ CN 2.4bg and 2.4bgn support Channel 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13.
11.	beacon dtim-period <i>value</i>	Specify the Delivery traffic indication message (DTIM), which informs the clients about the presence of buffered multicast or broadcast data on the access point. The default value is 1. Value range is 1-100.
12.	beacon period <i>value</i>	Specify the interval between periodic beacons. The default value is 100. Value range is 50-1000.
13.	rts_threshold <i>value</i>	Configure the request to send (RTS) threshold, which specifies the packet size of an RTS transmission. This parameter can help control traffic flow through the access point, especially when there are many clients connected. The default value is 2346. Value range is 1000-2347.
14.	packet retries <i>value</i>	Specify the maximum data retries. Value range is 1-10. Default is 5.

	Command	Purpose
15.	fragment-threshold <i>value</i>	Specify the maximum frame size which wireless device can transmit without fragmenting the frame. The default value is 2346. Value range is 1000-2346.
16.	exit	Return to global configuration mode.
17.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring AP Profiles

Beginning in privileged EXEC mode, follow these steps to create an AP profile and associate the radio interface to the profile.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	dot11ap ssid <i>ssid-name</i>	Create 802.11 AP profile
3.	authentication {open shared}	Choose authentication type, open or shared.
4.	encryption mode {none wep wpa2 wpa1wpa2}	Configure the encryption mode which the profile uses to access a WLAN. The modes include none, WEP, WPA2, and WPA1WPA2.
5.	encryption ciphers {none wep aes-ccmp aes-ccmp + tkip}	Configures the encryption cipher, which is a named combination of authentication, encryption, and message authentication code algorithms used to negotiate the security settings for a network connection using the transport layer security or secure sockets layer network protocol. This command is used in WEP, WPA2, and WPA1WPA2 mode.
6.	wep-key <i>0-3 size {64 128}</i> <i>encryption-key transmit-key</i> or wpa-psk {hex ascii} <i>wpa-psk-string</i>	Specify the encryption key for WEP mode or the passphrase for WPA2 and WPA1WPA2 mode.
7.	exit	Return to global configuration mode.
8.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the Wi-Fi Interface for Station Mode

- [Creating an STA Profile with an SSID, page 6](#)
- [Configuring SSID Scan, page 8](#)
- [Connecting To or Disconnecting From an AP, page 8](#)
- [Checking the STA Connecting Status, page 8](#)

Creating an STA Profile with an SSID

Beginning in privileged EXEC mode, follow these steps to create an STA profile with an SSID.

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	dot11sta ssid <i>ssid-name</i>	Create a 802.11 STA profile. The length of SSID is 1-32. You can create up to five STA profiles. These characters are not supported: +, \,], ?, \$, TAB, and trailing spaces. Do not use # or ! at the beginning of the SSID name. Note: Up to ten STA profiles can be connected to an AP.
3.	authmode { open shared }	(Optional) Choose open or shared authentication mode. ■ open—Although every user can connect to an AP, the receiver cannot receive any packets from the sender. ■ shared—Key-index and password are needed to connect to an AP. Note: Only WEP encryption requires to use the authmode command to connect to an AP.
4.	encryption { none wep wpa }	(Optional) Choose none encryption mode.
5.	wep-key <i>0-3 size {64 128}</i> <i>encryption-key</i> or wpa-psk { hex ascii } <i>wpa-psk-string</i>	(Optional) Specify the encryption key for WEP mode. ■ For 64, enter a string of 10 hexadecimal digits or 5 ASCII numbers. ■ For 128, enter a string of 26 hexadecimal digits or 13 ASCII numbers. The encryption is WEP. or (Optional) Specify the passphrase for WPA2 and WPA1WPA2 mode. ■ For hex, enter a string of 64 hexadecimal characters. ■ For ascii, enter a string of 8 to 63 ASCII characters (including special characters) and numbers. Note: In the STA mode, the mode of none, WEP, WPA2, or WPA1WPA2 cannot be automatically detected. And The encryption is WPA-PSK.
6.	priority <i>priority-level</i>	Set the priority of the STA profile. The priority level must be an integer larger than 0. A smaller value of priority level refers to a higher priority.
7.	exit	Return to global configuration mode.
8.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to create an STA profile with a WEP key:

```
Router(config)# configure terminal
Router(config)# dot11sta ssid test-sta
Router(config-ap)# wep-key 3 size 128 12345678901234567890123456 transmit-key
```

Configuring SSID Scan

To scan the SSIDs, use the **dot11 scan-channel** privileged EXEC command:

The following example shows an sample output of the **dot11 scan-channel 2.4g** command:

```
Router #dot11 scan-channel 2.4g
```

#	ch	ss	bssid	SSID
01	001	202	00:23:f8:0a:84:3e	AP999
02	001	195	00:03:7f:00:00:18	Fx_MIS2
03	001	211	00:03:7f:24:00:08	Fx _MIS
04	001	164	00:1b:0c:65:43:d0	MIS-XB
05	001	162	00:03:7f:46:01:5f	Fx _crd
06	001	159	00:1b:0c:65:43:d2	voice
07	001	169	00:22:cf:56:26:80	GW-USMicro300
08	001	157	00:03:7f:24:00:03	Fx _MIS
09	001	164	00:16:cf:10:65:b1	ERIC_TEST_LOCAL
10	001	162	00:1b:0c:65:43:d1	guest
11	002	186	84:c9:b2:6a:e7:16	FieC_Dlink
12	003	154	00:1b:0c:65:40:f1	guest

Connecting To or Disconnecting From an AP

To connect to an AP, use the **dot11sta connect** privileged EXEC command.

To connect to a list of APs, use the **dot11sta exec_connect_prefer** privileged EXEC command.

To disconnect from an AP, use the **dot11sta disconnect ssid** privileged EXEC command.

Checking the STA Connecting Status

To check the STA connection status, use the **dot11sta check_connect_status** privileged EXEC command.

Monitoring Wi-Fi Information

You can display specific statistics of the Wi-Fi settings. [Table 23](#) lists the privileged EXEC commands for displaying Wi-Fi information.

Table 23 Commands to Monitor Wi-Fi Information

Command	Purpose
show dot11 mode	Display the radio mode.
show interfaces dot11radio 0 association	Display the radio association.
show dot11ap profile {ssidssid-string all}	Display AP profiles.
show dot11sta prefer-list	Display the station prefer list.
show dot11sta ssid {ssid-string all}	Display station profiles.

The following command displays the radio association:

```
Router# show interfaces dot11radio 0 association
uap0      IEEE 802.11-DS  ESSID:""
          Mode:Master  Frequency:2.437 GHz  Access Point: Not-Associated
          Encryption key:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

The following command displays the AP profile:

```
Router# show dot11ap profile ssid testap
SSID          Mode          Encryption  WEP Key      WPA Key      Encrypcipher  Authserver
Addr  port  key
-----
testap
```

The following command displays the station prefer list:

```
Router# show dot11sta prefer-list
1. SSID:testap1
2. SSID:testap2
3. SSID:testap3
```




Configuring Cellular 3G Settings

This chapter provides details on how to configure the cellular 3G settings on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

The cellular 3G interface can be configured only on the IR910G-K9 and IR910G-NA-K9 model of Cisco 910 Industrial Routers.

This chapter includes the following sections:

- [Information About the 3G Module, page 1](#)
- [Configuring Cellular 3G Settings, page 1](#)
- [Monitoring Cellular 3G Information, page 7](#)

Information About the 3G Module

The 3G module of the router is a compact, lightweight, wireless UMTS and CDMA based modem. The wireless UMTS-based modem provides data connectivity on HSDPA and HSUPA, WCDMA, EDGE, GPRS, and CDMA EVDO Rev A, 1X networks as following:

- GSM850
- EGSM900
- DCS1800
- PCS1900
- Band 1 (UMTS2100)
- Band 2 (UMTS1900)
- Band 5 (UMTS850)
- Band 6 (UMTS800)
- RX diversity Band 2 (UMTS1900)
- RX diversity Band 5 (UMTS850)
- BC0 (CDMA 800)
- BC1 (CDMA 1900)

Configuring Cellular 3G Settings

This section include the following information:

- [Configuring Cellular Controller, page 2](#)
- [Configuring Cellular Interface, page 2](#)

- [Configuring Activation of Account Using OSTAP, page 3](#)
- [Configuring Cellular Mode and Band, page 5](#)
- [Configuring GSM Profiles, page 6](#)
- [Working With the SIM Card, page 6](#)

Configuring Cellular Controller

Beginning in privileged EXEC mode, follow these steps to configure the cellular controller on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	controller cellular <i>unit</i>	Specify the cellular controller.
3.	[no] radio off	(Optional) Turn off or turn on the radio power.
4.	gsm sim profile <i>profile_number</i>	(Optional) Configure the SIM card to use profiles for GSM. For <i>profile_number</i> , specify a value from 1 to 16.
5.	sim authenticate <i>pin</i>	(Optional) Store the SIM CHV1 code for verification. For <i>pin</i> , specify the character code provided by your carrier to lock or unlock the SIM card. The code contains 4 to 8 characters.
6.	cellular mode {1 2}	Switch the firmware between UMTS and CDMA for SIM or RUIM card. ■ 1—Activate China Unicom (UMTS). ■ 2—Activate China Telecom (CDMA).
7.	exit	Return to global configuration mode.
8.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure the cellular controller for UMTS:

```
Router# configure terminal
Router(config)# controller cellular 0
Router(config-controller)# cellular mode 1
Router(config-controller)# gsm sim profile 10
Router(config-controller)# sim authenticate 1234
Router(config-controller)# exit
Router(config)#
```

Configuring Cellular Interface

Beginning in privileged EXEC mode, follow these steps to configure the cellular interface on the router:

	Command	Purpose
1.	configure terminal	Enter global configuration mode.
2.	chat-script <i>script_name</i> [<i>expect1 send1</i>] [<i>expect2 send2</i>] ...	Create a script that will place a call over a modem. For <i>expect send</i> , specify pairs of information elements—an item to expect and an item to send in response.
3.	interface cellular <i>unit</i>	Specify the cellular interface and enter interface configuration mode.

	Command	Purpose
4.	dialer in-band	(Optional) Specify that dial-on-demand routing (DDR) is to be supported
5.	dialer idle-timeout <i>seconds</i>	(Optional) Specify the duration of idle time in seconds, after which a line will be disconnected. Default is 120 seconds.
6.	dialer string <i>string</i>	Specify the CHAT script to dial.
7.	ppp chap hostname <i>host</i>	Define an interface-specific CHAP hostname. It must match the username given by the carrier.
8.	ppp chap password <i>password</i>	Define an interface-specific CHAP password. It must match the password given by the carrier.
9.	ip address { negotiated <i>ip_address netmask</i> }	Specify the IP address for the interface. To obtain IP address via PPP/IPCP address negotiation, use the negotiated keyword of this command.
10.	exit	Return to global configuration mode.
11.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure the cellular interface:

```
Router# configure terminal
Router(config)# interface cellular 0
Router(config-if)# ip address negotiated
Router(config-if)# dialer in-band
Router(config-if)# dialer idle-timeout 30
Router(config-if)# dialer string gsm
Router(config-if)# ppp chap hostname cisco@wwan.ccs
Router(config-if)# ppp chap password cisco
Router(config-if)# exit
Router(config)#
```

Configuring Activation of Account Using OSTAP

To activate a wireless account using over-the-air service provisioning (OTASP), use the **cellular cdma activate otasp** command in privileged EXEC mode.

Note: The modem activation process is specific to the carrier. Check with your carrier if they support manual activation using OTASP.

cellular 0 cdma activate otasp *phone_number*

Syntax Description

<i>phone_number</i>	Phone number that you must dial to begin activation using OTASP. This number is specific to a wireless provider. For Verizon Wireless, it is *22899.
---------------------	--

Examples

```
Router# cellular 0 cdma
  activate 3G CDMA account provision
  mode      Configure the network registration mode

Router# cellular 0 cdma activate
  otasp Verizon account provision

Router# cellular 0 cdma activate otasp
  WORD Dialing number used during OTASP process, usually *22899
```

```
Router# cellular 0 cdma activate otasp *22899
Checking radio signal...
Radio signal: RSSI: -55 dBm, ECIO: -0.5 dBm.
Radio signal is good.
Beginning OTASP activation...
OTASP number: *22899
Activation OK, code: 0
Router#
```

The error code in the output and the definition are described as following:

Error Code	Definition
0	Activation OK
1	Activation cancelled by user
2	Device not ready
3	Write dummy NAI number failed
4	Write MN-HA SPI failed
5	Write Rev-Tun failed
6	Enable profile failed
7	Restore NAI failed
8	NAI restore completed
9	NAI number not updated during OTASP
10	Service not activated during OTASP

Configuring Cellular Mode and Band

Use the following commands to configure CDMA mode and GSM band:

Command	Purpose
cellular unit cdma mode mode	Configure the network registration mode to CDMA. For <i>mode</i>, specify one of the following options: ■ 1xRTT—Technology-specific protocol is CDMA 1xRTT ■ 1xEVDO—Technology-specific protocol is CDMA 1xEVDO ■ hybrid—Connect to hybrid technology protocol Note: A service mode change is followed by a modem reset.
cellular unit gsm band band	Specify the GSM/WCDMA frequency band. Only the bands that can be selected by the modem are listed. For <i>band</i>, specify one of the following options: ■ auto-band—Auto Band ■ gsm-all-bands—All GSM bands ■ wcdma-all-bands—All WCDMA bands
cellular unit gsm plmn {search select {auto manual}}	Configure public land mobile networks (PLMN). ■ search—Search for available PLMNs. ■ select—Manually or automatically select from the available PLMNs in an area to attach the modem to. — auto—Allows automatic selection of the PLMN for the modem. — manual—Allows manual selection of the PLMN for the modem.

The following example shows how to configure the network registration mode to CDMA hybrid:

```
Router# cellular 0 cdma mode hybrid
```

The following example shows how to configure the GSM band to auto band:

```
Router# cellular 0 gsm band auto-band
```

The following example shows how to configure PLMN search:

```
Router# cellular 0 gsm plmn search
```

The following example shows how to configure PLMN auto selection:

```
Router# cellular 0 gsm plmn select auto
```

Configuring GSM Profiles

Beginning in privileged EXEC mode, follow these steps to configure the cellular parameters on the router:

	Command	Purpose
1.	cellular unit gsm create <i>profile_number apn</i> [<i>authentication_type username</i> <i>password</i>] [<i>protocol</i>]	Create or modify a gsm modem data profile. ■ For <i>profile_number</i>, specify the number for the profile to be created. Up to 16 profiles can be created. ■ For <i>apn</i>, specify the Access Point Name (APN). APN is provided by the service provider. ■ (Optional) For <i>authentication_type</i>, specify CHAP or PAP. If you specify the authentication type, enter username and password which are provided by the service provider. ■ (Optional) For <i>protocol</i>, choose an option for the network protocol: IPv4, PPP, IPv6, or IPv4v6. To delete a GSM profile, use the cellular unit gsm create profile_number command.
2.	exit	Return to global configuration mode.
3.	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows how to configure a GSM profile:

```
Router# cellular 0 gsm profile create 3 apn.com chap gsm gsmPassword ipv4
```

Working With the SIM Card

PIN is a 4 to 8 character code provided by the carrier to lock or unlock the SIM card.

This section provide information on operating with the SIM card PIN code:

- [Changing the PIN, page 6](#)
- [Locking the SIM Card, page 6](#)
- [Unlocking the SIM Card, page 7](#)
- [Unblocking the SIM Card, page 7](#)

Changing the PIN

To change the CHV1 PIN for the SIM card, use the **cellular unit sim change-pin old_pin new_pin** privileged EXEC command.

Example:

```
Router# cellular 0sim change-pin 1234 5678
```

Locking the SIM Card

To lock the SIM card provided by the service provider, use the **cellular unit sim lock pin** privileged EXEC command.

Example:

```
Router# cellular 0 sim lock 1234
```

Unlocking the SIM Card

To unlock the SIM card provided by the service provider, use the **cellular unit sim unlock pin** privileged EXEC command.

Example:

```
Router# cellular 0 sim unlock 1234
```

Unblocking the SIM Card

The PUK is an 8-digit CHV1 code that you obtain from the carrier. When the CHV1 is blocked after the wrong input of PINs for four times, you must unblock the SIM card by providing PUK and a new PIN.

The SIM card will no longer be available again after you input the wrong PUK or PIN for 10 times.

To unblock the SIM card provided by the service provider when the CHV1 has been blocked, use the **cellular unit sim unblock puk new_pin** privileged EXEC command.

Example:

```
Router# cellular 0 sim unblock 60265772 1234
```

Monitoring Cellular 3G Information

You can display specific statistics of the cellular settings. [Table 24](#) lists the privileged EXEC commands for displaying cellular information.

Table 24 Commands to Monitor Cellular Information

Command	Purpose
show cellular unit all	Display all the cellular 3G information on the router.
show cellular unit connection	Display current active connection state and data statistics.
show cellular unit hardware	Display hardware information of the router.
show cellular unit network	Display information about the carrier network and service.
show cellular unit profile	Display the 3G profile information.
show cellular unit radio	Display the 3G radio statistics.
show cellular unit security	Display the SIM card status and modem lock state.

The following example shows a sample output of the **show cellular unit all** command:

```
Router# show cellular 0 all
Hardware Information
=====
Modem Firmware Version = D3200-SCAUTNZ-SWI6600U02000002 1
Modem Firmware built = Dec 24 2012 13:26:55
Hardware Version = 3
Electronic Serial Number (ESN) = 80EFE08B
Preferred Roaming List (PRL) Version = Unavailable
International Mobile Subscriber Identity (IMSI) = 466974804454330
International Mobile Equipment Identity (IMEI) = 013484000020678
```

```
Integrated Circuit Card ID (ICCID) =
Current Modem Temperature =
Modem Status =

Profile Information
=====
Profile 1 = INACTIVE*
-----
PDP Type = IPv4
Authentication = None
Access Point Name (APN) = internet
Username:
Source Address = 0.0.0.0
Primary DNS address= 0.0.0.0

Profile 2 = INACTIVE
-----
PDP Type = IPv4
Authentication = None
Access Point Name (APN) = twm
Username:
Source Address = 0.0.0.0
Primary DNS address= 0.0.0.0

* - Default profile

Data Connection Information
=====
Current Transmitted = 0 bytes, Received = 0 bytes
Total Transmitted = 0 KB, Received = 0 KB
Current Call Status = DISCONNECTED
Current Call Duration = 30 secs
Total Call Duration = 4482879 seconds

