USER GUIDE

Ruckus FastIron Web Management Interface User Guide, 08.0.70

Supporting FastIron Software Release 08.0.70

Part Number: 53-1005300-03
Publication Date: 24 May 2018

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **7**
- Document Conventions 7
  - Notes, Cautions, and Warnings 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9
  - What Support Do I Need? 9
  - Open a Case 9
  - Self-Service Resources 9

About This Document **11**
- Supported hardware 11
- What's new in this document 11

Getting Started with the GUI **13**
- Access requirements 13
- Prerequisite configuration 13
- Logging in to the Web Management Interface 14
- Logging out of the Web Management Interface 17
- Using the Web Management Interface 17
  - Web Management Interface areas 19

Monitoring Basic Device Information **21**
- Displaying the ARP cache 21
- Displaying the device information 22
- Displaying flash information 24
- Displaying memory information 25
- Displaying the front panel 26
  - Status LED display 26
  - Displaying the front panel for the Ruckus ICX 7750 device 26
  - Displaying the front panel for the Ruckus ICX 7450 device 27
  - Displaying the front panel for the Ruckus ICX 7250 device 27
  - Displaying the front panel for the Ruckus ICX 7150 28
  - Displaying the front panel for the Ruckus ICX 7650 28
- Displaying MAC addresses 29
- Displaying the system log 30

Monitoring Stacks **33**
- Displaying the stack details 33
- Displaying a stack module 35
- Displaying stack neighbors 35
- Displaying stack ports information 36
- Displaying stack port statistics 37
- Displaying stack port interfaces 38

Monitoring Ports **41**
- Displaying Ethernet port statistics 41

Displaying Ethernet port attributes....44
Displaying Ethernet port utilization....47
Displaying the management port information....49
Displaying the management port real-time information....51
Displaying port inline power for Ruckus ICX devices....52
Displaying inline power details....52
Displaying inline power statistics....54
Monitoring STP....59
Displaying STP information....59
Monitoring RSTP....65
Displaying RSTP information....65
Monitoring IP....69
Displaying IP cache....69
Displaying IP traffic information for devices running Layer 2 code....70
Displaying IP traffic information for devices running Layer 3 code....75
Monitoring RMON....81
Displaying RMON history....81
Displaying RMON Ethernet statistics....83
Changing polling interval....88
Displaying RMON Ethernet error statistics....89
Configuring Stack Components....93
Configuring the general settings for a traditional stack....93
Viewing stack priority details....94
Modifying stack ports....94
Configuring a stack module....96
Configuring System Components....99
Configuring the system clock....99
Configuring the system DNS....100
Configuring the general system settings....101
Configuring the system identification....103
Configuring the system IP address....104
Configuring a standard ACL....105
Configuring an extended ACL....106
Configuring an IP access group....110
Configuring the system MAC filter....111
Configuring a filter group....113
Configuring the maximum system parameter value....114
Configuring a system module....115
Configuring a RADIUS server....117
Configuring a TACACS/TACACS+ server....119
Configuring management authentication....120
Configuring management authorization....121
Configuring management accounting....122
Configuring an SNMP community string....123
Configuring the general management parameters....124
Configuring a management system log....126
Adding a log server....127

Configuring a trap 128
Configuring a trap receiver 129
Configuring a management user account 131
Configuring the web management preferences 131

Configuring Port Parameters 135
Configuring an Ethernet port 135
Configuring port inline power 138
Configuring a management port 139
Configuring the port uplink relative utilization 140

Configuring Monitor and Mirror Port 143
Configuring a mirror port 143
Configuring a monitor port 145

Configuring QoS 147
Configuring the QoS profile 147
Configuring the QoS profile bind 148

Configuring VLAN 151
Configuring a port VLAN 151
Modifying a port VLAN 155

Configuring STP 159
Configuring STP parameters 159
Changing STP bridge parameters 159
Changing STP port parameters 162

Configuring RSTP 167
Configuring RSTP parameters 167
Changing RSTP bridge parameters 167
Changing RSTP port parameters 169

Configuring LAGs 173
Configuring a static, dynamic, or keep-alive LAG 173
Displaying a configured LAG 177

Configuring a Static Station 179
Adding a static station 179
Modifying a static station 180

Configuring IP 183
Configuring the router IP address 183
Configuring a standard ACL 185
Configuring an extended ACL 186
Configuring an IP access group 190
Configuring an IP Autonomous System-path access list 192
Configuring an IP community list 193
Configuring an IP prefix list 194
Configuring a DNS entry 196
Configuring the general IP settings 197
Configuring IP interfaces 199
Configuring a static ARP 201
Configuring a static RARP 202
Configuring a UDP helper 204

Enabling forwarding for a UDP application 205
Specifying the UDP application 206

Configuring RIP 207
Configuring the general RIP settings 207
Configuring a RIP interface 208
Configuring a RIP neighbor filter 212
Configuring a RIP redistribution filter 214

Basic Device Commands 217
Clearing information for a Layer 2 switch 217
Clearing information for a Layer 3 switch 218
Disabling or enabling the menu view 219
Logging out 220
Reloading units in a stack 221
Saving the configuration to flash 222
Switching over to the active role 223
Accessing the Telnet command prompt 223
Performing a trace 225

Using TFTP 227
Configuring TFTP 227
Configuring a TFTP image 229

Preface

- Document Conventions 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9

Document Conventions

The following tables list the text and notice conventions that are used throughout this guide.

TABLE 1 Text conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples.	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the 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.

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.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - Ruckus Small Cell Alarms Guide SC Release 1.3
  - Part number: 800-71306-001
  - Page 88

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Request for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

The Support Portal at https://support.ruckuswireless.com/contact-us offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers

- Software Downloads and Release Notes—https://support.ruckuswireless.com/software
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management

About This Document

- Supported hardware 11
- What's new in this document 11

Supported hardware

This guide supports the following Ruckus products:

- Ruckus ICX 7750 Series
- Ruckus ICX 7650 Series
- Ruckus ICX 7450 Series
- Ruckus ICX 7250 Series
- Ruckus ICX 7150 Series

For information about what models and modules these devices support, see the hardware installation guide for the specific product family.

What's new in this document

Summary of enhancements in FastIron release 08.0.70: The Web Management Interface support is added for Ruckus ICX 7650.

Summary of enhancements in FastIron release 08.0.70 version 2: Minor editorial updates throughout the guide.

Getting Started with the GUI

- Access requirements....13
- Prerequisite configuration....13
- Logging in to the Web Management Interface....14
- Logging out of the Web Management Interface....17
- Using the Web Management Interface....17

Access requirements

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

The Web Management 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

For all the other older browsers, the Web Management Interface displays only the list view.

NOTE
Web management pages may not get properly displayed with Google Chrome when Network Mapper (Nmap 6.4) is active.

Prerequisite configuration

The following steps must be completed to enable access to the Web Management Interface.

1. Connect a PC via a serial connection to the device using the console port. Use a terminal program such as PuTTY to access the Command Line Interface (CLI).

   If the switch is already connected to a network, the switch will automatically receive its IP configuration via DHCP. To check the IP configuration of the switch, use the **show ip** command.

   If the switch is not connected to a network or you wish to assign an IP address manually, then use the commands described in step 2, otherwise go to step 3.

2. Assign an IP address to the device using the Command Line Interface (CLI).

```
device> enable
device# configure terminal
device(config)# ip address 10.37.71.212/24
device(config)# ip default-gateway 10.37.71.129
```

   For more information on assigning IP addresses for a device, refer to the *Ruckus FastIron Layer 3 Routing Configuration Guide*.

3. Generate a Secure Sockets Layer (SSL) certificate and then configure a username and password to log in.

```
device(config)# crypto-ssl certificate generate
device(config)# username ruckus password ruckus
device(config)# aaa authentication login default local
device(config)# aaa authentication web-server default local
```

   It may take several minutes to generate the certificate key.

4. Save the configuration.

```
device(config)# write memory
```

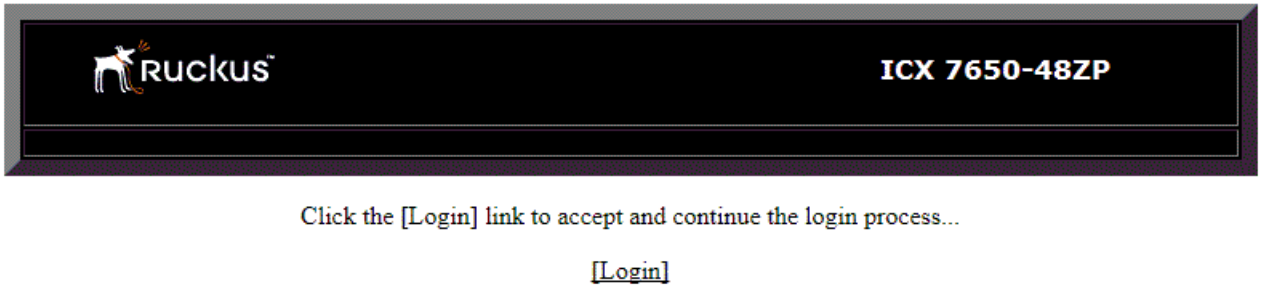
Logging in to the Web Management Interface

To log in to the Web Management Interface, perform the following steps.

1. Open a web browser and enter the IP address of the management port in the Location or Address field.

   The web browser contacts the Ruckus device and displays the login page, as shown in the figure below.

FIGURE 1 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 online help provided with your web browser.

2. Click **Login**. The dialog box as shown in the figure below is displayed.

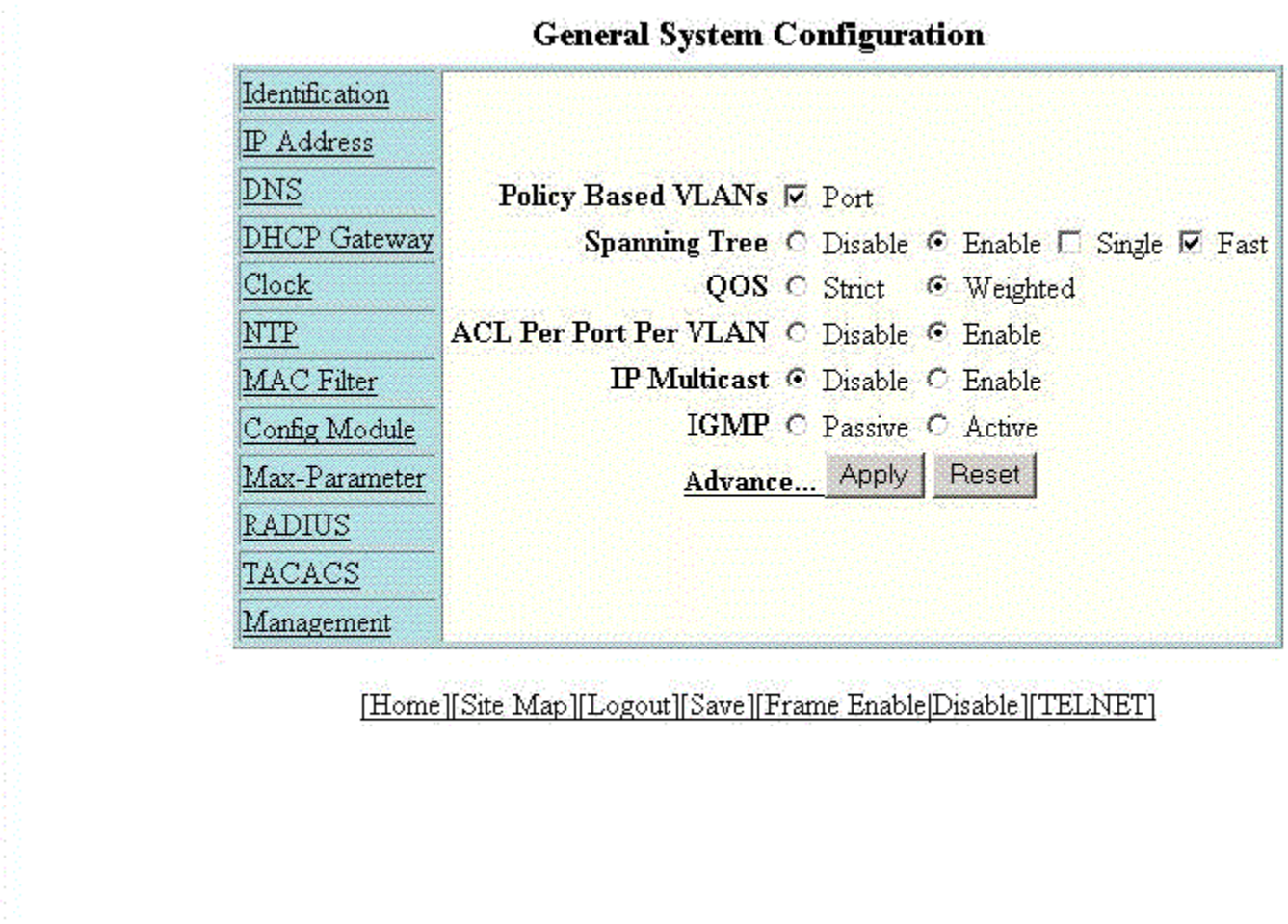
FIGURE 2 User name and password dialog box



3. Enter the user name and password that you created using the CLI as described in Prerequisite configuration on page 13.

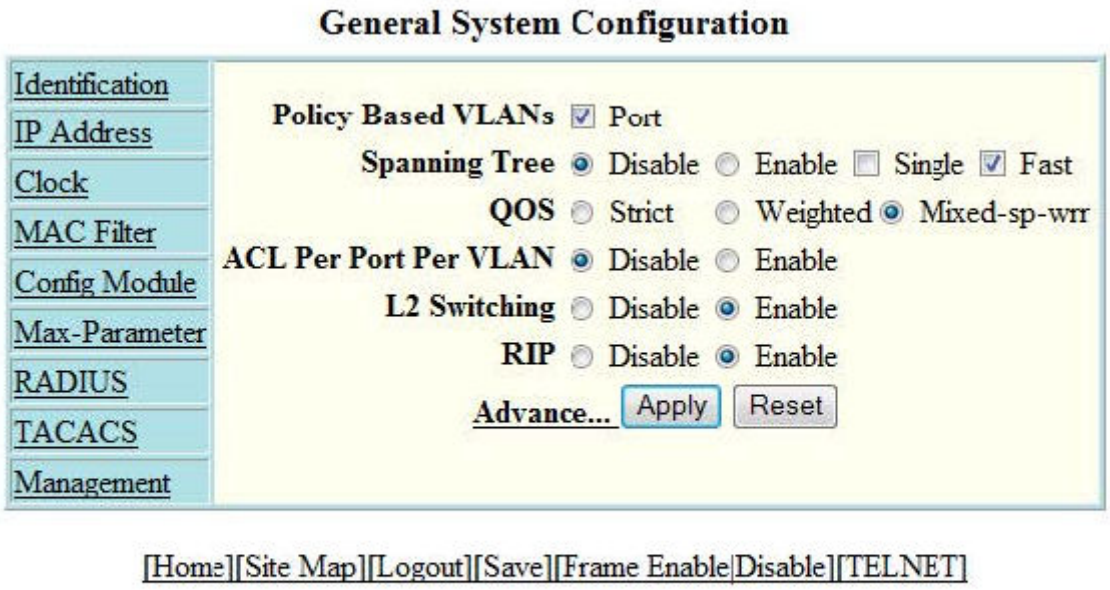
The figure below displays the home page of the Web Management Interface for a Layer 2 switch.

FIGURE 3 Home page for Layer 2 switch features



The figure below displays the home page of the Web Management Interface for a Layer 3 switch.

FIGURE 4 Home page for Layer 3 switch features



NOTE
If you are using Internet Explorer 6.0 to view the Web Management Interface, make sure the version you are running includes the latest service packs. Otherwise, the navigation tree (the left-most pane in the two figures above) will not display properly. For information on how to load the latest service packs, refer to the online help provided with your web browser.

Logging out of the Web Management Interface

You can log out of the Web Management Interface in two ways:

- Click **Logout** on the window.
- Click **Command** in the left pane and select **Logout**.

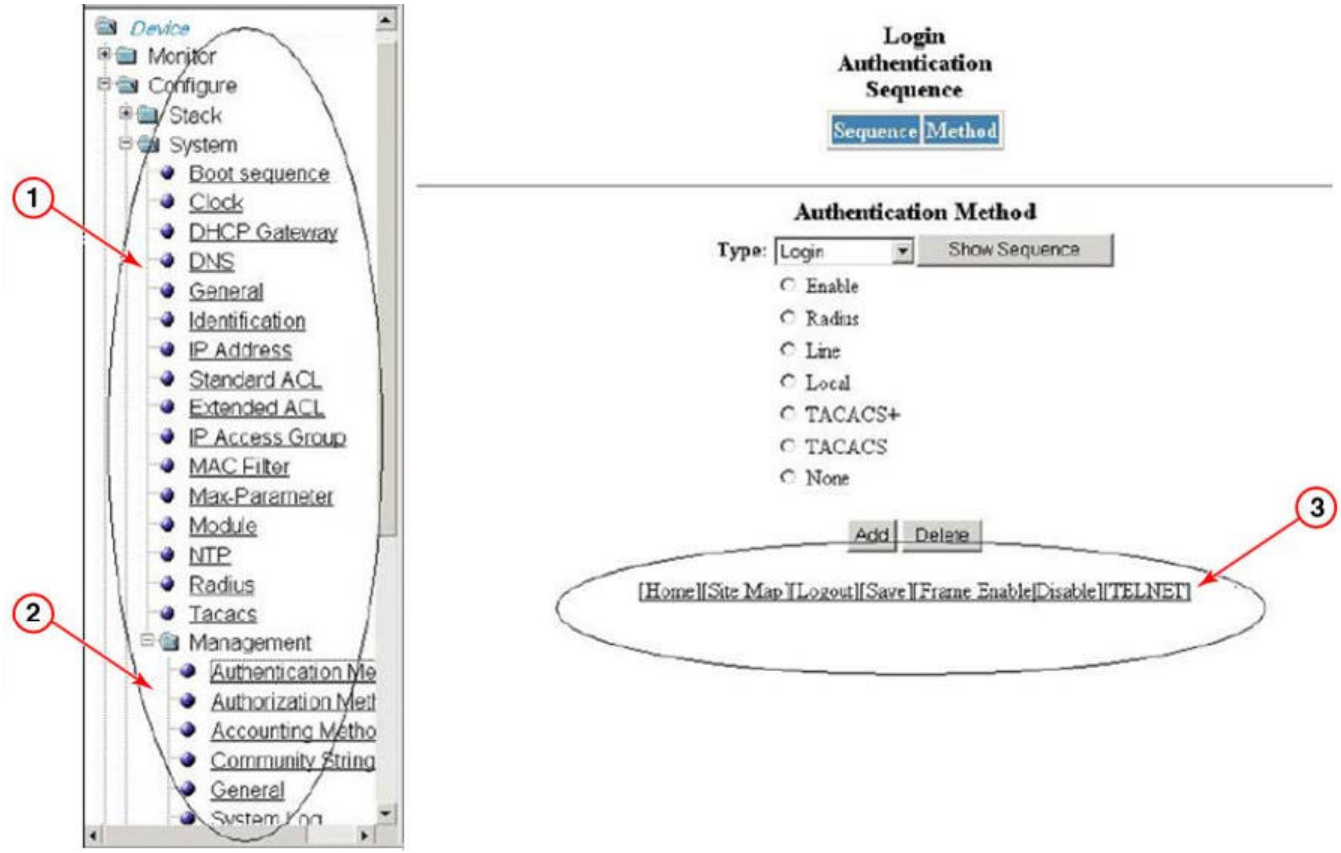
Using the Web Management Interface

The following procedure explains in detail about using the Web Management Interface.

