HP 1810 Switches

Management and Configuration Guide

HP 1810 Switches

September 2012

Management and Configuration Guide

Publication Number

5998-3208
September 2012

Applicable Products

HP 1810-8 Switch	J9800A
HP 1810-8G Switch	J9802A
HP 1810-24 Switch	J9801A
HP 1810-24G Switch	J9803A

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Java^{TM} is a US trademark of Sun Microsystems, Inc.

Open Source Code Notice

Open Source Software shall mean those portions of the software that were made available to HP pursuant to, and may only be distributed pursuant to, the GNU General Public License* or a similar license that prohibits distribution of Open Source Software or derivative works of the Open Source Software on alternative terms.

HP makes such Open Source Software available to you pursuant to the same terms on which such Open Source Software was made available to HP and on no other or additional terms.

The Open Source Software modules and "make" files contained in the Software are available for HP in the form of a compact disk (CD). The CD includes the "original package" (original source files plus the "make" files) as well as a "patch" file that accounts for the modification made from the original source code. To receive the CD, HP charges a small fee in order to cover the actual costs of manufacturing and shipping the CD.

The request must be sent via email to Hpn.gpl@hp.com. The modified GPL license can be found at ecos.sourceware.org.

The information contained herein is subject to change without notice.

Note: The eCos software distribution also contains other software packages covered by BSD, MIT, or similar licenses.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

For HP networking warranty information, visit
www.hp.com/networking/support

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.hp.com/networking/support

Preface

About This Document

HP 1810 series switches provide reliable, plug-and-play Gigabit network connectivity. As the follow-on to the popular HP Switch 1800 series, the HP 1810 series switches provide additional network security capabilities, enhancements to ease of use, improved energy efficiency, and expanded deployment flexibility. It is ideal for open offices that require silent operation or businesses making the transition from unmanaged to managed networks.

The HP 1810 series switches can be managed in-band from a remote network station using a web GUI, and its configuration may also be viewed using the SNMP manager. This guide describes how to configure and view the software features using the Web-based graphical user interface (GUI).

Audience

The information in this guide is primarily intended for System administrators and Support providers who are responsible for configuring, operating, or supporting a network using HP 1810 series switch software. An understanding of the software specifications for the networking device platform, and a basic knowledge of Ethernet and networking concepts, are presumed.

About Your Switch Manual Set

The switch manual set includes the following:

- **Quick Setup Guide** - a printed guide shipped with your switch. Provides illustrations for basic installation and setup guidelines.
- **Regulatory and Safety Information** - printed documentation shipped with your switch. Includes Regulatory statements and standards supported by the switch, along with product specifications.
- **Installation and Getting Started Guide** - (HP Web site only). Provides detailed installation guide for your switch, including physical installation on your network, basic troubleshooting, product specifications, supported accessories, Regulatory and Safety information.
- **Management and Configuration Guide** - This guide describes how to manage and configure switch features using a Web browser interface.
- **Release Notes** - (HP Web site only). Provides information on software updates. The Release Notes describe new features, fixes, and enhancements that become available between revisions of the above guides.

Note For the latest version of all HP documentation, visit the HP Web site at **www.hp.com/networking/support.** Then select your switch product.

Supported Features

HP 1810 series switches include support for the following features:

Feature	1810 Series Switches
Web session timeout	0–60 min
DHCP server configuration	1
HTTP sessions	10
SNMP v1/v2c (read-only) community	1
MAC table	8 k
SNTP server configuration	1
Time zones s count	91
Daylight Saving Time offset	1 min –1440 min
Jumbo frame size	9216 bytes
Soft session HTTPS timeout	1 min–60 min
Hard session HTTPS timeout	1 Hr–168 Hrs
HTTPS sessions	5
Trunk configuration (1810-24/1810-24G)	12
Trunk configuration (1810-8/1810-8G)	4
Trunk membership ports (1810-24/1810-24G)	8
Trunk membership ports (1810-8/1810-8G)	7
VLANs	64
VLAN IDs	4094
VLAN priority levels	0–7
Syslog servers	1
Buffered logs	100 (total storage 10K)
Maintenance users	1
Password length	8 chars–64 chars
Images	2

Contents

Preface

About This Document iii

About Your Switch Manual Set iii

Supported Features iv

1 Getting Started

Connecting the Switch to a Network 1-1

Operating System and Browser Support 1-2

Getting Started With the Web Interface 1-3

Logging On 1-3

Interface Layout and Features 1-3

Common Page Elements 1-4

Saving Changes 1-5

User-Defined Fields 1-5

Web Applet 1-5

System LEDs 1-5

2 Status Pages

System Description 2-1

Log 2-3

Port Summary 2-4

LLDP Statistics 2-6

Trunk 2-8

MAC Table 2-9

Loop Protection 2-10

Spanning Tree 2-11

Green Features 2-13

Dual Image 2-15

Clock 2-16

3 Network Setup

Get Connected 3-1

Simple Network Time Protocol 3-4

Time Zone 3-6

Daylight Saving Time 3-7

4 Switching Pages

Port Configuration 4-1

Auto Detect and Configure Fiber Modules 4-1

Jumbo Frames 4-2

Port Mirroring 4-3

Flow Control 4-5

Green Features 4-6

Loop Protection 4-8

Spanning Tree 4-10

5 Security

Advanced Security 5-1

Secure Connection 5-2

Downloading SSL Certificates and Diffie-Hellman Files 5-4

Generating Certificates 5-5

6 Trunks

Trunk Configuration and Membership 6-1

7 Virtual LAN

VLAN Configuration 7-1

VLAN Ports 7-2

VLAN Participation / Tagging 7-3

8 Link Layer Discovery Protocol (LLDP)

LLDP Configuration 8-1

LLDP Local Device 8-3

LLDP Remote Device 8-4

Energy Efficient Ethernet 8-5

9 Diagnostics

Ping Test 9-1

Log Configuration 9-2

Reboot Switch 9-3

Factory Defaults 9-3

Support File 9-4

Locator 9-5

10 Maintenance Pages

Backup Manager 10-1

Example—Backing Up a Configuration File 10-2

Update Manager 10-3

Example—Updating the Switch Software 10-4

Password Manager 10-7

Dual Image Configuration 10-8

1

Getting Started

This chapter describes how to make the initial connections to the switch and provides an overview of the Web interface.

Connecting the Switch to a Network

To enable remote management of the switch through a Web browser, the switch must be connected to the network. The switch is pre-configured with an IP address for management purposes. After initial configuration, the switch can also be configured to acquire its address from a DHCP server on the network.

By default, the switch is assigned the following static IP information for access to the Web interface:

- IP address: 192.168.2.10
- Network mask: **255.255.255.0**
- Gateway: 0.0.0.0

1. Connect the switch to the management PC or to the network using any of the available network ports.
2. Power on the switch.
3. Set the IP address of the management PC's network adaptor to be in the same subnet as the switch.

   Example: Set it to IP address 192.168.2.12, mask 255.255.255.0.
4. Enter the IP address shown above in the Web browser. See page 1-3 for web browser requirements.

Thereafter, use the Web interface to configure a different IP address or configure the switch as a DHCP client so that it receives a dynamically assigned IP address from the network.

Note

- If you enable DHCP for IP network configuration, the switch must be connected to the same network as the DHCP server. You will need to access your DHCP server to determine the IP address assigned to the switch.
- The switch supports LLDP (Link Layer Discovery Protocol), allowing discovery of its IP address from a connected device or management station.
- If DHCP is used for configuration and the switch fails to be configured, the IP address 192.168.2.10 is reassigned.

After the switch is able to communicate on your network, enter its IP address into your Web browser's address field to access the switch management features.

Operating System and Browser Support

The following operating systems and browsers with JavaScript enabled are supported:

Operating System	Browser
Windows XP SP3 and Windows 7	Internet Explorer 7, 8 Firefox 7–13 Google Chrome 13, 14
MacOS	Firefox 12 and 13 Google Chrome 19 and 20

Getting Started With the Web Interface

This section describes the following Web pages:

- "Logging On" on page 1-3
- "Interface Layout and Features" on page 1-3

Logging On

Follow these steps to log on through Web interface:

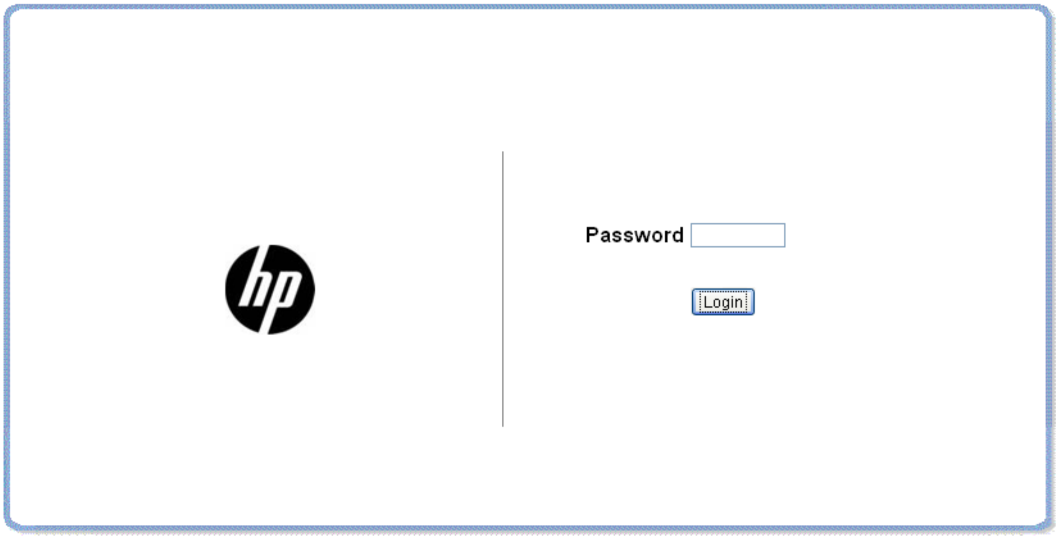
1. Open a Web browser and enter the IP address of the switch in the Web browser address field.
2. On the Login page, enter the password (if one has been set), and then click **Login**.

   By default, there is no password. After the initial log on, the administrator may configure a password.

Note

To set passwords, see "Password Manager" on page 10-7.

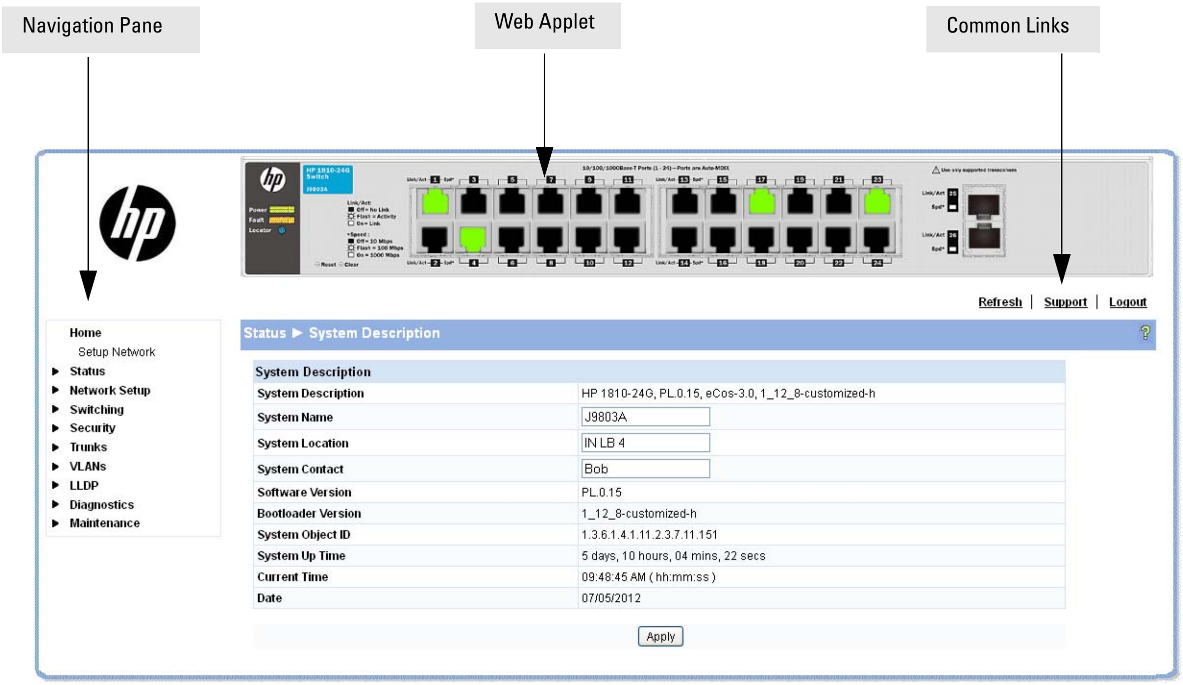
Figure 1-1. Login Page



Interface Layout and Features

Figure 1-2 shows the initial view.

Figure 1-2. Interface Layout and Features



System Description	
System Description	HP 1810-24G, PL.0.15, eCos-3.0, 1_12_8-customized-h
System Name	J9803A
System Location	IN LB 4
System Contact	Bob
Software Version	PL.0.15
Bootloader Version	1_12_8-customized-h
System Object ID	1.3.6.1.4.1.11.2.3.7.11.151
System Up Time	5 days, 10 hours, 04 mins, 22 secs
Current Time	09:48:45 AM (hh:mm:ss)
Date	07/05/2012

Click on any topic in the navigation page to display related configuration options.

The System Description page displays when you first log on and when you click **Home or Status > System Description** in the navigation pane. See "System Description" on page 2-1 for more information.

You can click the **Setup Network** link beneath **Home** to display the **Get Connected** page, which you use to set up a management connection to the switch. You can also click **Network Setup > Get Connected** to display this page. See "Get Connected" on page 3-1 for more information.

The Web Applet displays summary information for the switch LEDs and port status in a graphical format. For information on the Web Applet, see "Web Applet" on page 1-5.

Common Page Elements

- Click ? on each page to display a help panel that explains the fields and configuration options on the page.
- Click Apply to send the updated configuration to the switch. Configuration changes take effect immediately.

Note

Configuration changes take effect immediately and are saved to the system configuration file after a 1-minute delay. See "Saving Changes" on page 1-5 below.

- Click **Refresh** to refresh the page with the latest information from the switch.
- Click **Support** to access the HP ProCurve Web site (Internet access required).
- Click **Logout** to end the current management session.

Saving Changes

When you click Apply, changes are saved automatically to the system configuration file in flash memory.
A progress indicator is displayed next to the Help icon while the operation is in progress.

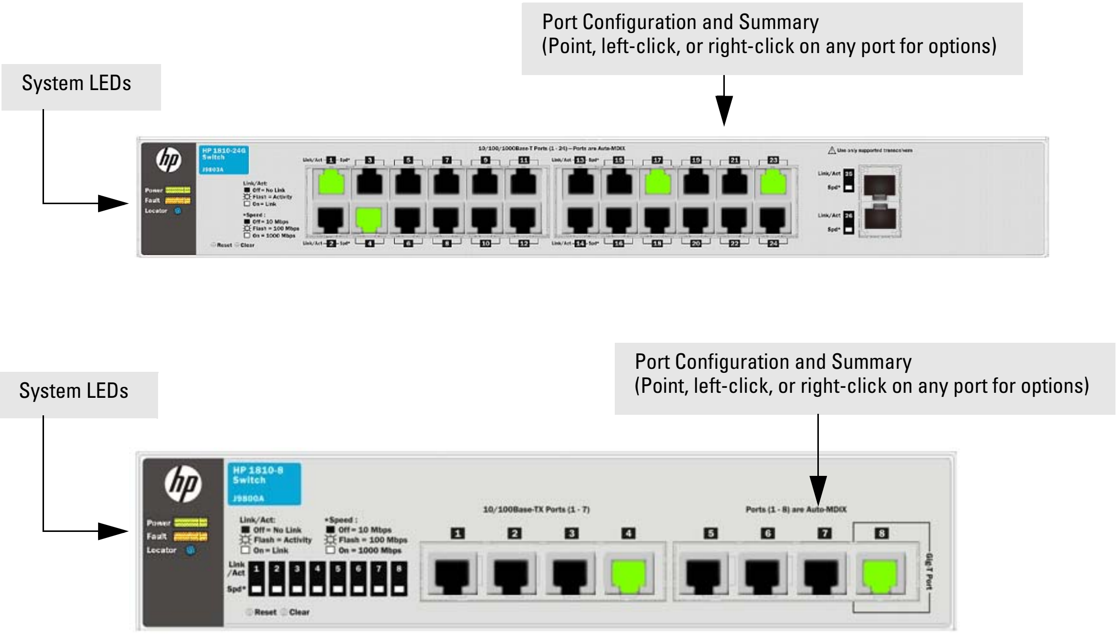
User-Defined Fields

User-defined fields can contain 1–31 characters, including hyphens, commas, and spaces.

Web Applet

The Web Applets, shown in Figure 1-3, display at the top of the page as a graphic representation of the switch to provide information regarding the status parameters of individual ports. The Web Applet enables easy system configuration and Web-based navigation.

Figure 1-3. Web Applet



Port Configuration and Summary—You can point to any port to display the following information about the port:

- Auto Negotiation Status
- Speed

Left-click a port to display its Port Configuration page, or right-click and select from the menu to display its Port Configuration Page or the Port Summary page for all ports.

System LEDs

Point to the System LEDs area to view information about the following LEDs:

- Power (Green)
  - On— The switch is receiving power.

  - Off—The switch is NOT receiving power.

- Fault (Orange)
  - Blinking—A fault has occurred, other than during self-test.
  - On—Self-test in progress.
  - Off—The switch is operating properly.
- Locator (Blue)
  - Blinking—The switch is in Locate mode, attempting to locate a specific switch.
  - Off—The locator is disabled. This mode can be enabled using the Web interface. See "Locator" on page 9-5.

Port LEDs

Each 10/100/1000 Mbps RJ45 port has two single color LEDs to indicate the, Link/Activity on the Left port LED and the Speed status indicated by the Right port LED.

The left-port LED indicates link status, as follows:

- On—The port is enabled and receiving a link indication or other signal from the connected device.
- Blinking—The port has network activity.
- Off—The port has no active network cable connected, is not receiving link signal, or is disabled.

The right-port LED indicates speed status, as follows:

- On—The port is operating continuously at 1000 Mbps.
- Blinking—The port is operating at 100 Mbps.
- Off—The port is operating at 10 Mbps.

Note

The PD LEDs on the HP1810-8G glow when the switch is powered via the PD Port 1 using an external PoE device.

Status Pages

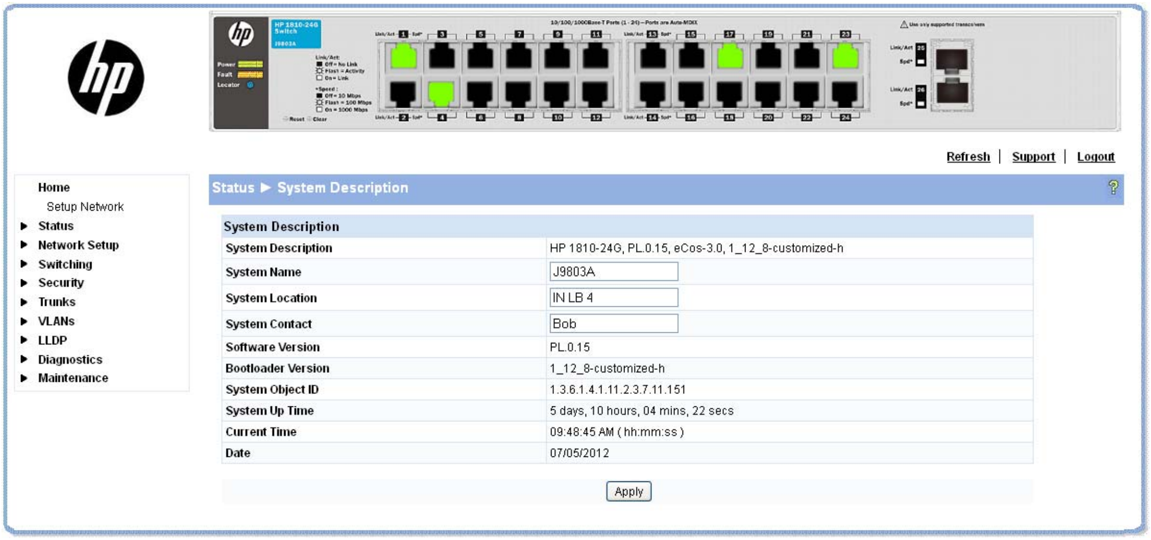
You can use the Status pages to view system information and statistics.

System Description

The System Description page displays basic information such as the product name, model, ports, and switch type: Gigabit Ethernet or a Fast Ethernet. The software and boot ROM versions are also displayed. In addition, the system name, location, and contact can be configured on this page.

This page is displayed when you first log on or when you click **Home** or **Status > System Description** in the navigation pane.

Figure 2-1. System Description Page



System Description	
System Description	HP 1810-24G, PL.0.15, eCos-3.0, 1_12_8-customized-h
System Name	J9803A
System Location	IN LB 4
System Contact	Bob
Software Version	PL.0.15
Bootloader Version	1_12_8-customized-h
System Object ID	1.3.6.1.4.1.11.2.3.7.11.151
System Up Time	5 days, 10 hours, 04 mins, 22 secs
Current Time	09:48:45 AM (hh:mm:ss)
Date	07/05/2012

Click Apply to save any changes for the current boot session; the changes take effect immediately.

