53-1002268-01
25 March 2011

PowerConnect B-Series FCX

Web Management Interface User Guide

Regulatory Model Codes: FCX624-I, FCX624-E, FCX624-S, FCX648-I, FCX648-E, FCX648-S

Contents

About This Document

In this chapter

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing. This guide includes the GUI and procedures for monitoring, configuring the various features of the PowerConnect B-Series FCX devices using the GUI.

If you are using a Layer 3 Switch, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP4, IGMP, PIM, DVMRP, FSRP, and VRRP.

Supported hardware and software

The following hardware platforms are supported by this release of *PowerConnect B-Series FCX Web Management Interface User Guide:*

- PowerConnect B-FCX624s
- PowerConnect B-FCX648s
- PowerConnect B-FCX624
- PowerConnect B-FCX648

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
code text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Notes, cautions, and danger notices

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Related publications

The following Dell documents supplement the information in this guide:

- *PowerConnect B-FCX Switch Hardware Installation Guide*
- *PowerConnect B-Series FCX Configuration Guide*

NOTE
For the latest edition of this document, which contains the most up-to-date information, refer to support.dell.com.

Getting technical help or reporting errors

Dell is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Dell Technical Support. When contacting Dell Technical Support have the device configuration file and an output capture of show tech-support command available.

Contacting Dell

For customers in the United States, call 800-WWW.DELL (800.999.3355).

NOTE
If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit http://support.dell.com.
2. Click your country or region at the bottom of the page. For a full listing of countries and regions, click **All**.
3. In the Support menu, click **All Support**.
4. Choose the method of contacting Dell that is convenient for you.

Chapter

1 Stackable Devices and Concepts

In this chapter

Stackable models

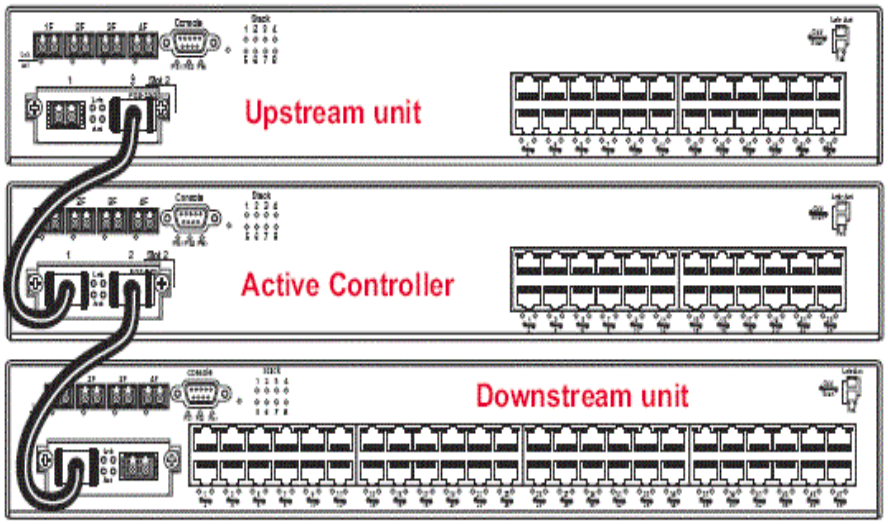
A stack is a group of devices that are connected so that they operate as a single chassis. For detailed information about Dell stacking technology, and for a list of stackable models, refer to the *PowerConnect B-Series FCX Configuration Guide*.

Stack topologies

Stack technology supports linear and ring stack topologies. Although stackable units may be connected in a simple linear topology, Dell recommends a ring topology because it offers the best redundancy and the most resilient operation.

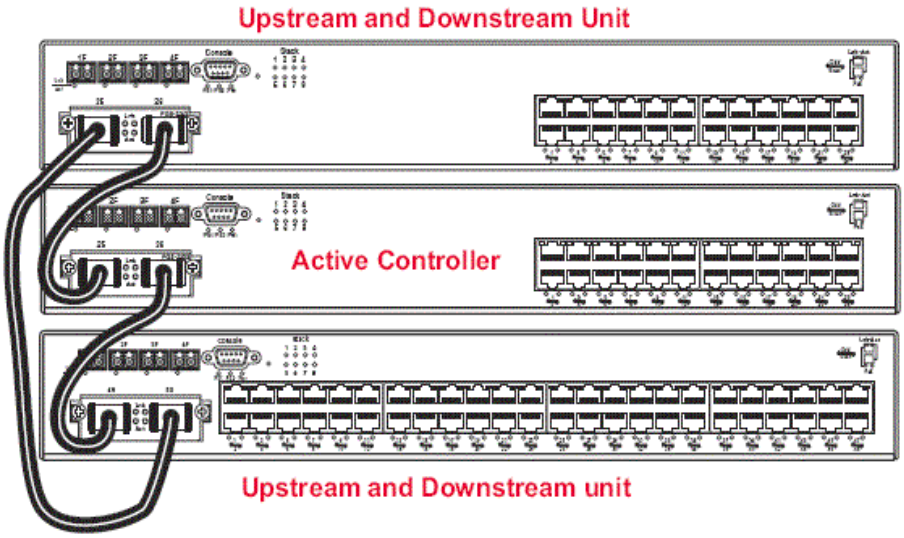
Figure 1 shows a linear stack topology. Figure 2 shows a ring stack topology. These illustrations depict only one cabling configuration, but cabling methods may differ depending on requirements.

FIGURE 1 Linear Stack Topology



NOTE
In linear topologies, stack units at either end of the stack use only one stacking port. The unused stacking port may be used as a data port.

FIGURE 2 Ring Stack Topology



NOTE
In ring topologies, stack units are considered both upstream and downstream because every unit can be reached from either direction.

For more detailed information about stack topologies and about stacking terminology, refer to the *PowerConnect B-Series FCX Configuration Guide*.

Chapter

The Web Management Interface 2

In this chapter

Access requirements

The Web Management Interface (WMI) is a browser-based interface that allows administrators to manage and monitor a single PowerConnect device, or a group of PowerConnect devices connected in an IronStack topology. For many of the features on a PowerConnect device, the interface can be used as an alternate to the CLI for creating new configurations, modifying existing ones, and monitoring the traffic on a device, or on an IronStack.

NOTE
The WMI does not provide network management capabilities. If you need to manage a network of PowerConnect devices, use the *Brocade Network Advisor* application.

The WMI is available on PowerConnect devices. Refer to the Release Notes for your device to determine if the Web Management Interface described in this manual applies to your product.

The interface can be accessed from a management station using a Web browser through an HTTP connection. The management options can be accessed from a menu tree, or a list. The menu tree view is available when you use the Web Management Interface with the following Web browsers:

- Netscape 4.0 or higher
- Internet Explorer 4.0 or higher
- Safari 3.1
- Google Chrome
- Mozilla Firefox
- Opera

If you use the WMI with an older browser, the Web Management Interface displays only the List view.

To access the Web Management Interface, PowerConnect devices must be set up as mentioned below:

- A management station, such as a PC, with a Web browser, that is either connected directly to the PowerConnect device or is on the network of the device to be managed.
- The device must have an IP address. Assign the IP address using the CLI. For more information on IP addresses for an IronStack, refer to the *PowerConnect B-Series FCX Configuration Guide.*

- A Simple Network Management Protocol (SNMP) community string must be configured on the device using the CLI. This community string is used as your password to log in through the WMI. A community string is required for read-write access and for read-only access.
- The device must be powered on before you begin management activities.

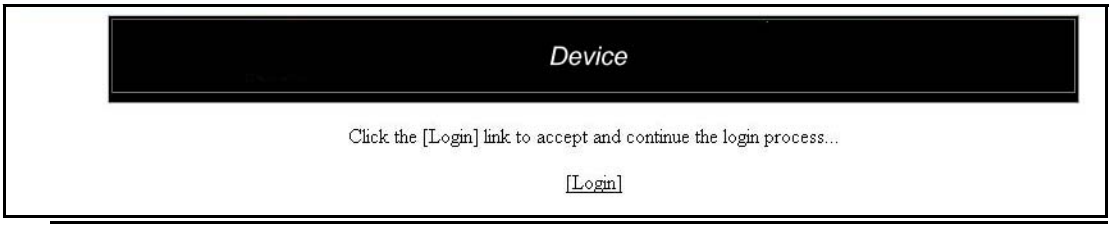
Logging in and logging out

Follow the procedures below to log in to the Web Management Interface.

1. Open a Web browser and enter the IP address of the PowerConnect device in the Location or Address field.

   The Web browser contacts the PowerConnect device and displays the device name in the login page, as shown in Figure 3.

FIGURE 3 Web Management Interface login page



NOTE
If you are unable to connect with the device through a Web browser due to a proxy problem, it may be necessary to set your Web browser for direct Internet access instead of using a proxy. For information on how to change a proxy setting, refer to the on-line help provided with your Web browser.

2. Click **Login** link. The following example dialog box appears.

FIGURE 4 User name and password dialog box

3. Do one of the following:
   - For read-only access, enter **get** for User Name and a read-only community string for the Password. The community string **public** is the default read-only community string.

- For read-write access, enter **set** for User Name and a read-write community string for the Password. There is no default read-write community string.

NOTE
If you have configured the device to secure Web Management Interface using local user accounts, you must enter the user name and password of one of the user accounts.

The home page appears. Figure 5 shows the home page for a Layer 2 switch. Home pages for a Layer 3 Switch will have different entries.

FIGURE 5 Example of Web Management Interface home page

1	Menu (tree- view).	3	General system panel.
2	Configuration panel.	4	Short-cuts to functions and other panels.

4. Click **Logout**, under the Command module in the menu tree on the left panel of the screen to log out of the application.

Navigating the Web Management Interface

The Web Management Interface panels (Figure 5) consist of several parts. The left panel shows the menu tree or list of options. The interface can be set up to display a menu tree or a list of options. The procedures in this document assume that the menu-tree view is selected for the interface.

The right panel of the interface contains a display area where you indicate the values of the parameters you are configuring or where you view data for the feature you are monitoring.

On an interface home page, the configuration panel is the same panel displayed when you select the **Configure** > **System** > **General** option. In this document, this panel will be referred to as the General System configuration panel.

The General System configuration panel displays a list of features and protocols that can be enabled or disabled using the Web Management Interface. For example, in Figure 5, you can enable or disable port-based VLANs, protocol-based VLANs, Quality of Service (QoS), Spanning Tree Protocol (STP), IP Multicast, and Internet Group Management Protocol (IGMP) on this panel.

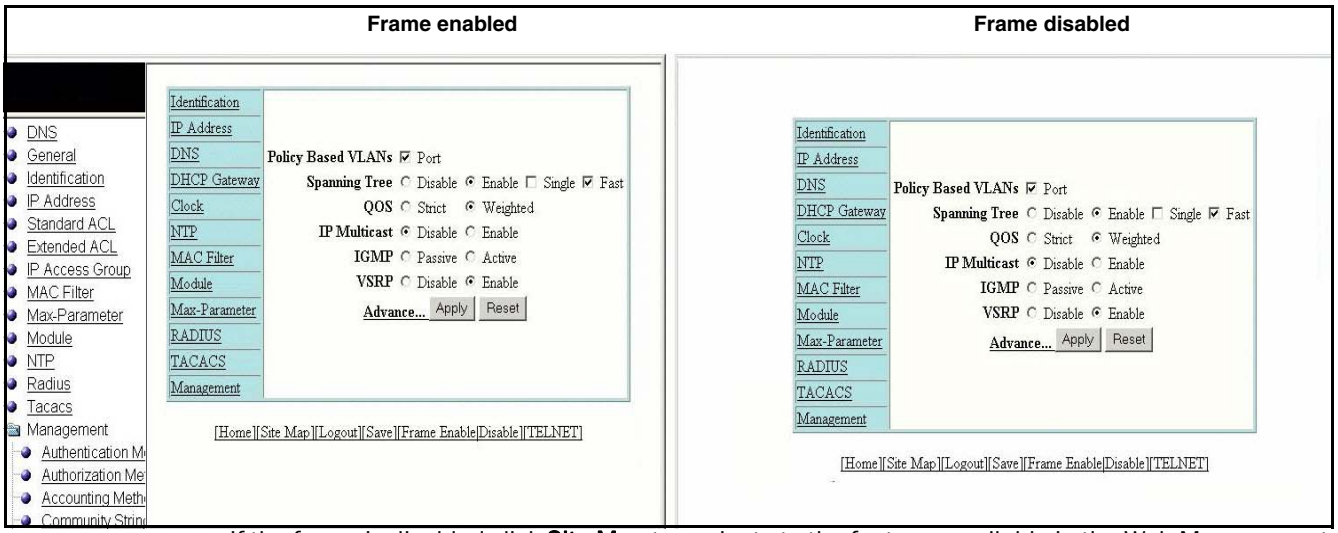
The General System configuration panel also has links to frequently-used panels. For example, instead of navigating to the Identification panel by selecting **Configure** > **System** > **Identification**, you can use the hyperlink displayed in every page of the main window. Other panels in the Web Management Interface may also contain hyperlinks.

The **Apply** and **Reset** buttons appear in many configuration panels. Click **Apply** to save changes to the running configuration. Click **Reset** before you click **Apply** if decided to abandon the entries.

All configuration panels also have links along the bottom. These links are shortcuts to frequently-used device management functions. Web Management Interface panels all have the following links:

- **[Home]** – Returns you to the home page of the Web Management Interface
- **[Site Map]** – Lists all options available from the Web Management Interface with links to the panels for those options. Use the Site Map links to navigate the interface if the menu is not displayed
- **[Logout]** – Logs you out of the Web Management Interface
- **[Save]** – Saves the changes you entered on the panels
- **[TELNET]** – Opens a Telnet session to the device
- **[Frame Enable|Disable]** – Enables or disables the bookmark options available in the left panel (Figure 6). If frames are disabled, you will not be able to choose any of the options on the Web Preference panel that uses frames.

FIGURE 6 Frame Enabled and Disabled



If the frame is disabled click **Site Map** to navigate to the features available in the Web Management Interface.

Chapter

Monitoring Stack Performance and Metrics 3

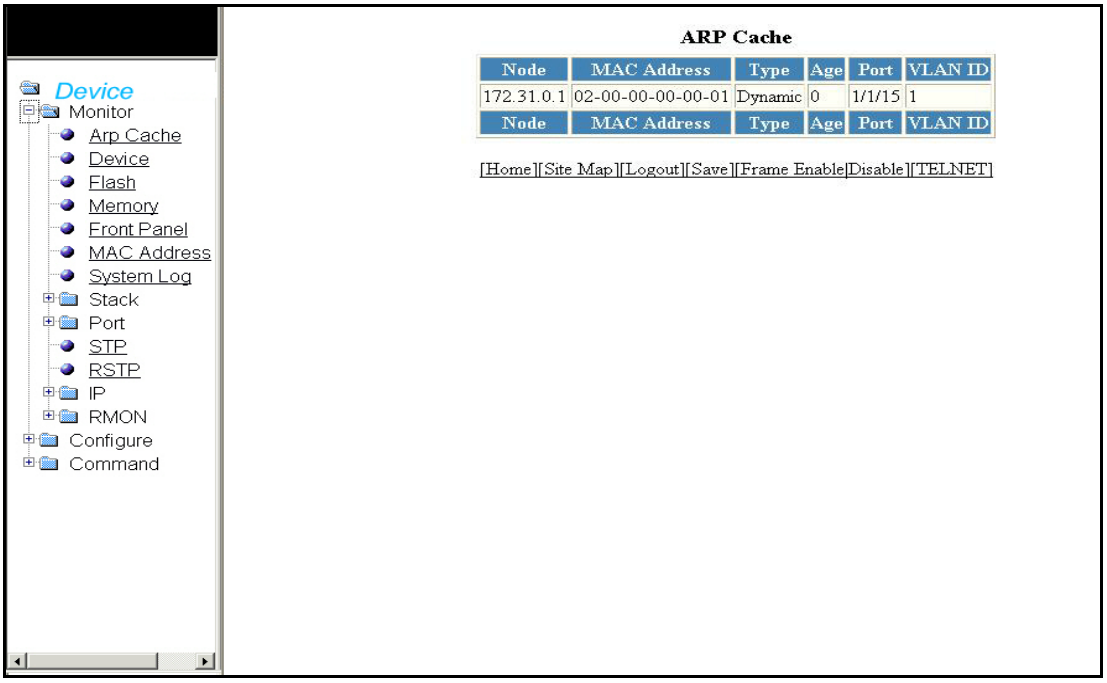
In this chapter

Monitoring the ARP cache

Once you have logged into the Web Management Interface (WMI), you can monitor the stack settings that determine performance.

The Address Resolution Protocol (ARP) Cache table contains entries for devices attached to the device you are monitoring. The ARP cache contains entries that map IP addresses to MAC addresses. The ARP cache can contain dynamic (learned) entries and static (user-configured) entries. Select **Monitor > ARP Cache** to view the ARP Cache information.

FIGURE 7 Monitoring the ARP Cache



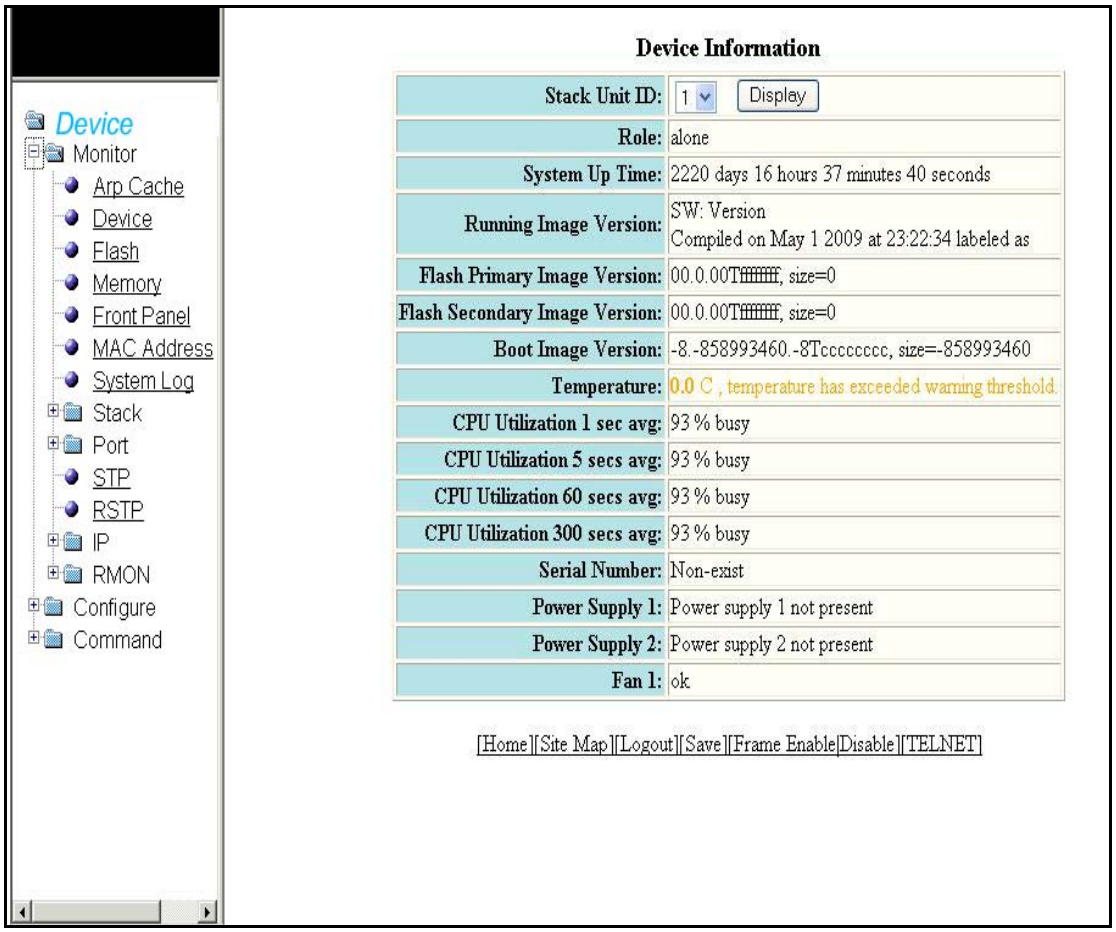
The ARP Cache display contains the following information.

Node	The IP address of the device.
MAC Address	The MAC address of the device.
Type	The type, which can be one of the following: • Dynamic – The Layer 3 Switch learned the entry from an incoming packet. • Static – The Layer 3 Switch loaded the entry from the static ARP table when the device for the entry was connected to the Layer 3 Switch.
Age	The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the cache. **NOTE:** Static entries do not age out.
Port	The port attached to the device for which the entry was made. For dynamic entries, this is the port on which the entry was learned.
VLAN ID	The port-based VLAN that contains this (instance of) spanning tree. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.

Monitoring the device

Select **Monitor > Device** to view the device information table.

FIGURE 8 Monitoring the device Information



Click **Display** and select the unit to view the information for any device in an IronStack

The **Device Information** display contains the following information.

Stack Unit ID	Number of the unit within a stack (1-8).
Role	Active, Standby, or Member.
System Up Time	Amount of time the system has been running since the last reboot.
Running Image Version	Software version currently running and some details on the version.
Flash Primary Image Version	Release number and size of the software loaded on the primary flash.
Flash Secondary Image Version	Release number and size of the software loaded on the secondary flash.
Boot Image Version	Release number and size of the boot image.

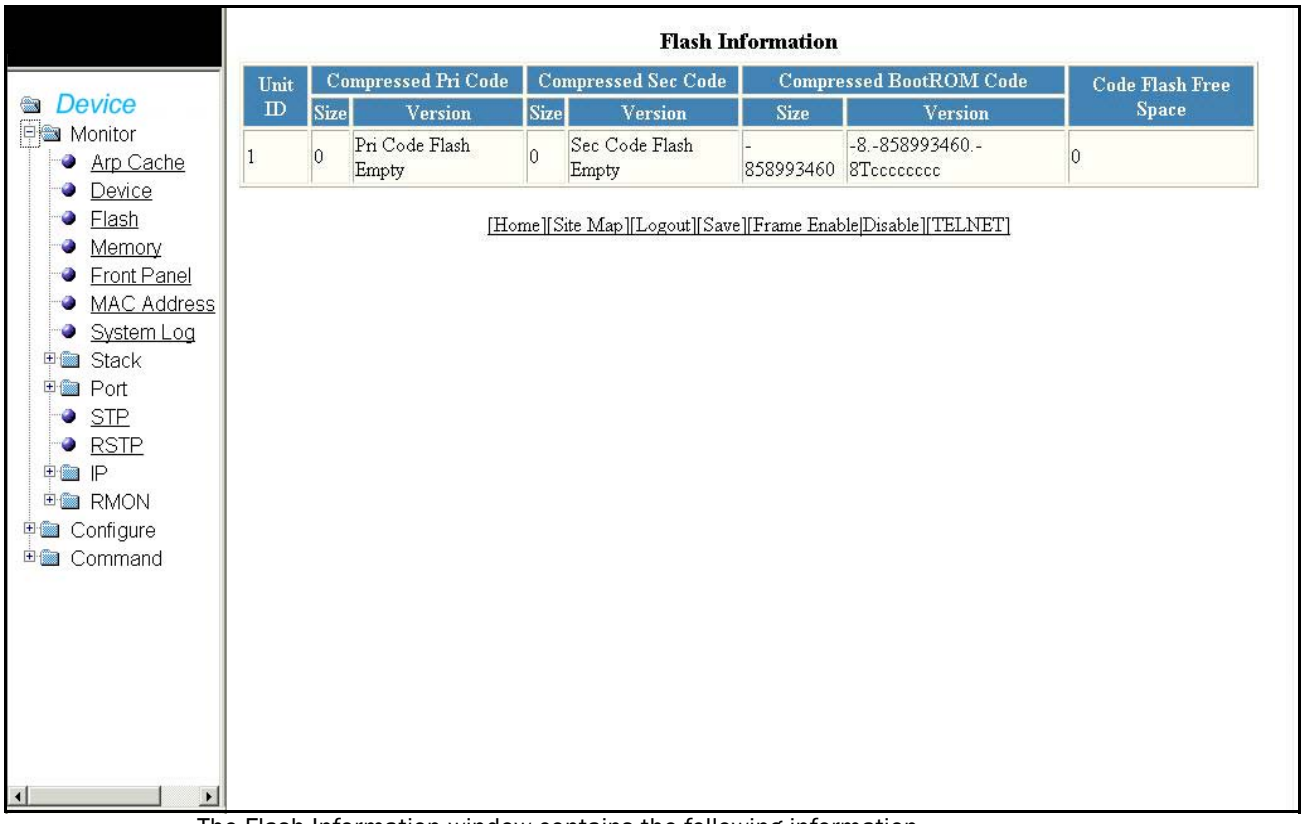
Temperature	In addition to the actual temperature, the color of the degrees provides a visual indicator for the device: • Green – The temperature is within the normal operating range. • Orange – The temperature has reached the warning level. • Red – The temperature has reached the shutdown level.
CPU Utilization	Percentage of CPU being used by the device.
Serial Number	The serial number of the device.
Power Supply 1	The status of the primary power supply.
Power Supply 2	The status of the secondary power supply, if present.
Fan (There is an entry for each fan in the device)	The status of the cooling fans.

Monitoring flash information

Stacking system behavior is defined by the runtime configuration, which is stored in a flash file called *startup-config.txt*. During bootup, the system reads and applies the *startup-config.txt* file to the runtime configuration.

Select **Monitor > Flash,** to view the flash information.

FIGURE 9 Monitoring the flash Information



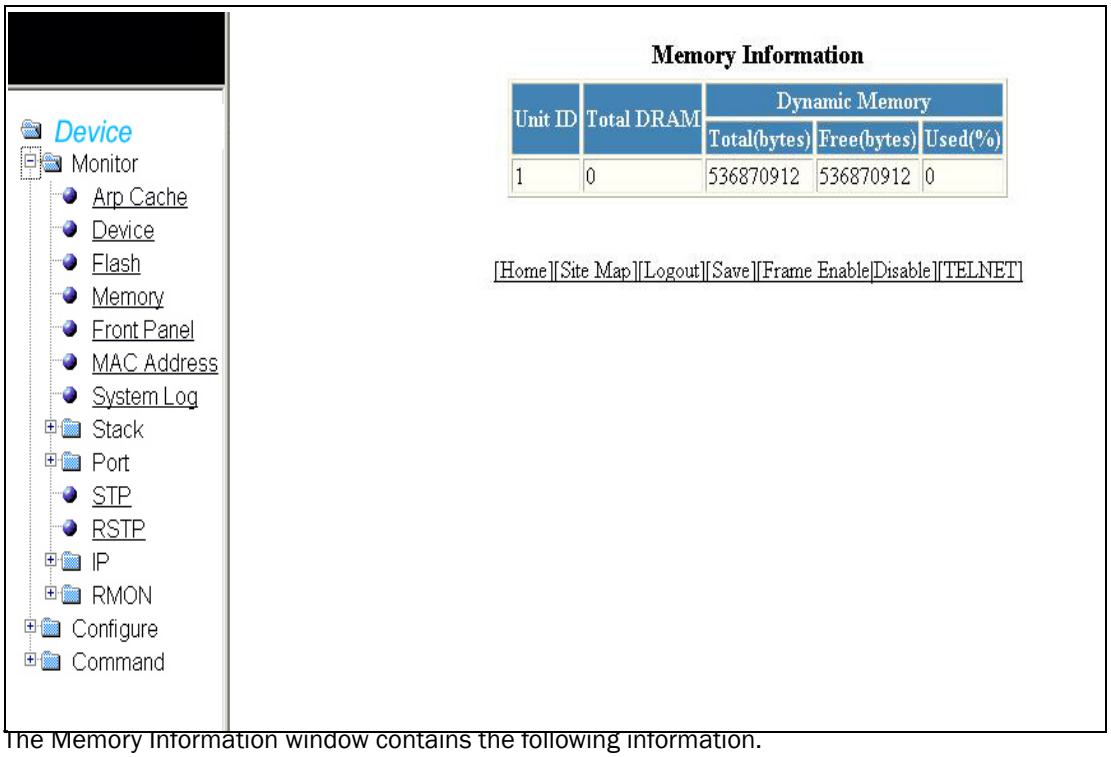
The Flash Information window contains the following information.

Unit ID	Number of the unit within a stack (1-8).
Compressed Primary Code	The compressed size, version, and image name for the Primary Code.
Compressed Secondary Code	The compressed size, version, and image name for the Secondary Code.
Compressed Boot ROM Code	The compressed size and version for the BootROM Code.
Code Flash Free Space	The amount of available free space on the Flash memory.

Monitoring memory information

Select **Monitor > Memory**, to view the memory information.

FIGURE 10 Monitoring the memory Information



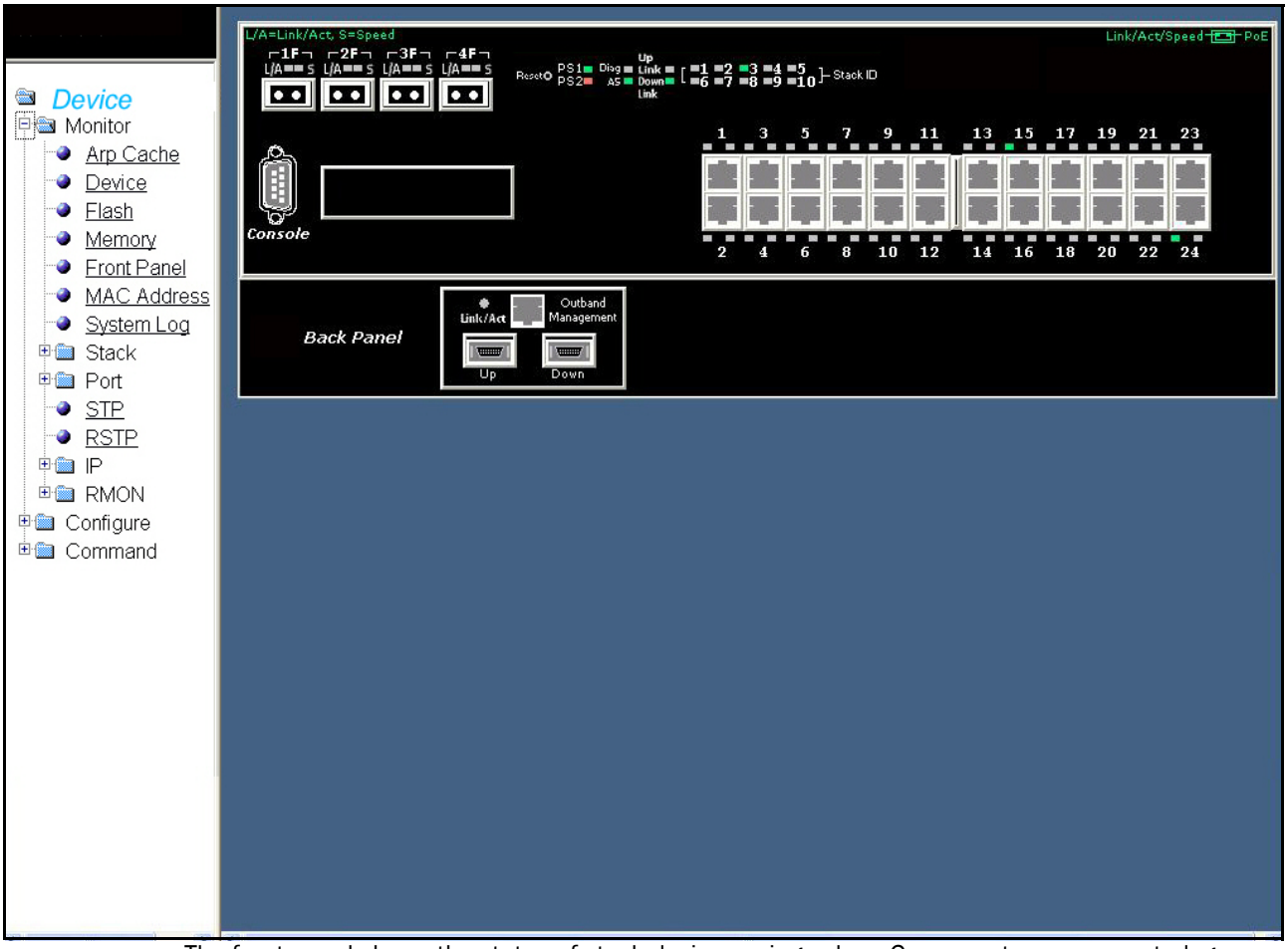
The Memory Information window contains the following information.

Unit ID	Number of the unit within a stack (1-8).
Total DRAM	The size (in bytes) of DRAM.
Dynamic Memory	The total number of bytes in dynamic memory, including the number of bytes that are available (free, or unused), and the percentage of memory used.

Monitoring the front panel

A display of the front and rear panels of device in an IronStack allows you to view the modules in each device and the ports within each module. Select **Monitor > Front Panel** to view the front and rear panels for all stack units.

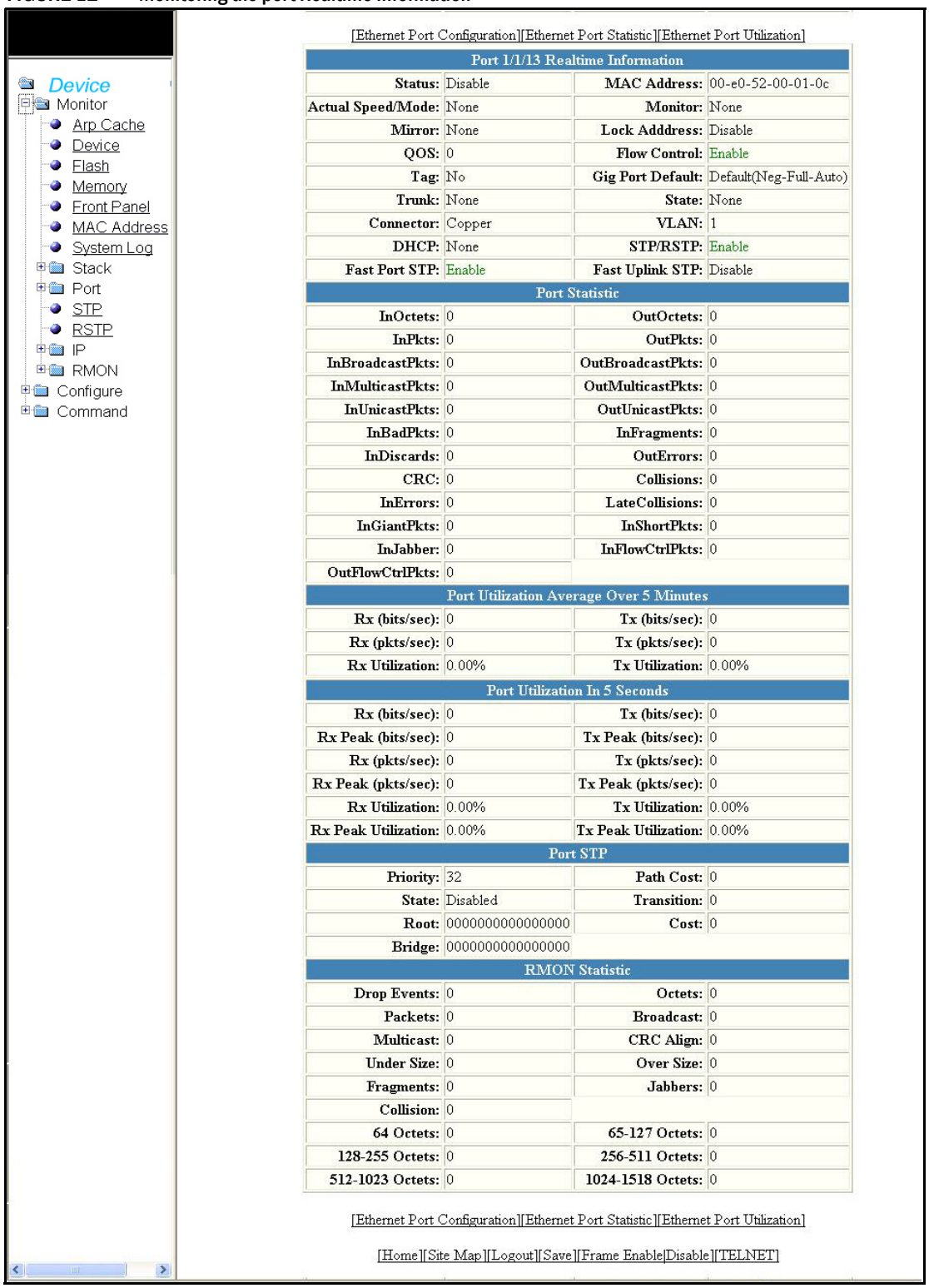
FIGURE 11 PowerConnect B-Series FCX Front panel



The front panel shows the status of stack devices using colors. Green ports are connected, gray ports are not connected.

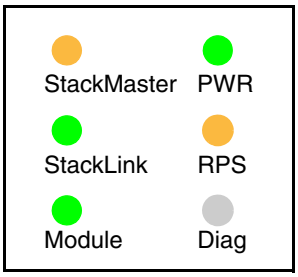
Stacking ports of the same color on two units are connected with stacking cables. For example, the green ports on the second and third devices are connected. A gray uplink port is not connected to anything. Click anywhere within a device will open the information for that particular device. Select **Monitor > Device** to view the details. For more information, refer to "Monitoring the device" on page 9. Click on any port will open the realtime Port Information for that port. The next illustration shows realtime port information.

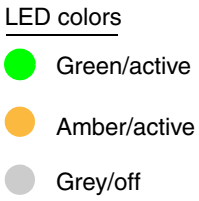
FIGURE 12 Monitoring the port Realtime Information



Status LED display

- The status LEDs that appear on the front panel provides information about system activity.





Active Controller (Device role in the stack)	• Green – Active Controller. • Amber – Standby Controller. • Off – Stack Member.
StackLink	• Green – Both stacking physical links are active. • Amber – One stacking physical link is active. • Off – None of stacking ports are active.
Module	• Green – Both stacking 10Gb modules are present. • Amber – One stacking 10Gb module is present. • Off – No stacking 10Gb module.
PWR (Power)	• Green – Power is on. • Amber - Power supply failure. • Off – Power is off.
RPS (Redundant Power Supply)	• Green – RPS is operational (the main supply, power is unplugged). • Amber – RPS is standby (the main supply power is on). • Gray – RPS is not plugged in.
Diag (Diagnostics)	• Green – Manufacturing diagnostics are in progress. • Off – No manufacturing diagnostics.

Monitoring MAC addresses

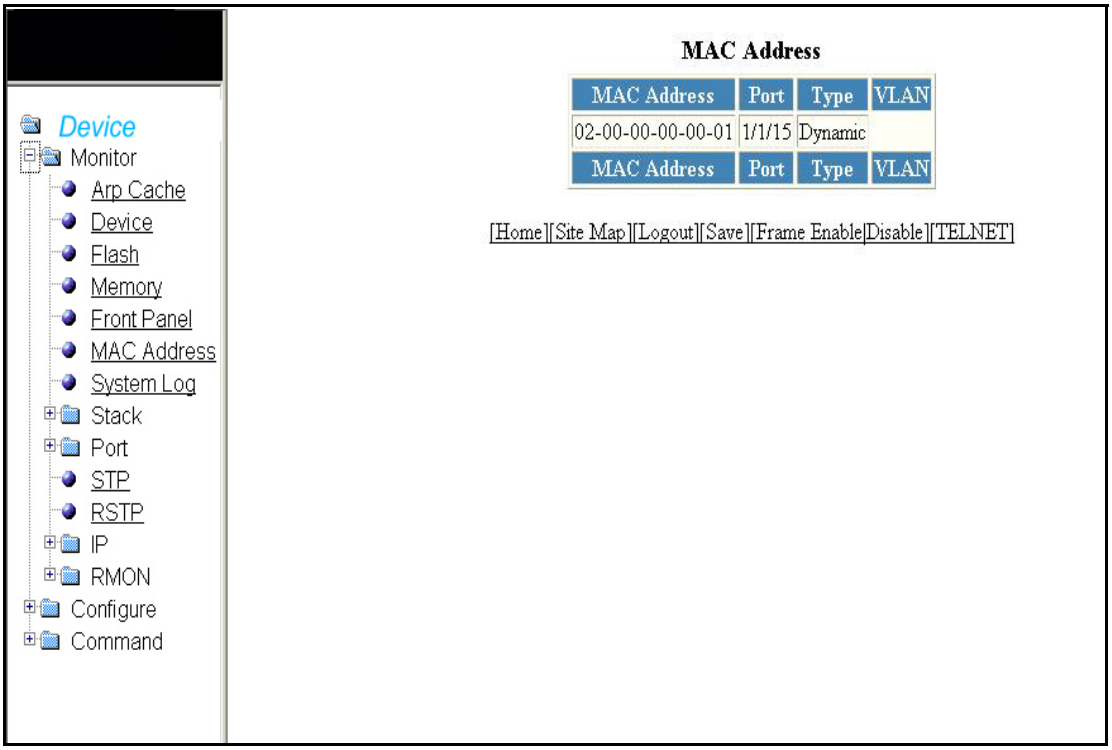
The Media Access Control (MAC) Address table contains a list of addresses that have been learned by the device. A MAC address is a unique identifier assigned to most network adapters or NICs, usually encoded with the manufacturer's registered ID number. MAC addresses appear in the format xx-xx-xx-xx-xx-xx.

The stack is identified in the network by a single MAC address, usually the MAC address of the Active Controller (the default). If a new Active Controller is elected, the MAC address of the new Active Controller (by default) becomes the MAC address for the entire stack. However, you can manually configure your stack to use a specified MAC address.

In a stack, the managing MAC address is generated by the software, and it is always the MAC address of the Active Controller first port. This ensures that the managing MAC address remains consistent across stack reboots, and helps prevent frequent topology changes as a result of protocol enabling and disabling, and configuration changes.

Select **Monitor > MAC Address**, to view the MAC Address details.

FIGURE 13 Monitoring the MAC Address



Click **Next Page** to view the remaining entries of the MAC address details.

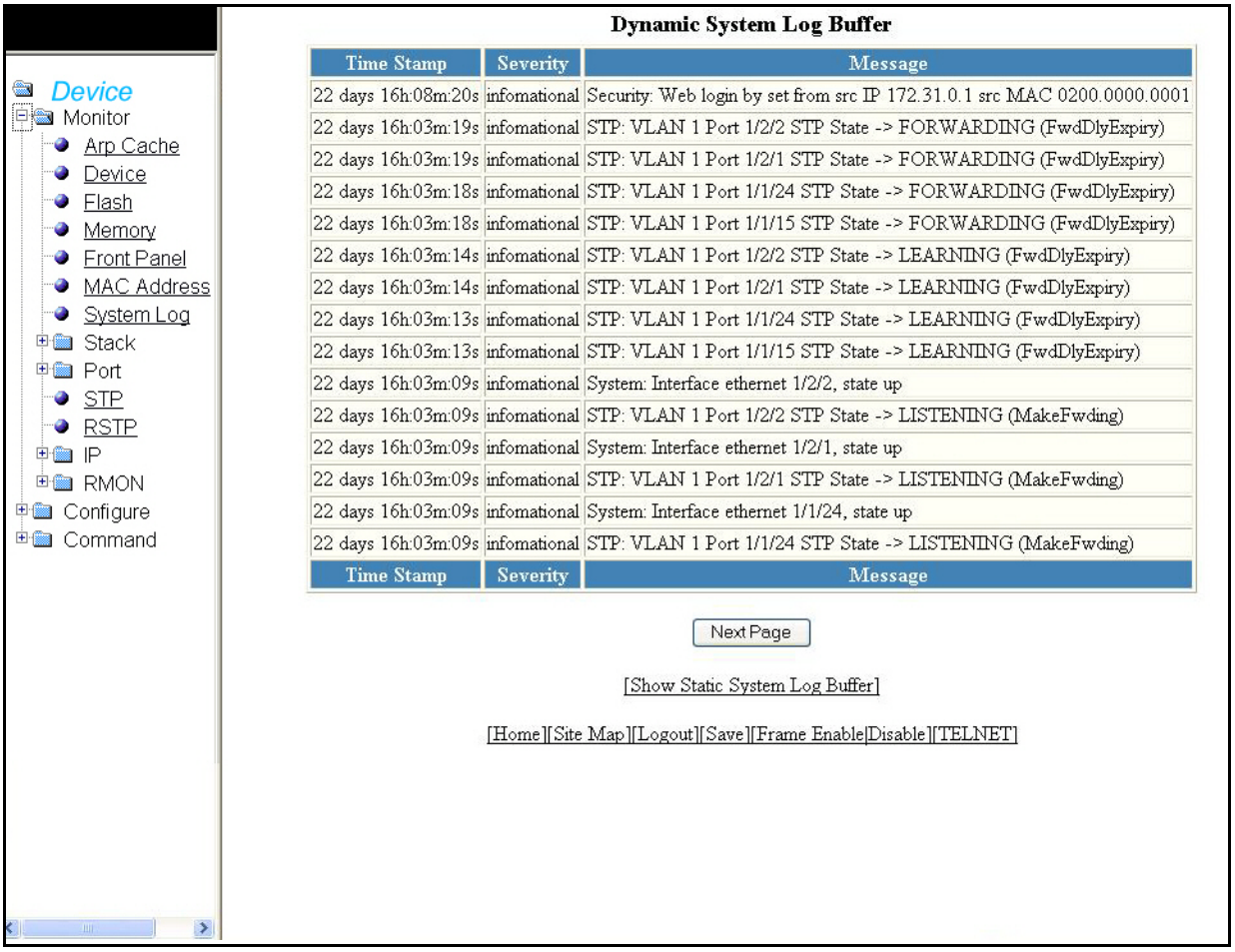
The MAC Address window contains the following information.

MAC Address	The MAC address of the device.
Port	The port attached to the device for which the entry was made. For dynamic entries, this is the port on which the entry was learned.
Type	The type, which can be one of the following: • Dynamic – The MAC address changes if the Active Controller changes. • Static – The MAC address will not change if the Active Controller changes.
VLAN	The port-based VLAN that contains this (instance of) spanning tree. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.

Monitoring the system log

Select **Monitor > System Log** to view the current information in the System Log Buffer.

FIGURE 14 Monitoring the dynamic system log buffer



Click **Next Page** to view the remaining information of the Dynamic System Log Buffer.

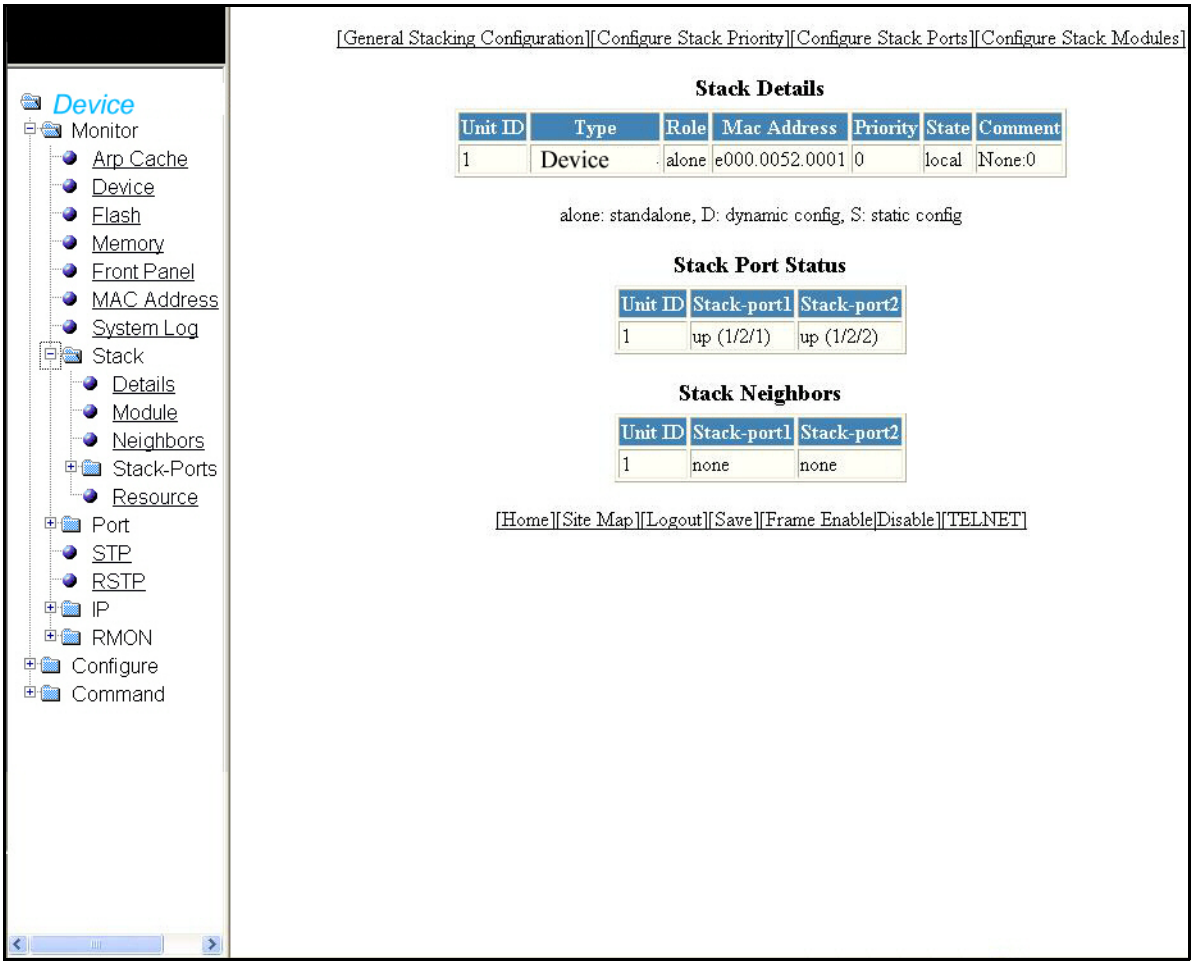
The Dynamic System Log Buffer contains the following information.

Time Stamp	The system uptime in DD:HH:MM:SS or the actual time if the date and time was set.
Severity	The Severity of the event.
Message	A description of the event.

Monitoring stack details

Select **Monitor > Stack > Details** to view current detailed stack information.

FIGURE 15 Monitoring stack details



The Stack Details window contains the following information. You can also view Stack Port Status and Stack Neighbors details in this window. Stack Details includes the following information.

Unit ID	Defines the number of the unit within the stack.
Type	Device model.
Role	The role of this unit within the stack: Active, Standby, or Member.
MAC Address	The MAC address of the device.
Priority	The priority assigned to this unit.
State	Local or Remote.

Comment	Additional information about this unit.
Alone	Indicates the device is operating as a standalone device.
D	Dynamic configuration. The configuration for this unit is dynamic and may be overwritten by a new stack unit. To change to a static configuration, enter the **write memory** command.
S	Static configuration. The configuration for this unit is static (has been saved with a **write memory** command).

The Stack Port Status includes the following information.

Unit ID	Defines the number of the unit within the stack.
Stack-port1	Indicates the port state and identifies the port by number (stack-ID or slot or port). Port states are: • Up - Each end is connected. • Down - Port is configured as a stacking port, but not connected. • None - Port is not configured as a stacking port.
Stack-port2	Indicates the port state and identifies the port by number (stack-ID or slot or port). Port states are: • Up - Each end is connected. • Down - Port is configured as a stacking port, but not connected. • None - Port is not configured as a stacking port.