Network Information
=====
Current Service Status = UMTS
Current Roaming Status =
Packet Service = None
Packet Session Status = Connected
Network Selection Mode = Automatic
Network = twm
Mobile Country Code (MCC) =
Mobile Network Code (MNC) =

Radio Information
=====
Radio power mode = on
Current RSSI = -114 dBm, ECIO = -14 dBm
Current Channel Number = 0
Current Band Class = 80

Modem Security Information
=====
Modem PIN Security = ENABLED
SIM Status = OK
SIM User Operation Required = CHV1
Number of Retries remaining = 3
```

The following example shows a sample output of the **show cellular unit connection** command:

```
Router# show cellular 0 connection
Data Transmitted = 0 bytes, Received = 0 bytes
Total Transmitted = 0 KB, Received = 0 KB
Current Call Status = DISCONNECTED
```

```
Current Call Duration = 30 secs
Total Call Duration = 4482879 seconds
```

The following example shows a sample output of the **show cellular unit network** command:

```
Router# show cellular 0 network
Current Service Status = UMTS
Current Roaming Status =
Packet Service = None
Packet Session Status = Connected
Network Selection Mode = Automatic
Network = twm
Mobile Country Code (MCC) =
Mobile Network Code (MNC) =
```

The following example shows a sample output of the **show cellular unit profile** command:

```
Router# show cellular 0 profile
Profile 1 = INACTIVE*
-----
PDP Type = IPv4
Authentication = None
Access Point Name (APN) = internet
Username:
Source Address = 0.0.0.0
Primary DNS address= 0.0.0.0

Profile 2 = INACTIVE
-----
PDP Type = IPv4
Authentication = None
Access Point Name (APN) = twm
Username:
Source Address = 0.0.0.0
Primary DNS address= 0.0.0.0

* - Default profile
```

The following example shows a sample output of the **show cellular unit radio** command:

```
Router# show cellular 0 radio
Radio power mode = on
Current RSSI = -114 dBm, ECIO = -14 dBm
Current Channel Number = 0
Current Band Class = 80
```

The following example shows a sample output of the **show cellular unit security** command:

```
Router# show cellular 0 security
Modem PIN Security = ENABLED
SIM Status = OK
SIM User Operation Required = CHV1
Number of Retries remaining = 3
```




Using Device Manager

The device manager is a graphic user interface (GUI) used to manage and configure the Cisco 910 Industrial Router and monitor the status of the router locally or remotely.

The recommended installation environment of the device manager is Cisco 910 Industrial Router OS (Linux). Internet Explorer 8.0, Internet Explorer 9.0, and Firefox 16 or above are the specified client end browsers.

To configure a router using the device manager, follow the steps described in these sections:

- [Introduction to the Device Manager, page 1](#)
- [Logging In to the Device Manager, page 3](#)
- [Language Setting, page 3](#)
- [Using Dashboard, page 4](#)
- [Configuring the Network, page 8](#)
- [Configuring Platform Settings, page 32](#)
- [Monitoring the Status of System and Network, page 49](#)
- [Maintenance of the Router, page 55](#)

Introduction to the Device Manager

The device manager displays real-time views of router configuration and performance. It simplifies configuration tasks with features such as Express Setup for quickly setting up the router and its ports. It uses graphical, color-coded displays, such as the Front Panel view, graphs, and animated indicators to simplify monitoring tasks and to help you to identify and solve networking problems.

For comprehensive configuration and monitoring features, use the router command-line interface (CLI).

You can display the device manager from anywhere in your network through a web browser such as Microsoft Internet Explorer.

We recommend that you use the device manager in a secured session to protect your device manager session from unauthorized access. See the [“Using Secured Sessions” section on page -3](#) for detailed information.

The router displays settings and status only in English. In addition, entries on the router can only be in English.

Using the Dashboard

The Dashboard provides information about the router and is the main window for monitoring the router status and its performance. It is the default window and appears each time that you display the device manager. For more information about the gauges, indicators, and graphs, see Dashboard.

Using the Toolbar Icons

The toolbar (Figure 1) is designed to provide options for refreshing the GUI, printing current page and accessing the online help. The title of the toolbar is “IR910 Series Device manager” with the router hostname.

Figure 1 Toolbar of the Device Manager



Table 1 shows the descriptions of each options on the toolbar.

Table 1 Toolbar Options

Toolbar Icon	Option	Description
	Refresh	Update the information displayed on the Front Panel view, the graphs, and the configuration and monitoring windows. Note Features that contain configurable parameters will not be refreshed.
	Print	Print a device manager window, such as the Dashboard or the Port Statistics window. Note The menu or the Front Panel view cannot be printed. To print an online help page, click Print in the online help title bar.
	Help	Provide descriptions of the device manager features and procedures on how to use the features. The Help also provides links to LED status definitions and to support resources, such as the router documentation and technical assistance.

Using the Menus

After you log in to the device manager, you will see the following menus on the left pane of the GUI:

- Dashboard—The primary window for monitoring overall router and port conditions.
- Network Configuration—Provides options to set up the basic network settings for the router and its ports, and to restart and to reset the router.
- Platform Configuration—Provides options to set up network application. For examples. LLDP, SNMP, and AAA.
- Monitor—Provides options to display status and detailed run-time statistics every 60 seconds or when you click **Refresh** in the toolbar.
- Troubleshooting—Provides Ping and Traceroute to check network status.
- Maintenance—Provides an option to start a Telnet session and an option to upgrade the router software.

Detailed information about using these menus will be described in the following sections:

- [Using the Dashboard](#)
- [Using the Toolbar Icons](#)
- [Using the Menus](#)
- [Using Secured Sessions](#)
- [Router Information](#)

- [System Information](#)
- [Port Utilization Graph](#)

Using Secured Sessions

The router uses the Secure Sockets Layer (SSL) protocol to secure the HTTP communications between the router and your network management station. When you attempt to display the device manager, this protocol

- Authenticates the web-based connection between the router and your network management station.
- Encrypts and decrypts the information exchanged between the router and your network management station to protect the information from unauthorized access over the Internet.

SSL is disabled by default on the router. You can enable/disable SSL in HTTPs window.

In SSL enable state, when you first display the device manager, it displays a message that asks if you want a secured session with the router. If you choose **Yes**, the router displays another message that asks if you want to proceed by using the security certificate of the router. If you choose **Yes** to use the certificate, the router displays the device manager in secure mode.

If you choose **No** for either message, the router displays the device manager in unsecured mode.

There are other ways to start a secured device manager session:

- Enter **https://** before the router IP address. (HTTP over SSL is abbreviated as HTTPS.)
- Click the **Session: Standard | Secured** link at the top right corner of the device manager window.

There are several ways to determine whether your device manager session is secured:

- Look at the URL in the browser Address field. A URL that starts with **https://** means that the session is secured through SSL. A URL that starts with **http://** means that the session is not secured.
- Look at the **Session: Standard | Secured** link at the top right corner of the device manager window.
 - If the link appears as **Session: Standard | Secured**, the router is running a secured session.
 - If the link appears as **Session: Standard |**, the router is not running a secured session.
- Look for a locked padlock image at the bottom of your browser window. The locked padlock only appears if the session is secured.

Logging In to the Device Manager

Access the device manager at **http://[router's IP address]** and log in to the web portal locally or remotely by entering the username and password of the admin account.

Language Setting

The GUI supports simplified Chinese and English by default. Other languages can be added easily when they are needed.

The GUI can detect the language the browser is using and display the pages in corresponding language when you log in for the first time. You can also change the language by selecting the proper language from the Language drop-down list as shown in [Figure 2](#).

Figure 2 Language Setting of the Device Manager



Using Dashboard

The Dashboard provides information about the router and is the main window for monitoring the router status and its performance. It is the default window and appears each time that you display the device manager. The Dashboard displays:

- Router Information
- System Information
- Port Utilization Graph

Router Information

The Router Information area provides reference information about the router (Figure 3).

Figure 3 Router Information

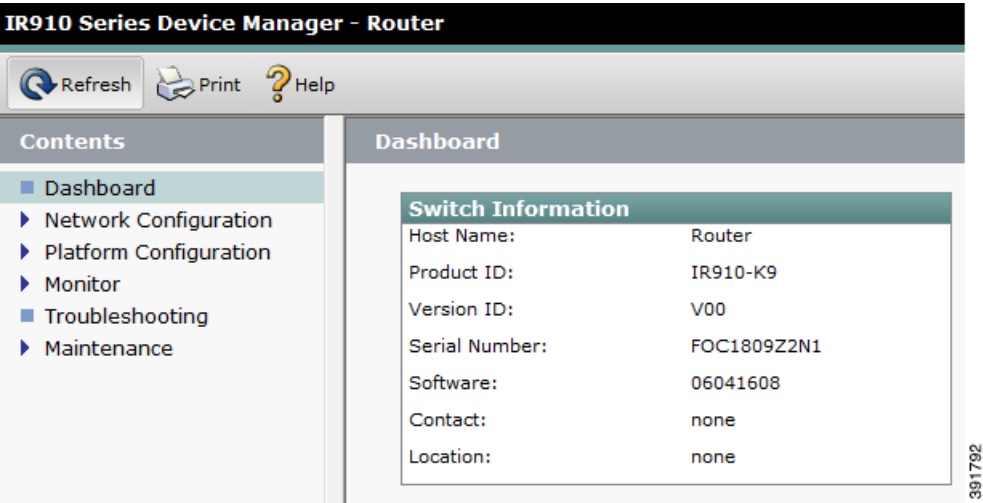


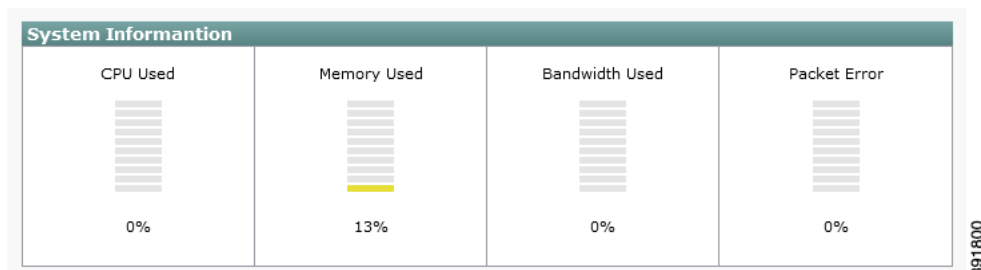
Table 2 shows the details of each options in the Router Information area.

Table 2 Router Information

Option	Description
Name	The name of this router configured during Express Setting or through the command-line interface (CLI). If no name was provided, this field displays the default name, Router.
Product ID	The model of this router. This information cannot be modified.
IP Address	The IP address of this router configured during Express Setting or through the CLI.
Version ID	The version ID of the router. This information cannot be changed.
Serial Number	The serial number of this router. This information cannot be modified.
Software	The software version that the router is running. This information is updated when you upgrade the router software.
Contact	The name of the person assigned as the administrative contact for this router. This information is configured during SNMP window or through the CLI.
Location	The location identified for router. This information is configured during SNMP window or through the CLI.

System Information

The System Information area has the gauges and indicators that show the overall status of the router ([Figure 4](#)).

Figure 4 System Information

Data is collected at each 60-second system refresh. To manually refresh the gauges, click **Refresh** in the toolbar. The following sections describes these gauges and indicators:

- [CPU Used Gauge](#)
- [Memory Used Gauge](#)
- [Bandwidth Used Gauge](#)
- [Packet Error Gauge](#)

CPU Used Gauge

The CPU Used gauge shows the total CPU percentage of the router being used. You can also move the pointer over the gauge to see this percentage. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total CPU used under 5 percent.

Memory Used Gauge

The Memory Used gauge shows the total memory percentage of the router being used. You can also move the pointer over the gauge to see this percentage. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total memory used under 5 percent.

Bandwidth Used Gauge

The Bandwidth Used gauge shows the total receive percentage of the router bandwidth being used. You can also move the pointer over the gauge to see this percentage. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total bandwidth under 5 percent.

The Bandwidth Used gauge changes as the router experiences the network activity from devices sending data packets through the network. As network activity increases, contention between devices to send data through the network increases. Contention can cause collisions (two devices sending data at the same time), and the devices need to resend their data. Excessive collisions can cause transmission delays. For example, users might experience excessive delays in sending or receiving information through the network.

As you monitor the router, note whether the bandwidth usage is consistently high. This can mean there is congestion in the network. If the router reaches its maximum bandwidth (above 90 percent usage) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the router is configured to help to recover lost packets (such as by signaling to other devices to resend data). However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, that can also increase bandwidth usage on the router.

Packet Error Gauge

The actual percentage appears below the graphic. You can also display the actual percentage by moving the pointer over the gauge. Each bar in the gauge represents 10 percent, and does not show increments that are less than 10 percent. The gauge does not show packet error percentages that are less than 5 percent.

The packet error percentage is calculated by comparing two values:

- The total number of packets that are sent and received.
- The total number of packets with errors that are sent and received.

If the packet-error percentage is high (that is, above 10 percent), the router bandwidth usage might also be too high (a sign that the network is congested). Other causes for packet errors are faulty cabling and port misconfiguration, such as a duplex-mode mismatch. These problems can cause network users to experience intermittent connectivity or loss of connectivity to network resources (such as servers and printers) or to the Internet. Excessive collisions can cause transmission delays. For example, users might experience excessive delays in sending or receiving information through the network.

The Port Statistics window displays some of the types of packet errors collected by the router. [Table 3](#) shows some cause for some network problems.

Table 3 Types of Packet Errors

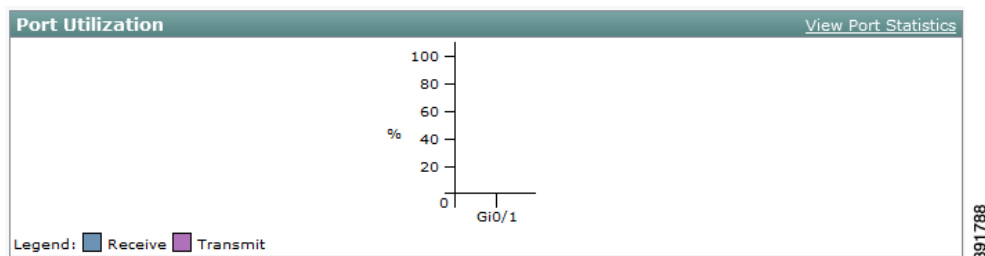
Option	Description
Runt packets	Packets that are smaller than the allowed minimum size (less than 64 bytes).
Giant packets	Packets that are larger than the allowed maximum size (more than 1518 bytes).
Cyclic redundancy checksum (CRC) errors	Errors generated by the originating LAN station or far-end device do not match the checksum calculated from the data received. On a LAN, this usually means noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or of a station sending bad data.
Overrun packets	Packets that the receiving device was unable to receive.
Frame packets	Packets received because of a CRC error and a non-integer number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Ignored packets	Packets that the interface ignores because the interface hardware is low on internal buffers. These buffers are different from the system buffers. Broadcast storms and bursts of noise can cause the ignored count to increase.

Port Utilization Graph

The Port Utilization graph displays the receive utilization (blue) and transmit utilization (purple) for all the ports. Move the pointer over the color-coded bars in the graph for the utilization percentage for the specific ports.

Using the Refresh option from your browser reloads the device manager.

For send and receive statistics for each port, click **View Port Statistics** on the top right of the Port Utilization graph (see Figure 5).

Figure 5 Port Utilization Graph

The proportion of bandwidth allocated to each port can be based on symmetric (evenly distributed bandwidth to each port) or asymmetric (unlike, or unequal, bandwidth among some ports) connections.

Symmetric connections are among ports with the same bandwidth, such as all 100BASE-T. Symmetric connections are optimized for a reasonably distributed traffic load, such as in a peer-to-peer desktop environment.

Asymmetric connections are among ports with unlike bandwidth, such as a combination of 10BASE-T, 100BASE-T, and 1000BASE-T. Asymmetric connections are optimized for client/server traffic flows in which multiple clients simultaneously communicate with a server, requiring more bandwidth dedicated to the server port to prevent a bottleneck at that port.

Bandwidth allocation can also be based on whether the connection is operating in half-duplex or full-duplex mode.

Configuring the Network

You can perform the following network configuration using the Network Configuration menus:

- [Configuring Ports](#)
- [Configuring Express Settings](#)
- [Configuring Layer 3 Settings](#)
- [Configuring Wireless](#)
- [Configuring 3G USB Modem](#)
- [Configuring PPPoE](#)
- [Configuring VLAN](#)
- [Configuring VPN](#)
- [Configuring DHCP](#)
- [Configuring NAT](#)

Configuring Ports

Use the Port Settings window to configure the basic port settings. These settings determine how data is received and sent between the router and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems.

Follow these steps to configure the port:

1. Click **Port** under Network Configuration in the left pane. The Port Settings window is displayed, as shown in [Figure 6](#).

Figure 6 Port Settings

Port	Description	Enable	Speed	Duplex
Gi0/1		☒	Auto	Auto

391789

2. You can view or configure the following information of the port:

- **Port**—Name of the port, including the type of the port (for example, Gi for GigabitEthernet), the module slot number (for example, 0), and the specific port number.
- **Description**—Description of the port. Valid values are strings with less than 256 characters. You are recommended to provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
- **Enable**—The status of the port. Check **Enabled** to enable the port. Uncheck the check box of a port to administratively (manually) shut down the port. It is recommended to disable the port if the port is not in use and is not attached to a device.

- **Speed**—The operating speed of the port. Choose the speed from the drop-down list:
 - Auto—Sets the interface to auto negotiate speed. This is the default.
 - 10 MB—Sets the interface to 10 MB (for TX interface only).
 - 100 MB—Sets the interface to 100 MB (for FX interface only).
 - 1000 MB—Sets the interface to 1 GB (for Gigabit Ethernet interface only).
- **Duplex**—The duplex mode of the port. The default is Auto. Choose the duplex mode from the drop-down list:
 - Auto (auto negotiation)—The connected device can negotiate with the router. This is the default.
 - Full (full duplex)—Both devices can send data at the same time.
 - Half (half duplex)—Both devices cannot send data at the same time.

On a Gigabit Ethernet port, you cannot set the port to half duplex if the port speed is set to Auto.

3. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Express Settings

The router can operate without an IP address assigned to it. However, you are recommended to set up the router with an IP address so that you can manage it through the device manager.

Use the Express Settings window to setup the router. Follow these steps to configure the express settings:

1. Click **Express Settings** under Network Configuration in the left pane. The Express Settings window is displayed, as shown in [Figure 7](#).

Figure 7 Express Settings

The screenshot shows the 'Express Setting' window with two main sections: 'Network Settings' and 'Optional Settings'.

Network Settings:

- Gigabit Ethernet: GigabitEthernet 0/1
- IPv4 Address: [] . [] . [] . []
- IPv4 Netmask: 128.0.0.0 (dropdown)
- IPv4 Default Gateway: 173 . 39 . 202 . 129
- IPv6 prefix Address: [] / 64 [x] EUI-64
- IPv6 Default Gateway: []
- Switch Enable Password: []
- Confirm Password: []

Optional Settings:

- Host Name: Router
- SSH Login Timeout(seconds): 120
- SSH Auth Retries: 3 (dropdown)

At the bottom, there are 'Submit' and 'Cancel' buttons.

2. Enter the IPv4 or IPv6 address of the router.
3. Click the drop-down arrow in the IPv4 Netmask field, and select an IP Subnet Mask; or enter Subnet prefix length field when you use IPv6, and the range is 0 to 128.
4. Enter the IP address for the IPv4 or IPv6 default gateway in the Default Gateway field.

5. Enter the password in the Switch Enable Password field. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and can have embedded spaces. The password cannot contain a question mark (?) or a tab, and cannot have spaces at the beginning or end. The default is cisco.

Note: To complete the initial setup, you must change the password.
6. Enter the password again in the Confirm Password field.
7. (Optional) Enter a host name for the router in the Host Name field. The host name is limited to 31 alphanumeric characters and embedded spaces are not allowed.
8. (Optional) Specify the SSH Login Timeout value in seconds. The value should not to exceed 120 seconds. The default is 120.
9. (Optional) Specify the number of authentication retries in the SSH Auth Retries field. The value range is not to exceed 5 authentication retries. The default is 3.
10. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Layer 3 Settings

You can configure the following layer 3 settings on the router:

- [Configuring Management VLAN](#)
- [Configuring Gigabit Ethernet Interface](#)
- [Configuring Wi-Fi Station](#)
- [Configuring Route](#)
- [Configuring DNS](#)

Configuring Management VLAN

The management VLAN is the broadcast domain where management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should be limited to a specific group of users (such as the administrators of your network). It also ensures secure, administrative access to all devices in the network at all times.

Follow these steps to configure the IP address of the management VLAN:

1. Click **Layer 3 Settings** under Network Configuration in the left pane. The VLAN tab of Layer 3 Settings window is displayed, as shown in [Figure 8](#).

Figure 8 Layer 3 Settings-VLAN

Layer 3 Setting

VLAN GE Route DNS

Management VLAN ID: 1

IPv4 Address Settings

IPv4 Connection Type: DHCP

IPv4 Address: 173.39.202.144 IPv4 Netmask: 255.255.255.128

IPv6 Address Settings

Dynamic Address:

☐ Stateful Auto-Configuration

☐ Stateless Auto-Configuration

Static Address:

IPv6 Prefix Address: /64 ☒ EUI-64

Submit Cancel

391778

2. Choose a VLAN ID from the Management VLAN ID drop-down list. The ID can be from 1 to 4094. This information cannot be modified through the device manager. Use the CLI to change this setting.

Note: Make sure that the router and your network management station are in the same VLAN. Otherwise, you will lose management connectivity to the switch.

3. If you use IPv4 address, choose Static or DHCP from the IPv4 Connection Type drop down list.
4. If you choose Static, enter the address and netmask in the IPv4 Address and IPv4 Netmask fields; If you choose DHCP, the IPv4 Address and IPv4 Netmask fields will obtain the values automatically.
5. If you use IPv6 address, follow these guidelines to choose configure Dynamic Address setting:
 - Choose Dynamic Stateful Auto-Configuration if you want to enable the DHCPv6 client function on the interface and obtain IPv6 address automatically from a DHCPv6 server.
 - Choose Dynamic Stateless Auto-Configuration if you want to enable stateless auto-configuration on the interface and to configure IPv6 addresses based on prefixes received in Router Advertisement messages.
6. Enter IPv6 Prefix Address in the Static Address field if you want to produce a static IPv6 global address. Enter related IPv6 Default Router and IPv6 DNS Server address.
7. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Gigabit Ethernet Interface

Follow these steps to configure the Gigabit Ethernet (GE) interface on the router:

1. Click **Layer 3 Settings** under Network Configuration in the left pane and then click **GE** in the right pane. The GE tab is displayed, as shown in [Figure 9](#).

Figure 9 Layer 3 Settings-GE

2. If you use IPv4 address, choose Static or DHCP from the IPv4 Connection Type drop down list.
3. If you choose Static, enter the address and netmask in the IPv4 Address and IPv4 Netmask fields; If you choose DHCP, the IPv4 Address and IPv4 Netmask fields will obtain the values automatically.
4. If you use IPv6 address, follow these guidelines to choose configure Dynamic Address setting:
 - Choose Dynamic Stateful Auto-Configuration if you want to enable the DHCPv6 client function on the interface and obtain IPv6 address automatically from a DHCPv6 server.
 - Choose Dynamic Stateless Auto-Configuration if you want to enable stateless auto-configuration on the interface and to configure IPv6 addresses based on prefixes received in Router Advertisement messages.
5. Enter IPv6 Prefix Address in the Static Address field if you want to produce a static IPv6 global address. Enter related IPv6 Default Router and IPv6 DNS Server address.
6. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Wi-Fi Station

Follow these steps to configure the Wi-Fi Station IP address on the router:

1. Click **Layer 3 Settings** under Network Configuration in the left pane and then click **WiFi Station** in the right pane. The Wi-Fi Station tab is displayed, as shown in [Figure 10](#).

Figure 10 Layer 3 Settings-Wi-Fi Station

Layer 3 Setting

VLAN GE **Wi-Fi Station** Route DNS

IPv4 Address Settings

IPv4 Connection Type: Static

IPv4 Address: [] [] [] [] IPv4 Netmask: 128.0.0.0

IPv6 Address Settings

Dynamic Address:

☐ Stateful Auto-Configuration

☐ Stateless Auto-Configuration

Static Address:

IPv6 Prefix Address: [] / 64 ☐ EUI-64

Submit Cancel

2. If you use IPv4 address, choose Static or DHCP from the IPv4 Connection Type drop down list.
3. If you choose Static, enter the address and netmask in the IPv4 Address and IPv4 Netmask fields; If you choose DHCP, the IPv4 Address and IPv4 Netmask fields will obtain the values automatically.
4. If you use IPv6 address, follow these guidelines to choose configure Dynamic Address setting:
 - Choose Dynamic Stateful Auto-Configuration if you want to enable the DHCPv6 client function on the interface and obtain IPv6 address automatically from a DHCPv6 server.
 - Choose Dynamic Stateless Auto-Configuration if you want to enable stateless auto-configuration on the interface and to configure IPv6 addresses based on prefixes received in Router Advertisement messages.
5. Enter IPv6 Prefix Address in the Static Address field if you want to produce a static IPv6 global address. Enter related IPv6 Default Router and IPv6 DNS Server address.
6. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Route

Follow these steps to configure IPv4 or IPv6 route on the router:

1. Click **Layer 3 Settings** under Network Configuration in the left pane and then click **Route** in the right pane. The Route tab is displayed, as shown in [Figure 11](#).

Figure 11 Default Route Settings

The screenshot shows the 'Layer 3 Setting' page with tabs for VLAN, GE, Route, and DNS. The 'Route' tab is active. It contains two sections: 'IPv4 Default Route Setting' and 'IPv6 Default Route Setting'. Each section has fields for Interface (a dropdown), Interface Number (a text box), IPv4/IPv6 Default Gateway (a text box), and Metric (a text box). The IPv4 Metric is pre-filled with '1'. At the bottom are 'Submit' and 'Cancel' buttons. A vertical label '391791' is on the right side.

2. To configure IPv4 route:

- a.** Choose an interface from the Interface drop-down list in the IPv4 Default Route Setting area.
- b.** Enter the IP address of the IPv4 default gateway and metric.

To configure IPv6 route:

- a.** Choose an interface from the Interface drop-down list in the IPv6 Default Route Setting area.
- b.** Enter the IP address of the IPv6 default gateway and metric.

3. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring DNS

Follow these steps to configure DNS information on the router:

- 1.** Click **Layer 3 Settings** under Network Configuration in the left pane and then click **DNS** in the right pane. The DNS tab is displayed, as shown in [Figure 12](#).

Figure 12 DNS Settings

Layer 3 Setting

VLAN GE Route **DNS**

Static DNS Server 1:

Static DNS Server 2:

Static DNS Server 3:

Submit Cancel

391773

2. Enter the IPv4 or IPv6 DNS server address in the Static DNS Server field. You can also set the value to blank.
3. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Wireless

You can configure the following wireless settings on the router:

- [Switching Wireless Mode](#)
- [Configuring AP Mode](#)
- [Configuring Station Mode](#)

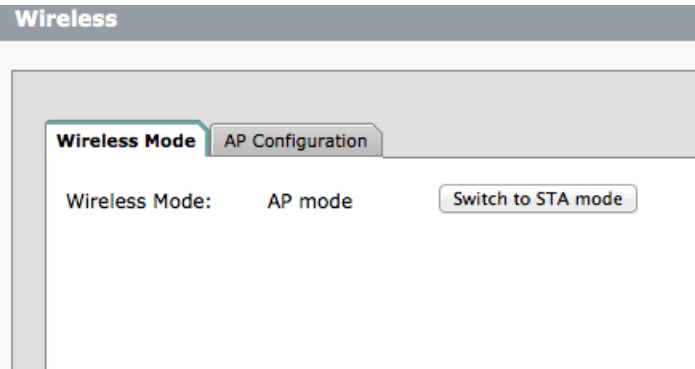
Switching Wireless Mode

You can get the information of current wireless mode and switch the wireless mode in the Wireless Mode tab.

Follow these steps to view or switch wireless mode on the router:

1. Click **Wireless** under Network Configuration in the left pane. The Wireless Mode tab is displayed, as shown in [Figure 13](#).

Figure 13 Wireless Mode



- 2. The current wireless mode is displayed in the right pane.
- 3. (Optional) Click the **Switch to STA mode** or **Switch to AP mode** button to change current wireless mode. If you change the wireless mode, there will be a pop up windows warning you the system should be switched mode to apply the changes and asking whether you want to continue or not.
- 4. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring AP Mode

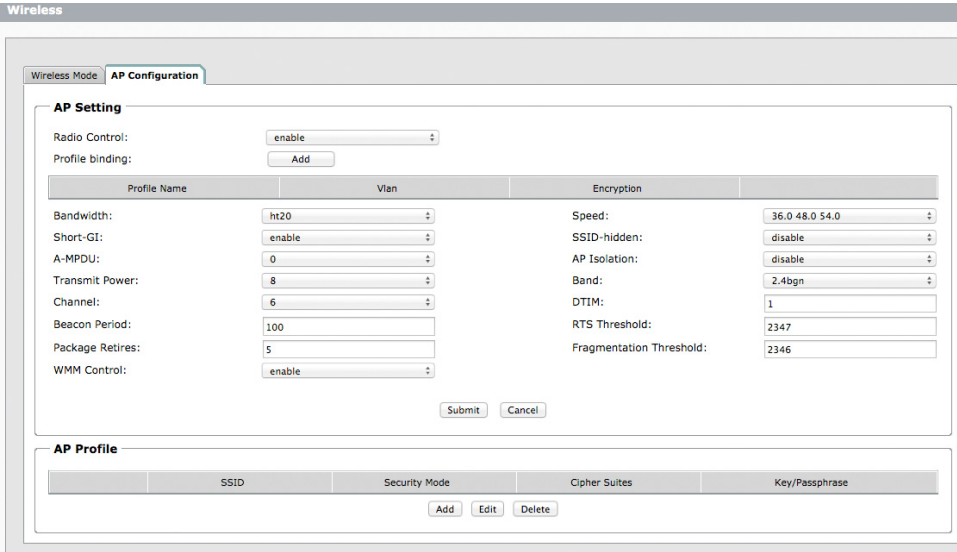
Use the AP Configuration tab to configure AP settings and manage the AP profiles.

Configuring AP Settings

Follow these steps to configure AP settings on the router:

- 1. Click **Wireless** under Network Configuration in the left pane and then click **AP Configuration** in the right pane. The AP Configuration tab is displayed, as shown in Figure 14.

Figure 14 AP Configuration