Table 2-1. System Description Fields

Field	Description
System Description	The product name of the switch including the model, ports, and whether a Gigabit Ethernet or a Fast Ethernet switch. The software and Boot ROM version are also displayed.
System Name	Enter the preferred name to identify this switch. A maximum of 31 alpha-numeric characters including hyphens, commas and spaces are allowed. This field is blank by default.
System Location	Enter the location of this switch. A maximum of 31 alpha-numeric characters including hyphens, commas, and spaces are allowed. This field is blank by default.
System Contact	Enter the name of the contact person for this switch. A maximum of 31 alpha-numeric characters including hyphens, commas, and spaces are allowed. This field is blank by default.
Software Version	The version of the code running on the switch in the format "release.version.maintenance."
Bootloader Version	The version of the current system bootloader.
System Object ID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current Time	The current time in hours, minutes and seconds as configured(24 or 12-hr AM/PM format) by the user.
Date	The current date in month, day, and year format.

Note

The System Name, System Location, and System Contact accept all alphanumeric characters including hyphens, commas and spaces.

Log

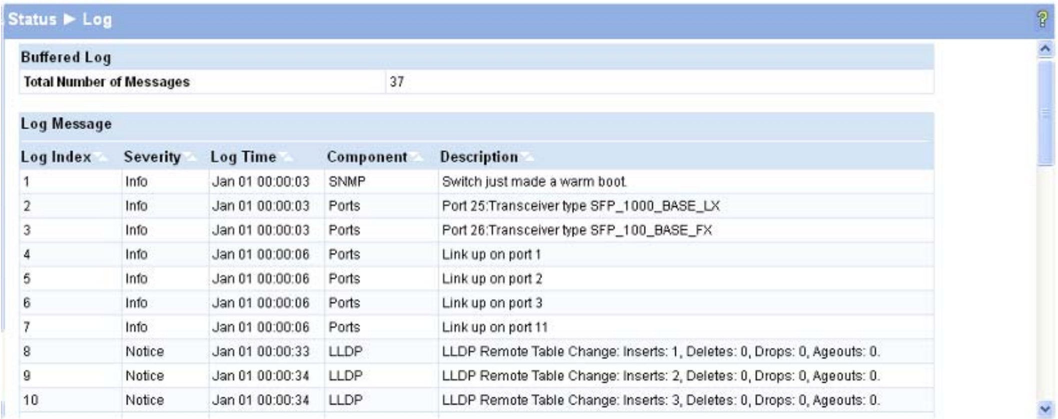
The Log status page displays logged system messages, such as configuration failures and user sessions. The log page displays the 100 most recent log entries. The newest log entry, by default, is displayed at the bottom of the list.

Note

If more than 100 logs accumulate, their Log Index numbers continue to increment beyond 100 and the oldest entries are deleted (for example, if 200 log entries were generated since the system was last restarted or the log file was cleared, then the log file would display entries 101–200).

To display the Log status page, click **Status > Log** in the navigation pane.

Figure 2-2. Log Page



Status ▶ Log

Buffered Log

Total Number of Messages	37

Log Message

Log Index	Severity	Log Time	Component	Description
1	Info	Jan 01 00:00:03	SNMP	Switch just made a warm boot.
2	Info	Jan 01 00:00:03	Ports	Port 25:Transceiver type SFP_1000_BASE_LX
3	Info	Jan 01 00:00:03	Ports	Port 26:Transceiver type SFP_100_BASE_FX
4	Info	Jan 01 00:00:06	Ports	Link up on port 1
5	Info	Jan 01 00:00:06	Ports	Link up on port 2
6	Info	Jan 01 00:00:06	Ports	Link up on port 3
7	Info	Jan 01 00:00:06	Ports	Link up on port 11
8	Notice	Jan 01 00:00:33	LLDP	LLDP Remote Table Change: Inserts: 1, Deletes: 0, Drops: 0, Ageouts: 0.
9	Notice	Jan 01 00:00:34	LLDP	LLDP Remote Table Change: Inserts: 2, Deletes: 0, Drops: 0, Ageouts: 0.
10	Notice	Jan 01 00:00:34	LLDP	LLDP Remote Table Change: Inserts: 3, Deletes: 0, Drops: 0, Ageouts: 0.

- Click the arrows next to the column headings to sort the list by the column, in ascending or descending order.
- Click **Clear** to delete all log messages.
- Click the **Refresh** link above the page to re-display the page with new logs.

Table 2-2. System Description Fields

Field	Description
Total Number of Messages	Total number of log messages reported during System up time.
Log Message	
Log Index	Log number in the log table.
Severity	Severity associated with the log message.
Log Time	Time at which the log was entered in the table.
Component	Component from which the massage was logged.
Description	Description of the entry.

For information on configuring log settings, see "Log Configuration" on page 9-2.

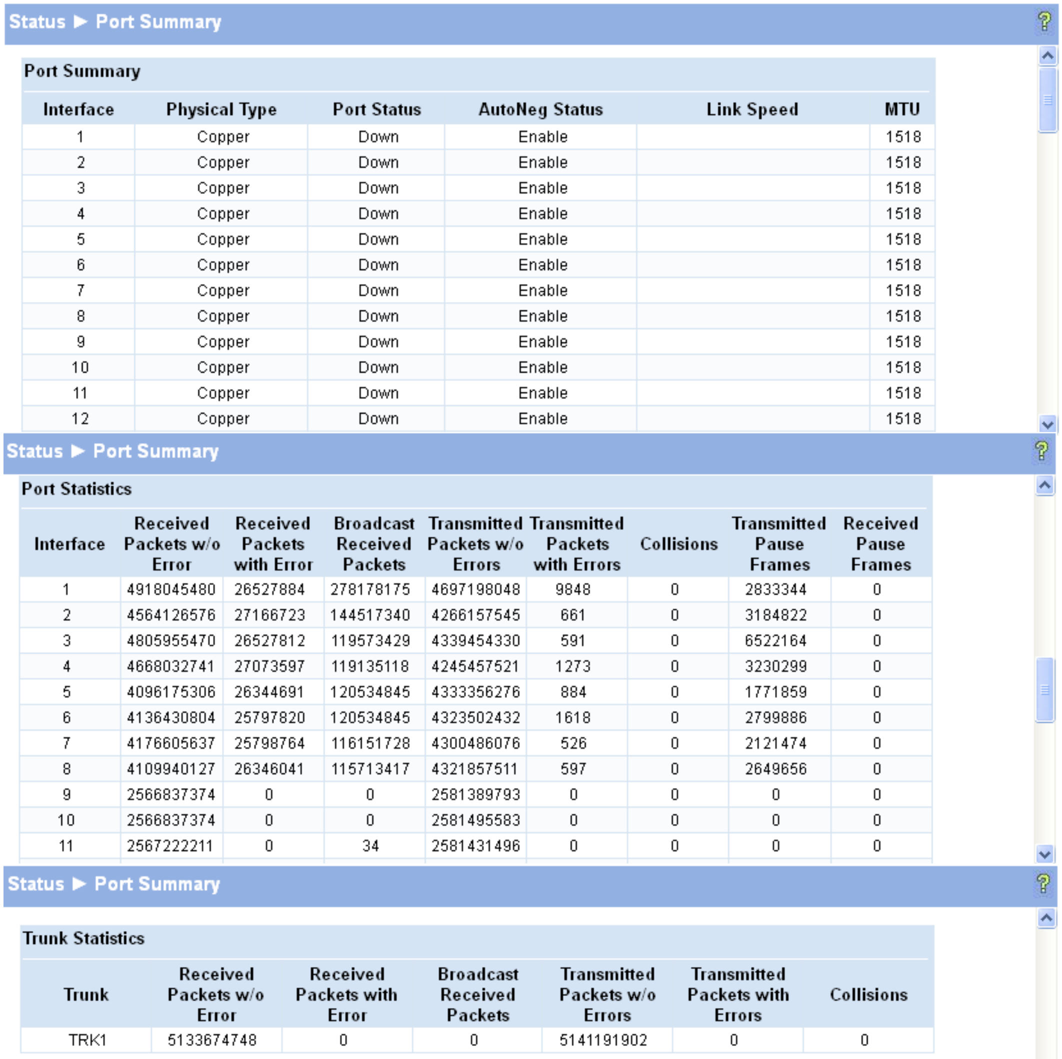
Port Summary

The Port Summary page displays a summary of network traffic from the ports. This summary can be used to identify potential problems with the switch. It also helps to identify what has been configured on this port. The displayed values are accumulated after the last clear operation. Refreshing the page shows the latest statistics, which provide per-port statistics on packets transmitted and received for all the ports. Scroll down the page to view the Port Statistics table, which provides per-port statistics on packets transmitted and received.

To display the Port Summary page, click **Status > Port Summary** in the navigation pane.

A configuration summary and status of all physical and logical ports are displayed in Figure 2-3.

Figure 2-3. Port Summary Page



Status ▶ Port Summary

Port Summary

Interface	Physical Type	Port Status	AutoNeg Status	Link Speed	MTU
1	Copper	Down	Enable		1518
2	Copper	Down	Enable		1518
3	Copper	Down	Enable		1518
4	Copper	Down	Enable		1518
5	Copper	Down	Enable		1518
6	Copper	Down	Enable		1518
7	Copper	Down	Enable		1518
8	Copper	Down	Enable		1518
9	Copper	Down	Enable		1518
10	Copper	Down	Enable		1518
11	Copper	Down	Enable		1518
12	Copper	Down	Enable		1518

Status ▶ Port Summary

Port Statistics

Interface	Received Packets w/o Error	Received Packets with Error	Broadcast Received Packets	Transmitted Packets w/o Errors	Transmitted Packets with Errors	Collisions	Transmitted Pause Frames	Received Pause Frames
1	4918045480	26527884	278178175	4697198048	9848	0	2833344	0
2	4564126576	27166723	144517340	4266157545	661	0	3184822	0
3	4805955470	26527812	119573429	4339454330	591	0	6522164	0
4	4668032741	27073597	119135118	4245457521	1273	0	3230299	0
5	4096175306	26344691	120534845	4333356276	884	0	1771859	0
6	4136430804	25797820	120534845	4323502432	1618	0	2799886	0
7	4176605637	25798764	116151728	4300486076	526	0	2121474	0
8	4109940127	26346041	115713417	4321857511	597	0	2649656	0
9	2566837374	0	0	2581389793	0	0	0	0
10	2566837374	0	0	2581495583	0	0	0	0
11	2567222211	0	34	2581431496	0	0	0	0

Status ▶ Port Summary

Trunk Statistics

Trunk	Received Packets w/o Error	Received Packets with Error	Broadcast Received Packets	Transmitted Packets w/o Errors	Transmitted Packets with Errors	Collisions
TRK1	5133674748	0	0	5141191902	0	0

Table 2-3. Port Summary Fields

Field	**Description**
Port Summary	
Interface	List of physical and logical interfaces supported or configured on a particular platform.
Physical Type	Displays whether the port is operating in copper mode or fiber mode.
Port Status	The physical status (up or down) of the link at the port.
AutoNeg Status	Displays whether Auto negotiation is enabled or disabled on the port.
Link Speed	The physical speed at which the port is operating.
MTU	The Maximum Transmission Unit (MTU), also referred to as Max Frame size acceptable on the specified port.
Port Statistics and Trunk Statistics **Note**: The following statistics are collected for both individual port and for trunks.	
Interface/Trunk	List of physical and logical interfaces supported on that platform.
Received Packets w/o Error	The packet count received on the port with out any packet errors.
Received Packets with Error	The packet count received on the port with errors.
Broadcast Received Packets	The packet count for Broadcast packets received on the port.
Transmitted Packets w/o Errors	The number of packets transmitted out of that port with out any packet errors.
Transmitted Packets with Errors	The number of packets transmitted out of the port with packet errors.
Collisions	The number of packet collisions.
Transmitted Pause Frames	The number of Ethernet pause frames transmitted. (This information is collected for ports but not for trunks.)
Received Pause Frames	The number of Ethernet pause frames received. (This information is collected for ports but not for trunks.)

- Click **Clear** to reset all statistics to their initial values.
- Click the **Refresh** link above the page to re-display the page with the latest port information.

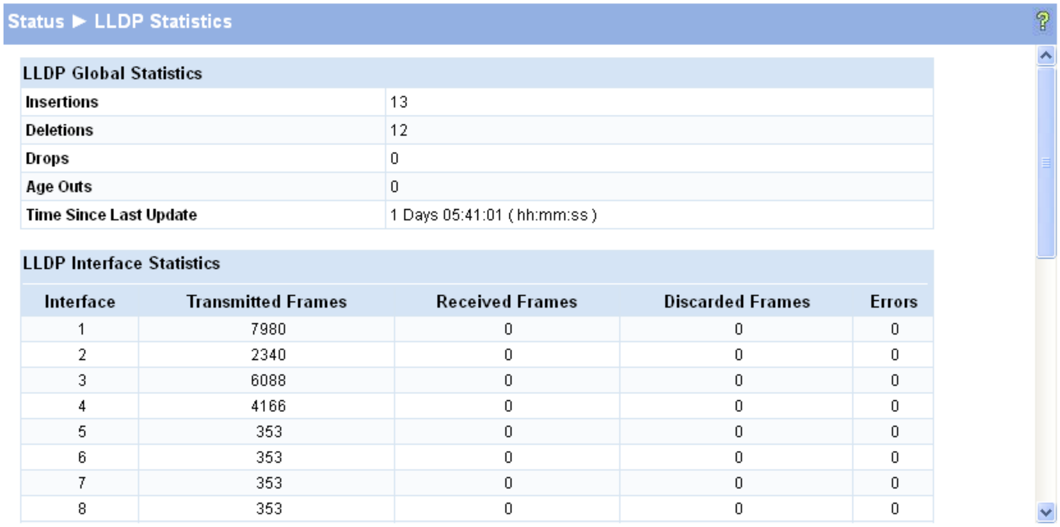
For instructions on configuring port settings, see “Port Configuration” on page 4-1.

LLDP Statistics

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.

To display the LLDP Statistics page, click **Status > LLDP Statistics** in the navigation pane.

Figure 2-4. LLDP Statistics Page



LLDP Global Statistics

Insertions	13
Deletions	12
Drops	0
Age Outs	0
Time Since Last Update	1 Days 05:41:01 (hh:mm:ss)

LLDP Interface Statistics

Interface	Transmitted Frames	Received Frames	Discarded Frames	Errors
1	7980	0	0	0
2	2340	0	0	0
3	6088	0	0	0
4	4166	0	0	0
5	353	0	0	0
6	353	0	0	0
7	353	0	0	0
8	353	0	0	0

Table 2-4. LLDP Statistics Page Fields

Field	Description
LLDP Global Statistics	
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by a particular MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems because the information timeliness interval has expired.
Time Since Last Update	Time when an entry was created, modified, or deleted in the tables associated with the remote system.
LLDP Interface Statistics	
Interface	List of interfaces present or configured on the system.
Transmitted Frames	The number of LLDP frames transmitted on the corresponding port.
Received Frames	The number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discarded Frames	The number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Errors	The number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.

- Click **Clear** to reset all statistics to their initial values.
- Click the **Refresh** link above the page to re-display the page with current data from the switch.

For instructions on configuring LLDP, see “LLDP Configuration” on page 8-1.

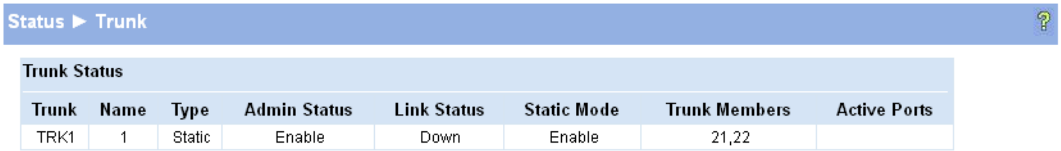
Trunk

The Trunk status page displays the configuration summary and status of each trunk.

To display the Trunk page, click **Status > Trunk** in the navigation pane.

Figure 2-5 displays the configuration summary and status of a trunk named Trunk1. This trunk is configured in dynamic mode and has 3 and 5 interfaces as its active members.

Figure 2-5. Trunk Page



Trunk Status

Trunk	Name	Type	Admin Status	Link Status	Static Mode	Trunk Members	Active Ports
TRK1	1	Static	Enable	Down	Enable	21,22	

Table 2-5. Trunk Port Configuration Fields

Field	Description
Trunk	ID assigned to the trunk by the system when the trunk is created.
Name	User-created name for the trunk.
Type	Indicates whether the trunk is Static or Dynamic. • Dynamic trunks use the Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them. • Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports.
Admin Status	Displays whether the trunk has been enabled or disabled administratively. When disabled, no traffic will flow. The messages that members of the trunk exchange in order to manage the trunk (LACPDUs) will be dropped, but the links that form the Trunk will not be released. The default is Enable.
Link Status	Displays whether the link is up or down.
Static Mode	Displays whether Static mode has been enabled on the trunk. When static mode is enabled, the trunk does not transmit or process received LACPDUs. The member ports do not transmit LACPDUs and all the LACPDUs it may receive are dropped. A static trunk does not require a partner system to be able to aggregate its member ports.
Trunk Members	List of member ports in the trunk.
Active Ports	List all active member ports in the trunk.

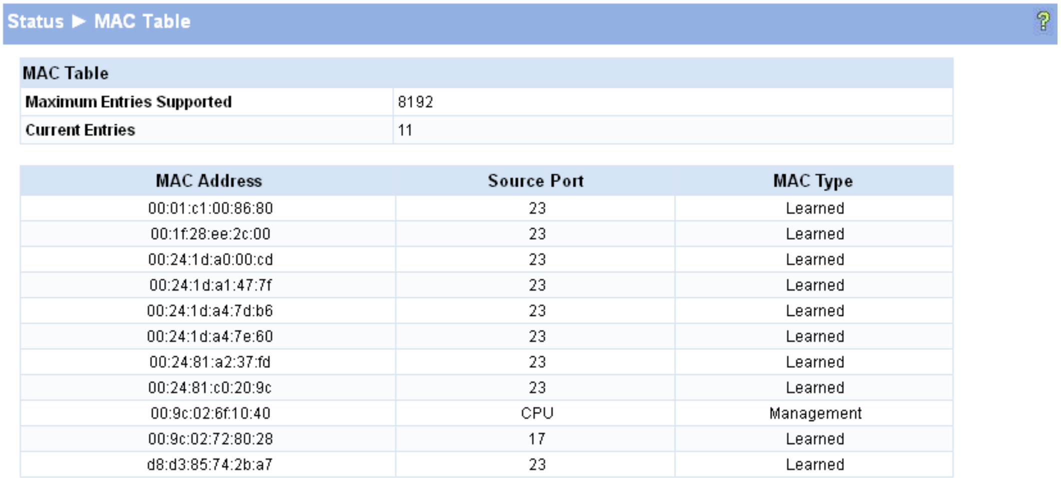
For information on configuring trunks, see “Trunk Configuration and Membership” on page 6-1.

MAC Table

The MAC Table page displays the MAC addresses configured for ports, and the MAC type including the maximum entries supported an d the current number of entries learned. The default aging interval for forwarding database is 300secs. Dynamically learned entries are removed if they are not updated within the aging interval on a particular interface

To display the MAC Table page, click **Status > MAC Table** in the navigation pane.

Figure 2-6. MAC Table Page



Status ▶ MAC Table

MAC Table	
Maximum Entries Supported	8192
Current Entries	11

MAC Address	Source Port	MAC Type
00:01:c1:00:86:80	23	Learned
00:1f:28:ee:2c:00	23	Learned
00:24:1d:a0:00:cd	23	Learned
00:24:1d:a1:47:7f	23	Learned
00:24:1d:a4:7d:b6	23	Learned
00:24:1d:a4:7e:60	23	Learned
00:24:81:a2:37:fd	23	Learned
00:24:81:c0:20:9c	23	Learned
00:9c:02:6f:10:40	CPU	Management
00:9c:02:72:80:28	17	Learned
d8:d3:85:74:2b:a7	23	Learned

Table 2-6. MAC Table Fields

Field	Description
Maximum Entries Supported	Displays a maximum of 8192 MAC address entries that can be learned on the switch.
Current Entries	Displays the number of MAC address entries currently learned.
MAC Address	The list of MAC addresses learned on a particular interface.
Source Port	The source interface on which the particular MAC address has been learned. *CPU* is a special source port used for internal management on the switch.
MAC Type	Shows whether the MAC address is dynamically learned or whether this is a management address.

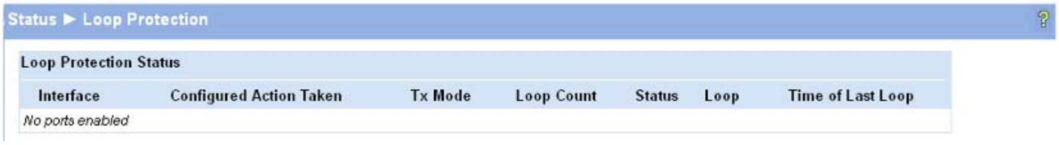
Click the **Refresh** link above the page to re-display the page with current data from the switch.

Loop Protection

The Loop Protection status page displays a summary of loop protection configured data on the switch and on each port, and loop protection network traffic for the switch and status information for each port.

To display the Loop Protection status page, click **Status > Loop Protection** in the navigation pane.

Figure 2-7. Loop Protection Page



Status ▶ Loop Protection

Loop Protection Status

Interface	Configured Action Taken	Tx Mode	Loop Count	Status	Loop	Time of Last Loop
No ports enabled						

Table 2-7. Loop Protection Fields

Field	Description
Interface	List of ports with loop protection currently enabled.
Configured Action Taken	The action that is set to occur when a loop is detected on the port with Loop Protection enabled: • **Shutdown port**—The port will be shut down for the configured period. • **Log**—The event will be logged and the port remains operational. • **Shutdown and log**—The event will be logged and the port it shut down for the configured period.
Tx Mode	Shows whether the port is configured to forward packets to the multicast destination MAC address designated for the Loop Protection feature.
Loop Count	The number of loops detected on this interface since the last system boot or since statistics were cleared.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

- Click **Clear** to reset all counters to 0.
- Click the **Refresh** link above the page to re-display the page with the latest status from the switch.