1. Click the plus sign (+) next to **Configure** in the tree view to expand the list of configuration options.
2. Click the plus sign (+) next to **System** in the tree view to expand the list of system configuration links.

3. Click the plus sign (+) next to **Management** in the tree view to expand the list of system management links.
4. Click **Authentication Methods** to display the **Authentication Method** panel.
5. Enable or disable elements on the Web Management Interface by clicking the appropriate options on the panel. The figure below identifies the elements you can change.

FIGURE 5 Web Management Interface elements



1. Menu Type (Tree view)
2. Menu Frame
3. Shortcut links

NOTE
The tree view is available when you use the Web Management Interface with Netscape 4.0 or higher or Internet Explorer 4.0 or higher. If you use the Web Management Interface with an older browser, the Web Management Interface displays the list view only, and the Web Management Preferences panel does not include an option to display the tree view.

6. When you have finished, click **Add** on the panel to add the authentication types. Click **Delete** to remove authentication types.

7. To save the configuration, click the plus sign (+) next to the **Command** folder, and then click **Save to Flash**.

NOTE
The only changes that become permanent are the settings to the Menu Type and the Panel Frame. Any other elements you enable or disable will go back to their default settings the next time you start the Web Management Interface.

Web Management Interface areas

The following sections describe the Web Management Interface areas and how to use them.

Menu tree or list

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. You can enable or disable the menu tree view in two ways:

- Click **Frame Enable|Disable** on the bottom of the window.
- Click **Command** and select **Disable Frame**
- .

Configuration panel

The configuration panel consists of the tables with the field elements that display information or the input fields for which the values have to be entered. The input fields can be of four types:

- Fields into which data must be entered using the keyboard.
- Lists from which one of several options can be chosen.
- Options allow you to select only one of the settings or features of a set of options.
- Check boxes allow you to turn on or off a parameter and you can also make multiple selections.

After entering the values, you must click the appropriate button to configure the values.

Shortcuts to functions and other panels

All the pages in the Web Management Interface provide shortcut links to the functions that are specific to that page and to other panels. All of the Web Management Interface panels 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** link to move through 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. If frames are disabled, you will not be able to choose any of the options on the web preference panel that use frames.

Monitoring Basic Device Information

- Displaying the ARP cache..... 21
- Displaying the device information..... 22
- Displaying flash information..... 24
- Displaying memory information..... 25
- Displaying the front panel..... 26
- Displaying MAC addresses..... 29
- Displaying the system log..... 30

Displaying the ARP cache

The Address Resolution Protocol (ARP) cache table contains entries that map IP addresses to Media Access Control (MAC) addresses. There are two types of ARP entries: static (user-configured) and dynamic (learned).

To display the **ARP cache** information, click **Monitor** on the left pane and select **ARP Cache.**

The **ARP Cache** window is displayed as shown in the figure below.

FIGURE 6 Monitoring the ARP cache

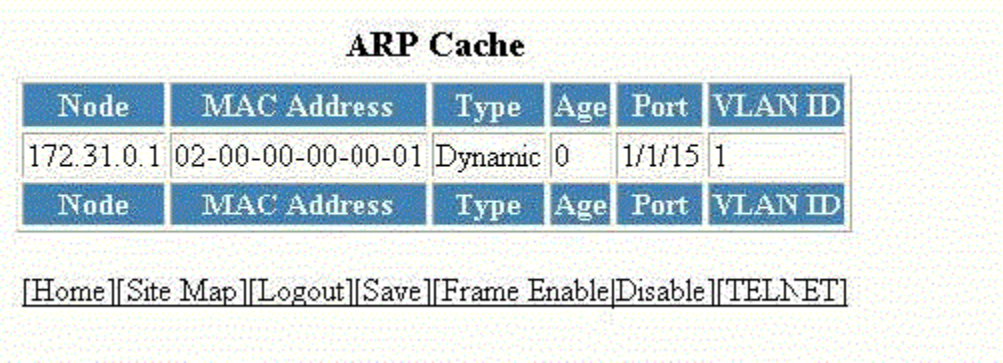


TABLE 2 Description of the fields in the ARP Cache window

Field	Description
Node	Displays the IP address of the device.
MAC Address	Displays the MAC address of the device.
Type	Displays the type of ARP entry, 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	Displays 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.

TABLE 2 Description of the fields in the ARP Cache window (continued)

Field	Description
Port	Displays 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. The port number for Ruckus ICX devices is stack-unit/slotnum/portnum
VLAN ID	Displays the VLAN Identifier of the port, which learned the entry.

Displaying the device information

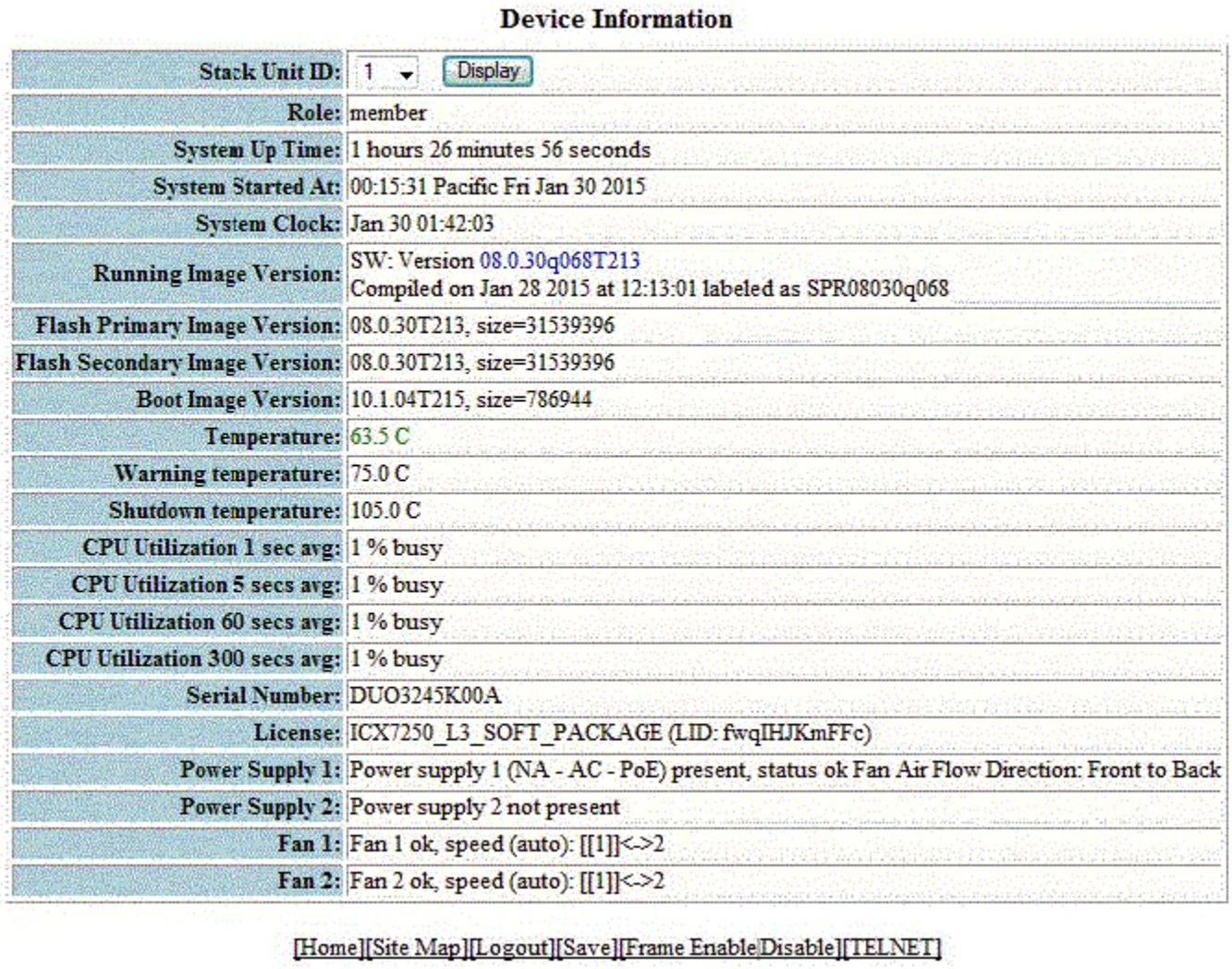
To display the device information, perform the following steps.

1. Click **Monitor** on the left pane and select **Device**.

2. Select a stack Identifier from the **Stack Unit ID** list and click **Display** to view the information for any device in an IronStack.

   The **Device Information** window is displayed as shown in the figure below.

FIGURE 7 Monitoring the device information



Device Information

Stack Unit ID:	1 Display
Role:	member
System Up Time:	1 hours 26 minutes 56 seconds
System Started At:	00:15:31 Pacific Fri Jan 30 2015
System Clock:	Jan 30 01:42:03
Running Image Version:	SW: Version 08.0.30q068T213 Compiled on Jan 28 2015 at 12:13:01 labeled as SPR08030q068
Flash Primary Image Version:	08.0.30T213, size=31539396
Flash Secondary Image Version:	08.0.30T213, size=31539396
Boot Image Version:	10.1.04T215, size=786944
Temperature:	63.5 C
Warning temperature:	75.0 C
Shutdown temperature:	105.0 C
CPU Utilization 1 sec avg:	1 % busy
CPU Utilization 5 secs avg:	1 % busy
CPU Utilization 60 secs avg:	1 % busy
CPU Utilization 300 secs avg:	1 % busy
Serial Number:	DUO3245K00A
License:	ICX7250_L3_SOFT_PACKAGE (LID: fwqIHJKmFFc)
Power Supply 1:	Power supply 1 (NA - AC - PoE) present, status ok Fan Air Flow Direction: Front to Back
Power Supply 2:	Power supply 2 not present
Fan 1:	Fan 1 ok, speed (auto): [[1]]<->2
Fan 2:	Fan 2 ok, speed (auto): [[1]]<->2

[Home][Site Map][Logout][Save][Frame Enable Disable][TELNET]

TABLE 3 Description of the fields in the Device Information window

Field	Description
Stack Unit ID	Displays the number of the unit within a stack.
Role	Displays the role of the device, which can be *Active*, *Standby*, *Member*, or *alone*. If the role is *alone*, the device is operating as a standalone device.
System Up Time	Displays the quantity of time the system has been running since the last restart.
System Started At	Displays the time when the system started.

TABLE 3 Description of the fields in the Device Information window (continued)

Field	Description
System Clock	Displays the time configured in the system.
Running Image Version	Displays the software version currently running and some details on the version.
Flash Primary Image Version	Displays the release number and size of the software loaded on the primary flash.
Flash Secondary Image Version	Displays the release number and size of the software loaded on the secondary flash.
Boot Image Version	Displays the release number and size of the boot image.
Temperature	This field displays 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.
Warning temperature	Displays the warning level temperature.
Shutdown temperature	Displays the shutdown level temperature.
CPU Utilization	Displays the percentage of CPU being used by the device at 1-second, 5-second, 1-minute, and 5-minute intervals.
Serial Number	Displays the serial number of the device.
License	Displays the software license and License ID (LID) of the device.
Power Supply 1	Displays the status of the primary power supply.
Power Supply 2	Displays the status of the secondary power supply, if present.
Fan 1	Displays the status of the primary cooling fan.
Fan 2	Displays the status of the secondary cooling fan, if present. **NOTE** There is an entry for each fan in the device.

NOTE
License details and serial number are not displayed for PE devices on an SPX stack.

Displaying flash information

To display the flash information, click **Monitor** on the left pane and select **Flash.**

The **Flash Information** window is displayed as shown in the figure below.

FIGURE 8 Monitoring the flash information



Flash Information

Unit ID	Compressed Pri Code		Compressed Sec Code		Compressed BootROM Code		Code Flash Free Space
	Size	Version	Size	Version	Size	Version	
1	8272492	(ICX64S08020q033.bin)	8295076	(ICX64S08020q042.bin)	786944	10.1.03T310	4587520
3	8272492	(ICX64S08020q033.bin)	8295076	(ICX64S08020q042.bin)	786944	10.1.03T310	6963200
4	8272492	08.0.20qT311(ICX64S08020q033.bin)	8295076	08.0.20qT311(ICX64S08020q042.bin)	786944	10.1.03T310	6881280
5	8272492	08.0.20qT311 (ICX64S08020q033.bin)	8295076	08.0.20qT311 (ICX64S08020q042.bin)	786944	10.1.03T310	6918144

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

The table below describes the fields in the **Flash Information** window.

TABLE 4 Description of the fields in the Flash Information window

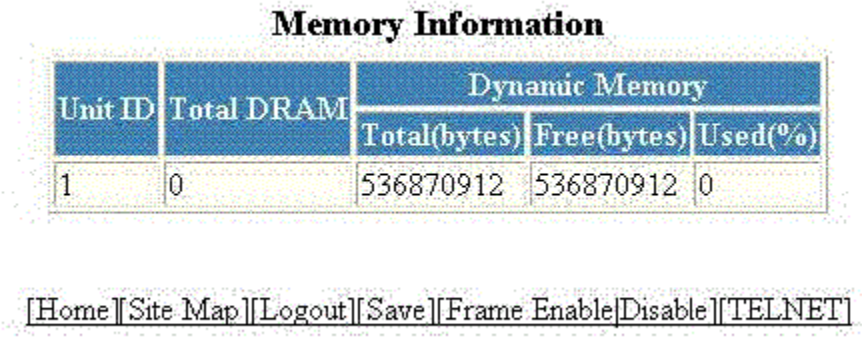
Field	Description
Unit ID	Displays the number of the unit within a stack.
Compressed Pri Code	Displays the compressed size and version for the primary code.
Compressed Sec Code	Displays the compressed size and version for the secondary code.
Compressed BootROM Code	Displays the compressed size and version for the BootROM code.
Code Flash Free Space	Displays the amount of free space available on the flash memory.

Displaying memory information

To display the memory information of the device, click **Monitor** on the left pane and select **Memory**.

The **Memory Information** window is displayed as shown in the figure below.

FIGURE 9 Monitoring the memory information



Memory Information

Unit ID	Total DRAM	Dynamic Memory		
		Total(bytes)	Free(bytes)	Used(%)
1	0	536870912	536870912	0

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

TABLE 5 Description of the fields in the Memory Information window

Field	Description
Unit ID	Displays the number of the unit within a stack.

TABLE 5 Description of the fields in the Memory Information window (continued)

Field	Description
Total DRAM	Displays the size (in bytes) of dynamic random access memory (DRAM).
Dynamic Memory	Displays 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.

Displaying the front panel

The front panel of the device allows you to view the modules in each device and the ports within each module.

The front panel shows the status of devices using colors. Green ports are connected, and gray ports are not connected. Ports of the same color on two units are connected with cables. A gray uplink port is not connected to a device. Ports with amber LEDs linked up have downgraded speeds from their default speeds.

NOTE
In 802.1BR system, the front panel display is supported only for CB units. PE units are not displayed in the front panel.

Status LED display

The status LEDs that appear on the front panel provide information about system activity. The figure below shows the LEDs that appear on the front panel of an ICX 7750 device.

FIGURE 10 Front panel LEDs



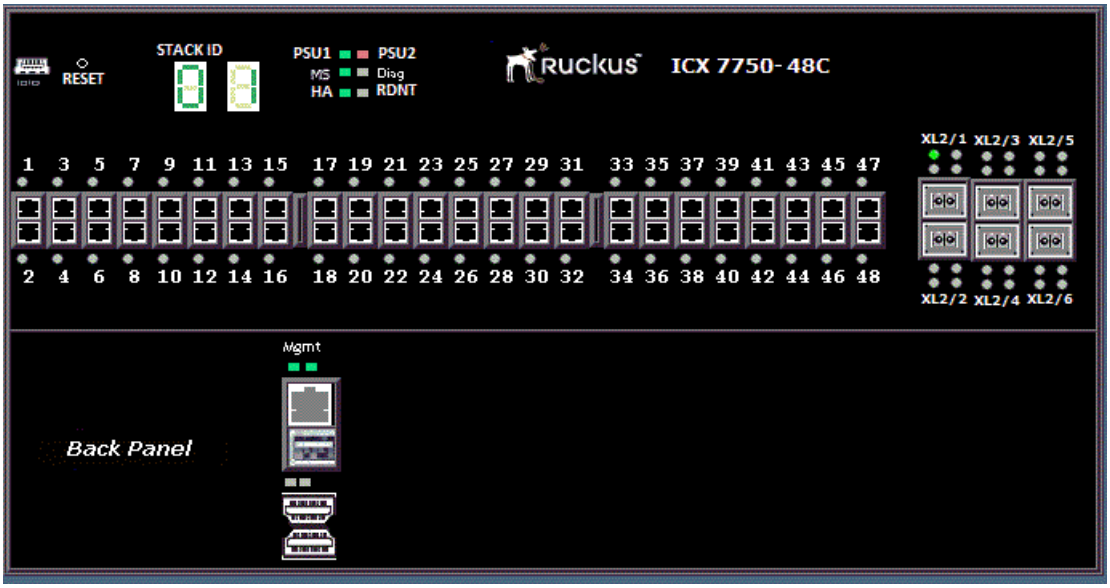
For more information about the LED labels and status indicators in Ruckus ICX devices, refer respective Hardware Installation Guides.

Displaying the front panel for the Ruckus ICX 7750 device

To display the front panel, click **Monitor** on the left panel and select **Front Panel**.

The figure below shows the front panel of the Ruckus ICX 7750 device.

FIGURE 11 Ruckus ICX 7750 device front panel

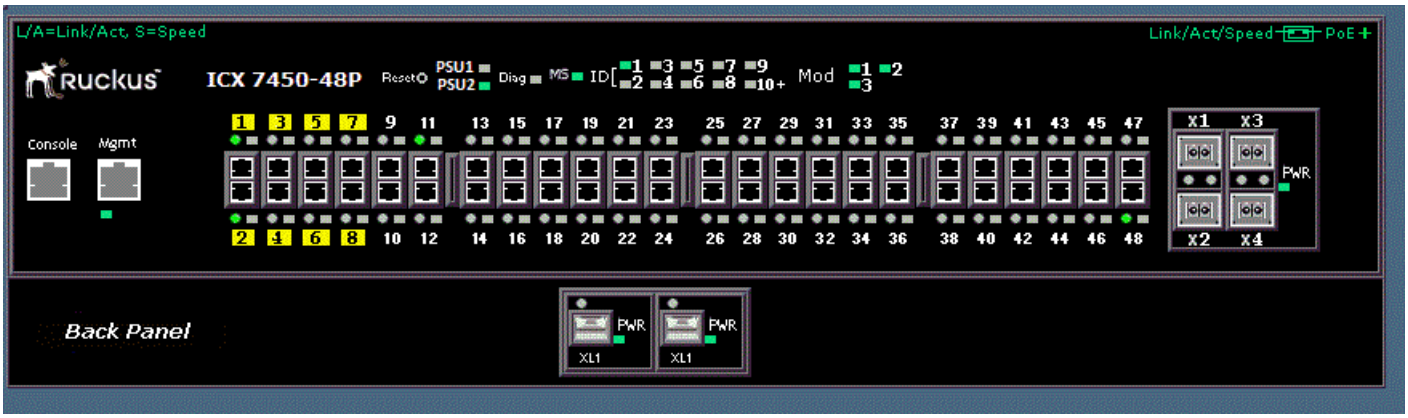


Displaying the front panel for the Ruckus ICX 7450 device

To display the front panel, click **Monitor** on the left panel and select **Front Panel**.