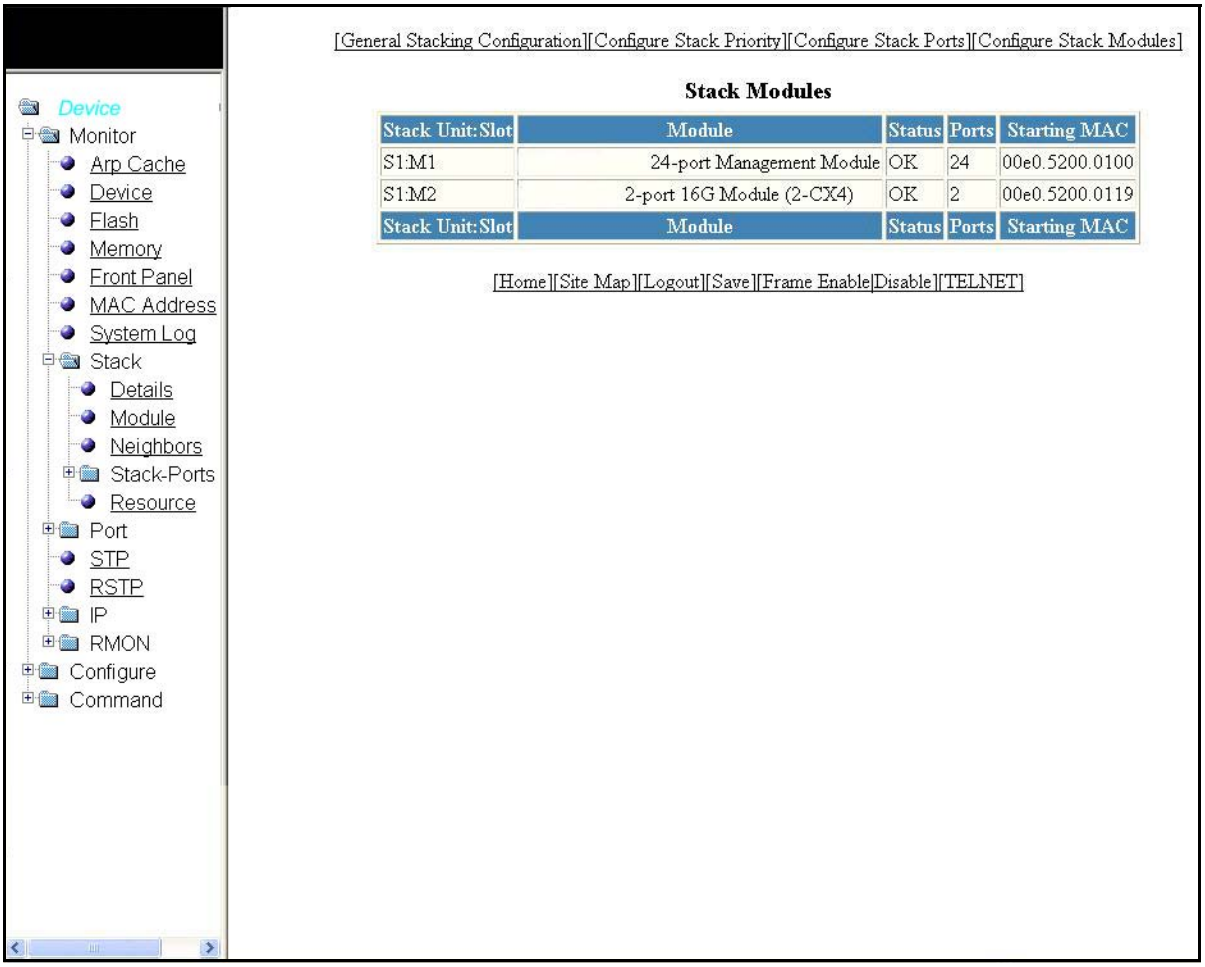
The Stack Neighbors includes the following information.

Unit ID	Defines the number of the unit within the stack.
Stack-port1	Identifies the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Identifies the neighbor stack unit for stack-port2 for this unit ID.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring a stack module

Select **Monitor > Stack > Module** to view current information about Stack Modules.

FIGURE 16 Monitor stack modules



The Stack Module contains the following information.

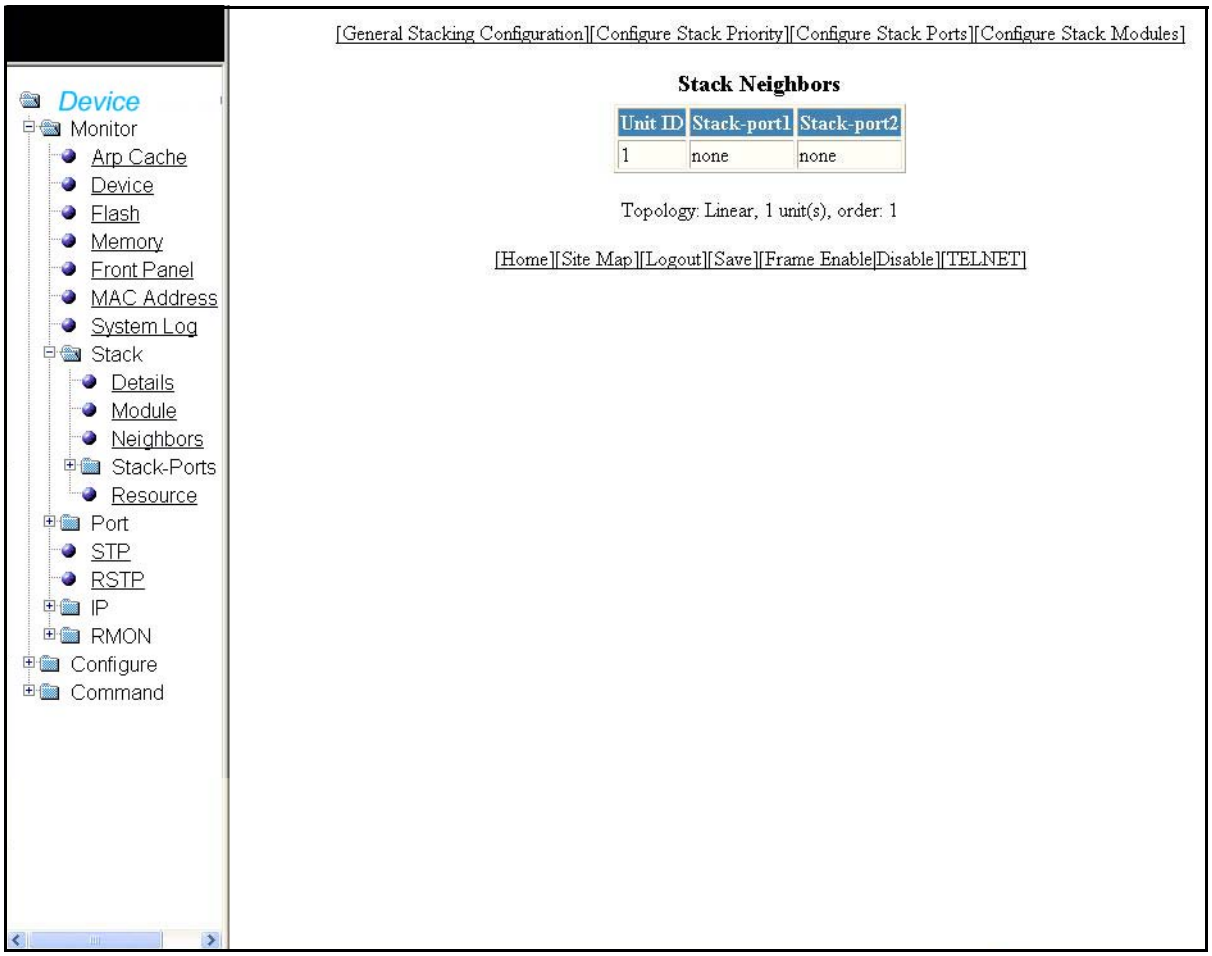
Stack Unit: Slot	Defines the number of the unit within the stack and the slot number.
Module	The device description.
Status	Status options are: • OK – The module came up and is operating normally. • CFG – The module is configured, but does not physically exist within the units of the stack.
Ports	The number of ports on the module.
Starting MAC	The MAC address of the module.

General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring stack neighbors

Select **Monitor > Stack > Neighbors** to view current information about Stack Neighbors.

FIGURE 17 Monitoring stack neighbors



The Stack Neighbors contains the following information.

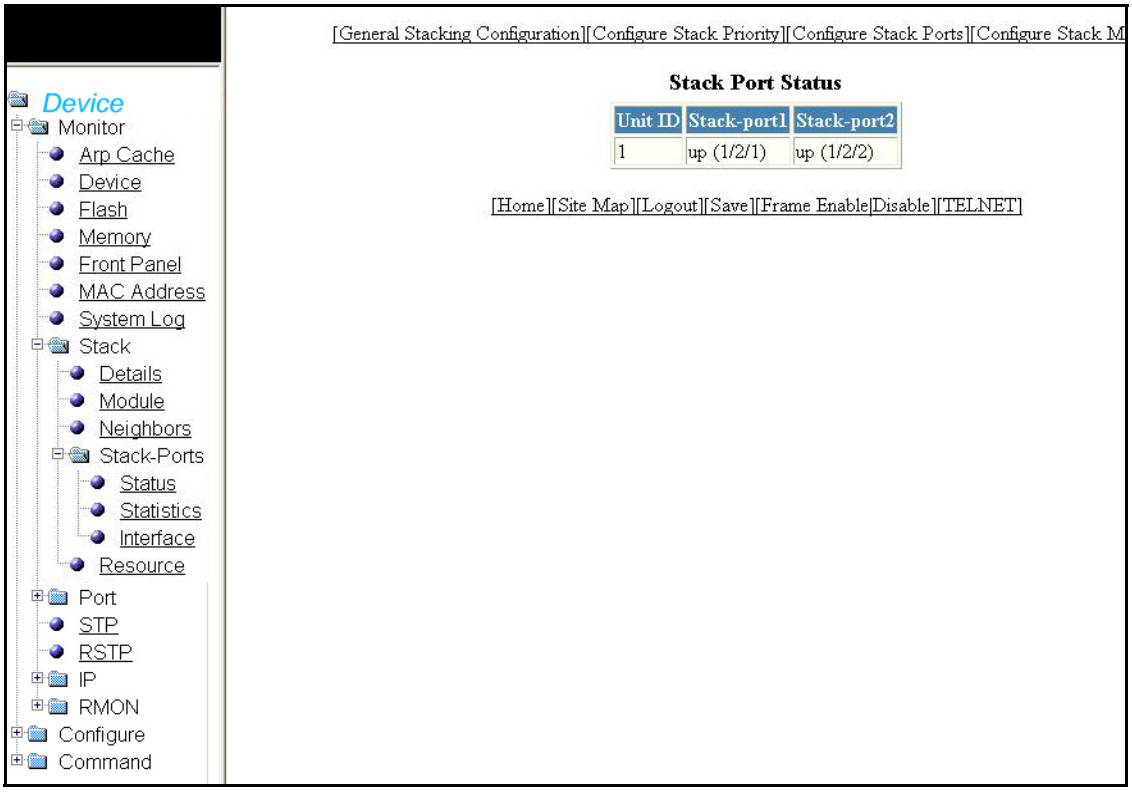
Unit ID	Identifies the number of the unit within the stack.
Stack-port1	Identifies the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Identifies the neighbor stack unit for stack-port2 for this unit ID.
Topology	Shows either Linear or Ring.

Units	The number of units within the stack.
Order	The order of the unit IDs within the stack.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring stack ports status

Select **Monitor > Stack > Stack-Ports > Status** to view information about the status of Stack Ports.

FIGURE 18 Monitoring stack port status



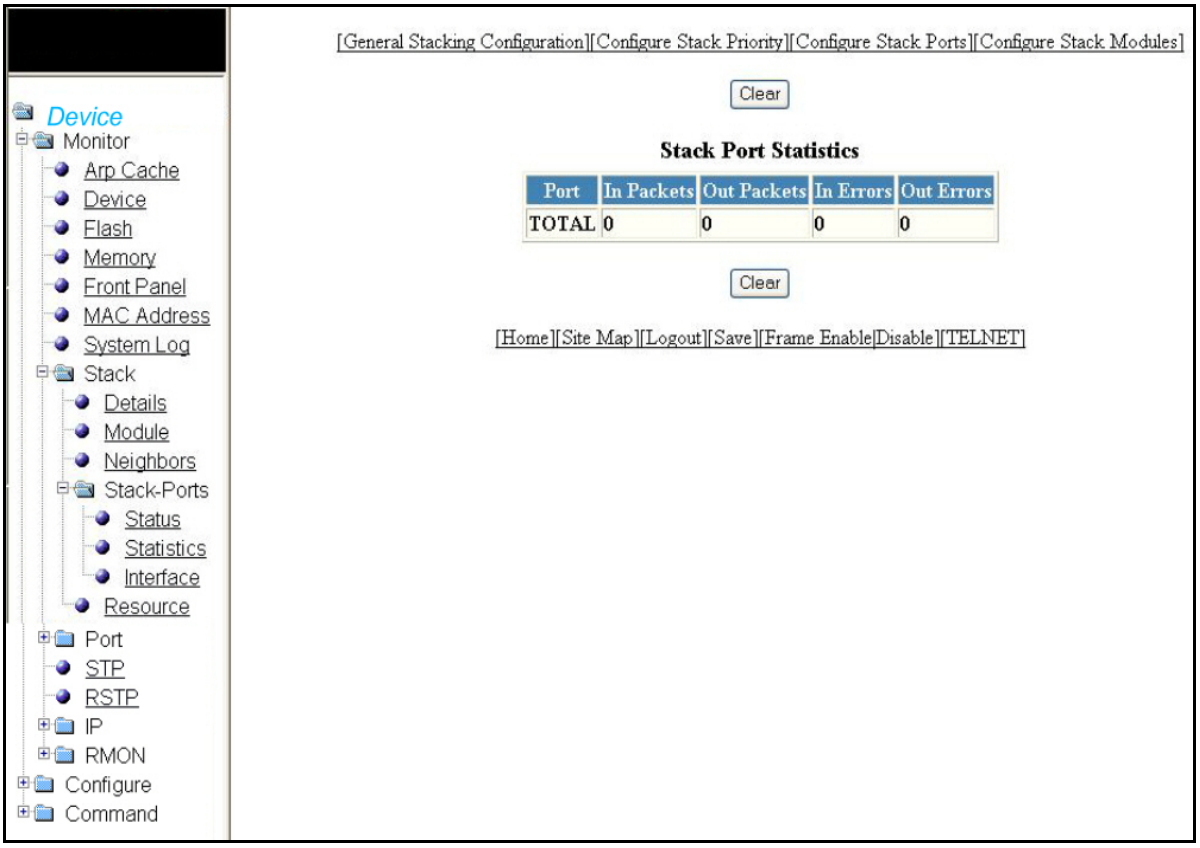
The Stack Port Status contains the following information.

Unit ID	Defines the number of the unit within the stack.
Stack-port1	Indicates the port state and identifies the port by number (stack-ID or slot or port). Port states are: • Up - Each end is connected. • Down - Port is configured as a stacking port, but not connected. • None - Port is not configured as a stacking port.
Stack-port2	Indicates the port state and identifies the port by number (stack-ID or slot or port). Port states are: • Up - Each end is connected. • Down - Port is configured as a stacking port, but not connected. • None - Port is not configured as a stacking port.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring stack port statistics

Select **Monitor > Stack > Stack-Ports > Statistics** to view current Stack Port Statistics,.

FIGURE 19 Monitoring stack port statistics



The Stack Port Statistics contains the following information.

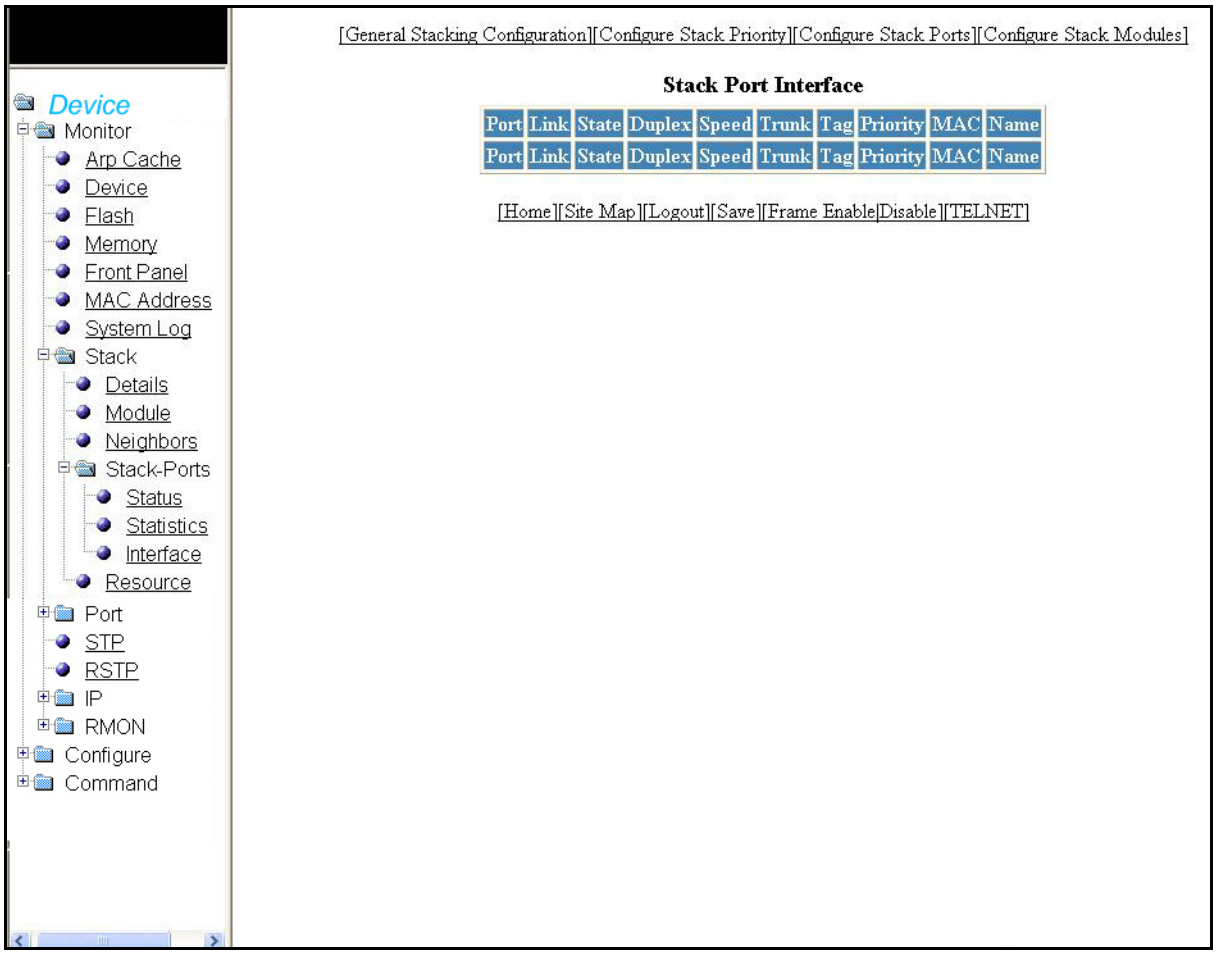
Port	The stack identification number for this port.
In Packets	The number of incoming packets on this port.
Out Packets	The number of outgoing packets on this port.
In Errors	The number of errors on the incoming packets on this port.
Out Errors	The number of errors on the outgoing packets on this port.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Click **Clear** to clear the information and begin a new monitoring cycle.

Monitoring stack port interfaces

Select **Monitor > Stack > Stack-Ports > Interface** to view current information about Stack Port Interfaces.

FIGURE 20 Monitoring stack port interfaces



The Stack Port Interfaces contains the following information.

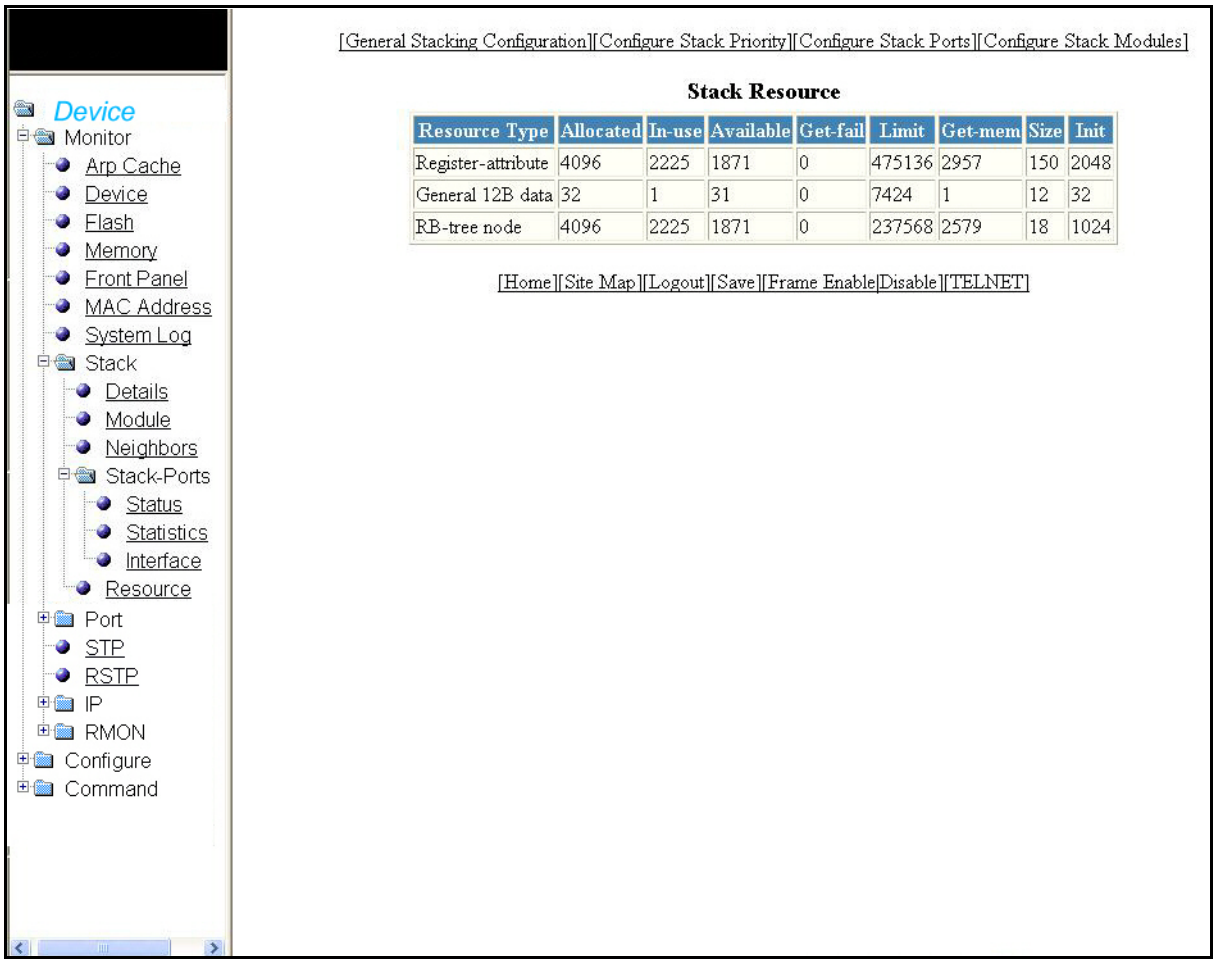
Port	The stack identification number for this port.
Link	Identifies the configuration for modules on this unit.
State	Indicates that a priority has been assigned to this stack unit.
Duplex	Indicates whether the port is configured as half or full duplex.
Speed	Indicates the port speed.
Trunk	Indicates whether the port is part of a trunk.
Tag	Indicates whether the port is tagged or untagged.
Priority	Port priority.
MAC	The MAC address of the port.

Name	An optional name assigned to the port.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring stack resources

Select **Monitor > Stack > Resource** to view current information about Stack Resources.

FIGURE 21 Monitoring stack resources



The Stack Resources contains the following information.

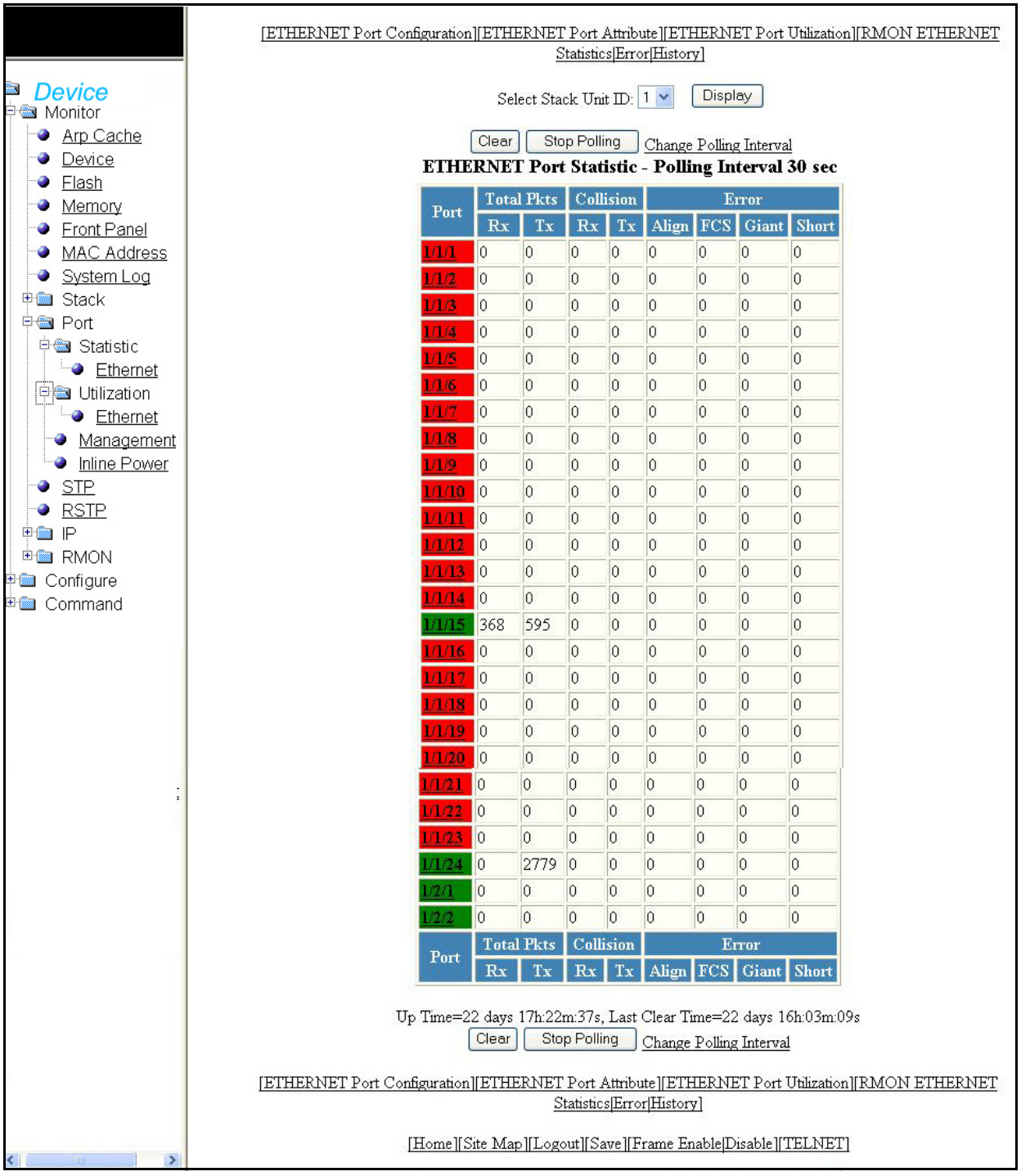
Resource Type	Identifies the specific resource.
Allocated	The number of entries that the system has allocated.
In-use	The number of entries being used by the application.
Available	The number of available entries.
Get-fail	The number of entries out of resources.
Limit	The maximum number of entries the system could allocate.
Get-mem	The number of entries that require more memory.
Size	The size, in bytes, or each entry.
Init	The initial number of allocated entries.
General Stacking Configuration	Allows you to configure the general stacking configuration.
Configure Stack Priority	Allows you to configure the stack unit priority.
Configure Stack Port	Allows you to configure the stack port.
Configure Stack Modules	Allows you to configure the stack modules.

Monitoring Ethernet port statistics

The Ethernet Port Statistics lists the total packets, number of collisions, and number of errors that have occurred on a port.

Select **Monitor > Port > Statistic > Ethernet** to view the information.

FIGURE 22 Monitoring ETHERNET Port Statistic



The Ethernet Port Statistics contains the following information.

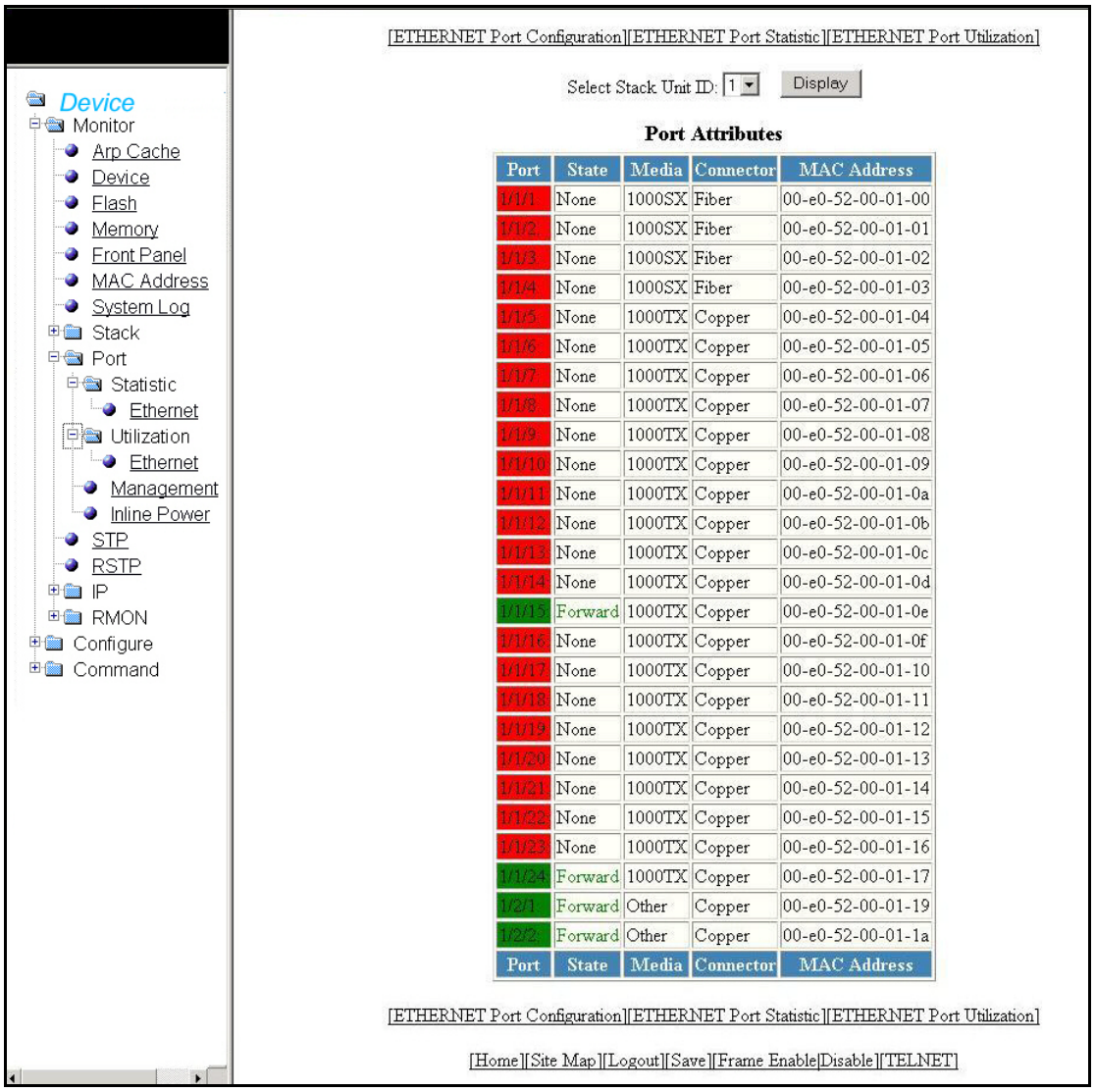
Port	Port ID for which the statistics was collected.
Total Packets	Shows the total number of packets received (RX) and transmitted (TX) on the port.
Collision	Shows the number of RX and TX collisions on the port.
Error	Shows the number of the following types of errors on the port: • Alignment – Packets with frame alignment errors. • FCS – Packets with Frame Check Sequence errors. • Giant – Packets that were longer than the configured MTU. • Short – Packets that were shorter than the minimum valid length.
Select Stack Unit ID	View information about a specific stack unit by selecting the unit ID number from the drop-down list and clicking Display.
Clear	Click Clear to remove the current data and restart the monitoring process.
Stop Polling	Click Stop Polling to stop the polling process.
Change Polling Interval	Change the current polling interval.
Ethernet Port Configuration	Displays the Ethernet port configuration details.
Ethernet Port Attribute	Displays the Ethernet port attribute details.
Ethernet Port Utilization	Displays the Ethernet port utilization details.
RMON Ethernet Statistics Error	Displays the RMON Ethernet Statistics Error details.
RMON Ethernet Statistics History	Displays the RMON Ethernet Statistics History details.

Monitoring port attribute

The Ethernet port attribute shows the port, state, media, connector, and MAC Address of the port.

Select **Monitor > Port > Statistic > Ethernet** to view the information.

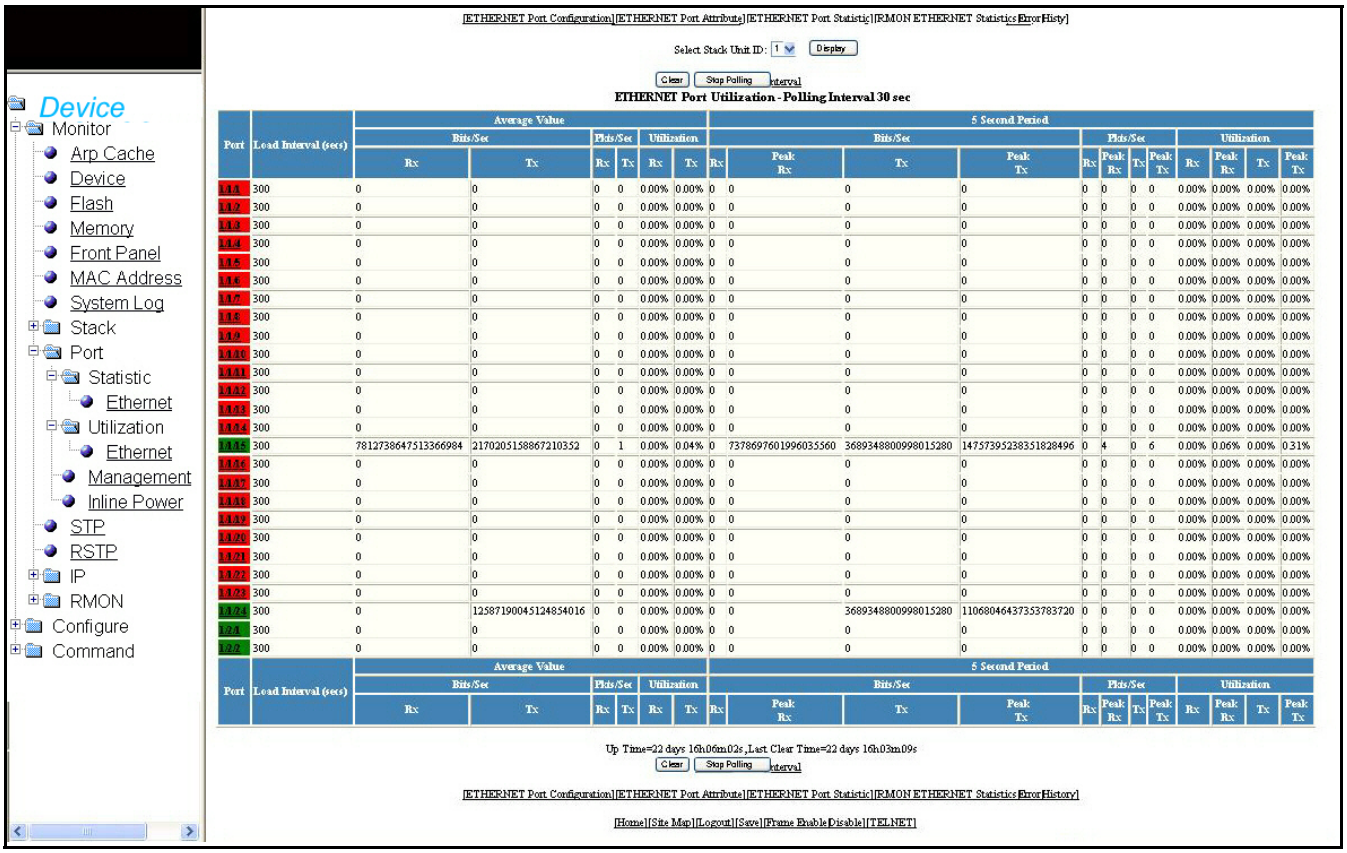
FIGURE 23 Monitoring Ethernet Port attributes



Monitoring port utilization

The Port Utilization display shows the traffic that is received and transmitted on a port. To view the Port Utilization information, select **Monitor > Port > Utilization > Ethernet**. If interface options are available, select the interface type, for example **Ethernet,** to show the Port Utilization display.

FIGURE 24 Monitoring ETHERNET Port Utilization



The Port Utilization contains the following information.

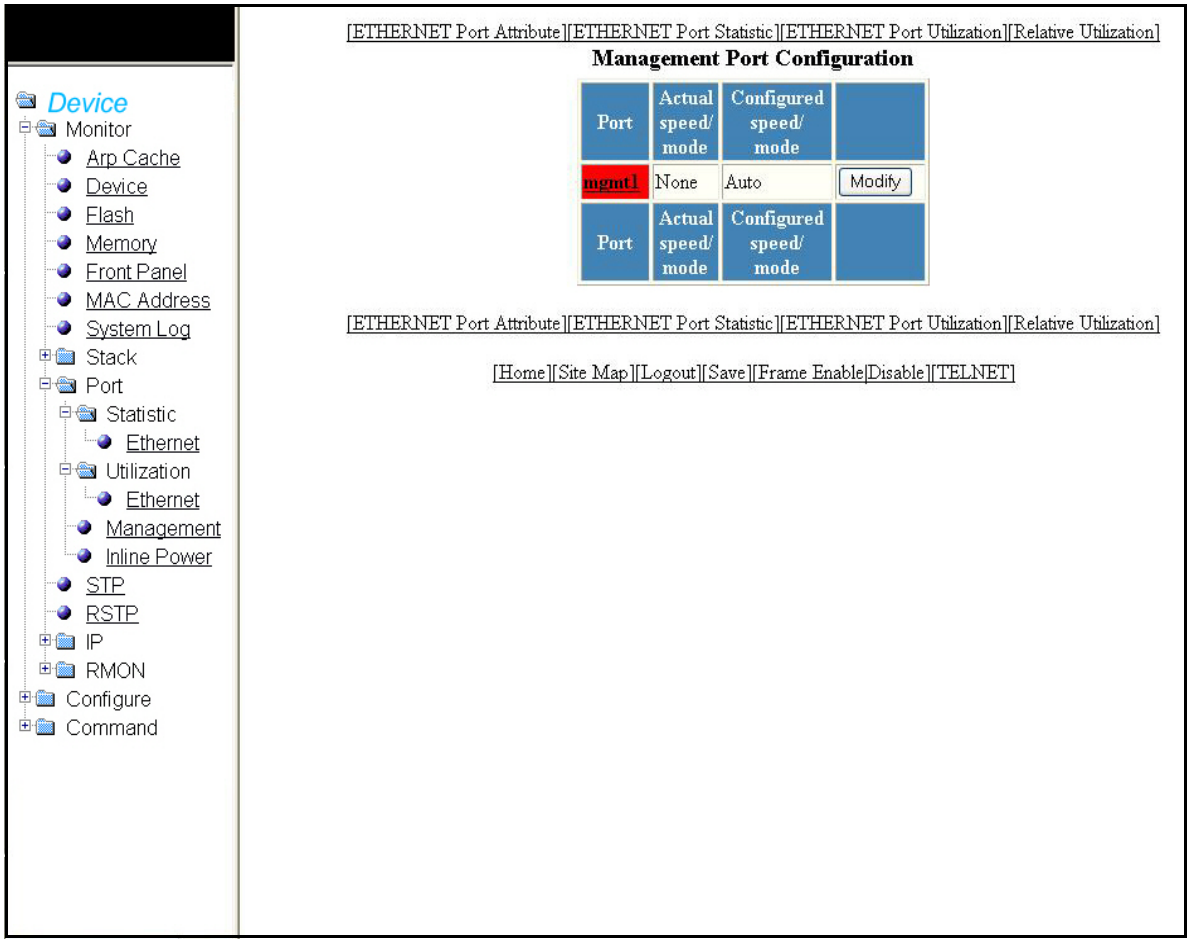
Port	Number of the port. Each entry has a link to detailed information about the port.
Load Interval (secs)	The number of seconds for which average port utilization should be calculated. This object can have a value from 30 to 300, in 30 second increments. The default: 300 seconds.
Average Value	This set of columns shows the following: • Bits/Sec – The average number of bits per second received and transmitted on the port. • Pkts/Sec – The average number of packets per second received and transmitted on the port. • Utilization – The average percent utilization received and transmitted on the port.
5 Second Period	This set of columns show the bits per second, packets per second, and utilization percentages received and transmitted on a port at each 5 second interval. Peak activities for each category are also provided.

Select Stack ID	Use the drop-down box to select the ID number of the stack unit you want to view, then click Display.
Clear	Click clear to remove the current data and restart the monitoring process.
Stop Polling	Click Stop Polling to stop the statistics polling process.
Change Polling Interval	Click Change Polling Interval to change the interval at which the polling occurs.
Ethernet Port Configuration	Displays the Ethernet port configuration details.
Ethernet Port Attribute	Displays the Ethernet port attribute details.
Ethernet Port Utilization	Displays the Ethernet port utilization details.
RMON Ethernet Statistics Error	Displays the RMON Ethernet Statistics Error details.
RMON Ethernet Statistics History	Displays the RMON Ethernet Statistics History details.

Monitoring the management port

Select **Monitor > Port > Management** to view the current management port configuration details.

FIGURE 25 Monitoring management port configuration

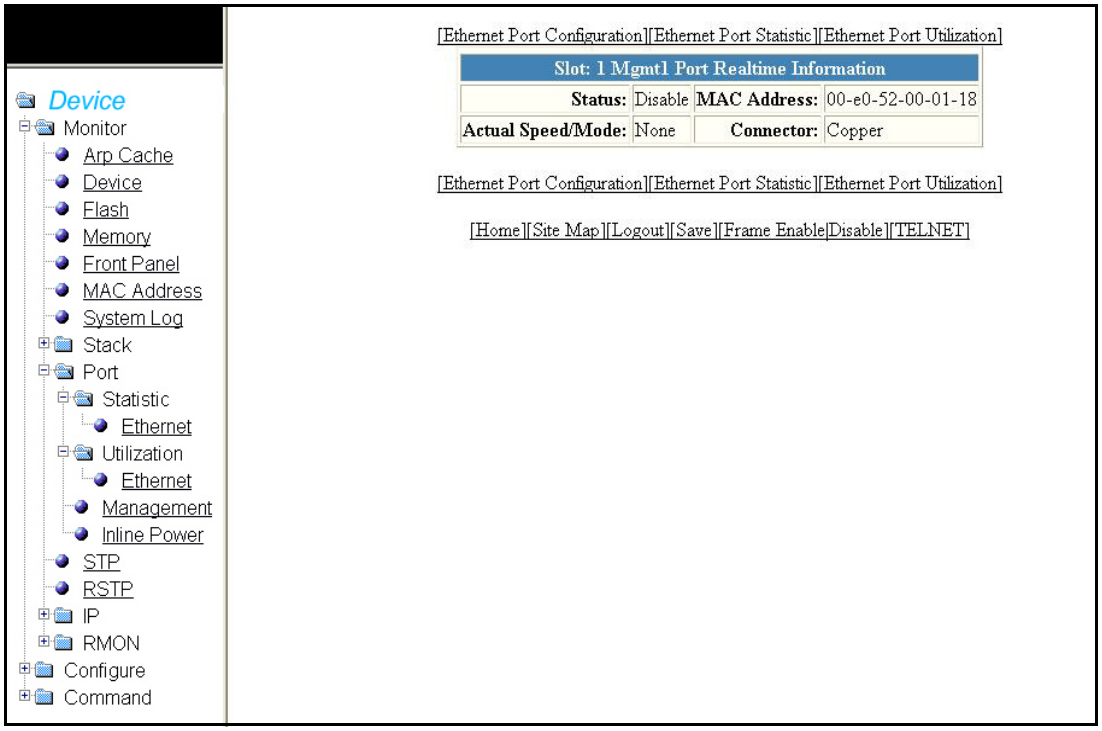


The Management Port Configuration contains the following information.

Port	Name of the management port. Each entry has a link to detailed realtime information about the port.
Actual speed mode	Shows whether the actual speed matches the configured speed. If the configured speed is set to Auto, then the speed is provided.
Configured speed mode	The speed duplex set for the port.
Modify	Allows you to configure a management port or change the configuration of a current management port.

Click on any of the management port will open the realtime information for that port.

FIGURE 26 Monitor - Management port realtime information



The realtime management port contains the following information.

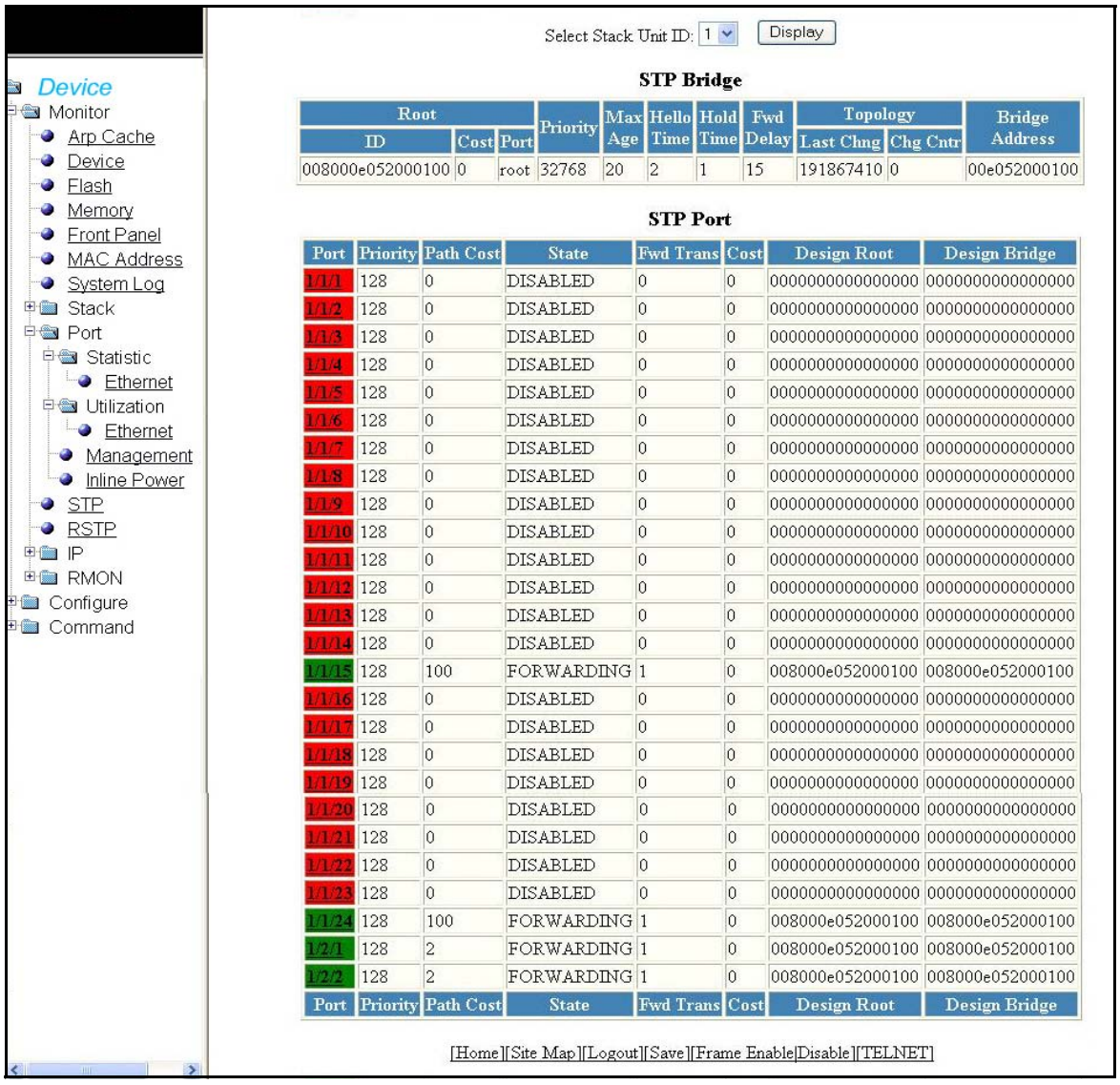
Status	The status of the port.
MAC Address	The MAC address of the port.
Actual Speed/Mode	Shows whether the actual speed matches the configured speed. If the configured speed is set to Auto, then the speed is provided.
Connector	The physical type of connector.

Monitoring STP

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, you can configure based on global (bridge) and local (port) parameters. PowerConnect devices support standard STP as described in the IEEE 802.1D specification.

To view current STP information for a stack unit, select **Monitor > STP**. From the STP display, select stack unit ID from the drop-down list, and click **Display**. The following information appears.

FIGURE 27 Monitoring the STP Bridge



STP Bridge

Root			Priority	Max Age	Hello Time	Hold Time	Fwd Delay	Topology		Bridge Address
ID	Cost	Port						Last Chng	Chg Cntr	
008000e052000100	0	root	32768	20	2	1	15	191867410	0	00e052000100

STP Port

Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge
1/1/1	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/2	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/3	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/4	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/5	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/6	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/7	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/8	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/9	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/10	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/11	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/12	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/13	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/14	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/15	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/1/16	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/17	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/18	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/19	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/20	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/21	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/22	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/23	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/24	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/1	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/2	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge

The STP contains the following information.

STP Bridge Parameters (global parameters)	
Root ID	The ID assigned by STP to the root bridge for this spanning tree.
Root Cost	The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.
Root Port	The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number.
Priority	This device or VLAN’s STP priority. The value is shown in hexadecimal format.
Max Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time	The interval between each configuration BPDU sent by the root bridge.
Hold Time	The minimum number of seconds that must elapse between transmissions of consecutive Configuration BPDUs on a port.
Forward Delay	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Topology Last Change	The number of seconds since the last time a topology change occurred.
Topology Change Counter	The number of times the topology has changed since this device was reloaded.
Bridge Address	The STP address of this device or VLAN.
STP Port Parameters	
VLAN	The VLAN that the port is in. This field appears only when port VLAN is enabled.
Port	The port number.
Priority	The port’s STP priority, in hexadecimal format.
Path Cost	The port’s STP path cost.
State	The port’s STP state. The state can be one of the following: • **BLOCKING** – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • **DISABLED** – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • **FORWARDING** – STP is allowing the port to send and receive frames. • **LISTENING** – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No user frames are transmitted or received during this state. • **LEARNING** – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP’s reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.

Forward Transition	The number of times STP has changed the state of this port between BLOCKING and FORWARDING.
Cost	The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Design Bridge field.
Design Root	The root bridge as recognized on this port. The value is the same as the root bridge ID listed in the Root ID field.
Design Bridge	The designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge.