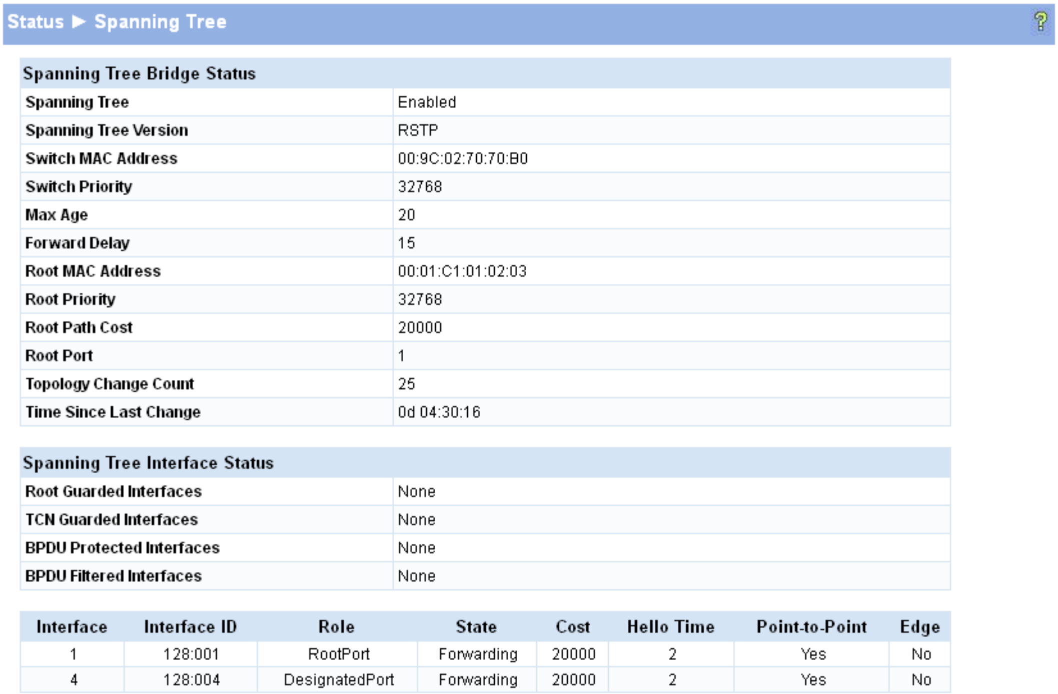
For instructions on configuring this feature and a description of these fields, see “Loop Protection” on page 4-8.

Spanning Tree

The Spanning Tree status page displays the global bridge configuration and the per-port spanning tree states.

To display the Spanning Tree page, click **Status > Spanning Tree** in the navigation pane.

Figure 2-8. Spanning Tree Status Page



Spanning Tree Bridge Status	
Spanning Tree	Enabled
Spanning Tree Version	RSTP
Switch MAC Address	00:9C:02:70:70:B0
Switch Priority	32768
Max Age	20
Forward Delay	15
Root MAC Address	00:01:C1:01:02:03
Root Priority	32768
Root Path Cost	20000
Root Port	1
Topology Change Count	25
Time Since Last Change	0d 04:30:16

Spanning Tree Interface Status	
Root Guarded Interfaces	None
TCN Guarded Interfaces	None
BPDU Protected Interfaces	None
BPDU Filtered Interfaces	None

Interface	Interface ID	Role	State	Cost	Hello Time	Point-to-Point	Edge
1	128:001	RootPort	Forwarding	20000	2	Yes	No
4	128:004	DesignatedPort	Forwarding	20000	2	Yes	No

Table 2-8. Spanning Tree Fields

Field	Description
Spanning Tree Bridge Status	
Spanning Tree	The current operational state of the bridge (enabled or disabled).
Spanning Tree Version	The current protocol version of the bridge (STP or RSTP).
Switch MAC Address	MAC address of the switch.
Switch Priority	The configured spanning tree priority of the switch.
Max Age	The current Max Age bridge parameter setting.
Forward Delay	The current Forward Delay bridge parameter setting.
Root MAC Address	MAC address of the current Root bridge.
Root Priority	Spanning Tree priority of the current Root bridge.

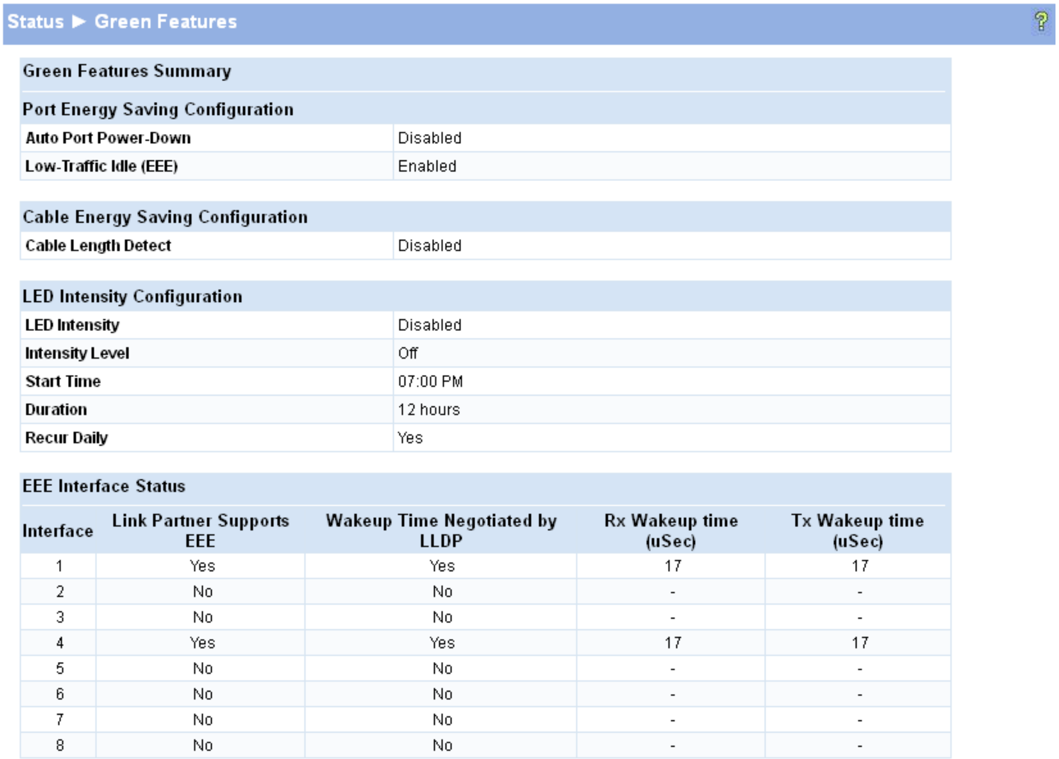
Field	Description
Root Path Cost	The sum of the Port Path costs on the least cost path to the Root bridge. For the Root bridge this is zero.
Root Port	The port on the switch that forwards traffic toward the Spanning Tree root.
Topology Change Count	Number of topology changes since STP was enabled.
Time Since Last Change	Time since last topology change was detected.
Spanning Tree Interface Status	
Root Guarded Interfaces	Interfaces with the Root Guard parameter currently set.
TCN Guarded Interfaces	Interfaces with the TCN Guard parameter currently set.
BPDU Protected Interfaces	Interfaces with the BPDU Guard parameter currently set.
BPDU Filtered Interfaces	Interfaces with the BPDU FIlter parameter currently set.
Interface	The port number.
Interface ID	The priority and port index used by the Spanning Tree protocol.
Role	The current Spanning Tree port role. The port role can be one of the following values: • **RootPort—**A forwarding port that is the best port from non-root bridge to Root bridge. • **DesignatedPort—**Each LAN segment has one designated port, a single bridge port to which packets destined toward the Root bridge are sent. • **AlternatePort—**When the Designated port is currently on a different bridge, the Alternate Port is a port on this bridge that may become the Designated port if needed. • **BackupPort—** When the Designated port is currently a different port on this bridge, the Backup port is a port on this bridge that can become the Designated port if needed. • **DisabledPort—**Not strictly part of the Spanning Tree protocol; a network administrator can manually disable the port.
State	The current Spanning Tree port state. The port state can be one of the following values: • **Blocking—**A port that may cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. • **Forwarding—**A port receiving and sending data. STP still monitors incoming BPDUs that may indicate it should return to the blocking state to prevent a loop. • **Disabled—**Not strictly part of STP, a network administrator can manually disable a port.
Cost	The current Spanning Tree port path cost. This value is either computed from the Auto setting or from any explicitly configured value.
Hello Time	Hello time parameter currently in use on the port
Point-to-Point	A yes/no value. Yes indicates a switched link with only two nodes. No indicates a shared network segment with more than two nodes. The value may be automatically computed or explicitly configured.
Edge	A yes/no value. Yes means there are no bridges attached to this port. No means there are, or might be, bridges attached. The value may be automatically computed or explicitly configured. If the value is Yes, the port transitions directly to the Forwarding Port state when Spanning Tree is enabled.

Green Features

The Green Features status page displays the status of the power-saving or green features.

To display the Green Features page, click **Status > Green Features** in the navigation bar.

Figure 2-9. Green Features Status Page



Status ► Green Features

Green Features Summary

Port Energy Saving Configuration	
Auto Port Power-Down	Disabled
Low-Traffic Idle (EEE)	Enabled

Cable Energy Saving Configuration	
Cable Length Detect	Disabled

LED Intensity Configuration	
LED Intensity	Disabled
Intensity Level	Off
Start Time	07:00 PM
Duration	12 hours
Recur Daily	Yes

EEE Interface Status

Interface	Link Partner Supports EEE	Wakeup Time Negotiated by LLDP	Rx Wakeup time (uSec)	Tx Wakeup time (uSec)
1	Yes	Yes	17	17
2	No	No	-	-
3	No	No	-	-
4	Yes	Yes	17	17
5	No	No	-	-
6	No	No	-	-
7	No	No	-	-
8	No	No	-	-

Table 2-9. Green Features Status Fields

Field	Description
Port Energy Saving Configuration	
Auto Port Power-Down	The current Auto Port Power-Down setting (Enabled or Disabled). When enabled, the port is set in power save mode when there is no link.
Low-Traffic Idle (EEE)	The current Energy Efficient Ethernet (EEE) setting (Enabled or Disabled). When enabled, ports that are not passing traffic are powered off until the link partner indicates the port should power on to receive new data.
Cable Energy Saving Configuration	
Cable Length Detect	The current Cable Length Detect setting (Enabled or Disabled). When enabled, port power consumption is adjusted based upon cable length. Short cables use less power than long cables.
LED Intensity Configuration	
LED Intensity	The setting (Enabled or Disabled) that indicates if the switch is configured to change LED intensity levels at certain times of day.
Intensity Level	The desired LED intensity level that takes effect if the LED Intensity setting is enabled. Valid values are High, Medium, Low, or Off. Default value is Off.
Start Time	The time of day when the configured LED Intensity Level is activated.
Duration	The number of hours the configured LED Intensity Level is in effect.
Recur Daily	The current setting (Yes or No) that indicates if the LED intensity levels will change daily at the configured time.
EEE Interface Status	
Interface	The port number.
Link Partner Supports EEE	Indicates if the link partner supports EEE (Yes or No).
Wakeup Time Negotiated by LLDP	Indicates if the EEE wakeup time is negotiated with the link partner (Yes or No). If No, the Rx Wakeup time and Tx Wakeup time columns display a dash.
Rx Wakeup Time (µSec)	The Rx Wakeup time in effect for that port.
Tx Wakeup Time (µSec)	The Tx Wakeup time in effect for that port.

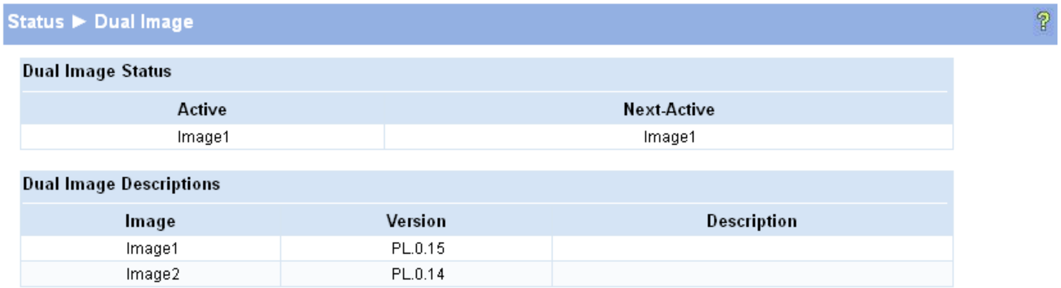
Dual Image

The Dual Image status page displays the status of the two software images (*image1* and *image2*) on the switch. It also provides details about the current active and alternate images, and software image versions.

To display the Dual Image page, click **Status > Dual Image** in the navigation bar.

As shown in Figure 2-10, Image1 is the active image and will continue to be the active image after a reboot.

Figure 2-10. Dual Image Status Page



Status ▶ Dual Image

Dual Image Status

Active	Next-Active
Image1	Image1

Dual Image Descriptions

Image	Version	Description
Image1	PL.0.15	
Image2	PL.0.14	

Table 2-10. Dual Image Status Fields

Field	Description
Active	The currently active image name.
Next-Active	The next active image name. The administrator can configure the image to take effect the next time the system is booted. It may be a different than the currently active image (for example, if the administrator configures the backup image to take effect upon the next reboot).
Image	The name of the firmware image. The primary image is Image1; the alternate image is Image2.
Version	The version of the firmware image.
Description	The configured descriptions for the images.

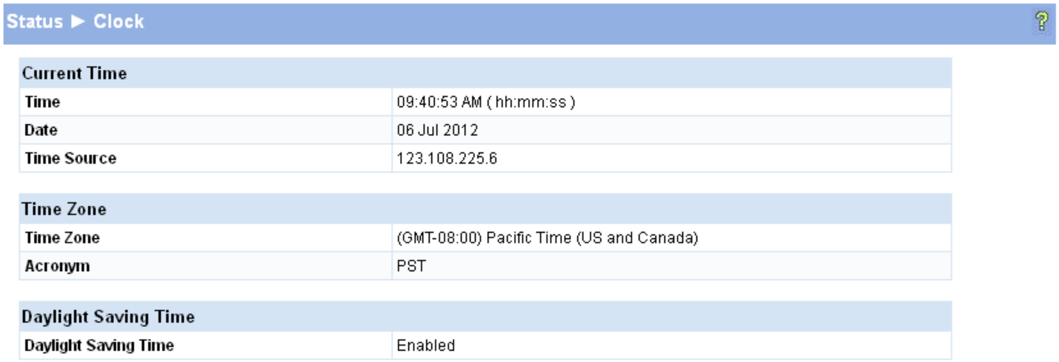
For instructions on configuring the active image, see "Dual Image Configuration" on page 10-8.

Clock

The Clock status page displays the current time, time zone, and Daylight Savings Time settings.

To display the Clock page, click **Status > Clock** in the navigation bar.

Figure 2-11. Clock Status Page



Current Time	
Time	09:40:53 AM (hh:mm:ss)
Date	06 Jul 2012
Time Source	123.108.225.6

Time Zone	
Time Zone	(GMT-08:00) Pacific Time (US and Canada)
Acronym	PST

Daylight Saving Time	
Daylight Saving Time	Enabled

Table 2-11. Clock Status Fields

Field	Description
Current Time	
Time	The current time. This value is determined by an SNTP server. When SNTP is disabled, the system time increments from 00:00:00, 1 Jan 1970, which is set at bootup.
Date	The current date.
Time Source	Source from which the time and date is obtained.
Time Zone	
Time Zone	The currently set time zone.
Acronym	The acronym configured on the system for the time zone (e.g., PST, EDT).
Daylight Savings Time	
Daylight Savings Time	Shows whether Daylight Savings Time is enabled and the mode of operation: • **Enabled**—Clock adjustment made for Daylight Savings time. • **Disabled**—No clock adjustment will be made for Daylight Savings time. • **Recurring**—The settings will be in effect for the upcoming period and subsequent years. • **Non-Recurring**—The settings will be in effect for only one period (i.e., they will not carry forward to subsequent years).

For instructions on configuring the system time, see "Simple Network Time Protocol" on page 3-4, "Time Zone" on page 3-6, and "Daylight Saving Time" on page 3-7.

3

Network Setup

You can use the Network Setup pages to configure how a management computer connects to the switch and how the switch connects to a server to synchronize its time.

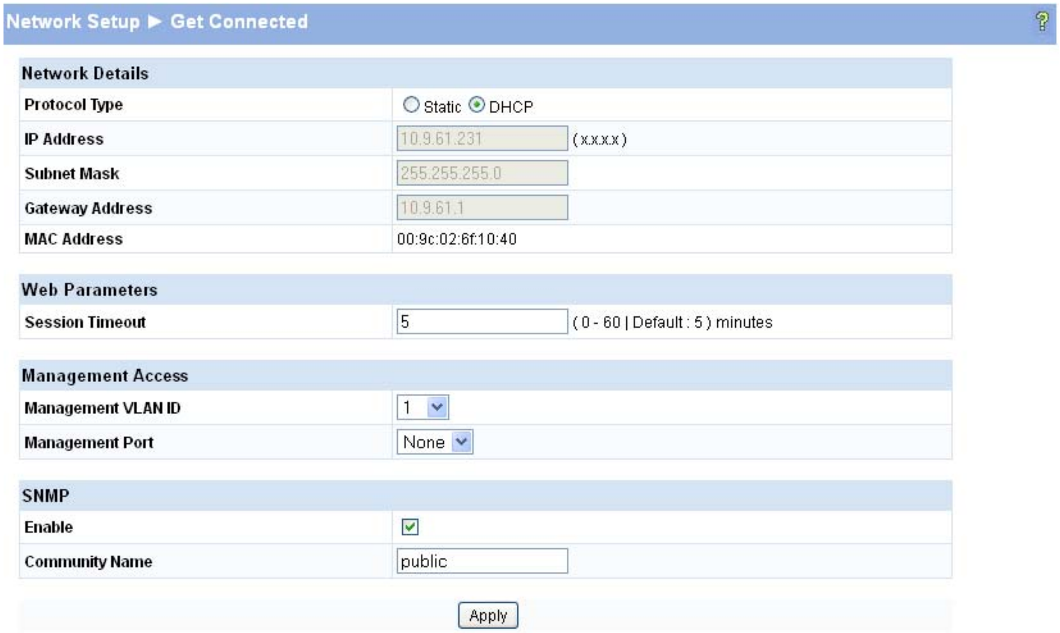
Get Connected

Use the Get Connected page to configure settings for the network interface. The network interface is defined by an IP address, mask, and gateway. Any one of the switch's front-panel ports can be selected as the management port for the network interface. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or forwarded, except that for the management port, the PVID will be the management VLAN.

To display the Get Connected page, click **Network Setup > Get Connected**.

As shown in the example configuration in Figure 3-1, the switch has been configured to acquire its IP address through DHCP. In this example, access to the management software is restricted to members of VLAN 1.

Figure 3-1. Get Connected Page



Network Setup ▶ Get Connected

Network Details	
Protocol Type	○ Static ● DHCP
IP Address	10.9.61.231 (x.x.x.x)
Subnet Mask	255.255.255.0
Gateway Address	10.9.61.1
MAC Address	00:9c:02:6f:10:40
Web Parameters	
Session Timeout	5 (0 - 60 | Default : 5) minutes
Management Access	
Management VLAN ID	1
Management Port	None
SNMP	
Enable	☑
Community Name	public

Table 3-1. Get Connected Fields

Field	Description
Network Details	
Protocol Type	Select the type of network connection: • **Static:** Select this option to enable the IP address, mask, and gateway fields for data entry. • **DHCP:** Select this option to enable the switch to obtain IP information from a DHCP server on the network. If the DHCP server responds, then that IP address will be used. Otherwise if DHCP is enabled but the DHCP server does not respond, the fall-back IP address will be used. Only user-configured, static IP address is saved to flash. **CAUTION:** Changing the protocol type or IP address discontinues the current connection; you can log on again using the new IP information.
IP Address	The IPv4 address to be used. The default IP address is 192.168.2.10.
Subnet Mask	The IPv4 subnet address to be used. The default IP subnet address is 255.255.255.0.
Gateway Address	The IPv4 gateway address to be used. When in doubt, set this to be the same as the default gateway address used by your PC.
MAC Address	The burned-in universally administered MAC address of this switch.
Web Parameters	
Session Timeout	Specify the amount of time in minutes that a connection to the Web interface remains active, assuming no user activity. To keep the connection active regardless of user activity, set this value to 0. **CAUTION:** When a session window is closed without logging out, the server connection remain open until the session timeout. When the session timeout is set to 0, closing a session window without logging out keeps the session open at the server indefinitely. In such cases, you may fail to connect after maximum sessions are left open indefinitely.
Management Access	
Management VLAN ID	Access to the management software is controlled by the assignment of a VLAN ID. By default, the management VLAN ID is 1. The allowed range is 2 to 4094. All ports are members of VLAN 1 by default; the administrator may want to create a different VLAN to assign as the management VLAN and associate it to a management port. Any change in configured management VLAN ID may cause disruption in connectivity when the network protocol is configured to be DHCP; this is because the switch acquires a new IP Address because the management subnet has changed. To re-connect to the switch, the user must determine the new IP address assigned by the DHCP server.
Management Port	Access to the management software also requires the selection of a management port. Any one physical port can be selected as the management port. The selected management port is auto-configured to be an untagged 'Management VLAN' member and it is excluded from any untagged VLANs. When the switch boots with default configuration, any port can be used as management port and it is displayed as 'None'. Configure a management port to ensure a port always remains an untagged member in configured management VLAN to provide management connectivity in case of an accidental change in VLAN membership. **Note:** All ports that are members of VLAN 1 (the management VLAN) will have management access to the switch even though the management port is configured as port 1.
SNMP	
Enable	Enable or disable Simple Network Management Protocol (SNMP). If enabled, the administrator can view switch data using an SNMPv1/v2c manager. The switch supports read-only access to a limited set of MIBs.