The figure below shows the front panel of the Ruckus ICX 7450 device.

FIGURE 12 Ruckus ICX 7450 device front panel

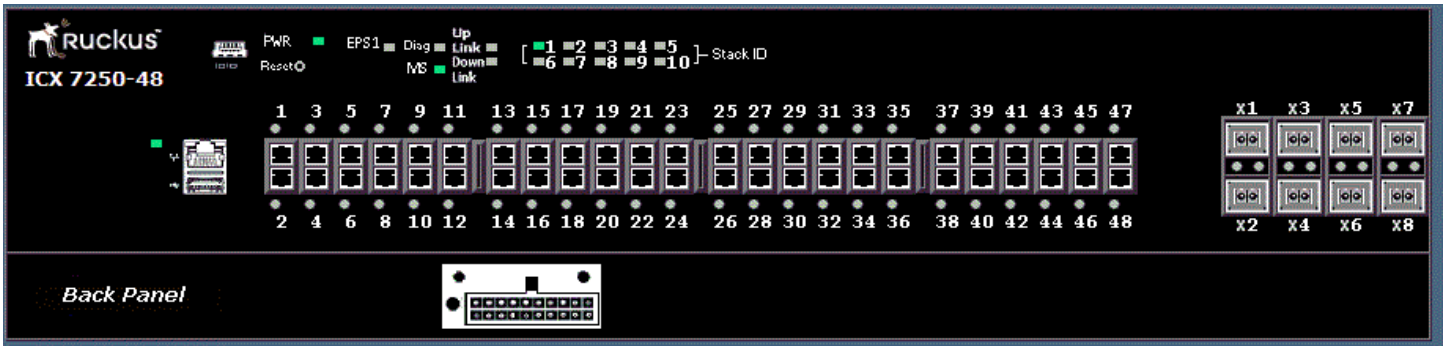


Displaying the front panel for the Ruckus ICX 7250 device

To display the front panel, click **Monitor** on the left panel and select **Front Panel**.

The figure below shows the front panel of the ICX 7250-48 device.

FIGURE 13 Ruckus ICX 7250 device front panel

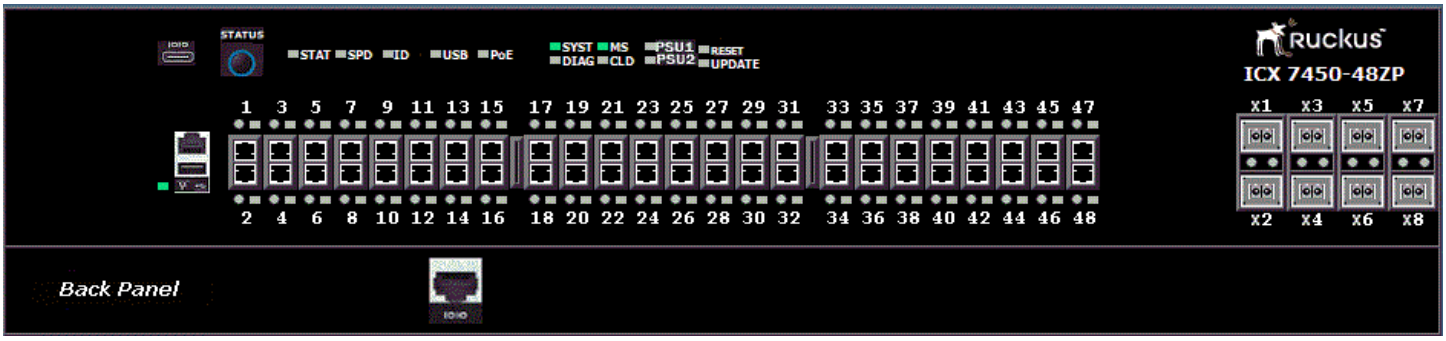


Displaying the front panel for the Ruckus ICX 7150

To display the front panel, click **Monitor** on the left panel and select **Front Panel**.

The figure below shows the front panel of the Ruckus ICX 7150-48ZP device.

FIGURE 14 Ruckus ICX 7150-48ZP device front panel

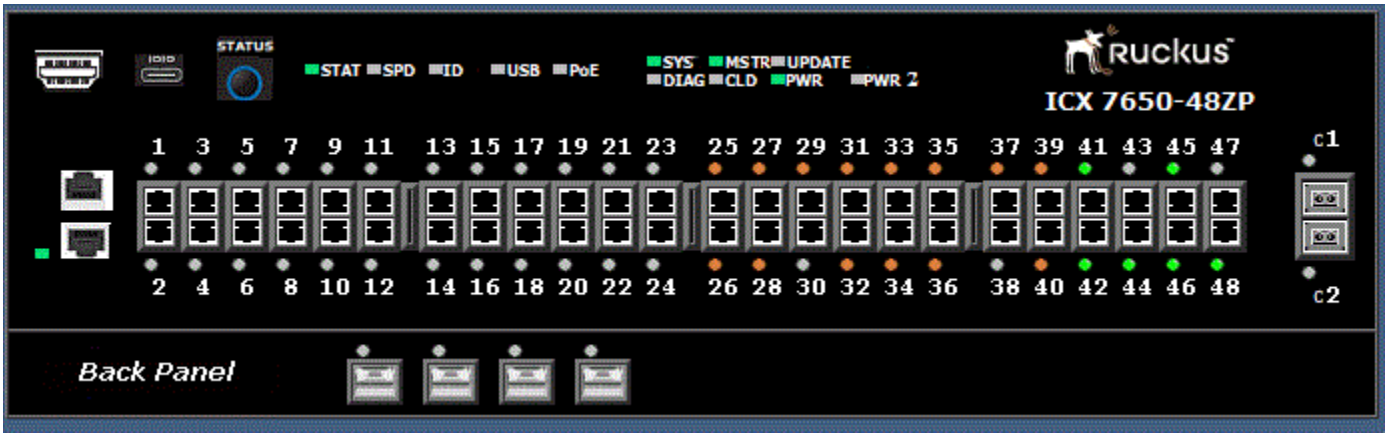


Displaying the front panel for the Ruckus ICX 7650

To display the front panel, click **Monitor** on the left panel and select **Front Panel**.

The figure below shows the front panel of the Ruckus ICX 7650-48ZP device.

FIGURE 15 Ruckus ICX 7650-48ZP device front panel



Displaying MAC addresses

To display the list of MAC addresses that have been learned by the device, click **Monitor** on the left pane and select **MAC Address**.

The **MAC Address** window is displayed as shown in the figure below.

FIGURE 16 Monitoring the MAC address

MAC Address

MAC Address	Port	Type	Index	VLAN
74-8e-f8-40-fc-8f	5/1/15	Dynamic	1722	1
cc-4e-24-07-b0-d3	5/1/24	Dynamic	60968	1
74-8e-f8-ea-05-ab	5/1/4	Dynamic	43573	1
74-8e-f8-ed-8e-f1	5/1/15	Dynamic	35542	1
MAC Address	Port	Type	Index	VLAN

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

The table below describes the fields in the **MAC Address** window.

TABLE 6 Description of the fields in the MAC Address window

Field	Description
MAC Address	Displays the MAC address of the device.
Port	Displays 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.

TABLE 6 Description of the fields in the MAC Address window (continued)

Field	Description
Type	Displays the type of the entry, 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.
Index	Displays the index of the entry in the MAC address table.
VLAN	Displays 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.

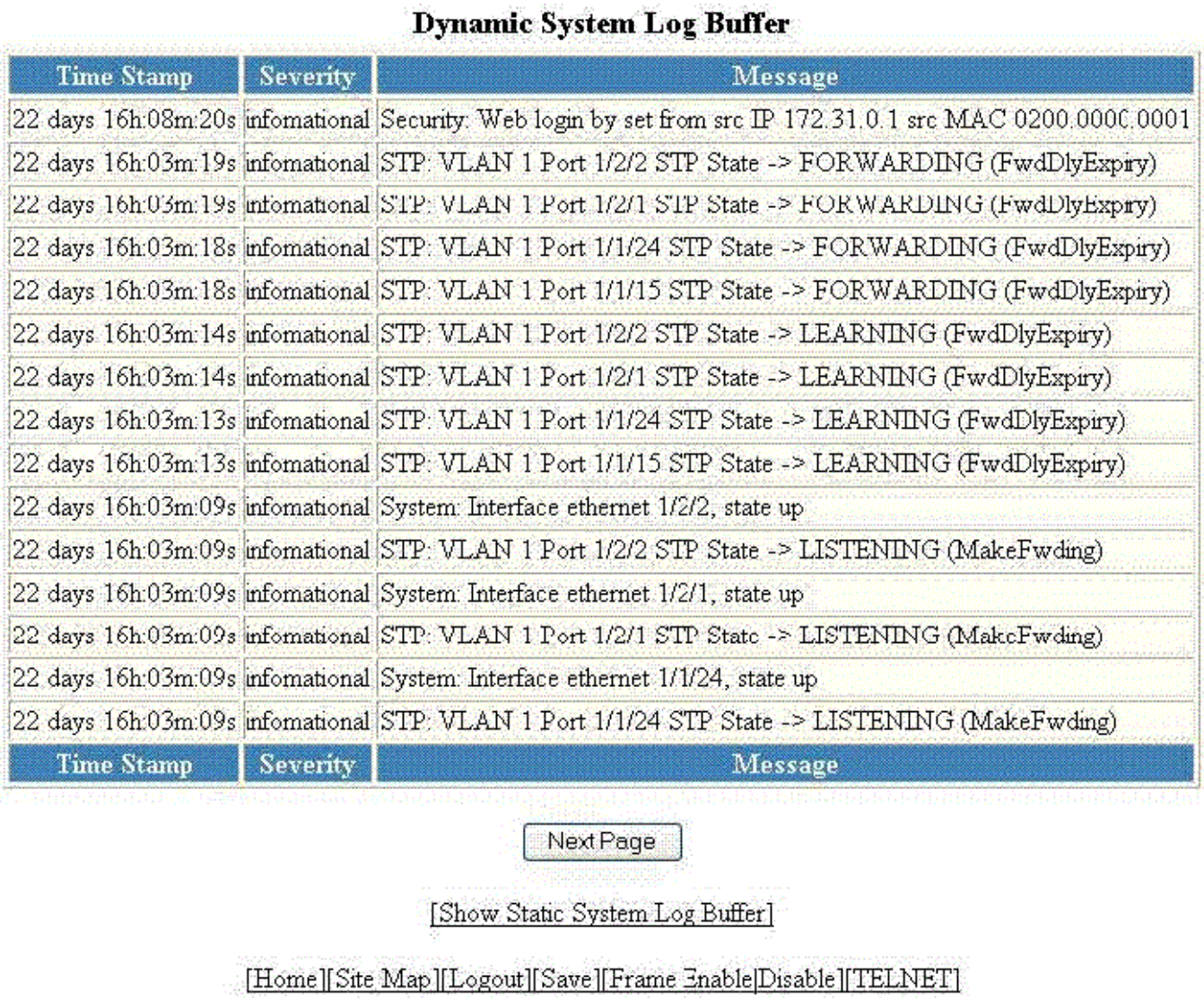
Displaying the system log

The software provides two types of system log buffers:

- Static—Logs power supply failures, fan failures, and temperature warning or shutdown messages.
- Dynamic—Logs all other message types.

To display the current information of the system log buffer, click **Monitor** on the left pane and select **System Log**.

The **Dynamic System Log Buffer** window is displayed as shown in the figure below.



Dynamic System Log Buffer

Time Stamp	Severity	Message
22 days 16h:08m:20s	infomational	Security: Web login by set from src IP 172.31.0.1 src MAC 0200.0000.0001
22 days 16h:03m:19s	infomational	STP: VLAN 1 Port 1/2/2 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:19s	infomational	STP: VLAN 1 Port 1/2/1 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:18s	infomational	STP: VLAN 1 Port 1/1/24 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:18s	infomational	STP: VLAN 1 Port 1/1/15 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:14s	infomational	STP: VLAN 1 Port 1/2/2 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:14s	infomational	STP: VLAN 1 Port 1/2/1 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:13s	infomational	STP: VLAN 1 Port 1/1/24 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:13s	infomational	STP: VLAN 1 Port 1/1/15 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:09s	infomational	System: Interface ethernet 1/2/2, state up
22 days 16h:03m:09s	infomational	STP: VLAN 1 Port 1/2/2 STP State -> LISTENING (MakeFwding)
22 days 16h:03m:09s	infomational	System: Interface ethernet 1/2/1, state up
22 days 16h:03m:09s	infomational	STP: VLAN 1 Port 1/2/1 STP State -> LISTENING (MakeFwding)
22 days 16h:03m:09s	infomational	System: Interface ethernet 1/1/24, state up
22 days 16h:03m:09s	infomational	STP: VLAN 1 Port 1/1/24 STP State -> LISTENING (MakeFwding)
Time Stamp	Severity	Message

The table below describes the fields in the **Dynamic System Log Buffer** window.

TABLE 7 Description of the fields in the Dynamic System Log Buffer window

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

To view the next set of the **Dynamic System Log Buffer** entries, click **Next Page**. To display the static system log buffer information, click **Show Static System Log Buffer**.

The **Static System Log Buffer** window is displayed as shown in the figure below.

Static System Log Buffer

Time Stamp	Severity	Message
00 days 00h:00m:21s	alert	System: Fan 1 (bottom row, leftmost), failed
00 days 00h:00m:21s	alert	System: Fan 2 (bottom row, middle), failed
00 days 00h:00m:21s	alert	System: Fan 3 (bottom row, rightmost), failed
00 days 00h:00m:21s	alert	System: Fan 4 (top row, leftmost), failed
00 days 00h:00m:21s	alert	System: Fan 5 (top row, middle), failed
00 days 00h:00m:21s	alert	System: Fan 6 (top row, rightmost), failed
Time Stamp	Severity	Message

[Show Dynamic System Log Buffer]

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

For information on the **Static System Log Buffer** fields, refer to the table above.

Monitoring Stacks

- Displaying the stack details....33
- Displaying a stack module....35
- Displaying stack neighbors....35
- Displaying stack ports information....36
- Displaying stack port statistics....37
- Displaying stack port interfaces....38

Displaying the stack details

To display current stack details, stack port status, and stack neighbors information, perform the following steps.

NOTE
Stacking is not supported on ICX 7150 device.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Details**.

   The **Stack Details** window is displayed in the figure below.

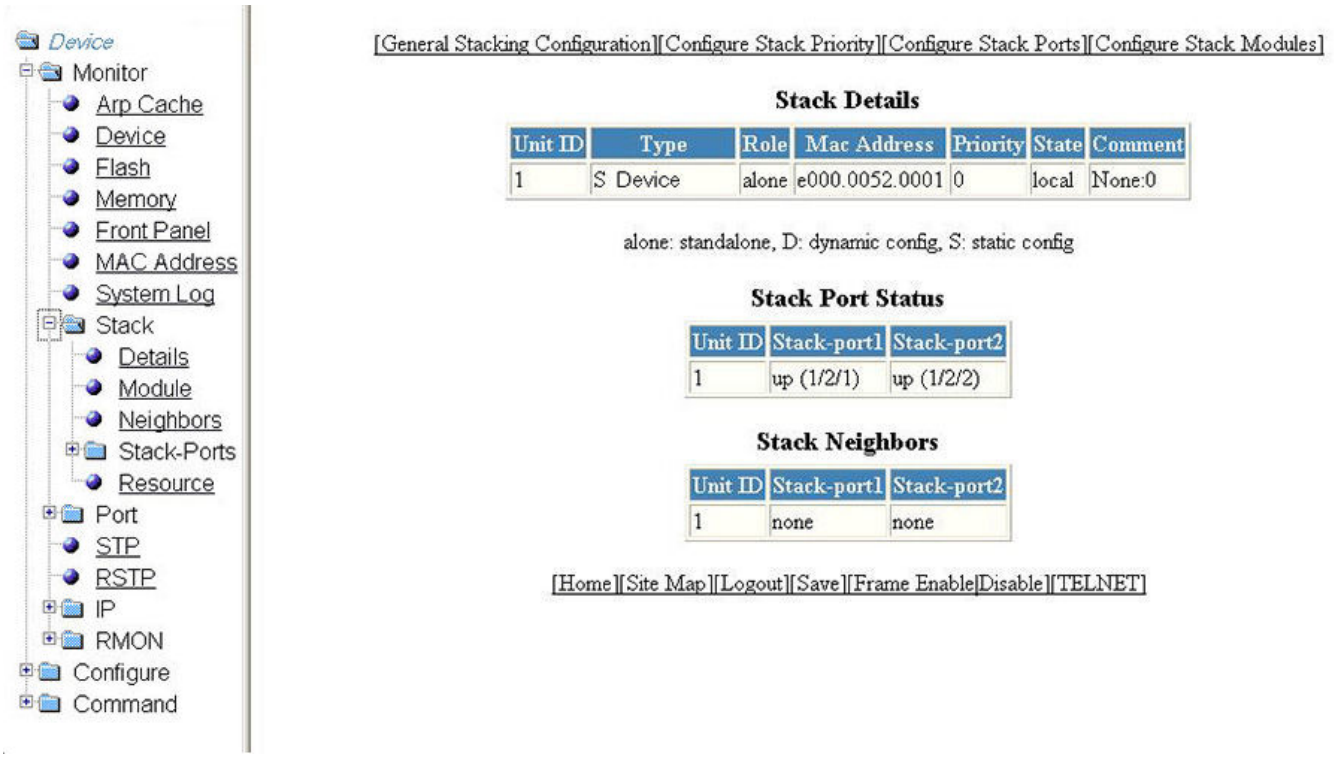


TABLE 8 Description of the fields in the Stack Details window

Field	Description
Stack Details parameters	

TABLE 8 Description of the fields in the Stack Details window (continued)

Field	Description
Unit ID	Displays the number of the unit within a stack.
Type	Displays the type of configuration and the device model. The types of configuration are as follows: • *alone* --Indicates that the device is operating as a standalone device. • *S* --Indicates that the configuration for this unit is static. • *D* --Indicates that the configuration for this unit is dynamic and may be overwritten by a new stack unit.
Role	Displays the role of this unit within the stack: *Active*, *Standby*, *Member*, or *alone*.
Mac Address	Displays the MAC address of the device.
Priority	Displays the priority assigned to this unit.
State	Displays the operational state of this unit: *local* or *remote*.
Comment	Displays additional information about this unit.
Stack Port Status parameters	
Unit ID	Displays the number of the unit within a stack.
Stack-port1	Displays the port state and the port number for stack-port1. The port states are as follows: • *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	Displays the port state and the port number for stack-port2. The port states are as follows: • *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 Neighbors parameters	
Unit ID	Displays the number of the unit within a stack.
Stack-port1	Displays the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Displays the neighbor stack unit for stack-port2 for this unit ID.

The **Stack Details** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To view the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to Viewing stack priority details on page 94.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to the “Modifying stack ports” section.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to the “Configuring a stack module” section.