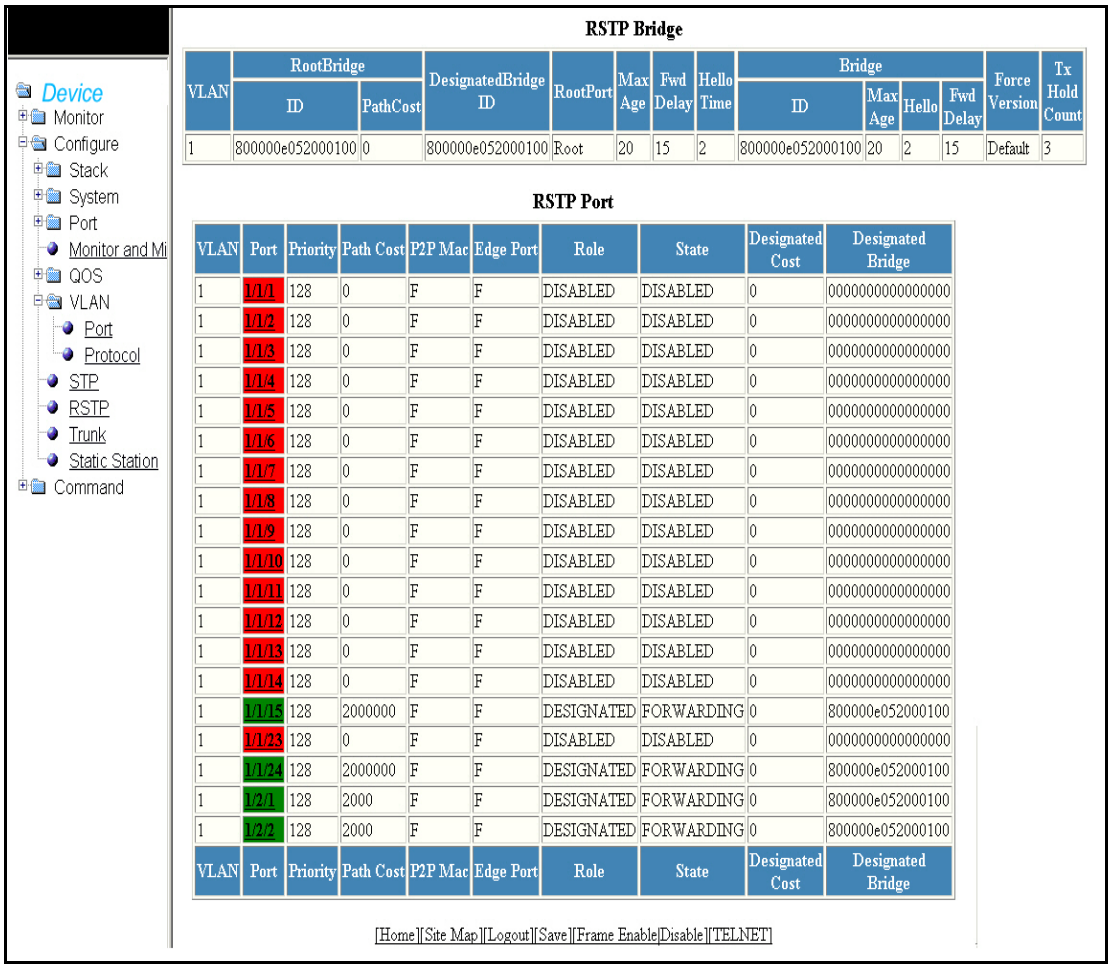
Monitoring RSTP

The Rapid Spanning Tree Protocol (RSTP 802.1W) feature provides rapid traffic reconvergence for point-to-point links within a few milliseconds (0 – 500 milliseconds), following the failure of a bridge or bridge port. This reconvergence occurs more rapidly than the reconvergence provided by the 802.1D Spanning Tree Protocol (STP)) or by RSTP Draft 3.

Configure RSTP before you view current RSTP information for a stack unit. For more information on how to configure RSTP, refer to "Configuring the RSTP bridge" on page 126.

After configuring RSTP select **Monitor > RSTP** to view the bridge and port details. Select stack unit ID from the drop-down list, and click **Display**. The following information appears.

FIGURE 28 Monitoring the RSTP bridge



RSTP Bridge

VLAN	RootBridge		DesignatedBridge ID	RootPort	Max Age	Fwd Delay	Hello Time	Bridge				Force Version	Tx Hold Count
	ID	PathCost						ID	Max Age	Hello	Fwd Delay		
1	800000e052000100	0	800000e052000100	Root	20	15	2	800000e052000100	20	2	15	Default	3

RSTP Port

VLAN	Port	Priority	Path Cost	P2P Mac	Edge Port	Role	State	Designated Cost	Designated Bridge
1	1/1/1	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/2	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/3	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/4	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/5	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/6	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/7	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/8	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/9	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/10	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/11	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/12	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/13	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/14	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/15	128	2000000	F	F	DESIGNATED	FORWARDING	0	800000e052000100
1	1/1/23	128	0	F	F	DISABLED	DISABLED	0	0000000000000000
1	1/1/24	128	2000000	F	F	DESIGNATED	FORWARDING	0	800000e052000100
1	1/2/1	128	2000	F	F	DESIGNATED	FORWARDING	0	800000e052000100
1	1/2/2	128	2000	F	F	DESIGNATED	FORWARDING	0	800000e052000100
VLAN	Port	Priority	Path Cost	P2P Mac	Edge Port	Role	State	Designated Cost	Designated Bridge

The RSTP bridge display contains the following information.

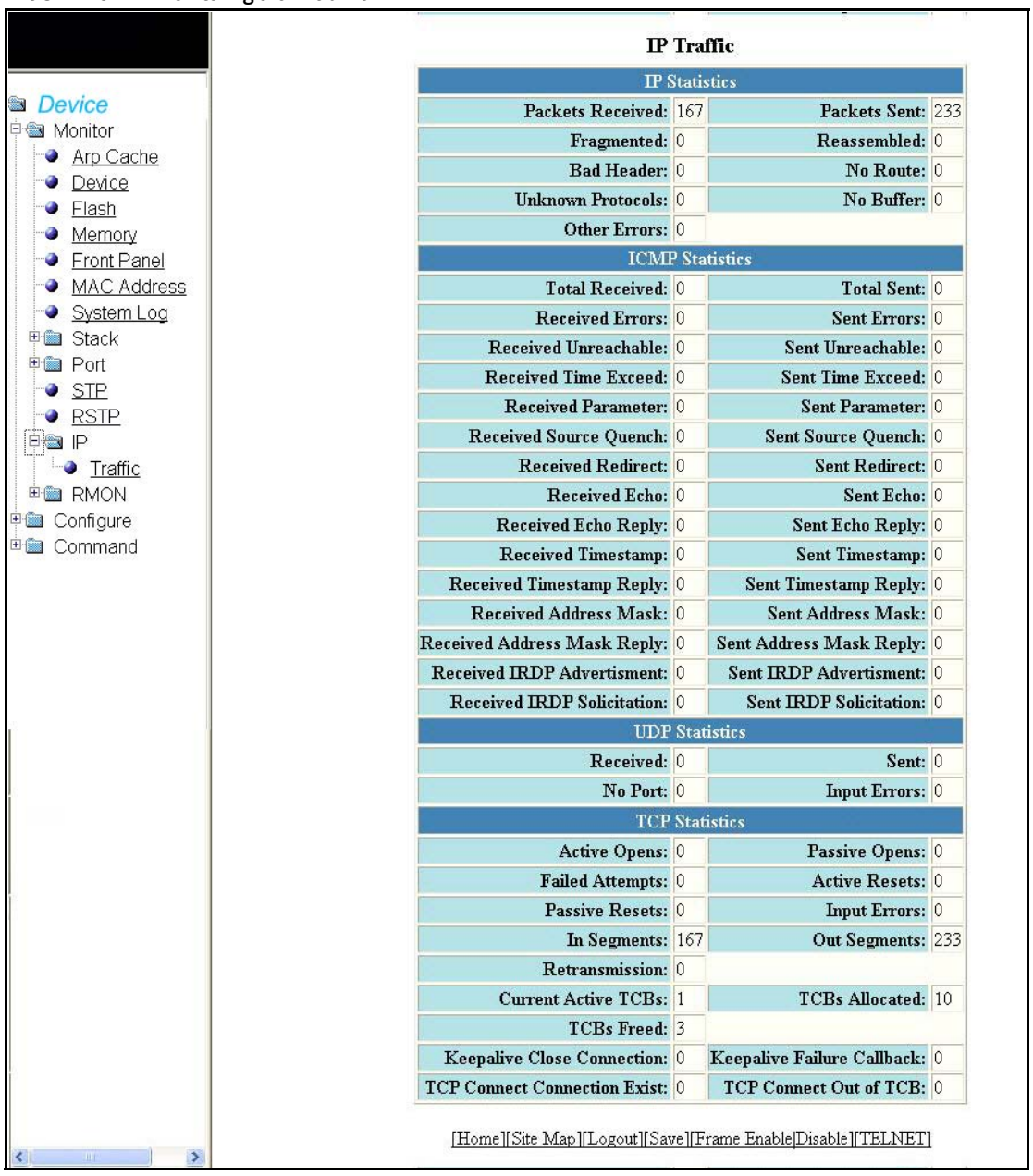
RSTP Bridge Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
RootBridge ID	The ID assigned by STP to the root bridge for this spanning tree.
RootBridge PathCost	The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.
DesignateBridge ID	The bridge from where the root information was received.It can be from the root bridge itself, but it could also be from another bridge.
Root Port	The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number.
Max.Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Fwd Delay	The number of seconds a non-edge Designated port waits until it can apply any of the following transitions, if the RST BPDU it receives does not have an agreed flag: • Discarding state to learning state • Learning state to forwarding state When a non-edge port receives the RST BPDU it goes into forwarding state within 4 seconds or after two hello timers expire on the port. Fwd Dly is also the number of seconds that a Root port waits for an RST BPDU with a proposal flag before it applies the state transitions listed above. If the port is operating in 802.1D compatible mode, then forward delay functionality is the same as in 802.1D (STP).
Hello Time	The interval between each configuration BPDU sent by the root bridge.
Bridge ID	The ID of the bridge
Bridge MaxAge	The configured max age for this bridge. The default is 20.
Bridge Hello	The configured hello time for this bridge.The default is 2.
Bridge Fwd Delay	The configured forward delay time for this bridge. The default is 15.
Force Version	The configured force version value. One of the following value is displayed: • 0 – The bridge has been forced to operate in an STP compatibility mode. • 2 – The bridge has been forced to operate in an 802.1W mode. (This is the default.)
Tx Hold Count	The number of BPDUs that can be transmitted per Hello Interval. The default is 3.
RSTP Port Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
Port	The port number.
Priority	The configured priority of the port. The default is 128 or 0x80.
Path Cost	The port’s STP path cost.
P2P Mac	Indicates if the point-to-point-mac parameter is configured to be a point-to-point link: • T – The link is configured as a point-to-point link. • F – The link is not configured as a point-to-point link. This is the default.

Edge Port	Indicates if the port is configured as an operational Edge port: • T – The port is configured as an Edge port. • F – The port is not configured as an Edge port. This is the default.
Role	The current role of the port: • Root • Designated • Alternate • Backup • Disabled For more information, refer to "Bridges and bridge port roles" of *PowerConnect B-Series FCX Configuration Guide*.
State	The port's STP state. The state can be one of the following: • BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • FORWARDING – STP is allowing the port to send and receive frames. • LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No user frames are transmitted or received during this state. • LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP's reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
Designated Cost	The best root path cost that this port received, including the best root path cost that it can transmit.
Designated Bridge	The ID of the bridge that sent the best RST BPDU that was received on this port.

Monitoring IP traffic

Select **Monitor > IP > Traffic** to view current IP statistics.

FIGURE 29 Monitoring the IP traffic



The IP Statistics contains the following information.

IP statistics	
Packets Received	The number of IP packets received by the device.
Packets Sent	The number of IP packets originated and sent by the device.
Packets Forwarded	The number of IP packets received from another device and forwarded by this device.
Filtered	The number of IP packets filtered by this device.
Fragmented	The number of IP packets fragmented by this device before sending or forwarding them.
Reassembled	The number of fragmented IP packets received and re-assembled by the device.
Bad Header	The number of packets dropped because they had a bad header.
No Route	The number of packets dropped because they had no route information.
Unknown Protocols	The number of packets dropped because they were using an unknown protocol.
No Buffer	The number of packets dropped because the device ran out of buffer space.
Other Errors	The number of packets dropped due to errors other than the ones listed above.
ICMP statistics	
Total Received	The number of ICMP packets received by the device.
Total Sent	The number of ICMP packets sent by the device.
Received Errors	This information is used by Dell customer support.
Sent Errors	This information is used by Dell customer support.
Received Unreachable	The number of Destination Unreachable messages received by the device.
Sent Unreachable	The number of Destination Unreachable messages sent by the device.
Received Time Exceed	The number of Time Exceeded messages received by the device.
Sent Time Exceed	The number of Time Exceeded messages sent by the device.
Received Parameter	The number of Parameter Problem messages received by the device.
Sent Parameter	The number of Parameter Problem messages sent by the device.
Received Source Quench	The number of Source Quench messages received by the device.
Sent Source Quench	The number of Source Quench messages sent by the device.
Received Redirect	The number of Redirect messages received by the device.
Sent Redirect	The number of Redirect messages sent by the device.
Received Echo	The number of Echo messages received by the device.
Sent Echo	The number of Echo messages sent by the device.
Received Echo Reply	The number of Echo messages received by the device.
Sent Echo Reply	The number of Echo messages sent by the device.
Received Timestamp	The number of Timestamp messages received by the device.
Sent Timestamp	The number of Timestamp messages sent by the device.
Received Timestamp Reply	The number of Timestamp Reply messages received by the device.
Sent Timestamp Reply	The number of Timestamp Reply messages sent by the device.

Received Address Mask	The number of Address Mask Request messages received by the device.
Sent Address Mask	The number of Address Mask Request messages sent by the device.
Received Address Mask Reply	The number of Address Mask Replies messages received by the device.
Sent Address Mask Reply	The number of Address Mask Replies messages sent by the device.
Received IRDP Advertisement	The number of ICMP Router Discovery Protocol (IRDP) Advertisement messages received by the device.
Sent IRDP Advertisement	The number of IRDP Advertisement messages sent by the device.
Received IRDP Solicitation	The number of IRDP Solicitation messages received by the device.
Sent IRDP Solicitation	The number of IRDP Solicitation messages sent by the device.
UDP statistics	
Received	The number of UDP packets received by the device.
Sent	The number of UDP packets sent by the device.
No Port	The number of UDP packets dropped because the packet did not contain a valid UDP port number.
Input Errors	This information is used by Dell customer support.
TCP statistics The TCP statistics are derived from RFC 793, “Transmission Control Protocol”.	
Active Opens	The number of TCP connections opened by this device by sending a TCP SYN to another device.
Passive Opens	The number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.
Failed Attempts	This information is used by Dell customer support.
Active Resets	The number of TCP connections this device reset by sending a TCP RESET message to the device at the other end of the connection.
Passive Resets	The number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.
Input Errors	This information is used by Dell customer support.
In Segments	The number of TCP segments received by the device.
Out Segments	The number of TCP segments sent by the device.
Retransmission	The number of segments that this device retransmitted because the retransmission timer for the segment had expired before the device at the other end of the connection had acknowledged receipt of the segment.
RIP statistics The RIP statistics are derived from RFC 1058, “Routing Information Protocol”.	
Requests Sent	The number of requests this device has sent to another RIP router for all or part of its RIP routing table.
Requests Received	The number of requests this device has received from another RIP router for all or part of this device’s RIP routing table.
Responses Sent	The number of responses this device has sent to another RIP router’s request for all or part of this device’s RIP routing table.
Responses Received	The number of responses this device has received to requests for all or part of another RIP router’s routing table.

Unrecognized	This information is used by Dell customer support.
Bad Version	The number of RIP packets dropped by the device because the RIP version was either invalid or is not supported by this device.
Bad Address Family	The number of RIP packets dropped because the value in the Address Family Identifier field of the packet's header was invalid.
Bad Request Format	The number of RIP request packets this router dropped because the format was bad.
Bad Metrics	This information is used by Dell customer support.
Bad Response Format	The number of responses to RIP request packets this router dropped because the format was bad.
Resp Not From RIP Port	This information is used by Dell customer support.
Response From Loopback	The number of RIP responses received from loopback interfaces.
Packets Rejected	This information is used by Dell customer support.

Monitoring RMON (Remote Monitoring) history

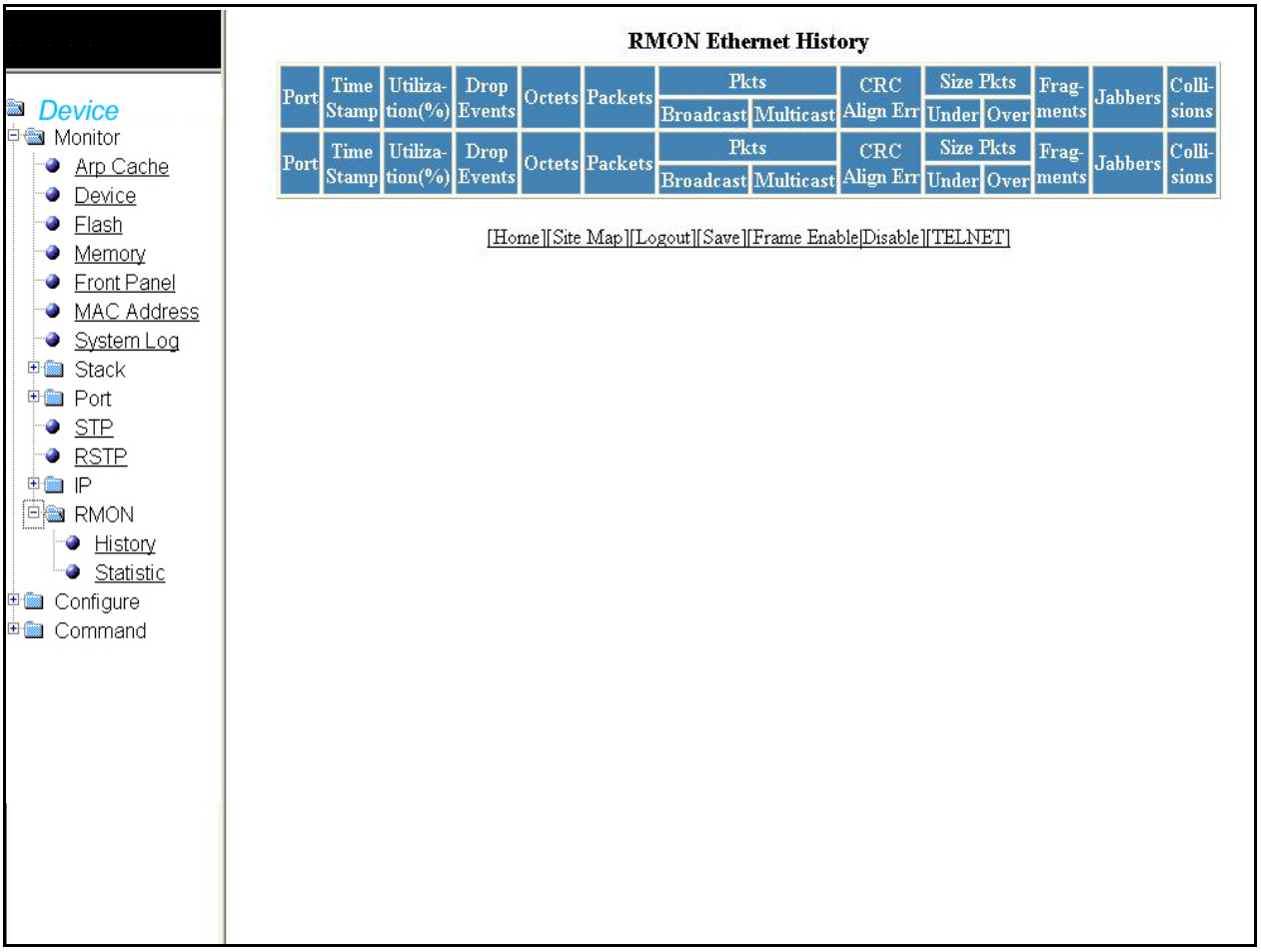
All active ports by default will generate two history control data entries per active port. An active port is defined as one with a link up. If the link goes down the two history entries are automatically deleted.

The following history entries are generated for each device:

- A sampling of statistics every 30 seconds
- A sampling of statistics every 30 minutes

Select **Monitor > RMON > History** to view RMON history data details.

FIGURE 30 Monitoring the RMON Ethernet history



The RMON History table contains the following information.

Port	Slot number or Port number for which the history data is being presented.
Time Stamp	Day and time when the data was collected.
Utilization	Percentage of the port that was being utilized when the data was taken.
Drop Events	Indicates an overrun at the port. The port logic could not receive the traffic at full line rate and had to drop some packets as a result. The counter indicates the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.
Octets	The total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Packets	The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.

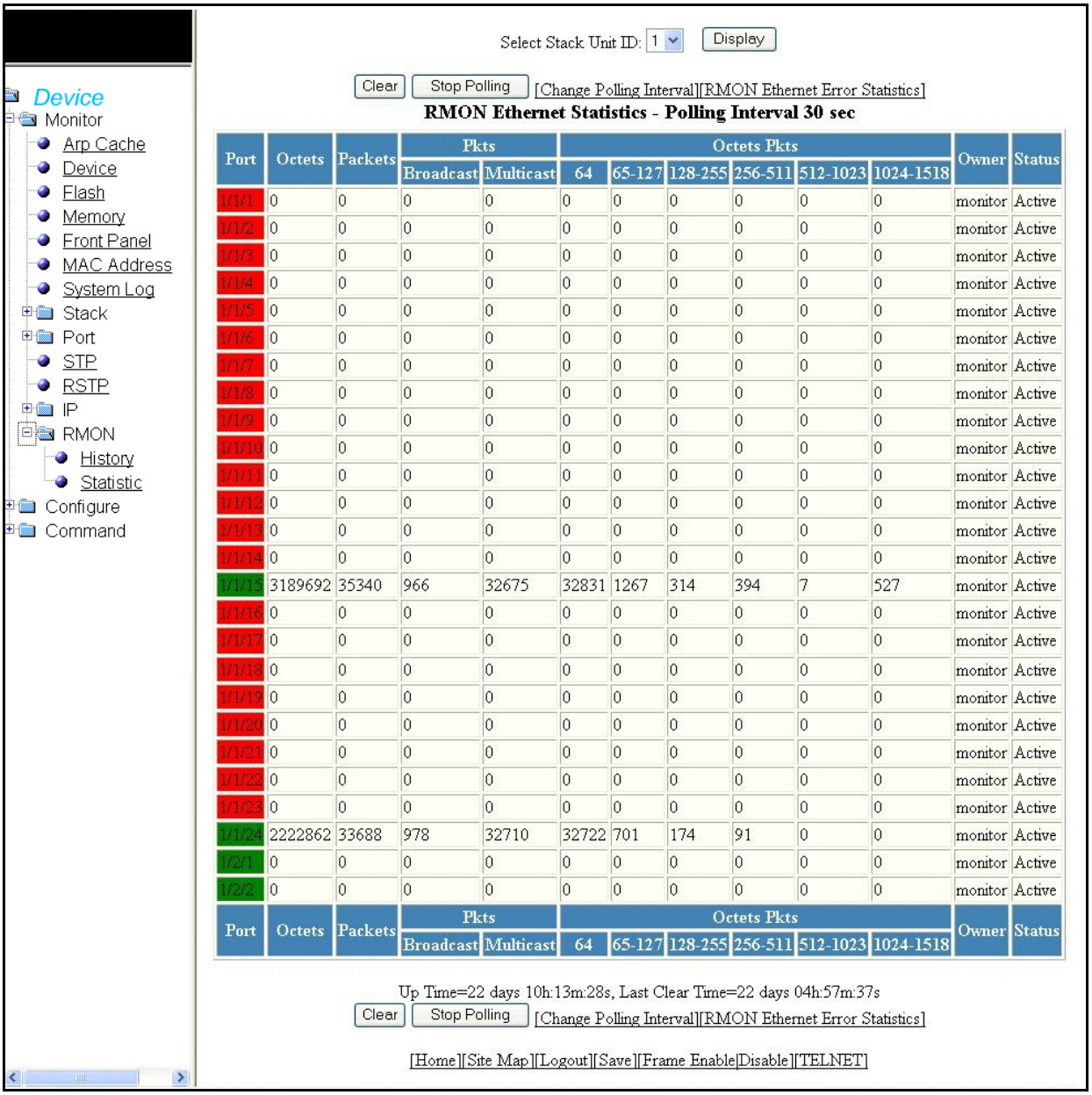
Packets: Broadcast	The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Alignment Errors	The total number of packets received that were from 64 – 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The packet length does not include framing bits but does include FCS octets.
Size Packets: Under	The total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Size Packets: Over	The total number of packets received that were longer than 1518 octets and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Fragments	The total number of packets received that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for this counter to be incremented, since it counts both runts (which are normal occurrences due to collisions) and noise hits. This number does not include framing bits but does include FCS octets.
Jabbers	The total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **NOTE:** This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. This number does not include framing bits but does include FCS octets.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

Monitoring RMON statistics

RMON statistics provides count information on multicast and broadcast packets. This information includes total packets sent, undersized and oversized packets, CRC alignment errors, jabbers, collisions, fragments, and dropped events for each port on the system. RMON statistics collection is activated automatically during system startup, and requires no configuration.

Select **Monitor > RMON > Statistics** to view current RMON Statistics. Select the stack unit ID from the drop-down list and click **Display**.

FIGURE 31 Monitoring RMON Ethernet statistics



Port	Octets	Packets	Pkts		Octets Pkts						Owner	Status
			Broadcast	Multicast	64	65-127	128-255	256-511	512-1023	1024-1518		
1/1/1	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/2	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/3	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/4	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/5	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/6	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/7	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/8	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/9	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/10	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/11	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/12	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/13	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/14	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/15	3189692	35340	966	32675	32831	1267	314	394	7	527	monitor	Active
1/1/16	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/17	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/18	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/19	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/20	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/21	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/22	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/23	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/24	2222862	33688	978	32710	32722	701	174	91	0	0	monitor	Active
1/2/1	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/2/2	0	0	0	0	0	0	0	0	0	0	monitor	Active
Port	Octets	Packets	Pkts		Octets Pkts						Owner	Status
			Broadcast	Multicast	64	65-127	128-255	256-511	512-1023	1024-1518		

The RMON Statistics contains the following information.

Port	Slot number or port number of the port for which the statistics are being reported.
Octets	The total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Packets	The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Packets: Broadcast	The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Octet Packets: 64	The total number of packets received that were 64 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 65 – 127	The total number of packets received that were 65 – 127 octets long.
This number includes bad packets.	This number does not include framing bits but does include FCS octets.
Octet Packets: 128 – 255	The total number of packets received that were 65 – 127 octets long.
This number includes bad packets.	This number does not include framing bits but does include FCS octets.
Octet Packets: 128 – 255	The total number of packets received that were 128 – 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 256 – 511	The total number of packets received that were 128 – 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 512 – 1023	The total number of packets received that were 1024 – 1518 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Owner	The owner of the packets.
Status	Status of the port.
Clear	Removes the data currently in the table and restarts monitoring.
Stop Polling	Stops reporting the statistics.
Change Polling Interval	Allows you to change the current polling interval.
RMON Ethernet Error Statistics	Shows the error statistics table.
Up Time	The length of time the device has been available.
Last Clear Time	The length of time data has been accumulating in the current table.

Chapter

4

Configuring Stack Components

In this chapter

Configuring the general settings for an IronStack

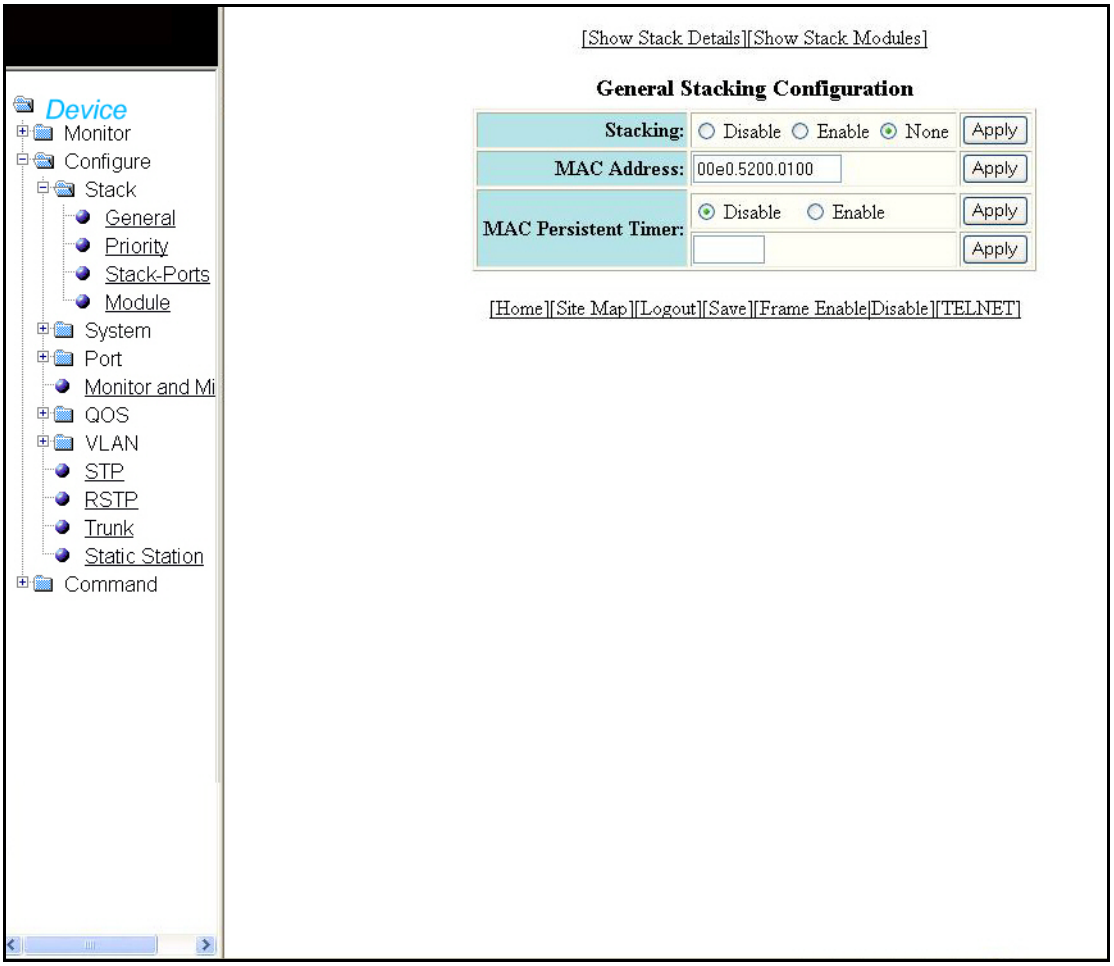
Once you have logged into the Web Management Interface, you can add or modify the stack settings to improve performance and reliability.

For more configuration information, refer to *PowerConnect B-Series FCX Configuration Guide.*

The unit with the highest priority is the Active Controller (128 by default). The stack member with the highest priority after the Active Controller is the Standby Controller, which takes over if the current Active Controller fails.

Select **Configure > Stack > General** to configure the priority of units within a stack. Click **Modify** to change the priority of a unit.

FIGURE 32 General Stacking Configuration



The General Stacking Configuration window contains the following information.

Stacking	Disable – Prevents a unit from sending or listening for any stacking probe messages. In this mode, the unit cannot be forced to join a stack. Enable – Enable stacking mode on a new unit before you add it to the stack. None – Prevents the unit from actively sending out probe messages, however the unit can still be called to join a stack by an Active Controller.
MAC Address	The MAC address of the device.
MAC Persistent Timer	If Enabled, allows you to set a time delay before the stack MAC address changes. During this configured interval, if the previous Active Controller is reinstalled in the stack, the stack continues to use the MAC address of this unit, even though it may no longer be the Active Controller. If the previous Active Controller does not rejoin the stack during the specified time interval, the stack assumes the address of the new Active Controller as the stack MAC address.

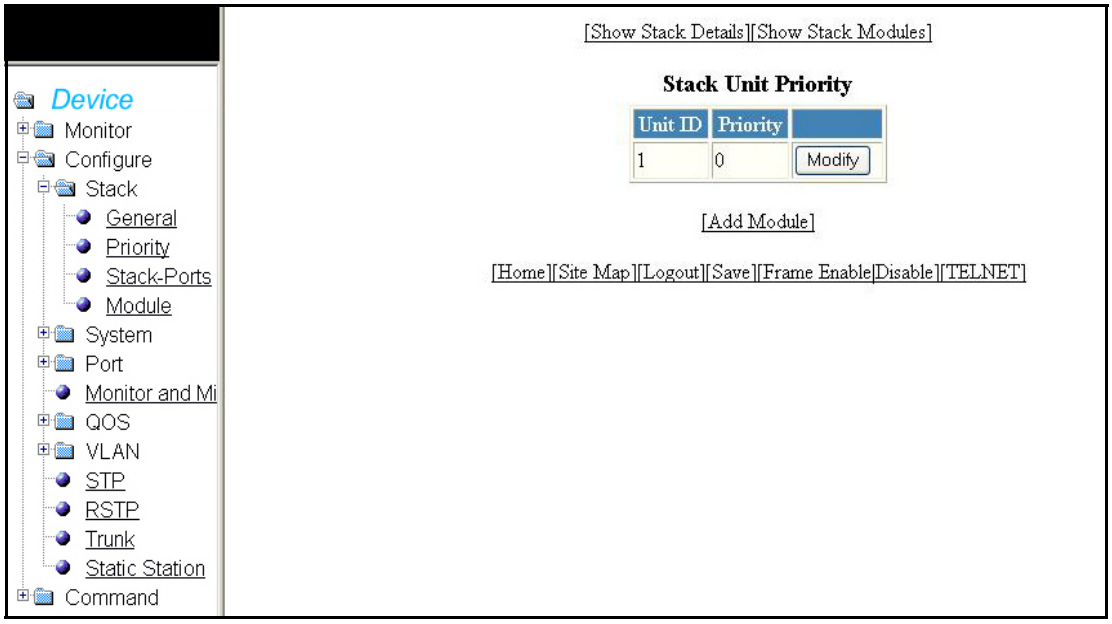
The following information can be viewed in General Stacking Configuration window.

- Show Stack Details
- Show Stack Modules

Configuring stack priority

Select **Configure > Stack > Priority** to configure the priority of units within a stack. Click **Modify** to change the priority of a unit.

FIGURE 33 Configuring stack unit priority



The Stack Unit Priority window contains the following information.

Unit ID	The stack identification number for this unit.
Priority	A number from 0 to 255 (255 is the highest priority).

The additional items you can configure or view in the Stack unit priority window includes:

- Stack Details
- Stack Modules
- Add module (refer to page 56)

Modifying priority

Assign the highest priority value to the stack unit if you want to function as the Active Controller. When you enter a new priority value for a stack unit, that value takes effect immediately, but does not affect the current Active Controller until the next reset.

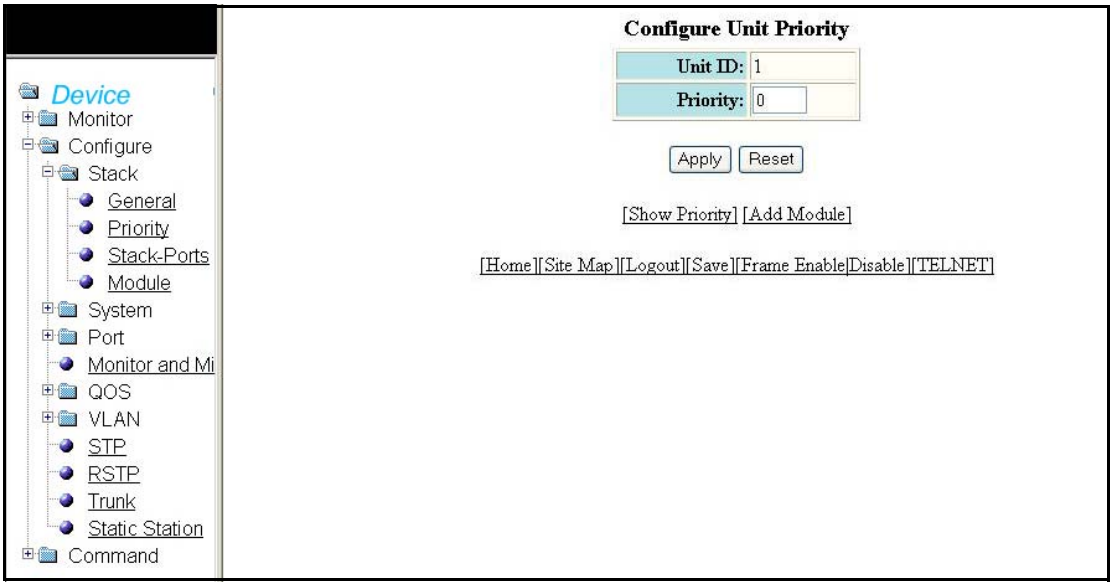
It is possible to assign the same priority for an Active and Standby Controllers, or different priorities (Active highest, Standby second-highest). When Active and Standby Controllers have the same priority, if the Active fails and the Standby takes over, then the original Active becomes operational again, it will not be able to resume its original role. In the same situation, when the priorities of the Active and Standby Controllers are different, the old Active Controller will regain its role and will reset the other units.

You can assign the same priority to the Active and Standby Controllers once after the stack is formed. This prevents the intended Standby Controller from becoming the Active Controller during stack construction.

Changing the priority of a stack member will trigger an election that takes effect immediately unless the Active Controller's role changes. This changes will not take effect until after the next stack reload.

Click **Modify** to modify the priority of units within a stack, in the row associated with the unit ID. Click **Apply** to save your changes or click **Reset** to undo any changes.

FIGURE 34 Configuring unit priority



The Configure Unit Priority window contains the following information.

Unit ID	The stack identification number for this unit.
Priority	A number from 0 to 255 (255 is the highest priority).

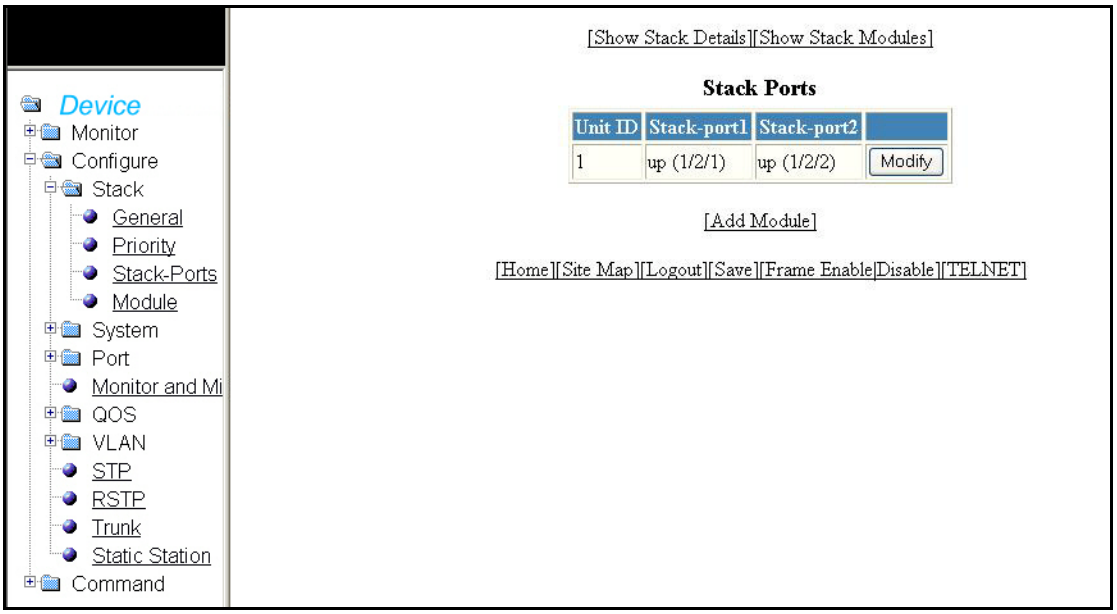
Additional information you can configure or view includes:

- Show priority
- Add module (refer to page 56)

Configuring stack ports

Select **Configure > Stack > Stack-Ports** to configure a stack. Click **Modify** to modify the configuration of a port. Click **Apply** to save your configuration.

FIGURE 35 Configuring stack ports



NOTE
When you assign an unused ID to a new stack unit, once this unit is reset, it assumes the new ID. All configuration information related to the previous unit that used the ID is deleted. The Active Controller learns the configuration for the new unit (instead of creating an interface configuration for the new unit).

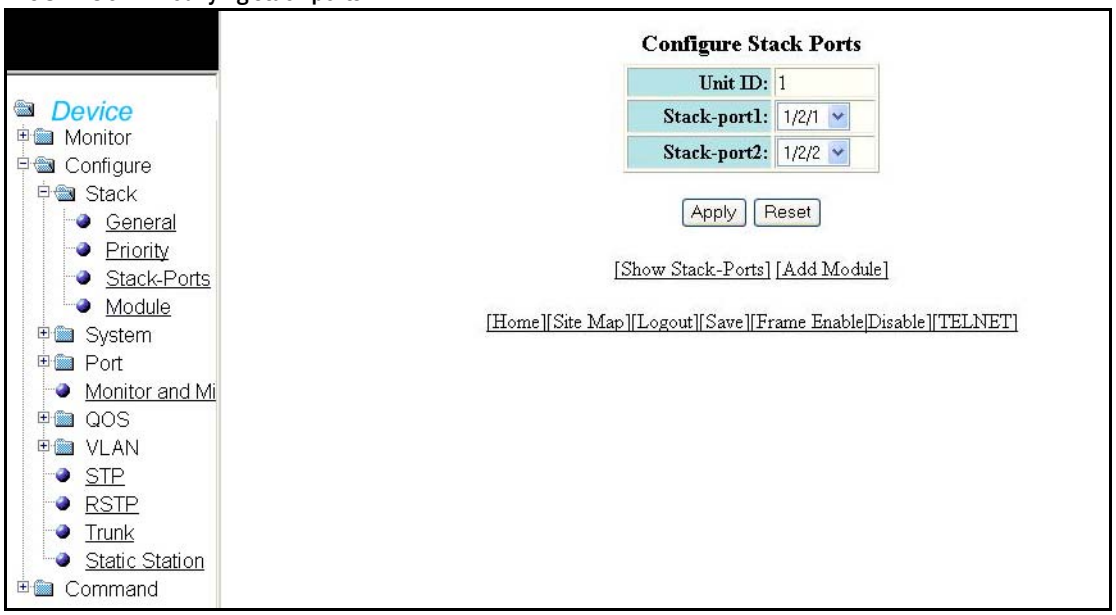
If the configuration for a unit being replaced does not match the new unit type, the Active Controller removes the unit configuration and associated interface configuration.

You can also view details of Show Stack Details, Show Stack Modules, and Add Module. For more information on adding a module, refer to page 56.

Modifying stack ports

Click **Configure** > **Stack** > **Stack Ports** > **Modify** to modify the configuration of the stack ports. Configure the stack ports and Click **Apply.**

FIGURE 36 Modifying stack ports

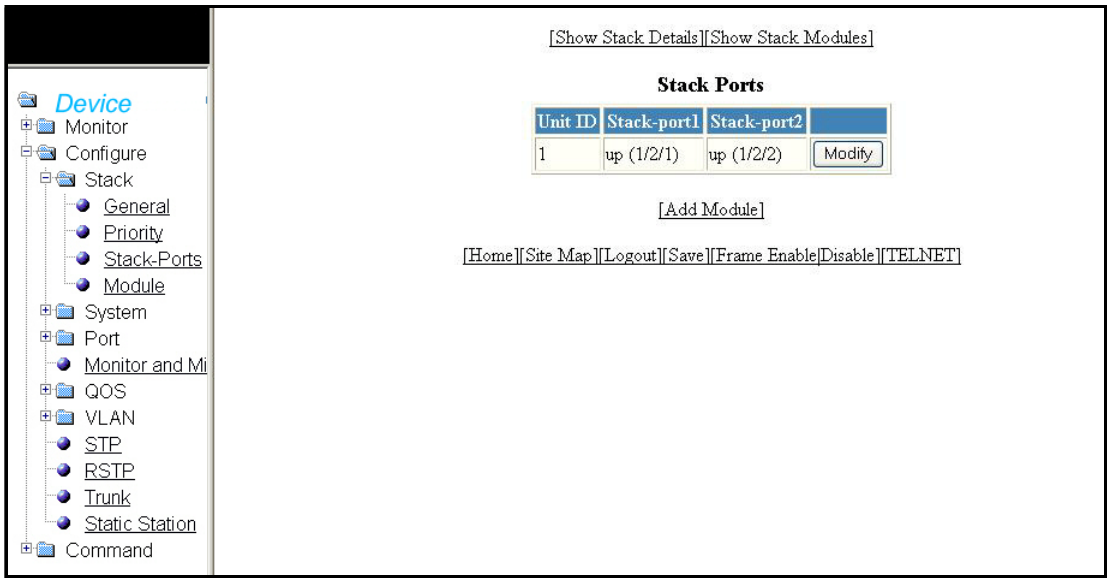


The configurable options include the following.

Unit ID	The stack identification number for this unit.
Stack-port1	Identifies the port by number (stack-ID or slot or port).
Stack-port2	Identifies the port by number (stack-ID or slot or port).

Click **Show Stack-Ports** to view the details of selected stack ports as shown below.

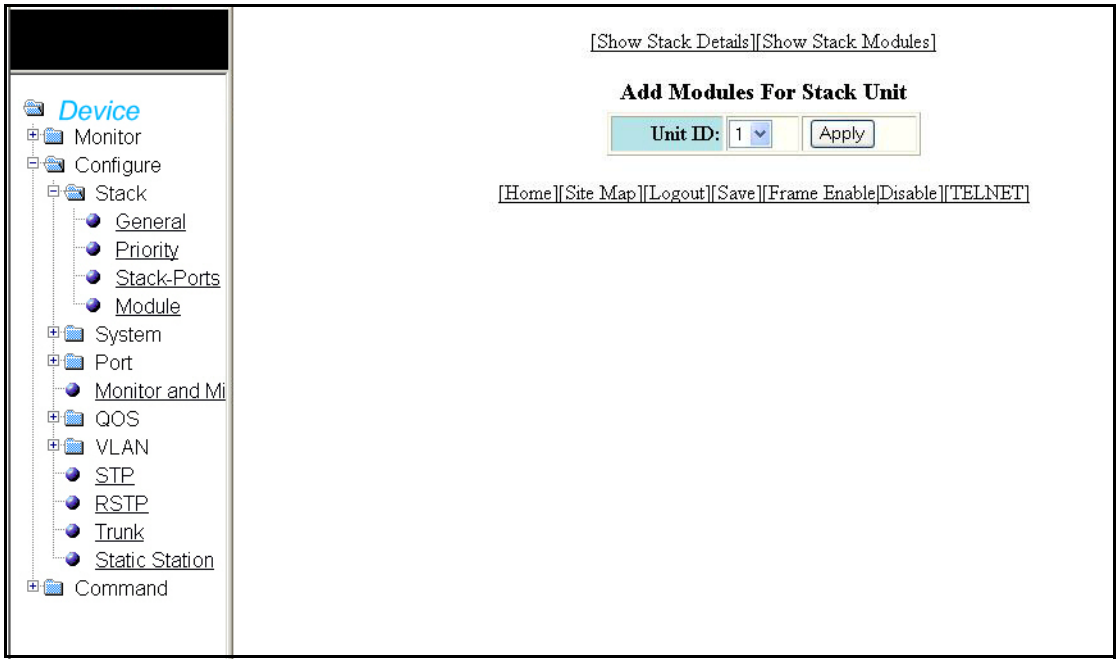
FIGURE 37 Show Stack-Ports



Configuring a stack module

Select **Configure > Stack > Module** to configure a stack module. Select a Unit ID from 1 to 8 in the drop-down menu, then click **Apply**.

FIGURE 38 Add Modules for Stack Unit



Adding a module

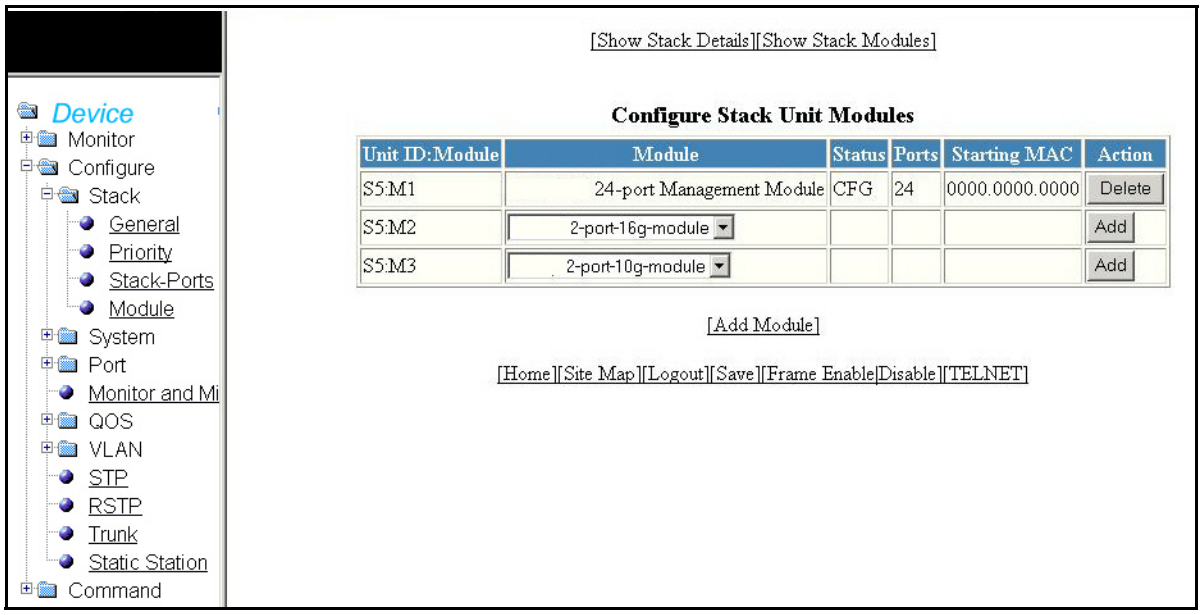
Click **Add Module** to add a module to the stack.

Configuring a new module can be accomplished by following steps below:

- When you add a new module, the Active Controller **learns** the configuration from the new unit dynamically. You can change this configuration to a static configuration by doing a write memory on the Active Controller.
- If the new unit is replacing an old unit, and the configuration of the new unit matches the base module (module 1) configuration of the old unit, no action is necessary. If the configuration of the new unit does not match the configuration of the old unit, the Active Controller learns the module types for the new unit and merges this information with what it knows for the base module. This merged configuration remains static and stays on the Active Controller even if the new unit leaves the stack.

Click **Add** to display the new stack module. Click **Delete** to delete a module.

FIGURE 39 Adding and deleting a stack unit module



The Configure Stack Unit Modules contains the following information.

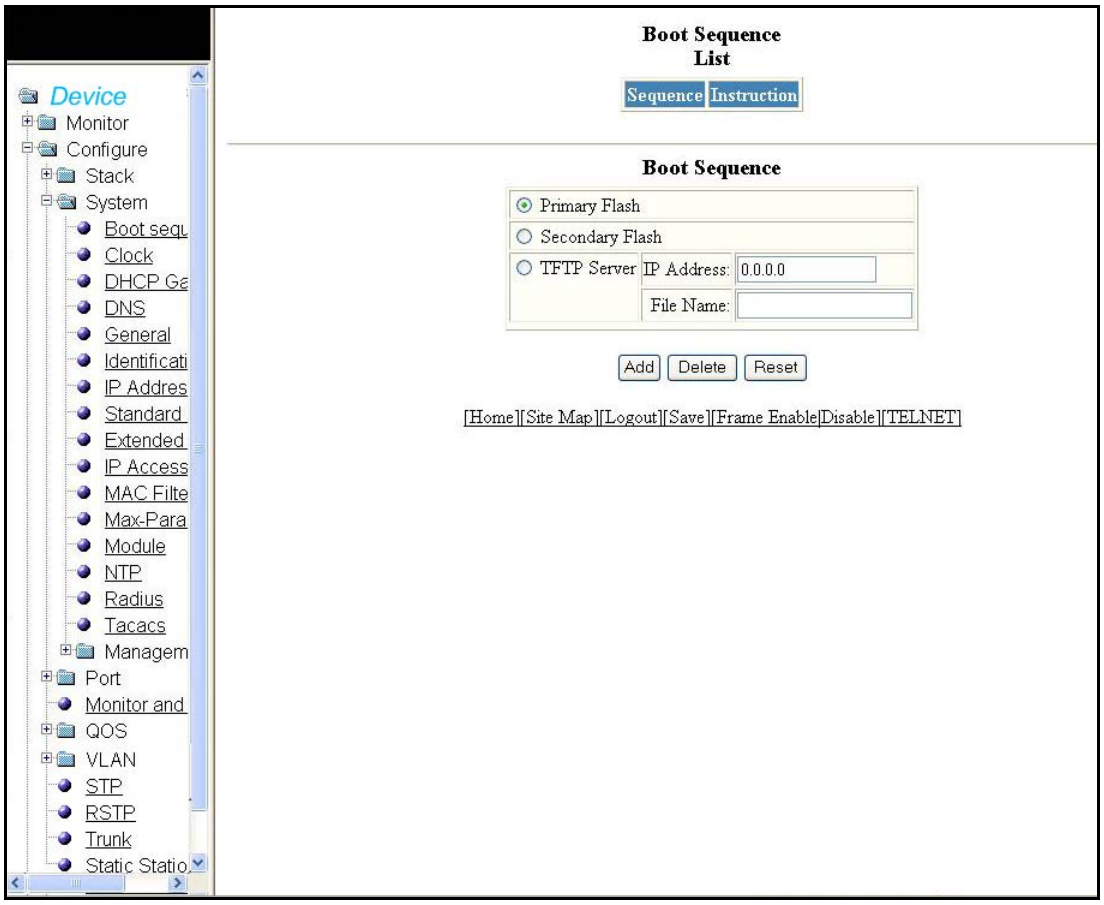
Unit ID: Module	The stack identification number for this unit and the number for the module.
Module	Identifies the module by module type.
Status	The status of this module.
Ports	The number of ports in this module.
Starting MAC	The starting MAC address for this module.