- 2. Choose a value for the fields with drop-down list and enter a value for the fields with a text box. For detailed information about AP settings, see the chapter of Configuring Wi-Fi.

3. Click **Submit** to save the changes and **Cancel** to discard the unsaved changes.

Managing AP Profiles

Use the AP profile area of the AP Configuration tab to add, edit, or delete AP profiles.

Follow these steps to add an AP profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **AP Configuration** in the right pane. The AP Configuration tab is displayed, as shown in [Figure 14](#).
2. To create a n AP profile, click **Add** in the AP Profile area to add a row in the profile binding table. The Add Profile window is displayed, as shown in [Figure 15](#).

Figure 15 Adding AP Profile

Add Profile [close](#)

SSID:

Auth Mode:

Encryption Mode:

391759

- c. Enter SSID in the SSID field,
- d. Choose authentication mode and encryption mode.
- e. Click OK to add the new profile.

Follow these steps to delete an AP profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **AP Configuration** in the right pane. The AP Configuration tab is displayed, as shown in [Figure 14](#).
2. Choose an profile in the binding table and click **Delete** to delete that row.

Follow these steps to modify an AP profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **AP Configuration** in the right pane. The AP Configuration tab is displayed, as shown in [Figure 14](#).
2. Choose an profile in the binding table and click **Edit**. The Edit Profile window is displayed, with the same options with the Add Profile window.
3. Enter SSID in the SSID field,
4. Choose authentication mode and encryption mode.
5. Click OK to save the changes.

Configuring Station Mode

Use the STA Configuration tab to configure station mode settings and manage the STA profiles.

Configuring STA Settings

Follow these steps to configure STA settings on the router:

1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in [Figure 16](#).

Figure 16 STA Configuration

Wireless

Wireless Mode 2.4G AP configuration 5G AP configuration STA configuration

☒ Auto-connect

	SSID	Security	Status
☒	test1	wep	Connected
☐	test2	wpa	

Add Connect Edit Move up Move down Delete

Submit Cancel

391799

2. Check **Auto-connect** to enable or uncheck to disable auto-connect feature.
3. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

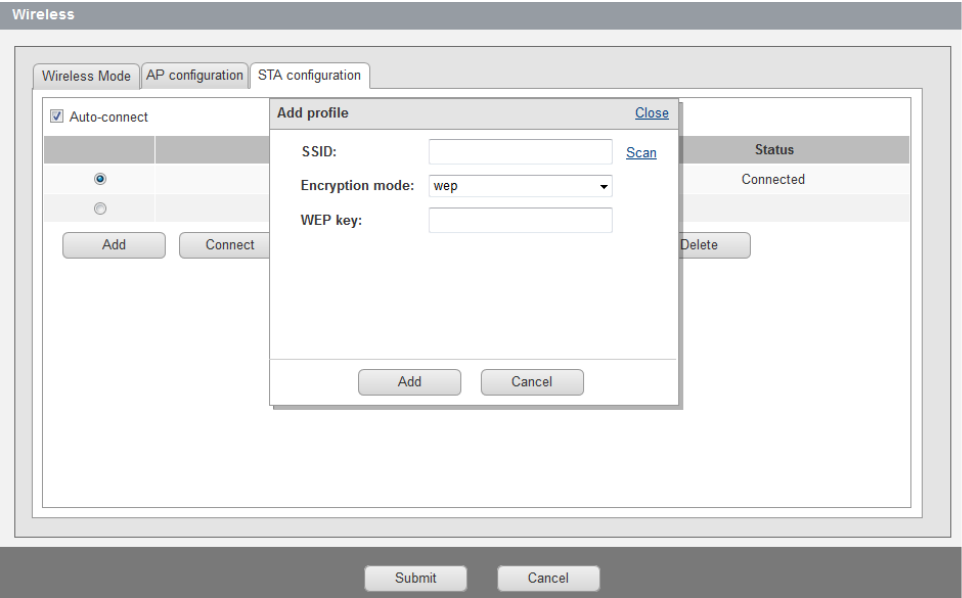
Managing STA Profiles

You can add, edit, or delete STA profiles, connect to or disconnect from an SSID, and change the SSID prefer list in the STA Configuration tab.

Follow these steps to add an STA profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in [Figure 16](#).
2. Click **Add** to add a row in the profile binding table. The Add Profile window is displayed, as shown in [Figure 17](#).

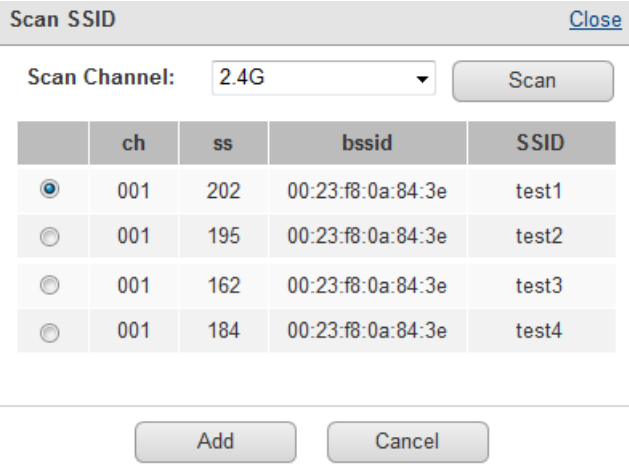
Figure 17 Adding STA Profile



- f. Enter the SSID directly in the SSID field and choose encryption mode from the drop-down list, or click **Scan** to list all SSIDs the router have scanned and choose one.

If you click **Scan**, the Scan SSID window opens. Choose the channel and click **Scan**. The SSIDs could be scanned and shown in the SSID list, as shown in Figure 18. Click **Add** to select the SSID.

Figure 18 Scaned SSID List



- 3. Choose encryption mode and enter the encryption key.
- 4. Click **OK** to add the new profile.

Follow these steps to connect to or disconnect from an SSID:

- 1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in Figure 16.
- 2. Choose an SSID from the list and click **Connect** or **Disconnect**.

Note: If the SSID you select is connected, the button will be shown as **Disconnect**.

Follow these steps to modify an STA profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in [Figure 16](#).
2. Choose an profile in the binding table and click **Edit**. The Edit Profile window is displayed, with the same options of the Add Profile window.
3. Enter SSID in the SSID field.
4. Choose authentication mode and encryption mode.
5. Click **OK** to save the changes.

Follow these steps to change the SSID prefer list:

1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in [Figure 16](#).
2. Choose an profile in the binding table and click **Priority**. The Priority Profile window is displayed.
3. Choose an profile in the list and click **Move up** or **Move down** to change the order.

Note: In AP mode, the **Connect/Disconnect** button in STA configuration tab is disabled. You can edit SSID profiles, but you cannot connect to any SSID in the STA configuration.

Follow these steps to delete an STA profile:

1. Click **Wireless** under Network Configuration in the left pane and then click **STA Configuration** in the right pane. The STA Configuration tab is displayed, as shown in [Figure 16](#).
2. Choose an profile in the list and click **Delete** to delete that row.

Configuring 3G USB Modem

You can configure the following 3G USB Modem settings on the router:

- [Configuring 3G Settings](#)
- [Binding GSM SIM Profiles](#)
- [Managing PIN](#)
- [Switching Firmware](#)

Configuring 3G Settings

You can search PLMN and configure 3G settings for UMTS or CDMA on the 3G Settings Tab.

- [Searching Available PLMNs](#)
- [Configuring 3G Settings for UMTS](#)
- [Configuring 3G Settings for CDMA](#)

Searching Available PLMNs

Follow the steps below to search available PLMNs.

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **3G Settings** in the right pane. The 3G Settings tab is displayed, as shown in [Figure 19](#).

Figure 19 3G Settings

3G USB Modem

3G setting profile pin Firmware

Radio: ON

Authentication Pin: The pin is verified

Timeout: 120 sec

PPP Authentication: NONE

IP Negotiated: ENABLE

Chat Name: gsm

Band: Auto-Band

PLMN Select: AUTO

Profile: 1

DDR: ON

Dialer String: gsm

Expect Send: ATDT*99***1# TIMEOUT 20

MCC	MNC	Inuse	Roaming	Forbidden	Preferred	Description	RAT

Search

PPP Status: Connecting

2. Click **Search**.
3. Make sure that the PIN is verified.
4. Click **Submit** and wait several minutes.
5. Complete the search operation according to the prompt information.

Configuring 3G Settings for UMTS

Follow the steps below to configure 3G settings for UMTS.

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **3G Settings** in the right pane. The 3G Settings tab is displayed, as shown in [Figure 19](#).
2. Choose **ON** or **OFF** from the Radio drop-down list, to turn on or turn off the radio hardware resources.
3. From the Profile drop-down list, choose the profile number from 1 to 16, to configure the SIM card to use profiles for GSM.
4. In the Authentication Pin field, enter a 4 to 8 character code to store the SIM CHV1 code for verification. You should input the correct PIN provided by your carrier to unlock the SIM card when you see a prompt message says "Please input the right pin."
5. Choose **ON** or **OFF** from the DDR drop-down list, to specify whether dial-on-demand routing (DDR) is supported or not.
6. In the Timeout field, specify the duration of idle time in seconds. This field is only valid when DDR is On.
7. Enter the name of the CHAT scrip in the Dialer String field.
8. Choose **NONE** or **CHAP** from the PPP Authentication drop-down list, to specify whether PPP configuration is supported or not. If you choose CHAP, specify PPP hostname and password as well.

- PPP hostname—An interface-specific CHAP hostname used for authentication. The hostname must match the username provided by the carrier.
- PPP Password—The password required for authentication of the remote router. The password must match the password provided by the carrier.
- 9. Choose **DISABLE** or **ENABLE** from the IP Negotiated drop-down list, to specify whether you can configure IP address and Net mask or not. When you choose **DISABLE**, manually enter IP address and net mask in both fields.
- 10. Enter the name of the CHAT script in the Chat Name field, to create a script that will place a call over a modem.
- 11. In the Expect Send field, enter a pair of information elements, which contains an item to expect and an item to send in response.
- 12. Choose one of the following bands from the Band drop-down list:
 - Auto-Band
 - GSM-All-Bands
 - WCDMA-All-Bands
- 13. Choose **AUTO** or **MANUAL** from the PLMN Select drop-down list, to automatically or manually select from the available public land mobile network (PLMN) to attach. If you select **MANUAL**, you must select one of the available technologies from the list of PLMNs.
- 14. Click **Submit**.

Configuring 3G Settings for CDMA

Follow the steps below to configure 3G settings for CDMA.

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **3G Settings** in the right pane. The 3G Settings tab is displayed, as shown in [Figure 19](#).
2. Choose **ON** or **OFF** from the Radio drop-down list, to turn on or turn off the radio hardware resources.
3. In the Authentication pin field, enter a 4 to 8 character code to store the SIM CHV1 code for verification. You should input the correct PIN provided by your carrier to unlock the SIM card when you see a prompt message says “Please input the right pin.”
4. Choose **ON** or **OFF** from the DDR drop-down list, to specify whether dial-on-demand routing (DDR) is supported or not.
5. In the Timeout field, specify the duration of idle time in seconds. This field is only valid when DDR is On.
6. Enter the name of the CHAT scrip in the Dialer String field.
7. Choose **NONE** or **CHAP** from the PPP Authentication drop-down list, to specify whether PPP configuration is supported or not. If you choose CHAP, specify PPP hostname and password as well.
 - PPP hostname—An interface-specific CHAP hostname used for authentication. The hostname must match the username provided by the carrier.
 - PPP Password—The password required for authentication of the remote router. The password must match the password provided by the carrier.
8. Choose **DISABLE** or **ENABLE** from the IP Negotiated drop-down list, to specify whether you can configure IP address and Net mask. When you choose **DISABLE**, manually enter IP address and net mask in both fields.
9. Enter the name of the CHAT script in the Chat Name field, to create a script that will place a call over a modem.

10. In the Expect Send field, enter a pair of information elements, which contains an item to expect and an item to send in response.
11. Choose one of the following modes from the Cellular Mode drop-down list:
 - 1xRTT
 - 1xEVDO
 - hybrid
12. Click **Submit**.

Binding GSM SIM Profiles

Follow the steps below to bind GSM SIM profiles.

The CDMA profile tab cannot be edit. It is only used to display the information.

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **Profile** in the right pane. The Profile tab is displayed, as shown in [Figure 20](#).

Figure 20 3G Profiles

	Profile Id	APN	Authentication	UserName	Password	Protocol
☐	1	internet	NONE			IPv4
☐	2	wap.cingular	NONE			IPv4

391896

2. Click **Create** in Profile binding field, the Profile Binding Table will add a row. You can click **Modify** or **Remove** if you want to modify or delete that row. You can assign one profile ID to a SIM profile.
3. In the Profile Id field, enter the ID of the profile.
4. Enter the Access Point Name (APN) in the APN field.
5. Choose CHAP, PAP, or None from the Authentication drop-down list.
6. Enter the user name and password required for authentication.
7. From the Protocol drop-down list, choose IPv4, IPv6, IPv4v6, or PPP.
8. Click **Submit**.

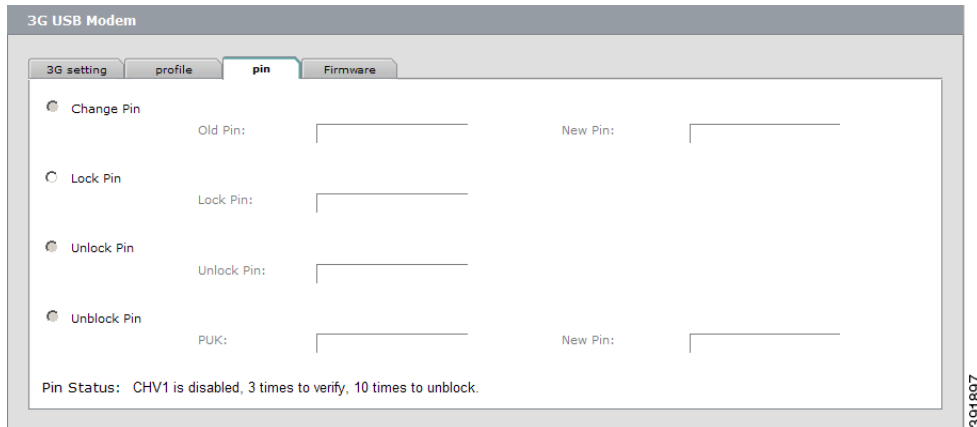
Managing PIN

You can use the PIN tab to change the PIN, lock or unlock the PIN, and unblock a PIN.

Follow the steps below to manage the PIN:

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **PIN** in the right pane. The PIN tab is displayed, as shown in [Figure 21](#).

Figure 21 Managing PIN



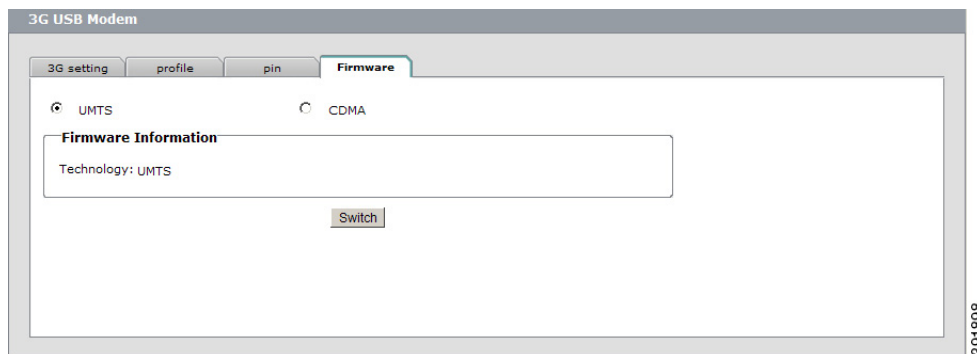
2. Choose the option that you want and click **Submit**.

Switching Firmware

Follow the steps below to switch the firmware:

1. Click **3G USB Modem** under Network Configuration in the left pane and then click **Firmware** in the right pane. The Firmware tab is displayed, as shown in [Figure 22](#).

Figure 22 Switching Firmware



2. Choose the firmware that you want and click **Switch**.

Configuring PPPoE

You can configure the following PPPoE settings on the router:

- [Adding a PPPoE Profile](#)
- [Editing a PPPoE Profile](#)
- [Connecting or Disconnecting a PPPoE](#)

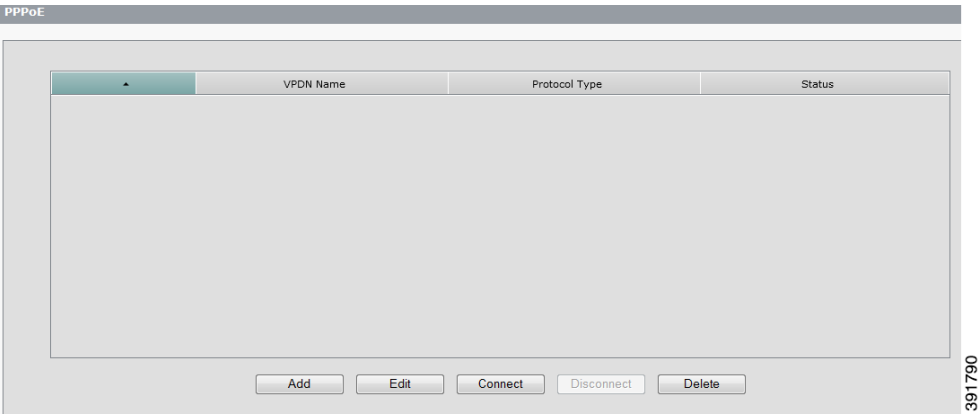
■ Deleting a PPPoE Profile

Adding a PPPoE Profile

Follow these steps to add a PPPoE profile:

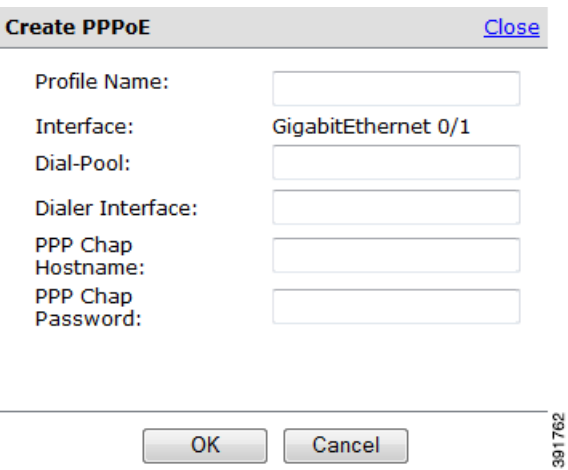
- 1. Click **PPPoE** under Network Configuration in the left pane. The PPPoE window is displayed, as shown in [Figure 23](#).

Figure 23 PPPoE Configuration



- 2. Click **Add** to add a row in the profile table. The Create PPPoE window is displayed, as shown in [Figure 24](#).

Figure 24 Add PPPoE Profile



- 3. Enter the following values to create the PPPoE profile:
 - Profile Name—Specify the PPPoE profile name.
 - Dial-Pool—Specify the dialing pool for PPPoE.
 - Dialer Interface—Specify Dialer interface number for PPPoE.
 - PPP Chap Hostname—Specify an interface-specific CHAP hostname.
 - PPP Chap Password—Specify an interface-specific CHAP password.

4. Click **OK** to add the new profile.

Editing a PPPoE Profile

Follow these steps to edit a PPPoE profile:

1. Click **PPPoE** under Network Configuration in the left pane.
2. Choose a profile from the list and click **Edit**. The Edit Profile window is displayed, with the same options with the Add Profile window.
3. Make the changes that you want.
4. Click **OK** to save the changes.

Connecting or Disconnecting a PPPoE

Follow these steps to connect to or disconnect from a PPPoE connection:

1. Click **PPPoE** under Network Configuration in the left pane.
2. Choose an profile in the list and click **Connect** or **Disconnect**.

Deleting a PPPoE Profile

Follow these steps to delete a PPPoE profile:

1. Click **PPPoE** under Network Configuration in the left pane.
2. Choose an profile in the list and click **Delete** to delete that row.

Configuring VLAN

You can configure the following VLAN settings on the router:

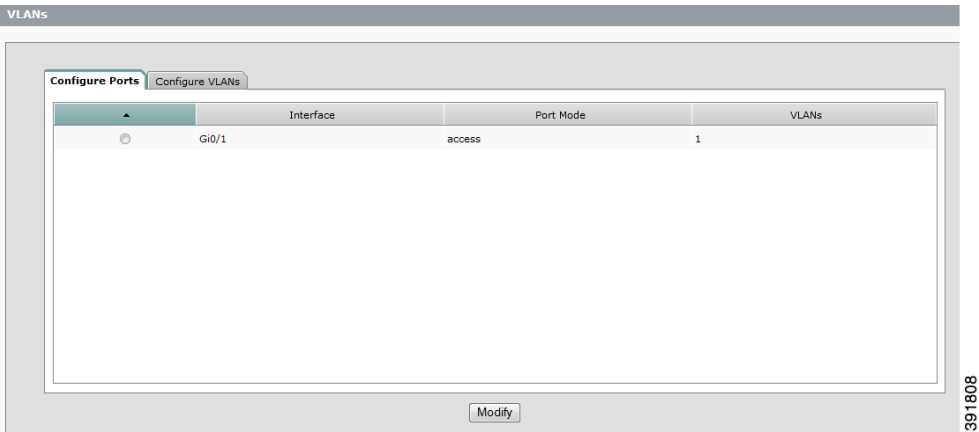
- [Creating VLANs](#)
- [Deleting VLANs](#)
- [Configuring Port and VLAN Membership](#)

Creating VLANs

Follow these steps to create a VLAN:

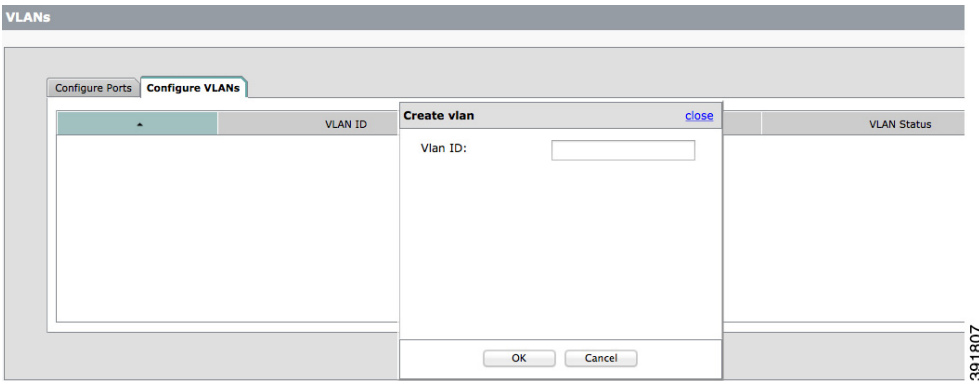
1. Click **VLAN** under Network Configuration in the left pane. The Configure Ports tab is displayed, as shown in [Figure 25](#).

Figure 25 VLAN Ports Settings



2. Click **Configure VLANs** tab to display the VLAN Configuration.
3. Click the **Create** button. The Create VLAN window is displayed, as shown in Figure 26.

Figure 26 VLAN Settings-Creating VLAN



4. Enter VLAN ID.
5. Click **OK** to create the VLAN.

Deleting VLANs

Follow these steps to delete a VLAN:

1. Click **VLAN** under Network Configuration in the left pane. The VLAN settings window is displayed, as shown in Figure 23.
2. Click **Configure VLANs** to display the VLAN Configuration.
3. Choose a VLAN from the list and click **Delete** to delete that row.

Configuring Port and VLAN Membership

Follow these steps to configure the VLAN setting of the port:

1. Click **VLAN** under Network Configuration in the left pane. The Configure Ports tab is displayed, as shown in [Figure 25](#).
2. Choose the port and click **Modify**. The Modify ports window is displayed, as shown in [Figure 27](#).

Figure 27 Modify Ports

Modify ports [Close](#)

Interface:

Port mode:

Access vlan:

391781

1. Choose the port mode, **access** or **trunk**.
2. If you choose access mode, enter access VLAN ID; If you choose trunk, choose trunking mode, configure allowed VLAN and native VLAN.
3. Click **OK** to save the changes and **Cancel** to restore the previous values.

Configuring VPN

The router supports the following types of VPN connections:

- PPTP
- IPSEC
- L2TP

To add, edit, and remove a VPN connection, or connect to a VPN, click **VPN** in the left pane. The VPN information window is displayed in the right pane.

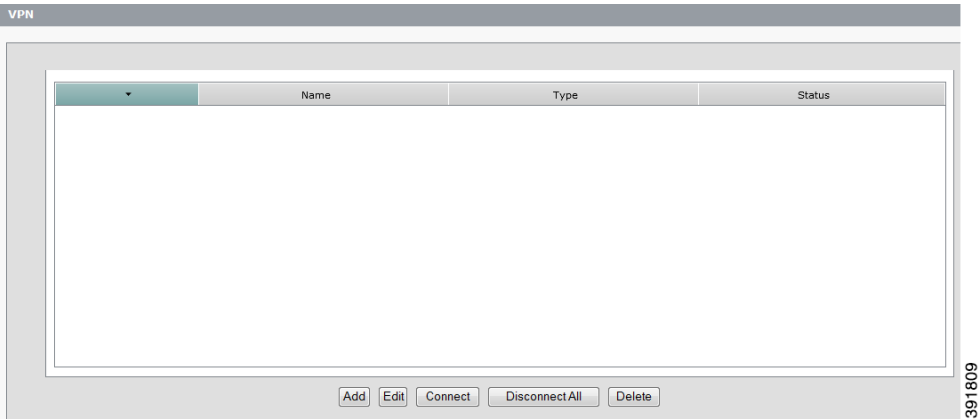
- [Adding a VPN connection](#)
- [Connecting a VPN Connection](#)
- [Disconnecting a VPN Connection](#)
- [Deleting a VPN Connection](#)

Adding a VPN connection

To add a VPN connection of PPTP type, follow these steps:

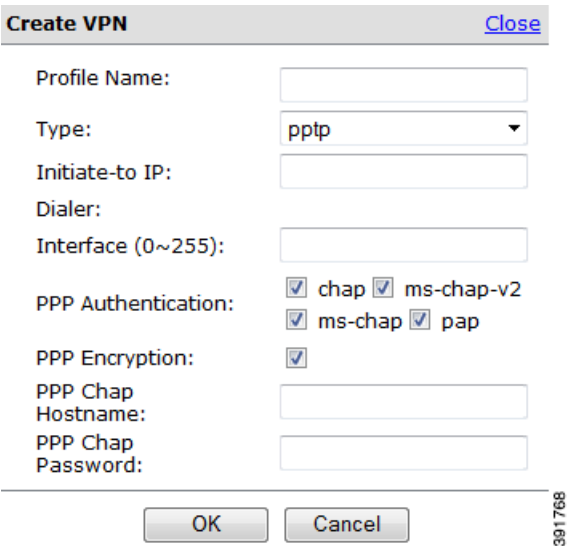
- 1. Click **VPN** in the left pane under Network Configuration. The VPN window is displayed, as shown in [Figure 28](#).

Figure 28 VPN Settings



- 2. Click **Add** in the right pane. A new window is displayed, as shown in [Figure 29](#).

Figure 29 Add VPN Connection



- 3. Enter the name of the VPN connection that you want to add in the Profile Name field.
- 4. Choose a VPN connection type from the Type drop-down list.
- 5. Enter the fields for each type.
- 6. Click **OK** to add the VPN connection.

Connecting a VPN Connection

To connect a VPN connection, select the VPN connection that you want to connect from the connection list in the VPN tab, and click **Connect**.

Disconnecting a VPN Connection

To disconnect a VPN connection, select the VPN connection that you want to disconnect from the connection list in the VPN tab, and click **Disconnect**.

Deleting a VPN Connection

To delete a VPN connection, select the VPN connection that you want to delete from the connection list in the VPN tab, and click **Delete**.

Configuring DHCP

Use the DHCP window to configure IPv4 or IPv6 DHCP server.

- [Configuring IPv4 DHCP Server](#)
- [Configuring IPv6 DHCP Server](#)

Configuring IPv4 DHCP Server

Follow these steps to configure the IPv4 DHCP server:

1. Click **DHCP** in the left pane under Network Configuration. The DHCP window is displayed, as shown in [Figure 30](#).

Figure 30 DHCP Settings

DHCP

IPv4 DHCP Server

☐ Enable IPv4 DHCP Server

Network:

Range:

Domain Name:

Default Router:

Netmask:

to

DNS Server:

IPv6 DHCP Server

☐ Enable IPv6 DHCP Server

Address Prefix:

Range:

DNS Server:

Domain Name:

to:

Submit

Cancel

391772

2. Check **Enable IPv4 DHCP Server** to enable the IPv4 DHCP Server.
3. Enter the IP address of the server in the Network field and choose the netmask.
4. Enter the DHCP pool range in Range and to fields.
5. Enter the Domain Name, DNS Server and the Default Router if you want.
6. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

30

Configuring IPv6 DHCP Server

Follow these steps to configure the IPv6 DHCP server:

1. Click **DHCP** in the left pane under Network Configuration. The DHCP window is displayed, as shown in [Figure 30](#).
2. Check **Enable IPv6 DHCP Server** to enable the IPv6 DHCP Server.
3. Enter the address prefix for address assignment in the Address Prefix field.
4. Enter the DHCP pool range in Range and to fields.
5. Enter the Domain Name and DNS Server if you want.
6. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring NAT

Follow these steps to configure NAT on the router:

1. Click **NAT** in the left pane under Network Configuration. The NAT window is displayed, as shown in [Figure 31](#).

Figure 31 NAT Configuration

2. Check **Enable NAT** to enable the NAT on the router.
3. Choose the inside interface. If you choose a VLAN interface, make sure there is at least one VLAN exists.
4. Enter the IP address and subnet mask of the inside interface.
5. Choose one of the following as the outside interface:
 - GigabitEthernet—GigabitEthernet interface.
 - Dialer—If you choose a dialer interface, make sure there is at least one dialer interface exists.
 - Dot11 radio—Wi-Fi interface. Only available for the model IR910W-K9.
 - Cellular—3G interface. Only available for the models IR910G-K9 and IR910G-NA-K9.
6. Enter the IP address and subnet mask of the outside interface.
7. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Configuring Platform Settings

Platform configuration includes the following information:

- [Configuring Ports](#)
- [Configuring SNMP](#)
- [Configuring Authentication, Authorization, and Accounting](#)
- [Configuring Time](#)
- [Configuring HTTPS](#)
- [Displaying TDR Results](#)

Configuring LLDP

Use the LLDP window to configure LLDP settings and neighbors:

- [Configuring LLDP Settings](#)
- [Displaying LLDP Neighbors](#)

Configuring LLDP Settings

Follow these steps to configure the LLDP settings:

1. Click **LLDP** in the left pane under Platform Configuration. The LLDP Settings window is displayed, as shown in [Figure 32](#).

Figure 32 LLDP Settings

LLDP

LLDP Settings Neighbors

LLDP: ☒ Enable ☐ Disable

LLDP Holdtime: 120s

LLDP Timer: 30 s

LLDP Reinitialization Delay: 1s

391779

2. Choose **Enable** to enable LLDP. If you want to disable LLDP, choose **Disable**.
3. Enter the value of LLDP timer. LLDP Holdtime and LLDP Reinitialization Delay are read-only fields.
4. Click **Submit** to save the changes and **Clear** to discard the unsaved changes.

Displaying LLDP Neighbors

To display LLDP neighbor information, click **LLDP** in the left pane under Platform Configuration and click Neighbors in the right pane.

Configuring SNMP

Use the SNMP window to configure the following settings:

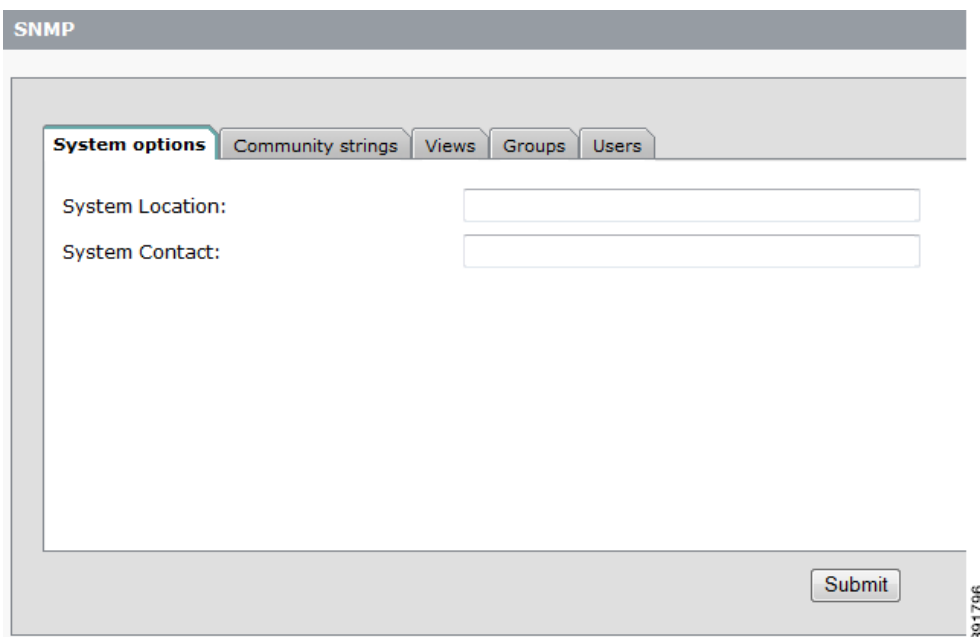
- [Configuring SNMP System Options](#)
- [Configuring SNMP Community Strings](#)
- [Configuring SNMP Views](#)
- [Configuring SNMP Groups](#)
- [Configuring SNMP Users](#)

Configuring SNMP System Options

Follow these steps to configure SNMP system options:

1. Click **SNMP** in the left pane under Platform Configuration. The System options tab of SNMP window is displayed, as shown in [Figure 33](#).

Figure 33 SNMP System Options



The screenshot shows the 'SNMP' configuration window. At the top, there is a tabbed interface with five tabs: 'System options' (which is selected and highlighted in green), 'Community strings', 'Views', 'Groups', and 'Users'. Below the tabs, there are two text input fields. The first field is labeled 'System Location:' and the second is labeled 'System Contact:'. Both fields are empty. At the bottom right of the window, there is a 'Submit' button. The window has a light gray background and a dark gray header bar with the text 'SNMP'.

2. In the System Location field, enter the location of the person that is identified as the system contact. The string can be up to 127 characters and is case sensitive. Spaces are allowed, but multiple spaces are shortened to a single space.
3. In the System Contact field, enter a person to notify when problems occur. The string can be up to 127 characters and is case sensitive. Spaces are allowed, but multiple spaces are shortened to a single space.
4. Click **Submit** to save the changes.

Configuring SNMP Community Strings

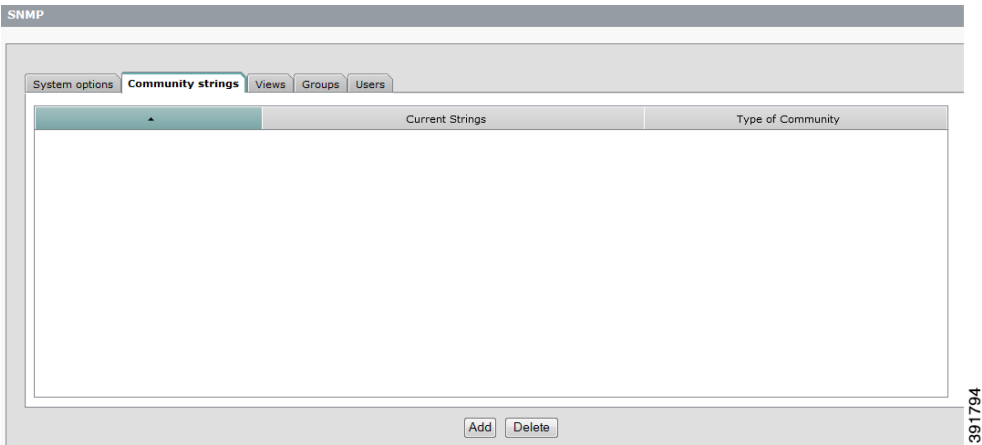
Use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. Optionally, you can specify one or more of these characteristics associated with the string.

Adding SNMP Community Strings

Follow these steps to add an SNMP community string:

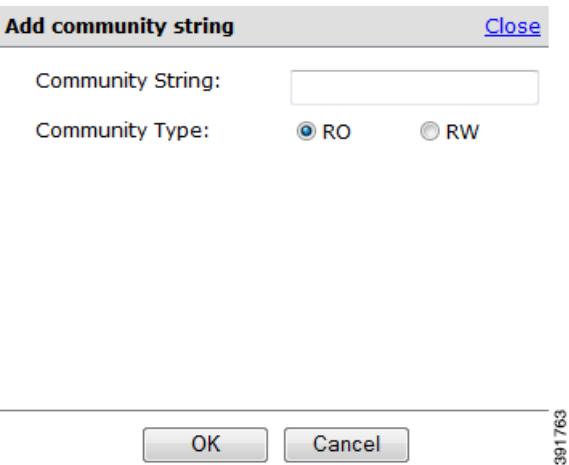
- 1. Click **SNMP** in the left pane under Platform Configuration and click Community strings in the right pane. The Community strings tab of SNMP window is displayed, as shown in Figure 34.

Figure 34 SNMP Community Strings



- 2. Click **Add** to open the Add Community Strings window, as shown in Figure 35.

Figure 35 Add SNMP Community String



- 3. Enter a string in the Community String field.
- 4. Choose **RO** or **RW** for the Community Type option. Specify read-only (RO) if you want authorized management stations to retrieve MIB objects; Specify read-write (RW) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects.
- 5. Click **Add** to add the community string.

Deleting SNMP Community Strings

Follow these steps to delete an SNMP community string:

- 1. Click **SNMP** in the left pane under Platform Configuration and click **Community strings** in the right pane. The Community strings tab of SNMP window is displayed, as shown in [Figure 34](#).
- 2. Choose the line that you want to delete and click **Delete**.

Configuring SNMP Views

To restrict a group of users to view a specific MIB tree, you must create an SNMP view using the device manager. Once you create the view, you need to create an SNMP group and SNMP users that belong to this group as described in later sections.

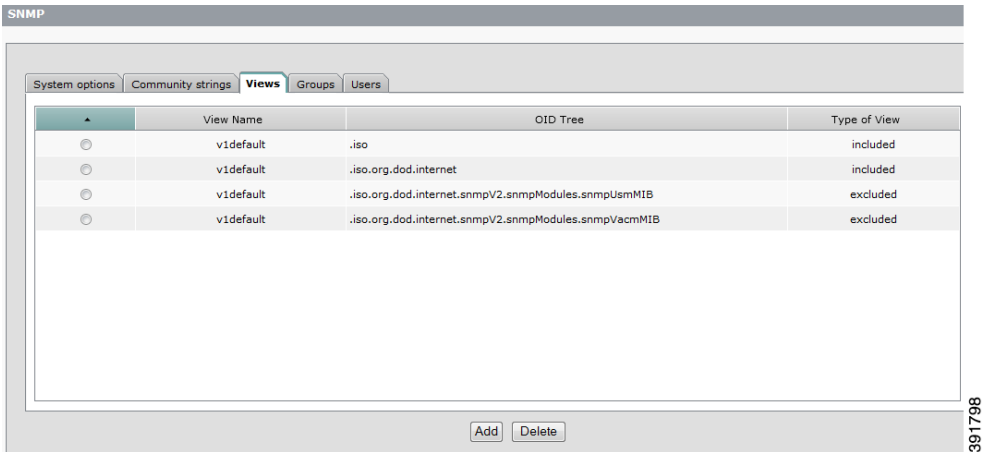
Views are listed in the order in which they have been created. You can create up to 10 views.

Adding SNMP Views

Follow these steps to add SNMP views:

- 1. Click **SNMP** in the left pane under Platform Configuration and click **Views** in the right pane. The Views tab of SNMP window is displayed, as shown in [Figure 36](#).

Figure 36 SNMP Views



- 2. Click **Add** to open the Add View window, as shown in [Figure 37](#).

Figure 37 Add SNMP View

Add view [Close](#)

View Name:

OID Tree:

Type of View: ☒ included ☐ excluded

391766

3. Enter a name in the View Name field.
4. Enter the object identifier in the OID Tree field. This value identifies a subtree of the MIB. It can be up to 64 alphanumeric characters.
5. Choose a type for the Type of View option.
 - **included**—The MIB family is included in the view.
 - **excluded**—The MIB family is excluded from the view.
6. Click **OK** to add the community string.

Deleting SNMP Views

Follow these steps to delete an SNMP view:

1. Click **SNMP** in the left pane under Platform Configuration and click **Views** in the right pane. The Views tab of SNMP window is displayed, as shown in [Figure 36](#).
2. Choose the line that you want to delete and click **Delete**.

Configuring SNMP Groups

You must set up an SNMP group if you are going to create any SNMP users or want to restrict a group of users to view a specific MIB subtree.

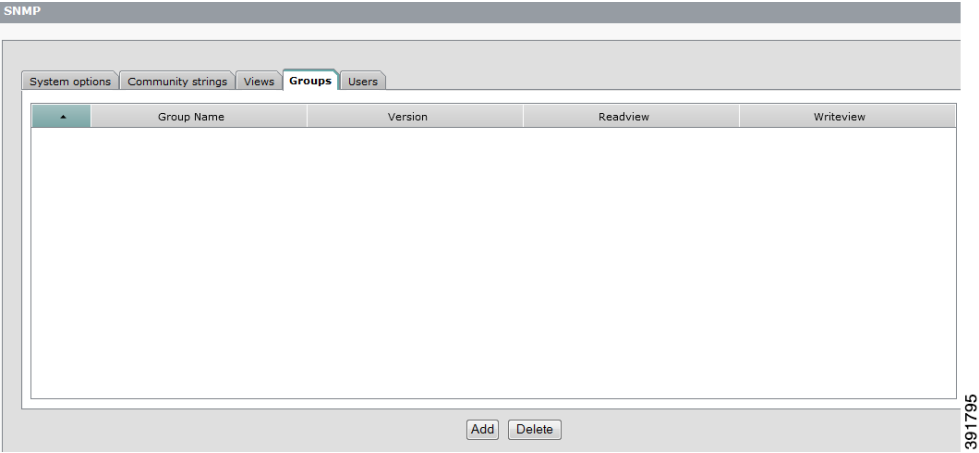
Groups are listed in the order in which they have been created. The maximum number of SNMP groups that can be created is 10.

Adding SNMP Groups

Follow these steps to add SNMP groups:

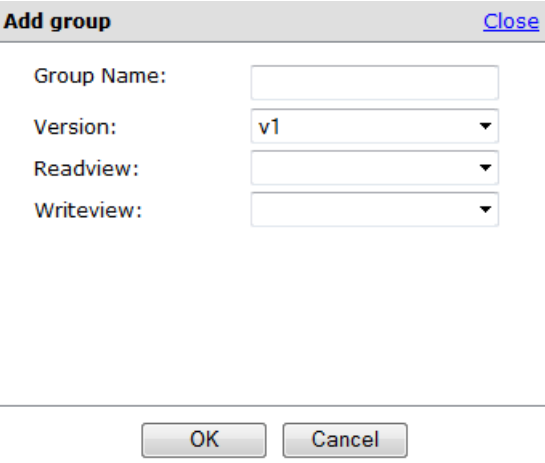
1. Click **SNMP** in the left pane under Platform Configuration and click **Groups** in the right pane. The Groups tab of SNMP window is displayed, as shown in [Figure 38](#).

Figure 38 SNMP Groups



2. Click **Add** to open the Add Group window, as shown in Figure 37.

Figure 39 Add SNMP Group



3. Enter a name in the Group Name field.
4. Choose a security version from the Version drop-down list. Valid values are:
- v1—Version 1 security model (SNMP Version 1 [noAuthNoPriv]).
 - v2c—Version 2c security model (SNMP Version 2 [noAuthNoPriv]).
 - v3-auth—User security level (SNMP Version 3 [AuthNoPriv]).
 - v3-noauth—User security level (SNMP Version 3 [noAuthNoPriv]).
 - v3-priv—User security level (SNMP Version 3 [AuthPriv]).
5. Choose Readview and Writerview.
6. Click **OK** to add the group.

Deleting SNMP Groups

Follow these steps to delete an SNMP group:

- 1. Click **SNMP** in the left pane under Platform Configuration and click **Groups** in the right pane. The Groups tab of SNMP window is displayed, as shown in [Figure 38](#).
- 2. Choose the line that you want to delete and click **Delete**.

Configuring SNMP Users

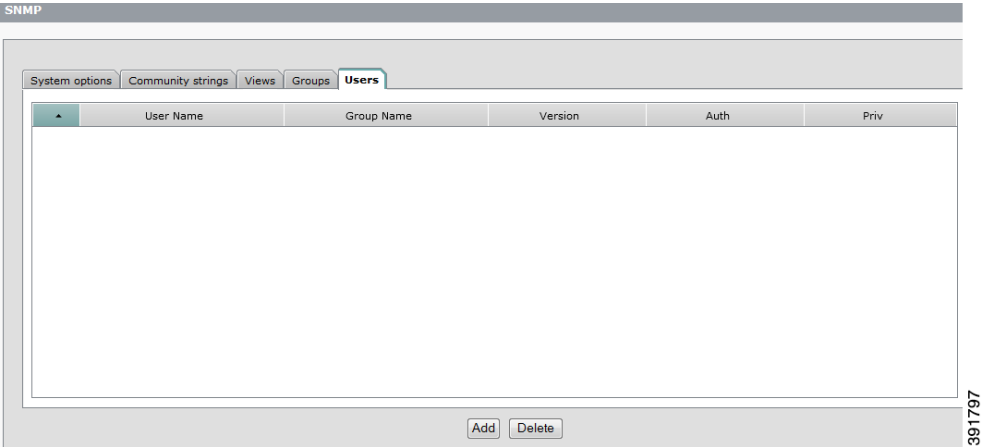
Users are listed in the order in which they have been created. The maximum number of users that can be created is 10. Before you add users, make sure there is at least one group that has already been created.

Adding SNMP Groups

Follow these steps to add SNMP groups:

- 1. Click **SNMP** in the left pane under Platform Configuration and click **Groups** in the right pane. The Users tab of SNMP window is displayed, as shown in [Figure 40](#).

Figure 40 SNMP Users



- 2. Click **Add** to open the Add User window, as shown in [Figure 41](#).

Figure 41 Add SNMP User

Add user [Close](#)

User Name:

Group Name:

Version:

391765

3. Enter a name in the User Name drop-down list.
4. Choose a group from the Group Name field.