Displaying a stack module

To display current information about the stack unit modules, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Module**.

   The **Stack Modules** window is displayed as shown in the figure below.

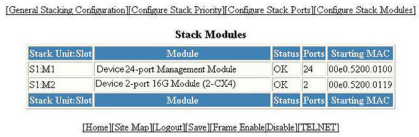


TABLE 9 Description of the fields in the Stack Modules window

Field	Description
Stack Unit: Slot	Displays the number of the unit within the stack and the slot number.
Module	Displays the device information, such as module number and module type.
Status	Displays the status, which can be one of the following: • *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	Displays the number of ports on the module.
Starting MAC	Displays the starting MAC address for this module.

The **Stack Modules** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to the "Modifying a stack priority" section.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to the "Modifying stack ports" section.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to the "Configuring Stack Components" section.

Displaying stack neighbors

To display information of the stack member neighbors, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.

2. Click **Neighbors**.

   The **Stack Neighbors** window is displayed as shown in the figure below.

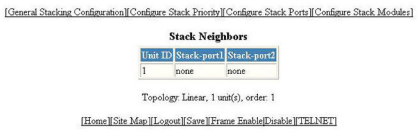


TABLE 10 Description of the fields in the Stack Neighbors window

Field	Description
Unit ID	Displays the number of the unit within the stack.
Stack-port1	Displays the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Displays the neighbor stack unit for stack-port2 for this unit ID.
Topology	Displays either *Linear* or *Ring* stack topology of the connected devices.
unit(s)	Displays the number of units within the stack.
order	Displays the order of the unit IDs within the stack.

The **Stack Neighbors** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration** . For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To configure the priority of units within a stack, click **Configure Stack Priority** . For more information, refer to the “Modifying a stack priority” section.
- To configure a stack port, click **Configure Stack Ports** . For more information, refer to the “Modifying stack ports” section.
- To configure a stack module, click **Configure Stack Modules** . For more information, refer to “Configuring a stack module” section.

Displaying stack ports information

To display the information of the stack ports, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack** .

2. Click **Stack-Ports** and then select **Status** .

   The **Stack Port Status** window is displayed as shown in the figure below.

FIGURE 17 Monitoring stack port status

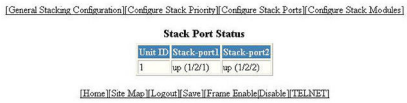


TABLE 11 Description of the fields in the Stack Port Status window

Field	Description
Unit ID	Displays the number of the unit within the stack.
Stack-port1	Displays the port state and the port number for stack-port1 for this unit ID. The port states are as follows: • *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	Displays the port state and the port number for stack-port2 for this unit ID. The 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 Port Status** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration** . For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To view the priority of units within a stack, click **Configure Stack Priority** . For more information, refer to Viewing stack priority details on page 94.
- To configure a stack port, click **Configure Stack Ports** . For more information, refer to Modifying stack ports on page 94.
- To configure a stack module, click **Configure Stack Modules** . For more information, refer to Configuring a stack module on page 96.

Displaying stack port statistics

To display stack port information for all ports in an IronStack topology, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack** .

2. Click **Stack-Ports** and then select **Statistics** .

   The **Stack Port Statistics** window is displayed as shown in the figure below.

FIGURE 18 Monitoring stack port statistics

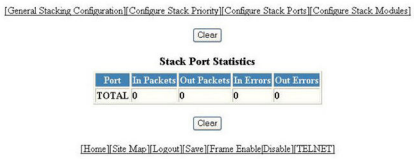


TABLE 12 Description of the fields in the Stack Port Statistics window

Field	Description
Port	Displays the stack identification number for this port.
In Packets	Displays the number of incoming packets on this port.
Out Packets	Displays the number of outgoing packets on this port.
In Errors	Displays the number of errors on the incoming packets on this port.
Out Errors	Displays the number of errors on the outgoing packets on this port.

To clear the information and begin a new monitoring cycle, click **Clear** . The **Stack Port Statistics** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration** . For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To view the priority of units within a stack, click **Configure Stack Priority** . For more information, refer to Viewing stack priority details on page 94.
- To configure a stack port, click **Configure Stack Ports** . For more information, refer to Modifying stack ports on page 94.
- To configure a stack module, click **Configure Stack Modules** . For more information, refer to Configuring a stack module on page 96.

Displaying stack port interfaces

To display information about stack port interfaces, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack** .

2. Click **Stack-Ports** and then select **Interface** .

   The **Stack Port Interface** window is displayed as shown in the figure below.

FIGURE 19 Monitoring stack port interfaces

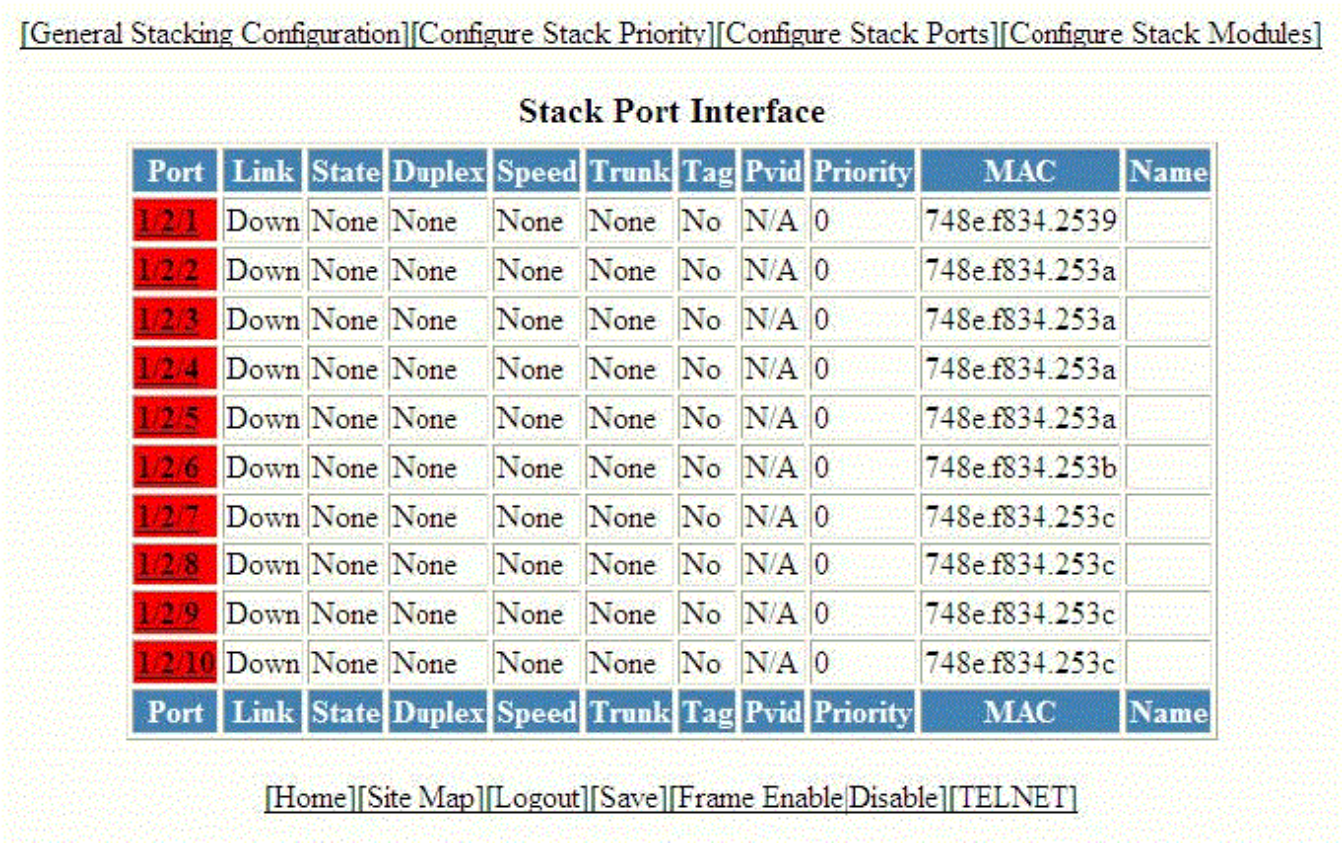


TABLE 13 Description of the fields in the Stack Port Interface window

Field	Description
Port	Displays the stack identification number for this port.
Link	Displays whether the link is up or down.
State	Displays the state of the stack unit.
Duplex	Displays whether the port is configured as half or full duplex.
Speed	Displays the port speed as 10 Mbps, 100 Mbps, or 1000 Mbps.
Trunk	Displays the trunk group number, if the port is a member of a trunk group.
Tag	Displays whether the port is tagged or untagged.
Priority	Displays the port priority.
MAC	Displays the MAC address of the port.
Name	Displays the name assigned to the port.

The **Stack Port Interface** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration** . For more information, refer to Configuring the general settings for a traditional stack on page 93.
- To view the priority of units within a stack, click **Configure Stack Priority** . For more information, refer to Viewing stack priority details on page 94.
- To configure a stack port, click **Configure Stack Ports** . For more information, refer to Modifying stack ports on page 94 .
- To configure a stack module, click **Configure Stack Modules** . For more information, refer to Configuring a stack module on page 96.

Monitoring Ports

- Displaying Ethernet port statistics..... 41
- Displaying Ethernet port attributes.....44
- Displaying Ethernet port utilization..... 47
- Displaying the management port information.....49
- Displaying port inline power for Ruckus ICX devices..... 52

Displaying Ethernet port statistics

The **ETHERNET Port Statistic** window lists the total number of packets, number of collisions, and number of errors that have occurred on a port. To display the Ethernet port statistics, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Statistic** and then select **Ethernet**.

   The **ETHERNET Port Statistic** window is displayed as shown in the figure below.

3. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

[ETHERNET Port Configuration][ETHERNET Port Attribute][ETHERNET Port Utilization][RMON ETHERNET Statistics|Error|History]

Select Stack Unit ID: 1 Display

Clear Stop Polling Change Polling Interval

ETHERNET Port Statistic - Polling Interval 30 sec

Port	Total Pkts		Collision		Error			
	Rx	Tx	Rx	Tx	Align	FCS	Giant	Short
1/1/1	0	0	0	0	0	0	0	0
1/1/2	0	0	0	0	0	0	0	0
1/1/3	0	0	0	0	0	0	0	0
1/1/4	0	0	0	0	0	0	0	0
1/1/5	0	0	0	0	0	0	0	0
1/1/6	0	0	0	0	0	0	0	0
1/1/7	0	0	0	0	0	0	0	0
1/1/8	0	0	0	0	0	0	0	0
1/1/9	0	0	0	0	0	0	0	0
1/1/10	0	0	0	0	0	0	0	0
1/1/11	0	0	0	0	0	0	0	0
1/1/12	0	0	0	0	0	0	0	0
1/1/13	0	0	0	0	0	0	0	0
1/1/14	0	0	0	0	0	0	0	0
1/1/15	368	595	0	0	0	0	0	0
1/1/16	0	0	0	0	0	0	0	0
1/1/17	0	0	0	0	0	0	0	0
1/1/18	0	0	0	0	0	0	0	0
1/1/19	0	0	0	0	0	0	0	0
1/1/20	0	0	0	0	0	0	0	0
1/1/21	0	0	0	0	0	0	0	0
1/1/22	0	0	0	0	0	0	0	0
1/1/23	0	0	0	0	0	0	0	0
1/1/24	0	2779	0	0	0	0	0	0
1/2/1	0	0	0	0	0	0	0	0
1/2/2	0	0	0	0	0	0	0	0
Port	Total Pkts		Collision		Error			
	Rx	Tx	Rx	Tx	Align	FCS	Giant	Short

Up Time=22 days 17h:22m:37s, Last Clear Time=22 days 16h:03m:09s

Clear Stop Polling Change Polling Interval

[ETHERNET Port Configuration][ETHERNET Port Attribute][ETHERNET Port Utilization][RMON ETHERNET Statistics|Error|History]

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

TABLE 14 Description of the fields in the ETHERNET Port Statistic window

Field	Description
Port	Displays the port number for which the statistics were collected.
Total Packets	Displays the total number of packets received (**Rx**) and transmitted (**Tx**) on the port.
Collision	Shows the number of received (**Rx**) and transmitted (**Tx**) collisions on the port.
Error	Displays the number of errors on the port for the following types: • *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.

To remove the current data and restart the monitoring process, click **Clear**. To stop the polling process, click **Stop Polling.** You can also change the current polling interval by clicking **Change Polling Interval**.

The **ETHERNET Port Statistic** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to the "Configuring an Ethernet port" section.
- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to the "Displaying Ethernet port attributes" section.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to the "Displaying Ethernet port utilization" section.
- To monitor Remote Monitoring (RMON) Ethernet statistics, click **RMON ETHERNET Statistics Error**. For more information, refer to the "Displaying RMON Ethernet statistics" section.
- To monitor RMON history, click **RMON ETHERNET Statistics History**. For more information, refer to the "Displaying RMON history" section.

Displaying Ethernet port attributes

The **Port Attributes** window lists the number, state, media, connector, and MAC address of the port. To display the Ethernet port attribute information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port** .
2. Click **Statistic** and then select **Ethernet** .
3. Click **ETHERNET Port Attribute** on the **ETHERNET Port Statistic** window.

4. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

   The **Port Attributes** window is displayed as shown in the figure below.

FIGURE 20 Monitoring Ethernet port attributes

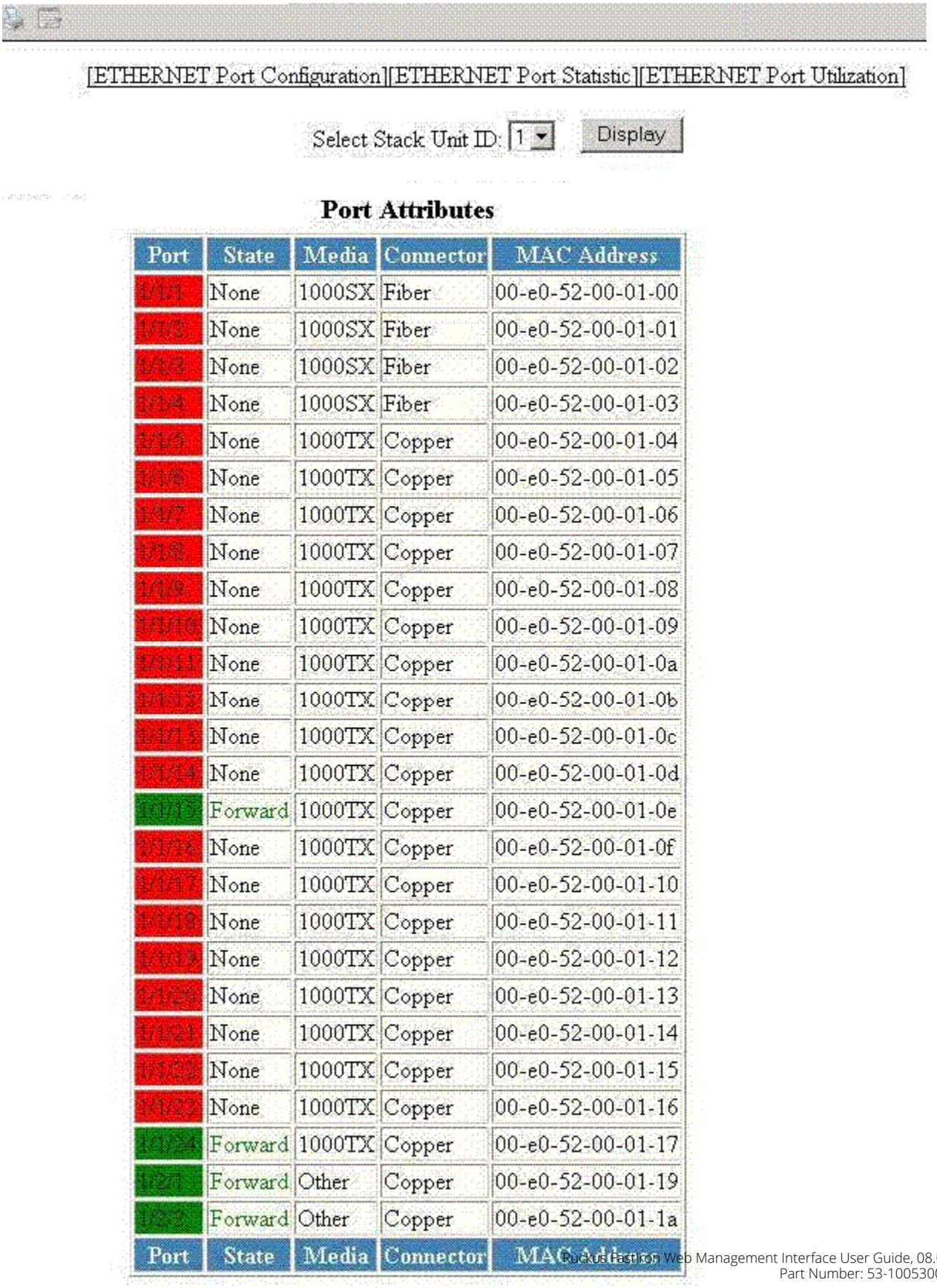


TABLE 15 Description of the fields in the Port Attributes window

Field	Description
Port	Displays the port number.
State	Displays the status of the port.
Media	Displays the type of the Ethernet cable used.
Connector	Displays the physical type of connector.
MAC Address	Displays the Media Access Control (MAC) address of the port.

The **Port Attributes** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration** . For more information on how to configure an Ethernet port, refer to Configuring an Ethernet port on page 135.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic** . For more information, refer to Displaying Ethernet port statistics on page 41.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization** . For more information, refer to Displaying Ethernet port utilization on page 47.

Displaying Ethernet port utilization

The **ETHERNET Port Utilization** window lists the traffic that is received and transmitted on a port. To display the Ethernet port utilization information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Utilization** and then select **Ethernet**.

   The **ETHERNET Port Utilization** window is displayed as shown in the figure below.

3. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

FIGURE 21 Ethernet port utilization

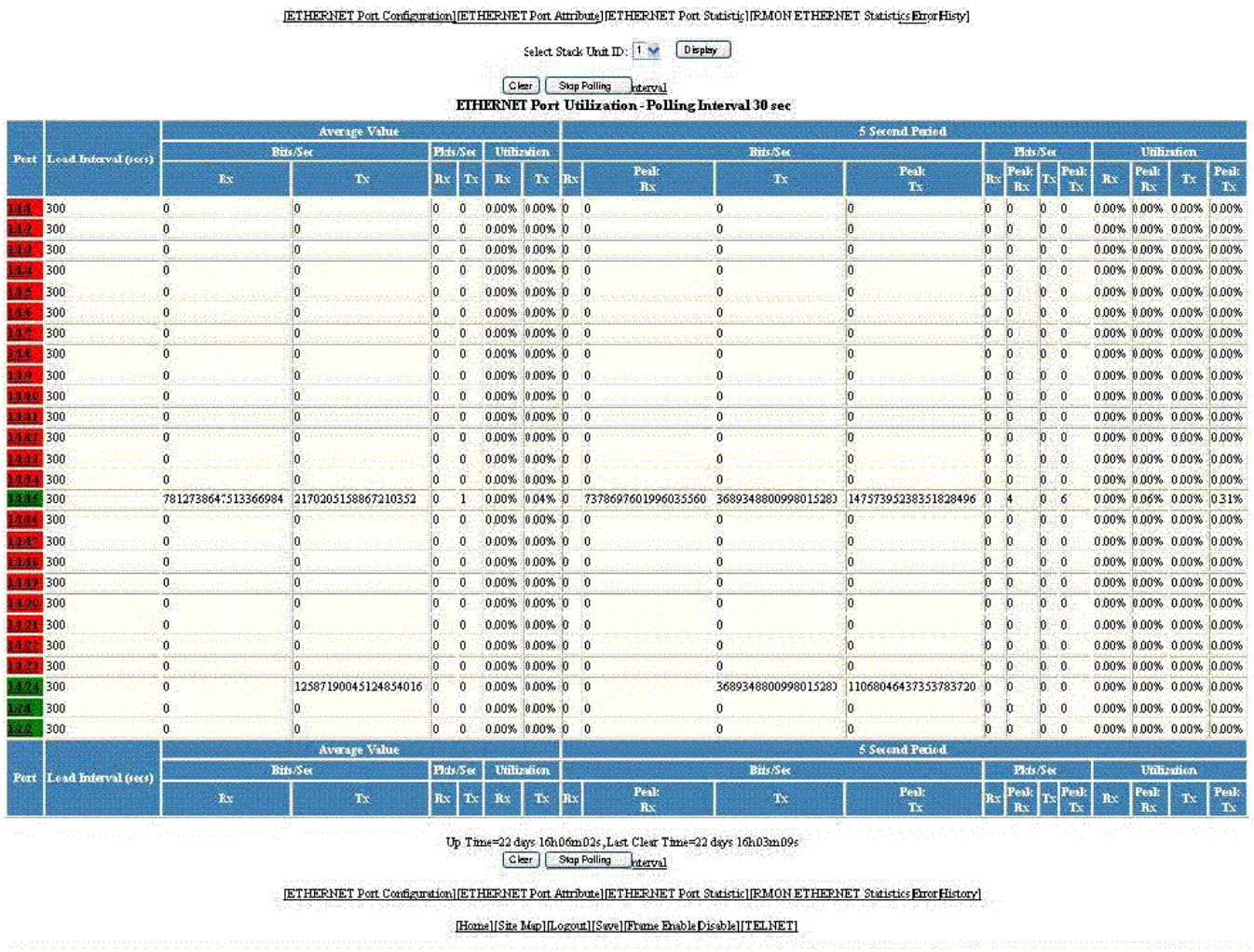


TABLE 16 Description of the fields in the ETHERNET Port Utilization window

Field	Description
Port	Displays the port number. Each entry has a link to detailed information about the port.
Load Interval (secs)	Displays the number of seconds for which average port utilization should be calculated. This object can have a value from 30 through 300, in 30-second increments. The default value is 300 seconds.
Average Value	Displays the following information: • *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.

TABLE 16 Description of the fields in the ETHERNET Port Utilization window (continued)

Field	Description
5 Second Period	This set of columns show the number of bits per second (**Bits/Sec**), number of packets per second (**Pkts/Sec**), and utilization percentages (**Utilization**) received and transmitted on a port at each 5-second interval. Peak activities for each category are also provided.

To remove the current data and restart the monitoring process, click **Clear** . To stop the statistics polling process, click **Stop Polling.** You can also change the current polling interval by clicking **Change Polling Interval** .

The **ETHERNET Port Utilization** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to Configuring an Ethernet port on page 135.
- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to the "Displaying Ethernet port attributes" section.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to the "Displaying Ethernet port statistics" section.
- To monitor Remote Monitoring (RMON) statistics, click **RMON ETHERNET Statistics Error**. For more information, refer to the "Displaying RMON Ethernet statistics" section.
- To monitor RMON history, click **RMON ETHERNET Statistics History** . For more information, refer to the "Displaying RMON history" section.

Displaying the management port information

To display the current management port configuration information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.

2. Click **Management**.

   The **Management Port Configuration** window is displayed as shown in the figure below.

FIGURE 22 Management port configuration

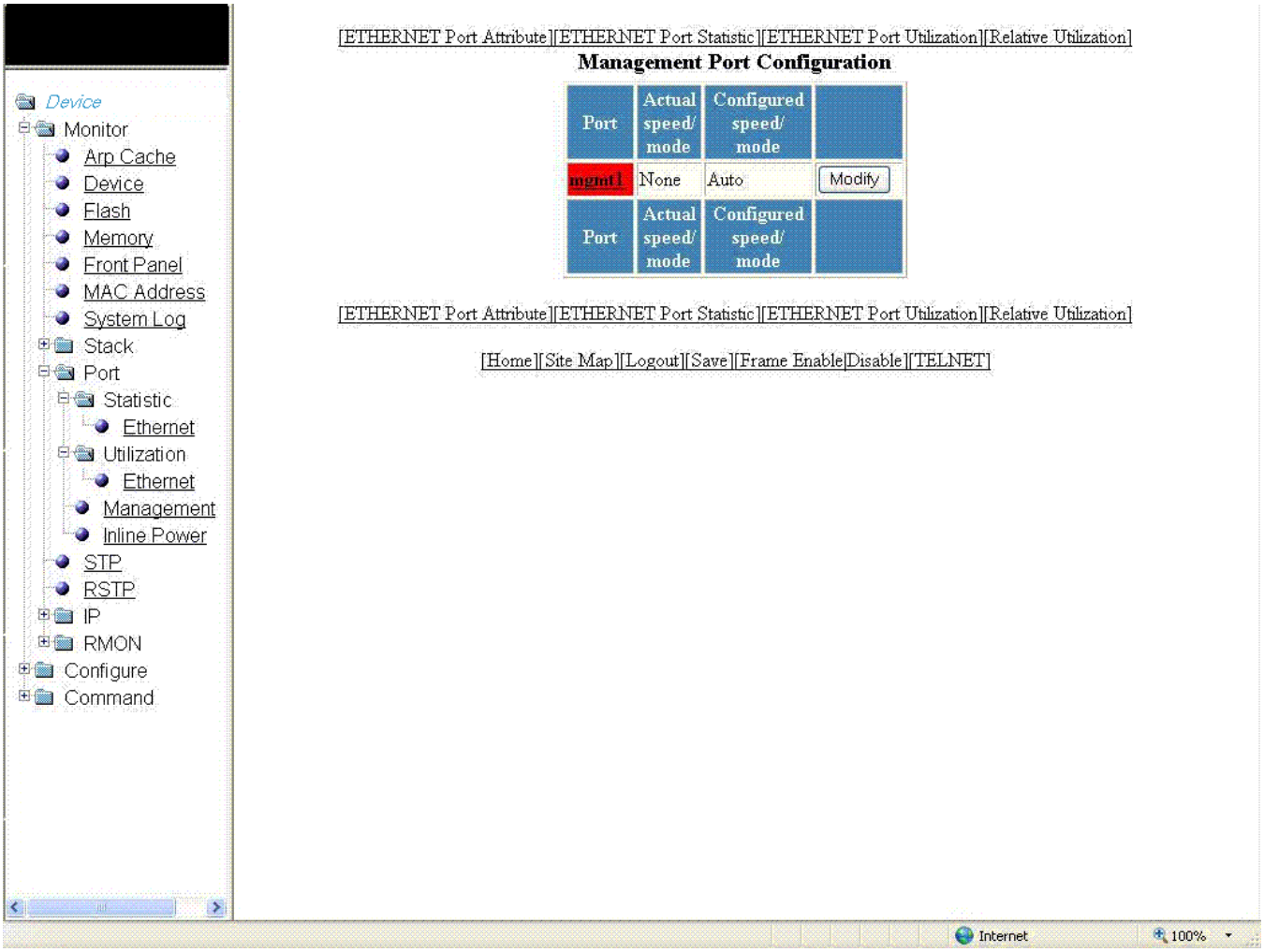


TABLE 17 Description of the fields in the Management Port Configuration window

Field	Description
Port	Displays the name of the management port. Each entry has a link to detailed real-time information about the port. Refer to the "Displaying the management port real-time information" section.
Actual speed/mode	Shows whether the actual speed matches the configured speed. If the configured speed is set to *Auto*, then the speed is set by the software.
Configured speed/mode	The speed duplex set for the port.

To configure a management port or change the configuration of a current management port, click **Modify**. For more information, refer to the "Configuring a management port" section.

The **Management Port Configuration** window provides links to configure the port parameters:

- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to the "Displaying Ethernet port attributes" section.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to the "Displaying Ethernet port statistics" section.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to the "Displaying Ethernet port utilization" section.
- To configure the port uplink utilization list, click **Relative Utilization**. For more information, refer to the "Configuring the port uplink relative utilization" section.

Displaying the management port real-time information

To display the real-time information of a port, click on the management port (for example, **mgmt1**).

The **Port Realtime Information** window is displayed as shown in the figure below.

FIGURE 23 Monitoring management port real-time information

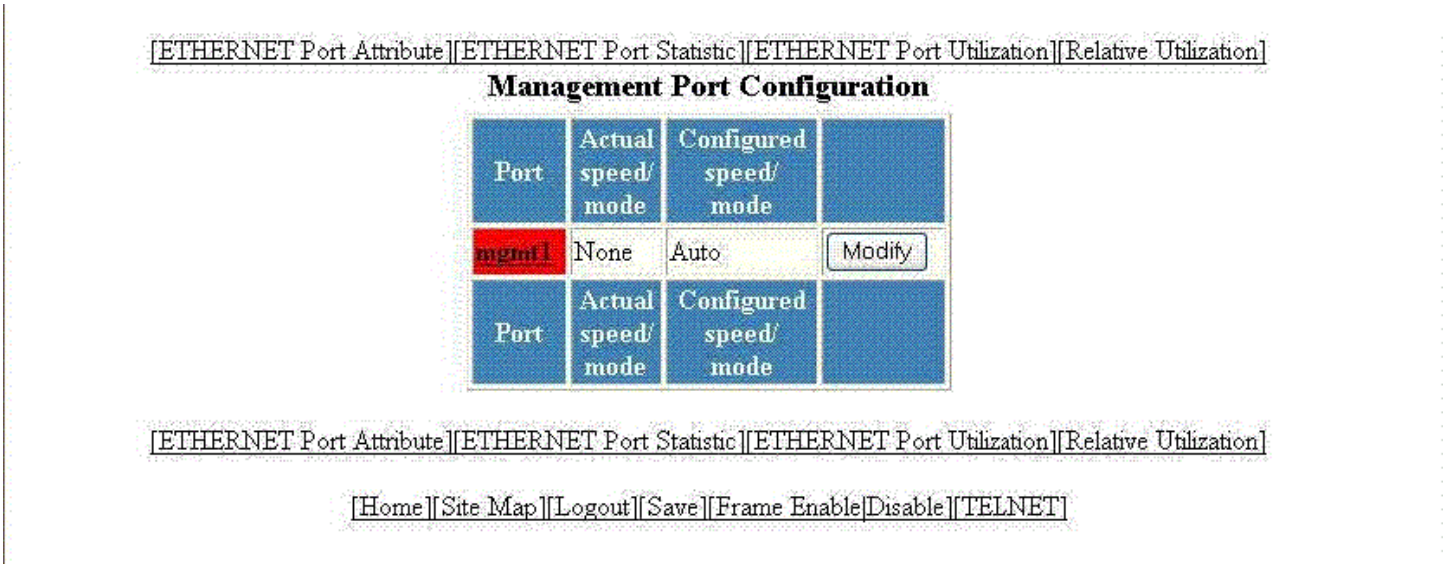


TABLE 18 Description of the fields in the Port Realtime Information window

Field	Description
Status	Displays the status of the port.
MAC Address	Displays 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 set by the software.
Connector	Displays the physical type of connector.

The **Port Realtime Information** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to the "Configuring an Ethernet port" section.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to the "Displaying Ethernet port statistics" section.

- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to the “Displaying Ethernet port utilization” section .

Displaying port inline power for Ruckus ICX devices

The port inline power statistics allow you to monitor Power over Ethernet (PoE), the ability to transfer electrical power and data to remote devices over standard twisted-pair cable in an Ethernet network. To display the inline power statistics for a PoE stack device, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Inline Power**.

   The port inline power window is displayed.
3. Select a unit ID in the **Select Stack POE Unit ID** list and click either **Inline Power Statistics** or **Inline Power Details**.

   NOTE
   Only PoE-capable units are displayed in the **Select Stack POE Unit ID** list. If there are no PoE units, you will receive `No units with POE modules` as an error message.

Displaying inline power details

To display the inline power details, select the unit ID in the **Select Stack POE Unit ID** list and click **Inline Power Details** .

The **Inline Power Details** window is displayed as shown in the figure below.

FIGURE 24 Monitoring inline power details

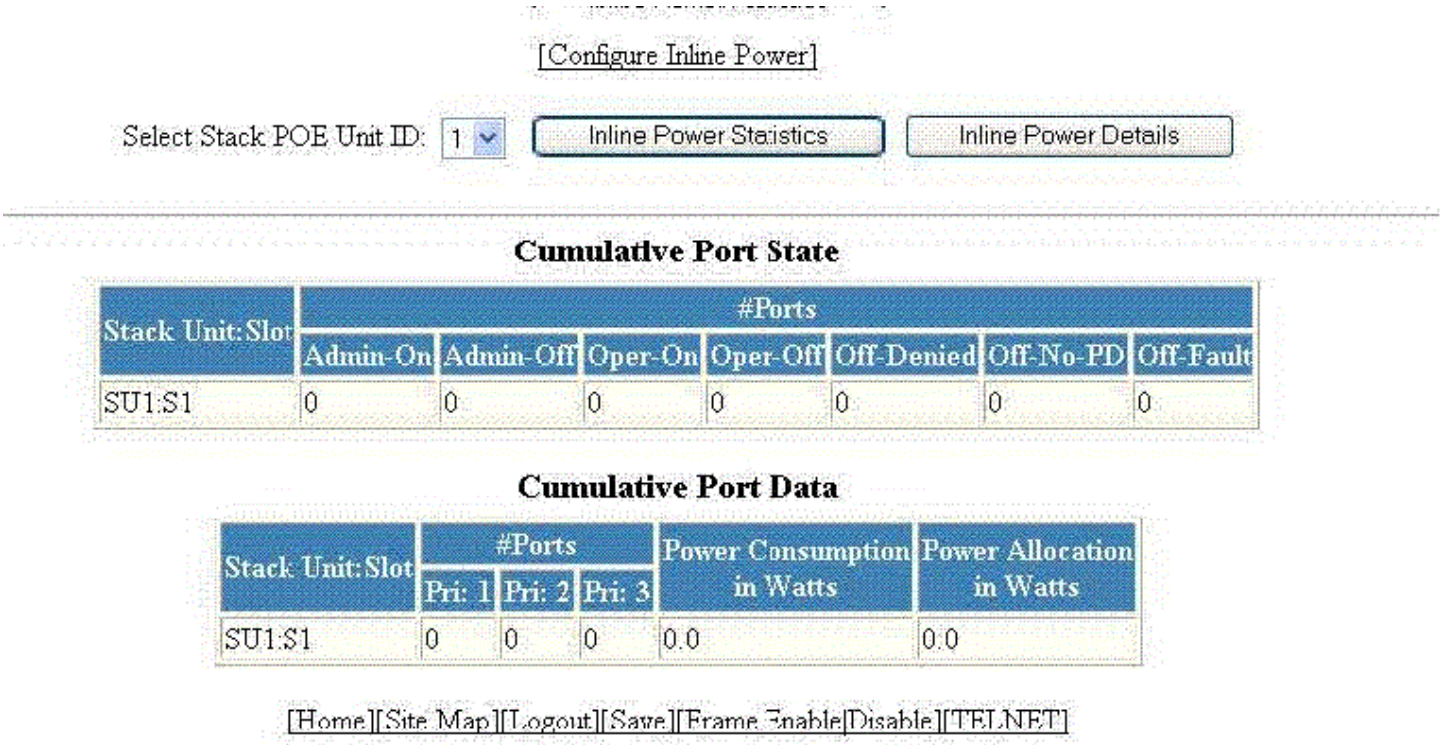


TABLE 19 Description of the fields in the Inline Power Details window

Field	Description
Cumulative Port State parameters	
Stack Unit: Slot	Displays the stack ID and slot ID (1 or 2). The PoE-capable slots are available on PoE stack units.
# Ports Admin-On	Displays the number of ports on the interface module on which the inline power was configured.
# Ports Admin-Off	Displays the number of ports on the interface module on which the inline power was not configured.
# Port Oper-On	Displays the number of ports on the interface module that are receiving inline power from the PoE power supply.
# Port Oper-Off	Displays the number of ports on the interface module that are not receiving inline power from the PoE power supply.
# Ports Off-Denied	Displays the number of ports on the interface module that were denied power because of insufficient power.
# Ports Off No-PD	Displays the number of ports on the interface module to which no powered devices (PDs) are connected.
# Ports Off-Fault	Displays the number of ports on the interface module that are not receiving power because of a subscription overload.
Cumulative Port Data parameters	
Stack Unit: Slot	Displays the stack ID and slot ID (1 or 2). The PoE-capable slots are available on PoE stack units.

TABLE 19 Description of the fields in the Inline Power Details window (continued)

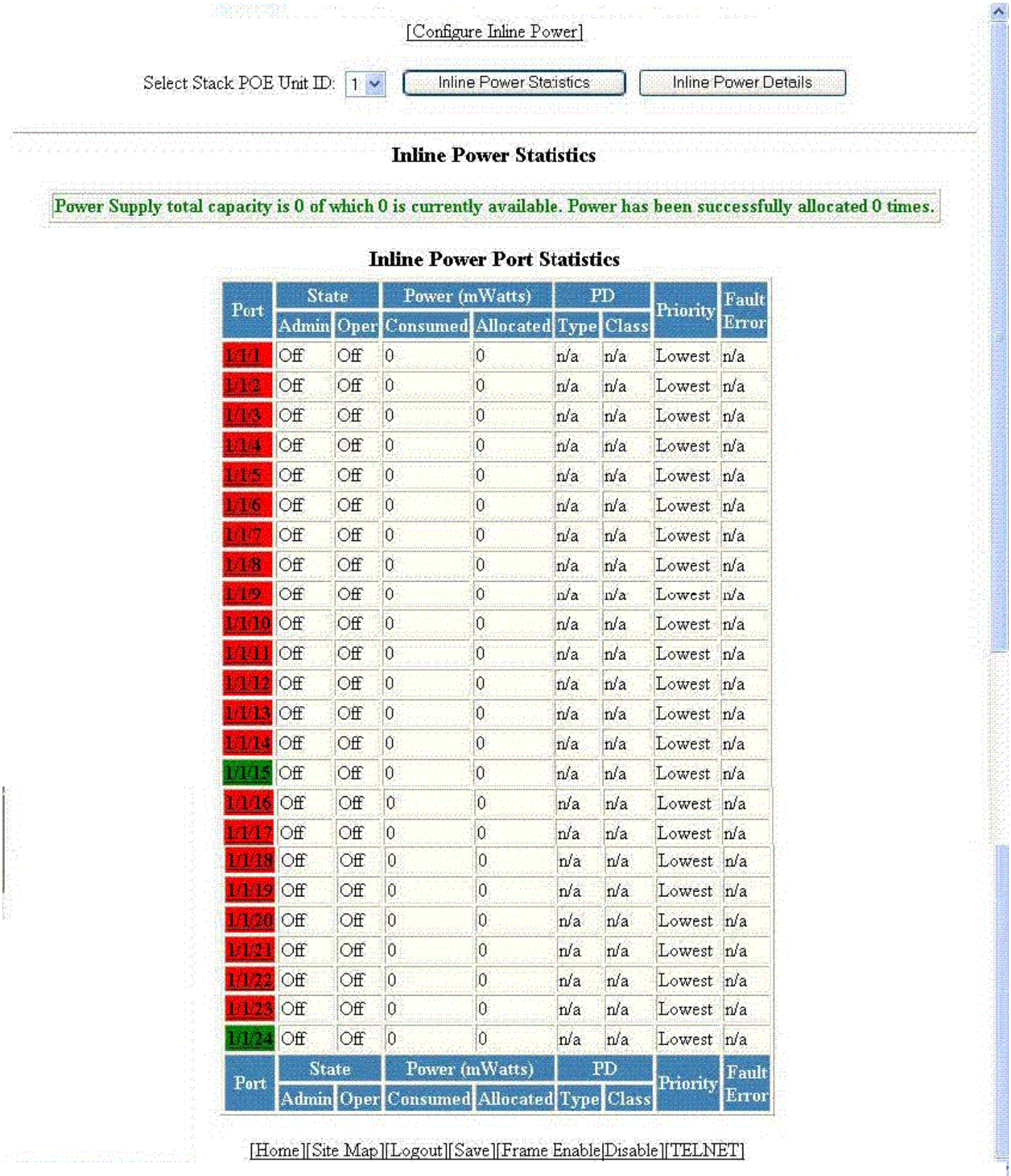
Field	Description
# Ports	Displays the total number of available ports in each level of priority.
Power Consumption in Watts	Displays the total number of watts consumed by both PoE power-consuming devices and the PoE module (daughter card) attached to the interface module.
Power Allocation in Watts	Displays the number of watts allocated to the interface module PoE ports. This value is the sum of port default or configured maximum power levels, or power classes automatically detected by the PoE device.

