

# Configuring and Monitoring from the Switch Manager

---

This chapter explains how to use the Cisco 1548 Switch Manager to change the configuration settings and to monitor the switch. This chapter assumes that you have already performed the following tasks described in this guide or in the *Cisco 1548M Micro Switch 10/100 Cabling and Start Up*.

- “Connecting to the Console Port” section on page 2-18
- “Assigning IP Information to the Switch” section on page 2-21
- “Accessing the Management Interfaces” section on page 2-23

---

**Note** Procedures for changing the configuration settings and detailed descriptions of the fields are also provided in the switch manager online help.

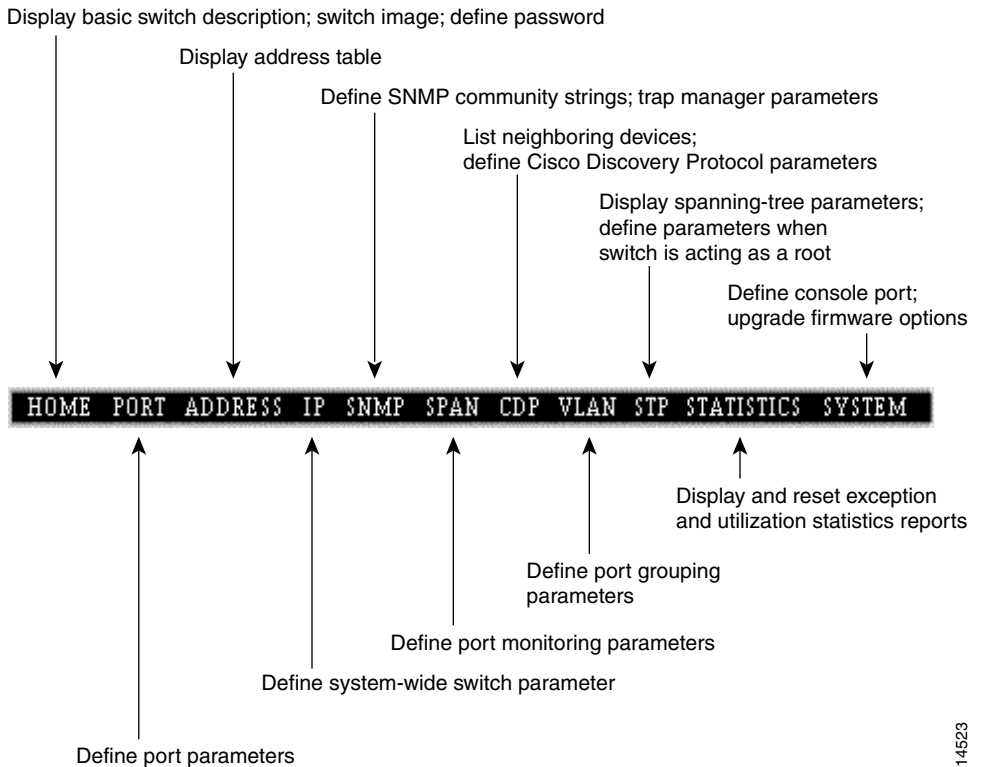
---

# Navigating in the Switch Manager

At the top of each switch manager page is a menu bar. Figure 3-1 describes the functions of the pages accessible from the menu bar.

**Note** On Netscape Communicator only, when the cursor is above a topic on the menu bar, a pop-up briefly describes the options on that particular page.

**Figure 3-1** Switch Manager Menu Bar



## Saving Your Changes

You can change the switch settings by entering information into fields, adding and removing list items, or selecting and deselecting check boxes. Click **Apply** to save your changes. Click **Revert** to discard *all* your *unsaved* changes and return the previous settings to the page.

---

**Note** After you click **Apply**, you cannot revert to the previous settings.

---

- When you enter information in fields and select or deselect check boxes, the changes are saved and immediately take effect after you click **Apply**.
- When you add items to or remove them from lists, the changes take effect immediately. It is not necessary to click **Apply**.

---

**Note** Wait approximately 30 seconds before turning off the switch to be sure the changes are saved.

---

# Assigning or Changing Basic Switch Information

You can assign or change basic descriptions about the switch from the switch manager Home Page (Figure 3-2). You can also assign a password to the switch management interfaces (switch manager and CLI-privileged commands) and monitor network activity through the live switch image. This page also provides a hotlink that opens a Telnet session to the switch command-line interface (CLI), in addition to hotlinks for contacting Cisco Systems' resources.

Click **HOME** on the menu bar to display the Home Page (Figure 3-2) and check and change switch information.

---

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** from the Home Page to access this information online.

---

**Figure 3-2 Home Page**

The screenshot displays the Cisco 1548 Switch Manager interface. At the top, a navigation bar contains tabs for HOME, PORT, ADDRESS, IP, SNMP, SPAN, CDP, VLAN, STP, STATISTICS, and SYSTEM. On the left, a sidebar includes an 'Apply' button with the text 'Apply the new settings to the current configuration', a 'Revert' button with 'Revert to the previous settings', and a 'Help' button. Below these is a copyright notice: 'All contents copyright © 1998 by Cisco Systems, Inc.' The main content area is titled 'Cisco 1548 Switch Manager' and 'Basic System Configuration'. It features several input fields: 'System Name' (empty), 'IP Address' (172.31.255.255), 'Physical Location' (empty), 'User/Contact Name' (empty), 'Assign/Change Password' (empty), and 'Reconfirm Password' (empty). An arrow points from the text 'Initially assigned after the switch is installed. Can be changed from the IP Management page.' to the IP Address field. Below the fields is a photograph of the Cisco 1548 switch. Underneath the photo are status indicators for Speed (100 Mbps, 10 Mbps or No Link Status), Duplex (Full Duplex, Half Duplex or No Link Status), and Ports (Link Up, No Link Status). At the bottom, there is a 'Telnet' section with the text 'Connect to the command line interface.' and a 'Connecting to Cisco Help Resources' section with three numbered links: 1. Cisco Connection Online (CCO), 2. Technical Assistance Center (TAC), and 3. HTML Interface Development Group.

Procedures and detailed field descriptions are provided here.

Initially assigned after the switch is installed. Can be changed from the IP Management page.