Field	Description
Community Name	Specify a community name or use the default name, *public*. The switch supports the following MIBs: • BRIDGE-MIB (IEEE 802.1Q) • LLDP-MIB (IEEE 802.3AB) • EtherLike-MIB • IF-MIB • RFC1213-MIB • RMON-MIB (RMON History as in v1)

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Note

A power cycle does not reset the IP address to its factory-default value. A manual reset to factory defaults is the only way to access a switch without the IP address.

Simple Network Time Protocol

The HP 1810 series switch software supports the Simple Network Time Protocol (SNTP). SNTP ensures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The software operates only as an SNTP client and cannot provide time services to other systems.

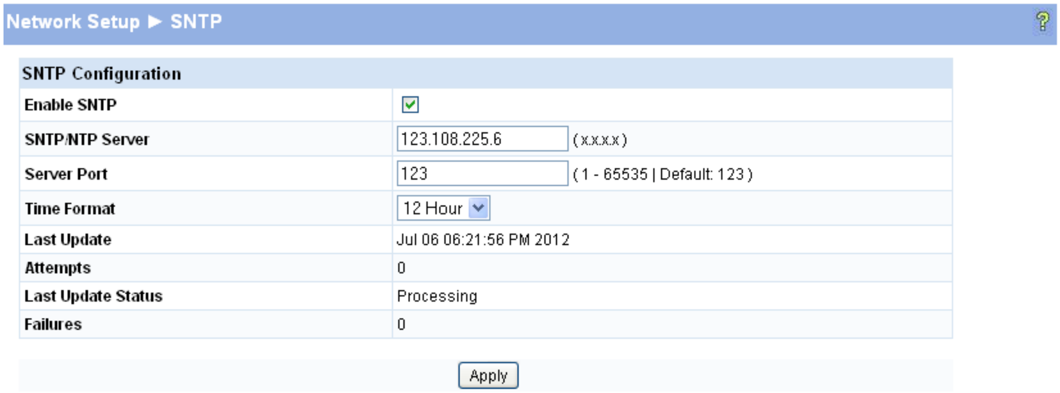
The SNTP server port of 123 is used by default. A log message is generated when the configured SNTP server is unreachable.

Note

SNTP acquires the Coordinated Universal Time (UTC) from an SNTP server. Configure the Time Zone (see page 3-6) and Daylight Saving Time (see page 3-7) to configure the offsets for your local time zone.

To display the SNTP page, click **Network Setup > SNTP** in the navigation pane.

Figure 3-2. SNTP Page



Network Setup ▶ SNTP

SNTP Configuration

Enable SNTP	☑
SNTP/NTP Server	123.108.225.6 (x.x.x.x)
Server Port	123 (1 - 65535 | Default: 123)
Time Format	12 Hour
Last Update	Jul 06 06:21:56 PM 2012
Attempts	0
Last Update Status	Processing
Failures	0

Table 3-2. SNTP Fields

Field	Description
Enable SNTP	Select to enable SNTP client mode. Clear to disable SNTP client mode. When disabled, the system time increments from 00:00:00, 1 Jan 1970, which is set at bootup.
SNTP/NTP Server	Specify the IP address of the SNTP server to send requests to.
Server Port	Specify the server's UDP port to listen for responses/broadcasts (range 1–65535, default = 123).
Time Format	Select either 24-hour (“military” time) format or 12-hour (standard) format.
Last Update	Last update date and time (UTC) assigned by this server.
Attempts	The number of requests made to the SNTP sever since the switch was rebooted.
Last Update Status	The status of the last update request to the SNTP server.
Failures	The number of failed SNTP requests made to this server since last reboot.

- Click **Apply** to save any changes for the current boot session; the changes take effect immediately.
- Click the **Refresh** link above the page to re-display the page with current settings from the switch.

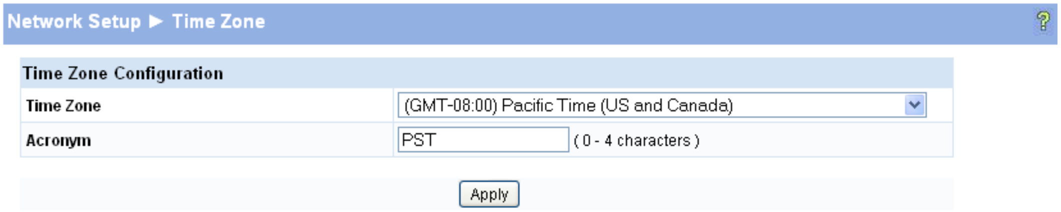
To view a summary of clock information, click **Status > Clock** in the navigation pane.

Time Zone

The Time Zone page is used to configure your local time zone. The switch must be configured to acquire the time from an SNTP server. An acronym can also be assigned to a selected time zone. No time zone is configured by default.

To display the Time Zone page, click **Network Setup > Time Zone** in the navigation pane.

Figure 3-3. Time Zone Page



Network Setup ▶ Time Zone

Time Zone Configuration

Time Zone	(GMT-08:00) Pacific Time (US and Canada)
Acronym	PST (0 - 4 characters)

Table 3-3. Time Zone Fields

Field	Description
Time Zone	Select the time zone for your location.
Acronym	Specify an acronym for the time zone.

- Click **Apply** to save any the changes for the current boot session; the changes take effect immediately.
- Click the **Refresh** link above the page to re-display the page with current settings from the switch.

To view a summary of clock and time zone information, click **Status > Clock** in the navigation pane.

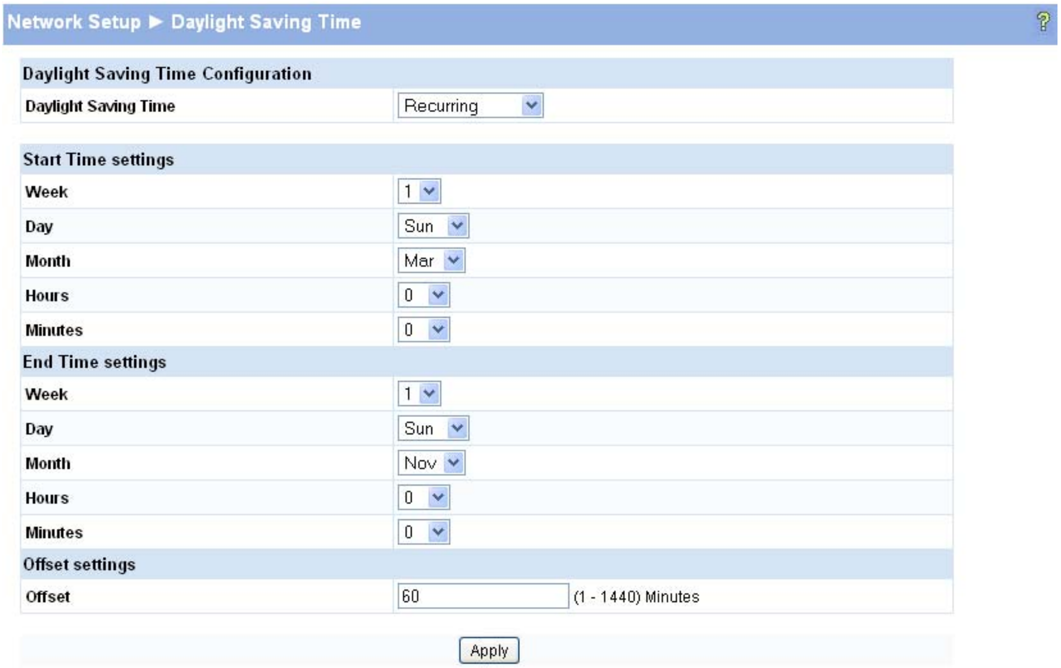
Daylight Saving Time

The Daylight Saving Time page is used to configure if and when Daylight Saving Time (DST) occurs for your time zone. When configured, the system time will adjust automatically during Daylight Saving Time.

To display the Daylight Saving Time page, click **Network Setup > Daylight Saving Time** in the navigation pane.

The page displays differently depending on the mode selected in the Daylight Saving Time field. In the following figure, the mode is set to *Recurring*.

Figure 3-4. Daylight Saving Time Page



Network Setup ► Daylight Saving Time

Daylight Saving Time Configuration	
Daylight Saving Time	Recurring
Start Time settings	
Week	1
Day	Sun
Month	Mar
Hours	0
Minutes	0
End Time settings	
Week	1
Day	Sun
Month	Nov
Hours	0
Minutes	0
Offset settings	
Offset	60 (1 - 1440) Minutes

Table 3-4. Daylight Saving Time Fields

Field	Description
Daylight Saving Time	Select how DST will operate: • **Disabled**—No clock adjustment will be made for DST. • **Recurring**—The settings will be in effect for the upcoming period and subsequent years. • **Non-Recurring**—The settings will be in effect for only one period (i.e., they will not carry forward to subsequent years).
Start Time settings / End Time settings	Set the following to indicate when the change to DST occurs and when it ends. When *Recurring* is selected as the DST mode, the following fields display: • **Week**—Set the week of the month, from 1 to 5, when the change to/from DST occurs. • **Day**—Set the day of the week when the change to/from DST occurs. • **Month**—Set the month when the change to/from DST occurs. • **Hours**—Set the hour of the day when the change to/from DST occurs. • **Minutes**—Set the minutes in the hour when the change to/from DST occurs. When *Non-Recurring* is selected as the DST mode, the following fields display: • **Month**—Set the month when the change to/from DST occurs. • **Date**—Set the day of the month when the change to/from DST occurs. • **Year**—Set the year in which these settings will take effect. • **Hours**—Set the hour of the day when the change to/from DST occurs. • **Minutes**—Set the minutes in the hour when the change to/from DST occurs.
Offset	Specify the time amount of time in minutes to advance the clock during DST.

- Click **Apply** to save any the changes for the current boot session; the changes take effect immediately.

- Click the **Refresh** link above the page to re-display the page with current settings from the switch.

To view a summary of clock and DST information, click **Status > Clock** in the navigation pane.

4

Switching Pages

You can use the Switching Pages to configure port operation and capabilities.

Port Configuration

Use the Port Configuration page to view and configure the Admin mode and link speed setting for each port on the switch. It is also used to display the link status and physical type of each switch port.

The Admin mode is enabled by default and the default link speed is set to auto so that the duplex mode and speed is set by the auto-negotiation process, and the port's maximum capability (full duplex and 1000 Mbps in the case of Gigabit ports) is advertised.

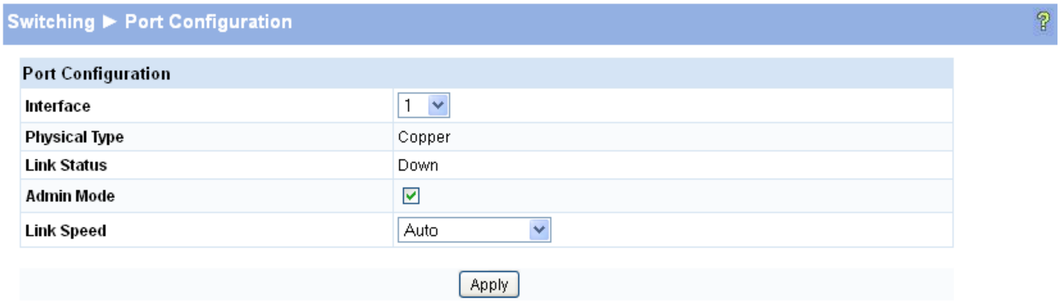
When the mini GBIC fiber transceivers are used, the link speed can be configured as 100/1000Mbps Full-Duplex depending on the transceiver capability.

Auto Detect and Configure Fiber Modules

The auto detect and configure feature detects the type of fiber module inserted in a fiber port and automatically configures it with the appropriate settings. When a fiber module is inserted or changed, the link speed menu shows the available speed options.

To display the Port Configuration page, click **Switching > Port Configuration** in the navigation pane.

Figure 4-1. Port Configuration Page



Port Configuration	
Interface	1
Physical Type	Copper
Link Status	Down
Admin Mode	☑
Link Speed	Auto

Note The display and the content of this page changes based on the physical port selected. For example, if the selected port is an optional copper/fiber port and fiber is being used, then the Link Speed selections will display only valid options for that port.

Table 4-1. Port Configuration Fields

Field	Description
Interface	Select the interface to configure.
Physical Type	Describes the port type (i.e., Copper or Fiber).
Link Status	Displays **Up** or **Down** to indicate operational status.
Admin Mode	Enable access to the port on the network. Clear to disable the port.
Link Speed	Configure the duplex mode and transmission rate for the selected port. (These options may change depending on the port type.) • **Auto**—The rates and duplex mode will be auto-negotiated. • **10HDX**—10Mbps, half-duplex • **100HDX**—100Mbps, half-duplex • **10FDX**—10Mbps, full-duplex • **100FDX**—100Mbps, full-duplex • **1000FDX**—1000Mbps, full duplex (for fiber ports) **Note:** The port's maximum capability is advertised.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

To view a summary of port information, click **Status > Port Summary** in the navigation pane.

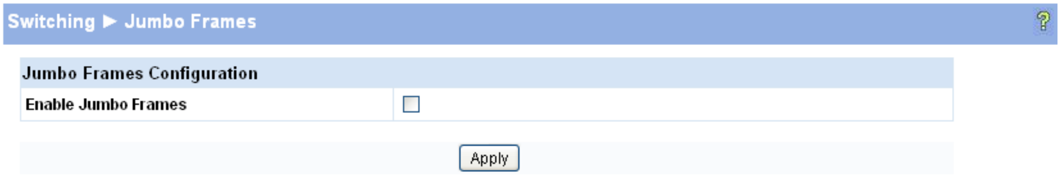
Jumbo Frames

Use the Jumbo Frames page to enable the switch to forward jumbo Ethernet frames. The jumbo frames feature extends the standard Ethernet Maximum Transmission Unit (MTU) from 1518 bytes (1522 bytes with a VLAN header) to 9216 bytes. If it is enabled, any device connecting to the same broadcast domain should also support jumbo frames.

This feature is disabled by default.

To display the Jumbo Frames page, click **Switching > Jumbo Frames** in the navigation pane.

Figure 4-2. Jumbo Frames Page



Jumbo Frames Configuration

Enable Jumbo Frames	□

Table 4-2. Jumbo Frames Fields

Field	Description
Enable Jumbo Frames	Enable the switch to forward jumbo frames up to 9216 bytes.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Port Mirroring

Port mirroring sends a copy of all packets sent and/or received on one port (the source port) to another port (the destination port) for monitoring and analysis by an external network analyzer. Multiple switch ports can be configured as source ports, with each port mirrored to the same destination. You can also mirror the internal CPU traffic to an external port for debugging the CPU. No destination port is defined by default. In its default state, the destination port does not participate in traffic forwarding, and it cannot be configured to participate in VLANs.

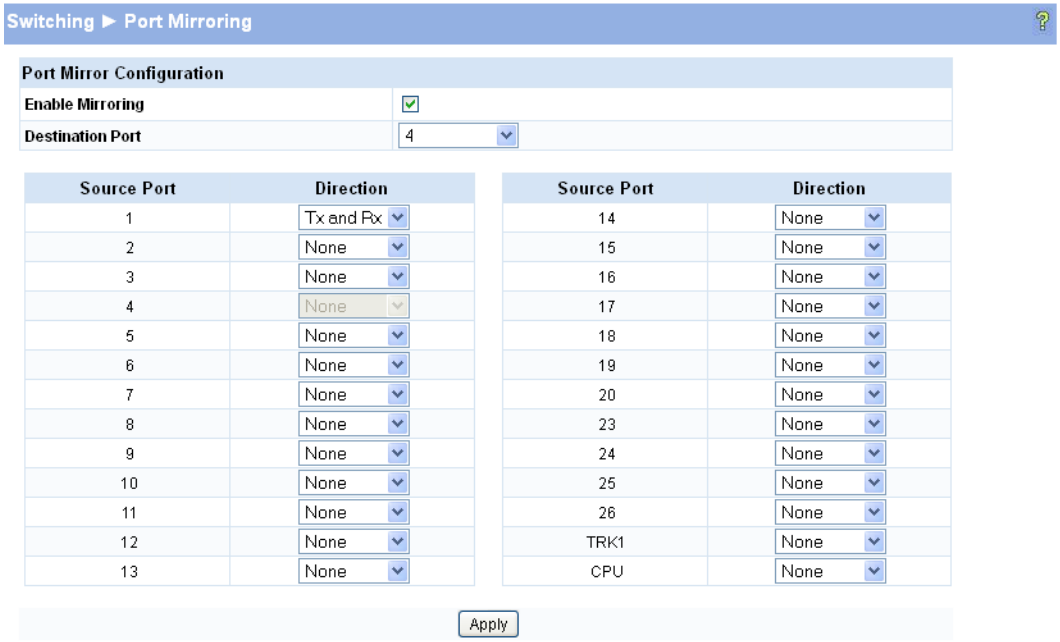
Caution

- When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.
- While a port is used as the destination port for mirrored data, the port cannot be used for any other purpose; the port will not receive and forward traffic.

To display the Port Mirroring page, click **Switching > Port Mirroring** in the navigation pane.

In the example configuration in Figure 4-3, port mirroring is configured to mirror TX and RX packets on Source Port 1 to Destination Port 4.

Figure 4-3. Port Mirroring Page



Port Mirror Configuration

Enable Mirroring	☑
Destination Port	4

Source Port	Direction	Source Port	Direction
1	Tx and Rx	14	None
2	None	15	None
3	None	16	None
4	None	17	None
5	None	18	None
6	None	19	None
7	None	20	None
8	None	23	None
9	None	24	None
10	None	25	None
11	None	26	None
12	None	TRK1	None
13	None	CPU	None

Table 4-3. Port Mirroring Fields

Field	Description
Enable Mirroring	Enable port mirroring capability globally on the switch. Clear to disable the feature.
Destination Port	Select the port to which packets will be mirrored.
Source Port Direction	For each source port you want to mirror to the destination port, select the direction of the packets to be mirrored: • **Tx and Rx**— All packets transmitted and received on the source port are mirrored. • **Rx**— Only packets received on the source port are mirrored. • **Tx**— Only packets transmitted on the source port are mirrored. • **None**— No packets are mirrored from this port (default). The port selected as the Destination Port is greyed-out and unavailable for selection. Ports that are included as part of a trunk cannot be selected individually as source ports, but trunks can be selected as source ports. **Note:** The Source Port *CPU* can be mirrored to an external port to debug traffic to and from the CPU.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Flow Control

When a port becomes oversubscribed, it may begin dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, a lower-speed switch can communicate with a higher-speed switch by requesting that the higher-speed switch refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

Note

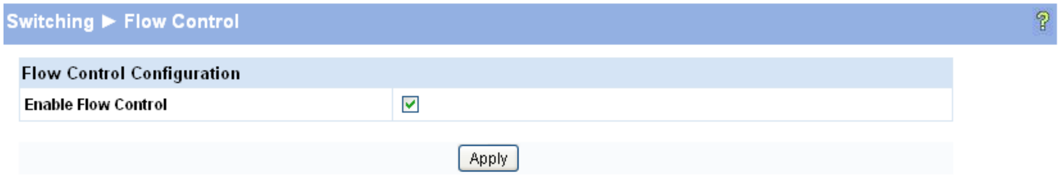
Flow control works well when the Link Speed is auto-negotiated.

Use the Flow Control page to enable or disable this functionality. It is disabled by default and can be configured globally across all the ports.

To display the Flow Control page, click **Switching > Flow Control** in the navigation pane.

As shown in the example configuration in Figure 4-4, flow control is enabled globally, which would enable flow control on all the ports in the switch.

Figure 4-4. Flow Control Page



Flow Control Configuration

Enable Flow Control	☑

Table 4-4. Flow Control Fields

Field	Description
Enable Flow Control	Enable flow control on the switch. Clear to disable the feature.

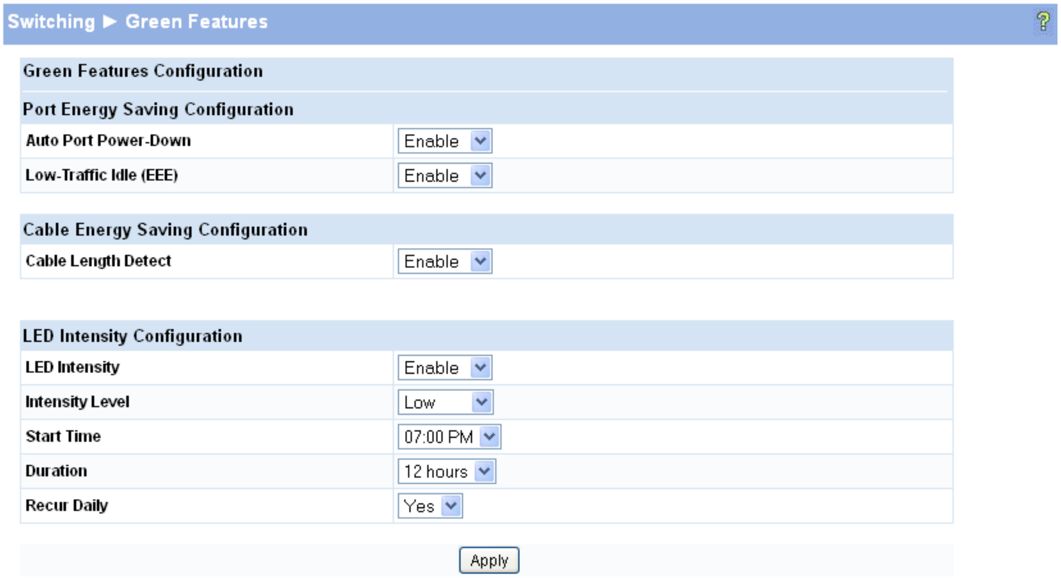
Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Green Features

The switch software allows the user to enable or disable port, cable, and LED energy saving features that consume less power than the normal high-performance mode.