NOTE
You cannot delete active modules.

Configuring the system boot sequence

Select **Configure > System > Boot Sequence** to configure the system boot sequence.

FIGURE 40 Configuring system boot sequence

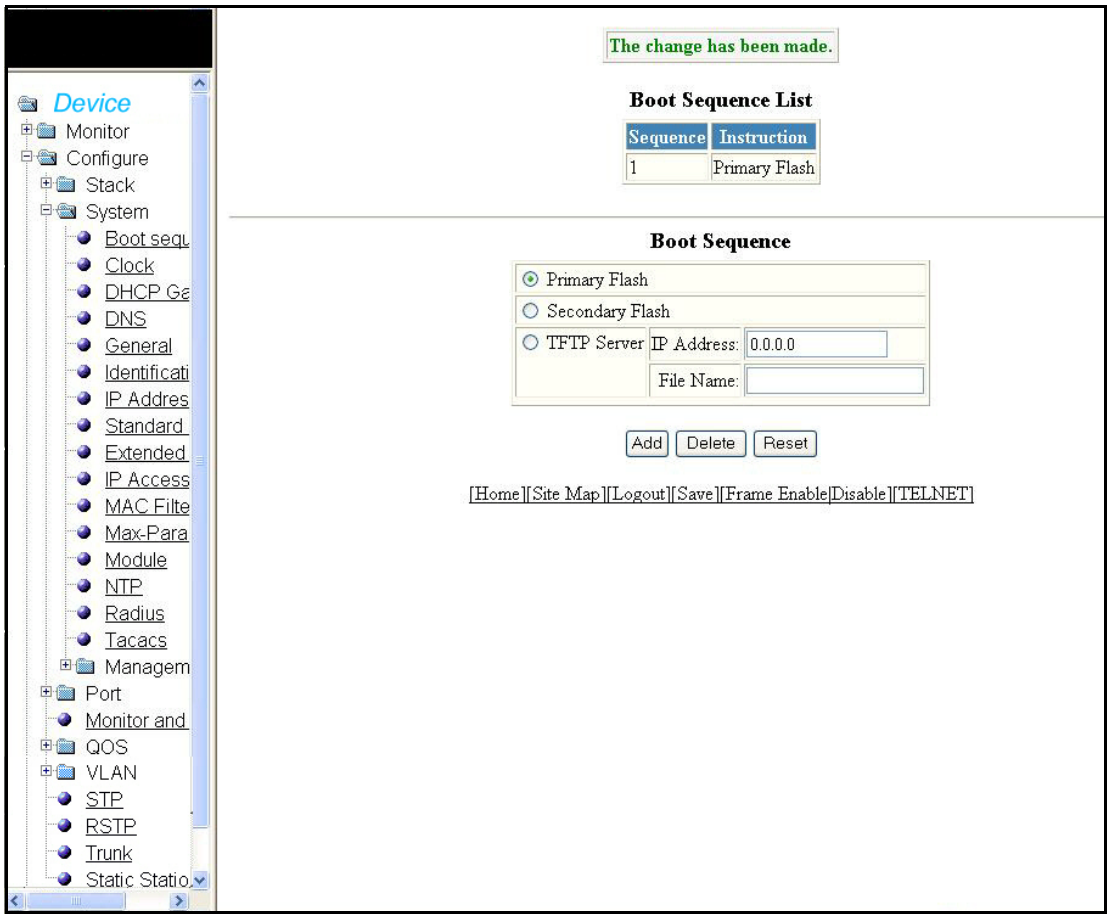


Other options in this panel includes:

Add	Enables you to add the Boot Sequence operations.
Delete	Enables you to delete the added Boot Sequence operations.
Reset	To undo your changes, click Reset.

Select any one of the boot sequence operation and click **Add** to display the selected operation in the Boot Sequence List as shown in Figure 41.

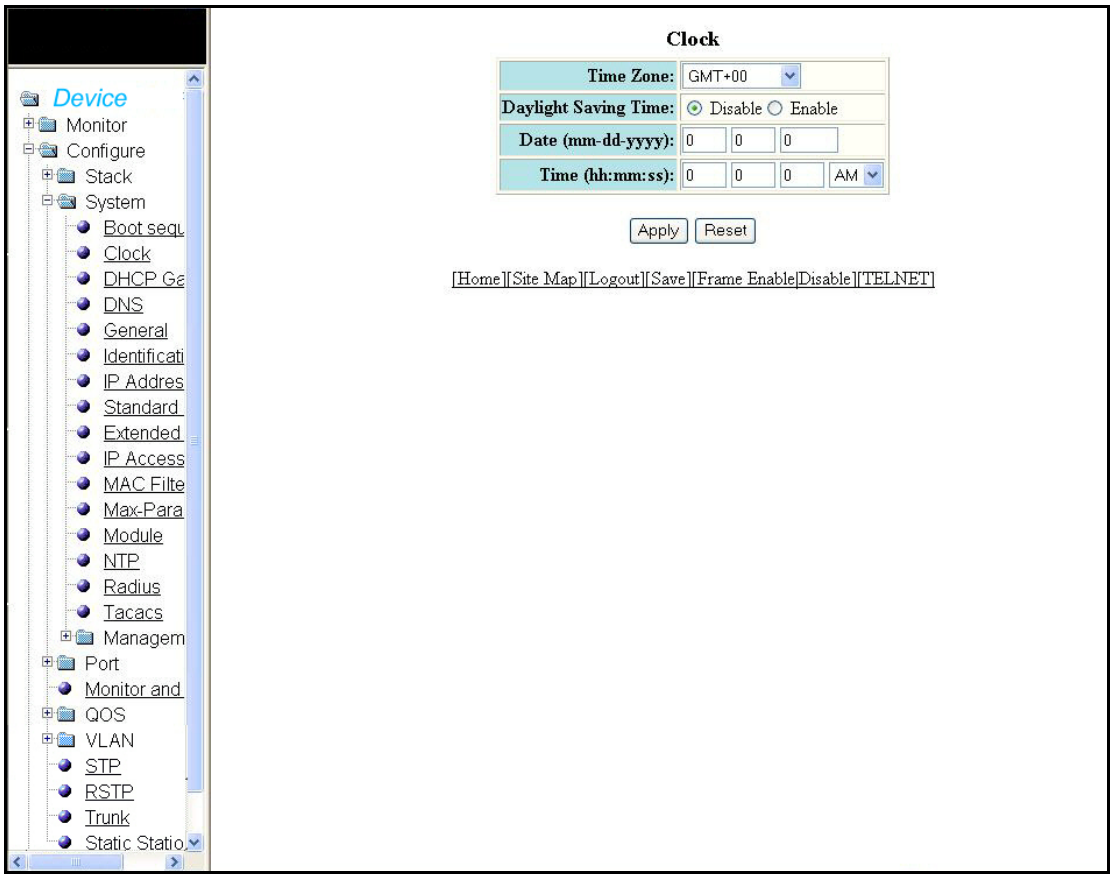
FIGURE 41 Boot Sequence List



Configuring the system clock

Select **Configure > System > Clock** to configure the system clock**.** Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 42 Configuring the system clock



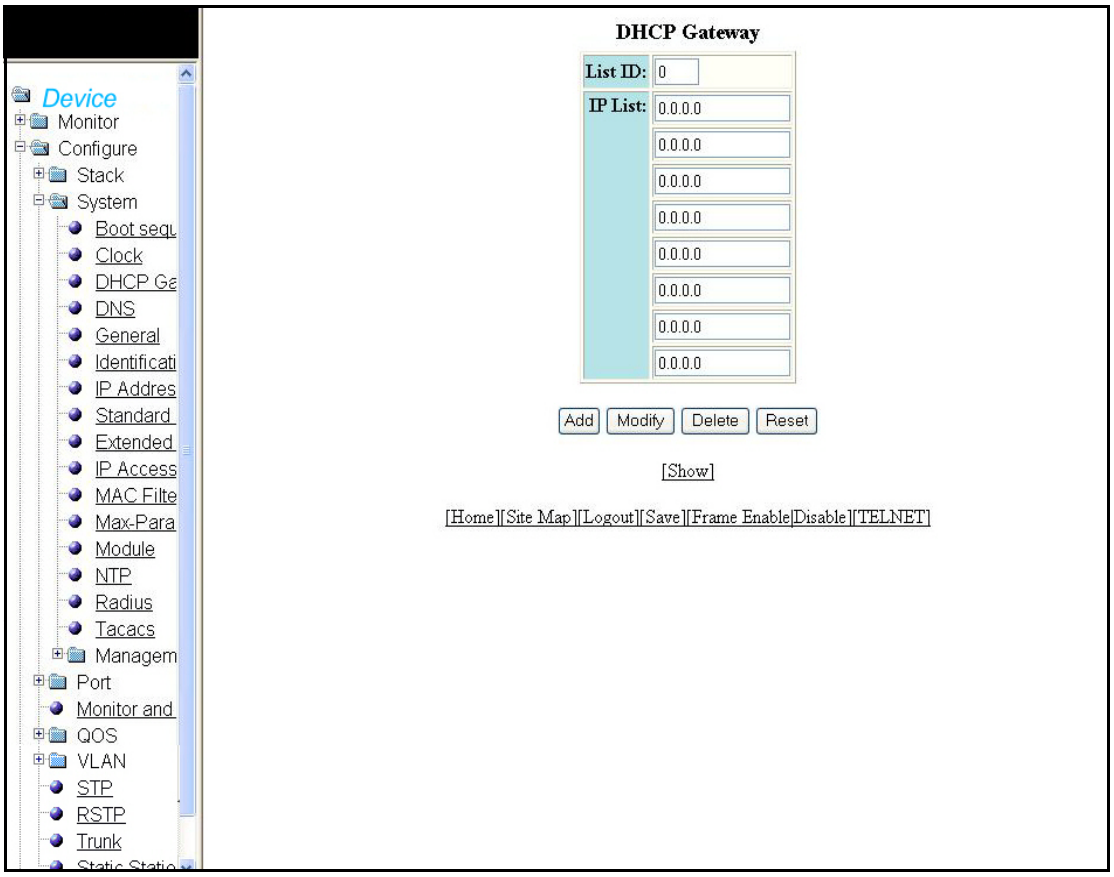
The clock menu contains the following information.

Time Zone	Configures the different time zones that can be configured for the device.
Daylight Saving time	Allows to enable or disable Daylight Saving Time option.The DST feature is automatic, but to trigger the device to the correct time, the device must be configured to the US time zone, not the GMT offset.
Date	Configures the system date in the mm-dd-yyyy format.
Time	Configures the system time in the hh:mm:ss format.

Configuring the system DHCP gateway

Select **Configure > System > DHCP Gateway** to configure a system DHCP gateway.

FIGURE 43 Configuring system DHCP gateway

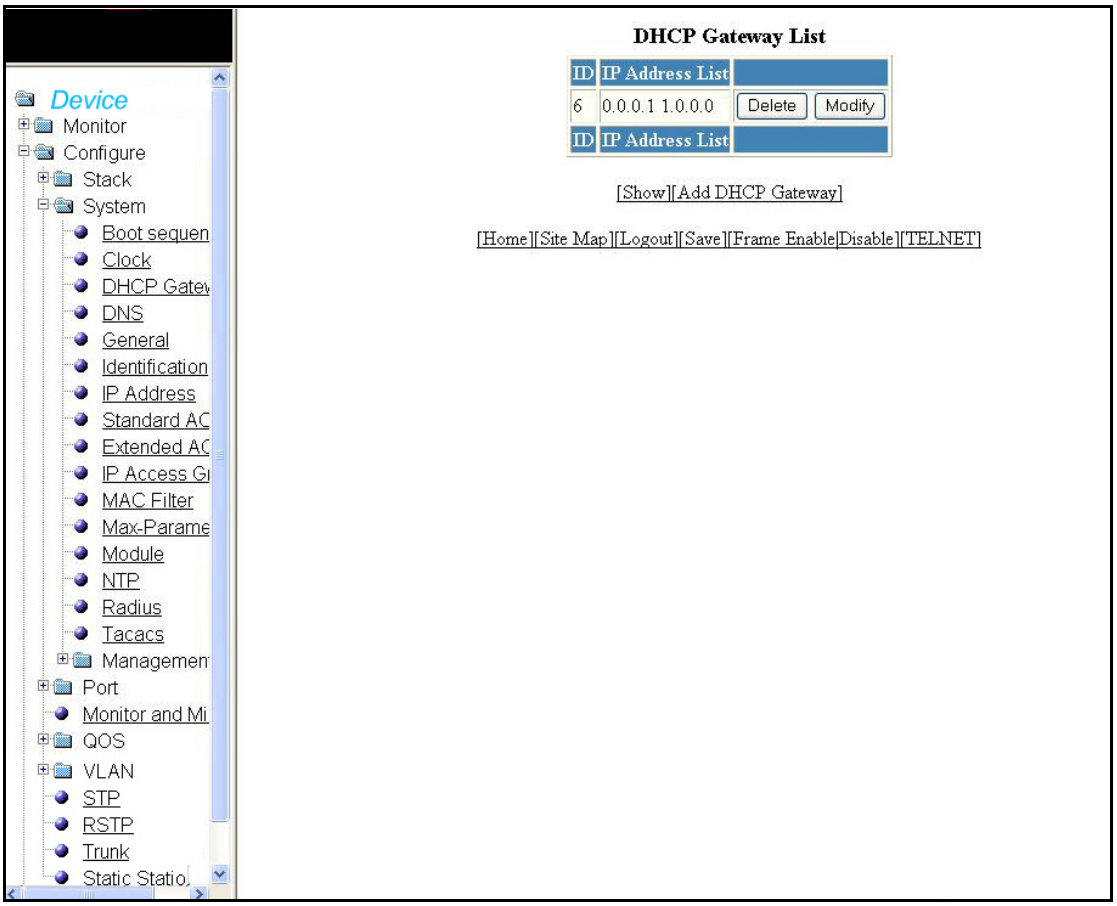


The DHCP gateway contains the following information.

Unit ID	The stack identification number for this unit.
IP List	Displays the list of IP addresses.
Add	Enables you to add Unit ID.
Modify	Enables you to modify, if any.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.

Click **Add** after entering the values for Unit ID and IP to display the added information in the DHCP Gateway list.

FIGURE 44 Adding Unit ID and IP



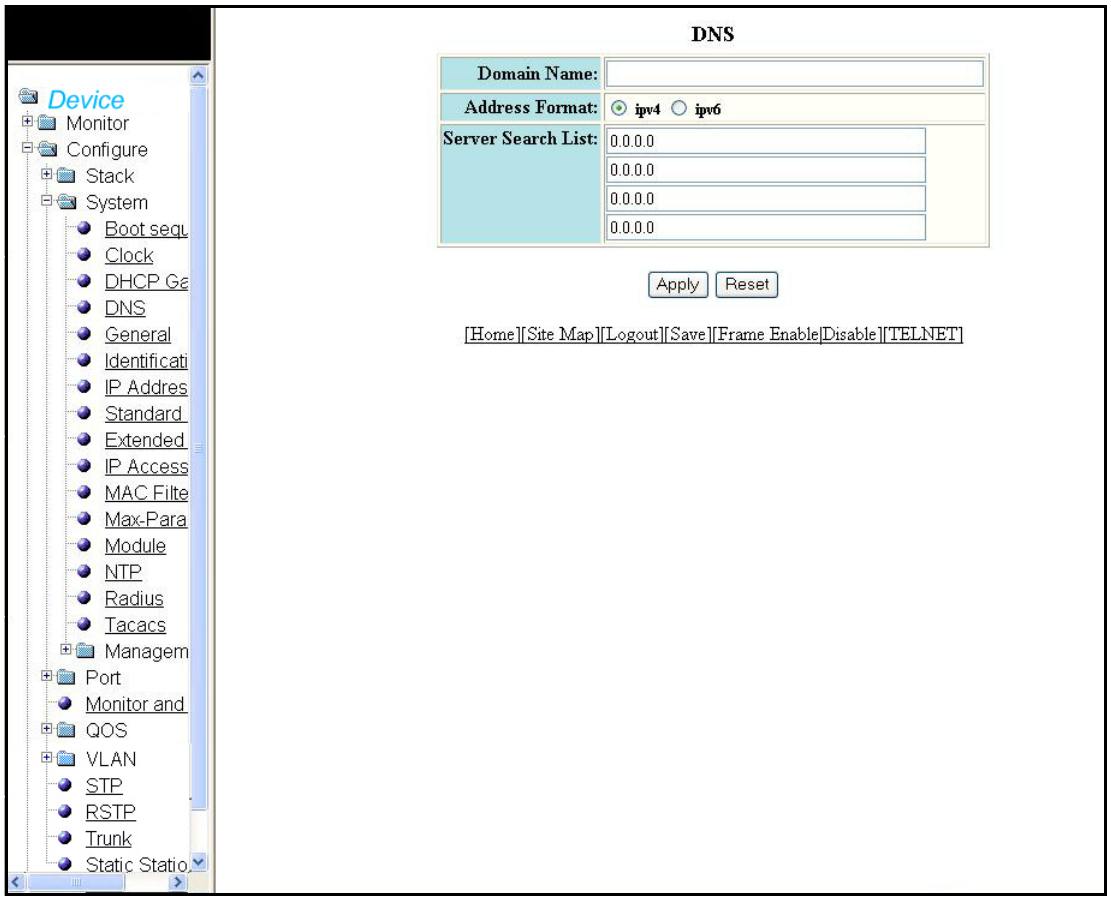
The DHCP gateway list contains the following information.

ID	The stack identification number for this unit.
IP Address List	Displays the list of IP addresses.
Show	Displays the added list of DHCP gateway.
Add DHCP Gateway	Allows you to add new ID and address list to the DHCP gateway list.

Configuring the system DNS

Select **Configure > System > DNS** to configure a system DNS. Click **Apply** to save your configuration or click **Reset t**o undo changes.

FIGURE 45 Configuring system DNS



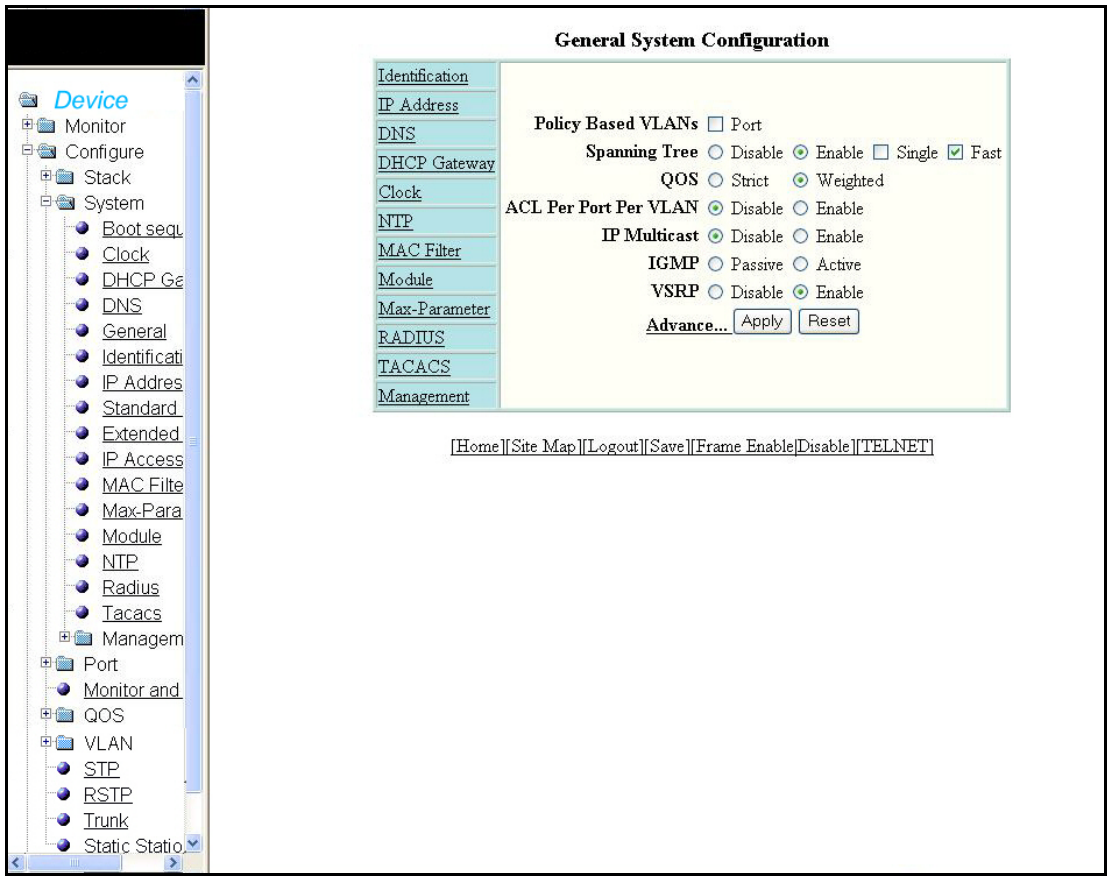
The DNS display contains the following information.

Domain Name	The label of the controlling system.
Address Format	Refers to the IPv4 or IPv6 format.
Server Search List	Provides the list of servers to configure DNS.

Configuring the general system

Select **Configure > System > General** to configure the general system. Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 46 Configuring general system



The general system configuration display contains the following information.

Policy based VLANs	Enables to configure port VLAN.
Spanning Tree	Enables and disables STP on the device. On enabling it allows to select the type of STP.
QoS	Defines the type of QoS to be selected.
ACL Per Port Per VLAN	Enables or disables the number of ACLs per port per VLAN.
IP Multicast	Enables or disables IP Multicast.
IGMP	Allows to configure IGMP to be active or passive.
VSRP	Enables or disables VSRP.

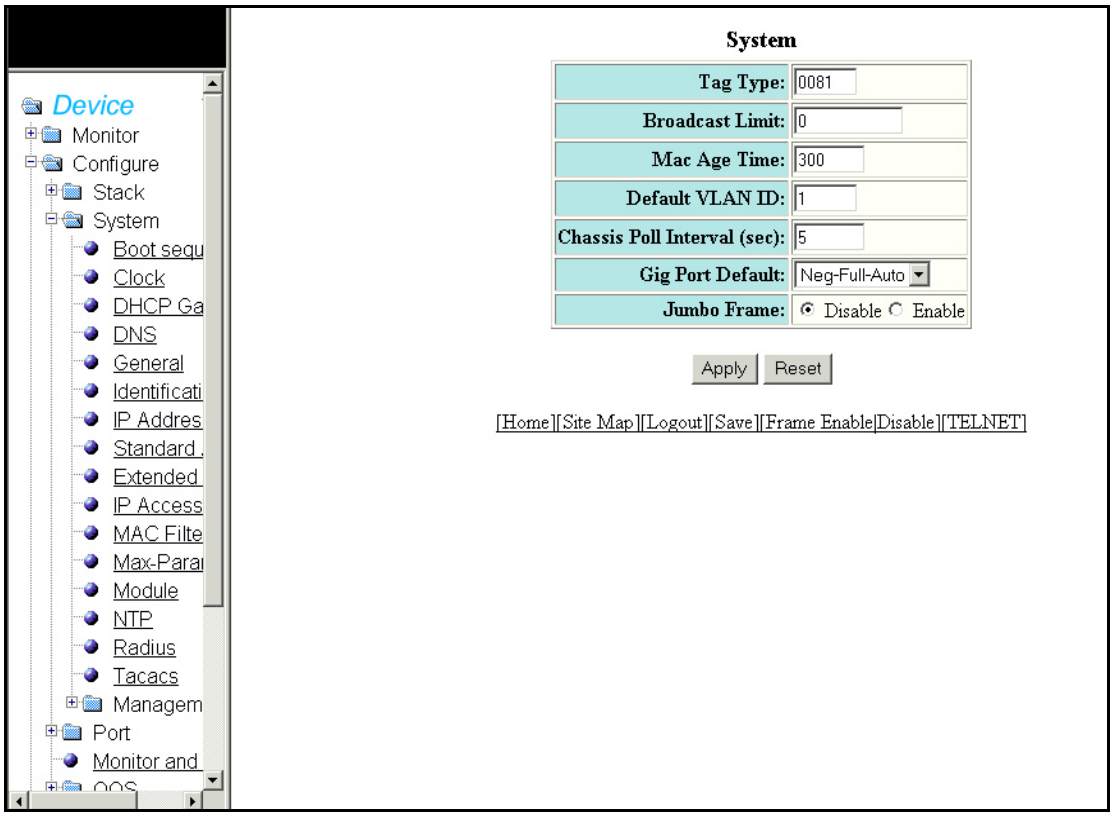
General system information includes:

- Identification
- IP Address
- DNS
- DHCP Gateway
- Clock
- NTP

- MAC Filter
- Module
- Max-Parameter
- RADIUS
- Tacacs
- Management

Click **Advance** to display the following additional system information.

FIGURE 47 Advance system information



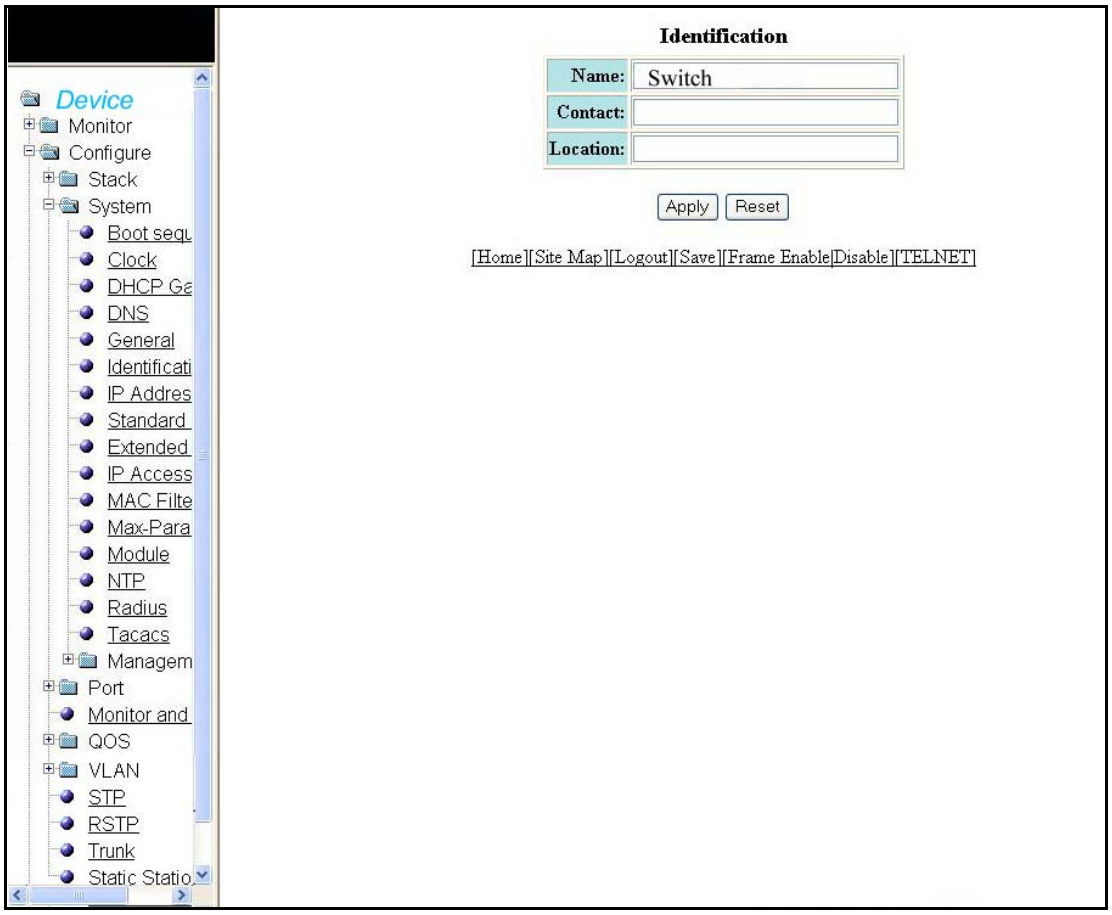
The Advance system display contains the following information.

Tag Type	Specifies the VLAN tag type of the device. The tag type can be a hexadecimal value from 0 – ffff. The default is 8100.
Broadcast Limit	Specifies the total number of broadcast packets or bytes allowed on the port.
Mac Age Time	Defines how long a port address remains active in the address table.
Default VLAN ID	Specifies the default VLAN ID number.
Chassis Poll Interval (sec)	Specifies the interval in which the chassis is polled.
Gig Port Default	Configures the default Gig Port.
Jumbo Frame	Enables or disables the Jumbo frame. Jumbo frames are Ethernet frames with more than 1,500 bytes MTU.

Configuring the system identification

Select **Configure > System > Identification** to configure system identification information. Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 48 Configuring system identification



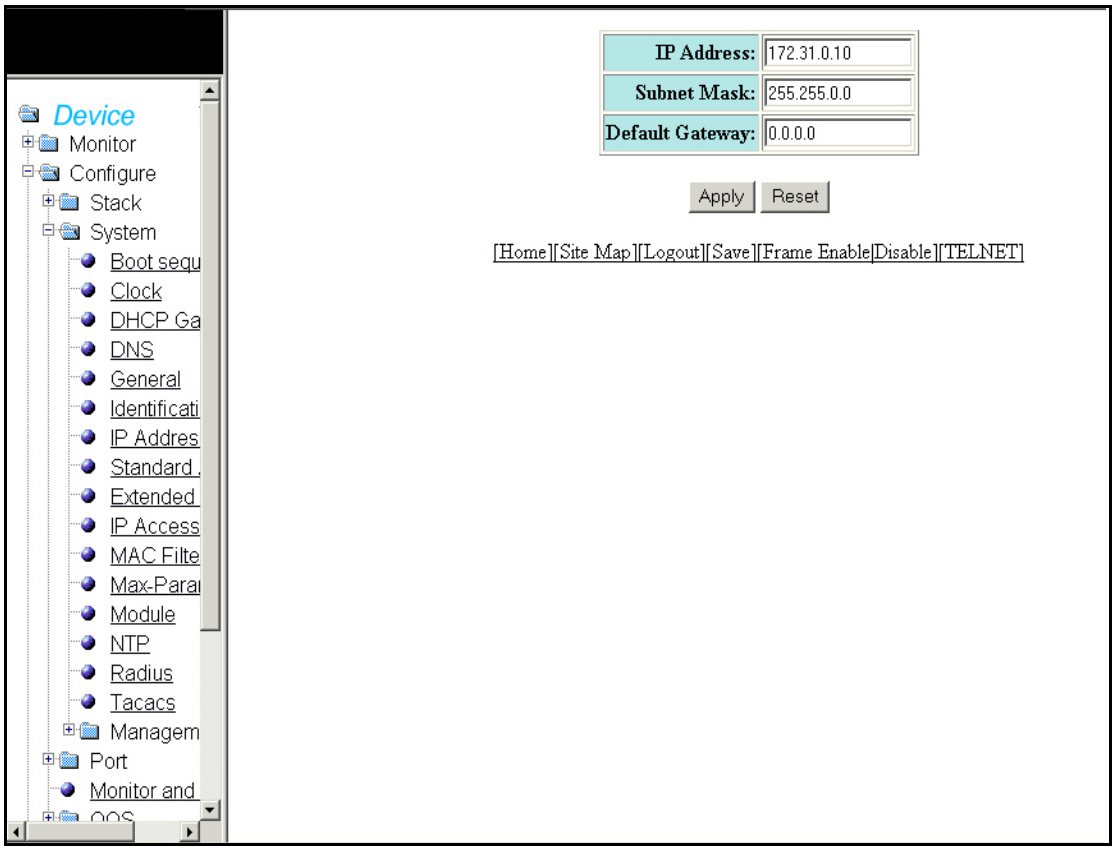
The System Identification contains the following information.

Name	Displays the name of the device.
Contact	Specifies the contact information of the device
Location	Specifies the location of the device.

Configuring the system IP address

Select **Configure > System > IP Address** to configure the IP address of a system. Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 49 Configuring system IP address



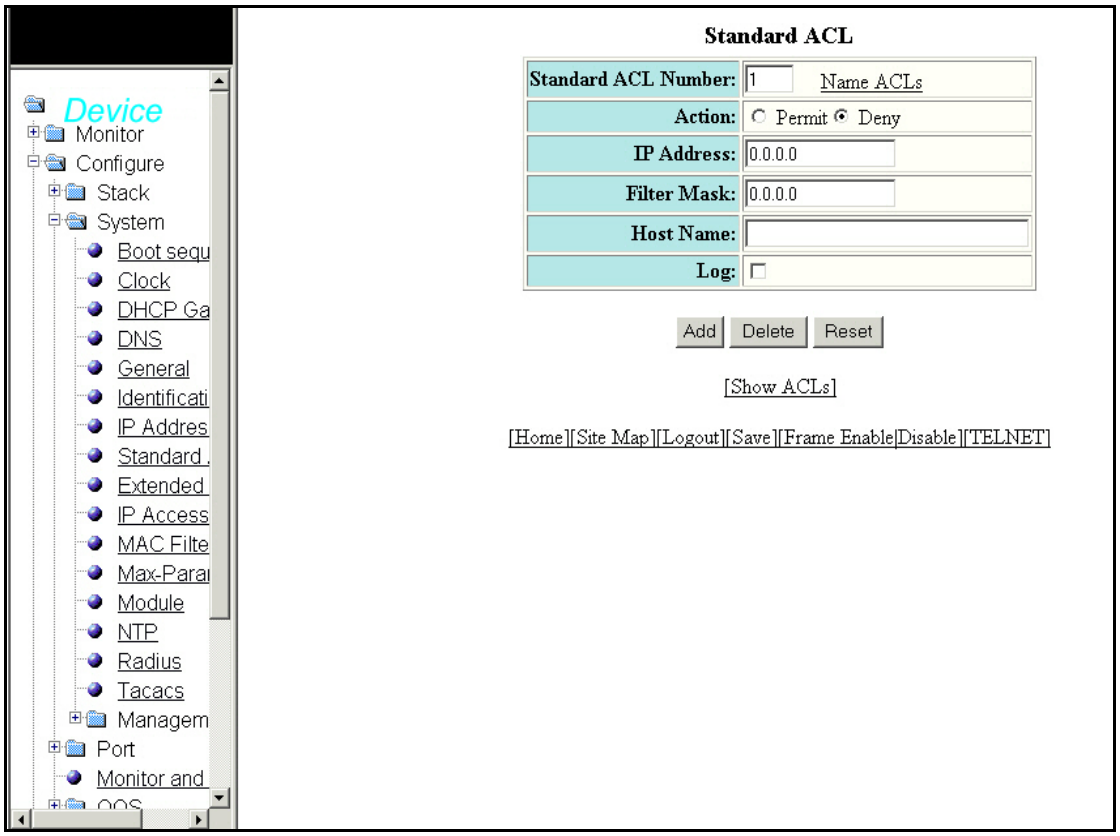
The system IP display contains the following information.

IP Address	Configures the IP Address of the device.
Subnet Mask	Configures the network mask for the IP Address.
Default Gateway	Configures the IP address of a locally attached router (or a router attached to the Layer 2 Switch by bridges or other Layer 2 Switches).

Configuring a standard ACL

Select **Configure > System > Standard ACL** to configure a standard ACL. Click **Reset** to undo changes.

FIGURE 50 Configuring a standard ACL

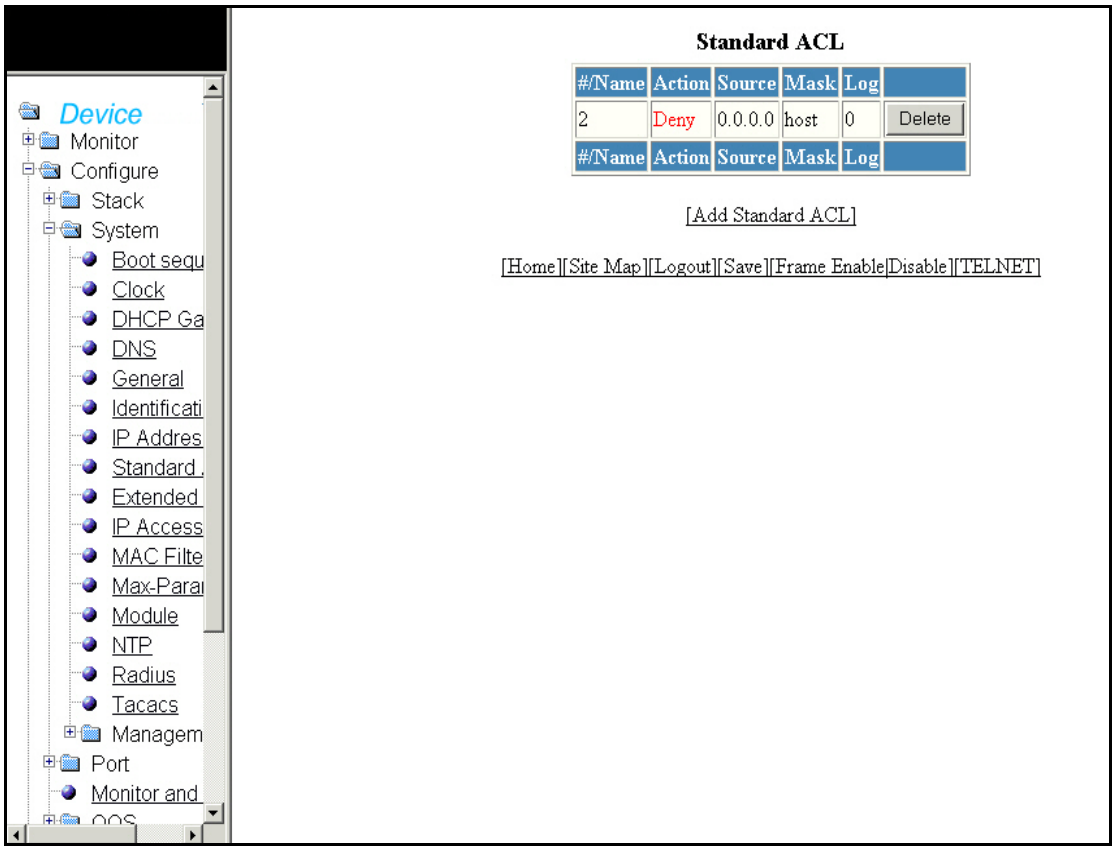


The standard ACL display contains the following information.

Standard ACL Number	Displays the Standard Access Control List number.
Action	The action the router takes if a RIP route packet matches the IP address and subnet mask of the filter. The action can be one of the following: • deny – The ACL will deny (drop) packets that match a policy in the access list. • permit – The ACL will permit (forward) packets that match a policy in the access list.
IP Address	The IP Address of the route's destination.
Filter Mask	Allows you to specify a range of IP addresses to include or exclude based on mask matching.
Host Name	Enables you to perform Telnet, ping and tracer route commands.
Log	Allows you to select if you want to log the entries.
Add	Allows you to add the Standard ACL Number.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show ACLs	Displays the standard ACL information.
Name ACLs	Clicking on this parameter allows you to enter the ACL Name

Click **Show ACL** to open the Standard ACL display.

FIGURE 51 Standard ACL



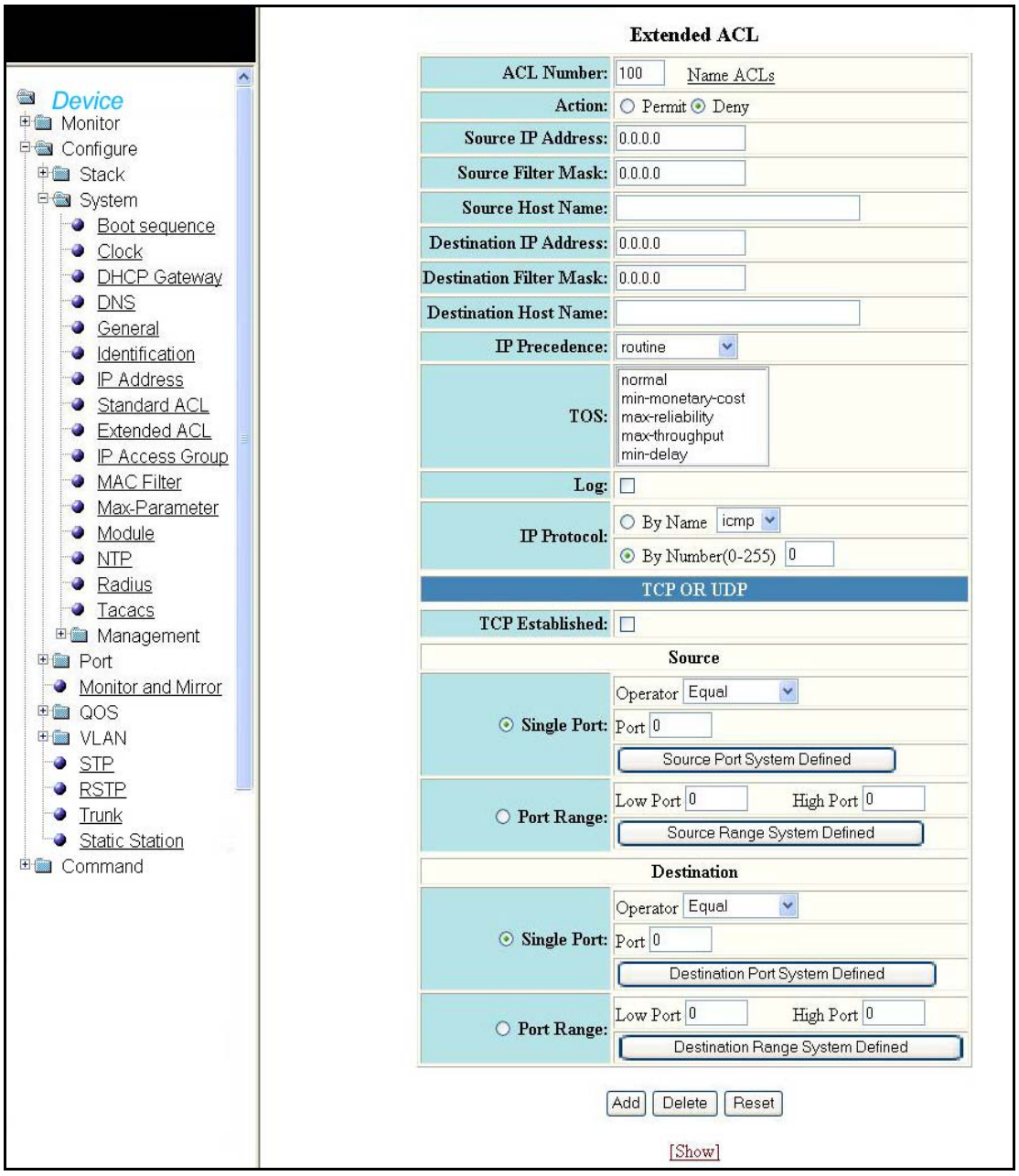
The Standard ACL display contains the following information.

#/Name	Displays the name of the Standard ACL.
Action	The action the router takes if a RIP route packet matches the IP address and subnet mask of the filter. The action can be one of the following: • deny – The ACL will deny (drop) packets that match a policy in the access list. • permit – The ACL will permit (forward) packets that match a policy in the access list.
Source	Identifies the source list that will be included or excluded on the interface.
Mask	This parameter provides a filter for displaying multiple MAC addresses that have specific values in common.
Log	Allows you to select if you want to log the entries.
Add Standard ACL	Allows you to add another standard ACL.

Configuring an extended ACL

Select **Configure > System > Extended ACL** to configure an extended ACL.

FIGURE 52 Configuring an extended ACL



The Extended ACL display contains the following information.

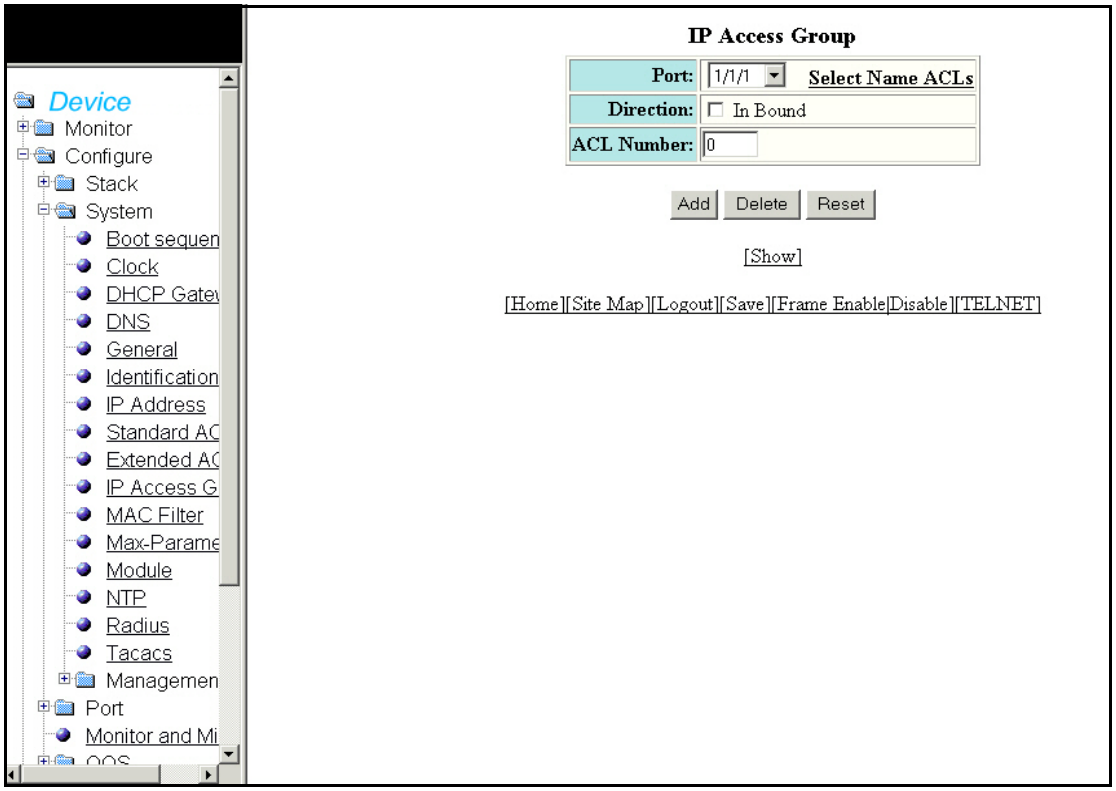
ACL Number	Displays the Extended Access Control List number.
Action	The action the router takes if a RIP route packet matches the IP address and subnet mask of the filter. The action can be one of the following: • deny – The ACL will deny (drop) packets that match a policy in the access list. • permit – The ACL will permit (forward) packets that match a policy in the access list.
Source IP Address	The software uses the lowest-numbered IP address configured on the port or interface as the source IP address.
Source Filter Mask	This parameter specifies the source IP address and mask.
Source Host Name	The IP address of the host at tbe source end.
Destination IP Address	This parameter indicates the destination IP address of the denied packets.
Destination Filter Mask	This parameter specifies the destination IP address and mask.
Destination Host Name	The IP address of the host at tbe destination end.
IP Precedence	This parameter is a 3-bit value in the type of service (TOS) byte of IP header used for assigning precedence to IP packets
TOS	The 8-bit field (Type of Service) in a IP datagram header.
IP Protocol	The IP protocol can be one of the following well-known names or any IP protocol number from 0 – 255. • Internet Control Message Protocol (ICMP) • Internet Group Management Protocol (IGMP) • Internet Gateway Routing Protocol (IGRP) • Internet Protocol (IP) • Open Shortest Path First (OSPF) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP)
TCP OR UDP	
TCP Established	This parameter indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The non-matching case is the initial TCP datagram to form a connection.
Source	
Single Port	Enables you to specify a single source port.
Port Range	Enables you to specify the source port range from low to high.
Destination	
Single Port	Enables you to specify a single destination port.
Port Range	Enables you to specify the destination port range from low to high.
Other options within the panel include:	
Add	Allows you to add the Extended ACL Number.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Source	
Source Port System defined	Enables you to define the source port system.

Source Range System defined	Enables you to define the source range system.
Destination	
Destination Port System defined	Enables you to define the destination port system.
Destination Range System defined	Enables you to define the destination range system.

Configuring an IP access group

Select **Configure > System > IP Access group** to configure an IP access group.

FIGURE 53 Configuring a IP access group



The IP group contains the following information.

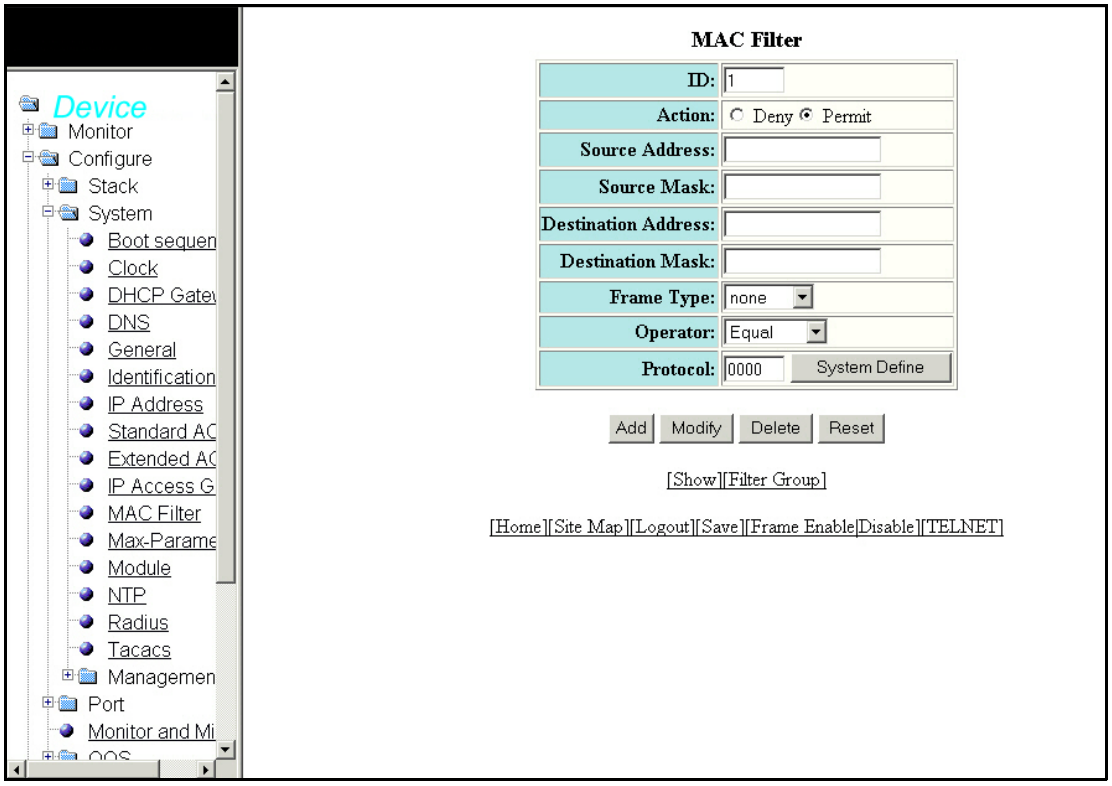
Port	The port attached to the device for which the entry was made.
Direction	Specifies the direction you want the filtering to take place.
ACL Number	Displays the ACL number.
Add	Allows you to add the port number.