15379

## Assigning or Changing the Switch Name and Description

You can assign or change the following information about the switch (be sure to click **Apply** to save changes):

- Name (maximum of 255 characters)
- Physical location (maximum of 255 characters)
- Name of the person responsible for managing the switch (maximum of 255 characters)

### Assigning or Changing the Switch Password

By default, no password is assigned to the switch management interfaces. You can restrict access to the switch manager or CLI-privileged commands by assigning a password. If a user fails to enter the password within a set number of attempts, the switch sends an SNMP trap to the SNMP trap manager to alert you, via in-band management messages, of the failed attempts. (For information about trap managers, see the “Changing the SNMP Settings” section on page 3-18.)

When a password is assigned, the password prompt is displayed when you or any other user opens a switch manager session and displays the Home Page. The Home Page is redisplayed only after you enter the correct password. If the password prompt reappears, reenter the correct password.

---

**Note** The management station from which you are assigning or changing the password must be connected to the switch console port.

---

To assign or change the password to the switch manager or CLI-privileged commands:

- Step 1** Enter a character string (4 to 8 characters, case sensitive) in the Assign/Change Password field.
- Step 2** Enter the same character string in the Reconfirm Password field.
- Step 3** Click **Apply**.  
The connection with the switch is broken. The browser prompts you for the new password.
- Step 4** Enter the new password at the password authentication prompt, and click **OK**.

If you have forgotten or do not know the password, see the “Recovering from a Lost or Forgotten Password” section on page 4-11.

# Using the Switch Image to Monitor the Switch

The Home Page displays the rear panel of the switch (Figure 3-3). The following sections provide information on how to use the switch image.

**Figure 3-3 Switch Image**

Procedures and detailed field descriptions are provided here.

**CISCO SYSTEMS**

HOME PORT ADDRESS IP SNMP SPAN CDP VLAN STP STATISTICS SYSTEM

**Cisco 1548 Switch Manager**

**Basic System Configuration**

System Name:

IP Address: 172.31.255.255

Physical Location:

User/Contact Name:

Assign/Change Password:

Reconfirm Password:

Speed:  100 Mbps  10 Mbps or No Link Status

Duplex:  Full Duplex  Half Duplex or No Link Status

Ports:  Link Up  No Link Status

**Telnet** - Connect to the command line interface.

**Connecting to Cisco Help Resources**

1. [Cisco Connection Online \(CCO\)](#) - Display the CCO home page, which displays links to other Cisco resources.
2. [Technical Assistance Center \(TAC\)](#) - Send e-mail to TAC. You can also call TAC at 1-800-553-2447 or 1-408-526-7209.
3. [HTML Interface Development Group](#) - Send e-mail to the development group responsible for the Switch Manager.

17740

### LEDs on the Switch Image

The switch image on the Home Page shows the rear-panel LED colors at the last poll interval and refreshes every 30 seconds. The LEDs show port status, speed, and duplex mode (see Table 3-1).

**Table 3-1** Descriptions of the LEDs on the Switch Image

LED Color	Description
<b>Port Status (RJ-45 port images)</b>	
Blue (off)	No link.
Solid green	Link is up.
<b>Port Speed</b>	
Blue (off)	Operating at 10 Mbps.
Solid green	Operating at 100 Mbps.
<b>Port Duplex</b>	
Blue (off)	Operating at half-duplex mode.
Solid green	Operating at full-duplex mode.

### Using Telnet to Open a CLI Session

Click **Telnet** to open a session on the switch command-line interface (CLI).

### Connecting to Cisco Systems' Resources

The Home Page provides these hotlinks to connect to Cisco Systems' resources:

- Click **Cisco Connection Online (CCO)** to display the CCO home page ([www.cisco.com](http://www.cisco.com)), which contains links to the support sites for downloading the latest software and displaying the latest Cisco documentation.
- Click **Technical Assistance Center (TAC)** to open a new message composition window to send e-mail to TAC ([tac@cisco.com](mailto:tac@cisco.com)). You can also phone TAC at 800-553-2447 or 408-526-7209.
- Click **HTML Interface Development Group** to open a new message composition window to send e-mail to the switch manager development group ([cs-html@cisco.com](mailto:cs-html@cisco.com)).

## Changing the Port Settings

By default, each 10/100 network port on the switch is enabled to transmit packets to and receive them from the device to which it is connected, automatically matching its speed and duplex mode.

Click **PORT** on the menu bar to display the Port Management Page (Figure 3-4), check the status of the port, and change the port settings.

---

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** from the Port Management Page to access this information online.

---

# Changing the Port Settings

**Figure 3-4 Port Management Page**

The screenshot shows the Cisco Port Management interface. At the top, there is a navigation bar with links: HOME, PORT, ADDRESS, IP, SNMP, SPAN, CDP, VLAN, STP, STATISTICS, SYSTEM. Below this is the 'Port Management' section. On the left, there are three buttons: 'Apply' (with text: 'Apply the new settings to the current configuration'), 'Revert' (with text: 'Revert to the previous settings'), and 'Help'. Below these buttons is the copyright notice: 'All contents copyright © 1998 by Cisco Systems, Inc.' The main part of the page is a table with 8 rows representing ports. Each row has columns for 'Port', 'Status: Requested/Actual', 'Duplex Mode: Requested/Actual', 'Speed: Requested/Actual', 'Port Name/Description', and 'Statistics'. The 'Status' column contains a checked 'Enable' checkbox and the text 'Link Up'. The 'Duplex Mode' column contains a dropdown menu with 'Auto' selected and the text 'Half' or 'Full'. The 'Speed' column contains a dropdown menu with 'Auto' selected and the text '100 Mbps', '10 Mbps', or '10 Mbpps'. The 'Port Name/Description' column contains an empty text box. The 'Statistics' column contains a 'View...' button. Arrows from external text point to the 'Enable' checkbox, the 'Auto' dropdown, and the 'View...' button. Below the table, there are three explanatory paragraphs: 'Shows when the port is operating at 10 or 100 Mbps. Autonegotiation allows the port to match the speed of the device to which it is connected.' (pointing to the Speed column), 'Shows when the port is operating at half- or full-duplex mode. Autonegotiation allows the port to match the duplex mode of the device to which it is connected.' (pointing to the Duplex Mode column), and 'Shows when the port is able or unable to transmit and receive data.' (pointing to the Status column).