Displaying inline power statistics

To display the inline power statistics, select the unit ID in the **Select Stack POE Unit ID** list and click **Inline Power Statistics** .

The **Inline Power Statistics** window is displayed as shown in the figure below.

FIGURE 25 Monitoring inline power statistics



[Configure Inline Power]

Select Stack POE Unit ID: 1 | Inline Power Statistics | Inline Power Details

Inline Power Statistics

Power Supply total capacity is 0 of which 0 is currently available. Power has been successfully allocated 0 times.

Inline Power Port Statistics

Port	State		Power (mWatts)		PD		Priority	Fault Error
	Admin	Oper	Consumed	Allocated	Type	Class		
1/1/1	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/2	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/3	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/4	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/5	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/6	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/7	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/8	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/9	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/10	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/11	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/12	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/13	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/14	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/15	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/16	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/17	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/18	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/19	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/20	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/21	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/22	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/23	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/24	Off	Off	0	0	n/a	n/a	Lowest	n/a
Port	State		Power (mWatts)		PD		Priority	Fault Error
	Admin	Oper	Consumed	Allocated	Type	Class		

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

TABLE 20 Description of the fields in the Inline Power Statistics window

Field	Description
Port	Displays the stack port identification of the port as stack#/slot#/port#.
State: Admin	Specifies whether PoE has been enabled on the port, using one of the following values: • *ON* --The inline power command was issued on the port. • *OFF* --The inline power command has not been issued on the port.
State: Oper	Displays the status of inline power on the port, using one of the following values: • *ON* --The PoE power supply is delivering inline power to the powered device. • *OFF* --The PoE power supply is not delivering inline power to the powered device. • *DENIED* --The port is in standby mode waiting for power because currently there is not enough available power for the port.
Power (mWatts) Consumed	Displays the amount of current (milliwatts) the powered device is consuming.
Power (mWatts) Allocated	Displays the amount of current (milliwatts) allocated to the port. This value is either the default or configured maximum power level, or the power class that was automatically detected.
PD Type	Displays the type of powered device connected to the port. This value can be one of the following: • *802.3at* --The PD connected to this port is 802.3at-compliant. • *802.3af* --The PD connected to this port is 802.3af-compliant. • *LEGACY* --The powered device connected to this port is a legacy product (not 802.3af-compliant). • *n/a*-- One of the following is true: – The device connected to this port is a non-powered device. – No device is connected to this port. – The port is in standby or denied mode (waiting for power).
PD Class	Displays the maximum amount of power received by a powered device. This value can be one of the following: • *Class1* --Receives 4 watts maximum. • *Class2* --Receives 7 watts maximum. • *Class3* --Receives 15.4 watts maximum. • *Class 4* --Receives 30 watts maximum. • *n/a* --The device attached to the port cannot advertise its class.
Priority	Displays the inline power priority of the port, which determines the order in which the port receives power while in standby mode (waiting for power). Ports with a higher priority receive power before ports with a low priority. The value of priority can be one of the following: • *1* --Critical priority • *2* --High priority • *3* --Low priority

TABLE 20 Description of the fields in the Inline Power Statistics window (continued)

Field	Description
Fault Error	Displays the fault or error that occurred on the port, if applicable. Otherwise, *n/a* is displayed. The value can be one of the following: • *critical temperature* --The PoE chip temperature limit rose above the safe operating level, thereby powering down the port. • *detection failed* --The port failed capacitor detection (legacy PD detection) because of a discharged capacitor. This can occur when connecting a non-PD on the port. • *detection failed* --The port failed capacitor detection (legacy PD detection) because of an out-of-range capacitor value. This can occur when connecting a non-PD on the port. • *internal h/w fault* --A hardware problem has hindered port operation. • *lack of power* --The port has shut down due to lack of power. • *main supply voltage high* --The voltage was higher than the maximum voltage limit, thereby tripping the port. • *main supply voltage low* --The voltage was lower than the minimum voltage limit, thereby tripping the port. • *overload state* --The PD consumed more power than the maximum limit configured on the port, based on the default configuration, user configuration, or CDP configuration. • *over temperature* --The port temperature rose above the temperature limit, thereby powering down the port. • *PD DC fault* --A succession of underload and overload states, or a PDDC/DC fault, caused the port to shutdown. • *short circuit* --A short circuit was detected on the port delivering power. • *underload state* --The PD consumes less power than the minimum limit specified in the 802.3af standard. • *voltage applied from ext src* --The port failed capacitor detection (legacy PD detection) because the voltage applied to the port was from an external source.

Monitoring STP

- Displaying STP information.....59

Displaying STP information

Ruckus ICX Layer 2 switches and Layer 3 switches support standard Spanning Tree Protocol (STP) as described in the IEEE 802.1D specification. By default, STP is enabled on Layer 2 switches and disabled on Layer 3 switches. To display the STP information, perform the following steps.

1. Click **Monitor** on the left pane and select **STP** .

   By default, STP is disabled on Layer 3 switches and therefore the message `STP is disabled. Go to system to enable STP` is displayed.

2. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

   The STP window is displayed as shown in the figure below.

FIGURE 26 Monitoring the STP bridge and port

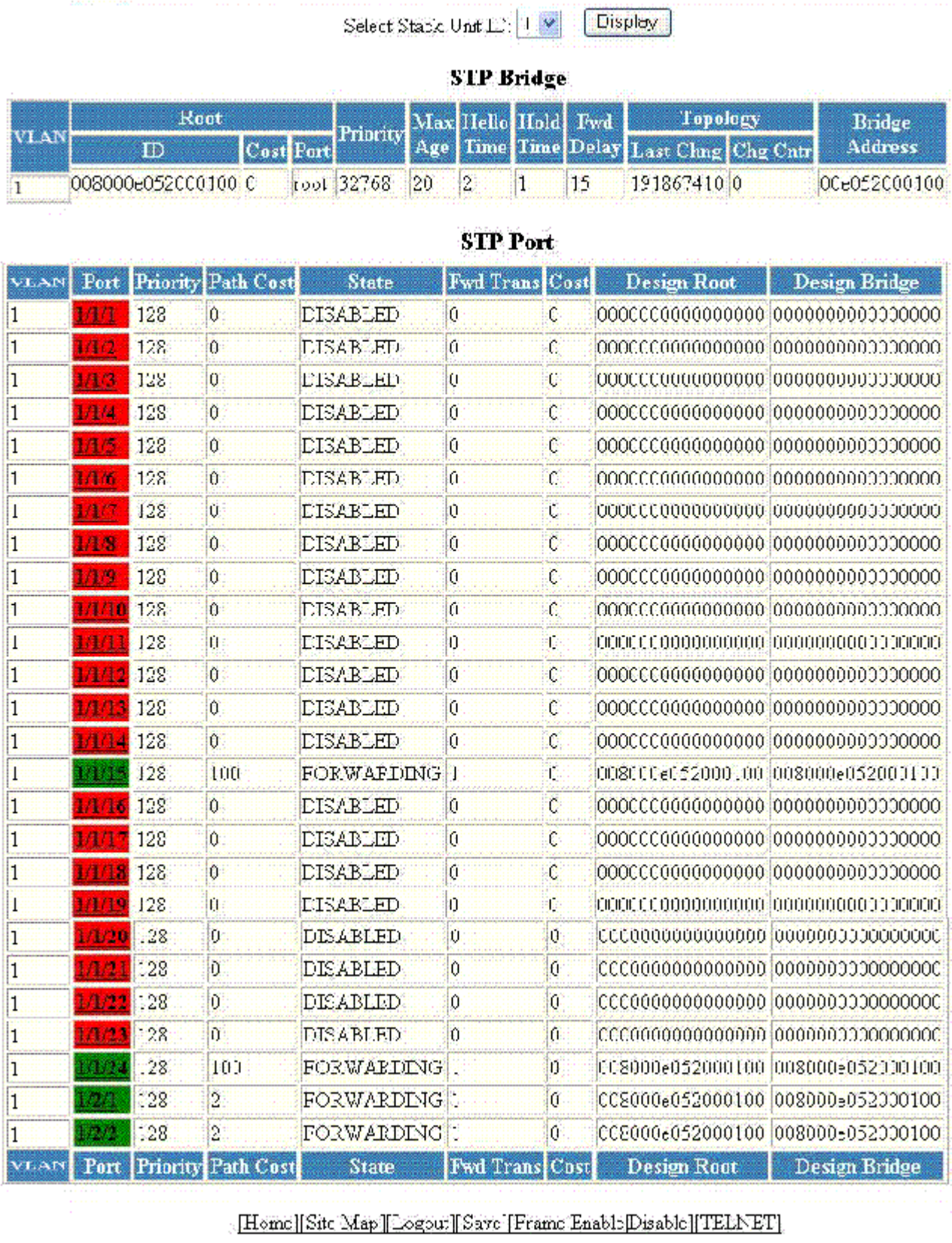


TABLE 21 Description of the fields in the STP window

Field	Description
STP Bridge parameters (global parameters)	
VLAN	Displays the port-based virtual local area network (VLAN) that contains this spanning tree (instance of STP). VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.
Root ID	Displays the ID assigned by STP to the root bridge for this spanning tree.
Root Cost	Displays 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	Displays 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	Displays the STP priority of this device or VLAN. The value is shown in hexadecimal format.
Max Age	Displays the number of seconds this device or VLAN waits for a Hello message from the root bridge before deciding that the root has become unavailable and performing a reconvergence.
Hello Time	Displays the interval between each configuration Bridge Packet Data Unit (BPDU) sent by the root bridge.
Hold Time	Displays the minimum number of seconds that must elapse between transmissions of consecutive configuration BPDUs on a port.
Fwd Delay	Displays the number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Topology Last Chng	Displays the number of seconds since the last time a topology change occurred.
Topology Chg Cntr	Displays the number of times the topology has changed since the device was reloaded.
Bridge Address	Displays the STP address of this device or VLAN.
STP Port parameters	
VLAN	Displays the VLAN that the port is in. This field displays only when port VLAN is enabled.
Port	Displays the port number - stack-unit/slotnum/portnum.
Priority	Displays the STP priority of the port in hexadecimal format.
Path Cost	Displays the STP path cost of the port.
State	Displays the STP state of the port. 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 the BLOCKING 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

TABLE 21 Description of the fields in the STP window (continued)

Field	Description
	order to determine the new topology. No 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 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.
Fwd Trans	Displays the number of times STP has changed the state of this port between BLOCKING and FORWARDING.
Cost	Displays 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.
Design Root	Displays 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	Displays 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

- Displaying RSTP information.....65

Displaying RSTP information

To view current Rapid Spanning Tree Protocol (RSTP) information for a device, you must configure RSTP. For more information on how to configure RSTP, refer to Monitoring RSTP on page 65. By default, RSTP is enabled on Layer 2 switches and disabled on Layer 3 switches.

To display RSTP bridge and port information, click **Monitor** on the left pane and select **RSTP** .

The RSTP window is displayed as shown in the figure below. Select a Unit ID from the **Select Unit ID** list and click **Display** to view the RSTP parameters of a specific port.

FIGURE 27 Monitoring the RSTP bridge and port

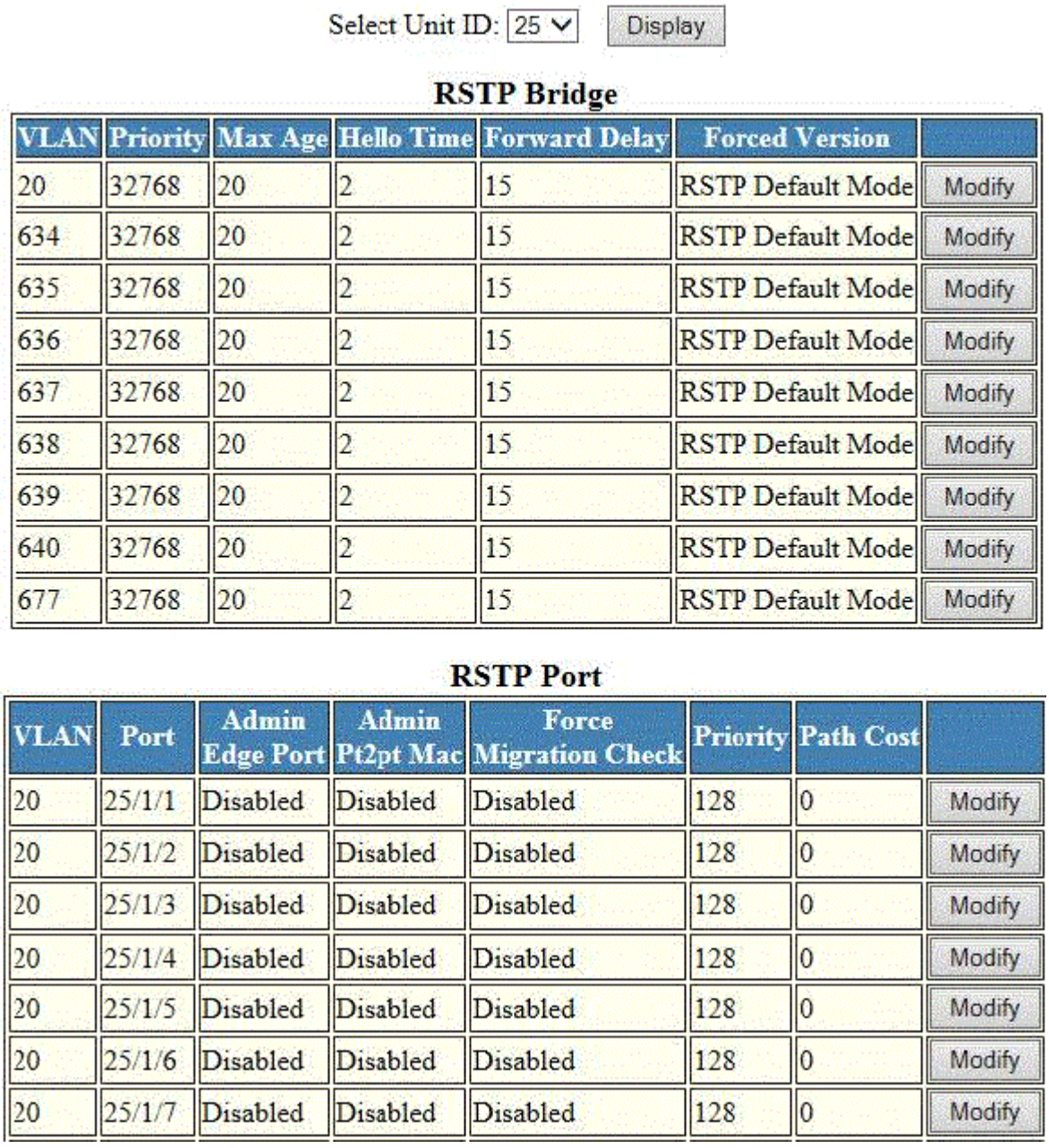


TABLE 22 Description of the fields in the RSTP window

Field	Description
Select Unit ID	
RSTP Bridge parameters	
VLAN	Displays 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 RSTP information is for VLAN 1.
Priority	Displays the configured priority.

TABLE 22 Description of the fields in the RSTP window (continued)

Field	Description
Max.Age	Displays 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	Displays the duration (secs) between two Hello packets.
Forward Delay	Displays the number of seconds a non-edge designated port waits until it can apply any of the following transitions, if the received RST BPDU 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. Forward delay 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).
Forced Version	Displays the configured force version value, which can be one of the following: • *0* --The bridge has been forced to operate in an STP compatibility mode. • *2* --The bridge has been forced to operate in an RSTP mode. This is the default.
RSTP Port parameters	
VLAN	Displays 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 RSTP information is for VLAN 1.
Port	Displays the port number - stack-unit/slotnum/portnum.
Admin Edge Port	Displays whether 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.
Admin Pt2pt Mac	Displays whether 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.
Force Migration Check	Displays whether the port is enabled or disabled to forcefully send one RST BPDU. If only STP BPDUs are received in response to the send RST BPDU, then the port will return to sending STP BPDUs.
Priority	Displays the configured priority of the port. The default is 128 or 0x80.
Path Cost	Displays the configured path cost on a link connected to this port.

Monitoring IP

- Displaying IP cache....69
- Displaying IP traffic information for devices running Layer 2 code....70
- Displaying IP traffic information for devices running Layer 3 code....75

Displaying IP cache

NOTE
The IP cache is specific to Ruckus ICX devices running Layer 3 code.

To display the IP forwarding cache information, perform the following steps.

1. Click **Monitor** on the left pane and select **IP** .
2. Click **Cache** .

   The **IP Cache** window is displayed as shown in the figure below.