Delete	Allows you to delete any changes made.
Reset	To undo your changes, click Reset.
Show	Displays if there are any entries.
Select Name ACLs	Clicking on this parameter allows you to enter the ACL Name

Configuring the system MAC filter

Select **Configure > System > MAC filter** to configure system MAC filter**.** Click **Reset** to undo changes.

FIGURE 54 Configuring a MAC filter

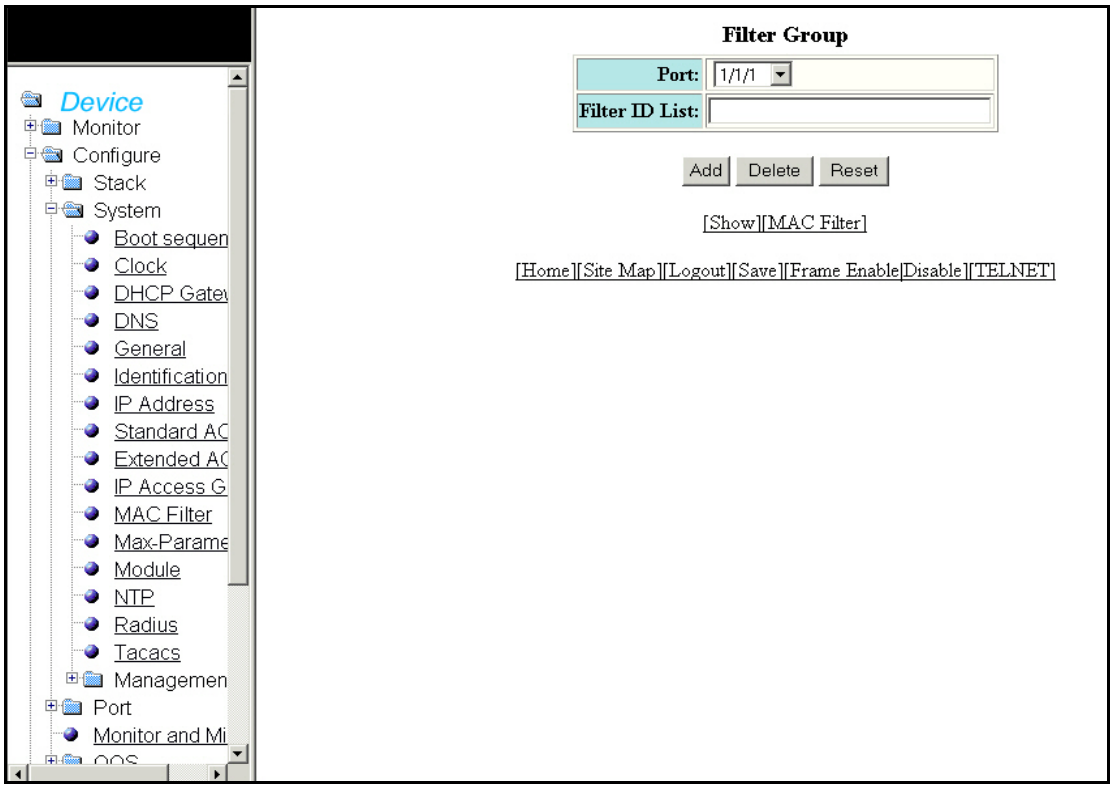


The MAC Address display contains the following information.

ID	Displays the identification of MAC Filter
Action	The action the router takes if a RIP route packet matches the IP address and subnet mask of the filter. The action can be one of the following: • deny – The ACL will deny (drop) packets that match a policy in the access list. • permit – The ACL will permit (forward) packets that match a policy in the access list.
Source Address	The source identification number in the IP.
Source Mask	The source mask is a bitmap picture (jpg or bmp), where the black areas are ignored (thus transparent) and the white areas are used for the frame and text.

Destination Address	The destination identification number in the IP.
Destination Mask	This is a network mask applied to the destination address. It is specified as a 32-bit IP address in dotted decimal format. The destination-mask attribute apples to all protocols.
Frame type	The Frame type can be any one of the following: • none • ethernet • llc • snap
Operator	The comparison operator for TCP or UDP port names or numbers. **NOTE:** This field applies only if the IP protocol is TCP or UDP.
Protocol	The IP protocol can be one of the following well-known names or any IP protocol number from 0 – 255. • Internet Control Message Protocol (ICMP) • Internet Group Management Protocol (IGMP) • Internet Gateway Routing Protocol (IGRP) • Internet Protocol (IP) • Open Shortest Path First (OSPF) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP)
System Define	Displays the system defined protocol.
Add	Allows you to add the MAC Addresses.
Modify	Allows you to modify the changes made.
Delete	Allows you to delete the changes made.
Show	Click Show to see the current MAC Filter configuration.
Filter Group	Click Filter Group to see information about a specific MAC Filter group, as shown in Figure 55.

FIGURE 55 Filter Group



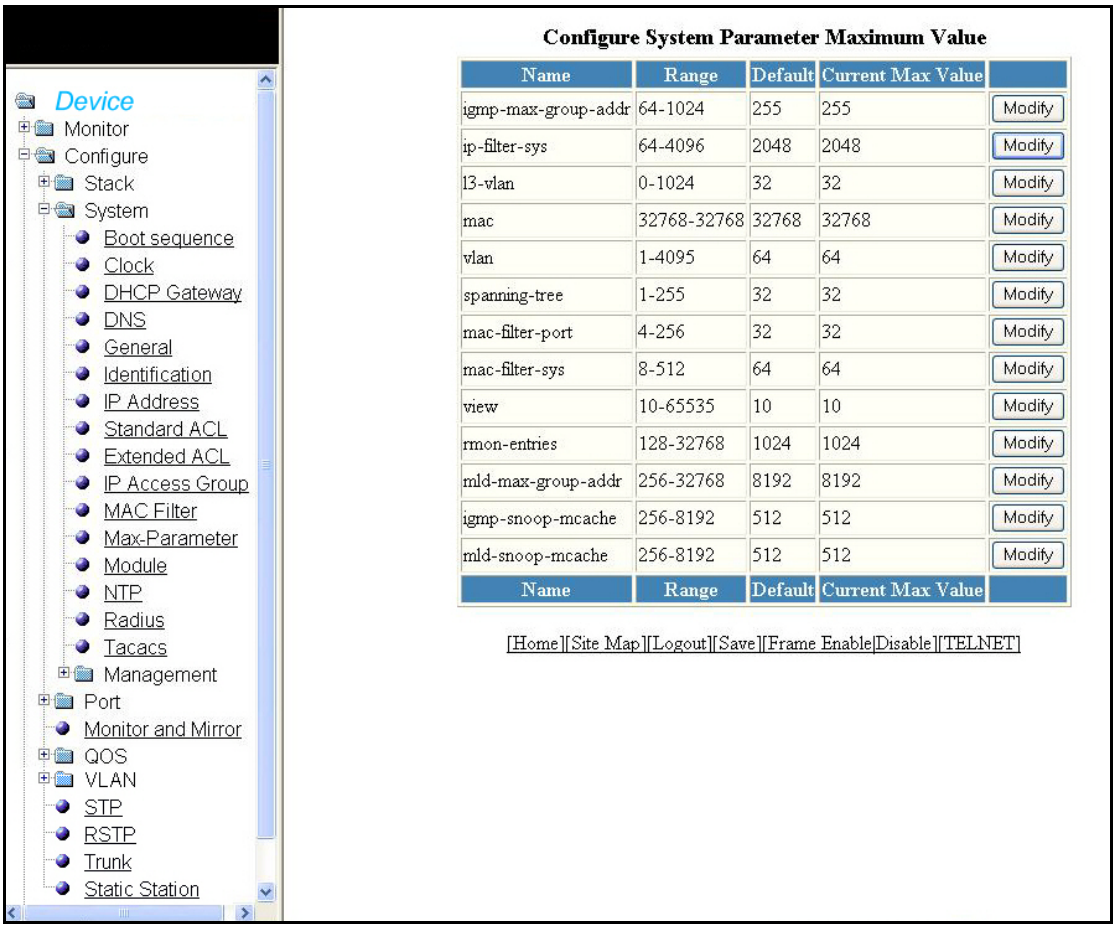
The Filter Group display contains the following information.

Port	Specifies the port number.
Filter ID List	Displays the list of Filter IDs.
Show	Displays the added MAC Filter entries.
MAC Filter	Click MAC Filter to go back to the MAC filter screen as shown in Figure 55.

Configuring the maximum system value

Select **Configure > System > Max-Parameter** to configure the maximum system value parameter.

FIGURE 56 Configuring the maximum system parameter

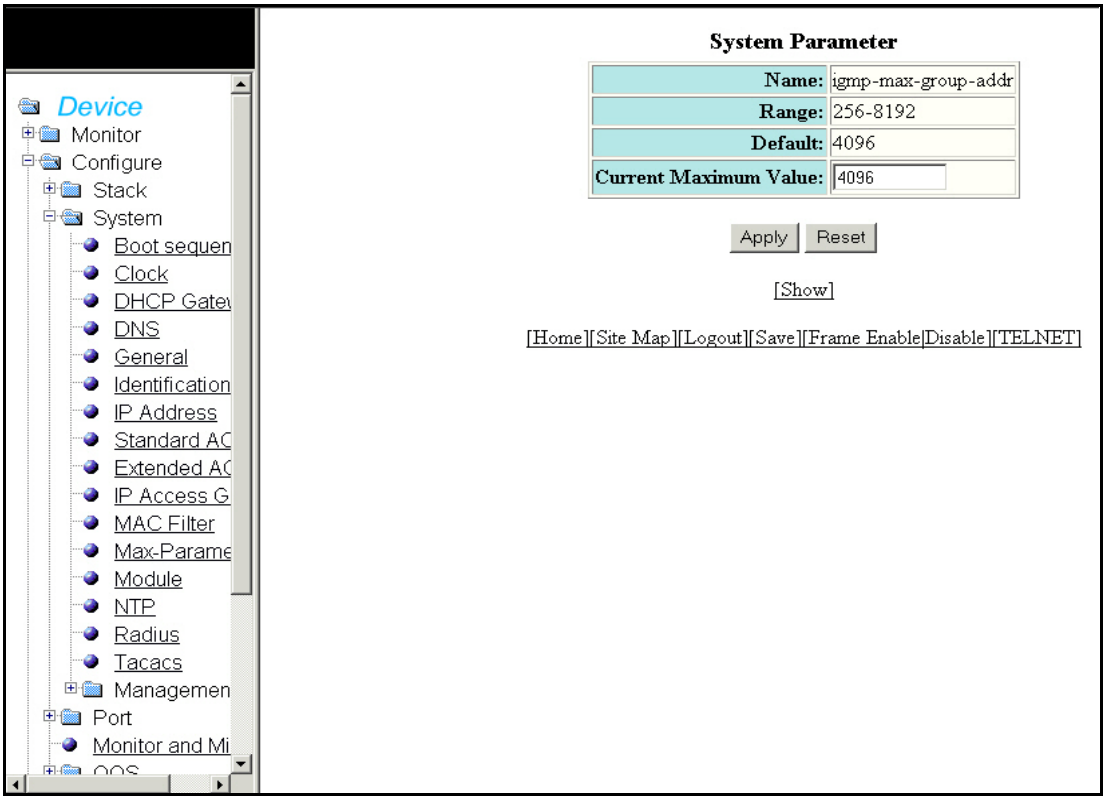


The Configure System Parameter Maximum Value display contains the following information.

Name	An optional name assigned to the port
Range	Specifies the range of values for the port.
Default	Displays the default value for the port.
Current Max Value	Displays the current maximum value for the port.

Click **Modify** to change the maximum value. Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 57 Modifying the maximum parameter value

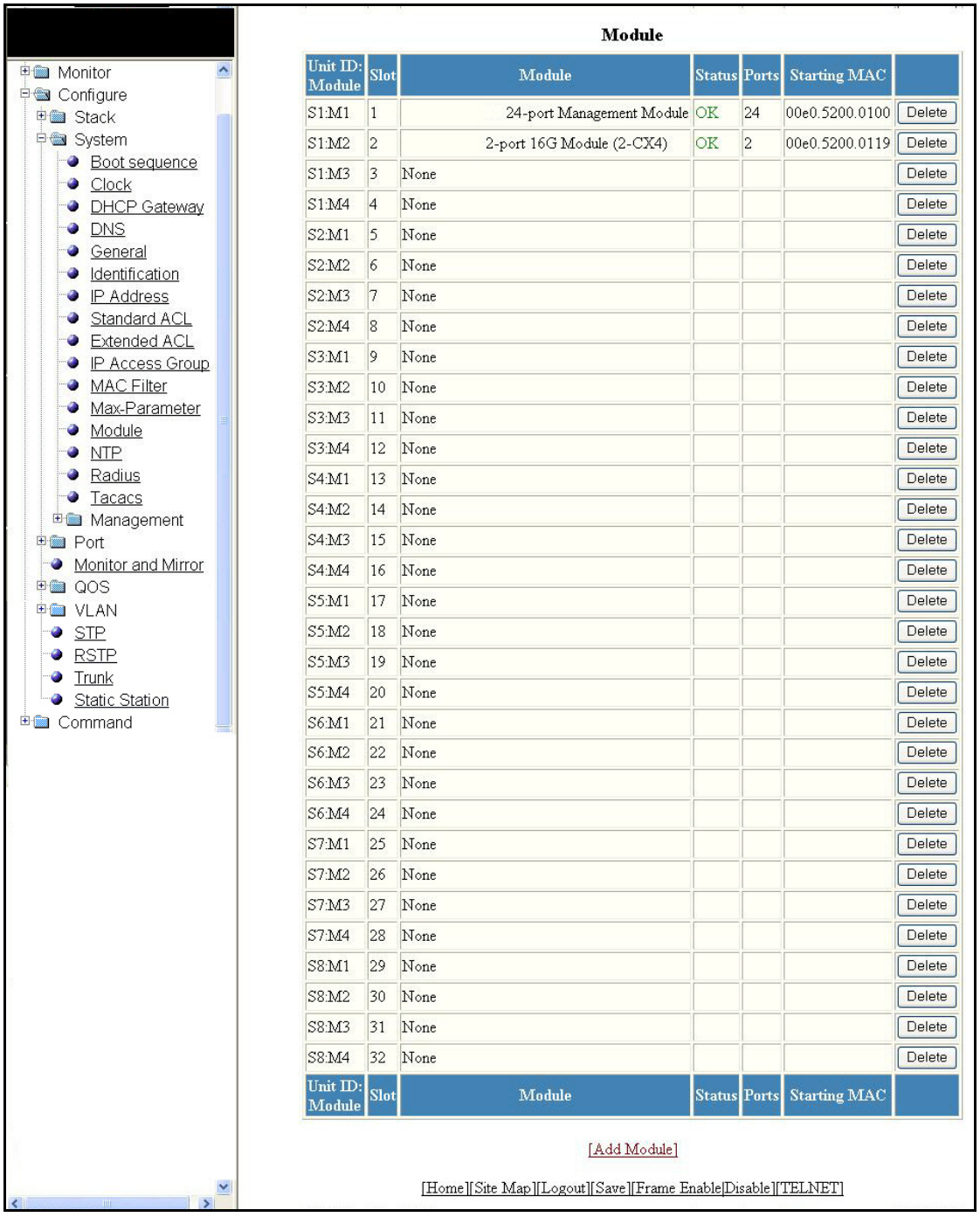


Click **Show** to show the new maximum parameter value.

Configuring a system module

Select **Configure > System > Module** to configure a system module. Click **Delete** to delete any module.

FIGURE 58 Configuring system module

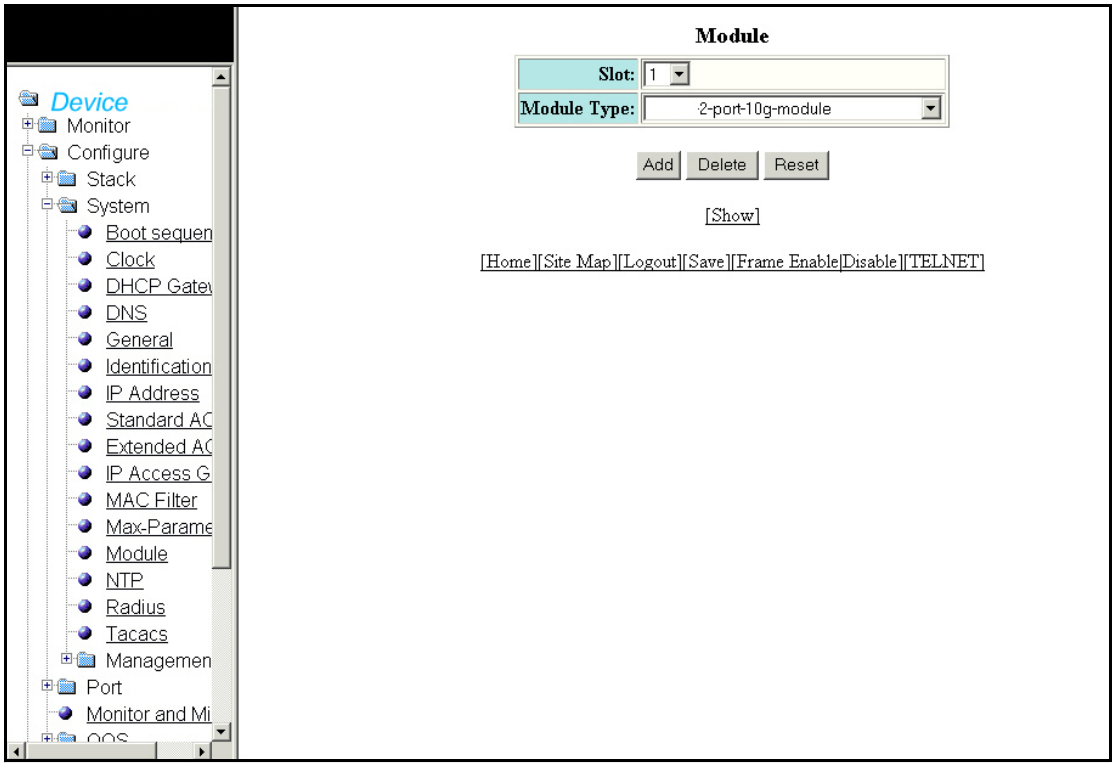


Unit ID: Module	Slot	Module	Status	Ports	Starting MAC	
S1:M1	1	24-port Management Module	OK	24	00e0.5200.0100	Delete
S1:M2	2	2-port 16G Module (2-CX4)	OK	2	00e0.5200.0119	Delete
S1:M3	3	None				Delete
S1:M4	4	None				Delete
S2:M1	5	None				Delete
S2:M2	6	None				Delete
S2:M3	7	None				Delete
S2:M4	8	None				Delete
S3:M1	9	None				Delete
S3:M2	10	None				Delete
S3:M3	11	None				Delete
S3:M4	12	None				Delete
S4:M1	13	None				Delete
S4:M2	14	None				Delete
S4:M3	15	None				Delete
S4:M4	16	None				Delete
S5:M1	17	None				Delete
S5:M2	18	None				Delete
S5:M3	19	None				Delete
S5:M4	20	None				Delete
S6:M1	21	None				Delete
S6:M2	22	None				Delete
S6:M3	23	None				Delete
S6:M4	24	None				Delete
S7:M1	25	None				Delete
S7:M2	26	None				Delete
S7:M3	27	None				Delete
S7:M4	28	None				Delete
S8:M1	29	None				Delete
S8:M2	30	None				Delete
S8:M3	31	None				Delete
S8:M4	32	None				Delete
Unit ID: Module	Slot	Module	Status	Ports	Starting MAC	

The table shows the following information.

Unit Id:Module	Displays the Unit Id of the management module.
Slot	The Interface module / slot number.
Module	Identifies the module, by stack unit ID, module number, module type
Status	Displays the status of this module.
Ports	Displays the number of ports in this module.
Starting MAC	The starting MAC address for this module
Add Module	Click **Add Module** to add a management module, as shown in Figure 59.

FIGURE 59 Adding system module



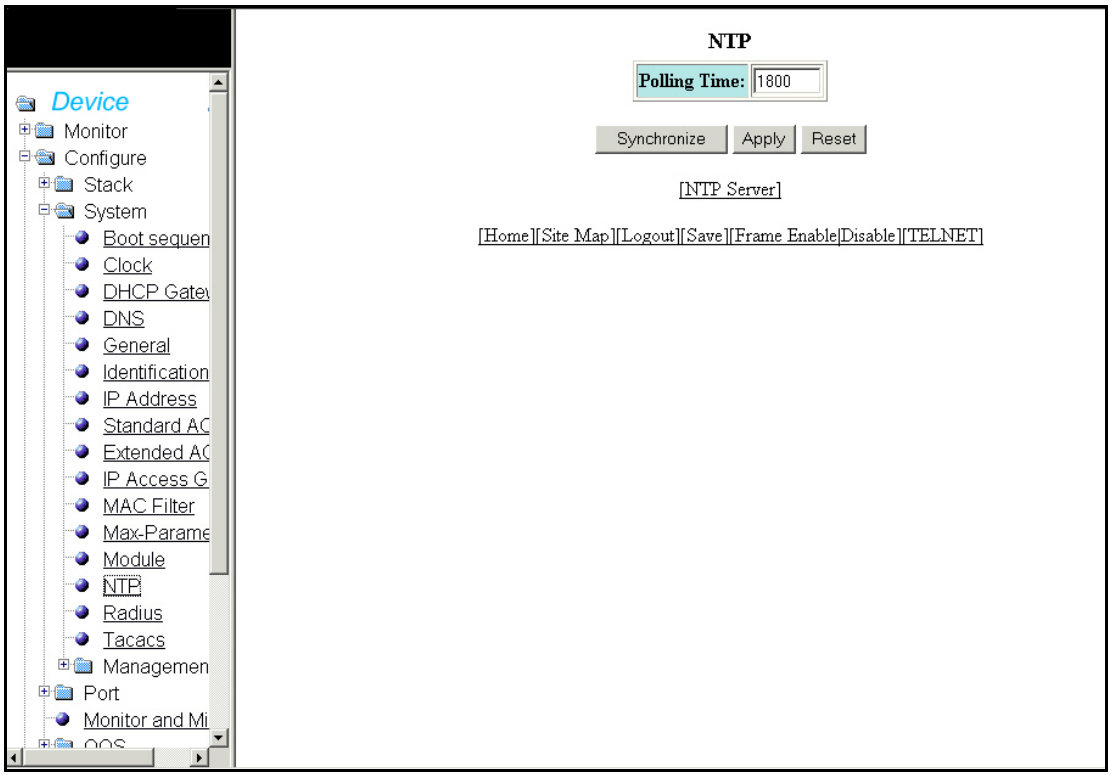
The Module display contains the following information.

Slot	The Interface module / slot number.
Module Type	Identifies the module type.
Add	Allows you to add the MAC Addresses.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the added module details.

Configuring an NTP Server

Select **Configure > System > NTP** to configure an NTP server.

FIGURE 60 Configuring a Network Transfer Protocol (NTP) server



The table shows the following information.

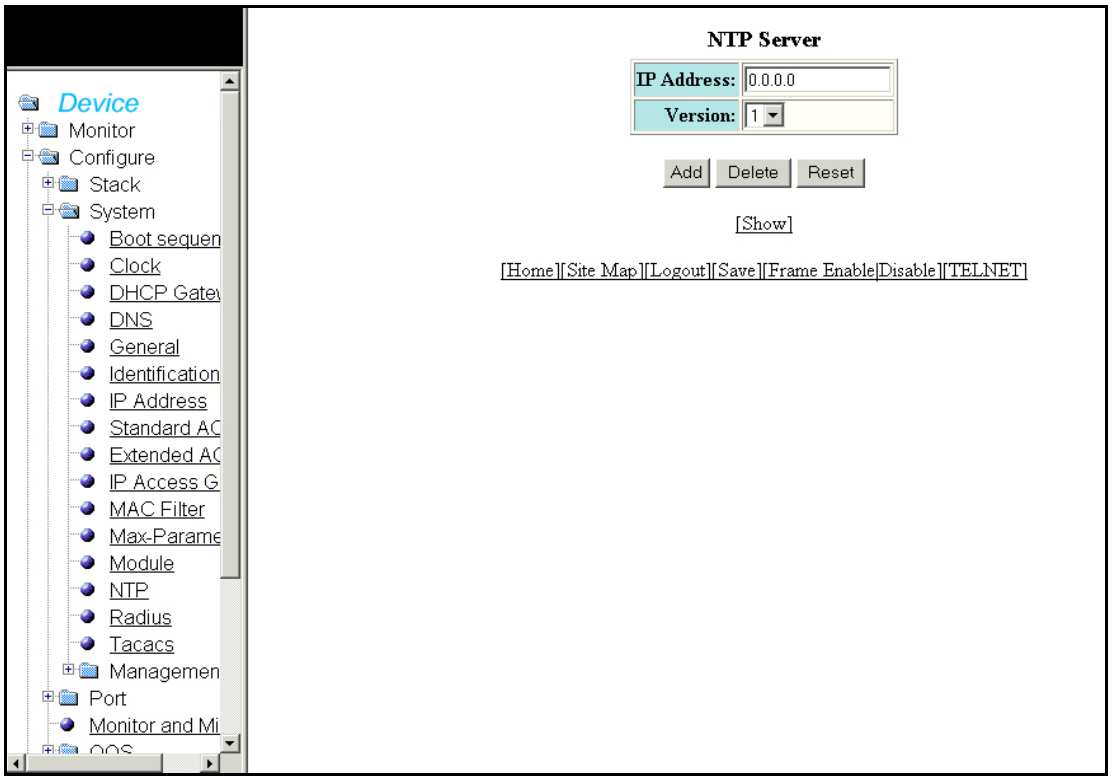
Polling Time	This parameter allows you to specify the minimum poll interval for NTP messages.
• Synchronize	System is synchronized to an NTP peer.
• Apply	To save your configuration, click **Apply**.
• Reset	To undo your changes, click Reset.

You can view the details of:

- NTP Server

Click **NTP Server** to display the NTP server information.

FIGURE 61 NTP server information



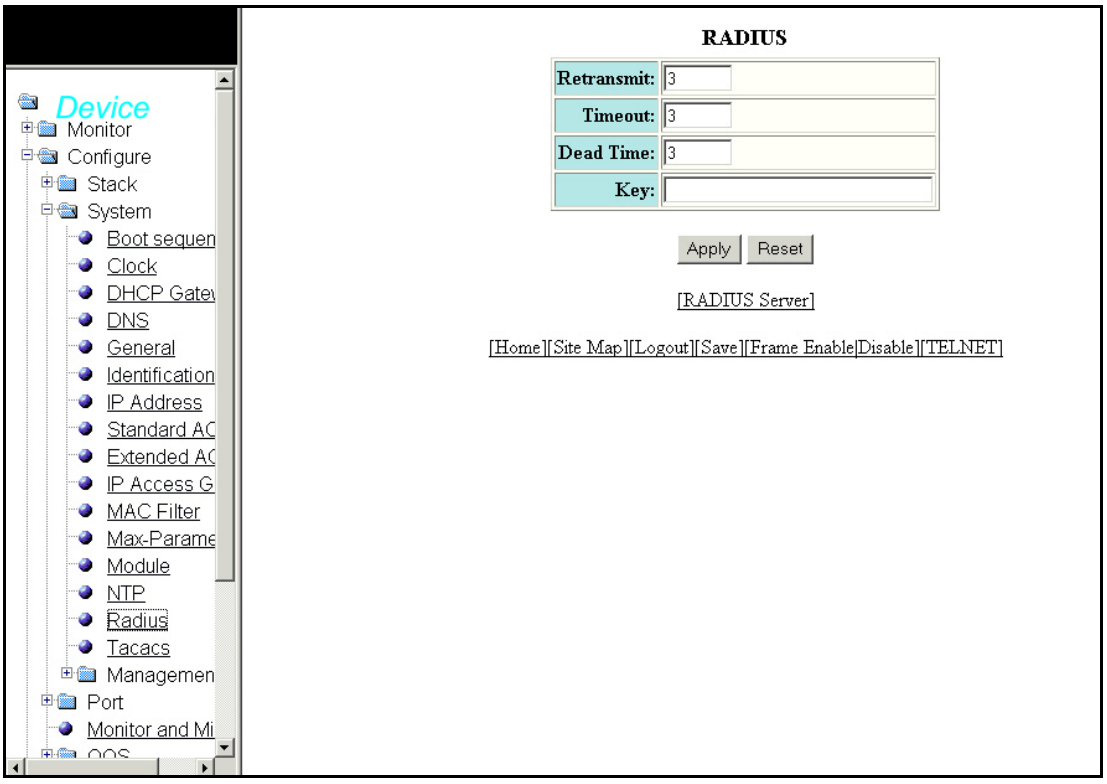
The NTP display contains the following information.

IP Address	The IP Address of the route's destination.
Version	Displays the version of the NTP Server.
Add	Allows you to add the IP Address.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the NTP Server entries.

Configuring a RADIUS server

Select **Configure > System > RADIUS** to configure a RADIUS server**.** Click **Apply** to save your configuration or click **Reset**. to undo changes.

FIGURE 62 Configuring a RADIUS server

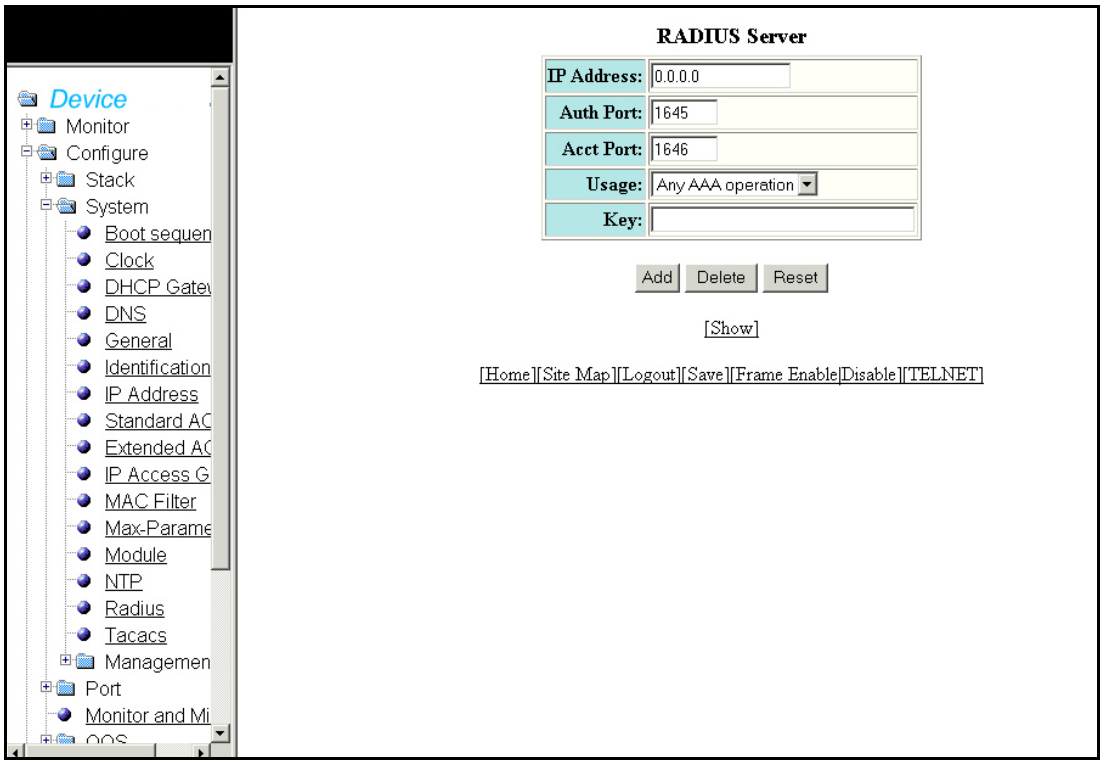


The RADIUS display contains the following information.

Retransmit	This parameter specifies how many times the Dell device will resend an authentification request when the RADIUS server does not respond. The retransmit value can from 1-5 times. The default is 3 times.
Timeout	This parameter specifies how many seconds the Dell device waits for a response from a RADIUS server before either retrying the authentication request, or determining that the RADIUS servers are unavailable and moving on to the next authentication method in the authentication-method list. The timeout can be from 1 – 15 seconds. The default is 3 seconds.
Dead Time	This parameter specifies how long the Dell device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3 seconds.
Key	This parameter in the RADIUS-server command is used to encrypt RADIUS packets before they are sent over the network. The value for the key parameter on the Dell device should match the one configured on the RADIUS server. The key can be from 1 – 32 characters in length and cannot include any space characters.

Click **Show** to display the current RADIUS server configuration, as shown in Figure 63.

FIGURE 63 RADIUS server information



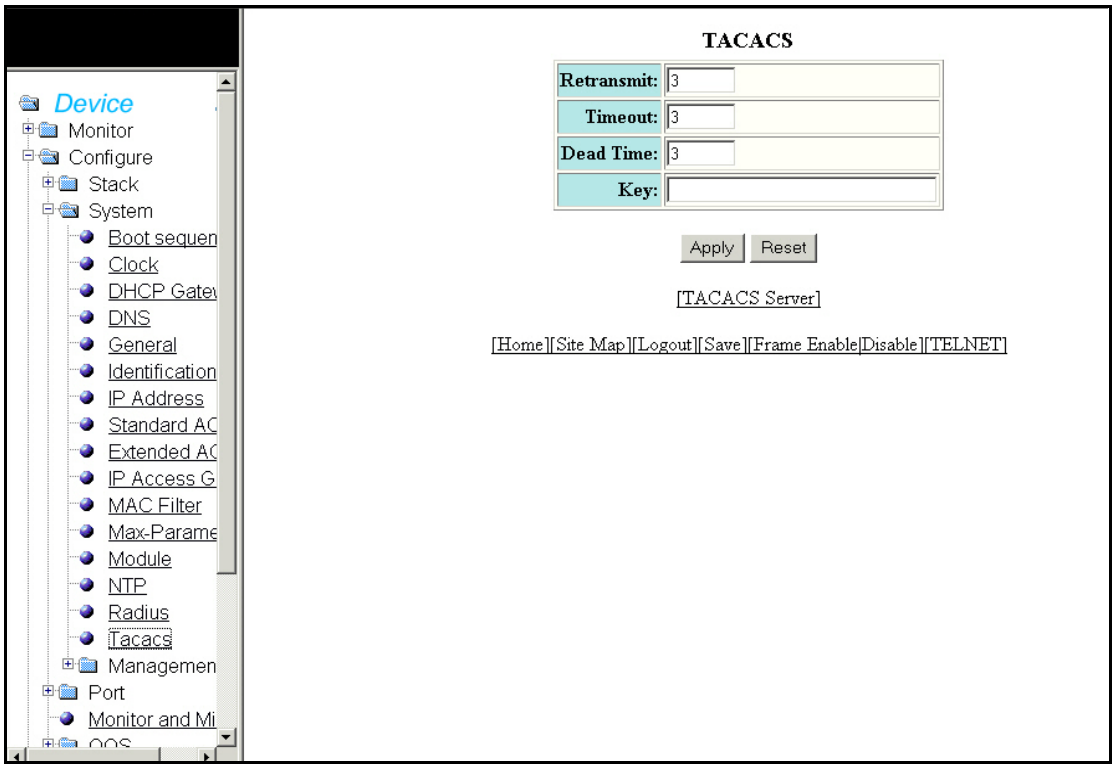
The RADIUS Server display contains the following information.

IP Address	The IP Address of the route's destination.
Auth Port	This parameter specifies the Authentication port number. It is an optional parameter. The default is 1645.
Acct Port	This parameter specifies the Accounting port number. It is an optional parameter. The default is 1646.
Usage	Enables the server to be used in any of the four modes: • Authentication-only • Authorization-only • Accounting-only • Any AAA operation
Add	Allows you to add the IP Address.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the RADIUS server entries.

Configuring a TACACS/TACACS+ server

Select **Configure > System > Tacacs** to configure a TACACS server. Click **Apply** to save your configuration or click **Reset** to undo changes.

FIGURE 64 Configuring a TACACS/TACACS+ server

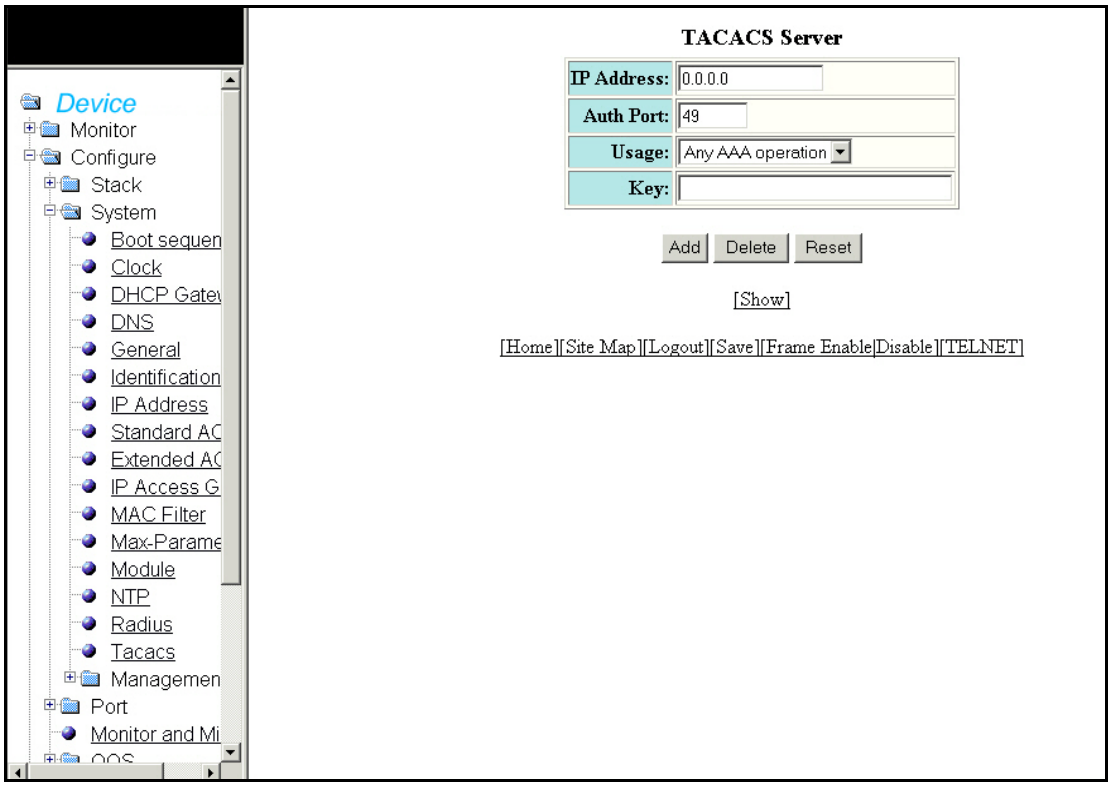


The TACACS display contains the following information.

Retransmit	This parameter specifies how many times the Dell device will resend an authentification request when the TACACS/TACACS+ server does not respond. The retransmit value can from 1-5 times. The default is 3 times.
Timeout	This parameter specifies how many seconds the Dell device waits for a response from a TACACS/TACACS+ server before either retrying the authentication request, or determining that the TACACS/TACACS+ servers are unavailable and moving on to the next authentication method in the authentication method list. The timeout can be from 1 – 15 seconds. The default is 3 seconds.
Dead Time	This parameter specifies how long the Dell device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3 seconds.
Key	This parameter in the tacacs-server command is used to encrypt TACACS+ packets before they are sent over the network. The value for the key parameter on the Dell device should match the one configured on the TACACS+ server. The key can be from 1 – 32 characters in length and cannot include any space characters.
Tacacs Server	Displays the TACACS Server information.

Click **Show** to display the current TACACS/TACACS+ server configuration, as shown in Figure 65.

FIGURE 65 TACACS/TACACS+ Server Information



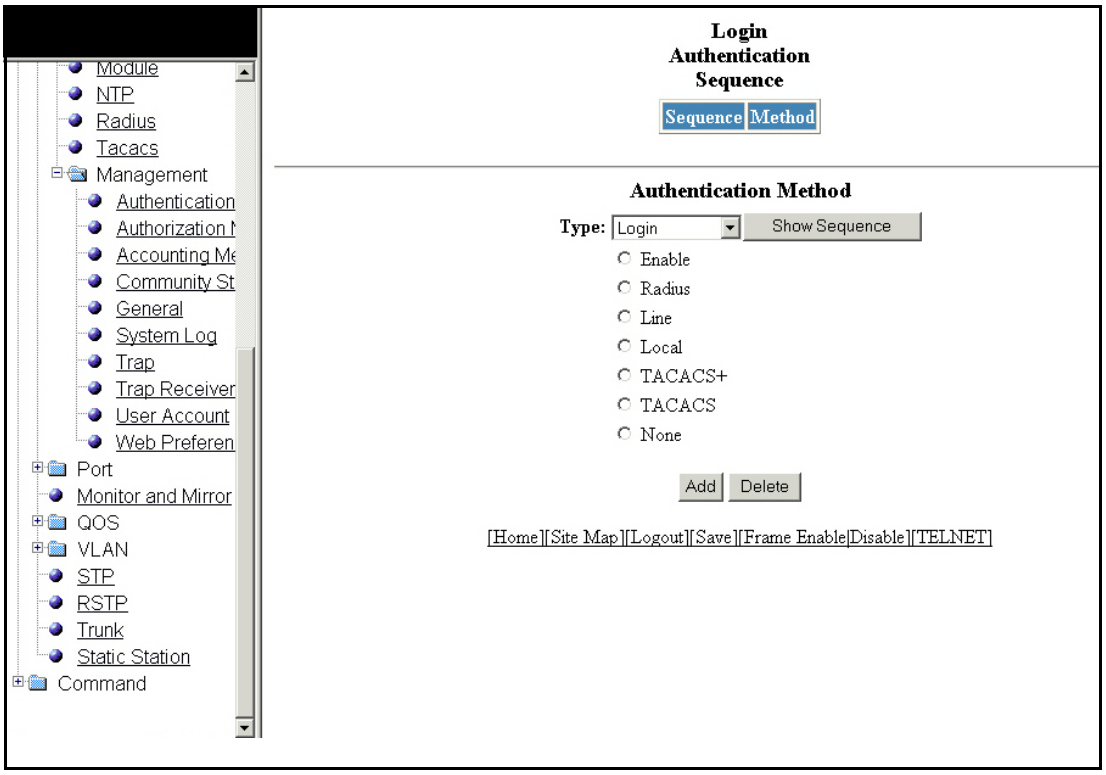
The TACACS Server display contains the following information.

IP Address	The IP Address of the destination for the route.
Auth Port	This parameter specifies the UDP (for TACACS) or TCP (for TACACS+) port number of the authentication port on the server.
Usage	Enables the server to be used in any of the four modes: • Authentication-only • Authorization-only • Accounting-only • Any AAA operation
Add	Allows you to add the IP Address.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the TACACS server entries.

Configuring management authentication

Select **Configure > System > Management > Authentication methods** to configure management authentication.

FIGURE 66 Configuring management authentication

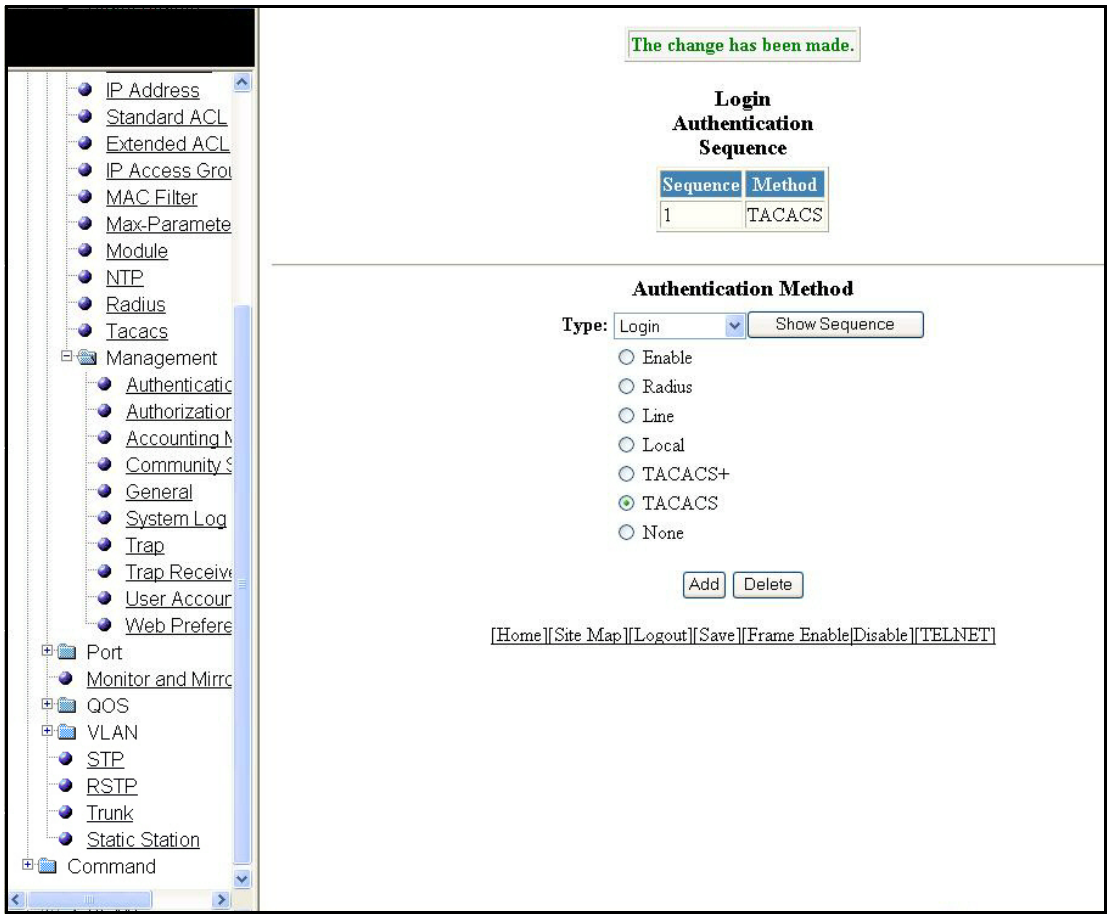


The Login Authentication Sequence display the following information.

Type	Specifies the type of authentication to be used • Login • Enable • Web Server • SNMP Server
Add	Enables to add the authentication methods.
Delete	Enables to delete the added methods.
Show Sequence	Displays the list of authentication methods added.

Click **Add** to display the current authentication method that is configured, as shown in Figure 67.

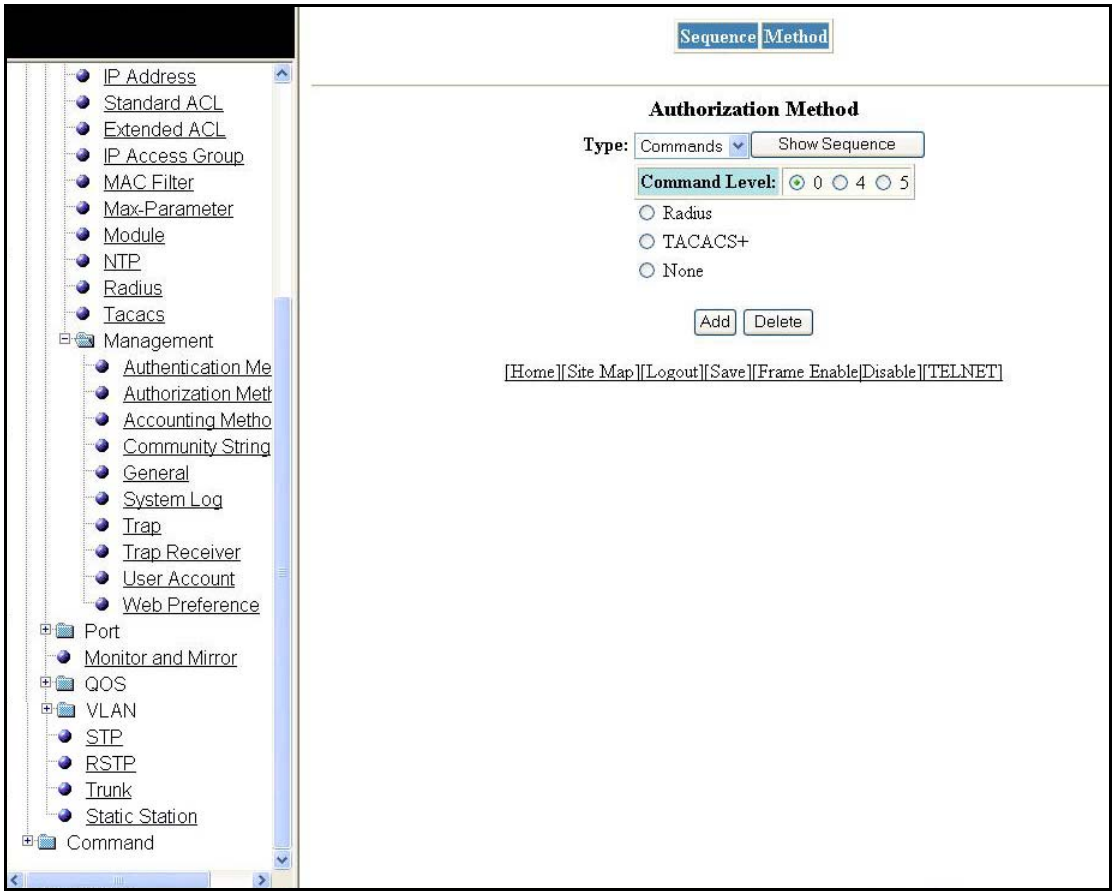
FIGURE 67 Viewing the configured management authentication method



Configuring management authorization

Select **Configure > System > Management > Authorization methods** to configure management authorization.

FIGURE 68 Configuring management authorization



The Authentication Method display contains the following information.

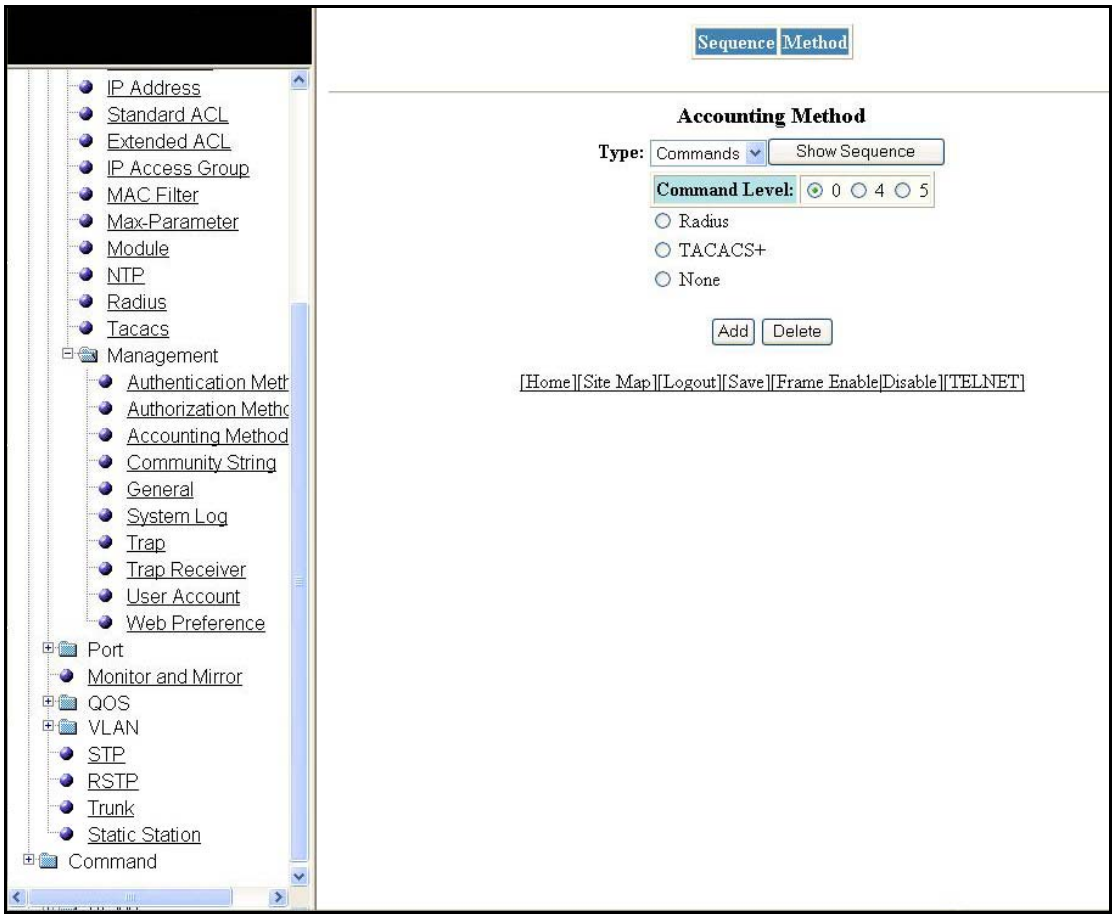
Type	Specifies the mode of authorization • Commands • Exec
Command Level	Allows you to select the command level.
Add	Enables to add the authorization methods.
Delete	Enables to delete the added methods.
Show Sequence	Displays the list of authorization methods added.