Port	Status: Requested Actual	Duplex Mode: Requested Actual	Speed: Requested Actual	Port Name/ Description	Statistics
1	<input checked="" type="checkbox"/> Enable Link Up	Auto Half	Auto 100 Mbps		View...
2	<input checked="" type="checkbox"/> Enable Link Up	Auto Full	Auto 100 Mbps		View...
3	<input checked="" type="checkbox"/> Enable Link Up	Auto Half	Auto 100 Mbps		View...
4	<input checked="" type="checkbox"/> Enable Link Up	Auto Half	Auto 100 Mbps		View...
5	<input checked="" type="checkbox"/> Enable Link Up	Auto Half	Auto 100 Mbps		View...
6	<input checked="" type="checkbox"/> Enable Link Up	Auto Full	Auto 10 Mbps		View...
7	<input checked="" type="checkbox"/> Enable Link Up	Auto Half	Auto 10 Mbpps		View...
8	<input checked="" type="checkbox"/> Enable Link Up	Auto Full Half Auto	Auto 10 Mbpps 100 Mbpps 100 Mbpps		View...

Procedures and detailed field descriptions are provided here.

Displays the statistics for a particular port.

Shows when the port is operating at 10 or 100 Mbps. Autonegotiation allows the port to match the speed of the device to which it is connected.

Shows when the port is operating at half- or full-duplex mode. Autonegotiation allows the port to match the duplex mode of the device to which it is connected.

Shows when the port is able or unable to transmit and receive data.

15381

## Enabling or Disabling a Port

By default, all ports are enabled. To disable a port:

**Step 1** In the Status: Requested/Actual column, deselect the **Enable** check box.

**Step 2** Click **Apply**.

A linkDown trap is sent to the management station if you configured an SNMP manager.

To reenable a port:

**Step 1** In the Status: Requested/Actual column, select the **Enable** check box.

**Step 2** Click **Apply**.

A linkUp trap is sent to the management station if you configured an SNMP manager.

## Checking the Port Status

The Status: Requested/Actual column displays the actual status of the port. Each port is always in one of these link states:

Link Up            Port can transmit and receive data.

Link Down        Port is unable to transmit or receive data.

## Changing the Port Duplex Mode

Full-duplex operation is simultaneous transmission of data in both directions across a link. For example, a 100BaseTX switched port operating in full-duplex mode can provide up to 200 Mbps of bandwidth across the switched link.

When autonegotiation is selected on the port, it automatically configures for full-duplex operation if the connected device also supports full duplex. If the attached device does not support full-duplex operation, the port automatically configures to half-duplex operation.

## Changing the Port Settings

---

To change the port duplex mode:

**Step 1** From the Duplex Mode: Requested/Actual drop-down list, select **Half**, **Full**, or **Auto** (autonegotiate). The default is Auto.

**Step 2** Click **Apply**.

---

**Note** If the other device does not autonegotiate, the switch port automatically negotiates to half duplex.

---

## Changing the Port Transmission Speed

By default, the port automatically matches the transmission speed of the attached device.

To change the port transmission speed:

**Step 1** From the Speed: Requested/Actual drop-down list, select **10 Mbps**, **100 Mbps**, or **Auto** (autonegotiate). The default is Auto.

**Step 2** Click **Apply**.

---

**Note** If the other device does not autonegotiate, the switch port automatically negotiates to 10 Mbps.

---

## Assigning or Changing a Port Name or Description

To assign a name or description to a port:

**Step 1** In the Port Name/Description column, enter the port name or a description (up to 80 characters) of how the port is connected.

**Step 2** Click **Apply**.

## Checking or Resetting Port Statistics

From the Port Management Page, select a port, and click **View** to see the statistics for a particular port on the switch. The Detailed Port Statistics Page (Figure 3-5) for the selected port displays the port statistics. Table 3-2 lists the statistics displayed on the page:

The switch manager does not automatically refresh the statistics shown on this page. Click **Reload** to refresh the statistics shown on this page.

**Figure 3-5 Detailed Port Statistics Page**

The screenshot shows the Cisco switch manager interface. At the top, there is a navigation bar with links: HOME, PORT, ADDRESS, IP, SNMP, SPAN, CDP, VLAN, STP, STATISTICS, SYSTEM. The main heading is "Detailed Port Statistics" and the sub-heading is "Port 1 Statistics Report".

On the left side, there are several buttons: "Apply" (with a description: "Apply the new settings to the current configuration"), "Revert" (with a description: "Revert to the previous settings"), and "Help". Below these buttons is the copyright notice: "All contents copyright © 1998 by Cisco Systems, Inc.".

The main content area is divided into two columns of statistics:

General Statistics		RMON Statistics	
Good Packet Bytes Received:	51	Total Bytes Received:	5
Good Packets Received:	105	Total Packets Received:	6
Bytes Sent:	57	Broadcast Packets Received:	0
Packets Sent:	117	Multicast Packets Received:	0
Late Collisions:	0	CRC/Alignment Errors:	0
MAC Receive Errors:	0	Oversize Packets:	0
		Fragments:	0
		Very Long Events:	0
		Collisions:	0
		64-Byte Packets:	0
		65-127-Byte Packets:	0
		128-255-Byte Packets:	0
		256-511-Byte Packets:	0
		512-1023-Byte Packets:	0
		1024-1518-Byte Packets:	0

At the bottom of the page, there is a "Reload" button. An annotation with an arrow points to this button, stating: "Refreshes the statistics displayed on this page." Another annotation with an arrow points to the "Apply" button, stating: "Procedures and detailed field descriptions are provided here." The page number "15382" is visible in the bottom right corner.

**Table 3-2 Error Descriptions on the Detailed Port Statistics Page**

---

**General Statistics**

Good-Packet Bytes Received	Total number of bytes received as part of good packets by the port.
Good Packets Received	Total number of good packets received by the port.
Bytes Sent	Total number of bytes sent by the port.
Packets Sent	Total number of packets sent by the port.
Late Collisions	Number of times the switch detects a collision on the port later than 512 bit-times into the transmission of a packet.
MAC Receive Errors	Number of times the port receives an invalid MAC frame.

**RMON Statistics**

Total Bytes Received	Total number of bytes received by the port.
Total Packets Received	Total number of packets received by the port.
Broadcast Packets Received	Total number of broadcast packets received by the port.
Multicast Packets Received	Total number of multicast packets received by the port.
CRC/Alignment Errors	Number of alignment errors (caused if all bytes are not received whole) or frames with CRC errors received by the port.
Oversize Packets	Number of packets longer than 1518 bytes received by the port.
Fragments	Number of SMT packets received by the port.
Very Long Events	Number of packets that exceed the maximum length prescribed in IEEE 802.3.
Collisions	Number of times the port and the connected device attempt to transmit at the same time.
64-Byte Packets 65-127-Byte Packets 128-255-Byte Packets 256-511-Byte Packets 512-1023-Byte Packets 1024-1518-Byte Packets	Number of packets received in these lengths in bytes.