To display the Green Features configuration page, click **Switching > Green Features** in the navigation pane.

Figure 4-5. Green Features



Switching ► Green Features

Green Features Configuration

Port Energy Saving Configuration

Auto Port Power-Down	Enable
Low-Traffic Idle (EEE)	Enable

Cable Energy Saving Configuration

Cable Length Detect	Enable

LED Intensity Configuration

LED Intensity	Enable
Intensity Level	Low
Start Time	07:00 PM
Duration	12 hours
Recur Daily	Yes

Table 4-5. Green Features Configuration Fields

Field	Description
Port Energy Saving Configuration	
Auto Port Power-Down	Enable power save mode when there is no link. This feature is disabled by default.
Low-Traffic Idle (EEE)	EEE (Energy Efficient Ethernet) is designed to save power by turning off network ports that are not passing traffic. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps Full Duplex or 1 Gbps (1000 Mbps) Full Duplex. Valid values are Disable and Enable. This feature is disabled by default.
Cable Energy Saving Configuration	
Cable Length Detect	Enable port power consumption based upon the cable length such that shorter cables use less power. This feature is disabled by default.
LED intensity Configuration	
LED Intensity	Enable LED intensity control globally on all ports.
Intensity Level	Sets the desired LED intensity level. Valid values are High, Medium, Low, and Off. Default value is Off.
Start Time	Specifies the time of day when the configured LED intensity level is activated. Valid values are any hour or half-hour from midnight (12:00 AM) through 11:30 PM. Default value is 7:00 PM.
Duration	Specifies the number of hours the configured LED Intensity level is in effect. Valid values are in the range of 1 hour to 24 hours. Default value is 12 hours.
Recur Daily	Specifies whether the LED intensity settings are in effect one time only, or daily. Set to Yes to repeat the configured LED Intensity level daily. Valid values are Yes and No. Default value is Yes.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Loop Protection

Loops in a network can consume switch resources and degrade performance. Detecting loops manually can be very cumbersome and time consuming. The HP 1810 series switch software provides an automatic Loop Protection feature.

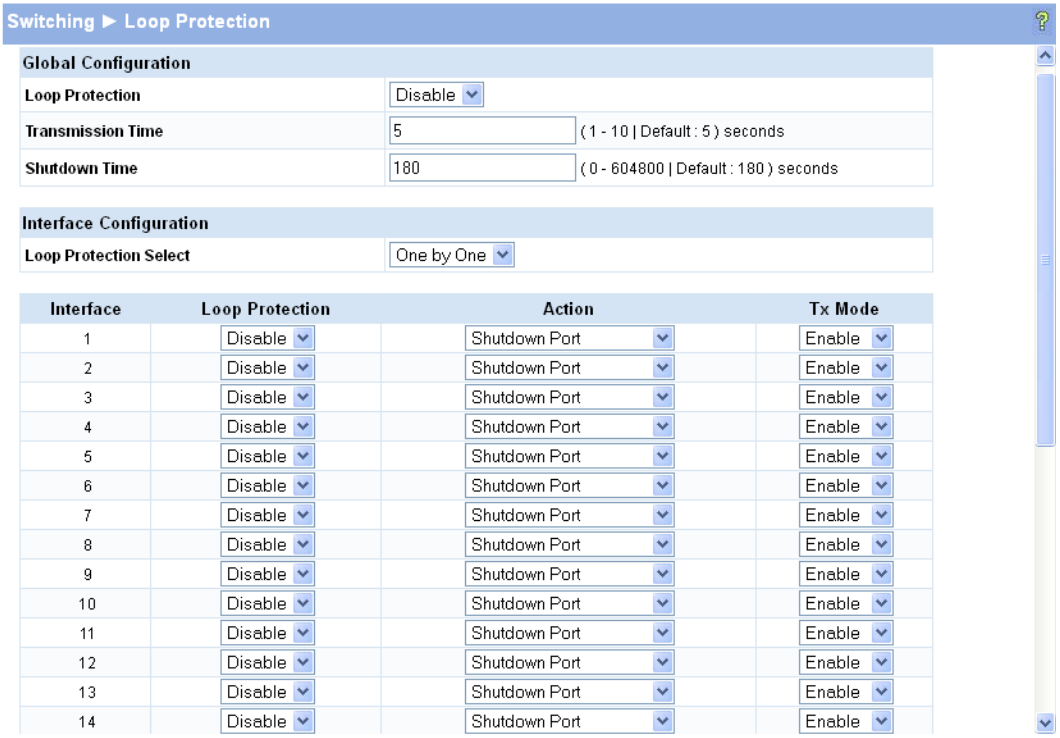
Loop Protection may be enabled or disabled globally and on a port-by-port basis. When enabled globally, the software sends loop protection packets to a reserved layer 2 multicast destination address on all the ports on which the feature is enabled. Transmission of the packet can be disabled selectively on certain ports, even when Loop Protection is enabled.

If this multicast packet comes back to the switch with any of the ports' MAC addresses as the source, the switch determines that a loop has occurred. The port that received the loop protection packet from the switch can be shut down for a configured period, or a log entry can be made.

Ports on which Loop Protection is disabled drop the loop protection packets silently.

To display the Loop Protection configuration page, click **Switching > Loop Protection** in the navigation pane.

Figure 4-6. Loop Protection



Switching ▶ Loop Protection

Global Configuration	
Loop Protection	Disable
Transmission Time	5 (1 - 10 | Default : 5) seconds
Shutdown Time	180 (0 - 604800 | Default : 180) seconds

Interface Configuration	
Loop Protection Select	One by One

Interface	Loop Protection	Action	Tx Mode
1	Disable	Shutdown Port	Enable
2	Disable	Shutdown Port	Enable
3	Disable	Shutdown Port	Enable
4	Disable	Shutdown Port	Enable
5	Disable	Shutdown Port	Enable
6	Disable	Shutdown Port	Enable
7	Disable	Shutdown Port	Enable
8	Disable	Shutdown Port	Enable
9	Disable	Shutdown Port	Enable
10	Disable	Shutdown Port	Enable
11	Disable	Shutdown Port	Enable
12	Disable	Shutdown Port	Enable
13	Disable	Shutdown Port	Enable
14	Disable	Shutdown Port	Enable

Table 4-6. Loop Protection Fields“

Field	Description
Loop Protection	Enable this feature globally.
Transmission Time	Enter the time interval, in seconds, between sending Loop Protection packets.
Shutdown Time	Set the number of seconds that a port remains shut down if a loop has been detected on the port.
Loop Protection Select	Select how you want to configure Loop Protection: • **All**—Enables all interfaces with Loop Protection. • **One by One**—Enables you to configure Loop Protection on ports individually (default). • **None**—Disables Loop Protection on all interfaces.
Interface / Loop Protection	Select **Enable** for each port on which you want to use this feature.
Action	If Loop Protection is enabled on a port, select one of the following actions to occur when a loop is detected: • **Log**—The event is logged and the port remains operational. • **Shutdown port**—The port is shut down for the configured period. • **Log and Shutdown Port**—The event is logged and the port it shut down for the configured period.
Tx Mode	If Loop Protection is enabled on a port, select **Enable** to allow the port to forward packets to the multicast destination MAC address designated for the Loop Protection feature. Select **Disable** to disallow forwarding.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

To view a summary of how this feature is configured on each port, click **Status > Loop Protection** in the navigation pane.

Spanning Tree

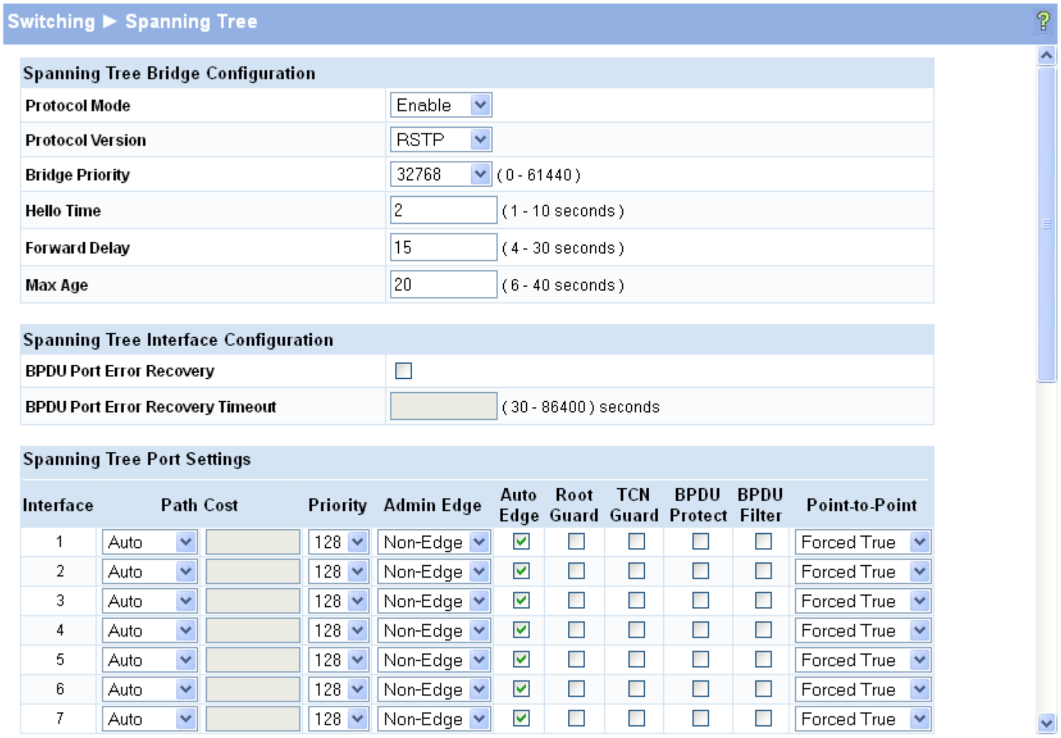
The Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) reduces the convergence time for network topology changes to about 3-5 seconds from the 30 seconds or more for the IEEE 802.1D STP standard.

RSTP is intended as a complete replacement for STP, but can still interoperate with switches running the STP protocol by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

HP 1810 series switches support the Spanning Tree versions IEEE 802.1D STP, and 802.1w RSTP in conformance with the IEEE802.1Q 2005.

To display the Spanning Tree configuration page, click **Switching > Spanning Tree** in the navigation pane.

Figure 4-7. Spanning Tree



Switching ▶ Spanning Tree

Spanning Tree Bridge Configuration

Protocol Mode	Enable	
Protocol Version	RSTP	
Bridge Priority	32768	(0 - 61440)
Hello Time	2	(1 - 10 seconds)
Forward Delay	15	(4 - 30 seconds)
Max Age	20	(6 - 40 seconds)

Spanning Tree Interface Configuration

BPDU Port Error Recovery	□	
BPDU Port Error Recovery Timeout		(30 - 86400) seconds

Spanning Tree Port Settings

Interface	Path Cost		Priority	Admin Edge	Auto Edge	Root Guard	TCN Guard	BPDU Protect	BPDU Filter	Point-to-Point
1	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
2	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
3	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
4	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
5	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
6	Auto		128	Non-Edge	☑	□	□	□	□	Forced True
7	Auto		128	Non-Edge	☑	□	□	□	□	Forced True

Table 4-7. Spanning Tree Fields

Field	Description
Spanning Tree Bridge Configuration	
Protocol Mode	Enable the Spanning Tree protocol mode globally. This feature is disabled by default.
Protocol Version	Specify the protocol, RSTP or STP. RSTP is set by default.
Bridge Priority	Specify an STP/RSTP bridge priority value between 0–61440. The default is 32768.
Hello Time	Interval between periodic transmissions of STP BPDUs by designated ports. The default is 2 seconds.
Forward Delay	Delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The default is 15 seconds.

Field	Description
Max Age	Number of seconds until the BPDU information is considered to be aged out or invalid. This value must be <= (FwdDelay-1)*2 and >= (HelloTime+1)*2. The default is 20 seconds.
Spanning Tree Interface Configuration	
BPDU Port Error Recovery	Set the port to recover from an error-disabled state. If recovery is not enabled, a port has to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
BPDU Port Error Recovery Timeout	Time after which a port in the error-disabled state can be enabled. This value is also applicable on the per-port BPDU Guard operations.
Spanning Tree Port Settings	
Interface	List of all physical ports and trunk interfaces configured on the system.
Path Cost	The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Specify Auto or assign a value between 1-200000000. The default is Auto where the path cost is set using the 802.1D recommended values.
Priority	Specify a value between 0-240 in increments of 16 to control the priority of ports with identical port costs. The default is 128; 64 for trunk ports.
Admin Edge	Configure the port to act as a non-edge or edge port for Spanning Tree. The default is non-edge.
Auto Edge	Enable automatic edge port detection for the port.
Root Guard	When root guard is enabled on a port, that port cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an “alternate” port role and enters a blocking state if it receives superior STP BPDUs. Select this option to enable root guard for the port. It is not selected by default.
TCN Guard	With TCN guard enabled, a port does not propagate received topology change notifications and topology changes to other ports. Select this option to enable TCN guard for the port. It is not selected by default.
BPDU Protect	When an STP BPDU is received on a port that has BPDU protection enabled, the port disables itself. Select this option to enable BPDU protection for the port. It is not selected by default.
BPDU Filter	With BPDU filtering enabled, the port does not participate in Spanning Tree, and the port remains in the forwarding state. Select this option to enable BPDU filtering for the port. It is not selected by default.
Point-to-Point	This parameter informs the switch whether the port connects to a single device or to a shared medium with multiple devices. A point-to-point link has only one device at the far end. This can be automatically determined, or forced either true or false. Valid values are Forced True, Forced False, and Auto. Default value is Forced True.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

5

Security

The HP 1810 series switch software includes a robust set of built-in denial-of-service (DoS) and storm-control protections, and allows configuring secure HTTP (HTTPS) management sessions.

Advanced Security

The HP 1810 series switch software provides the following built-in security features:

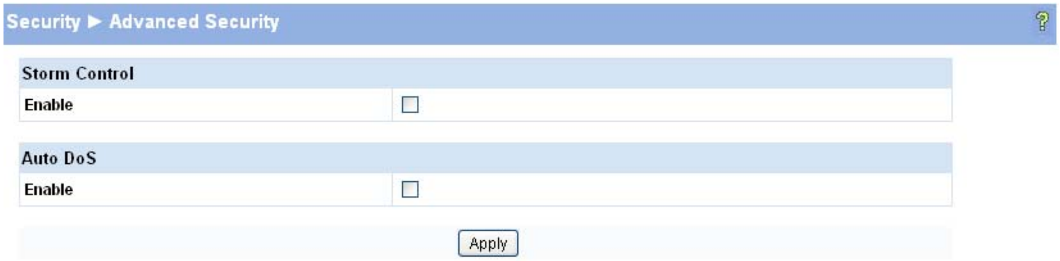
- Storm Control—This feature protects against condition where incoming packets flood the LAN, causing network performance degradation. The software includes Storm Control protection for unicast, broadcast, and multicast traffic. The traffic is dropped if the rate of incoming traffic on an interface increases beyond the threshold of 64K pps for 1810-24G/1810-8G or 4K pps for 1810-24/1810-8.
- Auto Denial-of-Service (DoS) protections—A DoS attack is an attempt to saturate the switch with external communication requests to prevent the switch from performing efficiently, or at all. You can enable Auto DoS protection that prevents common types of DoS attacks.

Caution

The DoS feature does not generate any notifications (such as error messages, syslog messages, SNMP traps) if a DoS attack occurs.

To display the Advanced Security page, click **Security > Advanced Security** in the navigation pane.

Figure 5-1. Advanced Security Page



Security ► Advanced Security

Storm Control

Enable □

Auto DoS

Enable □

Table 5-1. Advanced Security Fields

Field	Description
Storm Control	Activate storm control protection for broadcast and multicast globally in the system. The default threshold is 64K pps on the 1810 Gigabit switches and 4K pps on the Fast Ethernet switches. Clear to not use the Storm Control feature.
Auto DoS	Enable denial of service attack protection, or clear to disable DoS protection. It is disabled by default.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Secure Connection

The HP 1810 series switch software allows the administrator to enable or disable Secure HTTP protocol (HTTPS). When enabled, the administrator can establish a secure connection with the switch using the Secure Sockets Layer (SSL) protocol. Secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdropping and man-in-the-middle attacks. The HP 1810 series switch software supports SSL version 3.0.

SSL enables the switch to generate and store a certificate that functions as a digital passport, enabling client Web browsers to verify the identity of the switch before accessing it.

Note

SSL is described in client/server terminology, where the SSL-enabled switch is the server and a Web browser is the client.

The certificate provides information to the browser such as the server name, the trusted certificate authority (CA) that issued the certificate, the date it was issued, and the switch's public key.

The browser and server use this information to negotiate a secure connection in the following manner:

- The browser verifies the certificate authority's authenticity by checking it against its own list of CAs. (Web browsers such as Microsoft Internet Explorer and Mozilla Firefox maintain data on trusted CAs.)
- After validating the CA, the browser and switch negotiate the highest level of security available to both. The browser uses the public key to encrypt a random number and send it to the switch. The switch uses a private key stored in memory (not advertised on the certificate) to decrypt it. From this process, the browser and switch determine an algorithm for encrypting and decrypting all further communication during the HTTPS session.

To enable secure HTTPS connections via SSL, the HTTPS Admin mode must be enabled on the switch, and the Web server must have a public key certificate. The switch can generate its own certificates, or you can generate these externally and download them to the switch.

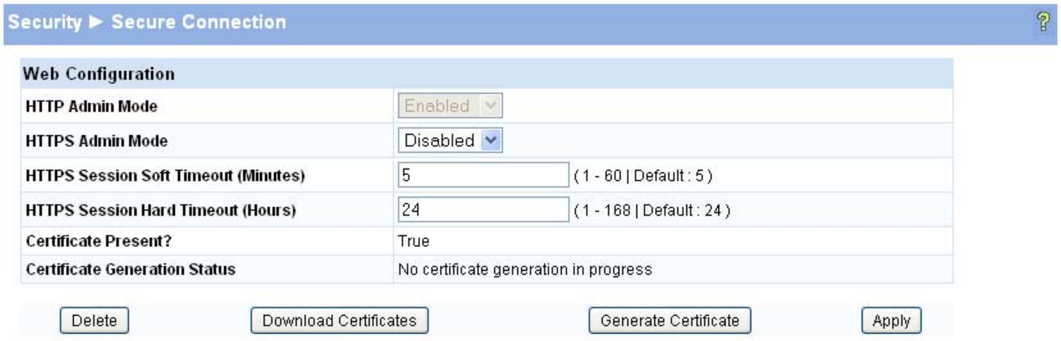
- Certificates generated by the switch are *self-signed*; that is., the validity of the information provided in the certificate is attested to by the switch itself.
- Downloaded certificates can also be self-signed (by a server other than the switch), or they can be *root certificates*. A root certificate has been digitally signed by a CA, and is therefore considered to provide a higher level of security.

You can also download the encryption parameter files that provide algorithms for encrypting the key exchanges.

To manage HTTP parameters and certificates, you use both the Secure Connection page and the Update Manager page.

To display the Secure Connection page, click **Security > Secure Connection** in the navigation pane.

Figure 5-2. Secure Connection Page



Web Configuration	
HTTP Admin Mode	Enabled
HTTPS Admin Mode	Disabled
HTTPS Session Soft Timeout (Minutes)	5 (1 - 60 | Default : 5)
HTTPS Session Hard Timeout (Hours)	24 (1 - 168 | Default : 24)
Certificate Present?	True
Certificate Generation Status	No certificate generation in progress

Table 5-2. Secure Connection Fields

Field	Description
HTTP Admin Mode	Enable the Administrative mode of HTTP. This mode can only be disabled when the HTTPS Admin mode is enabled.
HTTPS Admin Mode	Enable secure HTTPS sessions. (Verify that the Certificate Present field is set to *True*.) You can only download SSL certificates when this mode is disabled.
Session Soft Timeout	The number of minutes after which an HTTPS session times-out if there is no user activity.
Session Hard Timeout	The number of minutes after which an HTTPS session times-out, regardless of recent user activity.
Certificate Present?	**True**—A certificate is available for use with HTTPS sessions. **False**—No certificate is available on the switch.
Certificate Generation Status	Indicates that a certificate is being generated or that no certificate generation is in progress.

- If the value of the **Certificate Present?** field is **True**, you can click **Delete** to delete the existing certificate.
- If you click **Download Certificates**, the Update Manager page will be displayed to enable you to download a certificate file to the switch. See "Downloading SSL Certificates and Diffie-Hellman Files" on page 5-4.
- If you click **Generate Certificates**, the switch creates its own self-signed public key certificate. See "Generating Certificates" on page 5-5.
- If you enable or disable HTTPS Admin Mode, or change the timeout settings, click **Apply** to save the changes for the current boot session; the changes take effect immediately.

Note

Download or regenerate a certificate when the previous certificate has expired, or when you have reason to suspect that security has been breached and the certificate has been taken for use by another server.

Downloading SSL Certificates and Diffie-Hellman Files

Use the Update Manager page to download a public key certificate that has been signed by another server, or a root certificate that has been signed by a certificate authority. You can also download Diffie-Hellman (DH) encryption parameter files, which establish the algorithms for encrypting key exchanges.