Click **Add** to display the authorization method currently configured, as shown in Figure 69

Configuring management accounting

Select **Configure > System > Management > Accounting methods** to configure management accounting,.

FIGURE 69 Configuring management accounting methods



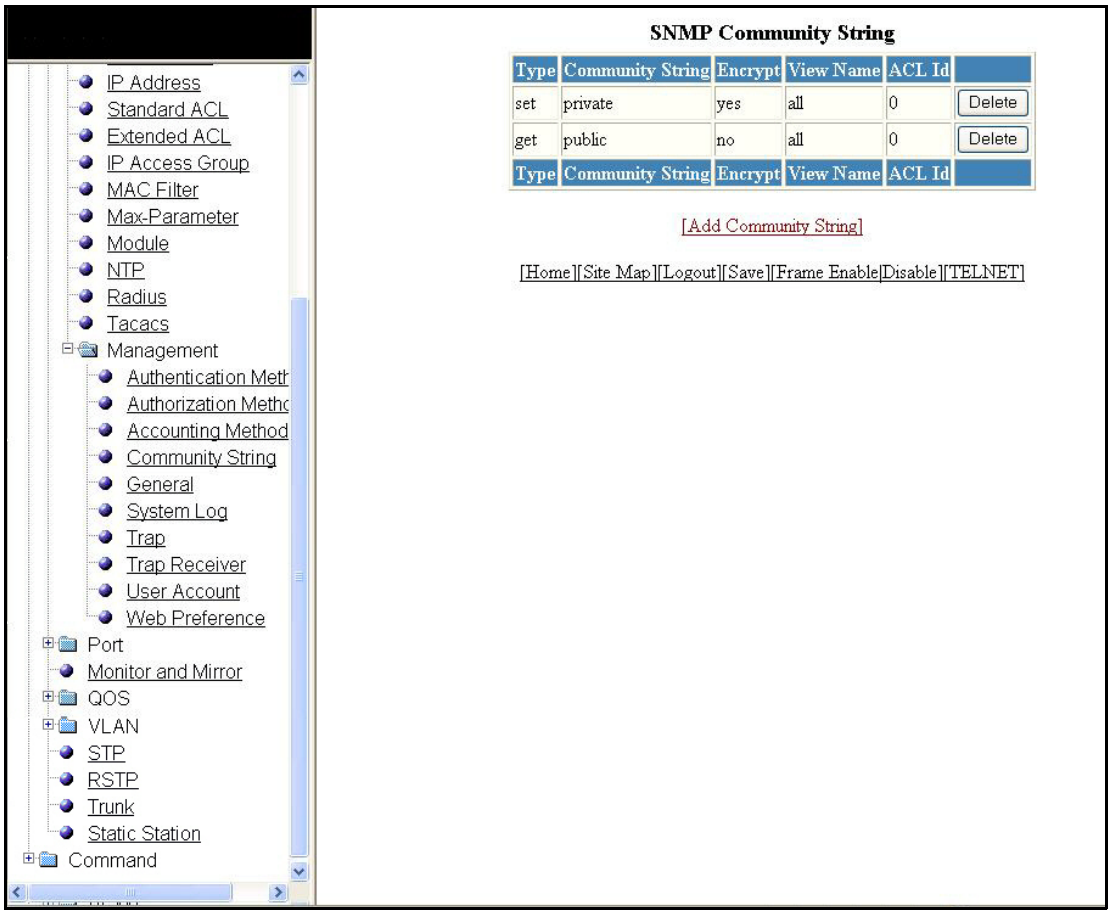
The Accounting Method display contains the following information.

Type	Specifies the mode of authorization • Commands • Exec • System
Command Level	Allows you to select the command level.
Add	Enables to add the accounting methods.
Delete	Enables to delete the added methods.
Show Sequence	Displays the list of accounting methods added.
Add	Click Add to show the current configured accounting method.

Configuring an SNMP community string

Select **Configure > System > Management > Community String** to configure an SNMP community string.

FIGURE 70 Configuring an SNMP community string

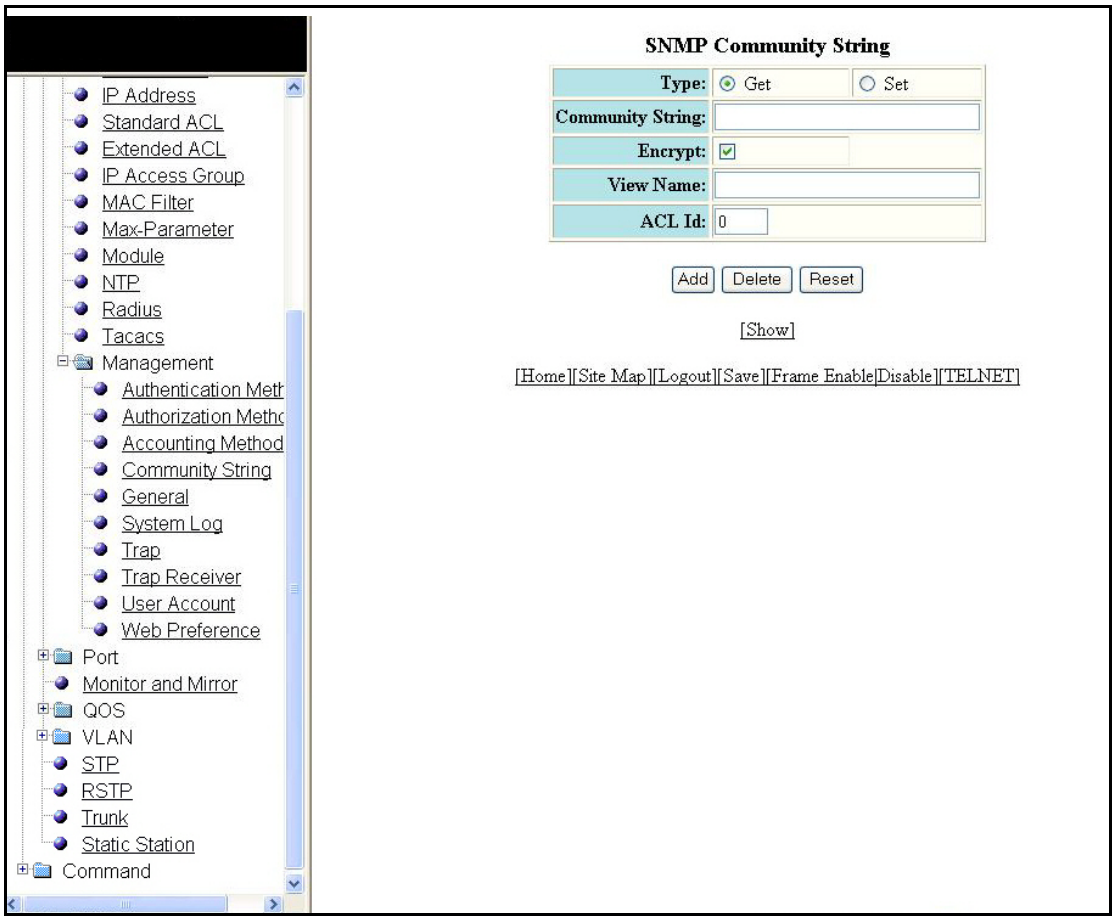


The SNMP Community String display contains the following information.

Type	Displays the type of login username and password.
Community String	Displays the username to open a web management session.
Encrypt	Specifies if encryption is enabled for a particular string.
View Name	Specifies the name of the community string.
ACL Id	This parameter identifies a collection of individual ACL entries.
Delete	Enables you to delete the community string.
Add Community String	Allows you to add a new community string.

Click **Add** to view the current configured SNMP Community String, as shown in Figure 71.

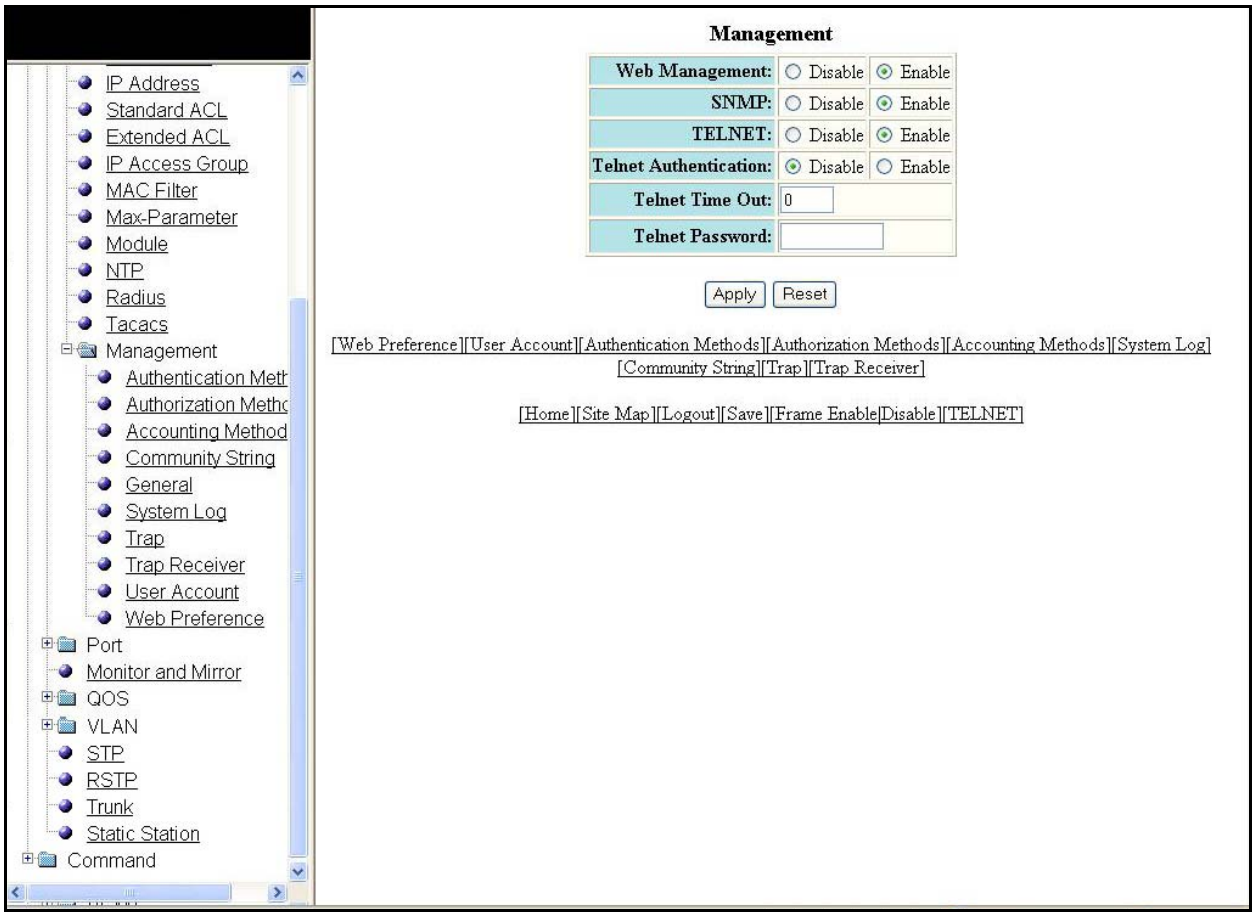
FIGURE 71 Adding Community strings



Configuring general management parameters

Select **Configure > System > Management > General** to configure the management**.** Click **Apply** to save the configuration or click **Reset** to undo changes.

FIGURE 72 Configuring general management parameters



The Management display contains the following information.

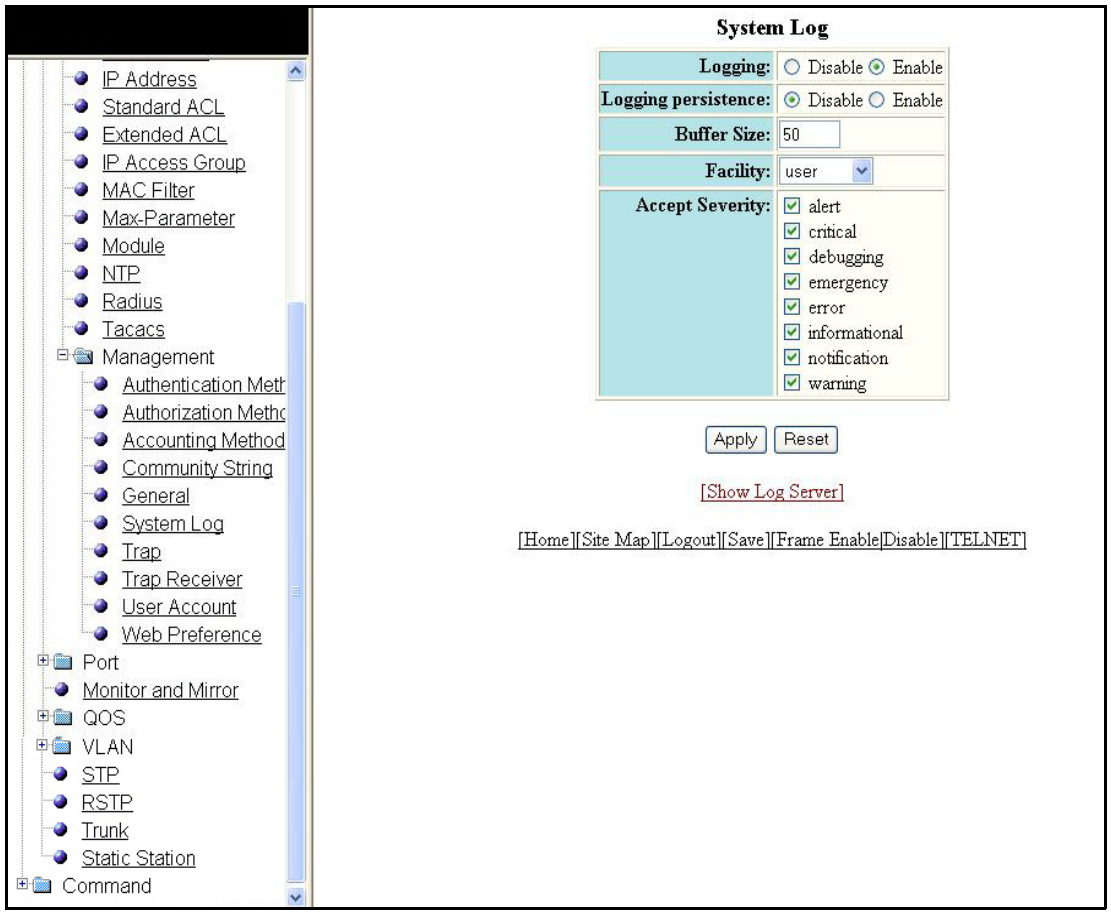
Web Management	Allows you to enable or disable Web Management.
SNMP	Allows you to enable or disable SNMP.
Telnet	Allows you to enable or disable TELNET.
Telnet Authentication	Allows you to enable or disable Telnet Authentication.
Telnet Time Out	Set a default timeout to wait for a response. Specified in seconds. Default is no timeout.
Telnet Password	Enables you to enter the Telnet password.
Web Preference	Allows you to configure the web management preferences.
User Account	Allows you to login with the user account.
Authentication Methods	Allows you to configure the authentication methods.
Authorization Methods	Allows you to configure the authorization methods.
Accounting Methods	Allows you to configure the accounting methods.

System Log	Allows you to modify the system log.
Community String	Allows you to modify.
Trap	Allows you to configure the Trap.
Trap Receiver	Allows you to configure the Trap Receiver.

Configuring a management system log

Select **Configure > System > Management > System Log** to configure a system log. Click **Apply** to save the configuration or click **Reset** to undo changes.

FIGURE 73 Configuring a system log

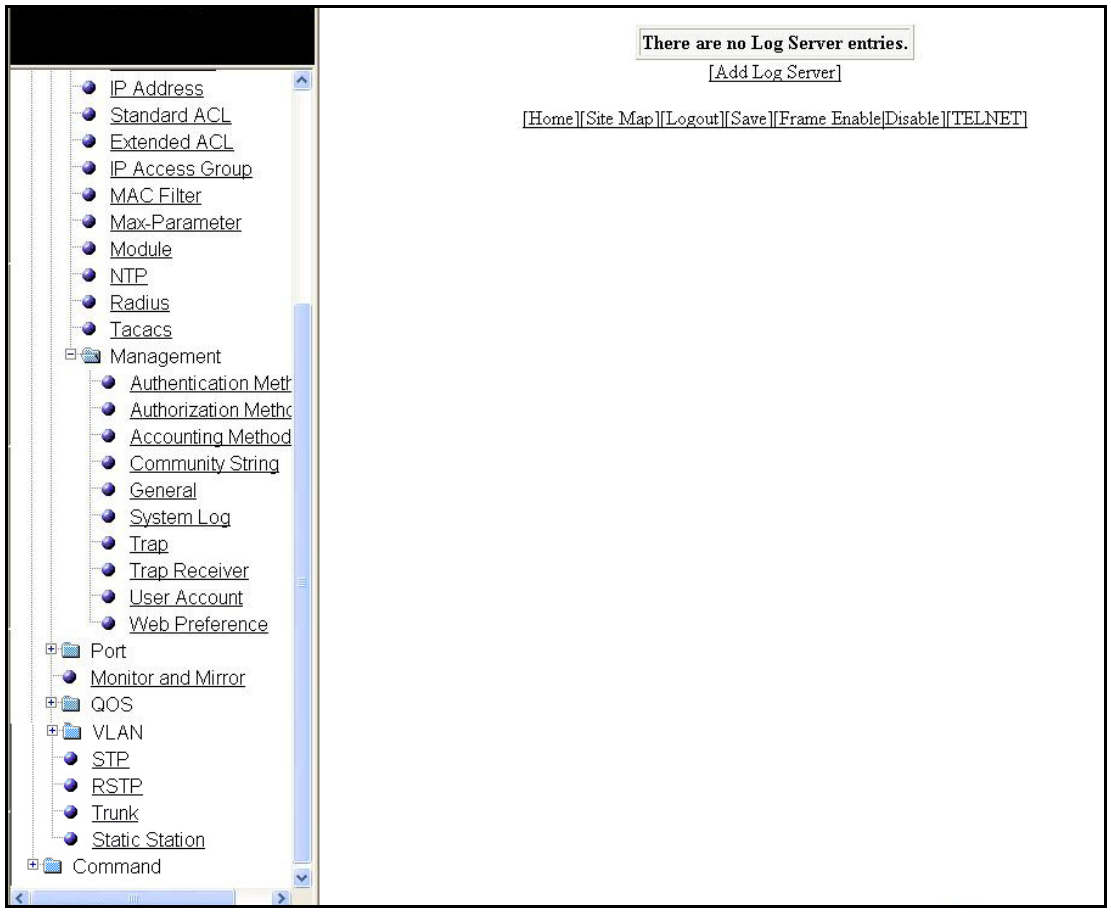


The System Log display contains the following information.

Logging	The state (enabled or disabled) of the Syslog buffer.
Logging persistence	Allows you to enable or disable Logging persistence.
Buffer size	The number of messages.
Facility	Displays the list of facilities available.
Accept Severity	Displays the severity levels.

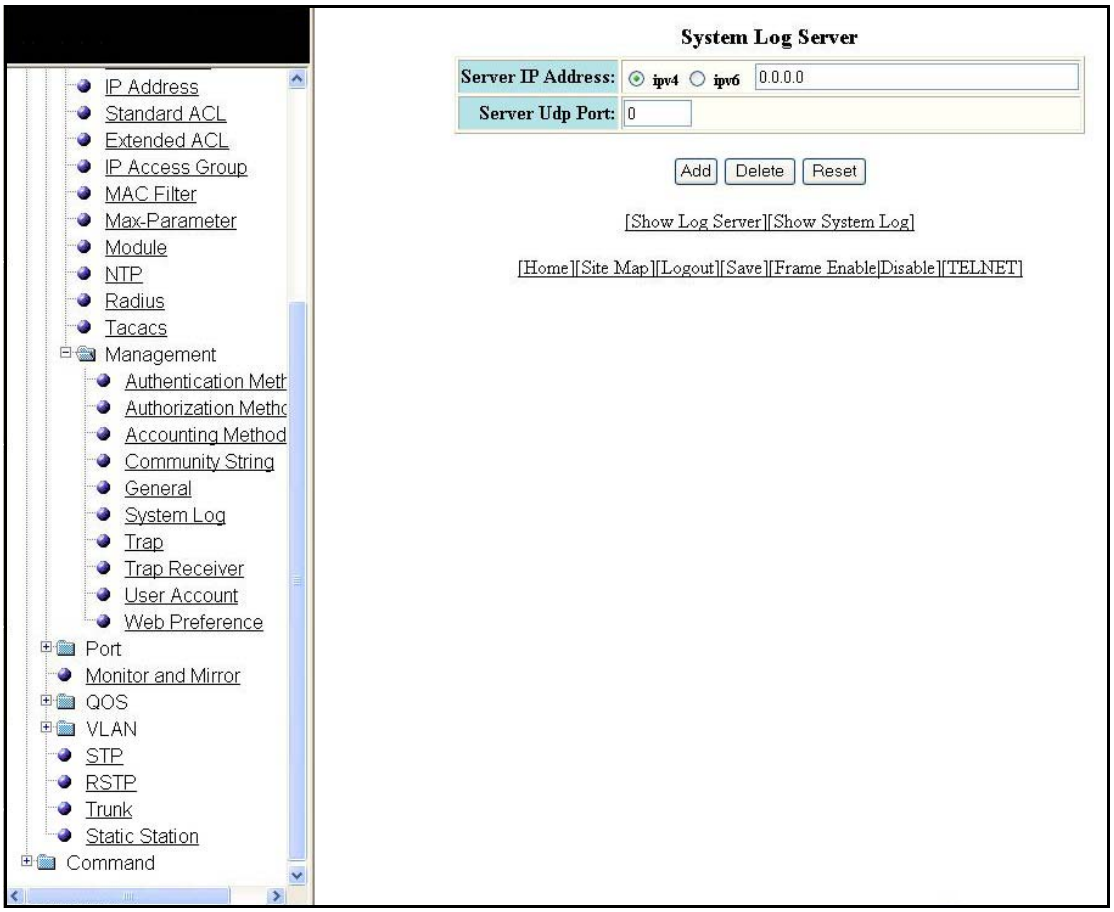
Click **Show Log Server to** display log server entries, if any, as shown in Figure 74.

FIGURE 74 Viewing Log Server entries Log Server



Click **Add Log Server** to add extra log servers to your system log configuration, as shown in Figure 75.

FIGURE 75 Add a Log Server



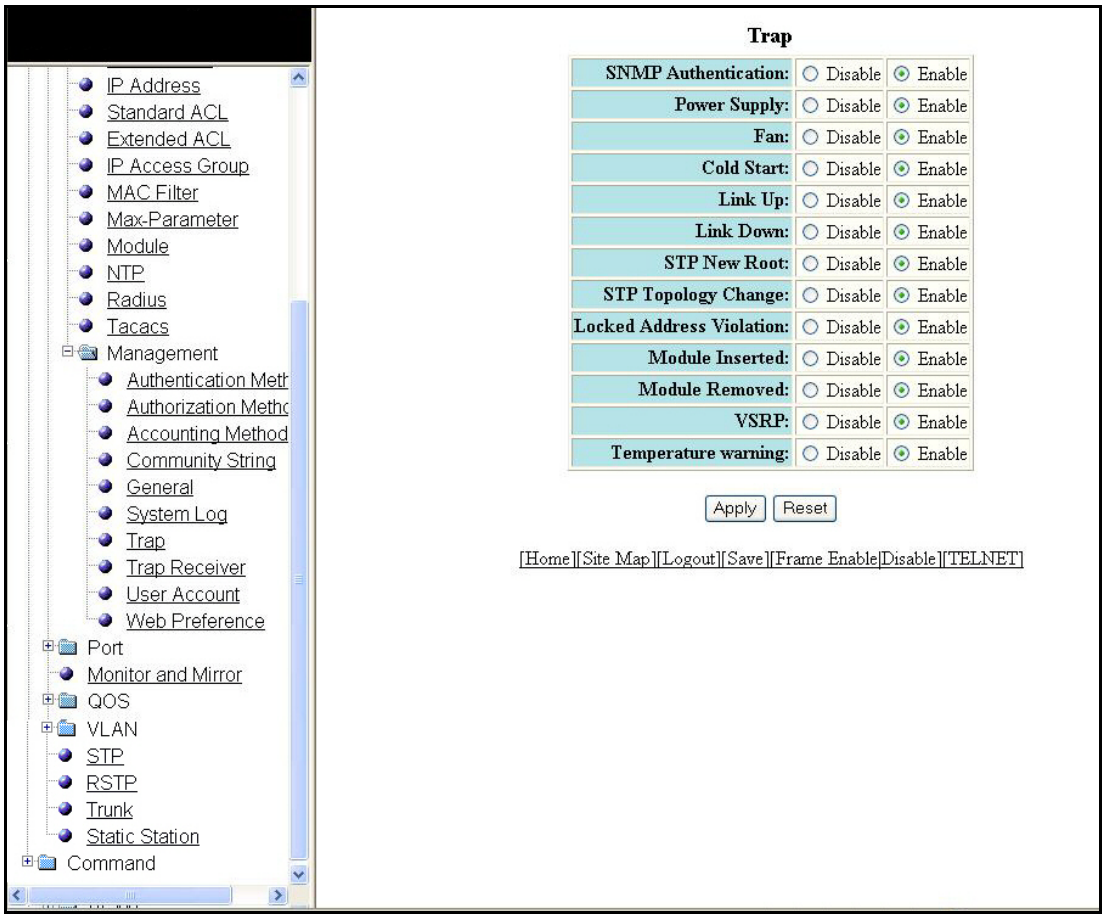
The System Log Server display contains the following information.

Server IP Address	Displays the IP address of IPv4 or IPv6.
Server Udp Port	This parameter specifies the application port used for the Syslog facility. The default is 514.
Add	Allows you to add the server IP Address.
Delete	Allows you to delete the changes made.
Reset	To undo your changes, click Reset.
Show Log Server	Displays the Log Server entries.
Show System Log	Clicking this displays the default screen of the system log.

Configuring a trap

Select **Configure > System > Management > Trap** to configure a trap. Click **Apply** to save the configuration or click **Reset** to undo changes.

FIGURE 76 Configuring a trap



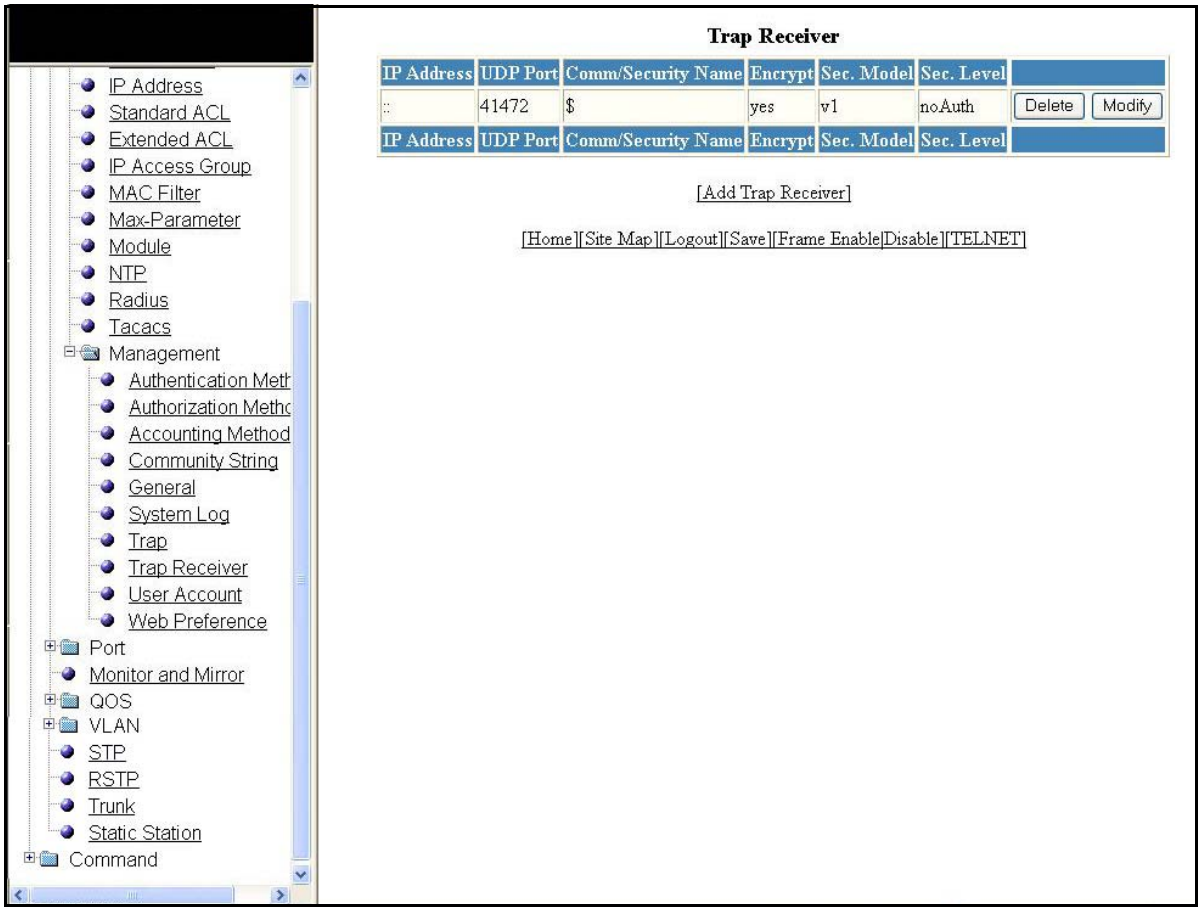
The Trap display contains the following information.

SNMP Authentication	Allows you to enable or disable SNMP Authentication.
Power Supply	Allows you to enable or disable Power Supply.
Fan	Allows you to enable or disable Fan.
Cold Start	Allows you to enable or disable Cold Start.
Link Up	Allows you to enable or disable Link Up.
Link Down	Allows you to enable or disable Link Down.
STP New Root	Allows you to enable or disable STP New Root.
STP Topology Change	Allows you to enable or disable STP Topology Change.
Locked Address Violation	Allows you to enable or disable Locked Address Violation.
Module Inserted	Allows you to enable or disable Module Inserted.
Module Removed	Allows you to enable or disable Module Removed.
VSRP	Allows you to enable or disable VSRP.
Temperature warning	Allows you to enable or disable Temperature warning.

Configuring a trap receiver

Select **Configure > System > Management > Trap Receiver** to configure a trap receiver.

FIGURE 77 Configuring a trap receiver



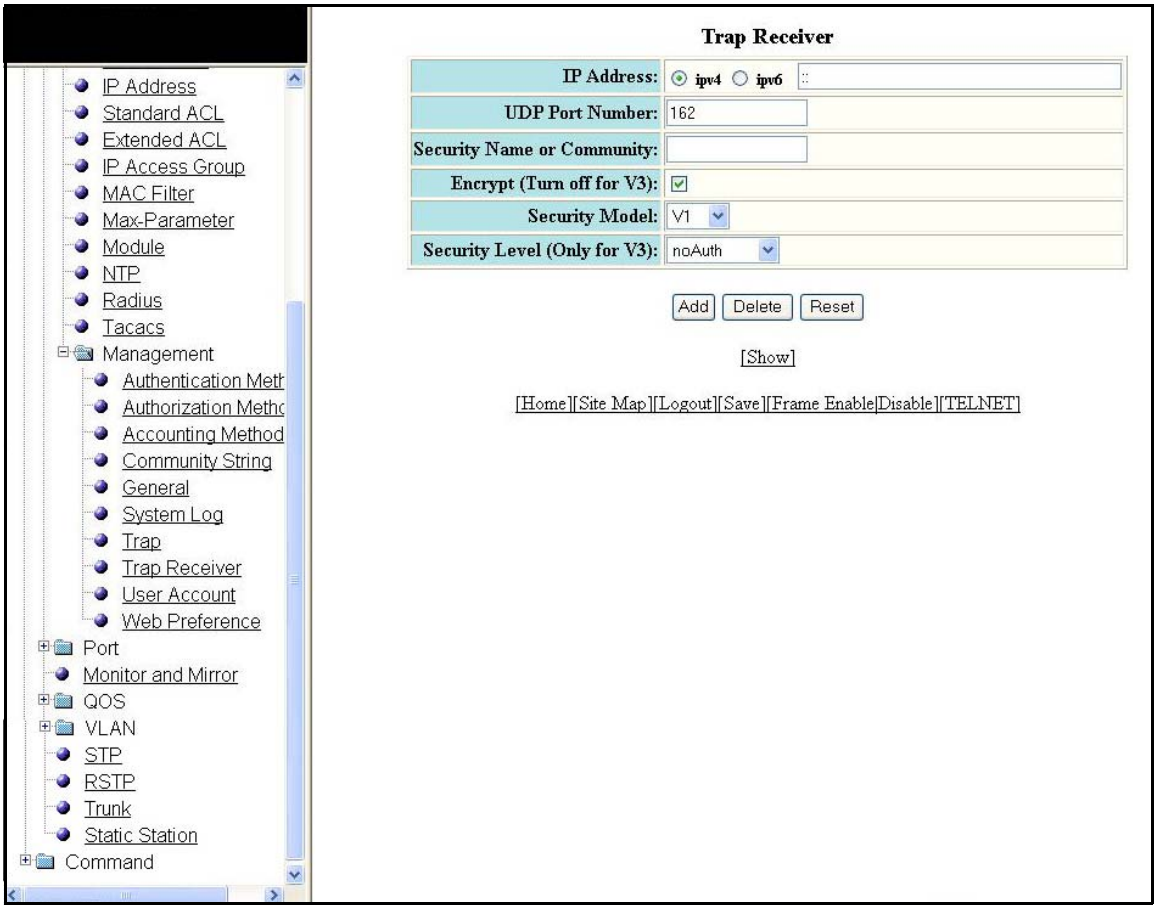
The Trap Receiver display contains the following information.

IP Address	The IP Address of the route's destination.
UDP Port	This parameter specifies the application port used for the Syslog facility. The default is 514.
Delete	Allows you to delete the trap receiver.
Modify	Allows you to modify the data.
Community/Security Name	Arbitrary values made of two five-digit integers joined by a colon. Each string in the community name can be a number from 0-65535.

Encryption	The encryption method used for the connection. This can be IDEA, ARCFOUR, DES, 3DES, AES, or BLOWFISH.
Security Model	Used to secure against the following threats: • Modification of information. • Masquerading the identity of an authorized entity. • Message stream modification. • Disclosure of information.
Security Level	The value for security level can be one of the following: • none - If the security model shows v1 or v2, then security level is blank. User names are not used to authenticate users; community strings are used instead. • noauthNoPriv - Displays if the security model shows v3 and user authentication is by user name only. • noauthNoPriv - Displays if the security model shows v3 and user authentication is by user name and the MD5 or SHA algorithm.
Add Trap Receiver	Allows you to add new Trap Receivers.

Click **Add Trap Receiver** to add and configure a new trap receiver, as shown in Figure 78.

FIGURE 78 Add a new trap receiver



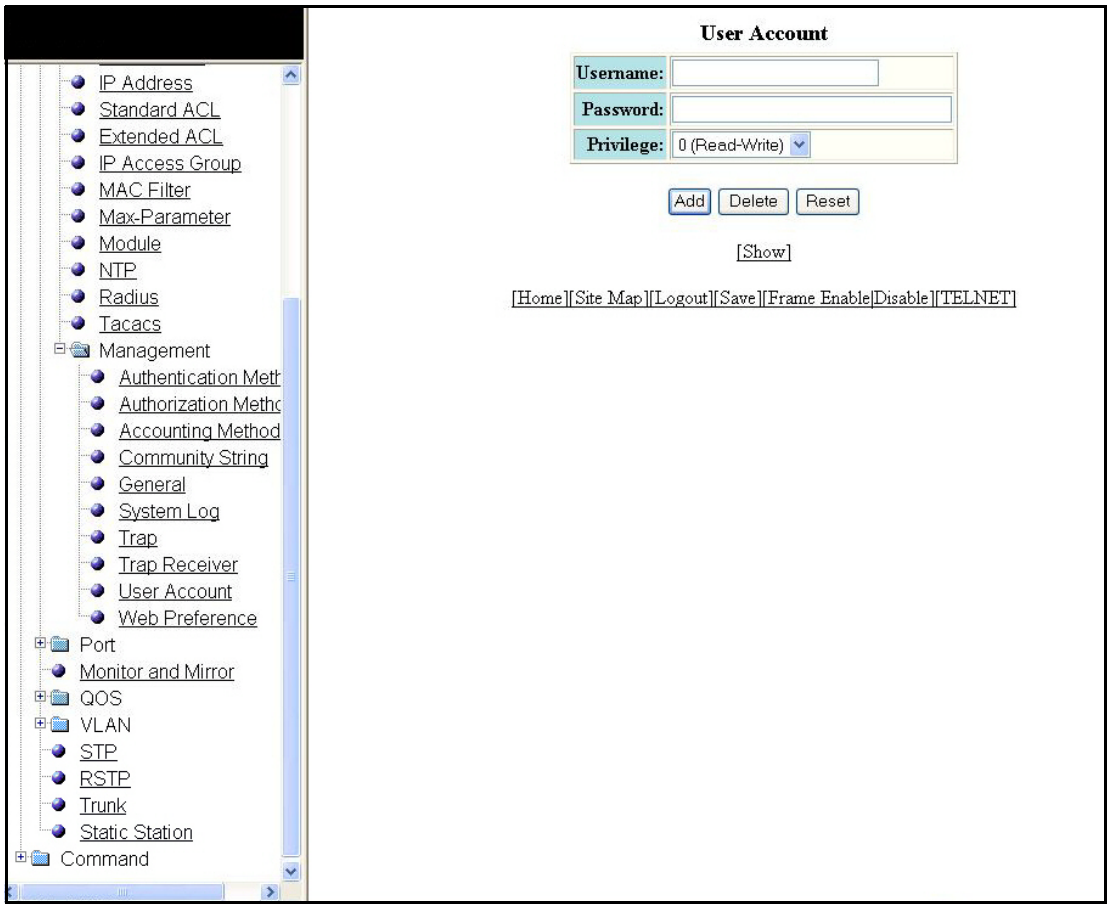
The Trap Receiver display contains the following information.

IP Address	The IP Address of the destination of the route.
UDP Port Number	Specifies the UDP port number on the host that will receive the trap.
Security Name or Community	Arbitrary values made of two five-digit integers joined by a colon. Each string in the community name can be a number from 0-65535.
Encrypt (Turn off for V3)	Allows you to enable or disable encryption for a particular string. It is turned off for V3.
Security Model	Used to secure against the following threats: • Modification of information. • Masquerading the identity of an authorized entity. • Message stream modification. • Disclosure of information.
Security Level (Only for V3)	The value for security level can be one of the following: • noauthNoPriv - Displays if the security model shows v3 and user authentication is by user name only. • noauthNoPriv - Displays if the security model shows v3 and user authentication is by user name and the MD5 or SHA algorithm.
Add	Enables you to add the IP Address.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the Trap Receiver entries.

Configuring a management user account

Select **Configure > System > Management > User Account** to configure a management user account.

FIGURE 79 Configuring a management user account



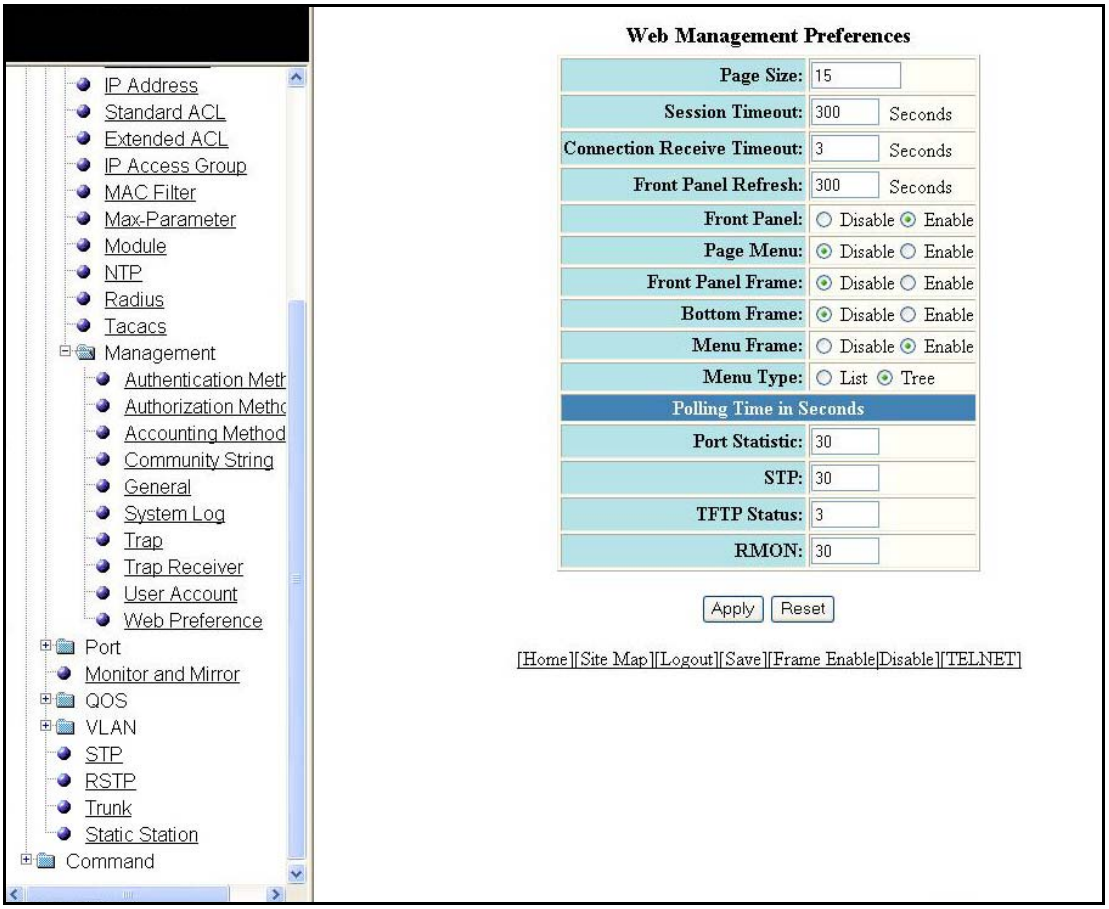
The User Account display contains the following information.

User Name	Specifies the User Id.
Password	Allows you to enter the login password.
Privilege	Lets you use the commands, allowed by the user level.
Add	Allows you to add information to the user account using the CLI commands.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Click **Show** to confirm the information added to the user account.

Configuring web management preference

Select **Configure > System > Management > Web Preference** to configure the Web management preferences. Click **Apply** to save the configuration or click **Reset** to undo changes.

FIGURE 80 Configuring Web management preference



The Web Management Preferences display contains the following information.

Page Size	Displays the page size.
Session Timeout	Specifies the console session timeout value.
Connection Receive Timeout	Specifies the time lapsed after getting disconnected from the application.
Front Panel Refresh	Specifies the time after which the front panel gets refreshed.
Front Panel	The ports are labelled on the front panel of the devices.
Page Menu	Displays the shortcuts to functions and other panels.
Front Panel Frame	Allows you to enable or disable the front panel frame.
Bottom Frame	Allows you to enable or disable the bottom frame.
Menu Frame	Allows you to enable or disable the menu frame.
Menu Type	The left pane of the Web management interface window contains a “tree view,” similar to the one found in Windows Explorer. These folders, when expanded, reveal additional options. To expand a folder, click on the plus sign to the left of the folder icon.
Polling Time in Seconds	

Port Statistic	Displays the port statistic polling time.
STP	Shows whether STP is Enabled or Disabled for the port.
TFTP Status	Displays the current TFTP polling time status in secs.
RMON	Displays the polling time for Remote Monitoring.

Configuring an Ethernet port

Select **Configure > Port > Ethernet** to configure an Ethernet port. The Ethernet Port Configuration window appears.

1. Select Stack Unit ID and Click **Display** to view the port details.
2. Click **Modify** to modify a respective port. For more information on how to modify an ethernet port, refer to "Modifying port settings" on page 104 for details.

FIGURE 81 Configuring an ETHERNET Port

Port	Actual speed/ mode	Configured speed/ mode	QOS	Lock Addr	Tag	STP/RSTP	Fast STP	Fast Uplink	Flow Ctrl	Gig Default	DHCP ID	Trunk	Inline Power	
1/1/1	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/2	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/3	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/4	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/5	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/6	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/7	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/8	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/9	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/10	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/11	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/12	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/13	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/14	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/15	10-half	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/16	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/17	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/18	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/19	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/20	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/21	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/22	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/23	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/1/24	10-half	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/2/1	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
1/2/2	None	Auto	0	Disable	No	Enable	Enable	Disable	Enable	Neg-Full-Auto	None	None	Disabled	Modify
Port	Actual speed/ mode	Configured speed/ mode	QOS	Lock Addr	Tag	STP/RSTP	Fast STP	Fast Uplink	Flow Ctrl	Gig Default	DHCP ID	Trunk	Inline Power	

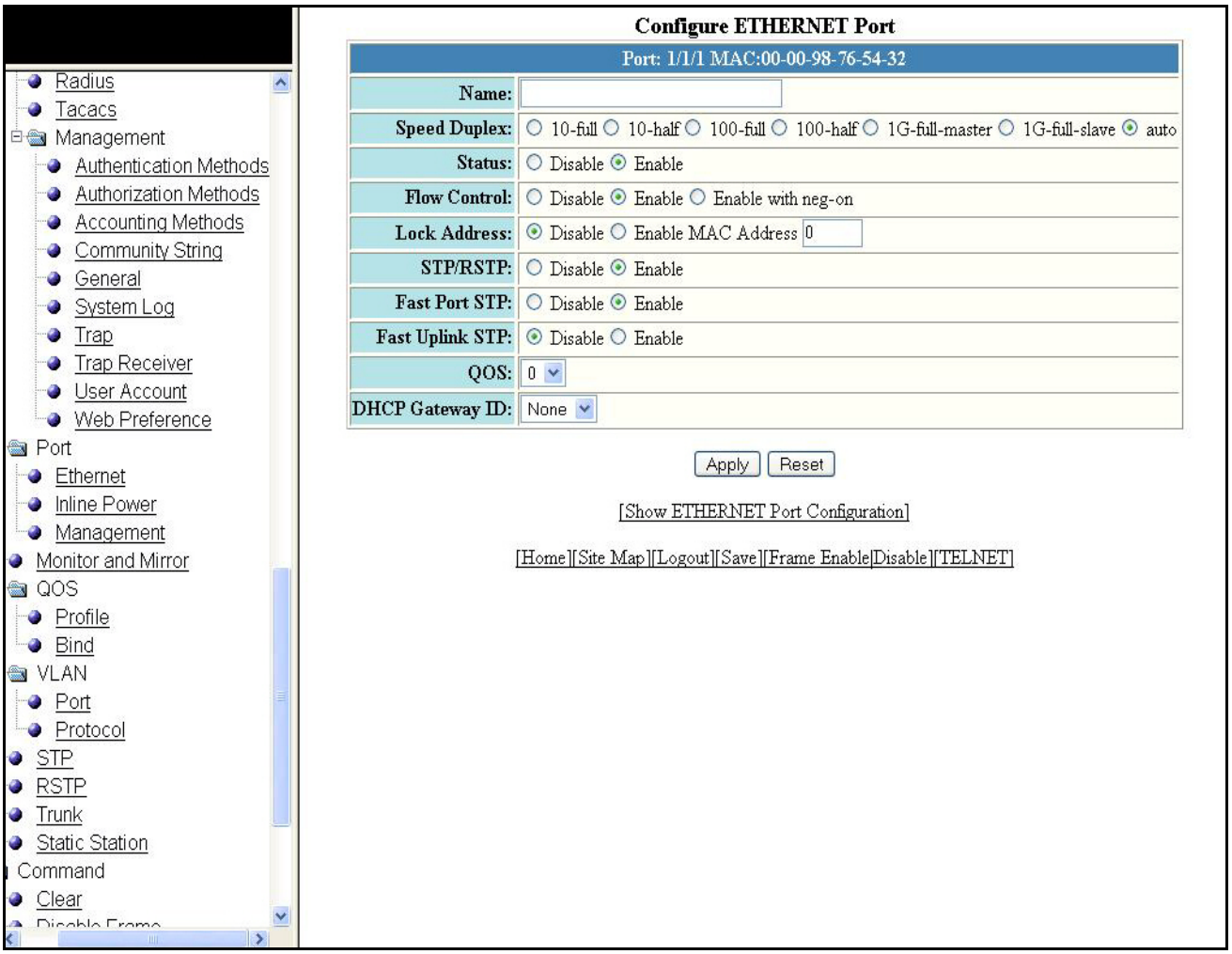
The Ethernet Port Configuration display contains the following information.

Port	The slot ID and port ID.
Actual Speed/Mode	Shows whether the Actual speed matches the Configured speed. If the Configured speed is set to Auto, then the speed is provided.
Configured Speed/Mode	The speed duplex set for the port.
QOS	Shows the setting (1-7) for Quality of Service.
Lock Addr	Shows whether a Lock Address is Enabled or Disabled.
Tag	Indicates whether the ports have VLAN tagging. The value is Yes or No.
STP	Shows whether STP is Enabled or Disabled for the port.
Fast STP	Shows whether Fast STP is Enabled or Disabled for the port.
Fast Uplink	Shows whether Fast Uplink is Enabled or Disabled for the port.
Flow Ctrl	Shows whether the ability to monitor flow control packets is Enabled or Disabled.
Gig Default	The globally configured Gigabit negotiation mode is the default mode for all Gigabit fiber ports. You can override the globally configured default and set individual ports to the following: • Negotiate-full-auto – The port first tries to perform a handshake with the other port to exchange capability information. If the other port does not respond to the handshake attempt, the port uses the manually configured configuration information (or the defaults if an administrator has not set the information). This is the default. • Auto-Gigabit – The port tries to perform a handshake with the other port to exchange capability information. • Negotiation-off – The port does not try to perform a handshake. Instead, the port uses configuration information manually configured by an administrator.
Ethernet Port Attribute	Allows you to monitor the port attributes.
Ethernet Port Statistic	Allows you to monitor the Ethernet port statistic details.
Ethernet Port Utilization	Allows you to monitor the Ethernet port utilization details.
Relative Utilization	Allows you to configure the uplink and downlink port members.

Modifying port settings

Click **Modify** to configure any Ethernet port in the row associated with the port number, as shown in the previous display. The following display will appear. Use this form to make changes, and click **Apply** to save the configuration or click **Reset** to undo the changes. Click **Show ETHERNET Port** Configuration to o view the new port configuration.