FIGURE 28 Monitoring the IP cache

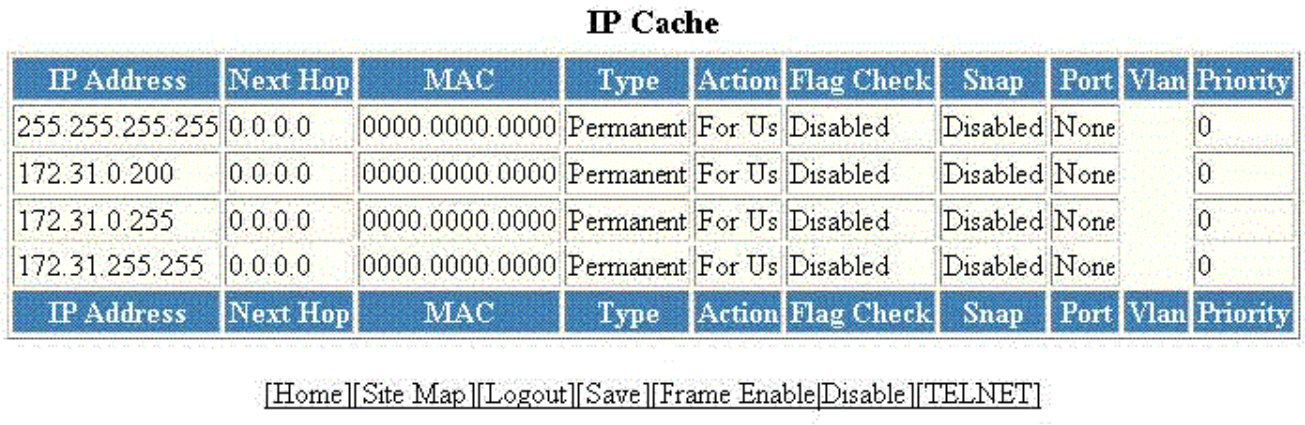


TABLE 23 Description of the fields in the IP Cache window

Field	Description
IP Address	Displays the IP address of the destination.
Next Hop	Displays the IP address of the next hop router to the destination. This field contains either an IP address or the value DIRECT. DIRECT means the destination is either directly attached or the destination is an address on this Ruckus device.
MAC	Displays the MAC address of the destination. **NOTE** If the entry is type Us (indicating that the destination is this Ruckus device), the address consists of zeroes.

TABLE 23 Description of the fields in the IP Cache window (continued)

Field	Description
Type	Displays the type of host entry, which can be one of the following: • *Dynamic* • *Permanent* • *Forward* • *Us* • *Complex Filter* • *Wait ARP* • *ICMP Deny* • *Drop* • *Fragment* • *Snap Encap*
Action	Displays the action the router takes for the packet.
Flag Check	Displays whether the flag check has been enabled or disabled.
Snap	Displays whether the snap encapsulation has been enabled or disabled.
Port	Displays the port through which this device reaches the destination. For destinations that are located on this device, the port number is shown as "n/a".
Vlan	Displays the VLAN the port is in.
Priority	Displays the Quality of Service (QoS) priority of the port or the VLAN.

Displaying IP traffic information for devices running Layer 2 code

To display the IP traffic statistics for Ruckus ICX devices running Layer 2 code, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.

2. Click **Traffic**.

   The **IP Traffic** window is displayed as shown in the figure below.

FIGURE 29 Monitoring the IP traffic for devices running Layer 2 code

IP Traffic

IP Statistics			
Packets Received:	167	Packets Sent:	233
Fragmented:	0	Reassembled:	0
Bad Header:	0	No Route:	0
Unknown Protocols:	0	No Buffer:	0
Other Errors:	0		

ICMP Statistics			
Total Received:	0	Total Sent:	0
Received Errors:	0	Sent Errors:	0
Received Unreachable:	0	Sent Unreachable:	0
Received Time Exceed:	0	Sent Time Exceed:	0
Received Parameter:	0	Sent Parameter:	0
Received Source Quench:	0	Sent Source Quench:	0
Received Redirect:	0	Sent Redirect:	0
Received Echo:	0	Sent Echo:	0
Received Echo Reply:	0	Sent Echo Reply:	0
Received Timestamp:	0	Sent Timestamp:	0
Received Timestamp Reply:	0	Sent Timestamp Reply:	0
Received Address Mask:	0	Sent Address Mask:	0
Received Address Mask Reply:	0	Sent Address Mask Reply:	0
Received IRDP Advertisment:	0	Sent IRDP Advertisment:	0
Received IRDP Solicitation:	0	Sent IRDP Solicitation:	0

UDP Statistics			
Received:	0	Sent:	0
No Port:	0	Input Errors:	0

TCP Statistics			
Active Opens:	0	Passive Opens:	0
Failed Attempts:	0	Active Resets:	0
Passive Resets:	0	Input Errors:	0
In Segments:	167	Out Segments:	233
Retransmission:	0		
Current Active TCBs:	1	TCBs Allocated:	10
TCBs Freed:	3		
Keepalive Close Connection:	0	Keepalive Failure Callback:	0
TCP Connect Connection Exist:	0	TCP Connect Out of TCB:	0

TABLE 24 Description of the fields in the IP Traffic window

Field	Description
IP Statistics parameters	
Packets Received	Displays the number of IP packets received by the device.
Packets Sent	Displays the number of IP packets originated and sent by the device.
Fragmented	Displays the number of IP packets fragmented by this device before sending or forwarding them.
Reassembled	Displays the number of fragmented IP packets received and re-assembled by the device.
Bad Header	Displays the number of IP packets dropped because they had a bad header.
No Route	Displays the number of packets dropped by the device because they had no route information.
Unknown Protocols	Displays the number of packets dropped by the device because the value in the protocol field of the packet header is unrecognized by this device.
No Buffer	Displays the number of packets dropped because the device ran out of buffer space.
Other Errors	Displays the number of packets dropped due to errors other than the ones already indicated in the **IP Statistics** parameters.
ICMP Statistics parameters	
Total Received	Displays the number of Internet Control Message Protocol (ICMP) packets received by the device.
Total Sent	Displays the number of ICMP packets sent by the device.
Received Errors	Displays the number of errors received by the device. This information is used by Ruckus customer support.
Sent Errors	Displays the number of errors sent by the device. This information is used by Ruckus customer support.
Received Unreachable	Displays the number of Destination Unreachable messages received by the device.
Sent Unreachable	Displays the number of Destination Unreachable messages sent by the device.
Received Time Exceed	Displays the number of Time Exceeded messages received by the device.
Sent Time Exceed	Displays the number of Time Exceeded messages sent by the device.
Received Parameter	Displays the number of Parameter Problem messages received by the device.
Sent Parameter	Displays the number of Parameter Problem messages sent by the device.
Received Source Quench	Displays the number of Source Quench messages received by the device.
Sent Source Quench	Displays the number of Source Quench messages sent by the device.
Received Redirect	Displays the number of Redirect messages received by the device.
Sent Redirect	Displays the number of Redirect messages sent by the device.
Received Echo	Displays the number of Echo messages received by the device.
Sent Echo	Displays the number of Echo messages sent by the device.

TABLE 24 Description of the fields in the IP Traffic window (continued)

Field	Description
Received Echo Reply	Displays the number of Echo Reply messages received by the device.
Sent Echo Reply	Displays the number of Echo Reply messages sent by the device.
Received Timestamp	Displays the number of Timestamp messages received by the device.
Sent Timestamp	Displays the number of Timestamp messages sent by the device.
Received Timestamp Reply	Displays the number of Timestamp Reply messages received by the device.
Sent Timestamp Reply	Displays the number of Timestamp Reply messages sent by the device.
Received Address Mask	Displays the number of Address Mask Request messages received by the device.
Sent Address Mask	Displays the number of Address Mask Request messages sent by the device.
Received Address Mask Reply	Displays the number of Address Mask Reply messages received by the device.
Sent Address Mask Reply	Displays the number of Address Mask Reply messages sent by the device.
Received IRDP Advertisement	Displays the number of ICMP Router Discovery Protocol (IRDP) Advertisement messages received by the device.
Sent IRDP Advertisement	Displays the number of IRDP Advertisement messages sent by the device.
Received IRDP Solicitation	Displays the number of IRDP Solicitation messages received by the device.
Sent IRDP Solicitation	Displays the number of IRDP Solicitation messages sent by the device.
UDP Statistics parameters	
Received	Displays the number of User Datagram Protocol (UDP) packets received by the device.
Sent	Displays the number of UDP packets sent by the device.
No Port	Displays the number of UDP packets dropped because the packet did not contain a valid UDP port number.
Input Errors	Displays the number of errors on the incoming packets. This information is used by Ruckus customer support.
TCP Statistics parameters	
Active Opens	Displays the number of Transmission Control Protocol (TCP) connections opened by this device by sending a TCP SYN to another device.
Passive Opens	Displays the number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.
Failed Attempts	Displays the number of failed attempts. This information is used by Ruckus customer support.
Active Resets	Displays 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	Displays the number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.

TABLE 24 Description of the fields in the IP Traffic window (continued)

Field	Description
Input Errors	Displays the number of incoming errors. This information is used by Ruckus customer support.
In Segments	Displays the number of TCP segments received by the device.
Out Segments	Displays the number of TCP segments sent by the device.
Retransmission	Displays 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.
Current Active TCBs	Displays the number of TCP Control Blocks (TCBs) that are currently active.
TCBs Allocated	Displays the number of TCBs that have been allocated.
TCBs Freed	Displays the number of TCBs that have been freed.

Displaying IP traffic information for devices running Layer 3 code

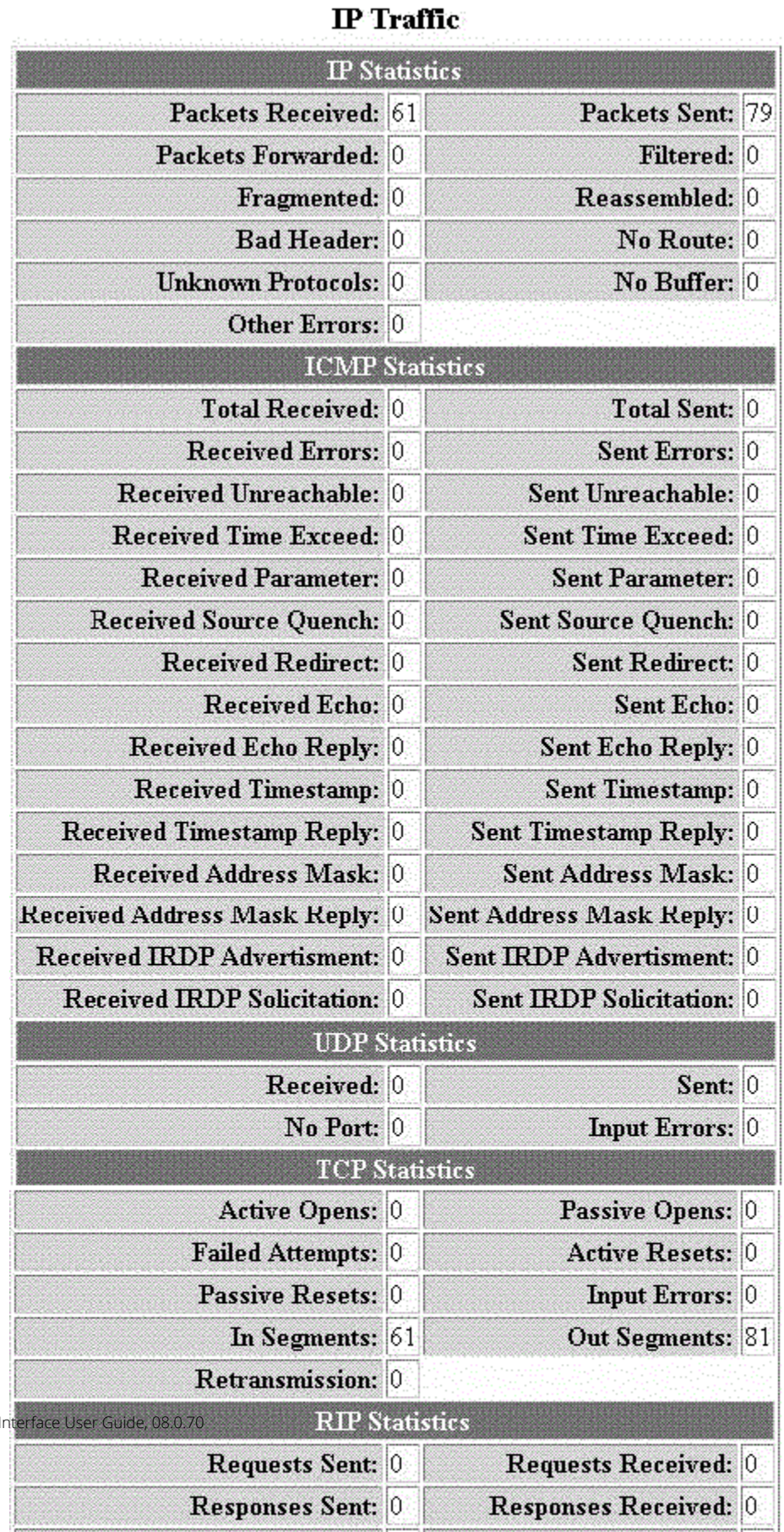
To display the IP traffic statistics for Ruckus ICX devices running Layer 3 code, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.

2. Click **Traffic**

   The **IP Traffic** window is displayed as shown in the figure below.

FIGURE 30 Monitoring the IP traffic information for devices running Layer 3 code



IP Traffic

IP Statistics			
Packets Received:	61	Packets Sent:	79
Packets Forwarded:	0	Filtered:	0
Fragmented:	0	Reassembled:	0
Bad Header:	0	No Route:	0
Unknown Protocols:	0	No Buffer:	0
Other Errors:	0		

ICMP Statistics			
Total Received:	0	Total Sent:	0
Received Errors:	0	Sent Errors:	0
Received Unreachable:	0	Sent Unreachable:	0
Received Time Exceed:	0	Sent Time Exceed:	0
Received Parameter:	0	Sent Parameter:	0
Received Source Quench:	0	Sent Source Quench:	0
Received Redirect:	0	Sent Redirect:	0
Received Echo:	0	Sent Echo:	0
Received Echo Reply:	0	Sent Echo Reply:	0
Received Timestamp:	0	Sent Timestamp:	0
Received Timestamp Reply:	0	Sent Timestamp Reply:	0
Received Address Mask:	0	Sent Address Mask:	0
Received Address Mask Reply:	0	Sent Address Mask Reply:	0
Received IRDP Advertisment:	0	Sent IRDP Advertisment:	0
Received IRDP Solicitation:	0	Sent IRDP Solicitation:	0

UDP Statistics			
Received:	0	Sent:	0
No Port:	0	Input Errors:	0

TCP Statistics			
Active Opens:	0	Passive Opens:	0
Failed Attempts:	0	Active Resets:	0
Passive Resets:	0	Input Errors:	0
In Segments:	61	Out Segments:	81
Retransmission:	0		

RIP Statistics			
Requests Sent:	0	Requests Received:	0
Responses Sent:	0	Responses Received:	0

TABLE 25 Description of the fields in the IP Traffic window

Field	Description
IP Statistics parameters	
Packets Received	Displays the number of IP packets received by the device.
Packets Sent	Displays the number of IP packets originated and sent by the device.
Packets Forwarded	Displays the total number of IP packets received by the device and forwarded to other devices.
Filtered	Displays the total number of IP packets filtered by the device.
Fragmented	Displays the number of IP packets fragmented by this device before sending or forwarding them.
Reassembled	Displays the number of fragmented IP packets received and re-assembled by the device.
Bad Header	Displays the number of IP packets dropped because they had a bad header.
No Route	Displays the number of packets dropped by the device because they had no route information.
Unknown Protocols	Displays the number of packets dropped by the device because the value in the protocol field of the packet header is unrecognized by this device.
No Buffer	Displays the number of packets dropped because the device ran out of buffer space.
Other Errors	Displays the number of packets dropped due to errors other than the ones already indicated in the **IP Statistics** parameters.
ICMP Statistics	Refer to Displaying IP traffic information for devices running Layer 2 code on page 70.
UDP Statistics	Refer to Displaying IP traffic information for devices running Layer 2 code on page 70.
TCP Statistics parameters	
Active Opens	Displays the number of TCP connections opened by this device by sending a TCP SYN to another device.
Passive Opens	Displays the number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.
Failed Attempts	Displays the number of failed attempts. This information is used by Ruckus customer support.
Active Resets	Displays 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	Displays 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	Displays the number of incoming errors. This information is used by Ruckus customer support.
In Segments	Displays the number of TCP segments received by the device.
Out Segments	Displays the number of TCP segments sent by the device.
Retransmission	Displays 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 parameters	

TABLE 25 Description of the fields in the IP Traffic window (continued)

Field	Description
Requests Sent	Displays the number of requests this device has sent to another Routing Information Protocol (RIP) Layer 3 switch for all or part of its RIP routing table.
Requests Received	Displays the number of requests this device has received from another RIP Layer 3 switch for all or part of this device's RIP routing table.
Responses Sent	Displays the number of responses this device has sent to another RIP Layer 3 switch's request for all or part of this device's RIP routing table.
Responses Received	Displays the number of responses this device has received to requests for all or part of another RIP Layer 3 switch's routing table.
Unrecognized	Displays the number of RIP packets that were not recognized by the device.
Bad Version	Displays 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	Displays 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	Displays the number of RIP request packets this Layer 3 switch dropped because the format was bad.
Bad Metrics	Displays the number of responses to RIP request packets this Layer 3 switch dropped because of the bad metric value. This information is used by Ruckus customer support.
Bad Response Format	Displays the number of responses to RIP request packets this Layer 3 switch dropped because the format was bad.
Response Not from RIP Port	Displays the number of RIP responses received from non-RIP ports. This information is used by Ruckus customer support.
Response from Loopback	Displays the number of RIP responses received from loopback interfaces.
Packets Rejected	Displays the number of RIP packets rejected by the device.

Monitoring RMON

- Displaying RMON history....81
- Displaying RMON Ethernet statistics.... 83
- Changing polling interval....88
- Displaying RMON Ethernet error statistics....89

Displaying RMON history

By default, all active ports 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 cleared.

The following history entries are generated for each device:

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

To display Remote Monitoring (RMON) history, perform the following steps.

1. Click **Monitor** on the left pane and select **RMON** .
2. Click **History** .

   The **RMON Ethernet History** window is displayed as shown in the figure below.

FIGURE 31 Monitoring the RMON Ethernet history

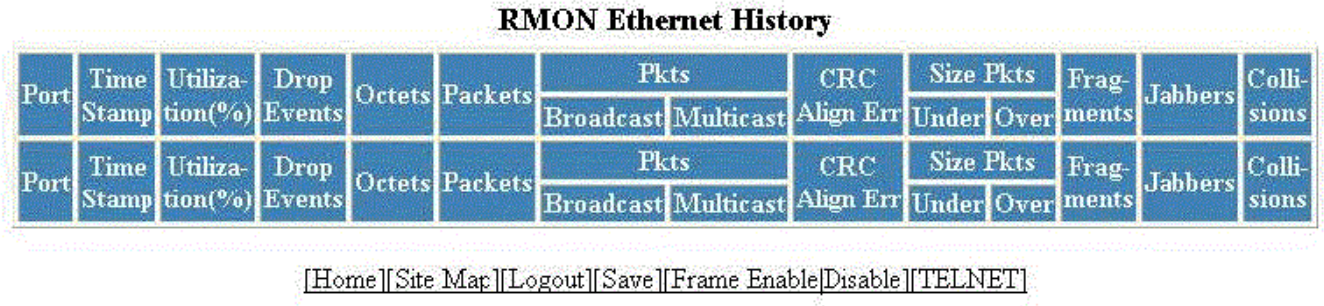


TABLE 26 Description of the fields in the RMON Ethernet History window

Field	Description
Port	Displays the port for which the history data is being presented - stack-unit/slotnum/portnum.
Time Stamp	Displays the day and time when the data was collected.
Utilization(%)	Displays the percentage of the port that was being utilized when the data was taken.
Drop Events	Displays 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.

TABLE 26 Description of the fields in the RMON Ethernet History window (continued)

Field	Description
Octets	Displays 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	Displays the total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Packets: Broadcast	Displays the total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	Displays 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	Displays the total number of packets received that were from 64 through 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	Displays 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	Displays 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	Displays 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, because 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	Displays 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).