---

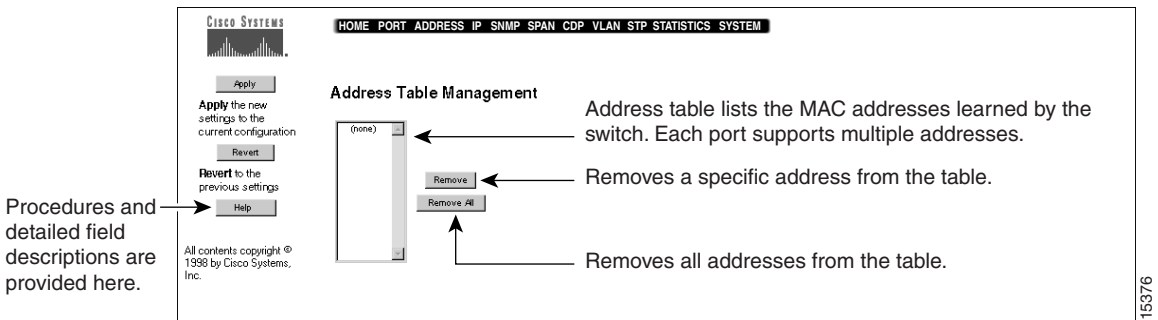
## Maintaining the Address Table

The switch learns the MAC addresses of connected devices, adding these addresses to the address table. The switch supports multiple addresses on each port and stores up to 4096 addresses.

Click **ADDRESS** on the menu bar to display the Address Table Management Page (Figure 3-7), check the address table, and remove addresses from the table.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** from the Address Table Management Page to access this information online.

**Figure 3-6** Address Table Management Page



## Removing Addresses from the Address Table

When the address table exceeds the maximum MAC address limit (4096), switch performance can be degraded.

To remove specific addresses from the table one at a time:

**Step 1** Select the addresses on the Address Table list.

**Step 2** Click **Remove**.

To remove all addresses from the table, click **Remove All**.

# Changing the Switch IP Information

IP information identifies the switch to the network and is necessary to manage the switch through the switch manager, the CLI, or SNMP. This information is usually assigned to the switch after it is installed and initially started up. (See the “Assigning IP Information to the Switch” section on page 2-21.)

The IP Address field displays the current IP address of the switch. Click **IP** on the menu bar to display the IP Management Page (Figure 3-7) and change switch IP information.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the IP Management Page to access this information online.

Figure 3-7 IP Management Page

Procedures and detailed field descriptions are provided here.

**IP Management**

IP State: User-Configured

IP Address: [text input]

Subnet Mask: 255.255.255.0

Default Gateway: 172.31.255.255

- User-Configured allows you to manually change the switch IP information. The IP address and subnet mask must be in the same subnet.
- BootP Get IP enables the switch to automatically assign switch IP information if it is connected to a network with a BootP server. When enabled, this option does not allow switch IP information to be manually changed.

All contents copyright © 1999 by Cisco Systems, Inc.

15380



**Caution** Changing the switch IP address on this page will end your switch manager session. To open a new session, enter the new IP address in the URL field if you are using Communicator (the Address field if you are using Internet Explorer).

To change the switch IP information:

**Step 1** Select **User-Configured** from the IP State drop-down list.

---

**Note** You can manually change the switch IP information only if the User-Configured option is enabled.

---

---

**Note** Use the BootP Get IP option if you want the BootP (Boot Protocol) server to assign the IP information. The switch must be connected to a network that has a BootP server. The BootP Get IP option becomes active when you restart the switch. If this option is enabled, you cannot manually change IP information.

---

The default is User-Configured.

**Step 2** Enter a new IP address for the switch in the IP Address field.



**Caution** If you enter a new address and click **Apply**, the switch manager loses contact with the switch. Enter the new IP address of the switch in the Location field if you are using Communicator (the Address field if you are using Internet Explorer) to redisplay the switch manager.

**Step 3** Enter the subnet mask for the switch.

The subnet mask must be in the same subnet as the IP address.

**Step 4** Enter the IP address of the default gateway.

The default gateway is the router that the switch uses to reach IP subnets other than the local subnet to which the switch is attached.

**Step 5** Click **Apply**.

# Changing the SNMP Settings

SNMP provides the means to manage and monitor the switch through the Management Information Base (MIB) objects. Additional information about SNMP and MIB objects is provided in the “Overview of SNMP” section on page 1-9 and the “Accessing the MIB Files through SNMP” section on page 2-26.

Click **SNMP** on the menu bar to display the SNMP Management Page (Figure 3-8) and check and change the SNMP settings.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the SNMP Management Page to access this information online.

Figure 3-8 SNMP Management Page

The screenshot shows the SNMP Management Page with the following elements:

- Navigation Bar:** HOME | PORT | ADDRESS | IP | **SNMP** | SPAN | CDP | VLAN | STP | STATISTICS | SYSTEM
- Left Panel:** Cisco Systems logo, Apply, Revert, and Help buttons. Text: "Apply the new settings to the current configuration", "Revert to the previous settings", and "All contents copyright © 1996 by Cisco Systems, Inc."
- SNMP Management Section:** Read Community String: public, Write Community String: private. Annotation: "Passwords that allow read-only (Get requests) and read-write (Set requests) access to the switch MIB-object information."
- Trap Managers (maximum of 4):** Current: (none), New: IP Address: [ ], Trap Manager Community String: [ ]. Annotation: "Up to four management stations can receive traps (alerts of certain events) generated by the switch. Use the traps to monitor the switch."
- Write Managers (maximum of 4):** Current: (none), New: IP Address: [ ]. Annotation: "Up to four management stations can issue write requests to change the switch configuration settings through the MIB variables."
- Annotations:** "Procedures and detailed field descriptions are provided here." points to the Help button.

15383

### Changing the SNMP Read and Write Community Strings

Community strings serve as passwords for SNMP messages. You can assign community strings that enable the switch to validate SNMP read and read-write requests from a management station.