FIGURE 82 Modifying the port settings



NOTE
You may encounter connectivity errors if the stacking port configuration was not saved. Click **Apply** immediately after making stacking-related configuration changes, such as priority and stacking ports. Click **Reset** to undo the changes and then Click **Apply** to retain the previous version data.

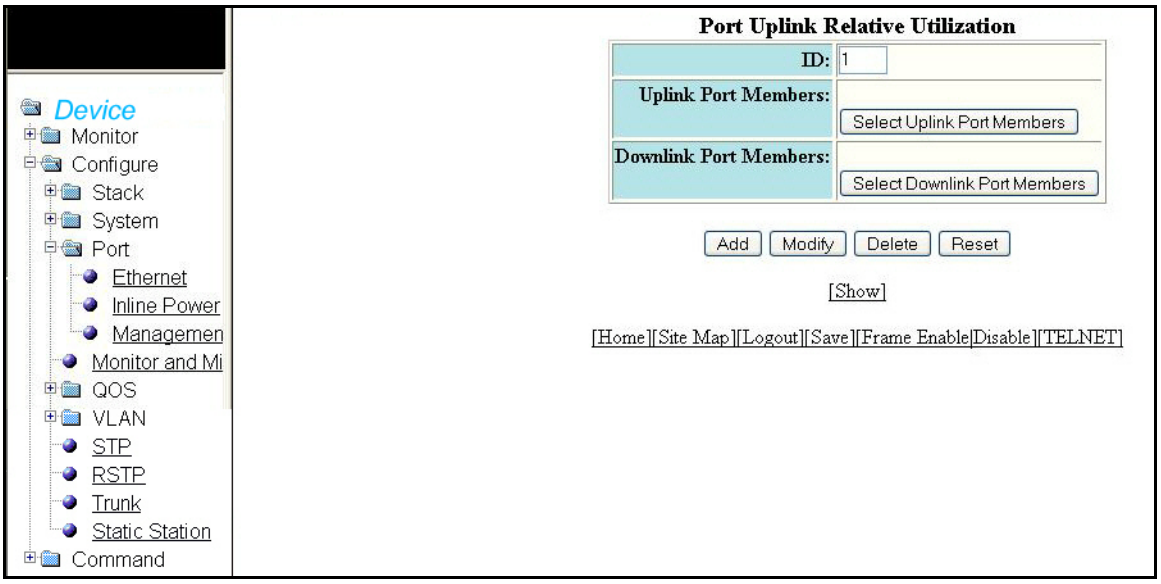
The configurable options shown in the Configure Ethernet Port display includes the following.

Name	A port name can be assigned to help identify interfaces on the network. You can assign a port name to physical ports, virtual interfaces, and loopback interfaces. The parameter is an alphanumeric string. The name can be up to 64 characters long. The name can contain blanks. You do not need to use quotation marks around the string, even when it contains blanks.
Speed Duplex	The 10/10/1000Base-T copper ports are designed to auto-sense and auto-negotiate the speed and mode of the connected device. If the attached device does not support this operation, you can manually enter the port speed to operate at either 10 Mbps or 100 Mbps. The default is auto.
Status	The port can be made inactive (disable) or active (enable) by selecting the appropriate status option. The default for a port is enabled.
Flow Control	You can configure full-duplex ports on a system to operate with or without flow control. Flow control is enabled by default.
Lock Address	Address-lock filters allow you to limit the number of devices that have access to a specific port. Access violations are reported as SNMP traps. By default this feature is disabled. A maximum of 2,048 entries can be specified for access. The default address count is eight.
STP	STP detects and eliminates logical loops in the network. STP also ensures that the least cost path is taken when multiple paths exist between ports or VLANs. If the selected path fails, STP searches for and then establishes an alternate path to prevent or limit retransmission of data. STP must be enabled at the system level to allow assignment of this capability on the VLAN level.
Fast Port STP	You can determine if you want STP enabled or disabled at the port.
Fast Uplink STP	You can determine if you want STP enabled or disabled at the uplink.
QOS	You can select a port priority from 0 – 7.
DHCP Gateway ID	The router can assist DHCP or BootP Discovery packets from one subnet to reach DHCP or BootP servers on a different sub-net by placing the IP address of the router interface that receives the request in the request packet's Gateway field.
Device Configuration	Many power consuming devices advertise their power requirements to power sourcing devices. If you configure a port with a maximum power level or a power class for a power consuming device, the power level or power class takes precedence over the device's power requirement.
Priority	You can configure an in-line power priority on ports, whereby ports with a higher in-line power priority will take precedence over ports with a low in-line power priority. The default is 3 (low priority). You can specify one of the following values: • 3 – low priority • 2 – high priority • 1 – critical priority

Configuring port relative utilization

You can configure uplink utilization lists that display the percentage of bandwidth for a given uplink port that is being used by a specific list of downlink ports. The percentages are based on 30-second intervals of RMON packet statistics for the ports. Both transmit and receive traffic is counted in each percentage. To configure port relative utilization, from the Ethernet Port Configuration panel, refer to "Configuring an Ethernet port" on page 101.

FIGURE 83 Configure - Port Uplink Relative Utilization



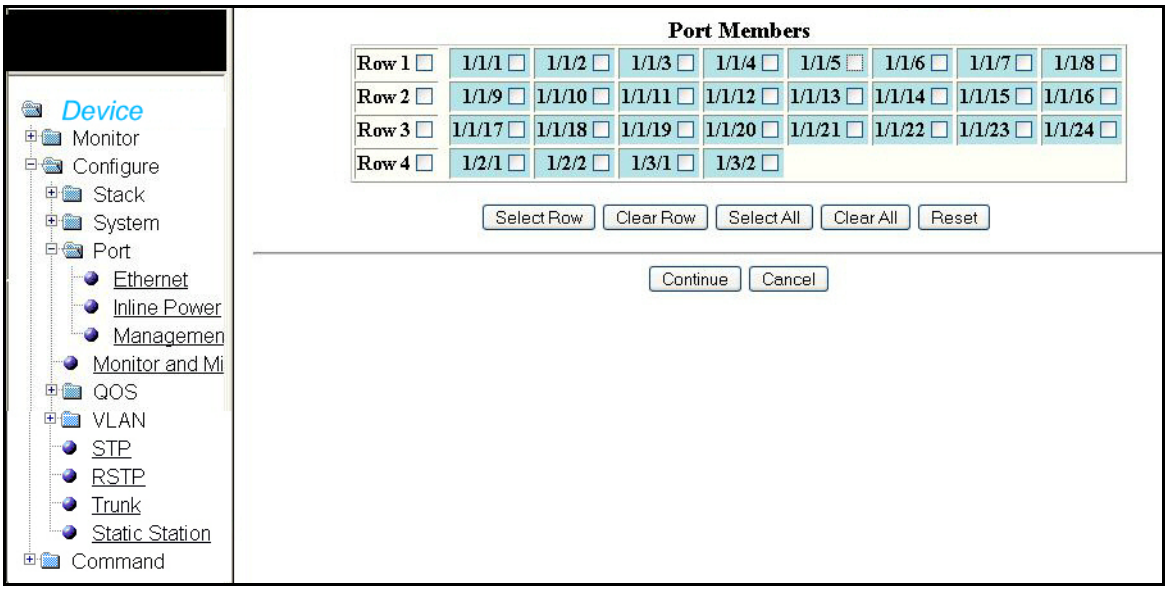
Click **Add** to add a port member. Click **Modify** to modify a port member. Click **Delete** to delete a port member. Click **Reset** to undo changes.

Once the updates are made to the uplink port members or to the downlink port members, the selected ports will appear in the related members field and a message appears at the top indicating the change.

Uplink port members

Click **Select Uplink Port Members**. You can enable individual ports or entire rows. Click **Continue** after selecting the necessary uplink port members.

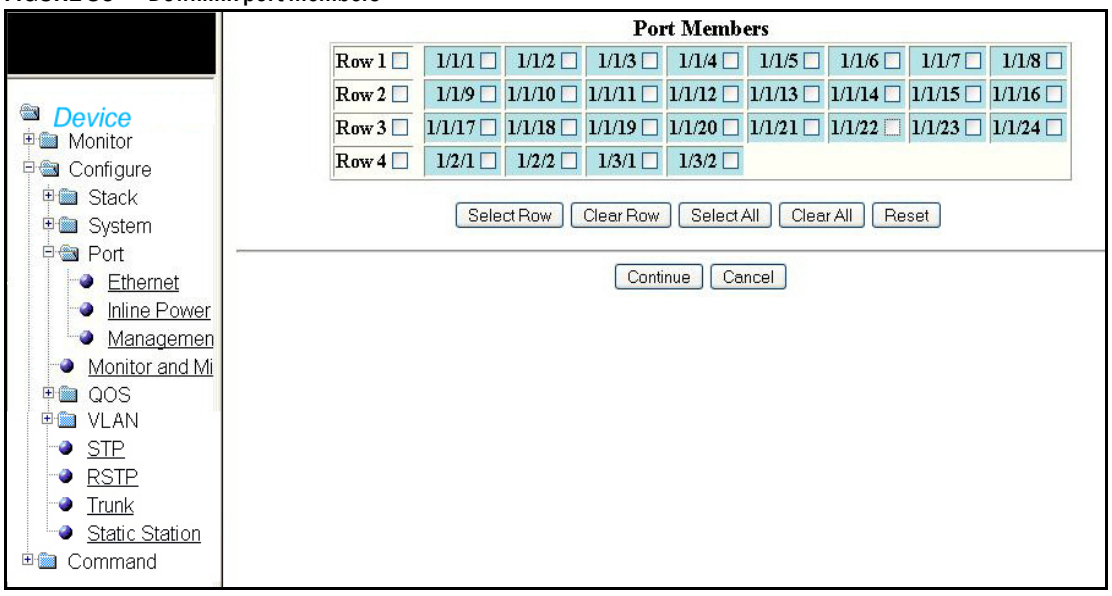
FIGURE 84 Uplink port members



Downlink port members

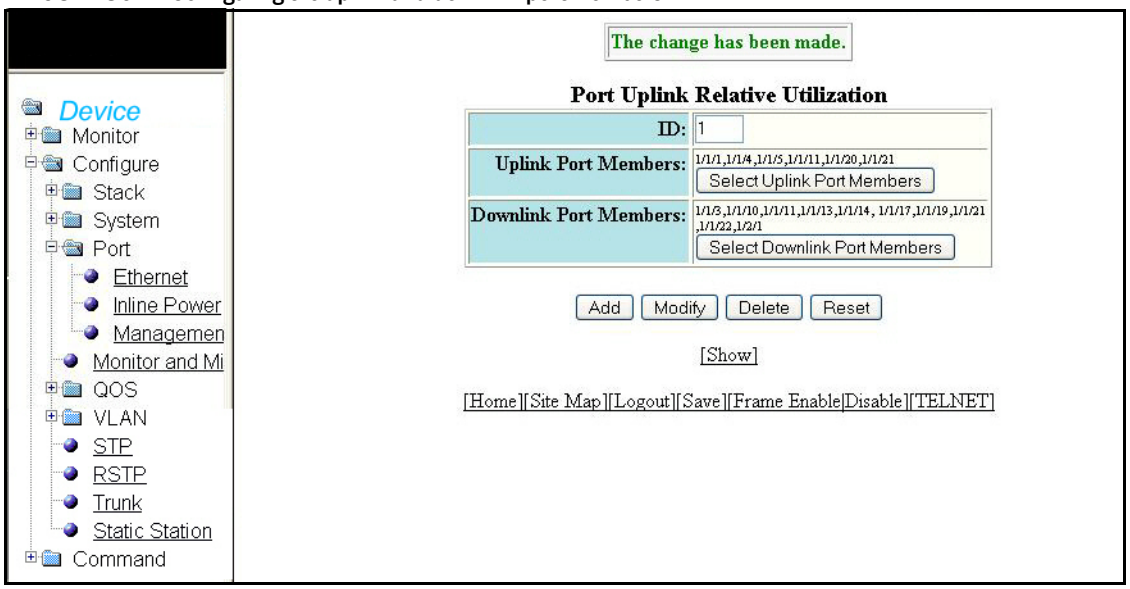
Click **Select Downlink Port Members**. You can enable individual ports or entire rows. Click **Continue** after selecting the necessary downlink port members.

FIGURE 85 Downlink port members



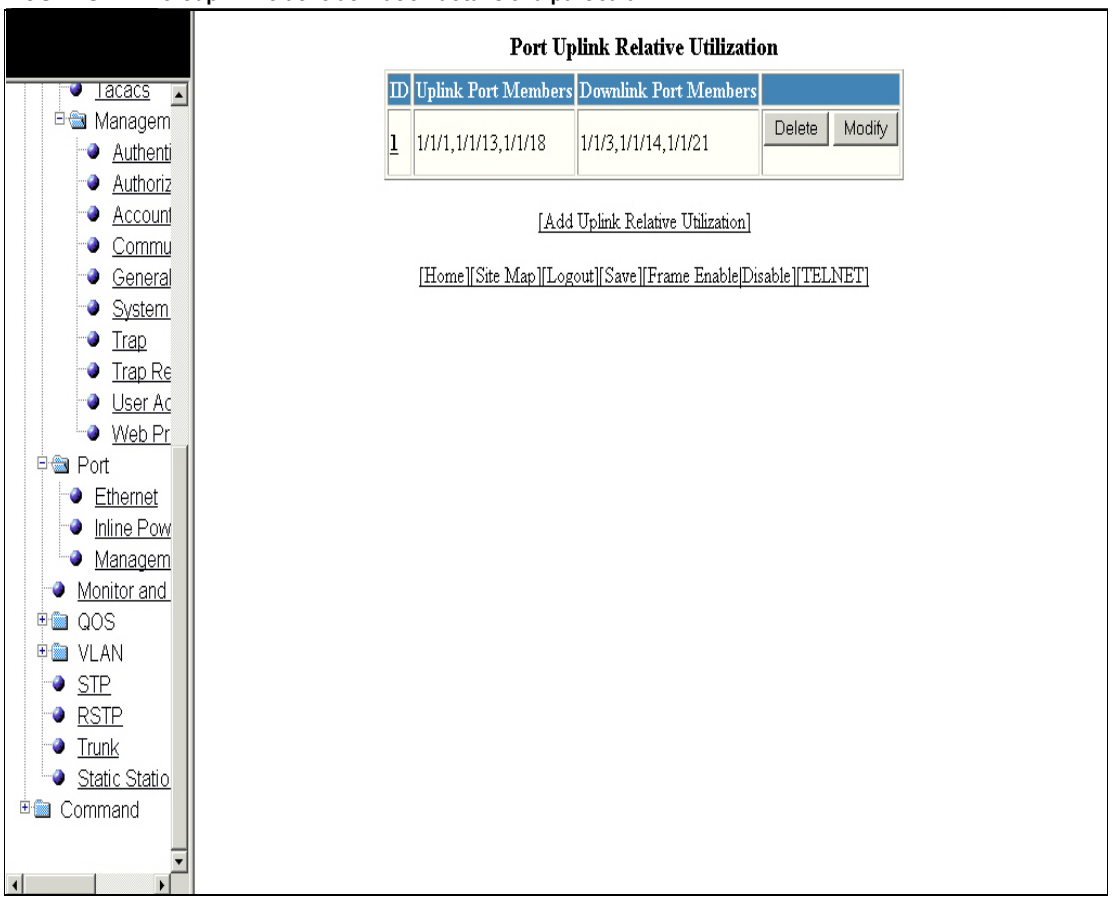
The selected port members is displayed as shown below.

FIGURE 86 Configuring the uplink and downlink port members



Click **Show** to view the details of the uplink and downlink port members of a particular ID. The Show port uplink relative utilization window appears as shown below.

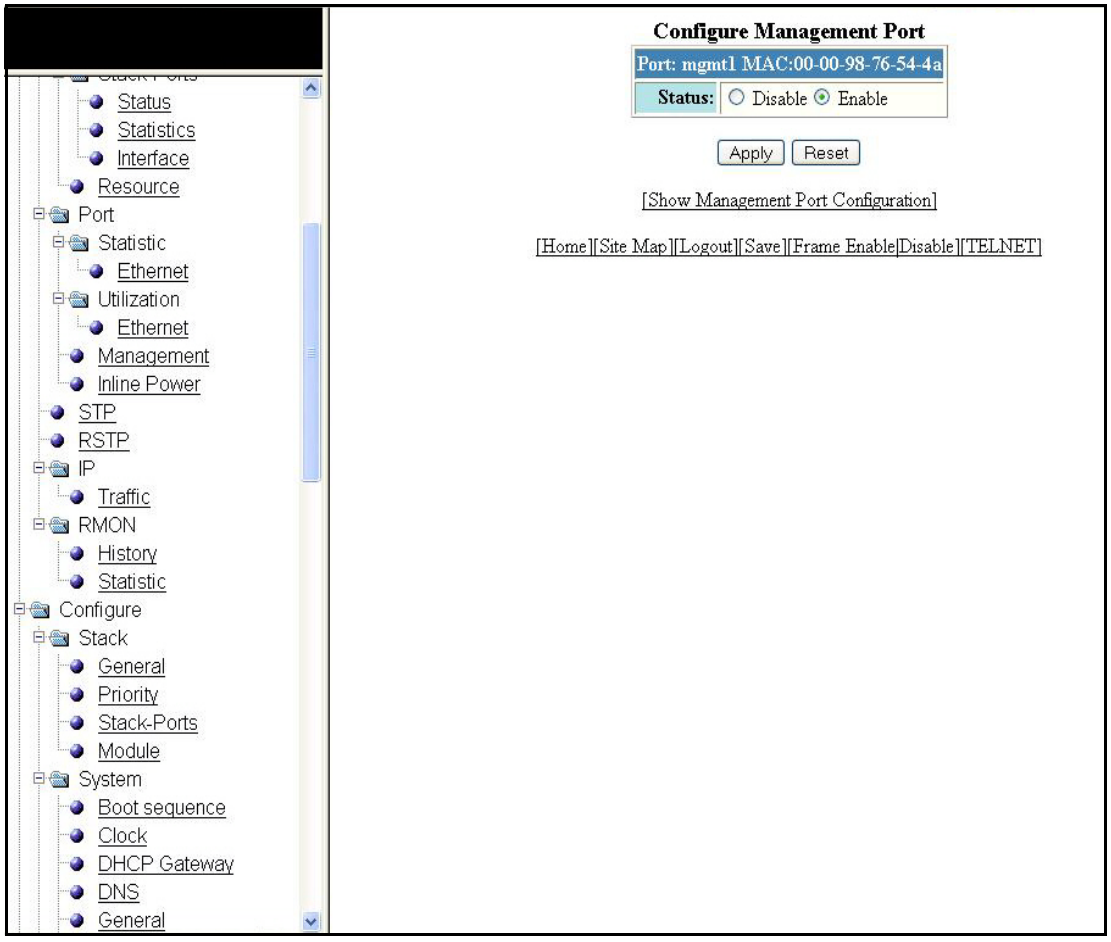
FIGURE 87 Port uplink relative utilization details of a particular ID



Configuring a management port

Select **Configure > Port > Management** to configure a management port.

FIGURE 88 Configure Management Port



NOTE
Click **Apply** to save the configuration or click **Reset** to undo changes. Select Status of the port and click **Apply. The change has been made** message appears at the top indicating the change.

The Configure Management Port display contains the following information.

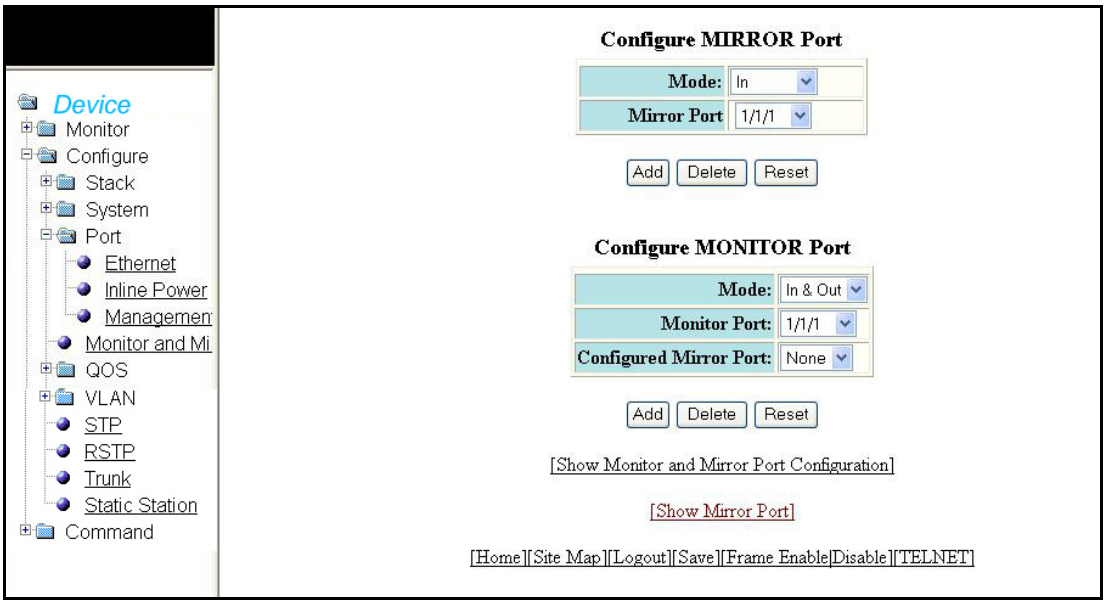
Management port name	The name of the management port.
MAC Address	The MAC address of the management port
Status	Allows you to enable or disable the management port.

Click **Show Management** to view the details of Management configuration.

Configuring the monitor and mirror port

Select **Configure > Monitor and Mirror** to configure the monitor and mirror port.

FIGURE 89 Configuring monitor and mirror port



The Monitor and Mirror port configuration display contains the following information.

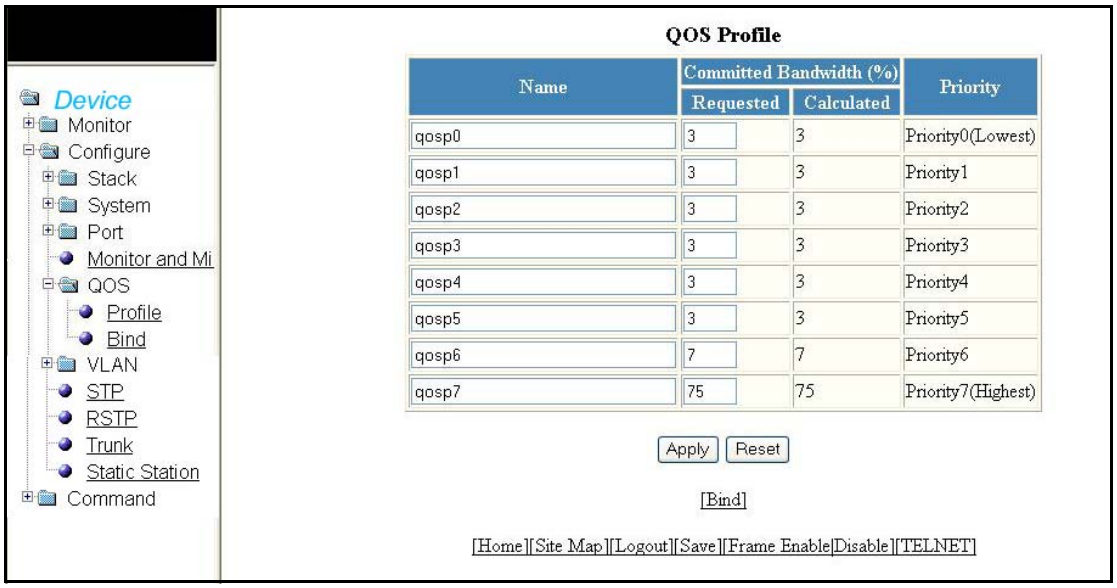
Configure Mirror Port	
Mode	Specifies the mode in which the port operates. • In • Out • In & Out
Mirror Port	Specifies the port to which the monitored traffic is copied.
Configure Monitor Port	
Mode	Specifies the mode in which the port operates. • In • Out • In & Out
Monitor Port	Specifies the port whose traffic you want to monitor.
Configured Mirror Port	Displays the configured mirror ports.
Add	Enables you to add the ports.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.

Show Mirror Port	Displays the newly added mirror ports.
Add	Enables you to add the ports.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.

Configuring the QOS profile

Select **Configure > QOS > Profile** to configure the QOS profile. Click **Apply** to save your configuration and click **Reset** to undo changes.

FIGURE 90 Configuring QOS profile



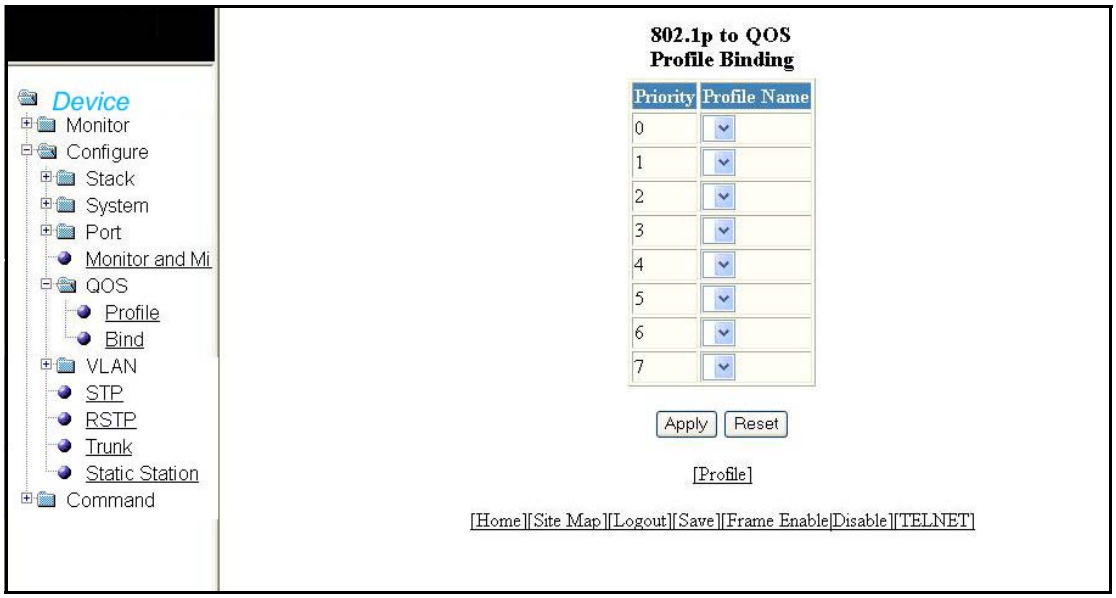
The QOS Profile display contains the following information.

Name	Specifies the QoS profile name.
Committed Bandwith(%)	This parameter can be any one of the following: • Requested • Calculated
Priority	Displays the priority level from lowest to highest (0 - 7).
Bind	Displays the QOS Bind screen.

Configuring the QOS bind

Select **Configure > QOS > Bind** to configure the QOS bind. Click **Apply** to save configuration and click **Reset** to undo changes.

FIGURE 91 Configuring QOS bind



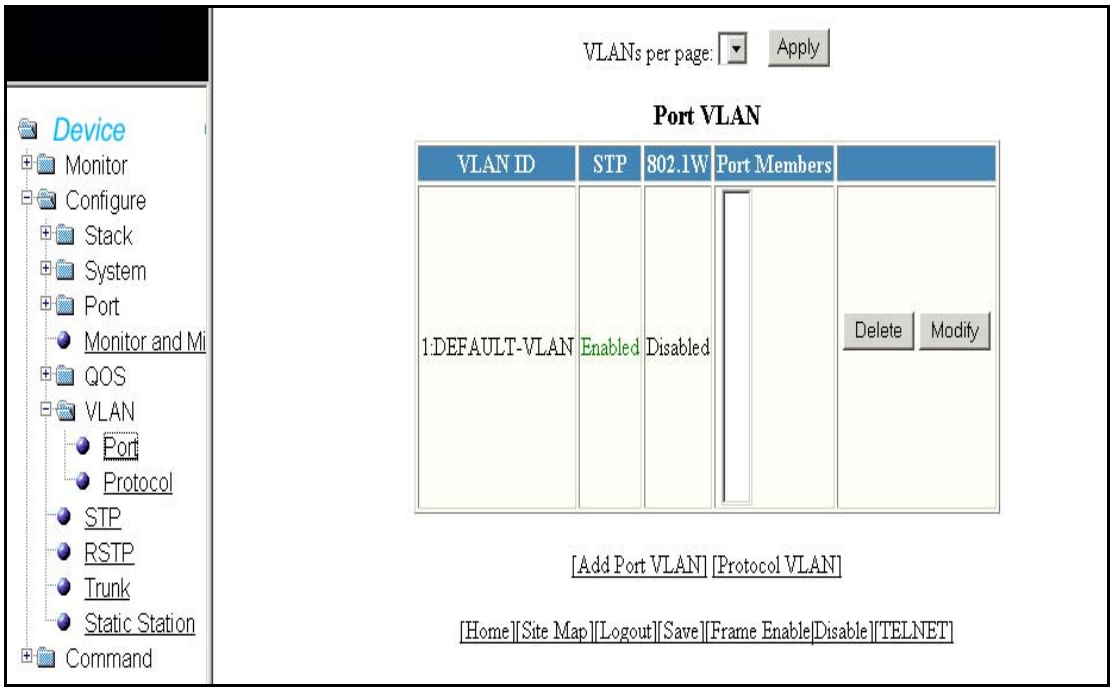
The QOS Bind display contains the following information.

Priority	Displays the priority level from lowest to highest (0 - 7).
Profile Name	Specifies the QoS profile name.
Profile	Displays the QOS Profile screen.

Configuring VLAN

Select **Configure > VLAN** to configure the VLAN.

FIGURE 92 Configuring Port VLAN

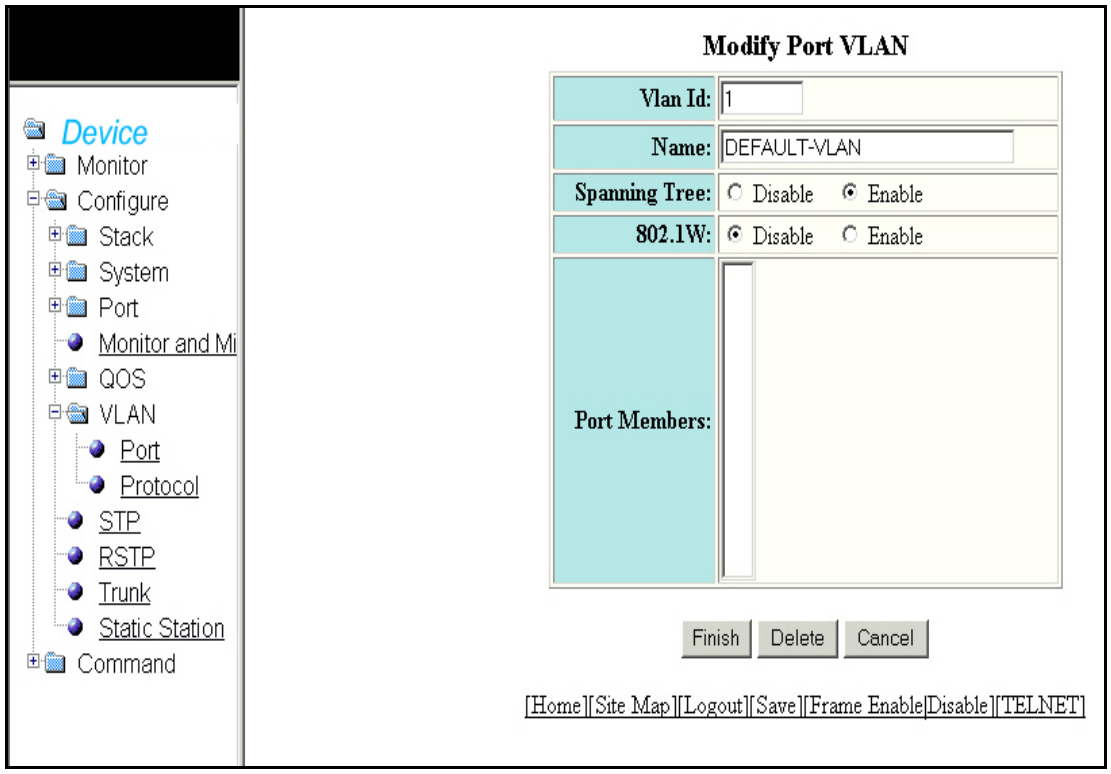


The Port VLAN contains the following information.

VLAN Id	This parameter displays STP information for the specified port-based VLAN.
STP	The type of STP enabled on the device.
802.1W	Rapid Spanning Tree Protocol (RSTP), which was now 802.1W feature if enabled, provides rapid traffic reconvergence for point-to-point links within a few milliseconds (0 – 500 milliseconds),
Port Members	Displays the list of port members.
Apply	To save your configuration, click Apply.
Delete	Enables you to delete the changes made.
Modify	Enables you to modify the VLAN settings.
Add Port VLAN	Allows you to add the port members.

Click **Modify** to change the VLAN settings.

FIGURE 93 Modifying VLAN settings

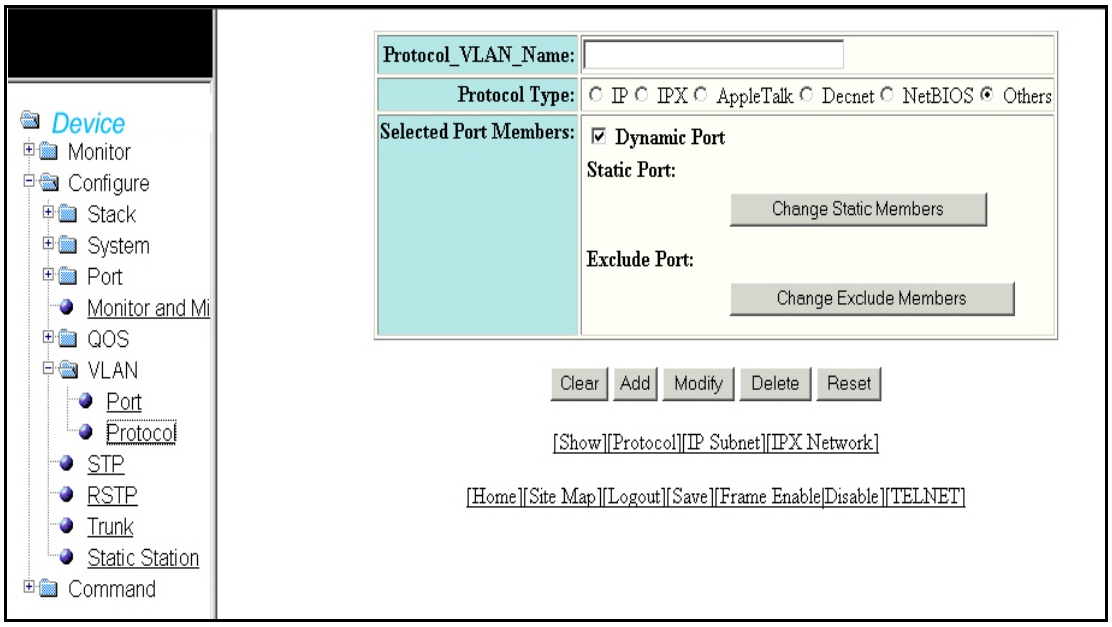


The Modify Port VLAN display contains the following information.

VLAN Id	This parameter displays STP information for the specified port-based VLAN.
Name	Displays the default VLAN name.
Spanning Tree	The type of STP enabled on the device.
802.1W	Enables you to modify the settings of RSTP configuration.
Port Members	Displays the list of port members.
Finish	Enables you to complete the operation.
Delete	Enables you to delete the changes made.
Cancel	Enables you to cancel the operation performed.

Select **Vlan > Protocol** to configure Vlan protocol.

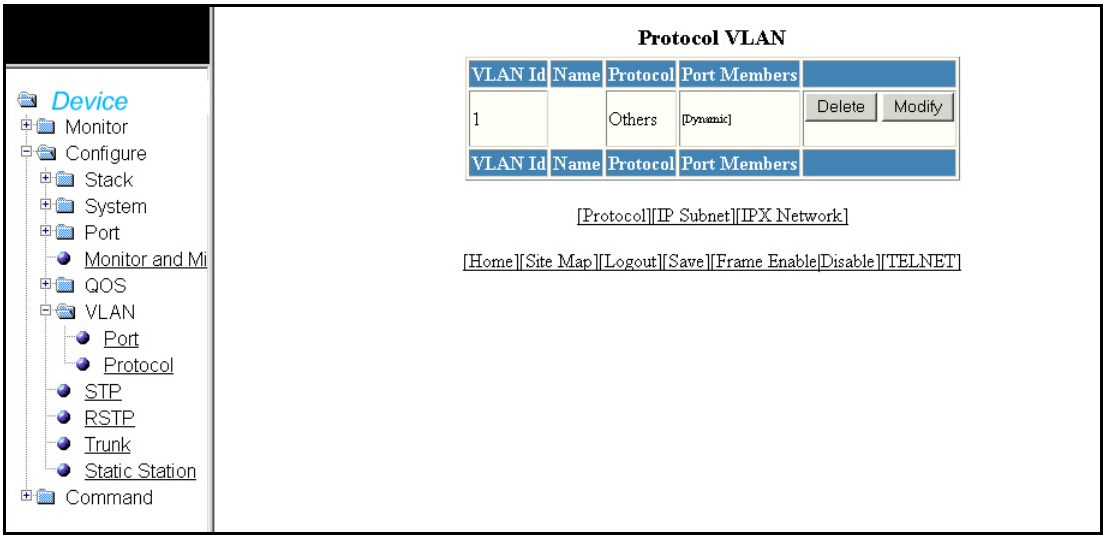
FIGURE 94 Configuring VLAN Protocol



The VLAN protocol display contains the following information.

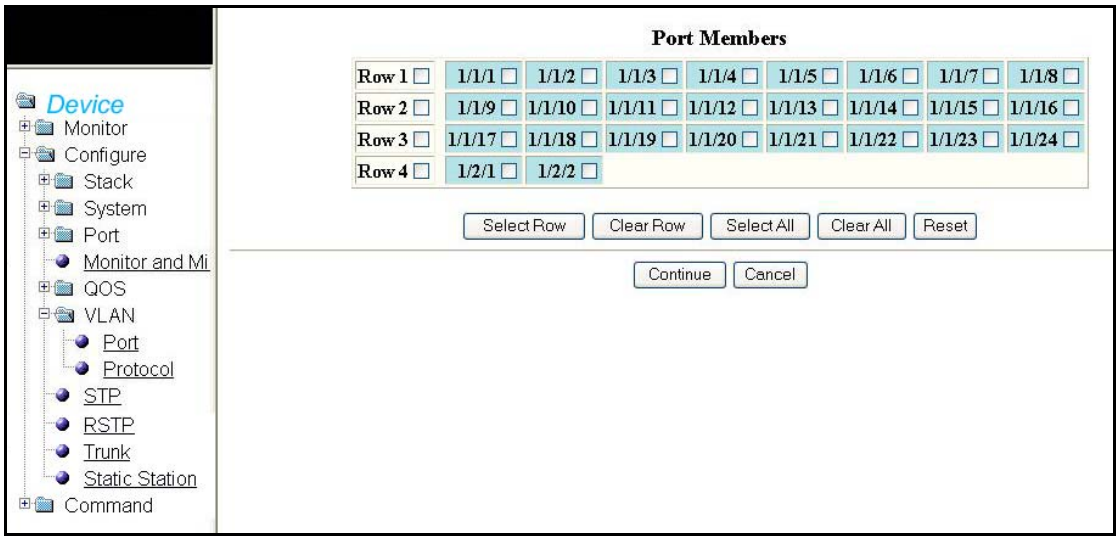
Protocol_VLAN_Name	Enter the name of the Protocol VLAN.
Protocol Type	Select a protocol type.
Selected Port Members	Displays the selected port members under the static port and exclude port.
Change Static members	Allows you to select the static port members.
Change Exclude members	Allows you to select the exclude port members.
Clear	Allows you to unselect the selected port members.
Add	Enables you to add the protocol types.
Modify	Enables you to modify the changes.
Delete	Enables you to delete the added protocol types.
Reset	To undo your changes, click Reset.
Show	Displays the Protocol VLAN entries.
Protocol	Displays the VLAN protocol.
IP Subnet	Displays the IP Address and mask for VLAN protocol.

FIGURE 95 Adding Protocol type



Click **Change Static Members** to view the Static port members as shown in Figure 96.

FIGURE 96 Static Port Members

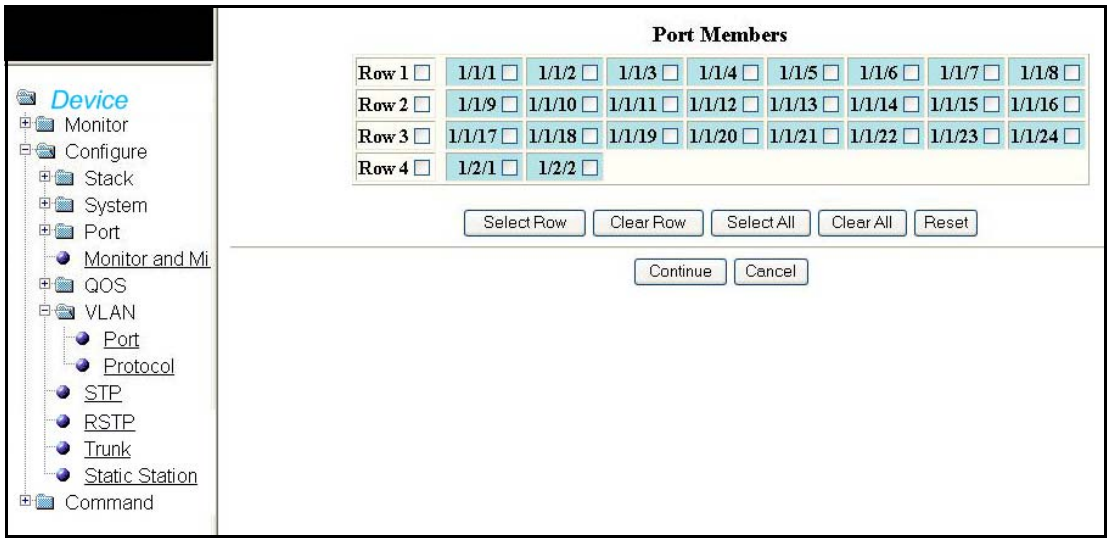


The options within the panel includes:

- Select Row — Allows you to select the entire row.
- Clear Row — Allows you to clear any selected row.
- Select All — Allows you to select all the port members.
- Clear All — Allows you to clear all the port members selected.
- Reset — To undo your changes, click Reset.
- Continue — Allows you to proceed to the next screen.
- Cancel — Allows you to cancel the changes made.

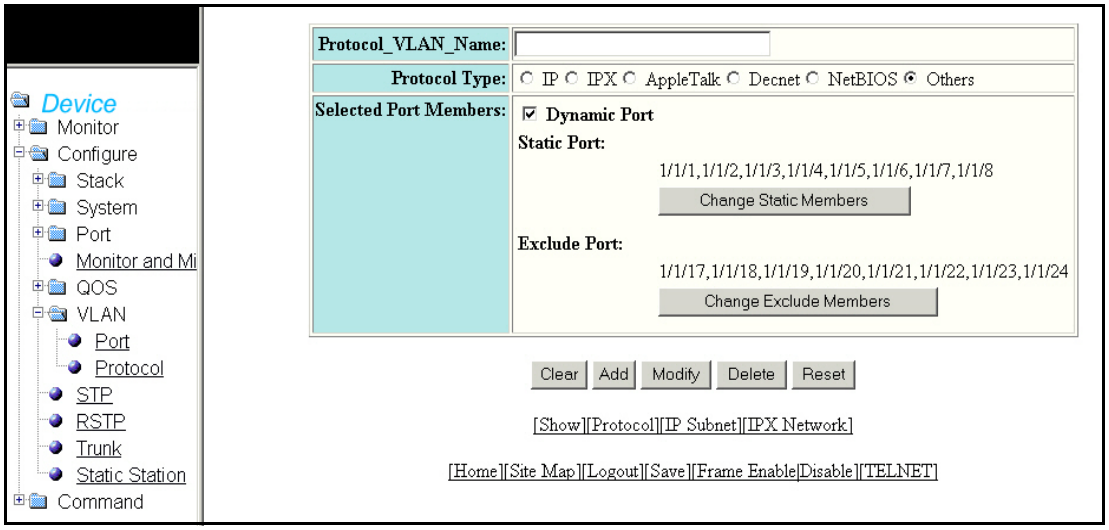
Click **Change Exclude Members** to exclude port members as shown in Figure 97.

FIGURE 97 Exclude Port Members



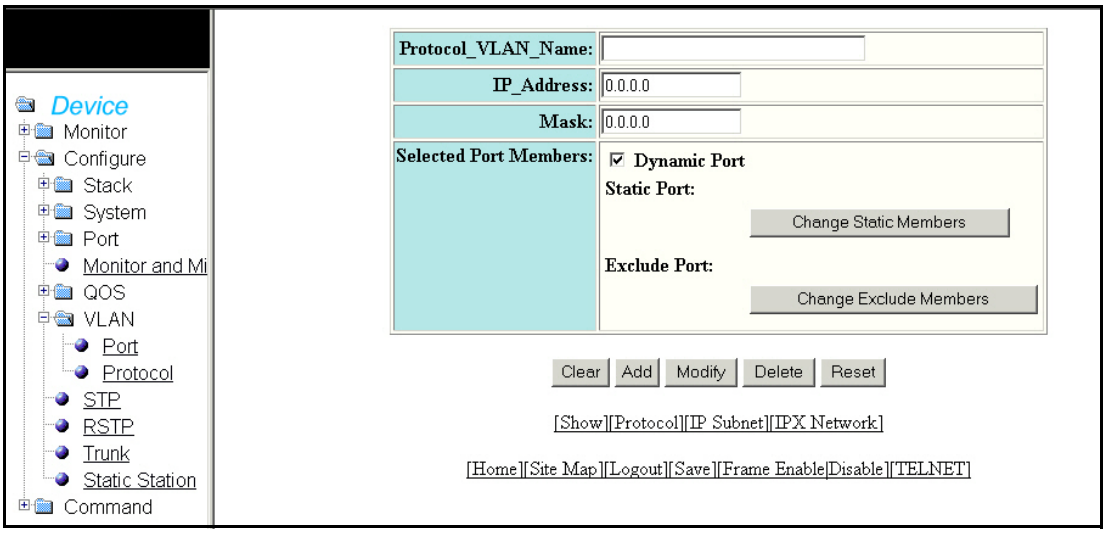
Select the port members and click **Continue** to view the selected port members as shown in Figure 98.

FIGURE 98 Display of selected port members



Click **IP Subnet** to view the details of IP Subnet as shown in Figure 99.

FIGURE 99 IP Subnet

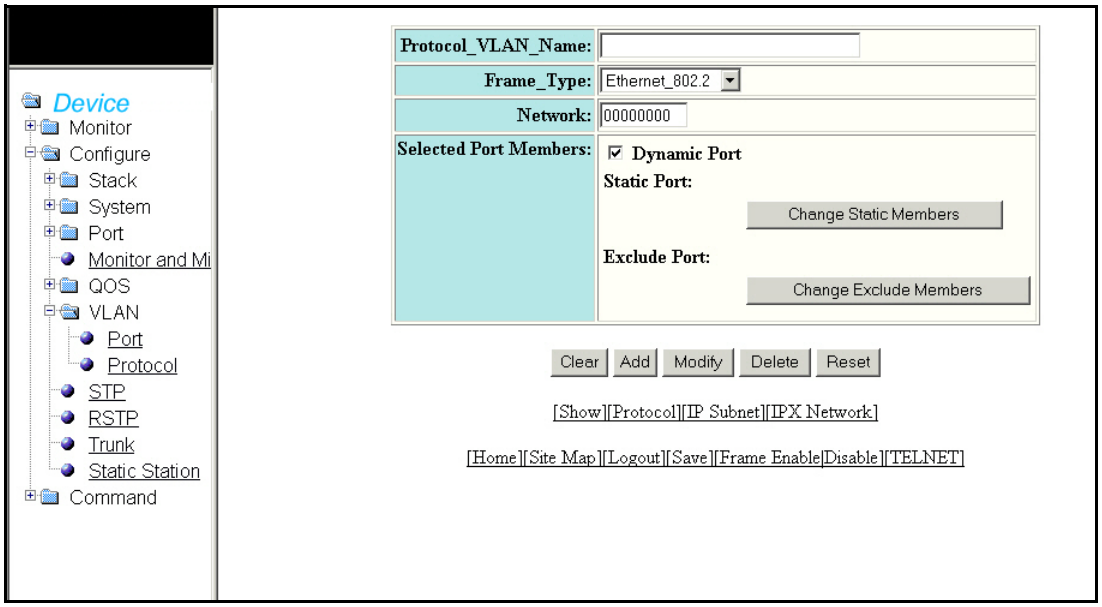


The IP Subnet display contains the following information.

Protocol_VLAN_Name	Specifies the name of the protocol VLAN.
IP Address	Configures the IP Address of the device.
Mask	This parameter provides a filter for displaying multiple MAC addresses that have specific values in common.
Selected Port Members	Displays the selected port members under the static port and exclude port.

Click **IPX Network** to display the information as shown in Figure 100.

FIGURE 100 IPX network



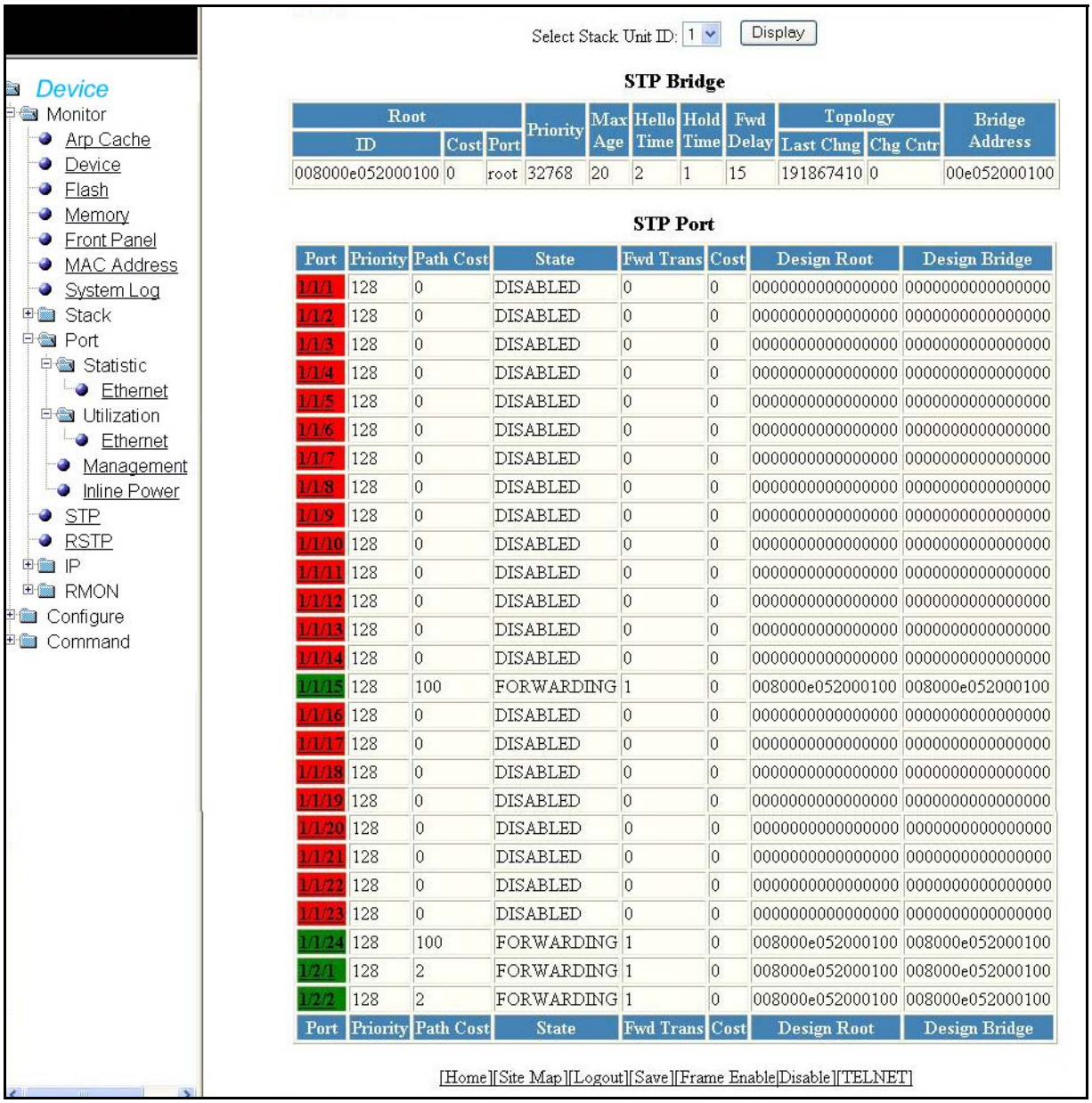
The IPX network window contains the following information.