Before you download a file to the switch, the following conditions must be true:

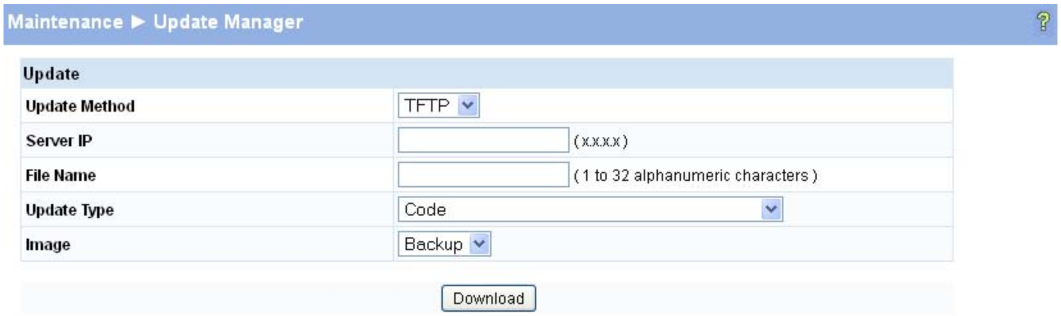
- The file is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the server.

Use the following procedures to download an SSL certificate or DH files.

1. Click **Download Certificates**.

The Update Manager page displays.

Figure 5-3. Using Update Manager to Download Certificates



Maintenance ▶ Update Manager

Update	
Update Method	TFTP
Server IP	(x.x.x.x)
File Name	(1 to 32 alphanumeric characters)
Update Type	Code
Image	Backup

2. Select the protocol to use, based on the server type that the certificate is stored on: **TFTP** or **HTTP**.
3. For an HTTP upload, browse for the file on your local computer or network.

   For a TFTP upload, enter the **Server IP** address, and specify the File Path and **File Name**.
4. From the **Update Type** field on the File Download page, select one of the following:
   - **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded)—An SSL certificate that has been digitally signed by a certificate authority.
   - **SSL Server Certificate PEM File:** SSL Server Certificate File (PEM Encoded)—An SSL certificate that has been signed by another server.
   - **SSL DH Weak Encryption Parameter PEM File** or **SSL DH Strong Encryption Parameter PEM File**—DH certificates provide the algorithms for encrypting key exchanges and are used independent of the certificate. The weak version uses a cipher strength of 512 bits and the strong version uses a cypher strength of 1024 bits. Browser settings determine which DH file parameters are requested at the start of the SSL session.
5. Click **Download**.

   To view that status of the update, you can view the **Status > Log** page.
6. To return to the Secure HTTP Configuration page, click **Security > Secure Connection** in the navigation pane.
7. To enable the HTTPS admin mode, select **Enable** from the **HTTPS Admin Mode** field, and then click **Apply**.

Generating Certificates

To have the switch generate the certificates:

1. Click **Generate Certificates**.

   The page refreshes with the message “Certificate has been generated.”

2. Click **Apply** to complete the process.

   When the process is complete, the page refreshes with the message “No certificate generation in progress,” and the **Certificate Present** field displays as **True**.

When a certificate is present a Delete button appears to enable deleting the certificate.

6

Trunks

Trunks allow for the aggregation of multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing capability. You assign the trunk VLAN membership after a trunk is created.

A trunk interface can be either static or dynamic, but not both.

- Dynamic trunks use the Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them.
- Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports.

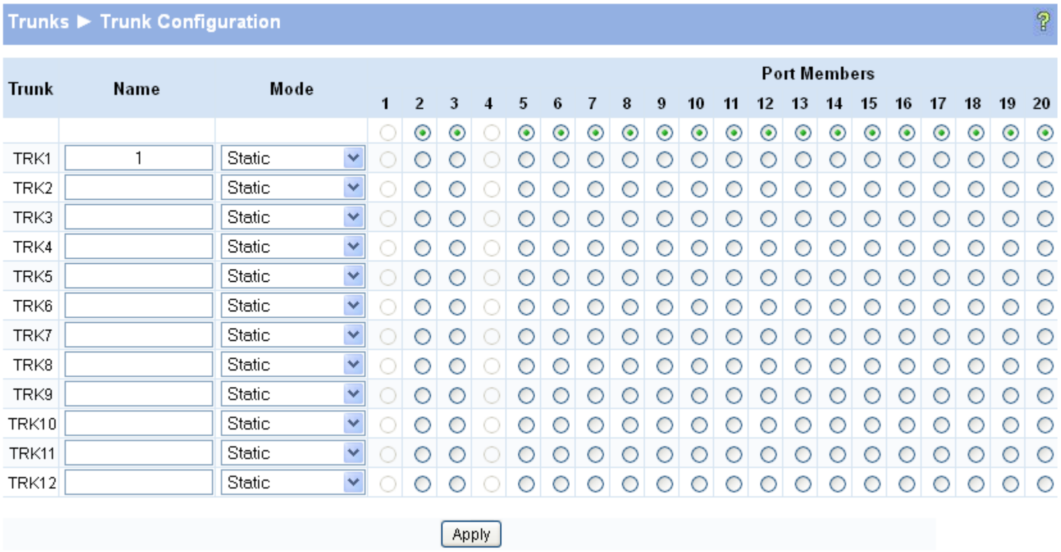
All members of a trunk must be either static or dynamic.

Trunk Configuration and Membership

Link Aggregation/Trunking enables one or more full duplex (FDX) Ethernet links to be aggregated together to form a link aggregation group, such that the networking device can treat this trunk as if it were a single link.

To display the Trunk Configuration page, click **Trunk > Trunk Configuration** in the navigation pane.

Figure 6-1. Trunk Configuration Page



Trunks ▶ Trunk Configuration

Trunk	Name	Mode	Port Members																			
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			○	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
TRK1	1	Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK2		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK3		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK4		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK5		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK6		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK7		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK8		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK9		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK10		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK11		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
TRK12		Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Table 6-1. Trunk Configuration Fields

Field	Description
Trunk	Trunk ID for the settings. "Normal" indicates the port is not part of any trunk.
Name	Trunk name. 1–15 alphanumeric characters.
Mode	Mode configured for the trunk.
Port Members	Select the trunk membership for a port. By default, no ports belong to any trunk. A grayed out port indicates that it has been configured as a member (destination or source port) of the mirroring configuration or that it is in half duplex. The user is not allowed to perform any trunk membership configuration on this port until the port is removed from the mirroring configuration or gets into full duplex mode.

Traffic is distributed among trunk members. All ports in a trunk have the same full duplex speed.

Loop protection is not supported on LACP trunks. Loop protection will be auto disabled if it was previously enabled on static trunk that is now being configured as LACP Active or Passive.

RSTP can be enabled on the Trunks. When RSTP is either enabled or disabled on the Trunks the individual Port members lose their STP configuration and will attain the Trunk's configuration. When ports are removed from a Trunk the port members attain their earlier configured STP states.

An active port added (LACP and Static active members) to a trunk loses port VLAN membership and gets assigned to trunk group VLAN membership. When the port is removed from a trunk it reverts to the default VLAN.

A trunk can be configured in different modes:

- Disabled—Trunk is disabled, no traffic will flow, and LACPDUs will be dropped. The links that form the trunk will not be released.
- Static—Trunk is enabled in static mode. A static trunk interface does not require a partner system to be able to aggregate its member ports. In this mode it does not transmit or process received LACPDUs. Member ports do not transmit LACPDUs and all the LACPDU received are dropped.

- LACP Active—Trunk will be initiated and maintained by the periodic exchanges of LACPDUs.
- LACP Passive—Trunk will only participate if the other end sends LACPDUs (other end is active).

Click **Apply** to save any changes to the currently selected trunk. The changes take effect immediately.

Virtual LAN

On a Layer 2 switch, Virtual LAN (VLAN) support offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. Many reasons exist for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which displays in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

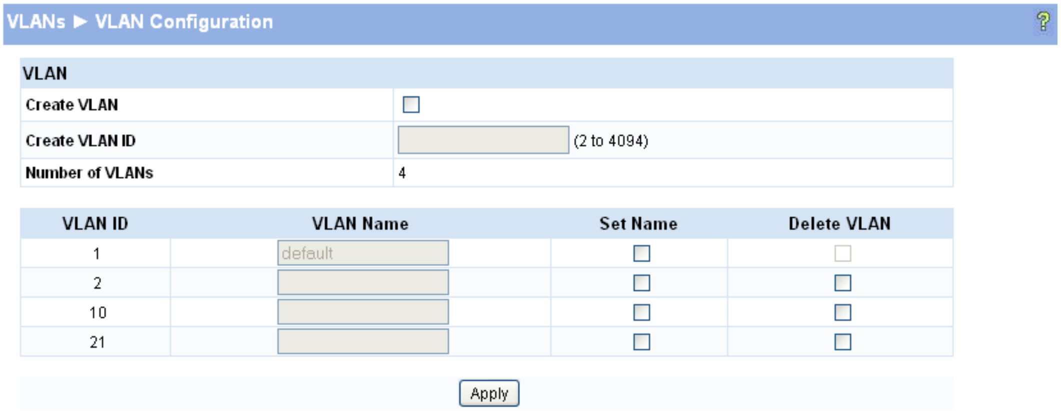
HP 1810 series switches support up to 64 VLANs.

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups. VLAN 1 is the default VLAN of which all ports are members. You can create up to 64 VLANs.

To display the VLAN Configuration page, click **VLANs > VLAN Configuration** in the navigation pane.

Figure 7-1. VLAN Configuration Page



VLAN	
Create VLAN	□
Create VLAN ID	(2 to 4094)
Number of VLANs	4

VLAN ID	VLAN Name	Set Name	Delete VLAN
1	default	□	□
2		□	□
10		□	□
21		□	□

Table 7-1. VLAN Configuration Fields

Field	Description
Create VLAN	Select this box to create a new VLAN.
Create VLAN ID	Specify the numeric VLAN Identifier from 2 to 4094 and click **Apply** to create the VLAN. **Note:** VLAN ID 1 is pre-configured on the switch and is always named "Default." The default VLAN cannot be deleted.
Number of VLANs	The current number of VLANs. Up to 64 VLANs can be created.
VLAN Name **Delete VLAN** **Set Name**	After the VLAN ID has been created using the previously described fields, you can apply a name to it or delete it. • To delete a VLAN, select **Delete VLAN** and click **Apply**. The default VLAN cannot be deleted. • To specify a VLAN name, select **Set Name**, type a name in the VLAN Name field, and click **Apply**. A VLAN name can have up to 32 alphanumeric characters, including spaces.

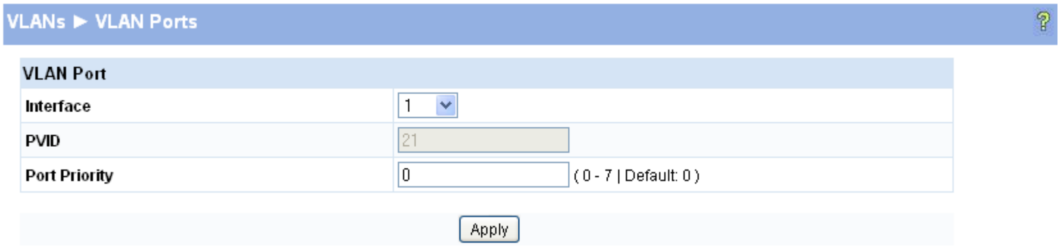
Click **Apply** to save any changes for the currently selected VLAN. The changes take effect immediately.

VLAN Ports

Use the VLAN Ports page to view the Port VLAN ID that a port will assign to untagged frames that it forwards, and to configure the port priority.

To display the VLAN Ports page, click **VLANs > VLAN Ports** in the navigation pane.

Figure 7-2. VLAN Ports Page



VLANs ▶ VLAN Ports

VLAN Port

Interface	1
PVID	21
Port Priority	0 (0 - 7 | Default: 0)

Table 7-2. VLAN Ports Fields

Field	Description
Interface	Select the port on which to configure the VLAN settings.
PVID	The VLAN ID that this port will assign to untagged frames or priority-tagged frames received on this port (range 1–4094, default = 1). The PVID is not user-configurable and always corresponds to VLAN ID of the port's untagged VLAN membership. You assign ports to VLANs on the VLAN Participation / Tagging page. The PVID value displays as *None* if all the VLANs are configured as tagged on this port or if this port is configured as the destination port in a port mirroring configuration.
Port Priority	Specify the default 802.1p priority assigned to untagged packets arriving at the port. A value of 0 indicates the lowest priority, commonly used for routine traffic, and 7 indicates the highest priority, often reserved for application such as voice and video. (0–7, default = 0)

Note

Ingress Filtering is enabled on all ports; therefore, a frame is discarded if the port is not a member of the VLAN that the frame is associated with. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

VLAN Participation / Tagging

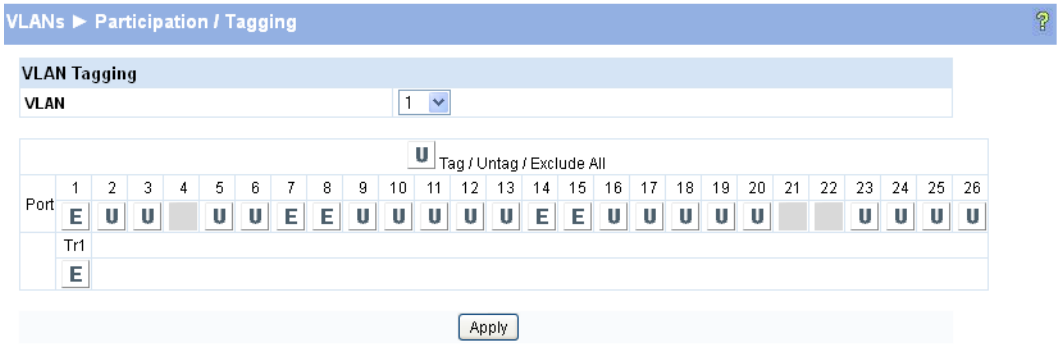
Use this page to include ports or trunks in particular VLANs and to specify the tagging policy for outgoing packets on a port or trunk.

Note

- All ports are members of VLAN1 by default.
- Each port must be a member of at least one VLAN. An error message is displayed if a user attempts to exclude a port from participation in its only VLAN.
- Ports belonging to a trunk cannot be assigned membership in a VLAN, although the trunk itself can be a member of one or more VLANs. When a member port is added to a Trunk, it loses any previous VLAN memberships and acquires those of the trunk. When deleted from a trunk, a port loses the VLAN memberships of the trunk and acquires untagged membership in VLAN 1.

To display the Participation/Tagging page, click **VLANs > Participation / Tagging** in the navigation pane.

Figure 7-3. Participation/Tagging Page



VLAN Tagging

VLAN: 1

U Tag / Untag / Exclude All

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	E	U	U		U	U	E	E	U	U	U	U	U	E	E	U	U	U	U	U			U	U	U	U

Tr1
E

Table 7-3. Participation/Tagging Fields

Field	Description
VLAN	Select the VLAN to configure.
Tag / Untag / Exclude All	For a port or trunk to participate in a VLAN, its tagging policy must be defined. By default, all ports and trunks are configured as untagged members of VLAN1, and are excluded from all other newly created VLANs. You can configure each port individually or use the **Tag / Untag / Exclude All** box to configure all ports at once. Click the box until the appropriate option is displayed: • **E**—exclude from VLAN. • **T**—participate in the selected VLAN and tag all frames. • **U**—participate in the selected VLAN and leave all outgoing frames untagged. Each port can have only one untagged VLAN membership. If a port is an untagged member of a VLAN and a second VLAN is selected for untagged membership, then the first VLAN membership is automatically changed to E (Exclude). • A grayed out box indicates the port is either configured as a member of a trunk or cannot participate in any VLAN
Port	Use the individual port boxes to specify whether a port participates in this VLAN by identifying the tagging policy, or by excluding the port from the VLAN.

Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

8

Link Layer Discovery Protocol (LLDP)

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows stations residing on an IEEE 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

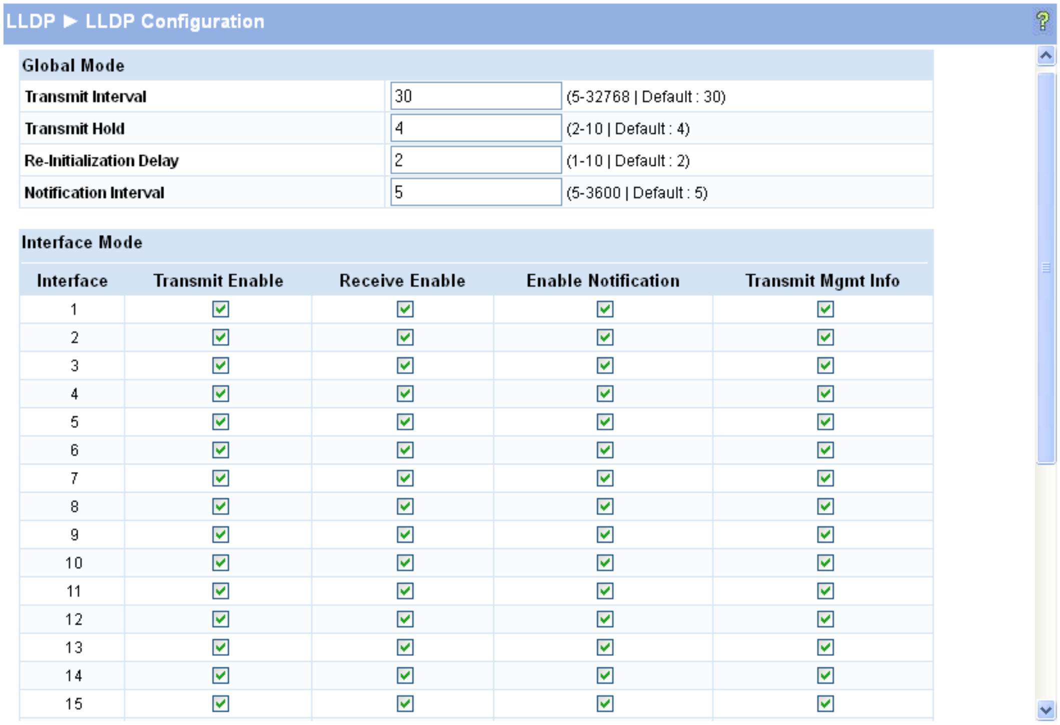
LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are enabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

LLDP Configuration

Use the LLDP Configuration page to specify global LLDP parameters and to configure the protocol on individual ports.

To display the LLDP Configuration page, click **LLDP > LLDP Configuration** in the navigation pane.

Figure 8-1. LLDP Configuration Page



LLDP ▶ LLDP Configuration

Global Mode

Transmit Interval	30	(5-32768 | Default : 30)
Transmit Hold	4	(2-10 | Default : 4)
Re-Initialization Delay	2	(1-10 | Default : 2)
Notification Interval	5	(5-3600 | Default : 5)

Interface Mode

Interface	Transmit Enable	Receive Enable	Enable Notification	Transmit Mgmt Info
1	☑	☑	☑	☑
2	☑	☑	☑	☑
3	☑	☑	☑	☑
4	☑	☑	☑	☑
5	☑	☑	☑	☑
6	☑	☑	☑	☑
7	☑	☑	☑	☑
8	☑	☑	☑	☑
9	☑	☑	☑	☑
10	☑	☑	☑	☑
11	☑	☑	☑	☑
12	☑	☑	☑	☑
13	☑	☑	☑	☑
14	☑	☑	☑	☑
15	☑	☑	☑	☑

Table 8-1. LLDP Configuration Fields

Field	Description
Global Mode	
Transmit Interval	Specify the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768 seconds.
Transmit Hold	Specify the multiplier on the transmit interval to, which is used to compute the TTL (range 2–10, default = 4).
Re-Initialization Delay	Specify the delay before a re-initialization (range 1–10 seconds, default = 2).
Notification Interval	Specify a limit for the transmission of notifications (range 5–3600 seconds, default = 5).
Interface Mode	
Interface	The list of all physical and trunk interfaces on the system.
Transmit Enable	Enable or disable the transmission of LLDP PDUs. The default is enabled.
Receive Enable	Enable or disable the ability of the port to receive LLDP PDUs. The default is enabled.
Enable Notification	Enable to have LLDP generate a log file entry.
Transmit Mgmt Info	Enable or disable the transmission of management information with the LLDP PDUs. The default is enabled.

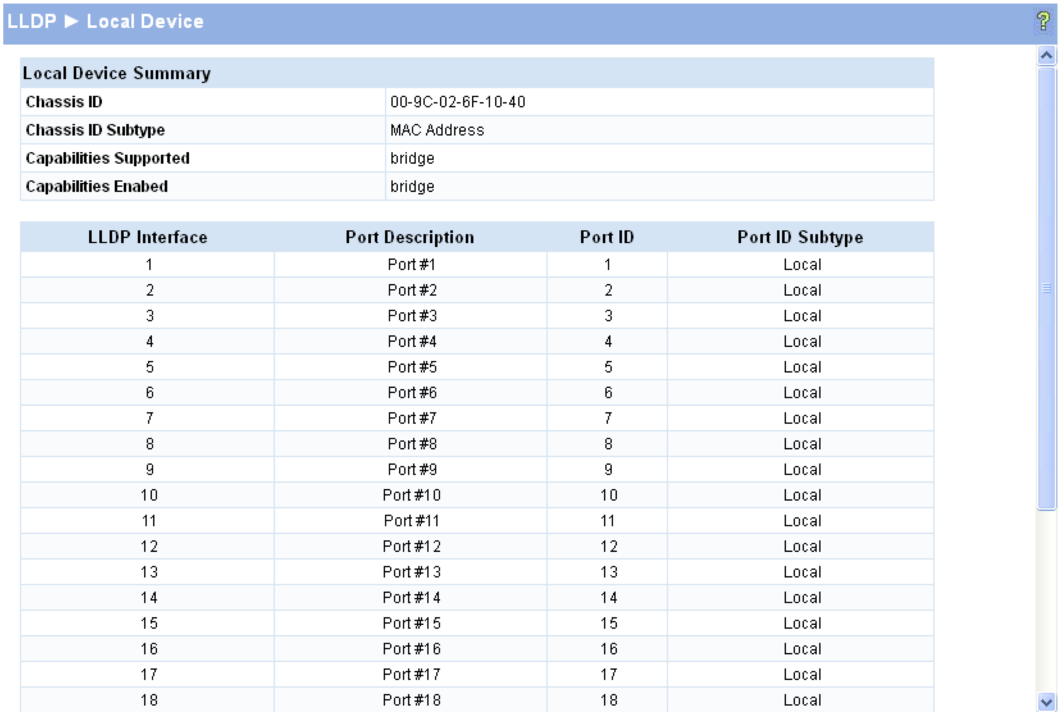
Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

LLDP Local Device

Use the LLDP Local Device page to view information about devices on the network for which the switch has received LLDP information.