To change the SNMP Read community string:

**Step 1** Enter up to 32 characters in the Read Community String field. The default is public.

**Step 2** Click **Apply**.

To change the SNMP Write community string:

**Step 1** Enter up to 32 characters in the Write Community String field. The default is private.

**Step 2** Click **Apply**.

### Assigning or Changing Trap Managers

A trap manager is an SNMP management station that receives traps, which are the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Up to four trap managers and their accompanying community strings can be entered.

To assign a trap manager:

**Step 1** Enter the IP address and a community string (up to 32 characters) in the IP Address and Trap Manager Community String fields.

**Step 2** Click **Add**.

To remove a trap manager:

**Step 1** Select the manager from the Current list.

**Step 2** Click **Remove**.

### Enabling or Disabling Trap Generation

By default, the Enable Authentication Trap Generation check box is selected (meaning this parameter is enabled). When this check box is selected, the switch generates authentication traps that alert a management station to SNMP requests that are not accompanied by a valid community string. However, even if this parameter is enabled, no trap can be generated if no trap manager addresses are specified. (For information about trap manager settings, see the “Assigning or Changing Trap Managers” section on page 3-19). If you change this check box, click **Apply** to save your changes.

By default, the Enable Link Up/Link Down Trap Generation check box is selected (meaning this parameter is enabled). If you change this check box, click **Apply** to save your changes.

The switch generates linkDown traps when a port is suspended or disabled for these reasons:

- User disables the port.
- Link is down.

The switch generates linkUp traps when a port is enabled for these reasons:

- Presence of linkbeat.
- Management intervention enables the port.

### Assigning or Changing Write Managers

A write manager is an SNMP management station that can issue write requests to the switch. Up to four IP addresses of stations can be defined.

To assign a write manager:

- Step 1** Enter the management station IP address in the IP Address field.
- Step 2** Click **Add**.

To remove a write manager:

- Step 1** Select the manager from the Current list.
- Step 2** Click **Remove**.

## Monitoring Port Activity

By enabling the Switched Port ANalyzer (SPAN), you can forward the incoming and outgoing traffic of one switch port in the same VLAN and monitor that traffic from another switch port. You can also use a network analyzer on the monitoring port to troubleshoot network problems by examining the traffic on other Cisco switched ports or segments.

By default, no port on the switch is designated as the monitoring port, and no ports on the switch are monitored. Remember the following restrictions when monitoring ports:

- The monitoring port cannot be a member of more than one VLAN.
- The monitoring port can monitor only one port at a time.
- Do not make VLAN membership changes on the monitoring port or monitored ports until after you disable monitoring.

Click **SPAN** on the menu bar to display the SPAN Configuration Page (Figure 3-9) and change the monitoring settings.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the SPAN Configuration Page to access this information online.

**Figure 3-9** SPAN Configuration Page

Procedures and detailed field descriptions are provided here.

**CISCO SYSTEMS** HOME PORT ADDRESS IP SNMP SPAN CDP VLAN STP STATISTICS SYSTEM

**SPAN Configuration**

**Port Monitoring**

Capturing Frames to the Monitoring Port:

Select Monitoring Port: 1

Select Monitored Port: none

Apply

Apply the new settings to the current configuration

Revert

Revert to the previous settings

Help

All contents copyright © 1998 by Cisco Systems, Inc.

15384

### Enabling or Disabling Port Monitoring

To enable one port to monitor traffic on another port:

- Step 1** Select the **Capturing Frames to the Monitoring Port** check box. By default, this check box is not selected (meaning port monitoring is disabled).
- Step 2** From the Select Monitoring Port drop-down list, select the monitoring port (the port to which captured frames are sent).
- You can designate any port as the monitoring port, but the following restrictions apply:
- The monitoring port cannot be a member of more than one VLAN.
  - The monitoring port can monitor only one port at a time.
  - Do not make VLAN membership changes on the monitoring port or monitored ports until after you disable monitoring.
- Step 3** From the Select Monitored Port drop-down list, select the port that you want to monitor.
- Step 4** Click **Apply**.

---

**Note** When you enable port monitoring, the system provides alerts that inform you that all ports on the switch will behave *as if* they belong to VLAN 1. Actually, no VLAN assignments are lost; all VLAN assignments are saved in Flash memory. When you disable port monitoring, all ports will operate according to their VLAN assignments.

No alerts are provided if you enable port monitoring via SNMP.

---

To disable port monitoring:

- Step 1** Deselect the **Capturing Frames to Monitoring Port** check box.
- Step 2** Click **Apply**.

# Changing the CDP Settings

The Cisco Discovery Protocol (CDP) enables the switch to advertise its existence to other Cisco devices in the network. When CDP is enabled, the switch manager and network management applications have an accurate picture of the network at any time because CDP gathers information about device types, links between devices, and the number of interfaces within each device.

By default, CDP is not enabled on the switch and all its ports.

Click **CDP** on the menu bar to display the CDP Management Page (Figure 3-10) and check and change the CDP settings.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the CDP Management Page to access this information online.

**Figure 3-10 CDP Management Page**

The screenshot shows the CDP Management page with the following sections and annotations:

- Navigation Bar:** HOME | PORT | ADDRESS | IP | SNMP | SPAN | CDP | VLAN | STP | STATISTICS | SYSTEM
- Buttons:** Apply, Revert, Help.
  - Apply:** Apply the new settings to the current configuration.
  - Revert:** Revert to the previous settings.
  - Help:** Procedures and detailed field descriptions are provided here.
- Discovered Neighboring Devices:** (none) | Browse | Telnet | Details...
  - Browse:** Opens the web console of a connected neighboring device.
  - Telnet:** Opens a Telnet session and logs you into a connected neighboring device.
  - Details...:** Displays detailed information about a connected neighboring device.
- CDP Options:**
  - Enable CDP:**
  - Packet Hold Time:** 180 seconds (10-255 [180])
  - Packets Transmission Time:** 60 seconds (5-900 [60])
  - Annotations:**
    - Length of time a neighboring device retains CDP information it received from this switch. The packet hold time should be higher than the packet transmission time.
    - Length of time between transmissions of CDP messages. The packet transmission time should be lower than the packet hold time.
- Select the Ports to be CDP Enabled:**
  - CDP Enabled:** 1, 2, 3, 4, 5, 6, 8
  - CDP Disabled:** (none)
  - Buttons:** << Enable <<, >> Disable >>
  - Annotation:** Select the switch ports to participate in exchanging CDP information with other Cisco devices.