Protocol_VLAN_Name	Enter the name of the protocol VLAN.
Frame Type	Enter the frame type of the protocol.
Network	IPX network must be between 0x00000001 to 0xFFFFFFFE.
Selected Port Members	Displays the selected port members under the static port and exclude port.

Configuring STP

Select **Configure > STP** to configure the STP bridge.

FIGURE 101 Configuring the STP bridge



STP Bridge

Root			Priority	Max Age	Hello Time	Hold Time	Fwd Delay	Topology		Bridge Address
ID	Cost	Port						Last Chng	Chg Cntr	
008000e052000100	0	root	32768	20	2	1	15	191867410	0	00e052000100

STP Port

Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge
1/1/1	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/2	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/3	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/4	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/5	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/6	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/7	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/8	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/9	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/10	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/11	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/12	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/13	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/14	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/15	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/1/16	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/17	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/18	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/19	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/20	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/21	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/22	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/23	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/24	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/1	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/2	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge

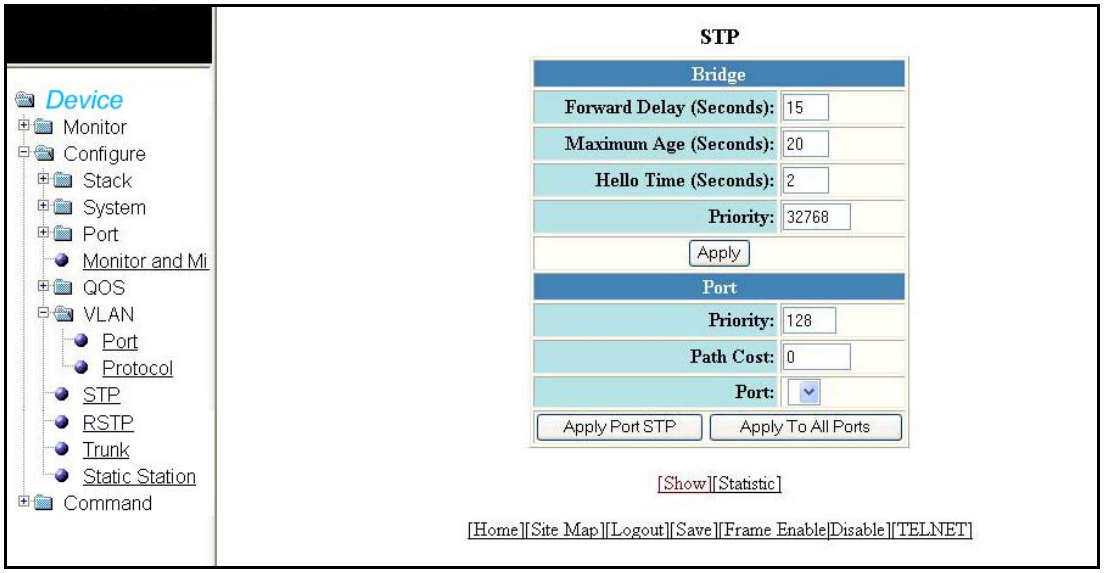
The STP Bridge and Port contains the following information.

STP Bridge Parameters	
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Max.Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time	The interval between each configuration BPDU sent by the root bridge.

Forward Delay	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
STP Port Parameters	
Port	The port number.
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Path Cost	The port's STP path cost.
Display	Changes the unit ID by selecting a unit from the drop-down list and clicking **Display**.
Modify	Enables you to modify any port.

Click **Modify** to modify any port. Click **Apply** to save the configuration.

FIGURE 102 Modifying STP parameters



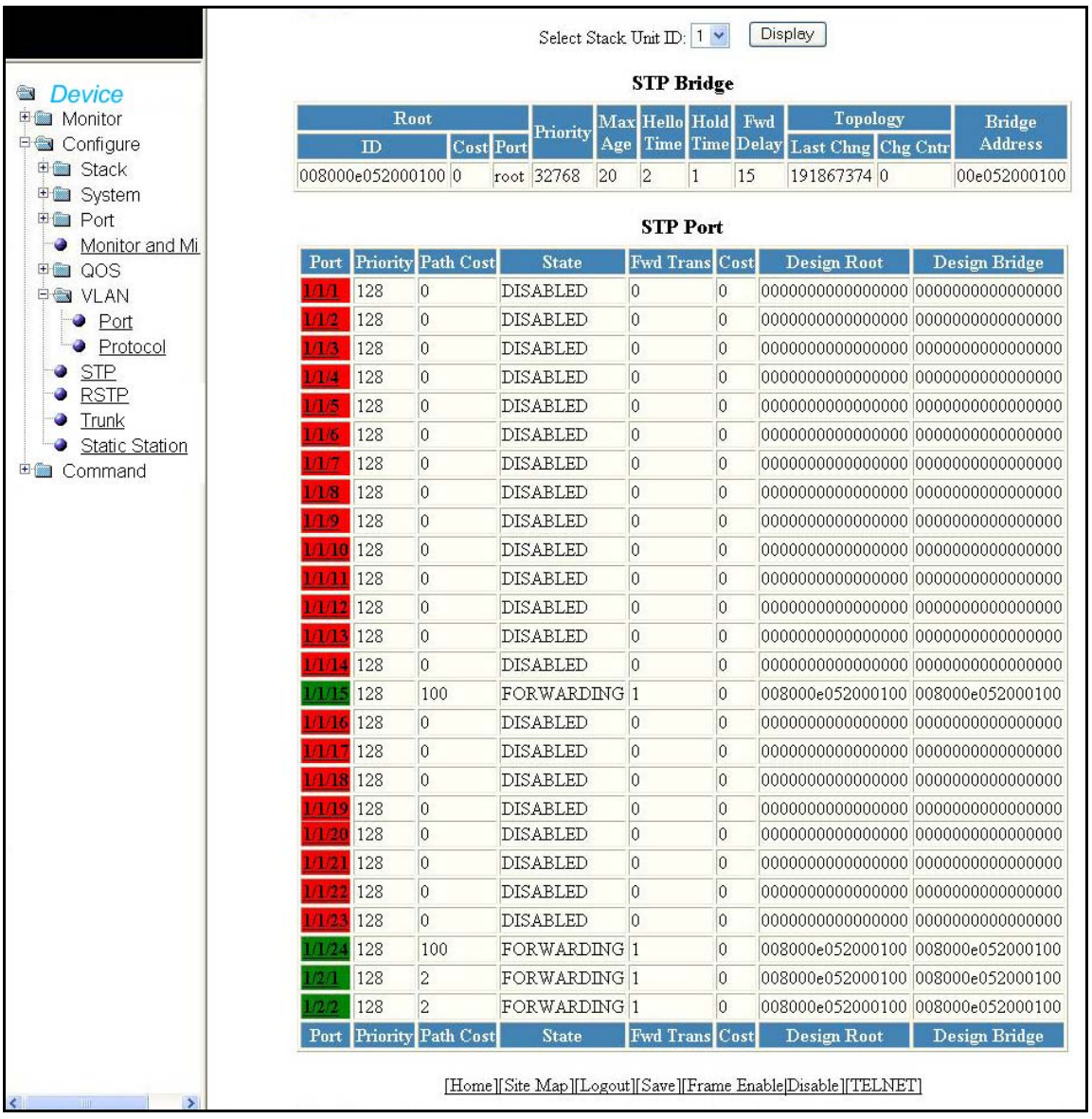
The STP parameters contains the following information.

STP Bridge Parameters	
Forward Delay (Seconds)	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Maximum Age (Seconds)	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time (Seconds)	The interval between each configuration BPDU sent by the root bridge.
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
STP Port Parameters	
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Path Cost	The port's STP path cost.

Port	The port number.
Apply port STP	Allows you to apply the changes to port STP.
Apply to all Ports	Allows you to apply the changes to all ports.
Show	Displays the changes in STP parameters, if any.
Statistic	Displays the Statistic STP parameters.

Click **Statistic** to display the details of RSTP statistic as shown in Figure 103

FIGURE 103 STP Statistic



STP Bridge

Root ID	Root Cost	Root Port	Priority	Max Age	Hello Time	Hold Time	Fwd Delay	Topology Last Chng	Topology Chg Cntr	Bridge Address
008000e052000100	0	root	32768	20	2	1	15	191867374	0	00e052000100

STP Port

Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge
1/1/1	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/2	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/3	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/4	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/5	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/6	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/7	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/8	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/9	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/10	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/11	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/12	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/13	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/14	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/15	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/1/16	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/17	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/18	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/19	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/20	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/21	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/22	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/23	128	0	DISABLED	0	0	0000000000000000	0000000000000000
1/1/24	128	100	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/1	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
1/2/2	128	2	FORWARDING	1	0	008000e052000100	008000e052000100
Port	Priority	Path Cost	State	Fwd Trans	Cost	Design Root	Design Bridge

The STP statistic display contains the following information.

STP Bridge Parameters	
Root ID	The ID assigned by STP to the root bridge for this spanning tree.
Root Cost	The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.
Root Port	The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number.
Priority	A parameter used to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root.
Max.Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time	The interval between each configuration BPDU sent by the root bridge.
Hold Time	The minimum number of seconds that must elapse between transmissions of consecutive Configuration BPDUs on a port.
Fwd Delay	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Topology Last Change	The number of seconds since the last time a topology change occurred.
Topology Change Counter	The number of times the topology has changed since this device was reloaded.
Bridge Address	The STP address of this device or VLAN.
STP Port Parameters	
Port	The port number.
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Path Cost	The port’s STP path cost.
State	The port’s STP state. The state can be one of the following: • BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • FORWARDING – STP is allowing the port to send and receive frames. • LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No user frames are transmitted or received during this state. • LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP’s reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
Forward Transition	The number of times STP has changed the state of this port between BLOCKING and FORWARDING.

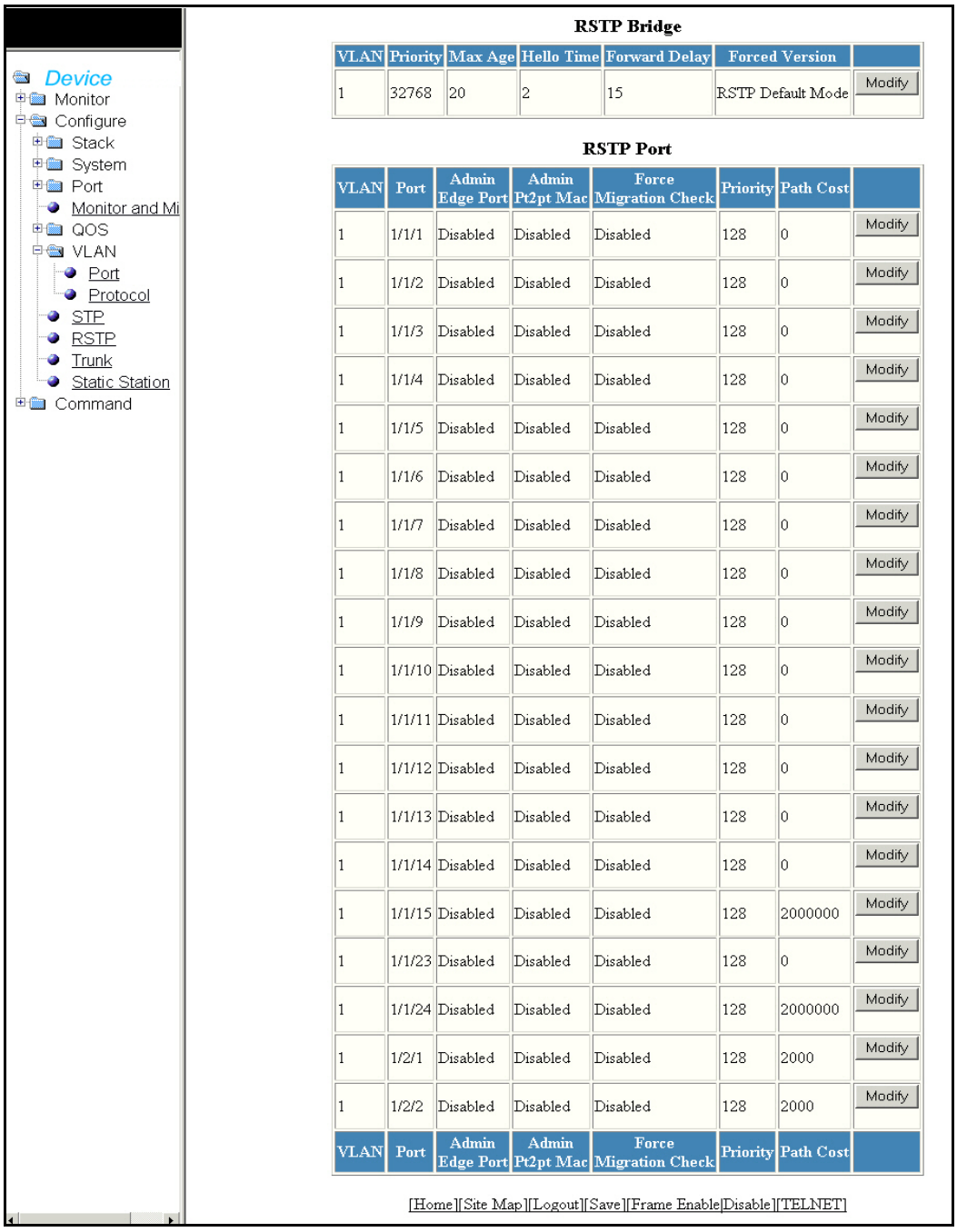
Cost	The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Design Bridge field.
Design Root	The root bridge as recognized on this port. The value is the same as the root bridge ID listed in the Root ID field.
Design Bridge	The designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge.
Display	Changes the unit ID by selecting a unit from the drop-down list and clicking **Display**.

Configuring RSTP

Select **Configure > RSTP**, to enable RSTP feature in the PowerConnect B-Series FCX switch.

NOTE
Earlier implementation of Rapid Spanning Tree Protocol (RSTP), which was 802.1W Draft 3 provides only a subset of the IEEE 802.1W standard; whereas the 802.1W RSTP feature provides the full standard. The implementation of the 802.1W Draft 3 is referred to as RSTP Draft3. RSTP Draft3 will continue to be supported on Dell devices for backward compatibility. Users currently using RSTP Draft 3 should migrate to 802.1W.

FIGURE 104 Configuring the RSTP bridge

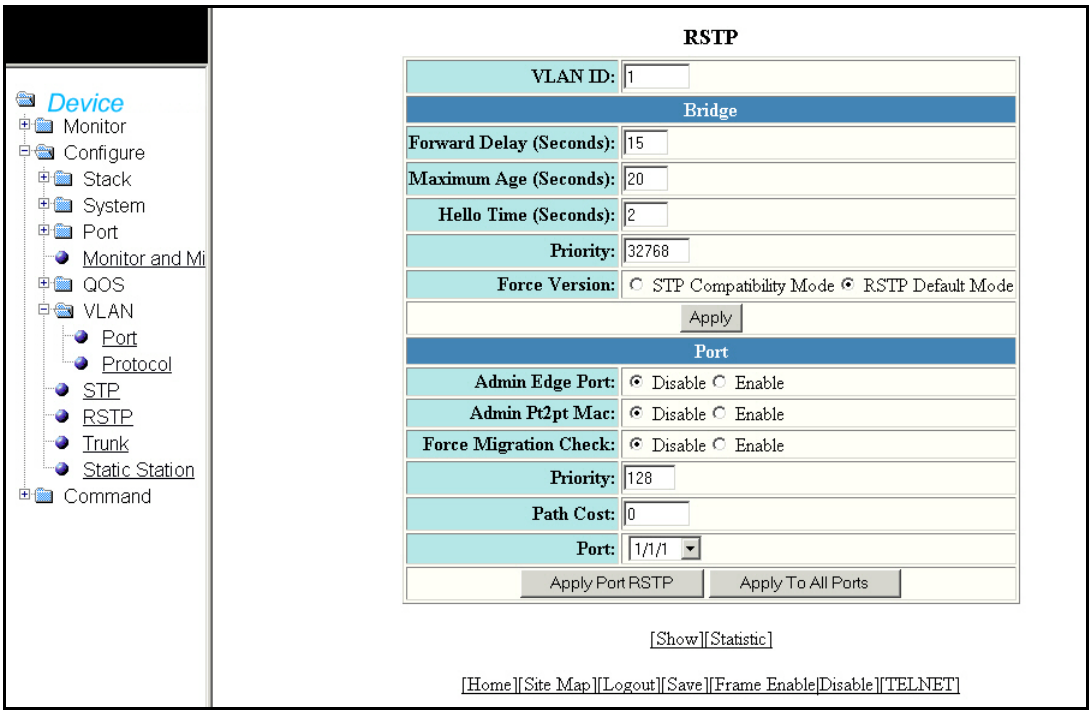


The RSTP Bridge and Port contains the following information.

RSTP Bridge Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Max.Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time	The interval between each configuration BPDU sent by the root bridge.
Forward Delay	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Forced version	The configured force version value. One of the following value is displayed: • 0 – The bridge has been forced to operate in an STP compatibility mode. • 2 – The bridge has been forced to operate in an 802.1W mode. (This is the default.)
RSTP Port Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
Port Admin Edge	If set to enabled, then the port becomes an edge port in the domain.
Port Admin Pt2pt Mac	If set to enabled, then a port is connected to another port through a point-to-point link. The point-to-point link increases the speed of convergence. This parameter, however, does not auto-detect whether or not the link is a physical point-to-point link.
Force Migration Check	The force-migration-check parameter forces the specified port to sent one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port will go return to sending STP BPDUs.
Priority	This specifies the priority of the bridge. You can enter a value from 0 – 65535. A lower numerical value means the bridge has a higher priority. Thus, the highest priority is 0. The default is 32768.
Path Cost	This specifies the cost of the port's path to the root bridge. 802.1W prefers the path with the lowest cost. You can specify a value from 1 – 20,000,000.

Click **Modify** to modify any port. Click **Apply** to save the configuration.

FIGURE 105 Modifying RSTP parameters



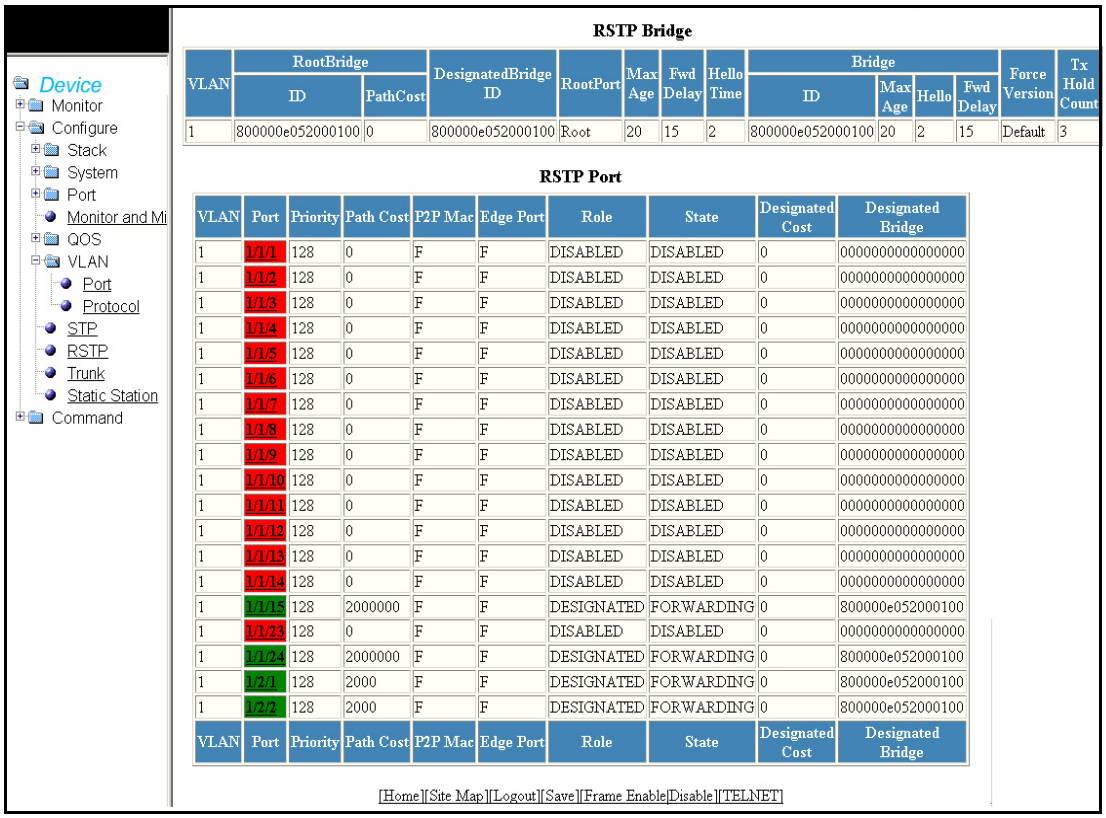
The RSTP parameters contains the following information.

RSTP Bridge Parameters	
Forward Delay (Seconds)	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Maximum Age (Seconds)	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello Time (Seconds)	The interval between each configuration BPDU sent by the root bridge.
Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority.
Force Version	The configured force version value. One of the following value is displayed: • 0 – The bridge has been forced to operate in an STP compatibility mode. • 2 – The bridge has been forced to operate in an 802.1W mode. (This is the default.)
RSTP Port Parameters	
Admin Edge Port	If set to enabled, then the port becomes an edge port in the domain.
Admin Pt2pt Mac	If set to enabled, then a port is connected to another port through a point-to-point link. The point-to-point link increases the speed of convergence. This parameter, however, does not auto-detect whether or not the link is a physical point-to-point link.

Force Migration Check	The force-migration-check parameter forces the specified port to sent one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port will go return to sending STP BPDUs.
Priority	The configured priority of the port. The default is 128 or 0x80.
Path Cost	The configured path cost on a link connected to this port.
Port	ID of the port in slot#/port#format.

Click **Statistic** to display the details of RSTP statistic as shown in Figure 106

FIGURE 106 RSTP Statistic



The RSTP statistic display contains the following information.

RSTP Bridge Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
RootBridge ID	The ID assigned by STP to the root bridge for this spanning tree.
RootBridge PathCost	The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.
DesignateBridge ID	The bridge from where the root information was received.It can be from the root bridge itself, but it could also be from another bridge.

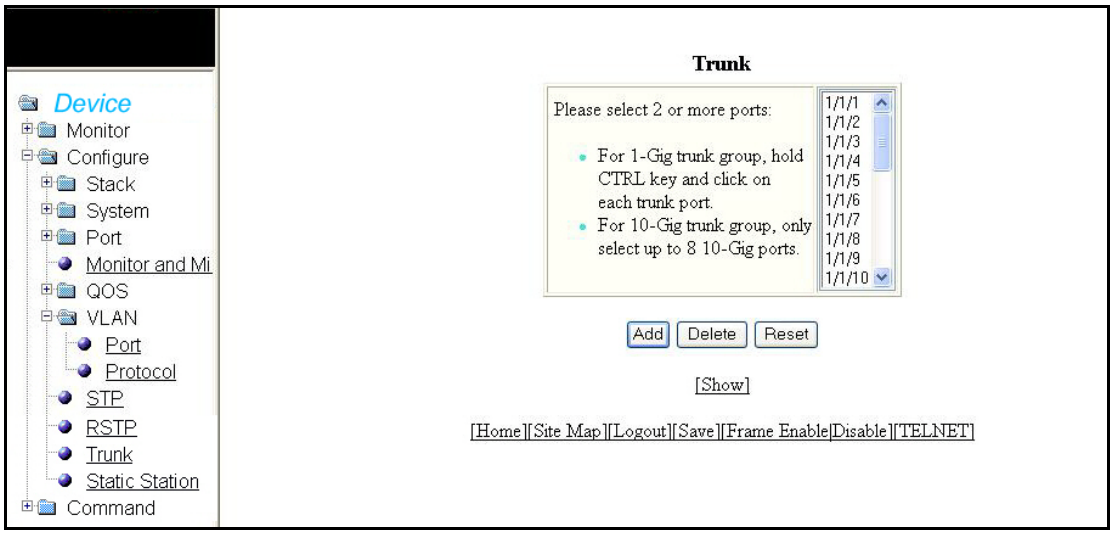
Root Port	The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number.
Max.Age	The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Fwd Delay	The number of seconds a non-edge Designated port waits until it can apply any of the following transitions, if the RST BPDU it receives does not have an agreed flag: • Discarding state to learning state • Learning state to forwarding state When a non-edge port receives the RST BPDU it goes into forwarding state within 4 seconds or after two hello timers expire on the port. Fwd Dly is also the number of seconds that a Root port waits for an RST BPDU with a proposal flag before it applies the state transitions listed above. If the port is operating in 802.1D compatible mode, then forward delay functionality is the same as in 802.1D (STP).
Hello Time	The interval between each configuration BPDU sent by the root bridge.
Bridge ID	The ID of the bridge
Bridge MaxAge	The configured max age for this bridge. The default is 20.
Bridge Hello	The configured hello time for this bridge.The default is 2.
Bridge Fwd Delay	The configured forward delay time for this bridge. The default is 15.
Force Version	The configured force version value. One of the following value is displayed: • 0 – The bridge has been forced to operate in an STP compatibility mode. • 2 – The bridge has been forced to operate in an 802.1W mode. (This is the default.)
Tx Hold Count	The number of BPDUs that can be transmitted per Hello Interval. The default is 3.
RSTP Port Parameters	
Vlan	The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1.
Port	The port number.
Priority	The configured priority of the port. The default is 128 or 0x80.
Path Cost	The port’s STP path cost.
P2P Mac	Indicates if the point-to-point-mac parameter is configured to be a point-to-point link: • T – The link is configured as a point-to-point link. • F – The link is not configured as a point-to-point link. This is the default.
Edge Port	Indicates if the port is configured as an operational Edge port: • T – The port is configured as an Edge port. • F – The port is not configured as an Edge port. This is the default.

Role	The current role of the port: • Root • Designated • Alternate • Backup • Disabled For more information, refer to “Bridges and bridge port roles” of *PowerConnect B-Series FCX Configuration Guide*.
State	The port’s STP state. The state can be one of the following: • BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • FORWARDING – STP is allowing the port to send and receive frames. • LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No user frames are transmitted or received during this state. • LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP’s reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
Designated Cost	The best root path cost that this port received, including the best root path cost that it can transmit.
Designated Bridge	The ID of the bridge that sent the best RST BPDU that was received on this port.

Configuring trunk

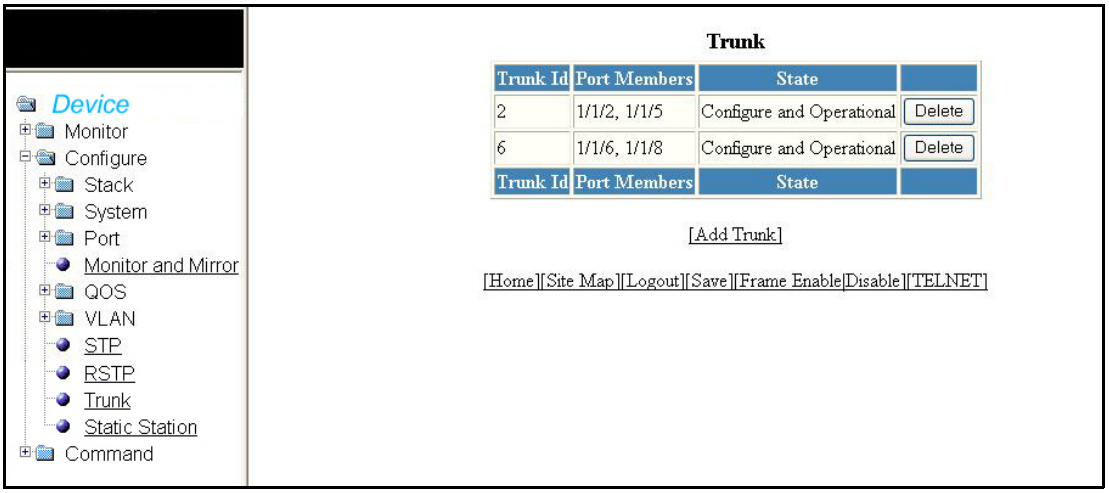
Select **Configure > Trunk** to configure trunk.

FIGURE 107 Configuring the Trunk



Select multiple ports using Ctrl key and click **Add** to display the added ports.

FIGURE 108 Adding port members in the Trunk



The trunk display contains the following information.

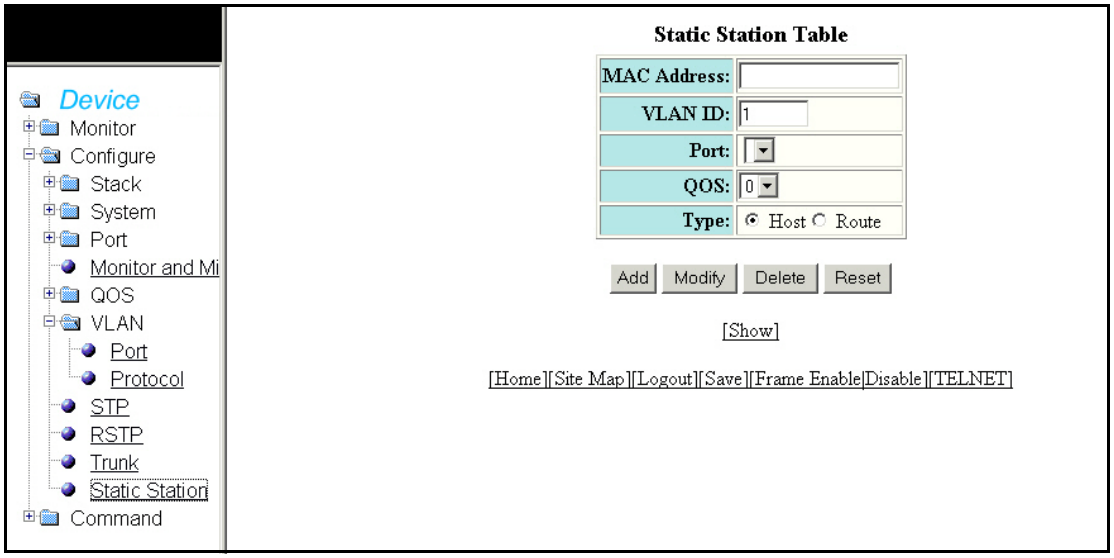
Trunk Id	The trunk group number. The software numbers the groups in the display to make the display easy to use.
Port Members	Displays the added port members in the trunk group.
State	Specifies the state of the port and indicates if it is configured and operational.
Add	Enables you to add the port members.

Delete	Enables you to delete the added port members.
Reset	To undo your changes, click Reset.
Show	Display the Trunk entries.
Add Trunk	Allows you to add new ports.

Configuring static station

Select **Configure > Static Station** to configure static station.

FIGURE 109 Configuring the static station



The static station display contains the following information.

MAC Address	The MAC address of the device.
Vlan ID	Enables you to select a Vlan ID. This Vlan ID field is disabled if no port was configured.
Port	The port number.
QOS	The QoS attribute specifies the priority of the incoming traffic based on any value between 0 (lowest priority) and 7 (highest priority). Default is 0.
Type	Specifies the type of the device; host or route
Add	Enables you to add the MAC Address.
Modify	Enables you to modify the changes.
Delete	Enables you to delete the changes made.
Reset	To undo your changes, click Reset.
Show	Displays the static station table entries.

Chapter

5

Stack Commands

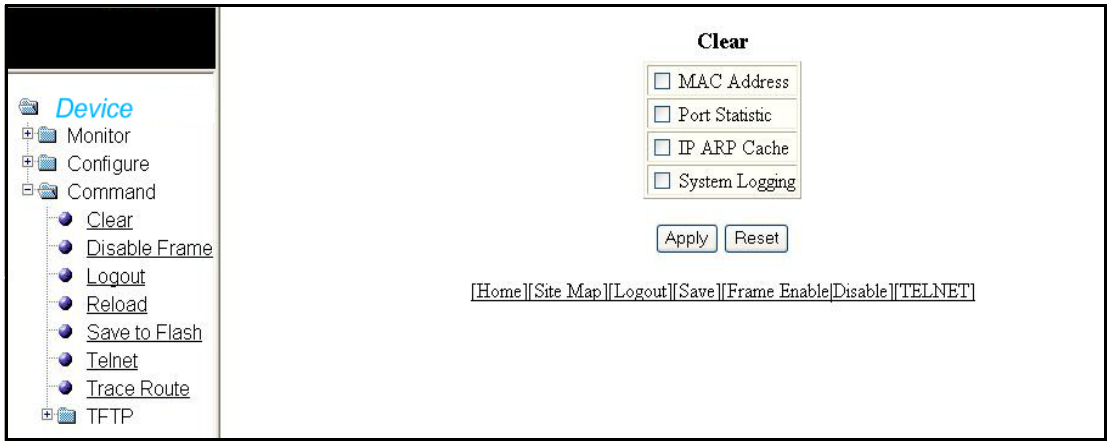
In this chapter

Clearing information

The Web Management Interface provides additional commands that include configuration settings and stack configuration.

Select **Command > Clear** to clear specific data related to a stack. Select the check boxes to clear information for MAC Address, Port Statistics, IP ARP Cache, or System Logging. This will delete all current entries and reset the entries to zero. Click **Apply** to clear the data.

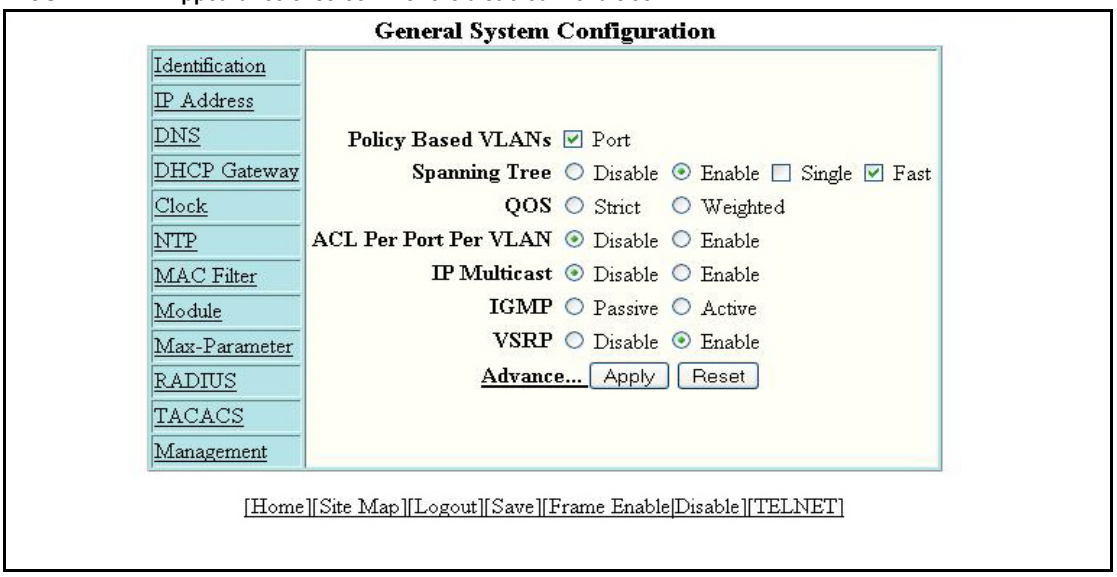
FIGURE 110 Command - Clear



Disabling or enabling the menu view

Select **Command > Disable Frame** to hide the menu tree from the left panel. Click **Frame Enable** hyperlink to show the menu tree appearing at the bottom of the window.

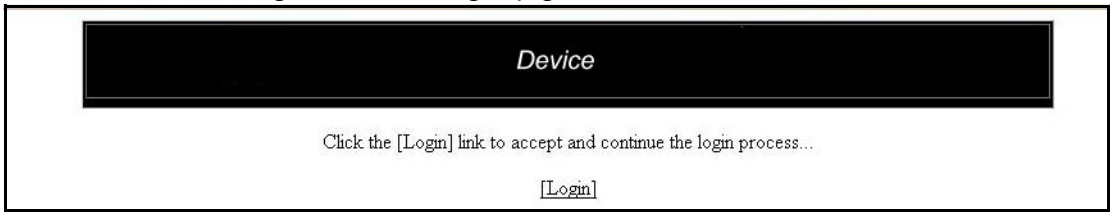
FIGURE 111 Appearance of screen with the disabled menu tree



Logging out

Select **Command > Logout** to exit the Web Management Interface. You can re-login through login hyperlink at the bottom.

FIGURE 112 Web Management Interface Logout page



Reloading units in a stack

Select **Command > Reload** to reload any or all of the units within a stack. Select the check box in the **Select** column allows you to specify the units you want to reload. Click **Yes** to start the process.

FIGURE 113 Command - Reloading Stack Units

The Reset Stack Units contains the following information.

Unit ID	Stack member to reload.
Type	Device model number.
Role	Stack unit roles include: • Active - Handles stack management and configures all system and interface-level features. • Standby - Takes over if the current active controller fails. • Member - A unit functioning in the stack in a capacity other than Active or Standby Controller.

NOTE

If the Active Controller is reset or removed from the stack, the entire stack reloads and Active Controller and Standby Controller elections are initiated. If the unit functioning as the previous Active Controller, is no longer part of the stack, the Standby Controller unit becomes the new Active Controller. After a reset, if no stack member qualifies as Active Controller, the existing Standby Controller waits 30 seconds and then assumes the role of Active Controller.

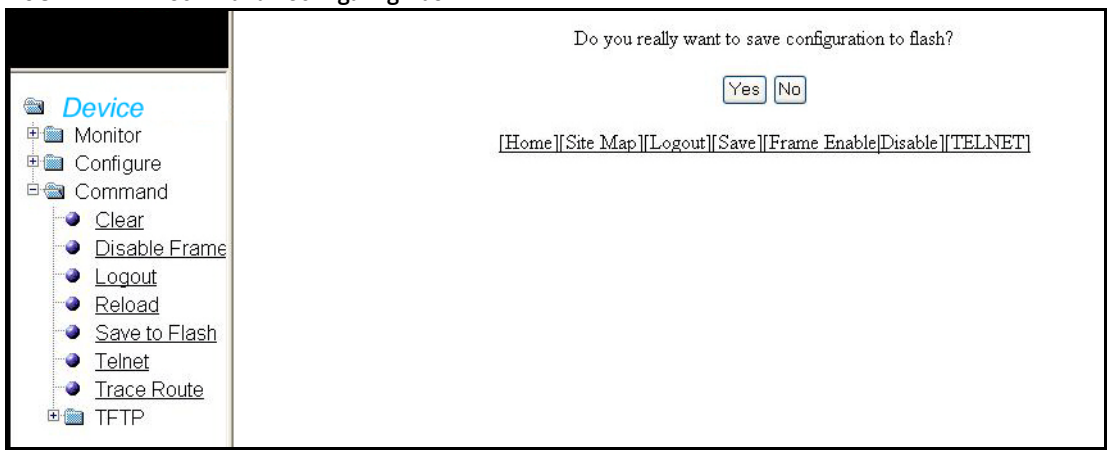
If both Active and Standby Controllers are removed the rest of the stack will continue to function because they are operating on whatever is programmed in the hardware. The stack members will not be able to learn any new addresses.

Saving the configuration to flash

Select **Command > Save To Flash** to save configuration changes. Click **Yes** to confirm saving the configuration.

NOTE
Changes to memory allocation require you to reload the software after you save the changes to the startup-config file.

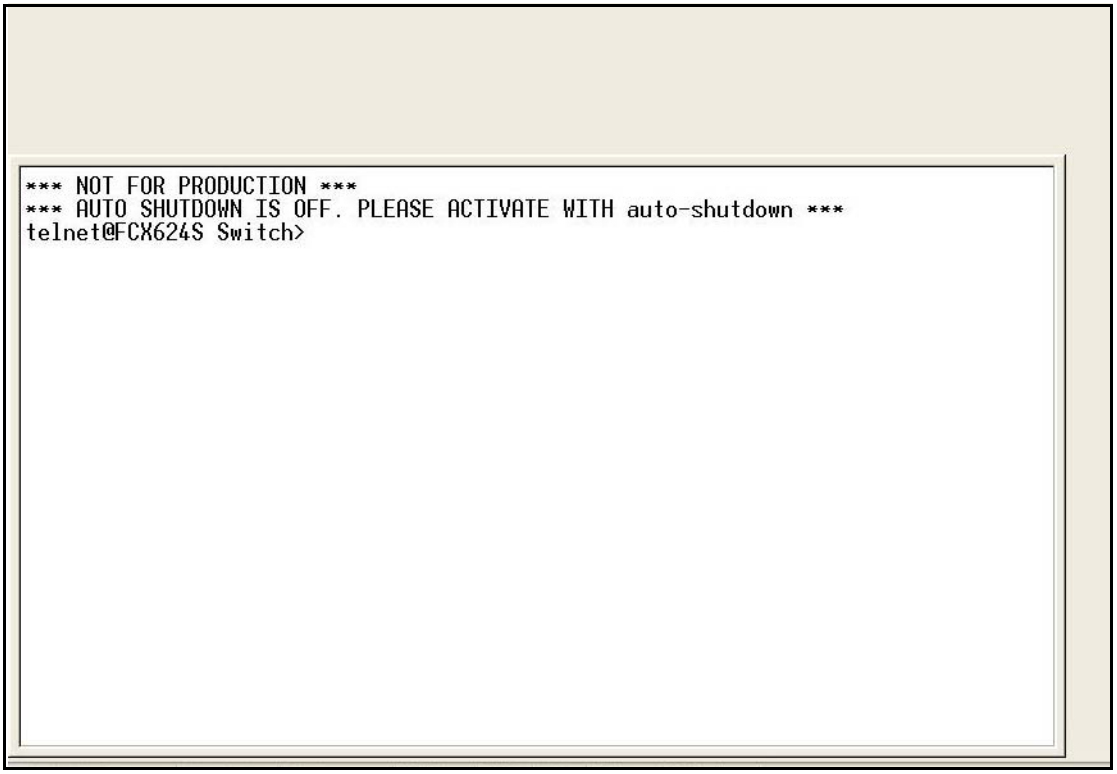
FIGURE 114 Command - Configuring Flash



Accessing a telnet command prompt

The Telnet command establishes a Telnet connection from a Dell device to a remote IPv6 host using the console. Select **Command > Telnet** to open a Telnet CLI window.

FIGURE 115 Telnet Command



The syntax for Telnet is:

Syntax: **telnet** *<ipv6-address> [<port-number> | outgoing-interface ethernet <port> | ve <number>]*

where:

- *<ipv6-address>* specifies the address of a remote host. You must specify this address in hexadecimal using 16-bit values between colons.
- *<port-number>* specifies the port number on which the Dell device establishes the Telnet connection. You can specify a value between 1 to 65535. If you do not specify a port number, the Dell device establishes the Telnet connection on port 23.
- If the IPv6 address you specify is a link-local address, you must specify the outgoing-interface Ethernet <port> | ve <number> parameter. This parameter identifies the interface that must be used to reach the remote host. If you specify an Ethernet interface, you must also specify the port number associated with the interface. If you specify a VE interface, also specify the VE number.

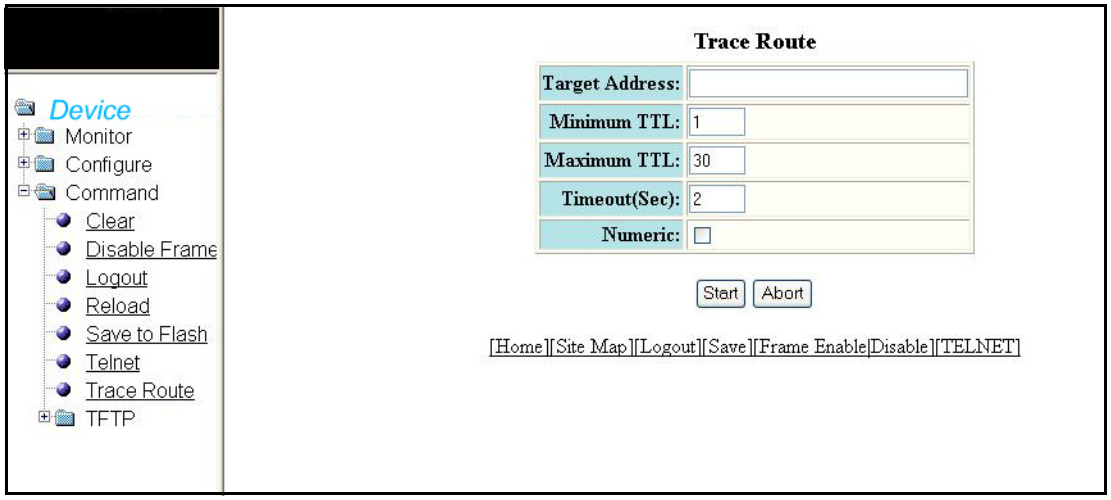
Performing a trace

The Trace Route command allows you to trace a path from the Dell device to an IPv6 host. Trace route requests show all responses to a minimum TTL of 1 second and a maximum TTL of 30 seconds. In addition, if there are multiple equal-cost routes to the destination, the Dell device displays up to three responses.

Select **Command > Trace Route** to reload any or all of the units within a stack.

Fill up the field with relevant information and click **Start** to begin the trace process or **Abort** to exit without performing the trace.

FIGURE 116 Command - Trace Route



The Trace Route option has the following details.

Target Address	Specifies the IP address of the host at the other end of the route. You must specify this address in hexadecimal using 16-bit values between colons.
Minimum TTL	Default is 1.
Maximum TTL	Default is 30.
Timeout (sec)	Specifies how many milliseconds the router waits for a reply from the pinged device. You can specify a timeout from 1 to 4294967296 milliseconds. The default is 5000 (5 seconds).
Numeric	For parameters that require a numeric value, the trace route does not check that the value you enter is within the allowed range. Instead, if you do exceed the range for a numeric value, the software rounds the value to the nearest valid value.

Using TFTP

When the device reboots, or the auto-configuration feature has been disabled and then re-enabled, the device uses information from the DHCP server to contact the TFTP server to update the running configuration file. If the DHCP server provides a TFTP server name or IP address, the device uses this information to request files from the TFTP server. If the DHCP server does not provide a TFTP server name or IP address, the device requests the configuration files from the DHCP server.

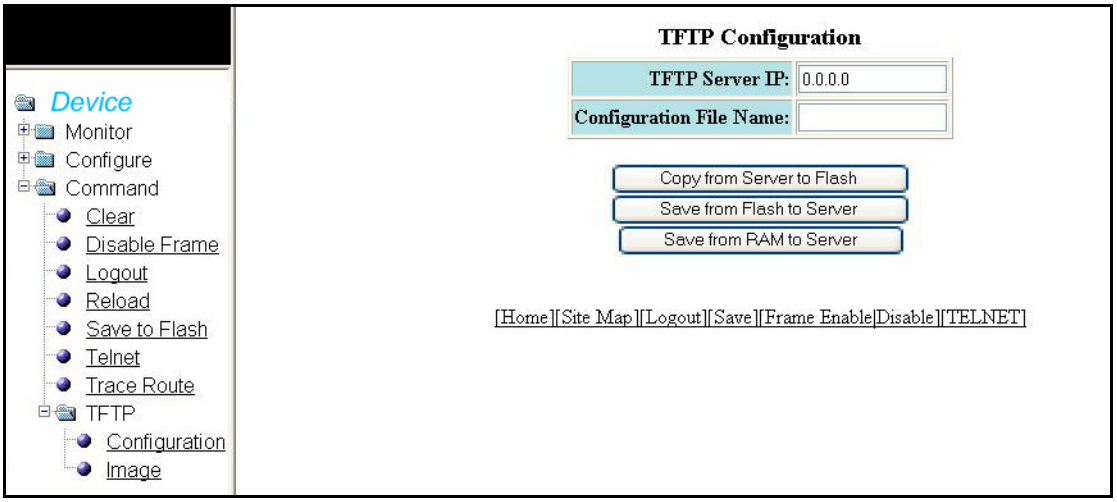
The device requests the configuration files from the TFTP server by asking for filenames in the following order:

- Boot file name provided by the DHCP server (if configured)
- Host name MAC address configuration file
- Dellconfiguration file

If the device is successful in contacting the TFTP server and the server has the configuration files, the files are merged. If there is a conflict, the server file takes precedence. If the device is unable to contact the TFTP server or if the files are not found on the server, the TFTP part of the configuration download process ends.

Select **Command > TFTP > Configuration** to access the TFTP configuration.

FIGURE 117 Command - TFTP Configuration



The TFTP Configuration contains the following information.

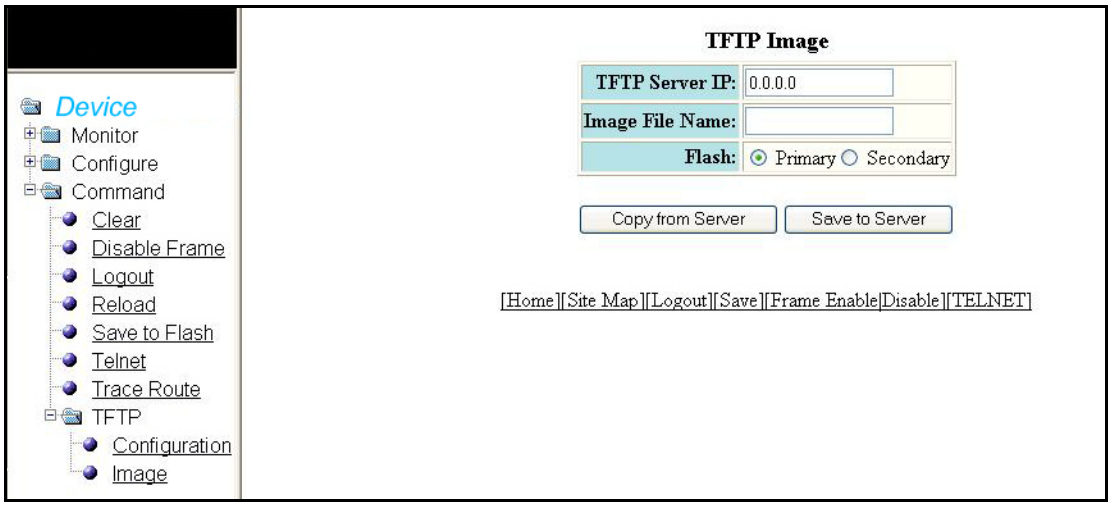
TFTP Server ID	The IP address of the most-recently contacted TFTP server, if the switch has contacted a TFTP server since the last time the software was reloaded or the switch was rebooted.
Configuration File Name	The name under which the Layer 2 Switch's startup-config file was uploaded or downloaded during the most recent TFTP access.

The options for creating and saving the TFTP configuration includes:

- Copy from Server to Flash
- Copy from Flash to Server
- Save from RAM to Server

Select **Command > TFTP > Image** to access the TFTP Image configuration.

FIGURE 118 Command - TFTP Image



The TFTP image display contains the following information.

TFTP Server ID	The IP address of the most-recently contacted TFTP server, if the switch has contacted a TFTP server since the last time the software was reloaded or the switch was rebooted.
Image File Name	The name of the Layer 2 Switch flash image (system software file) that was uploaded or downloaded during the most recent TFTP access.
Flash	Primary flash is the default local storage device for image files and configuration files. Secondary flash is a second flash storage device you can use to store redundant images for additional booting reliability or to preserve one software image while testing another one.

The options for creating and saving the TFTP image include:

- Copy from Server
- Save to Server