To display the Local Device page, click **LLDP > Local Device** in the navigation pane.

Figure 8-2. LLDP Local Device Page



LLDP ▶ Local Device

Local Device Summary	
Chassis ID	00-9C-02-6F-10-40
Chassis ID Subtype	MAC Address
Capabilities Supported	bridge
Capabilities Enabed	bridge

LLDP Interface	Port Description	Port ID	Port ID Subtype
1	Port #1	1	Local
2	Port #2	2	Local
3	Port #3	3	Local
4	Port #4	4	Local
5	Port #5	5	Local
6	Port #6	6	Local
7	Port #7	7	Local
8	Port #8	8	Local
9	Port #9	9	Local
10	Port #10	10	Local
11	Port #11	11	Local
12	Port #12	12	Local
13	Port #13	13	Local
14	Port #14	14	Local
15	Port #15	15	Local
16	Port #16	16	Local
17	Port #17	17	Local
18	Port #18	18	Local

Table 8-2. LLDP Local Device Fields

Field	Description
Local Device Summary	
Chassis ID	The source of the chassis identifier (System MAC address).
Chassis ID Subtype	The type of the source of the chassis identifier (MAC address).
Capabilities Supported	Displays the system capabilities of the local system. The default is Bridge.
Capabilities Enabled	Displays the system capabilities of the local system that are supported and enabled. The default is Bridge.
LLDP Interface Description	
LLDP Interface	The interface on which LLDP 802.1AB frames can be transmitted.
Port Description	The description of the selected port associated with the local system.
Port ID	The source of the port identifier.
Port ID Subtype	Displays the type of the source of the port ID.

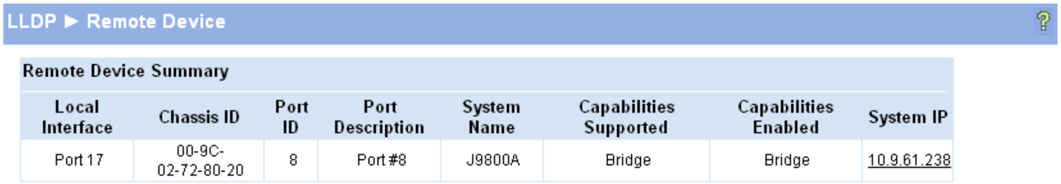
Click the **Refresh** link above the page to update the page with the latest data from the switch.

LLDP Remote Device

Use the LLDP Remote Device page to view information about remote devices for which the switch has received LLDP information.

To display the Remote Device page, click **LLDP > Remote Device** in the navigation pane.

Figure 8-3. LLDP Remote Device Page



Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	Capabilities Supported	Capabilities Enabled	System IP
Port 17	00-9C- 02-72-80-20	8	Port #8	J9800A	Bridge	Bridge	10.9.61.238

Table 8-3. LLDP Remote Device Fields

Field	Description
Local Interface	The port on the local system that received the LLDP data from the remote system.
Chassis ID	The chassis component associated with the remote system.
Port ID	The physical address of the port on the remote device that sent the LLDP data.
Port Description	The port description configured on the remote device. If the port description is not configured, the field is blank.
System Name	The system description configured on the remote device. If the system description is not configured, the field is blank.
System Capabilities	The capabilities on the remote device.
Capabilities Enabled	The capabilities on the remote device that are enabled.
System IP	IP address of the remote device.

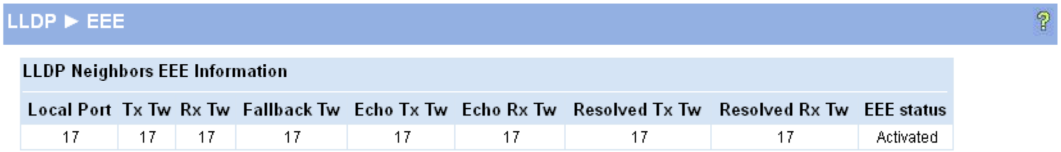
Click the **Refresh** link above the page to re-display the page with current settings from the switch.

Energy Efficient Ethernet

EEE (Energy Efficient Ethernet) is designed to save power by turning off network ports that are not passing traffic. EEE includes a mechanism to awaken the port when it needs to send or receive traffic. The transmitter sends LPI (low power idle) signals instead of the normal idle signals to indicate that the EEE protocol is in effect. After a period of time called Ts (time to sleep), the transmitter stops sending signals and the link is quiet. When the transmitter needs to send traffic, it begins sending normal idle signals. After a period of time called Tw (time to wake), the link becomes active and begins passing traffic. Ts and Tw are negotiated between the link partners using LLDP.

To display the EEE page, click **LLDP > EEE** in the navigation pane. EEE activated columns show if the switch and the link partner have agreed upon which wakeup times to use.

Figure 8-4. LLDP Neighbors EEE Information Page



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE status
17	17	17	17	17	17	17	17	Activated

Table 8-4. LLDP Neighbors EEE Information Fields

Field	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Tw	The time in microseconds that the transmitting link partner waits after leaving the low power idle mode, before sending data.
Rx Tw	The time in microseconds that the receiving link partner requests the transmitting link partner to wait after leaving the low power idle mode, before sending data.
Fallback Receive Tw	An alternate value for the time that the receiving link partner requests the transmitting link partner to wait after leaving LPI mode, before sending data.
Echo Tx Tw	Echo sent to the link partner of the latest values received from the link partner.
Echo Rx Tw	Echo sent to the link partner of the latest values received from the link partner.
Resolved Tx Tw	The current Tx Tw value in use.
Resolved Rx Tw	The current Rx Tw value in use.
EEE Status	Status of the Energy Efficient Ethernet. **Activated**—Switch and link partner have agreed upon wakeup time. **Not Activated**—Switch and link partner have not agreed upon wakeup time.

9

Diagnostics

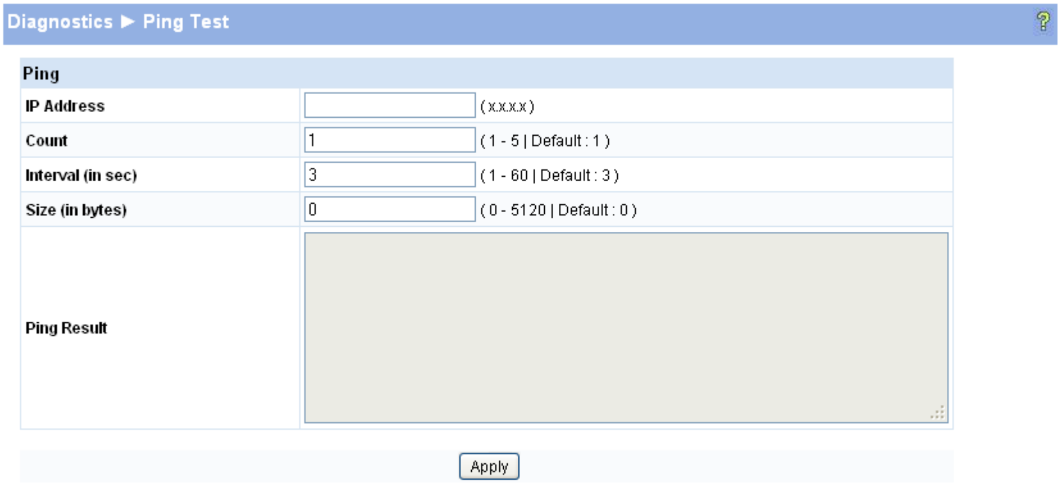
You can use the Diagnostics Pages to test, configure, and reboot the HP 1810 series switch.

Ping Test

Use the Ping Test page to determine whether another device on the network is reachable. Ping provides a synchronous response when initiated.

To display the Ping Test page, click **Diagnostics > Ping Test** in the navigation pane.

Figure 9-1. Ping Test Page



Diagnostics ▶ Ping Test

Ping		
IP Address		(x.x.x.x)
Count	1	(1 - 5 | Default : 1)
Interval (in sec)	3	(1 - 60 | Default : 3)
Size (in bytes)	0	(0 - 5120 | Default : 0)
Ping Result		

Table 9-1. Ping Test Fields

Field	Description
IP Address	Specify the IP address of the host you want to reach.
Count	Specify the number of packets to send. (Range 1 - 5 packets, Default = 1)
Interval	Specify the delay between ping packets. (Range 1–60 seconds, Default = 3 seconds)
Size	Specify the size of the ping packet to be sent. (Range 0–5120, Default = 0)

- Click **Apply** to ping the specified host. The output includes the following data:
  - IP Address—The IP address of the device that was pinged.
  - Sequence—The Internet Control Message Protocol (ICMP) number of the packet, starting from 0.
  - Time—The ping reply status.

- Transmitted Packets—The number of packets sent.
- Received Packets—Number of packets received.
- Min/Max/Avg RTT—Specifies the Minimum, Maximum, Average Round Trip Time (msec).

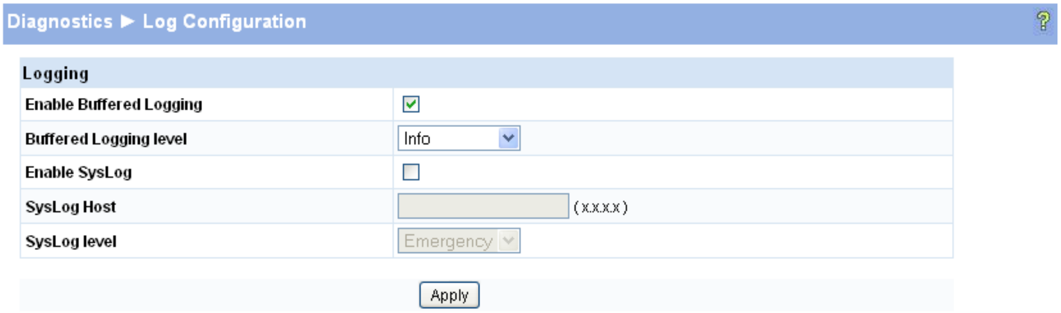
Log Configuration

The HP 1810 series switch software supports logging system messages to the Log file or forwarding messages over the network using the Syslog protocol. Syslog messages can be captured by a designated host on the network that is running a Syslog daemon.

Note The storage size of the log file is 10k, approximately 100 entries. The most recent 100 log entries are displayed; index numbering may not be 1-100. See your syslog entries to view more than 100 log messages.

To display the Log Configuration page, click **Diagnostics > Log Configuration** in the navigation pane.

Figure 9-2. Log Configuration Pages



Diagnostics ▶ Log Configuration ?

Logging	
Enable Buffered Logging	☑
Buffered Logging level	Info
Enable SysLog	□
SysLog Host	(x.x.x.x)
SysLog level	Emergency

Table 9-2. Log Configuration Fields

Field	Description
Enable Buffered Logging	Specify type of system messages logged using the Buffered Logging Level setting: • Emergency: Alerts the user of the highest level of system error classified as urgent. • Alert: Alerts the user of a high level of system error. • Critical: Alerts the user of a high level of system error which must be immediately addressed. • Error: Alerts the user of an error in the system. • Warning: Warns the user of an impending system error of a specified operation. • Notice: Notifies the user of a system error. • Info: Provides the user with system information. • Debug: An internal note to reconcile programming code.
Buffered Logging Level	Specify a logging level. A log records messages equal to or above a configured console logging level. (Info by default.)
Enable Syslog	Enable the switch to send Syslog messages. (Disabled by default.)
Syslog Host	Specify the IP address of a host on the network running a Syslog daemon that will capture the messages.

Field	Description
Syslog Level	Specify a Syslog logging level. A log records messages equal to or above a configured console logging level. (Emergency by default.)

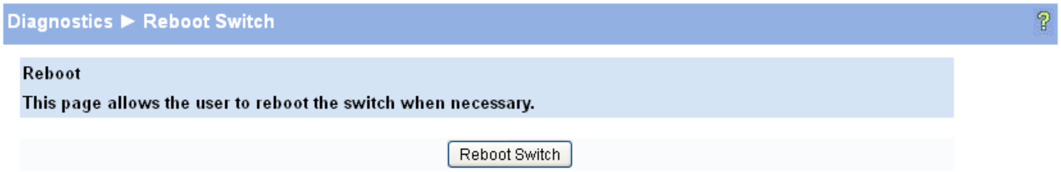
Click **Apply** to save any changes for the current boot session; the changes take effect immediately.

Reboot Switch

Use this feature to perform a software reboot of the switch. If you applied configuration changes, wait at least one minute before rebooting to ensure that the changes are saved to the system configuration file, or use the **Maintenance > Save Configuration** page to save them immediately.

To display the Reboot Switch page, click **Diagnostics > Reboot Switch**.

Figure 9-3. Reboot Switch Page



Reboot

This page allows the user to reboot the switch when necessary.

Click **Reboot Switch** to reboot the switch.

Factory Defaults

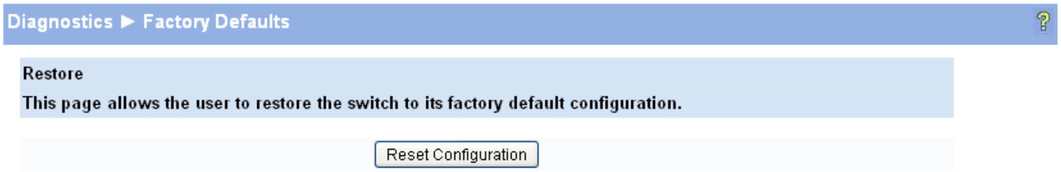
Two configuration files are kept in system memory: one contains custom settings; the other contains the factory defaults. Use this page to restore all settings to the factory defaults.

To display the Factory Defaults page, click **Diagnostics > Factory Defaults**.

Caution

Backup the current configuration file prior to restoring the factory defaults configuration. See “Backup Manager” on page 10-1 for instructions.

Figure 9-4. Factory Defaults Page



Restore

This page allows the user to restore the switch to its factory default configuration.

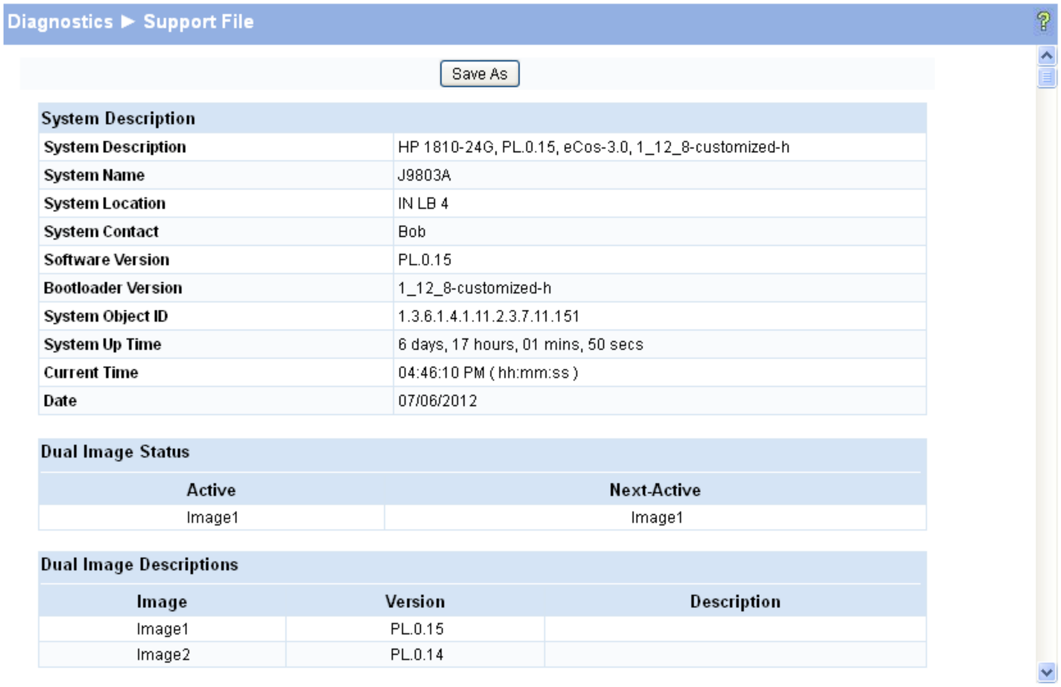
Click **Reset Configuration** to restore the system to the default settings.

Support File

Use the support file page to display summary information for the switch on a single page.

To display the Support File page, click **Diagnostics > Support File** in the navigation pane.

Figure 9-5. Support File Page



System Description	
System Description	HP 1810-24G, PL.0.15, eCos-3.0, 1_12_8-customized-h
System Name	J9803A
System Location	IN LB 4
System Contact	Bob
Software Version	PL.0.15
Bootloader Version	1_12_8-customized-h
System Object ID	1.3.6.1.4.1.11.2.3.7.11.151
System Up Time	6 days, 17 hours, 01 mins, 50 secs
Current Time	04:46:10 PM (hh:mm:ss)
Date	07/06/2012

Dual Image Status

Active	Next-Active
Image1	Image1

Dual Image Descriptions

Image	Version	Description
Image1	PL.0.15	
Image2	PL.0.14	

The support file page includes the following information:

- System description
- Dual image status and descriptions
- Buffered log messages
- Logging configuration details
- SNTP configuration
- Time zone configuration
- Network details
- Web parameters
- Management access
- SNMP
- Port configuration details, summary, and statistics
- Trunk statistics
- Jumbo frames configuration details

- Storm control, Auto DoS, and Flow control configuration
- Web configuration
- MAC address forwarding table and summary statistics
- VLAN configuration and membership details
- Trunk status
- LLDP global mode details
- Interface mode details
- LLDP global and interface statistics, and local and remote device summaries
- Port mirroring configuration
- Loop protection status per interface
- Spanning tree bridge and interface status and configuration, and port settings

To save the Support File data to a file, click **Save As** located at the top and bottom of the page.

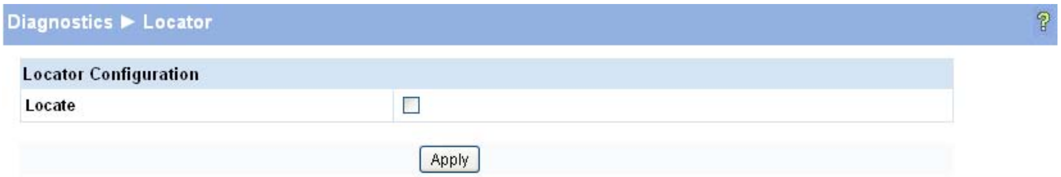
You can print the text from your text editor. Alternatively, your browser may support printing only the frame that contains the data (that is, it excludes the navigation pane and Web Applet) directly from the Web page. Right-click the data area to see if your browser provides this option.

Locator

The Locator LED is a special LED that enables locating the device physically. When enabling the Locate setting via the Web interface, the Locate LED on the switch blinks for 30 minutes and then turns off.

To display the Locator page, click **Diagnostics > Locator** in the navigation pane.

Figure 9-6. Locator Page



Locator Configuration	
Locate	□

Select **Locate** and click **Apply** to cause the Locator LED on the switch to blink for 30 minutes.

10

Maintenance Pages

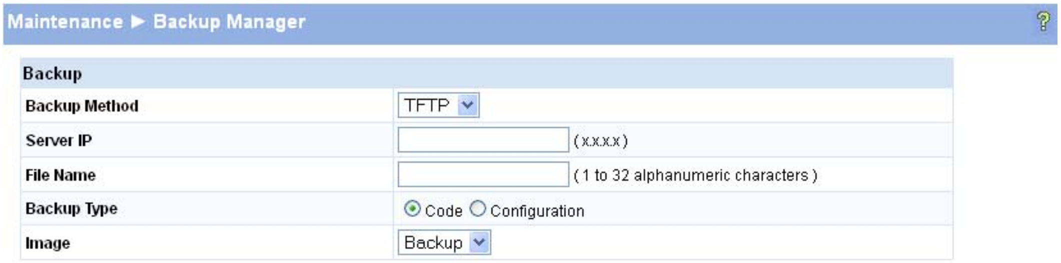
Backup Manager

The Backup Manager page provides a means to save a backup copy of the switch's image or configuration files on a local system or network directory.

The page displays different options depending on the protocol and image or file type selected for the backup. As shown in the example in Figure 10-1, TFTP (Trivial File Transfer Protocol) has been selected as the backup method for saving the code (entire image) onto a server.

To display the Backup Manager page, click the **Maintenance > Backup Manager**.

Figure 10-1. Backup Manager Page



Maintenance ▶ Backup Manager

Backup	
Backup Method	TFTP
Server IP	(x.x.x.x)
File Name	(1 to 32 alphanumeric characters)
Backup Type	● Code ○ Configuration
Image	Backup

Table 10-1. Backup Manager Fields

Field	Description
Backup Method	Select the protocol to use: • **HTTP**—The file is downloaded over the current browser session. • **TFTP**—This requires a TFTP server operating on the system/network.
Server IP (TFTP backup only)	If a TFTP backup is to be performed, enter the IP address of the TFTP server.
File Name (TFTP backup only)	If a TFTP backup is to be performed, enter the file name with which backup must be saved. This can differ from the actual file name on the switch.
Backup Type	Select the image or file to be backed up: • **Code**—The entire image is backed up. • **Configuration**—Only the configuration file is backed up.
Image Name	If Code is selected as the Backup Type, select one of the two images stored in memory: • **Active**—The currently active image is backed up. • **Backup**—The backup image is backed up. name *config.bin*).