16377

### Displaying CDP Neighbors

The Discovered Neighboring Devices list shows the devices with which the switch exchanges CDP messages. To display information about neighboring devices:

- Step 1** From the Discovered Neighboring Devices list, select a device.
- Step 2** Click one of these buttons:
- Click **Browse** to access the web console of a neighboring device. The neighbor must be a device that has web-console support.
  - Click **Telnet** to open a Telnet session and log into a neighboring device.
  - Click **Details** to display the detailed CDP information currently stored in the switch.

### Enabling or Disabling CDP on the Switch

By default, CDP is disabled on the switch. If you want the switch to exchange information with Cisco devices, you can enable CDP on the switch. To enable CDP:

- Step 1** Select the **Enable CDP** check box.
- Step 2** Click **Apply**.

To disable CDP:

- Step 1** Deselect the **Enable CDP** check box.
- Step 2** Click **Apply**.

## Changing the CDP Settings

To change the global CDP settings for the switch:

**Step 1** In the Packet Hold Time field, enter the number of seconds (between 10 and 255) that a neighboring device retains the CDP neighbor information received from this switch. The default setting is 180 seconds.

If a neighboring device does not receive a CDP message before the hold time expires, the device drops this switch as a neighbor. The packet hold time should be higher than the packet transmission time.

**Step 2** In the Packet Transmission Time field, enter the number of seconds (between 5 and 900) between transmissions of CDP messages. The default is 60 seconds. The packet transmission time should be lower than the packet hold time.

**Step 3** Click **Apply**.

## Enabling or Disabling CDP on a Port

By default, CDP is disabled on all ports on the switch. If you want a port to exchange information with Cisco devices, you can enable CDP on that port. To enable CDP on a port:

**Step 1** Select the port from the CDP Enabled list.

**Step 2** Click **Enable**.

To disable CDP on a port:

**Step 1** Select the port from the CDP Disabled list.

**Step 2** Click **Disable**.

## Assigning Ports to Different VLANs

A virtual LAN (VLAN) is a defined broadcast domain logically segmented by function, team, or application. Through VLANs, you can enhance network performance by allowing the transmission of traffic among member stations in the same VLAN and by blocking traffic from stations in other VLANs.

By default, all ports on the switch are assigned to VLAN 1, which is the management VLAN. You can create up to four VLANs on the switch and assign each switch port to one or all VLANs.

**Note** Only VLAN 1 supports Spanning-Tree Protocol (STP).

Click **VLAN** on the menu bar to display the VLAN Management Page (Figure 3-11) and assign ports to VLANs other than VLAN 1.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the VLAN Management Page to access this information online.

Figure 3-11 VLAN Management Page

Procedures and detailed field descriptions are provided here.

Select the VLAN ID to which the port should belong. VLAN 1 is always the management VLAN. Make sure the switch port to which your management station is connected is in VLAN 1. Ports belonging to all VLANs should only be connected to a router or server.

## Assigning Ports to or Removing Them from a Specific VLAN

A simple port-based VLAN consists of a switch port assigned to one VLAN. By default, all ports are assigned to VLAN 1. To assign a port to a different VLAN:

**Step 1** In the VLAN drop-down list, select **2, 3, or 4**.

**Step 2** Click **Apply**.

To remove a port from a VLAN membership other than VLAN 1:

**Step 1** In the VLAN drop-down list, select **1**.

**Step 2** Click **Apply**.

## Assigning Ports to or Removing Them from Multiple VLANs

An overlapping VLAN is a port (a multi-VLAN port) assigned to more than one VLAN and is usually connected to a server or router. This allows the stations on all VLANs to reach the server or router.

---

**Note** A multi-VLAN port cannot be designated as a monitoring port. For more information about port monitoring, see the “Monitoring Port Activity” section on page 3-21.

---

The multi-VLAN port functions normally in all its VLANs. For example, when an unknown MAC address is received on the multi-VLAN port, it is learned by all the port VLANs. The port also responds to the STP messages generated by separate instances of Spanning-Tree Protocol (STP) in each VLAN. Because the multi-VLAN port is a member of all VLANs, flooded traffic received on the port is forwarded to ports in all VLANs.



**Caution** To avoid unpredictable activity by STP, do not connect a port assigned to all VLANs to another switch or hub. Connect these ports only to routers or servers.

To assign a port to all VLANs:

**Step 1** In the VLAN drop-down list, select **All**.

**Step 2** Click **Apply**.

# Changing the Spanning-Tree Protocol Settings

The Spanning-Tree Protocol (STP) constructs network topologies that do not contain loops. When the network configuration changes, STP transparently reconfigures bridges and switches to avoid the creation of loops. STP avoids loops by placing ports in a forwarding or blocking state and establishes redundant paths (in the event of lost connections). The VLAN is treated as a separate bridge, and a separate instance of STP is applied to it.

STP requires approximately 30 seconds to complete its discovery of the network, and the switch does not forward packets during this time.

By default, STP is enabled only on VLAN 1 and cannot be enabled on other VLANs.

Click **STP** on the menu bar to display the Spanning-Tree Management Page (Figure 3-12) and change the appropriate STP settings for the switch and for the ports assigned to specific VLANs.

---

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the Spanning-Tree Management Page to access this information online.

---

Figure 3-12 Spanning-Tree Management Page

Procedures and detailed field descriptions are provided here.

Displays the VLAN to which the displayed STP settings apply.

You can enable STP only on VLAN 1.

Displays the read-only STP settings for the current root switch.

Lists the options that this switch will use as the root switch.

Lists the port-specific parameters that affect how the ports in a particular VLAN respond if a loop is formed.

Port	State	Forward Transitions	Path Cost	Priority	Port Fast Mode
1	Forwarding	2	19	128	<input type="checkbox"/>
2	Forwarding	2	19	128	<input type="checkbox"/>
3	Forwarding	2	10	128	<input type="checkbox"/>

**Note** You can enable STP on VLAN 1 only. The **Go** button and the VLAN 2, 3, 4, and All options from the Select VLAN drop-down list are automatically disabled when you select the Enable Spanning Tree check box.

None of the fields (such as operating parameters and STP switch settings) apply to VLAN 2, 3, 4, or All. In addition, the STP port settings do not apply to any ports assigned to VLAN 2, 3, 4, or All.