5. Choose a security version from the Version drop-down list. Valid values are v1, v2c, and v3. If you choose v3, enter the values in the Auth, Auth-password, Priv, and Prov-password fields as well.
6. Click **OK** to add the group.

Deleting SNMP Users

Follow these steps to delete an SNMP user:

1. Click **SNMP** in the left pane under Platform Configuration and click **Users** in the right pane. The Users tab of SNMP window is displayed, as shown in [Figure 38](#).
2. Choose the line that you want to delete and click **Delete**.

Configuring Authentication, Authorization, and Accounting

The router supports local authentication using the local lookup database or remote authentication using one or more RADIUS servers. Use the AAA window to configure the authentication.

- [Configuring Authentication Type](#)
- [Configuring RADIUS Server List](#)
- [Configuring RADIUS Group List](#)
- [Configuring Local Authentication](#)

Configuring Authentication Type

Follow these steps to configure authentication type:

1. Click **AAA** in the left pane under Platform Configuration. The Authentication Type tab of AAA window is displayed, as shown in [Figure 42](#).

Figure 42 Authentication Type

Authentication, Authorization and Accounting

Authentication Type Radius Server List Radius Group List Local Authentication

Authentication Type	Detail
☐ Radius Authentication	Radius Group Name
☒ Local Authentication	

Submit

391755

2. Choose **Radius authentication** or **Local Authentication** in the Authentication Type column.
3. Click **Submit** to save the change.

Configuring RADIUS Server List

Use the RADIUS Server List tab to add, edit, or delete RADIUS servers.

Adding RADIUS Servers

Follow these steps to add a RADIUS server:

1. Click **AAA** in the left pane under Platform Configuration and click **RADIUS Server List** in the right pane. The RADIUS Server List tab of AAA window is displayed, as shown in [Figure 43](#).

Figure 43 RADIUS Server List

Authentication, Authorization and Accounting

Authentication Type Radius Server List Radius Group List Local Authentication

Server ip / hostname	Port
----------------------	------

Add Edit Delete

391754

2. Click **Add** to open the Add RADIUS Server window, as shown in [Figure 44](#).

Figure 44 Add RADIUS Server

Add radius server [close](#)

server ip/name:

server port:

key:

key confirm:

OK Cancel

391758

3. Enter the domain name or IP address of the RADIUS server in the server ip/name field.
4. Enter the UDP destination port for authentication requests in the server port field.
5. Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server in the key field. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
6. Enter the value in the key field again in the key confirm field.
7. Click **OK** to add the RADIUS server.

Deleting RADIUS Servers

Follow these steps to delete a RADIUS server:

1. Click **AAA** in the left pane under Platform Configuration and click **RADIUS Server List** in the right pane. The RADIUS Server List tab of AAA window is displayed, as shown in [Figure 43](#).
2. Choose the line that you want to delete from the RADIUS server list and click **Delete**.

Configuring RADIUS Group List

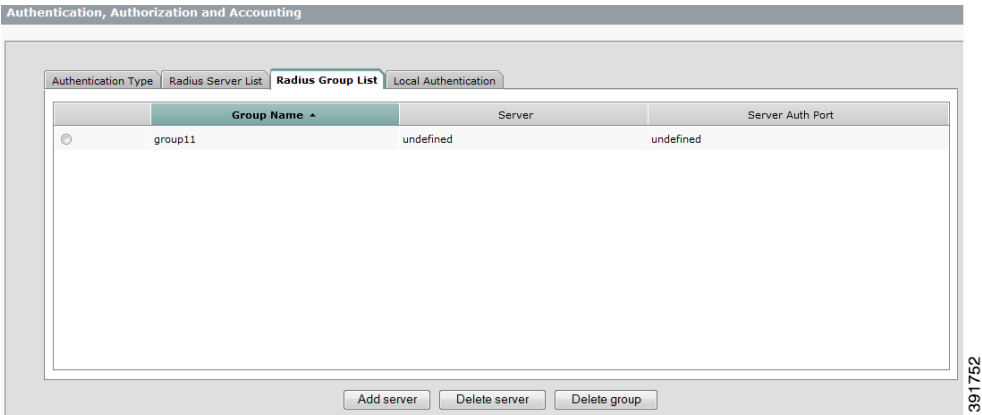
Use the RADIUS Group List tab to add, edit, or delete RADIUS groups.

Adding RADIUS Groups

Follow these steps to add a RADIUS group:

1. Click **AAA** in the left pane under Platform Configuration and click **RADIUS Group List** in the right pane. The RADIUS Group List tab of AAA window is displayed, as shown in [Figure 45](#).

Figure 45 RADIUS Group List



2. Click **Add** to open the Add RADIUS Group window, as shown in Figure 46.

Figure 46 Add RADIUS Group

Add Radius Group [close](#)

group name:

server:

server auth-port:

OK

Cancel

3. Enter a name in the group name field.
4. Enter the IP address or domain name of the server in the server field.
5. Enter the UDP destination port for authentication requests in the server auth-port field.
6. Click **OK** to add the RADIUS group.

Deleting RADIUS Groups

Follow these steps to delete a RADIUS group:

1. Click **AAA** in the left pane under Platform Configuration and click **RADIUS Group List** in the right pane. The RADIUS Group List tab of AAA window is displayed, as shown in Figure 45.
2. Choose the line that you want to delete from the RADIUS group list and click **Delete group**.

Configuring Local Authentication

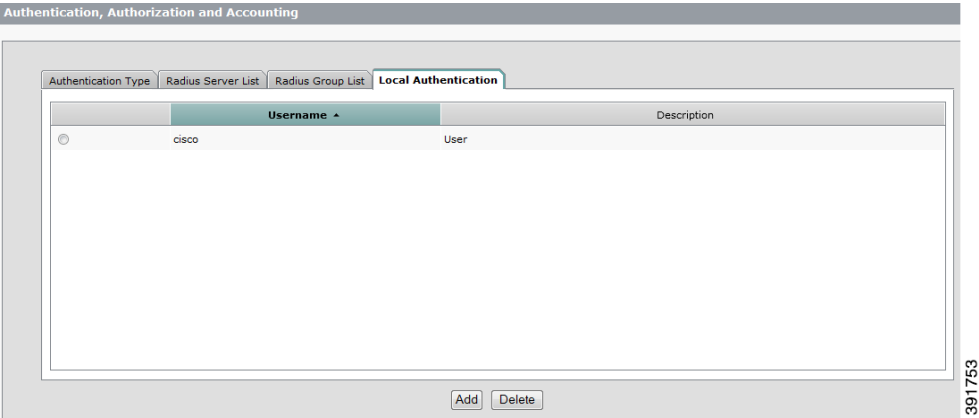
Use the Local Authentication tab to add or delete local users.

Adding Local Users

Follow these steps to add a local authentication user:

- 1. Click **AAA** in the left pane under Platform Configuration and click **Local Authentication** in the right pane. The Local Authentication tab of AAA window is displayed, as shown in [Figure 47](#).

Figure 47 Local Authentication



- 2. Click **Add** to open the Add local user window, as shown in [Figure 48](#).

Figure 48 Add Local User

Add local user [close](#)

user name:

password:

confirm passsword:

user description:

OK

Cancel

391757

- 3. Enter user name, password, and description of the user, and repeat the password in the confirm password field.
- 4. Click **OK** to add the local user.

Deleting Local Users

Follow these steps to delete a local user:

- 1. Click **AAA** in the left pane under Platform Configuration and click **Local Authentication** in the right pane. The Local Authentication tab of AAA window is displayed, as shown in [Figure 43](#).
- 2. Choose the line that you want to delete from the list and click **Delete**.

Configuring Time

The router allows you to perform time synchronization using Network Time Protocol (NTP) or set time manually. You can configure either way in this window:

- [Configuring NTP Server](#)
- [Configuring NTP Key](#)
- [Configuring Time Manually](#)

Configuring NTP Server

Use the NTP Server tab to add, edit, or delete NTP servers.

Adding NTP Servers

Follow these steps to add a NTP server:

1. Click **Time** in the left pane under Platform Configuration. The NTP Server tab of Time window is displayed.
2. Click **Add** to open the Add NTP Server window, as shown in [Figure 49](#).

Figure 49 Add NTP Server

Add ntp server [close](#)

Server Address:

Server Address Type: ☐ ip address ☐ hostname(v4) ☐ hostname(v6)

Key Number:

Maxpoll:

Minpoll:

Prefer: ☐

burst: ☐

iburst: ☐

391761

3. Enter the IP address of the NTP server in the Server Address field.
4. Choose the server address type:
 - IP address
 - hostname(V4)
 - hostname(V6)
5. Enter the key number in the Key Number field.
6. (Optional) Enter the maximum polling time interval in seconds in the Maxpoll field.
7. (Optional) Enter the minimum polling time interval in seconds in the Minpoll field.

8. Click **OK** to add the NTP server.

Deleting NTP Servers

Follow these steps to delete a NTP server:

1. Click **Time** in the left pane under Platform Configuration. The NTP Server tab of Time window is displayed.
2. Choose the line that you want to delete from the NTP server list and click **Delete**.

Configuring NTP Key

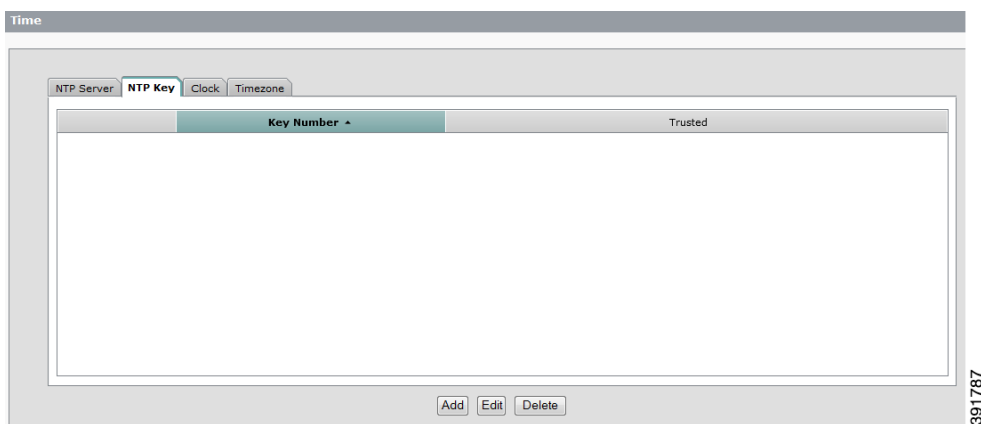
Use the NTP Key tab to add, edit, or delete NTP Keys.

Adding NTP Keys

Follow these steps to add a NTP key:

1. Click **Time** in the left pane under Platform Configuration and click **NTP Key** in the right pane. The NTP Key tab of Time window is displayed, as shown in [Figure 50](#).

Figure 50 NTP Key



2. Click **Add** to open the Add NTP Key window, as shown in [Figure 51](#).

Figure 51 Add NTP Key

Add ntp key [close](#)

Key Number:

Key Value:

Confirm Key Value:

Trusted: ☐

OK Cancel

391760

3. Enter the key number in the Key Number field. The key number is an unsigned 32 bit integer.
4. Enter the key value in the Key Value field. The key value is an 8-character ASCII string.
5. Confirm the key value.
6. Check Trusted if this key value is to be trusted.
7. Click **OK** to add the NTP key.

Deleting NTP Keys

Follow these steps to delete a NTP key:

1. Click **Time** in the left pane under Platform Configuration and click **NTP Key** in the right pane. The NTP Key tab of Time window is displayed, as shown in [Figure 50](#).
2. Choose the line that you want to delete from the NTP key list and click **Delete**.

Configuring Time Manually

In addition to configure the system time by NTP servers, you can configure the time manually using the Clock tab and Timezone tab.

Configuring System Clock

Follow these steps to configure local system time:

1. Click **Time** in the left pane under Platform Configuration and click **Clock** in the right pane. The Clock tab of Time window is displayed, as shown in [Figure 52](#).

Figure 52 Configuring Time Manually

The screenshot shows the 'Time' configuration window with the 'Clock' tab active. It contains two main sections: 'Date' and '24-hour-clock'. The 'Date' section has input fields for Year (2014), Month (Jun), and Day (25). The '24-hour-clock' section has input fields for Hour (16), Minute (55), and Second (47). A 'Submit' button is located at the bottom right of the form.

2. Enter values in the Year, Month, Day, Hour, Minute, and Second fields.
3. Click **Submit** to save the time.

Configuring Time Zone

Follow these steps to configure time zone for the local time:

1. Click **Time** in the left pane under Platform Configuration and click **Timezone** in the right pane. The Timezone tab of Time window is displayed, as shown in [Figure 53](#).

Figure 53 Time Zone Setting

The screenshot shows the 'Time' configuration window with the 'Timezone' tab active. It contains a single input field labeled 'Time Zone' with the value 'UTC'. A 'Submit' button is located at the bottom right of the form.

2. Enter a time zone value in the Time Zone field.
3. Click **Submit** to save the time zone setting.

Configuring HTTPS

Follow these steps to enable HTTPS on the router:

1. Click **HTTPS** in the left pane under Platform Configuration. The HTTPS window is displayed, as shown in [Figure 54](#).

Figure 54 HTTPS Setting

Https

☐ Enable https

Https port: 443

- 2. Check **Enable https** to enable the HTTPS function on the router.
- 3. In the HTTPS port field, enter the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.
- 4. Click **Submit** to save the changes.

Displaying TDR Results

The router allows you to show Time-Domain Reflectometer (TDR) test results for an interface.

Follow these steps to display TDR results:

- 1. Click **TDR** in the left pane under Platform Configuration.
- 2. Choose an interface from the Interface drop-down list.
- 3. Click the Test button on the right of the Interface drop-down list. The TDR results are displayed, as shown in [Figure 55](#).

Figure 55 TDR Results

TDR

Interface: Gi0/1 Test

Result:

Port	Speed	Local pair	Pair Length	Remote pair	Pair status
Gi0/1	1000M	Pair A	< 50M	Pair A	Normal
		Pair B	< 50M	Pair B	Normal
		Pair C	< 50M	Pair C	Normal
		Pair D	< 50M	Pair D	Normal

Monitoring the Status of System and Network

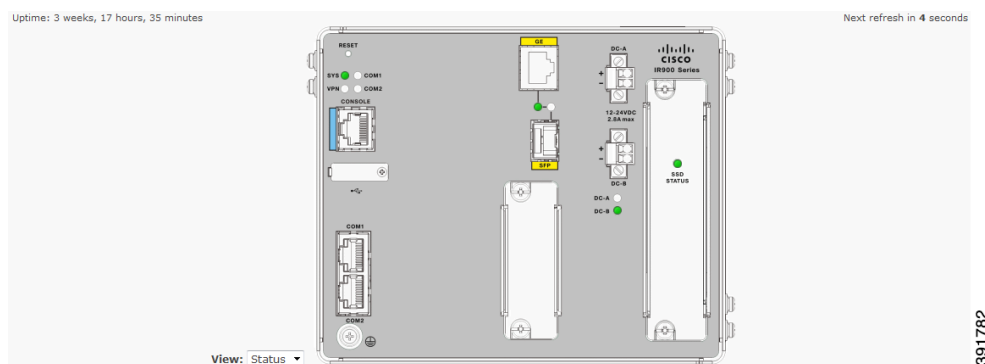
You can monitor the status of the router system and the network using the Monitor menus.

- [Viewing the Front Panel](#)
- [Monitoring the System](#)
- [Monitoring Port Status](#)
- [Monitoring Port Statistics](#)
- [Viewing MAC-Address Table](#)
- [Viewing DHCP or DHCPv6 Binding Table](#)
- [Viewing Logs](#)
- [Monitoring 3G Information](#)
- [Viewing PPPoE Statistics](#)
- [Monitoring NAT Status](#)

Viewing the Front Panel

The Front Panel view is a graphical display of the router front panel. Click **Overview** under Monitor in the left pane. The Front Panel View is displayed, as shown in [Figure 56](#).

Figure 56 Front Panel View



The **Uptime** field shows how long the router has been operating since it was last powered on or was restarted. Status is automatically refreshed every 60 seconds or when you click **Refresh**. The refresh counter shows the number of seconds that remain before the next refresh cycle starts.

The router components on the Front Panel view are color-coded by status. The colors help you to quickly see if a fault or an error condition exists. [Table 4](#) describes the meanings of the colors.

Table 4 LED Definition

LED	Color	Meaning
SYS	Off	System is not powered on or CPU has not completed boot up.
	Solid green	System is operating normally.
	Solid red	System is not functioning properly.
VPN	Off	VPN is not set up.
	Solid green	VPN is operating normally.
	Solid red	VPN is not functioning properly.
COM1/COM2	Off	COM port is enabled and is configured as RS232 port.
	Solid green	COM port is enabled and is configured as RS485 port.
	Solid red	Not defined.
Wi-Fi/3G	Off	No activity.
	Solid green	The connection between the router and the AP/client has been established.
GE-RJ-45/GE-SFP	Off	No link.
	Solid green	Port link, no activity.
DC-A/DC-B	Off	Power is not present on the circuit or the system is not powered up.
	Solid green	Power is present on the associated circuit and the router is already booted up.
SSD	Off	No power is provided to SSD.
	Solid green	Power is provided to SSD.

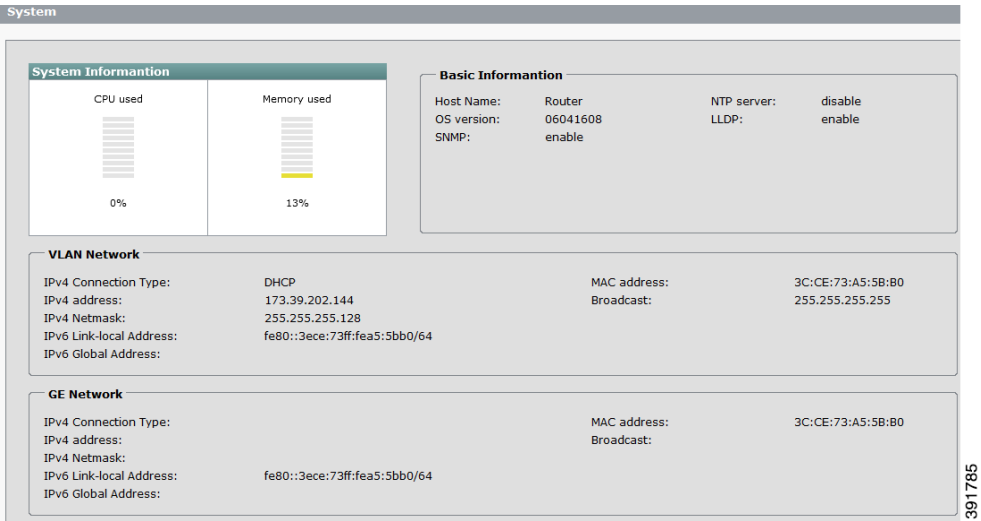
Monitoring the System

Click **System** under Monitor in the left pane to monitor the system status. The System tab is displayed as shown in [Figure 57](#).

The System tab shows the basic device information, system status, current VLAN and interface configurations, Wi-Fi settings, route information, and DNS settings.

The two charts in the System Information section indicate the CPU and memory usage.

Figure 57 System Information



Monitoring Port Status

If the router has link problems, such as traffic that is not being received on a port, verify the port status, and verify that the port settings are correct. You should also verify that the settings of the port before connecting a device to it.

Click **Port Status** under Monitor in the left pane to monitor the port status. The Port Status tab is displayed as shown in Figure 58.

Figure 58 Port Status



click on the column headings to sort information. Click **Refresh** to update the information displayed. The information on this window is automatically updated at each system refresh (every 60 seconds).

Monitoring Port Statistics

The Port Statistics window displays the statistics for data sent and received by the router ports since the router was last powered on, was restarted, or since the statistics were last cleared.

Click **Port Statistics** under Monitor in the left pane to monitor the port statistics. The Port Statistics tab is displayed as shown in Figure 59.

Figure 59 Port Statistics Overview

Interface	Tx rate (Mbps)	Rx rate (Mbps)	Tx bw usage	Rx bw usage	Tx rate (pps)	Rx rate (pps)	Tx Mcast/Bcast rates (pps)	Rx Mcast/Bcast rates (pps)
Gi0/1	0	0	0	0	0	0	0	0

click on the column headings to sort information. Click **Refresh** to update the information displayed. The information on this window is automatically updated at each system refresh (every 60 seconds).

The types of statistics collected and displayed are grouped under these tabs:

- Overview Tab
- Transmit Detail Tab
- Receive Detail Tab

Overview Tab

Use this tab to display the specific numbers of error packets received on and sent from the port, which is a level of detail that is not available from the Dashboard graphs. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity.

The Overview tab displays these statistics:

- The total transmit and received rate on each port.
- The total transmitted and received bandwidth usage each port.
- The total number of multicast/broadcast packets transmitted and received rate on each port.
- The total number of error packets.

Transmit Detail Tab

Use this tab to troubleshoot unusual changes in network traffic. If a port is sending an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal or if it could mean a problem.

The Transmit Detail tab displays these statistics:

- Unicast, multicast, and broadcast packets sent from each port.
- Detailed statistics of errors sent to each port.

Receive Detail Tab

Use this tab to troubleshoot unusual changes in network traffic. If a port is receiving an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal for the connected device or if it could mean a problem.

The Receive Detail Tab displays these statistics:

- Unicast, multicast, and broadcast packets received on each port.
- Detailed statistics of received errors on each port.

Viewing MAC-Address Table

When the router receives a frame, it associates the media access control (MAC) address of the sending network device with the LAN port on which it was received. The MAC-address table consists of a MAC address, an output interface where an address was learned by the router and an ID number of a VLAN where a port is a member together with a Type.

Click **MAC-addresses Table** under Monitor in the left pane to view the MAC addresses table. The Port Status tab is displayed as shown in Figure 60.

Figure 60 MAC-Address Table

MAC address ^	VLAN	Output Interface	Type
00:08:e3:ff:fd:cc	1	Gi0/1	Dynamic
00:21:0cc0:f6:d0	1	Gi0/1	Dynamic
00:21:0cc0:d2:e7:da	1	Gi0/1	Dynamic
00:50:b6:62:4e:d4	1	Gi0/1	Dynamic
08:00:37:b6:78:5c	1	Gi0/1	Dynamic
28:d2:44:01:66:81	1	Gi0/1	Dynamic
28:d2:44:25:5f:35	1	Gi0/1	Dynamic
2c:27:d7:f0:7b:cf	1	Gi0/1	Dynamic
3c:07:54:6a:fd:e2	1	Gi0/1	Dynamic
3c:97:0e:44:59:9a	1	Gi0/1	Dynamic
3c:97:0e:47:3c:73	1	Gi0/1	Dynamic
3c:97:0e:79:84:8b	1	Gi0/1	Dynamic
3c:ce:73:a5:5b:b0	1	Gi0/1	Static
40:2c:f4:e9:2b:e5	1	Gi0/1	Dynamic
74:27:ea:1a:d8:3d	1	Gi0/1	Dynamic
88:5a:92:54:4c:8f	1	Gi0/1	Dynamic
a8:20:66:3e:50:ee	1	Gi0/1	Dynamic
b8:ac:6f:d7:29:e8	1	Gi0/1	Dynamic
b8:ca:3a:7e:d0:37	1	Gi0/1	Dynamic
Ad:88:6A:cd:6d:ca:2	1	Gi0/1	Dynamic

Click on the column headings to sort information. Click **Refresh** to update the information displayed. The information on this window is automatically updated at each system refresh (every 60 seconds).

Viewing DHCP or DHCPv6 Binding Table

The DHCP Binding Table displays a list of bindings created on the DHCP server. The DHCPv6 Binding Table displays a list of bindings created on the DHCPv6 server. You can view MAC address, IP address, lease expiration, and type from these tables.

Click **DHCP Binding Table** or **DHCPv6 Binding Table** under Monitor in the left pane to view the DHCP Binding Table or DHCPv6 Binding Table. You can click on the column headings to sort the information.

Viewing Logs

The DHCP Binding Table displays a list of bindings created on the DHCP server. The DHCPv6 Binding Table displays a list of bindings created on the DHCPv6 server. You can view MAC address, IP address, lease expiration, and type from these tables.

Click **Logs** under Monitor in the left pane to view the system logs. You can filter the logs by choosing output modifiers:

- all
- begin
- exclude
- include

Monitoring 3G Information

You can monitor the 3G information by using these tabs of the Monitor -> 3G menu:

- Connection—Displays the current active connection state and data statistics.
- Hardware—Displays 3G hardware information.
- Network—Displays information about the carrier network and service.
- Profile—Displays 3G profile information.
- Radio—Displays 3G radio statistics.
- Security—Displays the SIM status and modem lock state.

Viewing PPPoE Statistics

The PPPoE Statistics window displays the statistics information about the PPPoE interface. Click **Refresh** to update the information displayed. The information on this window is automatically updated at each system refresh (every 60 seconds).

The following information is displayed:

- Link encap—Link encapsulation protocol.
- Inet addr—Local IP address.
- P-t-P—Remote IP address.
- Mask—IP subnet Mask to be used by the interface.
- UP—Indicates that the PPPoE interface has been loaded
- POINTTOPOINT—Denotes that the device supports point-to-point.
- RUNNING—Indicates the interface is ready to accept data.
- ARP/NOARP—Indicates if the interface enables ARP.
- MULTICAST—Indicates this interface supports multicasting.
- MTU—Maximum transmission unit.
- Metric—Interface routing metric.
- Rx Packets—The total number of packets and error counter of received side.
- Tx Packets—The total number of packets and error counter of transmit side.
- Collisions—Network congestion counter.
- TxqueueLen—Length of the transmit queue of the interface.
- RX bytes—Total amount of data that has passed through the Ethernet interface of received side.
- TX bytes—Total amount of data that has passed through the Ethernet interface of transmit side.

Monitoring NAT Status

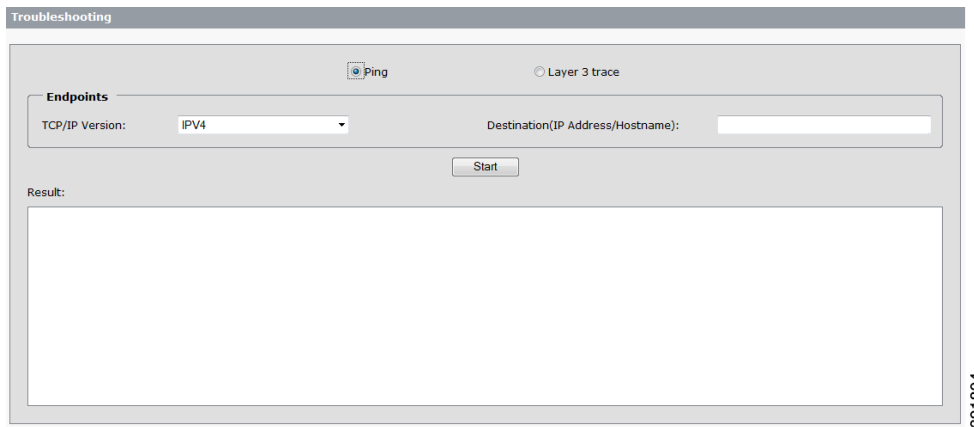
You can monitor the NAT statistics and view NAT translation by using these tabs of the Monitor -> NAT Status menu:

- NAT Statistics tab—Displays Total Active Translations, Inside Interface, Inside Source, and Outside Interface.
- NAT Translation tab—Displays Protocol Name, NATed Address, NAT-Host Address, and Destination Address.

Troubleshooting

Ping and traceroute are available as troubleshooting tool in the device manager. Click **Troubleshooting** in the left pane. The Troubleshooting window is displayed, as shown in [Figure 61](#).

Figure 61 Troubleshooting Window



Follow these steps to do troubleshooting.

1. Choose a troubleshooting approach: **Ping** or **Layer 3 trace**.
2. Select the TCP/IP version: **IPv4** or **IPv6**.
3. Enter the destination IP or hostname in the Destination (IP Address/Hostname) field.
4. Click **Start** to start troubleshooting. The result is displayed in the Result text area.

Maintenance of the Router

You can perform software upgrade, configuration archive, VPN auto config, and to restart or reset the router in the Maintenance section.

- [Software Upgrade](#)
- [Configuration Archive](#)
- [Restart or Reset](#)
- [Configuring VPN Auto Config](#)

Software Upgrade

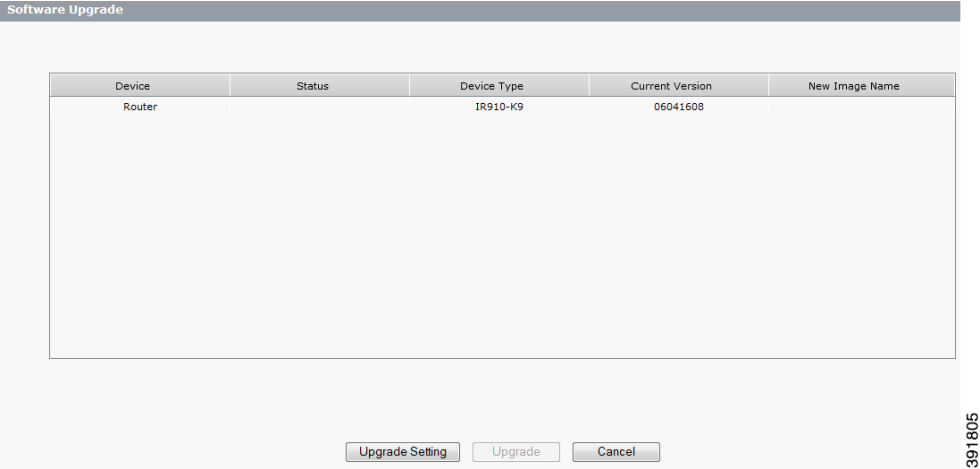
You can upgrade the router software to update the router with the latest software fixes and features.

You must have access to the Internet to download router software from Cisco.com to your PC or network drive. A Cisco.com account is required to access the software images from the Cisco.com website. Until after the upgrade process completes, do not use or close this browser session and do not access the device manager from another browser session.

Follow these steps to upgrade the router software:

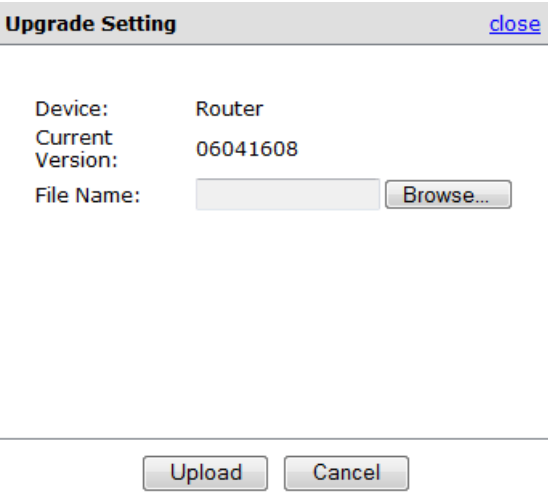
- 1. Click **Software Upgrade** under Maintenance in the left pane. The Software Upgrade window is displayed, as shown in [Figure 62](#).

Figure 62 Software Upgrade



- 2. Click **Upgrade Setting** and the Upgrading Setting window is displayed, as shown in [Figure 63](#).

Figure 63 Upgrade Setting



- 3. The Upgrade Setting window displays device name and current version information. Click **Browse** to select an image file.
- 4. Click **Upload** to upload this image file. The upgrade image file name is displayed in the New Image Name field and upload status is displayed in the Status field.

You must download and use the software image in zip file format (not bin file format) to upgrade the router through the device manager.

5. Click **Upgrade** to upgrade the router to the new image.

Note: During the upgrade process, do not use or close this browser session. Do not access the device manager from another browser session.

When the upgrade process completes, a success message appears, and the router automatically restarts. It might take a few minutes for the router to restart with the new software.

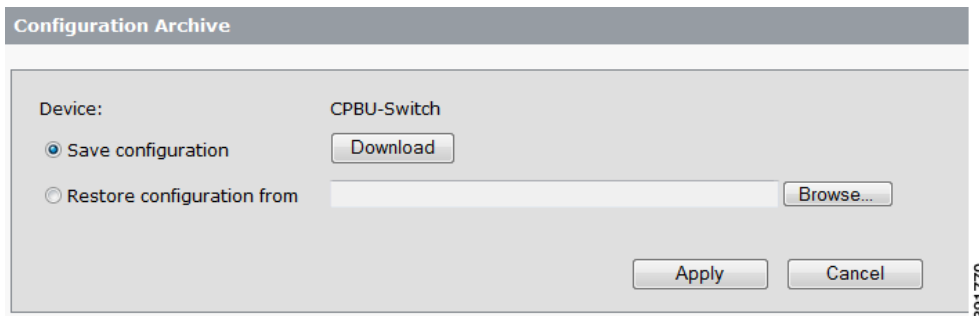
Make sure that the latest software version on the router appears in the Current Version field.

If the upgrade process does not complete, an error message appears. If the upgrade process fails or does not complete, try to upgrade the router again by following the procedures above.

Configuration Archive

Using the Configuration Archive pane, you can download the configuration file to a local directory or to restore a configuration from a local directory, as shown in [Figure 64](#).

Figure 64 Configuration Archive Information



To save the configuration file to a local directory, follow these steps:

1. Choose **Save configuration**.
2. Click the **Download** button to download the configuration file from the router.
3. A file named *running.cfg* will be downloaded to your local drive. You can change the file name or location by clicking the **Save as** option.

To restore a configuration file from the local directory, follow these steps:

1. Choose **Restore configuration from**.
2. Click **Browse** to select a configuration file from local drive.
3. Click **Apply**.

Restart or Reset

Using the Restart/Reset pane, you can restart the router with its current settings, or reset the router to factory defaults, and then reboot.

Follow these steps to restart or reset the device:

1. Click **Restart/Reset** under Administration in the left pane.

2. Choose the restart or reset option.
3. Click **Submit** to apply the change or **Cancel** to restore to the previous value.

Configuring VPN Auto Config

The VPN Auto Config window allows you to retrieve or restore the VPN configuration file, as shown in [Figure 65](#).

Figure 65 VPN Auto Config



To retrieve the VPN configuration file to a local directory, follow these steps:

1. Choose **Retrieve VPN Config**.
2. Click the **Retrieve as** button to download the VPN configuration file from the router.
3. A file named *vpncfg.xml* will be downloaded to your local drive. You can change the file name or location by clicking the **Save as** option.

To restore a VPN configuration file from the local directory, follow these steps:

1. Choose **Restore VPN Config**.
2. Click **Browse** to select a VPN configuration file from local drive.
3. Click **Apply**.



Working with the File System, Configuration Files, and Software Images

This appendix describes how to manipulate the router flash file system, how to copy configuration files, and how to download software images to a router.

- [Working with the File System](#)
- [Working with Configuration Files](#)
- [Working with Software Images](#)

Working with the File System

Commands in this document use URLs as part of the command syntax. URLs used in the Cisco 910 Industrial Router file system contain the following two parts:

- File system or network prefix
- File identification suffix

The following tables list URL keywords that can be used in the source-url and destination-url arguments for all commands in this document. The prefixes listed below can also be used in the filesystem arguments in this document.

[Table 5](#) lists common URL network prefixes used to indicate a device on the network.

Table 5 Network Prefixes, Descriptions, and Formats

Prefix	Description	Format
ftp	Specifies a File Transfer Protocol (FTP) network server.	<code>[[[//[username[:password]@]location]/directory]]/filename</code> For example: <code>ftp://network-config (prefix://filename)</code> <code>ftp://jeanluc:secret@enterprise.cisco.com/ship-config</code>
tftp	Specifies a TFTP server.	<code>tftp: [[[//location]/directory]]/filename</code>

[Table 6](#) common URL prefixes used to indicate memory locations on the system.

Table 6 URL Prefixes and Descriptions

Prefix	Description
flash0	On board NAND flash memory, corresponding to <code>/dev/mtd6</code> which is mounted as <code>/mnt/apps</code> .
flash1	On board NAND flash memory, corresponding to <code>/dev/mtd7</code> which is mounted as <code>/mnt/data</code> .
disk0	On board SATA disk. Only the first partition can be accessed.
usb0	The USB massive storage device. Only the first partition of the first inserted USB can be accessed.

You can specify the file system or directory that the system uses as the default file system by using the **cd** [*filesystem:*][*path*] privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

The default file system is *flash0*. If you do not specify a directory on a file system, the default is the root directory on that file system.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

In the following example, the **cd** command sets the default file system to the SATA disk:

```
Router# pwd
flash:/
Router# cd disk0:/work
Router# pwd
disk0:/work
```

These sections describes the commands that you can use to manipulate the file system:

- [Displaying Information about Files on a File System](#)
- [Changing Directories and Displaying the Working Directory](#)
- [Creating and Removing Directories](#)
- [Renaming Files](#)
- [Copying Files](#)
- [Deleting Files](#)
- [Displaying the Contents of a Files](#)
- [Formating the File System](#)

Displaying Information about Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use the **dir** [*/all*] [*filesystem:*][*filename*] privileged EXEC command.

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Command	Purpose
1.	dir [/all] [filesystem:][file-url]	Display the directories on the specified file system. (Optional) Specify /all to list hidden files. The hidden file is the filename with a dot (.) prefixed. (Optional) For <i>filesystem</i>, specify the URL of the directory or file systems followed by a colon. (Optional) For <i>file-url</i>, specify the name of the files to display on a specified device. The files can be any type. You can use wildcard mark in the filename. A wildcard character (*) matches all patterns.
2.	cd [filesystem:][path]	Change to the directory of interest. (Optional) For <i>filesystem</i>, specify the URL of the directory or file systems followed by a colon. (Optional) For <i>path</i>, specify the name of the path. Path starting with '/' represents absolute path; otherwise it is a relative path.
3.	pwd	Display the working directory. This command has no arguments or keywords.

The following example shows the sample output of a **dir** command:

```
Router# dir /all example
Directory of flash:/work/example
-rwx      1191   Aug 29 2013 17:49:36   file1
-rw-       639   Oct 01 2013 18:42:53   .file2
```

Table 7 describes the significant fields shown in the displays.

Table 7 Output Field Descriptions

Field	Description
-rwx	Permissions. The file can be any or all of the following: ■ d—directory ■ r—readable ■ w—writable ■ x—executable
1191	Size of the file.
Aug 29 2013 17:49:36	Last modification date.
file1	Filename.

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

	Command	Purpose
1.	dir [/all] [filesystem:][file-url]	Display the directories on the specified file system. (Optional) Specify /all to list hidden files. The hidden file is the filename with a dot (.) prefixed. (Optional) For <i>filesystem</i> , specify the URL of the directory or file systems followed by a colon. (Optional) For <i>file-url</i> , specify the name of the files to display on a specified device. The files can be any type. You can use wildcard mark in the filename. A wildcard character (*) matches all patterns.
2.	mkdir [filesystem:][path]	Create a new directory. (Optional) For <i>filesystem</i> , specify the URL of the directory or file systems followed by a colon. (Optional) For <i>path</i> , specify the name of the path. Path starting with '/' represents absolute path; otherwise it is a relative path.
3.	dir [/all] [filesystem:][file-url]	Verify your entry.

The following example creates a directory named newdir:

```
Router# mkdir newdir
Created dir flash:/newdir
```

To delete a directory with all its files and subdirectories, use the **delete [/force][/recursive] filesystem:/file-url** privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

Caution: When files and directories are deleted, their contents cannot be recovered.

Renaming Files

To rename a file, use the **rename source-url destination-url** privileged EXEC command. For the source and destination URLs, specify the location URL.

You can rename files on local systems only by using the rename command. If the destination URL is a directory, the source URL is moved into that directory. If the destination URL already exists and is not a directory, an error will be prompted.

In the following example, the file named *foo* is renamed to *bar* under usb0 storage.

```
Router# dir
Directory of disk0:/work
-rw-          123   Jan 21 2013 09:51:29   foo
```

```
-rw-          456   Jan 21 2013 09:51:29   xyz

Router# rename foo usb0:/bar
...
Router# dir usb0:
Directory of usb0:/
-rw-          123   Jan 21 2013 09:51:29   bar

Router# dir
Directory of disk0:/work
-rw-          456   Jan 21 2013 09:51:29   xyz
```

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

Network file system URLs include **ftp:** and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//username [:password]@location]/directory]/filename
- TFTP—**tftp:**[[//location]/directory]/filename

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

You can copy from remote to local, local to remote, and local to local. However, copying from remote to remote is not supported. During the copying process, one symbol ! printed on the screen indicates 100 blocks (512 bytes per block) transferred.

For specific examples of using the **copy** command with configuration files, see the [“Working with Configuration Files” section on page -6](#).

To copy software images either by downloading a new version or by uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the [“Working with Software Images” section on page -7](#).

Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the **delete** [**/force**] [**/recursive**] [*filesystem:*]/*file-url* privileged EXEC command.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem:* option, the router uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

Caution: When files are deleted, their contents cannot be recovered.

This example shows how to delete the file *myconfig* from the default flash memory device:

```
Router# delete myconfig
```

Displaying the Contents of a Files

To display the contents of any readable file, use the **more** [/binary] *file-url* privileged EXEC command.

Use the **/binary** keyword to displays a file in the hex/text format. For *file-url*, you specify URL of the file to be displayed.

You can only display files on local systems using the **more** command.

Formating the File System

To format on board NAND Flash file system, use the **format** [flash0: | flash1:] privileged EXEC command.

Working with Configuration Files

This section describes how to download or maintain configuration files.

You can copy (*download*) configuration files from a TFTP or FTP server to the running configuration or startup configuration of the router. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP is built on and uses the TCP/IP stack, which is connection-oriented.

These sections describes the configuration file types and actions that you can take:

- [Configuration File Types and Location](#)
- [Displaying Configuration Files](#)
- [Reloading the System](#)

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

Displaying Configuration Files

To display the configuration of the device, use the **show** [running-config | startup-config] EXEC command.

Reloading the System

To reboot the system, use the **reload** EXEC command.

The reload command will first check if the running configuration has been saved and prompt user if not. You can enter **yes** to save the configuration or **no** to skip this step. Then, you will be prompted to reload the system.

The following example shows the output of the reload command:

```
Router# reload
Running configuration has not been saved, save it now? [yes/no]: y
Configuration is saved.
Proceed with reload? [yes/no]: y
Router#
```

Working with Software Images

This section describes how to download software image files, which is stored as a .zip file and contains the kernel and root file system.

You can download a router image file from a TFTP or FTP server, or from a USB device, to upgrade the router software. If you do not have access to a TFTP server, you can download a software image file directly to your PC or workstation by using a web browser (HTTP) and then by using the device manager to upgrade your router.

These sections describes different ways to download image files:

- [Downloading Image Files By Using TFTP](#)
- [Downloading Image Files By Using FTP](#)
- [Downloading Image Files By Using USB](#)

Downloading Image Files By Using TFTP

You can download a router image file from a TFTP server to upgrade the router software.

Preparing to Download an Image File By Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the router has a route to the TFTP server. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the TFTP root directory is /srv/images and the image to be downloaded is in the TFTP root directory.

Downloading an Image File By Using TFTP

Beginning in privileged EXEC mode, follow these steps to download a new image from a TFTP server.

	Command	Purpose
1.	–	Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured; see the “Preparing to Download an Image File By Using TFTP” section on page -7 .
2.	–	Log into the router through the console port or a Telnet session.
3.	archive download-sw [/reload /force-reload] tftp://ip/image_name.zip	Download the image file from the TFTP server to the router. ■ The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. ■ The /force-reload option unconditionally reload the system after the successful software upgrade. ■ For <i>ip</i>, specify the IP address of the TFTP server. ■ For <i>/image_name.zip</i>, specify the image to download.

Downloading Image Files By Using FTP

You can download a router image file from an FTP server to upgrade the router software.

Preparing to Download an Image File By Using FTP

You can copy images files from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. The username and password must be associated with an account on the FTP server.

If the server has a directory structure, the image file is copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading an image file by using FTP, do these tasks:

- Ensure that the router has a route to the FTP server. Check connectivity to the FTP server by using the **ping** command.
- Ensure that the FTP root directory is /srv/images and the image to be downloaded is in the FTP root directory.

For more information, see the documentation for your FTP server.

Downloading an Image File By Using FTP

Beginning in privileged EXEC mode, follow these steps to download a new image from an FTP server.

	Command	Purpose
1.	–	Verify that the FTP server is properly configured by referring to the “Preparing to Download an Image File By Using FTP” section on page –8.
2.	–	Log into the router through the console port or a Telnet session.
3.	archive download-sw [/reload /force-reload] ftp: [//username[:password] @location]] image_name.zip	Download the image file from the FTP server to the router, and overwrite the current image. ■ The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. ■ The /force-reload option unconditionally reload the system after the successful software upgrade. ■ For //username[:password], specify the username and password; these must be associated with an account on the FTP server. ■ For @location, specify the IP address of the FTP server. ■ For image_name.zip, specify the image to download.

Downloading Image Files By Using USB

You can download a router image file from a USB disk to upgrade the router software.

Preparing to Download an Image File By Using USB

You can copy images files from a USB disk.

Before you begin downloading an image file by using USB, do these tasks:

- The partition that contains the image file should have been formatted in FAT/ext2/ext3/ext4. Other filesystem type is not supported.
- Make sure the image file is located at the first partition of the USB disk. For example, if you insert the USB disk to a PC and the device is recognized as **/dev/sdb**, the image file must be stored in the **/dev/sdb1** partition.

Downloading an Image File By Using USB

Beginning in privileged EXEC mode, follow these steps to download a new image from USB disk.

	Command	Purpose
1.	–	Verify that the USB disk is properly configured by referring to the “Preparing to Download an Image File By Using USB” section on page -9 .
2.	–	Log into the router through the console port or a Telnet session.
3.	archive download-sw [/reload /force-reload] usb0:/image_name.zip	Download the image file from the USB disk to the router. ■ The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. ■ The /force-reload option unconditionally reload the system after the successful software upgrade. ■ For <i>image_name.zip</i>, specify the image to download.
4.	eject	Safely remove the USB device. The command should be used before plug out the USB device; otherwise data written in the USB device may get lost.



Troubleshooting

This chapter describes how to identify and resolve software problems related to the software on the router. Depending on the nature of the problem, you can use the command-line interface (CLI) or the device manager to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

This chapter consists of these sections:

- [Using Ping, page 1](#)
- [Using IP Traceroute, page 2](#)
- [Using TDR, page -3](#)
- [Using Debug Commands, page 4](#)

Using Ping

These sections contain this information:

- [Understanding Ping, page 1](#)
- [Executing Ping, page 2](#)

Understanding Ping

The router supports IPv4 or IPv6 ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a *no-answer* message is returned.
- Unknown host—If the host does not exist, an *unknown host* message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a *destination-unreachable* message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a *network or host unreachable* message is returned.

Executing Ping

Beginning in privileged EXEC mode, use this command to ping another device on the network from the router:

Command	Purpose
ping {ip ipv6} [hostname ip_address] [repeat repeat-count size datagram-size source [interface-name source-address]]	Ping a remote host through IP or by supplying the hostname or network address. ■ (Optional) Specify repeat count. Default is 5 times. ■ (Optional) Specify datagram size. Default is 56 bytes. ■ (Optional) Specify source address. Default is none.

This example shows how to ping an IPv4 host:

```
Router# ping ip 173.39.202.144
PING 173.39.202.144 (173.39.202.144): 56 data bytes
64 bytes from 173.39.202.144: seq=0 ttl=64 time=0.345 ms
64 bytes from 173.39.202.144: seq=1 ttl=64 time=0.191 ms
64 bytes from 173.39.202.144: seq=2 ttl=64 time=0.175 ms
64 bytes from 173.39.202.144: seq=3 ttl=64 time=0.157 ms
64 bytes from 173.39.202.144: seq=4 ttl=64 time=0.152 ms

--- 173.39.202.144 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.152/0.204/0.345 ms
```

Using IP Traceroute

These sections contain this information:

- [Understanding IP Traceroute, page 2](#)
- [Executing IP Traceroute, page 3](#)

Understanding IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your routers can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the router is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate routers do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate router is a multilayer router that is routing a particular packet, this router shows up as a hop in the traceroute output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Executing IP Traceroute

Beginning in privileged EXEC mode, follow this step to trace that the path packets take through the network:

Command	Purpose
traceroute {ip ipv6} [hostname ip_address]	Trace the path that packets take through the network.

This example shows how to perform a **traceroute** to an IP host:

```
Router# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

 0 172.2.52.1 0 msec 0 msec 4 msec
 1 172.2.1.203 12 msec 8 msec 0 msec
 2 171.9.16.6 4 msec 0 msec 0 msec
 3 171.9.4.5 0 msec 4 msec 0 msec
 4 171.9.121.34 0 msec 4 msec 4 msec
 5 171.9.15.9 120 msec 132 msec 128 msec
 6 171.9.15.10 132 msec 128 msec 128 msec

Router#
```

Using TDR

These sections contain this information:

- [Understanding TDR, page 3](#)
- [Running TDR and Displaying the Results, page 4](#)

Understanding TDR

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported only on the GigabitEthernet port on the router. It is not supported on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a router
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

Running TDR and Displaying the Results

To run TDR and display the results, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

The following example shows the results of TDR on the Gigabit Ethernet port:

```
Router# test cable-diagnostics tdr interface GigabitEthernet 0/1
Port      Speed      Local pair  Pair Length  Remote pair  Pair status
-----
Gi0/1     1000M      Pair A      < 50M        Pair A        Normal
          Pair B      < 50M        Pair B        Normal
          Pair C      < 50M        Pair C        Normal
          Pair D      < 50M        Pair D        Normal
```

Using Debug Commands

These sections explain how you use **debug** commands to diagnose and resolve internetworking problems:

- [Enabling Debugging on a Specific Feature, page 4](#)
- [Redirecting Debug and Error Message Output, page 5](#)

Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Enabling Debugging on a Specific Feature

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for SNMP:

```
Router# debug snmp
```

The router continues to generate output until you enter the **no** form of the command.

If you enable a **debug** command and no output appears, consider these possibilities:

- The router might not be properly configured to generate the type of traffic you want to monitor. Use the **show running-config** command to check its configuration.
- Even if the router is properly configured, it might not generate the type of traffic you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the **ping** command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Router# no debug snmp
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Router# show debugging
```

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Be aware that the debugging destination you use affects system overhead. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see [Chapter 12, “Configuring System Message Logging.”](#)