- For a backup using HTTP, click **Upload** to begin the backup process. A window displays with a prompt to save the file in the desired location.
- For backup using TFTP, ensure that the TFTP server is running and click **Upload**. Use a TFTP application to initiate the backup.

Note

If using Internet Explorer, when you attempt a backup operation from a secure HTTP session using the HTTP protocol, you may receive the following error message, even though the document is available and downloaded from the server:

> Internet Explorer cannot download filename from <*site name*>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.

This error happens due to security limitations with Internet Explorer. Recent versions do not have this problem. To perform the operation, configure the following settings in your browser:

1. Click **Tools > Internet Options** and display the **Advanced** tab.
2. In the Security settings, select **Do not save encrypted pages to disk.**
3. Try the backup operation again.
4. After the backup operation is complete, restore your settings to the original values to avoid Web performance issues.

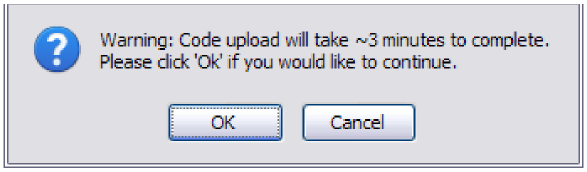
If you use a browser other than Microsoft Internet Explorer, such as Firefox or Mozilla, the download of the attachment should work as expected.

Example—Backing Up a Configuration File

Follow these instructions to back up a configuration file.

1. In the **Backup Method** field, select the protocol to use to upload the file to the system. To save the file on a local or network drive, select **HTTP**. To save the file on a TFTP server, select **TFTP**.
2. If TFTP is selected, specify the IP address of the TFTP server and the name to assign to the file when it is saved.
3. Select **Configuration** in the Backup Type field.
4. Click **Apply**.

   A window like following displays (the text may differ depending on the selected protocol and backup type):



Warning: Code upload will take ~3 minutes to complete.
Please click 'Ok' if you would like to continue.

5. Click **OK**. For an HTTP transfer, browse to the location where you want to save the file.

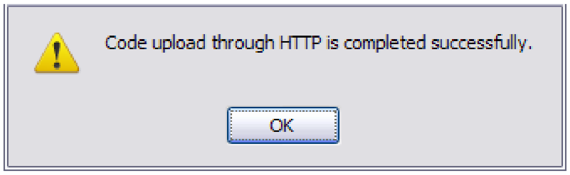
   A progress bar indicates that the backup is in progress and the page displays the following message:

   Code (Configuration) upload through HTTP (TFTP) is in Progress.
   Please wait...

Caution

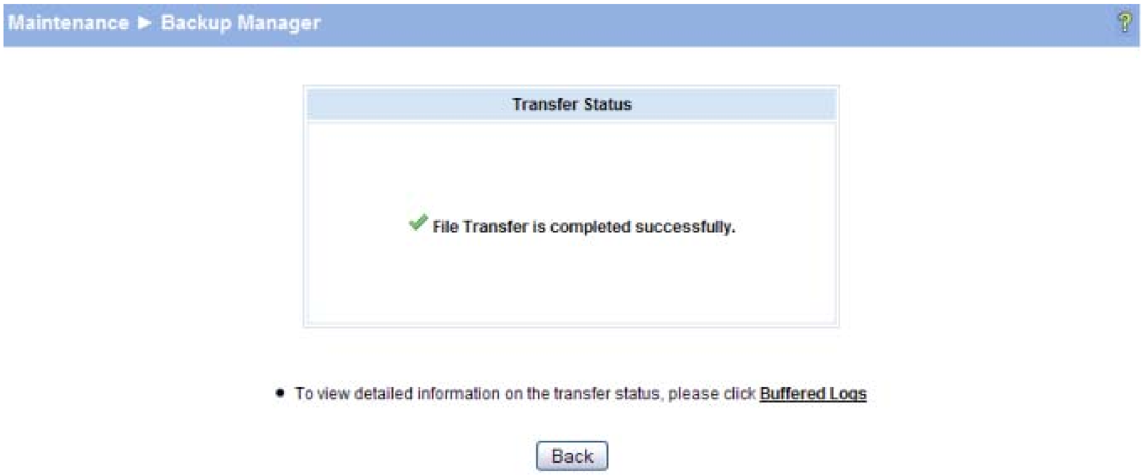
Do not disturb the browser window while the transfer is in progress.

When the backup is complete, a window like the following displays.


Code upload through HTTP is completed successfully.

6. Click **OK**.

   The Backup Manager page displays the following status message:



✓ File Transfer is completed successfully.

- To view detailed information on the transfer status, please click Buffered Logs

7. Click **Back** to re-display the Backup Manager page.

Note To restore a backed-up code or configuration file, use Update Manager.

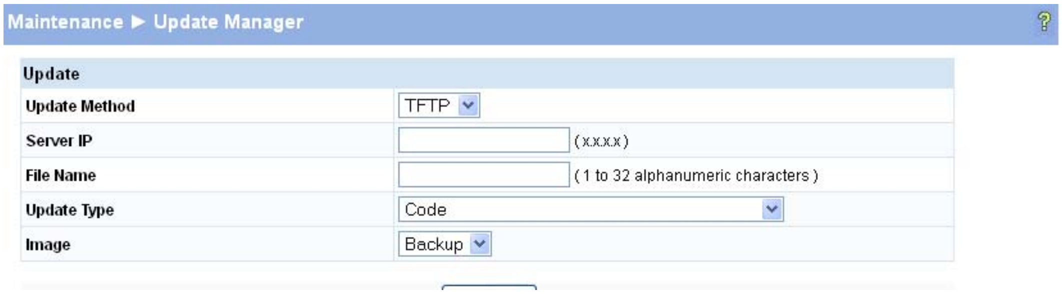
Update Manager

The Update Manager page enables a new image or configuration file to be uploaded from the local system or network to the switch.

Update Manager displays different options depending on the transfer protocol, file or image type selected for an update. In the example in Figure 10-2, the inactive (or “Backup”) image on the switch is being updated from a TFTP server. For example, if the *image1* file is being used as the currently-active image running on the switch, then the *image2* file is the backup file to be updated.

To display the Update Manager page, click **Maintenance > Update Manager** in the navigation pane.

Figure 10-2. Update Manager Page



Update	
Update Method	TFTP
Server IP	(x.x.x.x)
File Name	(1 to 32 alphanumeric characters)
Update Type	Code
Image	Backup

Table 10-2. Update Manager Fields

Field	Description
Update Method	Select the protocol to use: • **HTTP**—The file is downloaded using HTTP from a local or remote drive. • **TFTP**—The file is downloaded using TFTP from a TFTP server operating on the system/ network.
Browse for file (HTTP upload only)	If HTTP is used for the software update, click **Browse** to select the designated file. **Note**: If the file name differs from the default name on the switch, the file will be renamed to the default name when uploaded (see the **Update Type** field description).
Server IP (TFTP upload only)	If a TFTP download is performed, enter the IP address of the TFTP server.
File Name (TFTP upload only)	If a TFTP download is performed, enter the name, and file path as needed, of the software update file on the TFTP server.
Update Type	Select the file type to be updated: • **Code**—Update the software image file specified. • **Configuration**—Update up the configuration file. • To update an SSL certificate or key encryption file, select the certificate type (for a description of these files, see "Secure Connection" on page 5-2): • **SSL Trusted Root Certificate PEM File**—SSL Trusted Root Certificate File which is encoded using the Privacy Enhanced Mail (PEM) protocol. • **SSL Server Certificate PEM File**—SSL Server Certificate File (PEM-encoded). • **SSL DH Weak Encryption Parameter PEM File**—SSL Diffie-Hellman Weak Encryption Parameter File (PEM encoded). • **SSL DH Strong Encryption Parameter PEM File**—SSL Diffie-Hellman Strong Encryption Parameter File (PEM encoded).
Image (for Code updates only)	If **Code** is selected as the update type, select which of the two images stored on the switch is to be updated: • **Active—The uploaded image will replace the currently active image.** • **Backup**—The uploaded image will replace the backup image.

Example—Updating the Switch Software

Caution

It is recommended that you back up the image file before updating it. See "Backup Manager" on page 10-1 for instructions.

Follow these instructions to update the switch software (that is, a firmware code image):

1. In the **Update Method** field, select the protocol to use to upload the file to the system. If the file is located on a local or network drive, select **HTTP**. If the file is located on a TFTP server, select **TFTP**.

2. If TFTP is selected, specify the IP address of the TFTP server, the path to the file, and the name of the file as it appears on the server.

   If HTTP is selected, browse to locate the file on your network or local drive.

3. In the Update Type field, select **Code**.

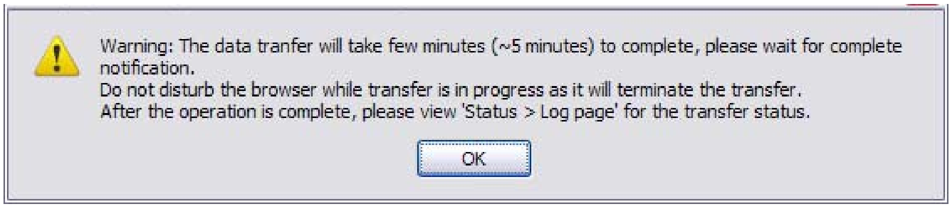
4. In the **Image** field, choose **Backup** or **Active**.

   If you choose **Backup**, the inactive (backup) image file will be updated. In the example in Figure 10-2 on page 10-4, the Backup image file is selected for update.

   If you choose **Active**, the active image file will be updated.

5. Click **Download**.

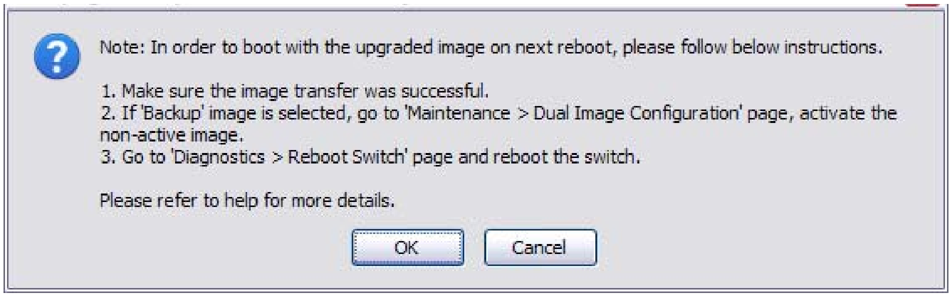
   A warning page like the following displays (the text may differ depending on the protocol selected):



Warning: The data tranfer will take few minutes (~5 minutes) to complete, please wait for complete notification.
Do not disturb the browser while transfer is in progress as it will terminate the transfer.
After the operation is complete, please view 'Status > Log page' for the transfer status.

6. Click **OK**.

   The following page displays:



Note: In order to boot with the upgraded image on next reboot, please follow below instructions.

1. Make sure the image transfer was successful.
2. If 'Backup' image is selected, go to 'Maintenance > Dual Image Configuration' page, activate the non-active image.
3. Go to 'Diagnostics > Reboot Switch' page and reboot the switch.

Please refer to help for more details.

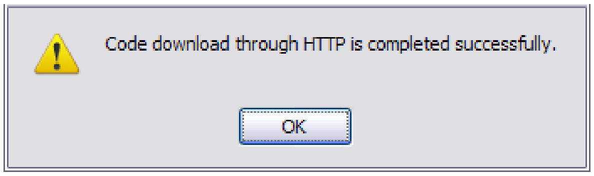
7. Click **OK**.

   The following message displays on the Update Manager page:

   Code (Configuration) download through HTTP (TFTP) is in Progress.

   Please wait...

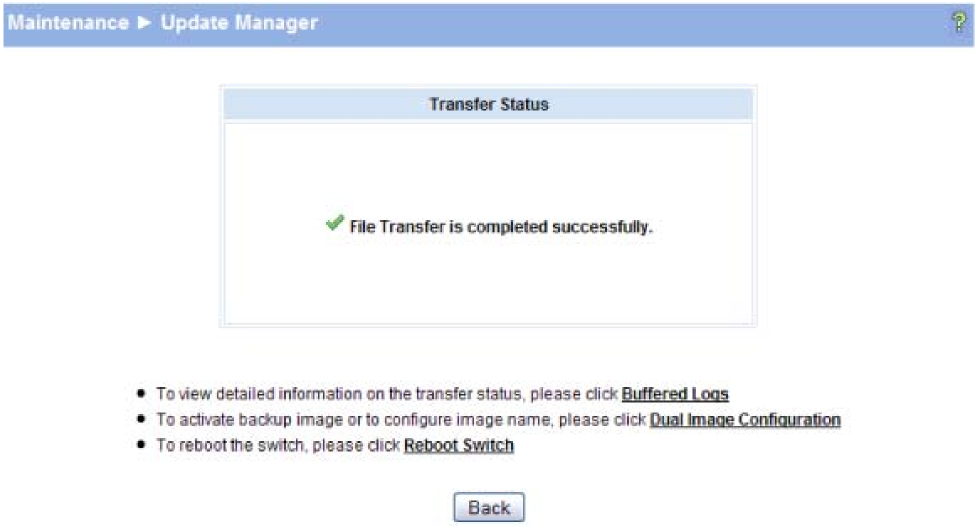
   When the transfer is complete, a window like the following displays:



Code download through HTTP is completed successfully.

8. Click **OK**.

Update Manager displays the following status message:



Transfer Status

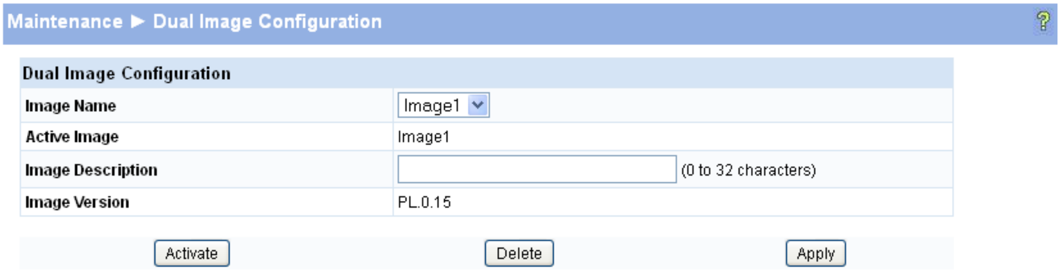
✓ File Transfer is completed successfully.

- To view detailed information on the transfer status, please click Buffered Logs
- To activate backup image or to configure image name, please click Dual Image Configuration
- To reboot the switch, please click Reboot Switch

9. Click **Back** to re-display the Update Manager page.

   Note that, in this example, the image was downloaded as the inactive (backup) image. To complete the update process and to activate the backup image as the operating software, use the Dual Image Configuration page.

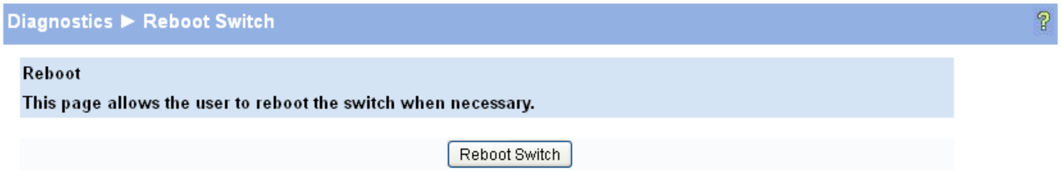
   In the following example, *Image1* is the active image, and *Image2* is the newly updated backup image. By clicking **Activate**, *Image2* will be activated on the next reboot (and *Image1* will become the inactive backup image).



Dual Image Configuration	
Image Name	Image1
Active Image	Image1
Image Description	(0 to 32 characters)
Image Version	PL.0.15

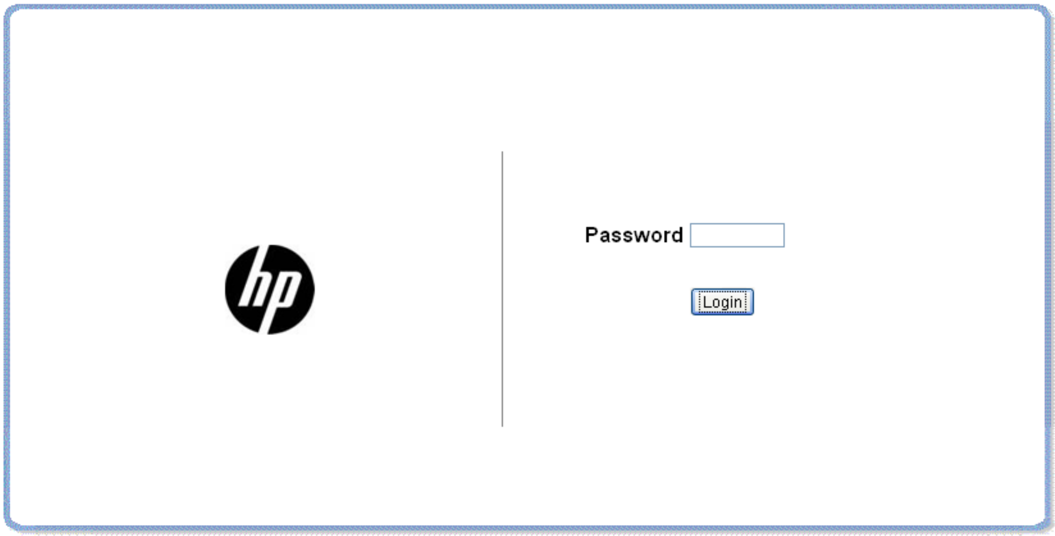
10. (Optional) Add a description for the selected image (*Image2*) and click **Apply**.
11. Click **Activate** to activate the selected image on the next reboot.

    Note: You can verify the next active image by viewing the **Status > Dual Image** screen.
12. Click **Diagnostics > Reboot Switch**, and then click **Reboot Switch** to complete the update.



Reboot
This page allows the user to reboot the switch when necessary.

Wait for the switch to reboot and display the login page.

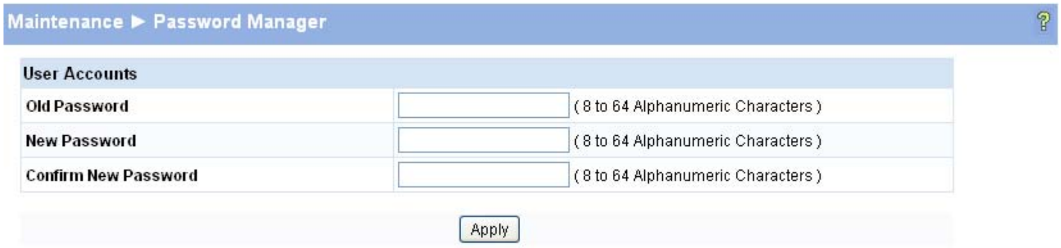


Password Manager

Use the Password Manager to change the password used to access the Web interface.

To display the Password Manager page, click the **Maintenance > Password Manager**.

Figure 10-3. Password Manager Page



Maintenance ▶ Password Manager

User Accounts	
Old Password	(8 to 64 Alphanumeric Characters)
New Password	(8 to 64 Alphanumeric Characters)
Confirm New Password	(8 to 64 Alphanumeric Characters)

Note

There is no default password. Passwords must be at least 8 characters but no more than 64 characters long. Passwords are case sensitive. There is no default password. Passwords are up to 64 alpha-numeric and special characters (~,`,!,@,#,$,%,^,&,*,(,),-,_,+,=,{,[,},],|,\,<,,,>,.,?,/",' and space) in length, and are case sensitive. The password needs to be entered again to confirm new password. In case of a forgotten password, manually reset the switch to its factory defaults.

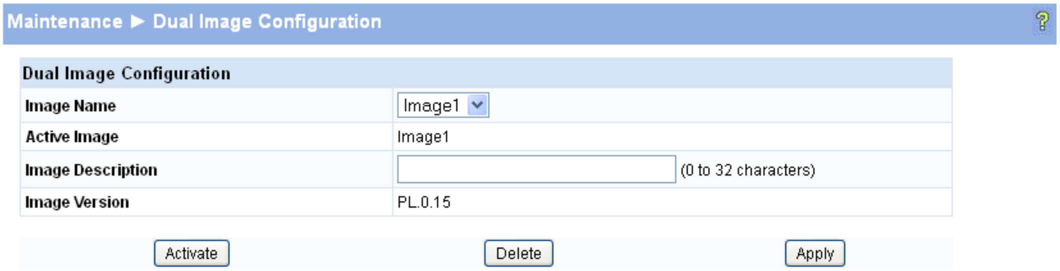
Enter the old password and the new password twice, and click **Apply**. At the next log on, use the new password.

Dual Image Configuration

Use the Dual Image Configuration page to name and change the next bootup image. The Dual Image Configuration allows activating either of the stored images: Image1 or Image2. When one image is activated, the other image serves as a backup; if Image1 either fails or does not boot, then the other image can be activated.

To display the Dual Image Configuration page, click **Maintenance > Dual Image Configuration**.

Figure 10-4. Dual Image Configuration Page



Dual Image Configuration	
Image Name	Image1
Active Image	Image1
Image Description	(0 to 32 characters)
Image Version	PL.0.15

Table 10-3. Dual Image Configuration Fields

Field	Description
Image Name	Select the image you want to perform an action on. You can activate the selected image, delete it, or configure a description of it. Options are Image1 and Image2.
Active Image	The currently active image.
Image Description	Specify a description of the image selected in the Image Name field.
Image Version	The software version associated with the active image.

- Click **Activate** to activate the selected image selected in the Image Name field. Be sure to configure the Image Description field to the version of the image loaded so that users can easily distinguish between the images.
- Click **Apply** to apply a description to the image selected in the **Image Name** field.
- Click **Delete** to delete the image selected in the **Image Name** field.

To view dual image status information, click **Status > Dual Image Status** in the navigation pane.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/

September 2012

Manual Part Number
5998-3208