**Note** The ports listed in Figure 3-12 shows that ports 1, 2, and 3 belong to VLAN 1. The Spanning-Tree Management Page only shows the ports assigned to VLAN 1.

### Checking the Current Spanning-Tree Root Settings

The Operating Parameters section displays the following read-only STP settings for the current root switch, which could be defined on another switch.

Bridge ID	Unique hexadecimal ID number that has a bridge priority and a unique MAC address.
Number of Member Ports	Number of ports configured with STP.
Max Age	Number of seconds a bridge waits for STP configuration messages before attempting a reconfiguration.
Hello Time	Number of seconds between the transmission of STP configuration messages. All bridges send configuration messages during reconfiguration to elect the designated root bridge. After STP completes its network discovery, only designated bridges send configuration messages.
Topology Changes	Number of bridge topology changes experienced by the network. A topology change occurs as ports on any bridge change from a nonforwarding to a forwarding state or when a new root is selected.
Designated Root	ID number of the bridge identified as the root by the STP.
Root Port	Port on this bridge with the lowest-cost path to the root bridge. This option identifies the port through which the path to the root bridge is established. N/A is displayed when STP is disabled or when this bridge is the root bridge.
Root Path Cost	Cost of the path from this bridge to the root bridge shown in the Designated Root field. It equals the path cost parameters held for the root port.
Forward Delay	Number of seconds before a port changes from its STP learning and listening states to a forwarding state. Every bridge on the network ensures that no loop is formed before the port can forward packets.
Last TopChange	Number of days (d), hours (h), minutes (min), and seconds (s) since the last topology change.

## Changing the Spanning-Tree Options for the Switch

The Spanning Tree Configuration section displays a list of STP parameters that this switch will use when it is the root switch. To change the STP configuration on this switch:

**Step 1** Enable STP if you have previously disabled it:

- (a) Select the **Enable Spanning Tree** check box to enable STP.
- (b) Click **Apply**.

---

**Note** You can enable STP on VLAN 1 only. The **Go** button and the VLAN 2, 3, 4, and All options from the Select VLAN drop-down list are automatically disabled when you select the Enable Spanning Tree check box.

---

**Note** You can slightly improve performance on the switch by disabling STP. However, disable STP only if you are sure there are no loops in your network topology. With STP disabled and loops present in the topology, network performance is degraded by excessive traffic and indefinite packet duplication.

---

**Step 2** In the Bridge Priority field, enter the value (0 to 65535) used in determining the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The default is 32768.

**Step 3** In the Hello Time field, enter the number of seconds (1 to 10) after which this switch becomes the root bridge. The default is 2.

**Step 4** In the Max Age field, enter the number of seconds (6 to 40) a switch waits for STP configuration messages before it attempts a reconfiguration. The default is 20.

**Step 5** In the Forward Delay field, enter the number of seconds (4 to 30) a port waits before changing from its STP learning and listening states to the forwarding state. This delay time is necessary to ensure that no loop is formed before the switch forwards a packet. The default is 15.

---

**Note** Each switch in a spanning tree adopts the Hello, Max age, and Delay parameters of the root bridge regardless of how it is configured.

---

**Step 6** Click **Apply**.

# Changing the Spanning-Tree Parameters for a VLAN and Its Ports

You can set STP parameters for VLAN 1 only on the switch. The Current VLAN field displays VLAN 1 when the STP settings are displayed. The Port Parameters list displays only ports that are members of VLAN 1, and the settings determine how the port responds if a loop is formed.

To modify spanning-tree parameters for VLAN 1 and its ports:

**Step 1** In the Select VLAN drop-down list, select **1**.

---

**Note** You can enable STP only on VLAN 1. The **Go** button and the VLAN 2, 3, 4, and All options from the Select VLAN drop-down list are automatically disabled when you select the Enable Spanning Tree check box.

---

**Step 2** Click **Go**.

The Spanning-Tree Management Page displays the current spanning-tree parameter settings and the member ports of VLAN 1.

**Step 3** Enable STP if you have previously disabled it. By default, STP is enabled on VLAN 1.

- (a) Select the **Enable Spanning Tree** check box to enable STP.
- (b) Click **Apply**.

---

**Note** You can slightly improve performance on the switch by disabling STP. However, disable STP only if you are sure there are no loops in your network topology. With STP disabled and loops present in the topology, network performance is degraded by excessive traffic and the indefinite packet duplication.

---

**Step 4** In the Path Cost column, enter a number from 1 to 65535 for each port. The default is 19.

The path cost is inversely proportional to the LAN speed of the network interface at the port. A high path cost means the port has low bandwidth and should not be used, if possible. A lower path cost represents higher-speed transmission; this setting can affect which port remains enabled in the event of a loop.

---

**Note** We recommend setting the path cost to 100 if the port is set to run at 10 Mbps.

---

**Step 5** In the Priority column, enter a number from 1 to 255 for each port. The default is 128. The lower the number, the higher the priority.

**Step 6** In the Port Fast Mode column, select a port, and select the check box to enable the Port Fast feature (if the port is connected to an end station). The default is Disabled (check box is not selected).

The Port Fast feature immediately brings a port from the blocking state into the forwarding state by eliminating the forward delay (the amount of time a port waits before changing from its STP learning and listening states to the forwarding state). Port Fast Mode-enabled ports should only be used for end-station attachments.

**Step 7** Click **Apply**.

## Checking the Port Status and Forwarding Status

The State column displays the state of the port. A port can be in one of the following states:

Blocking	The port is not forwarding frames and is not learning new addresses.
Listening	The port is not forwarding frames but is progressing toward a forwarding state. The port is not learning addresses.
Learning	The port is not forwarding frames but is learning addresses.
Forwarding	The port is forwarding frames and learning addresses.
Disabled	The port has been removed from STP operation. Administrative intervention is required to enable the port.

The Forward Transitions column displays the number of times STP changed forwarding states.

# Checking or Resetting Exception and Utilization Statistics

To see the exception and utilization statistics for the switch, Click **STATISTICS** on the menu bar to display the Statistics Reports Page (Figure 3-13) and check the switch statistics.

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the Statistics Reports Page to access this information online.

Figure 3-13 Statistics Reports Page

The screenshot shows the Cisco Statistics Reports Page. At the top, a navigation menu includes: HOME, PORT, ADDRESS, IP, SNMP, SPAN, CDP, VLAN, STP, **STATISTICS**, and SYSTEM. The main content area is titled "Statistics Reports" and includes a "Select Port:" dropdown menu and two buttons: "Reset Port Statistics" and "Reset All Statistics".

Annotations on the page include:

- An arrow pointing to the "Reset Port Statistics" button with the text: "Resets the statistics for the port displayed in the Select Port field."
- An arrow pointing to the "Reset All Statistics" button with the text: "Resets the statistics for the switch."
- An arrow pointing to the "Exception Statistics Report (frame counts):" section with the text: "Displays the number of receive and transmit errors for each port."
- An arrow pointing to the "Utilization Statistics Report:" section with the text: "Displays the number of frames received and transmitted for each port."
- An arrow pointing to the "Reload" button at the bottom with the text: "Refreshes the statistics displayed on this page."

On the left side of the screenshot, there are several buttons: "Apply", "Revert", and "Help". Text next to them reads: "Apply the new settings to the current configuration" and "Revert to the previous settings". A note states: "All contents copyright © 1996 by Cisco Systems, Inc."

On the far left, a separate text block says: "Procedures and detailed field descriptions are provided here."

Two data tables are shown:

**Exception Statistics Report (frame counts):**

Port	Receive Errors	Transmit Errors	Port	Receive Errors	Transmit Errors
1	55	61	5	59	65
2	56	62	6	60	66
3	57	63	7	61	67
4	58	64	8	62	68

**Utilization Statistics Report:**

Port	Receive Bytes	Transmit	Port	Receive Bytes	Transmit
1	51	57	5	55	61
2	52	58	6	56	62
3	53	59	7	57	63
4	54	60	8	58	64

15385

## Resetting Port and Switch Statistics

To reset the statistics of a switch port:

**Step 1** Select the port from the Select Port list.

**Step 2** Click **Reset Port Statistics**.

To reset the statistics for all ports on the switch, click **Reset All Statistics**.

The switch manager does not automatically refresh the statistics shown on this page. Click **Reload** to refresh the statistics shown on this page.

## Checking Exception Statistics

This report displays the number of receive and transmit errors for each port.

Receive      Number of giants and FCS and alignment errors.

Transmit     Number of excessive deferrals, late collisions, jabber errors, and other transmit errors.

## Checking Utilization Statistics

This report displays the number of bytes received and transmitted for each port.

Receive      Number of bytes received in good packets.

Transmit     Number of bytes transmitted.

# Changing the System Configuration

Cisco periodically provides new firmware to implement enhancements and maintenance releases. New firmware releases can be downloaded from Cisco Connection Online (CCO), the Cisco Systems' customer web site available at the following URLs: [www.cisco.com](http://www.cisco.com), [www-china.cisco.com](http://www-china.cisco.com), and [www-europe.cisco.com](http://www-europe.cisco.com).

The Firmware Version field displays the firmware version in use. You can download the latest switch firmware from a TFTP server.

---

**Note** When you download the firmware permanently to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Do not turn off the switch. The switch then resets and begins using the new firmware.

---



**Caution** If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted. For recovery procedures, see the “Recovering from Corrupted Firmware” section on page 4-8.

If you want to upgrade the switch firmware, click **SYSTEM** on the menu bar to display the System Configuration Page (Figure 3-14).

---

**Note** This section provides detailed information about this page and procedures on changing the settings. When you are using the switch manager, click **Help** on the System Configuration Page to access this information online.

---

Figure 3-14 System Configuration Page

The screenshot shows the Cisco System Configuration page with the following sections and annotations:

- System Configuration**
  - Console Configuration**
    - Baud Rate: 9600 baud
    - Data Bits: 8 bit(s)
    - Stop Bits: 2 bit(s)
    - Parity Setting: Even
    - CLI Inactivity Timeout: 0 seconds (0, 30-65500 [0])

Annotation: Before downloading the upgrade file to the switch via XMODEM protocol, make sure the settings of the switch console port and management station match.
  - Firmware Upgrade Options**
    - Firmware Version: 1.0.0.0
    - Server IP Address: 0.0.0.0
    - Filename for Firmware Upgrades: [empty field]
    - Download Mode: Permanent (selected), Temporary
    - System TFTP Upgrade button

Annotation: Displays the firmware version used by the switch.

    - Permanently downloads the new firmware to Flash memory.
    - Temporarily downloads the new firmware to DRAM. After a power cycle, the switch uses the previous firmware version.

On the left side of the page, there are buttons for **Apply**, **Revert**, and **Help**. A note states: "Apply the new settings to the current configuration" and "Revert to the previous settings". A copyright notice reads: "All contents copyright © 1998 by Cisco Systems, Inc."

On the far left, a text box says: "Procedures and detailed field descriptions are provided here." with an arrow pointing to the **Help** button.

### Configuring the Switch Console Port

The console port on the switch provides terminal and PC access to the switch. After the switch is installed, be sure to configure the console port settings of the switch to match the settings of the terminal or PC.

These are the default settings of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.

---

**Note** If data bits is 8, set parity to None.

---

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

If you change any of these settings, click **Apply** to save your changes.

### Changing the CLI Inactivity Timeout Setting

You can change the number of seconds that the CLI can wait without activity before it times out. After timeout, you must reenter the password.

To change the inactivity timeout parameter:

**Step 1** Enter the number of seconds (0, or 30 to 65500) in the CLI Inactivity Timeout field. The default is 0 (which means the console session does not time out).

**Step 2** Click **Apply**.

## Upgrading the Switch Firmware

The Firmware Version field displays the firmware version used by the switch. You can upgrade the firmware by following these steps to download the latest firmware from a TFTP server to your switch:

**Step 1** In the Server IP Address field, enter the IP address of the TFTP server on which the upgrade file is located.

**Step 2** Enter the upgrade filename (up to 80 characters) in the Filename for Firmware Upgrades field.

**Step 3** Select one of these download modes:

- **Permanent** to download the firmware to Flash memory.
- **Temporary** to download the firmware to DRAM. Use this option to test the new firmware before overriding the previous firmware. After a power cycle, the switch discards the new firmware and uses the previous firmware.

The default is Permanent.

**Step 4** Click **System TFTP Upgrade** to download the upgrade file from the TFTP server to the switch.

**Step 5** Click **OK** on the confirmation prompt.

---

**Note** When you download the firmware permanently to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Do not turn off the switch. The switch then resets and begins using the new firmware.

---



**Caution** If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted. For recovery procedures, see the “Recovering from Corrupted Firmware” section on page 4-8.