TABLE 26 Description of the fields in the RMON Ethernet History window (continued)

Field	Description
	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	Displays the best estimate of the total number of collisions on this Ethernet segment.

Displaying RMON Ethernet statistics

RMON statistics provide 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.

To display RMON statistics, perform the following steps.

1. Click **Monitor** on the left pane and select **RMON**.
2. Click **Statistic**.

3. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

   The **RMON Ethernet Statistics** window is displayed as shown in the figure below.

FIGURE 32 Monitoring RMON Ethernet statistics

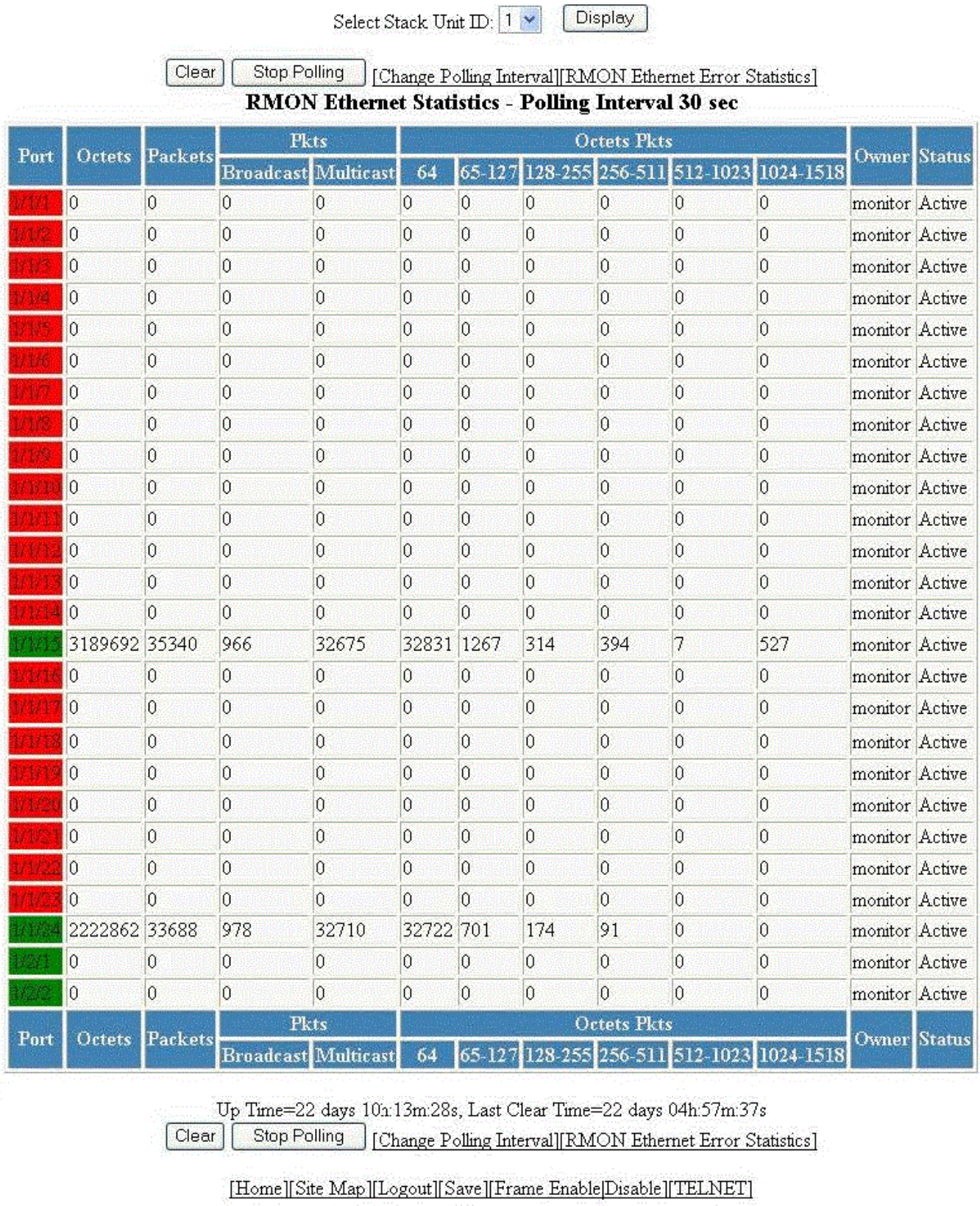


TABLE 27 Description of the fields in the RMON Ethernet Statistics window

Field	Description
Port	Displays the port number - stack-unit/slotnum/portnum.
Octets	Displays 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	Displays the total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Packets: Broadcast	Displays the total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	Displays 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	Displays 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	Displays the total number of packets received that were from 65 through 127 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 128 - 255	Displays the total number of packets received that were from 128 through 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 256 - 511	Displays the total number of packets received that were from 256 through 511 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 512 - 1023	Displays the total number of packets received that were from 512 through 1023 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 1024 - 1518	Displays the total number of packets received that were from 1024 through 1518 octets long. This number includes bad packets.

TABLE 27 Description of the fields in the RMON Ethernet Statistics window (continued)

Field	Description
	This number does not include framing bits but does include FCS octets.
Owner	Displays the owner of the packets.
Status	Displays the status of the port.
Up Time	Displays the length of time the device has been available.
Last Clear Time	Displays the length of time data has been accumulating in the current table.

To remove the current data in the table and restart monitoring, click **Clear**. To stop reporting the statistics, click **Stop Polling**.

The **RMON Ethernet Statistics** window contains the following links:

- To change the polling interval, click **Change Polling interval**. For more information, refer to the "Changing polling interval" section.
- To display the RMON Ethernet error statistics, click **RMON Ethernet Error Statistics**. For more information, refer to the "Displaying RMON Ethernet error statistics" section.

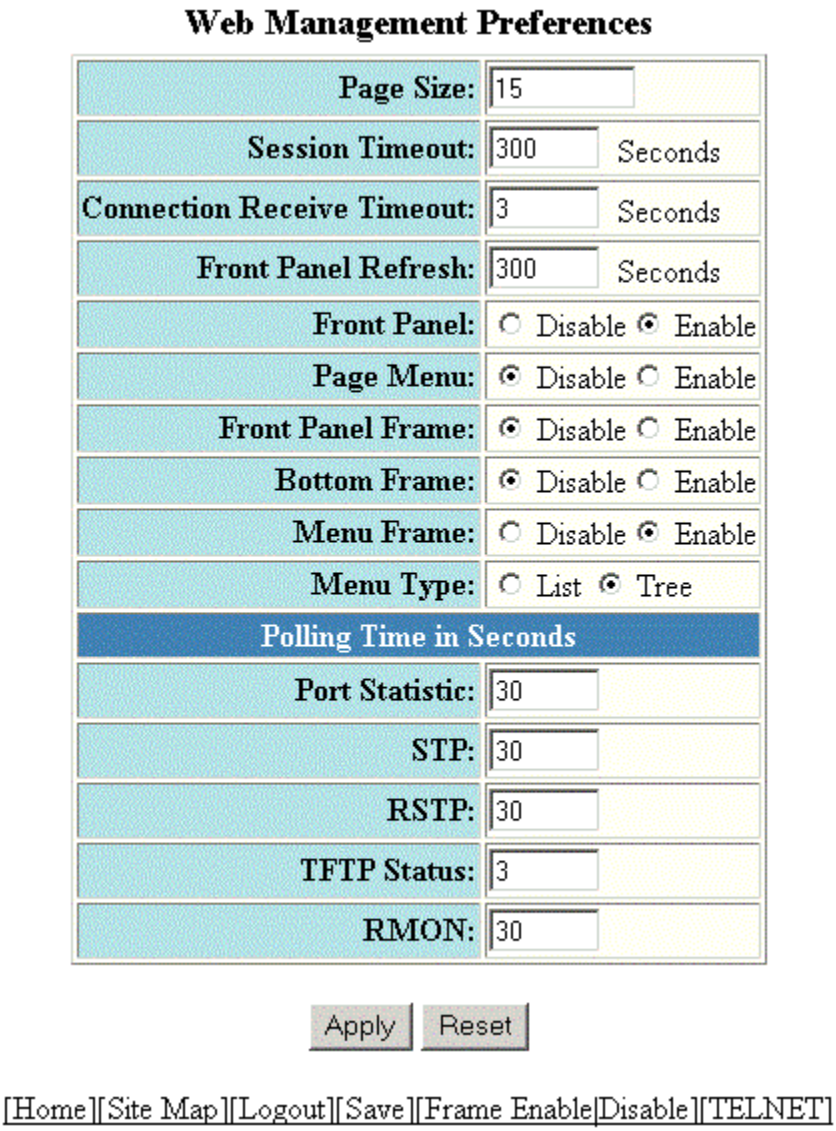
Changing polling interval

To change the number of seconds between reporting the RMON Ethernet statistics, perform the following steps.

1. Click **Change Polling interval** on the **RMON Ethernet Statistics** window.

   The **Web Management Preferences** window is displayed as shown in the figure below.

   FIGURE 33 Modifying web management preferences



2. Specify the RMON polling interval in the **RMON** field.

3. Click **Apply** .

   The message `The change has been made` is displayed at the top of the window. To undo the changes, click **Reset** .
   For more information on web management preferences, refer to Configuring the web management preferences on page 131.

Displaying RMON Ethernet error statistics

To display RMON error information, perform the following steps.

1. Click **RMON Ethernet Error Statistics** on the **RMON Ethernet Statistics** window.

2. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

   The **RMON Ethernet Error Statistics** window is displayed as shown in the figure below.

FIGURE 34 Monitoring the RMON Ethernet error statistics

Clear | Stop Polling | [Change Polling Interval][RMON Ethernet Statistics]

RMON Ethernet Error Statistics - Polling Interval 30 sec

Port	Drop Events	CRC Alignment Errors	Undersize Pkts	Oversize Pkts	Fragments	Jabbers	Collisions
1/1	0	0	0	0	0	0	0
1/2	0	0	0	0	0	0	0
1/3	0	0	0	0	0	0	0
1/4	0	0	0	0	0	0	0
1/5	0	0	0	0	0	0	0
1/6	0	0	0	0	0	0	0
1/7	0	0	0	0	0	0	0
1/8	0	0	0	0	0	0	0
1/9	0	0	0	0	0	0	0
1/10	0	0	0	0	0	0	0
1/11	0	0	0	0	0	0	0
1/12	0	0	0	0	0	0	0
1/13	0	0	0	0	0	0	0
1/14	0	0	0	0	0	0	0
1/15	0	0	0	0	0	0	0
1/16	0	0	0	0	0	0	0
1/17	0	0	0	0	0	0	0
1/18	0	0	0	0	0	0	0
1/19	0	0	0	0	0	0	0
1/20	0	0	0	0	0	0	0
1/21	0	0	0	0	0	0	0
1/22	0	0	0	0	0	0	0
1/23	0	0	0	0	0	0	0
1/24	0	0	0	0	0	0	0
mgmt1	2576980184	2576980184	2576980184	2576980184	2576980184	2576980184	2576980184
Port	Drop Events	CRC Alignment Errors	Undersize Pkts	Oversize Pkts	Fragments	Jabbers	Collisions

Up Time=00 days 00h:20m:13s, Last Clear Time=00 days 00h:00m:00s

Clear | Stop Polling | [Change Polling Interval][RMON Ethernet Statistics]

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

TABLE 28 Description of the fields in the RMON Ethernet Error Statistics window

Field	Description
Port	Displays the port number - stack-unit/slotnum/portnum.
Drop Events	Displays 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.
CRC Alignment Errors	Displays the total number of packets received that were from 64 through 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.
Undersize Pkts	Displays 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.
Oversize Pkts	Displays 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	Displays 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 increment, because 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	Displays 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	Displays the best estimate of the total number of collisions on this Ethernet segment.
Up Time	Displays the length of time the device has been available.
Last Clear Time	Displays the length of time data has been accumulating in the current table.

To remove the current data in the table and restart monitoring, click **Clear** . To stop reporting the statistics, click **Stop Polling** .

The **RMON Ethernet Error Statistics** window contains the following links:

- To change the polling interval, click **Change Polling interval** . For more information, refer to Changing polling interval on page 88.
- To display the RMON statistics, click **RMON Ethernet Statistics** . For more information, refer to Displaying RMON Ethernet statistics on page 83.

Configuring Stack Components

- Configuring the general settings for a traditional stack..... 93
- Viewing stack priority details..... 94
- Modifying stack ports.....94
- Configuring a stack module..... 96

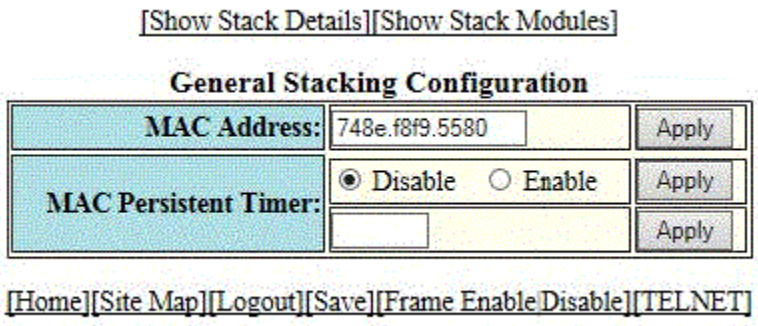
Configuring the general settings for a traditional stack

To change the stack settings to improve performance and reliability of the device, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.
2. Click **General**.

   The **General Stacking Configuration** window is displayed as shown in the figure below.

   FIGURE 35 General stacking configuration



3. Enter the Media Access Control (MAC) address of the device in the **MAC Address** field and then click **Apply**.
4. Click **Disable** or **Enable** for **MAC Persistent Timer** and then click **Apply**.

   If you click **Enable**, type the time delay before the stack MAC address changes in the **MAC Persistent Timer** field and then click **Apply**.

   The **General Stacking Configuration** window provides links to monitor stack parameters:

   - To display the current stack information, click **Show Stack Details** . For more information, refer to the “Displaying the stack details” section.
   - To display the current information about the stack modules, click **Show Stack Modules** . For more information, refer to the “Displaying a stack module” section.

Viewing stack priority details

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

It is possible to assign the same priority for Active and Standby Controllers, or different priorities (Active highest and Standby second-highest). When the Active and Standby Controllers have the same priority, if the Active Controller fails, the Standby Controller takes over. If the original Active Controller becomes operational again, it will not be able to resume its original role.

When the priorities of the Active and Standby Controllers are different, if the Active Controller fails, the Standby Controller takes over. If the original Active Controller becomes operational again, the old Active Controller regains its role and resets the other units.

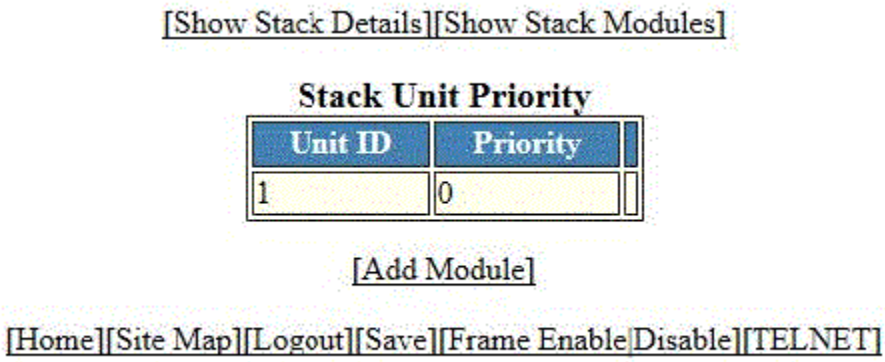
You can assign the same priority to the Active and Standby Controllers after the stack is formed. This prevents the intended Standby Controller from becoming the Active Controller during stack construction.

To view the priority of the units within a stack, perform the following steps.

1. Click **Configure** on the left pane and select **Stack** .
2. Click **Priority** .

   The **Stack Unit Priority** window is displayed as shown in the figure below.

   FIGURE 36 Stack unit priority



   To add a new stack module, click **Add Module** . For more information on how to configure a stack module, refer to Configuring a stack module on page 96.

Modifying stack ports

NOTE
You cannot change the stack ports for the Ruckus ICX devices.

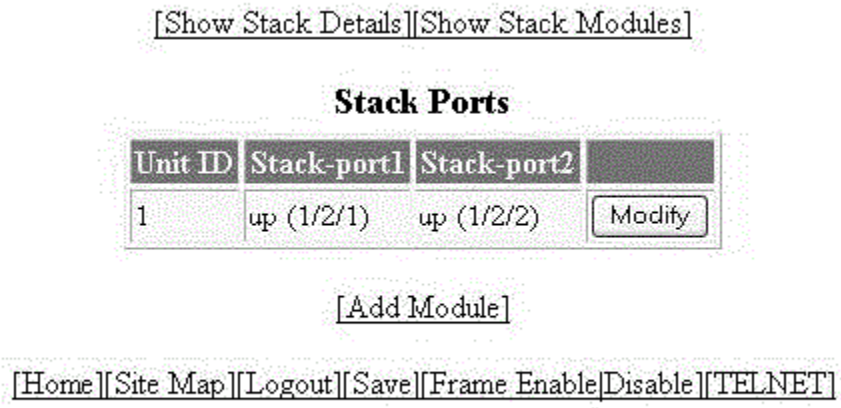
To modify the stack ports, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.

2. Click **Stack-Ports**.

   The **Stack Ports** window is displayed.

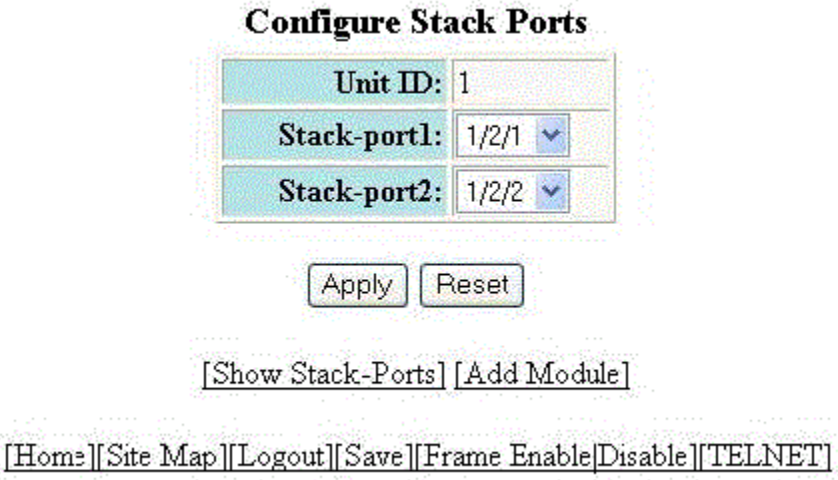
   FIGURE 37 Modifying stack ports



3. Click **Modify**.

   The **Configure Stack Ports** window is displayed as shown in the figure below.

   FIGURE 38 Modifying stack ports



4. Select a port in the **Stack-port1** list.
5. Select a port in the **Stack-port2** list.

6. Click **Apply**.

   The stack ports are modified and the **Stack Ports** window is displayed.

   To reset the data entered in the configuration pane, click **Reset**. To display the configured stack port, click **Show Stack-Ports**.

   To configure a stack module, click **Add Module**. For more information on how to configure a stack module, refer to the "Configuring a stack module" section.

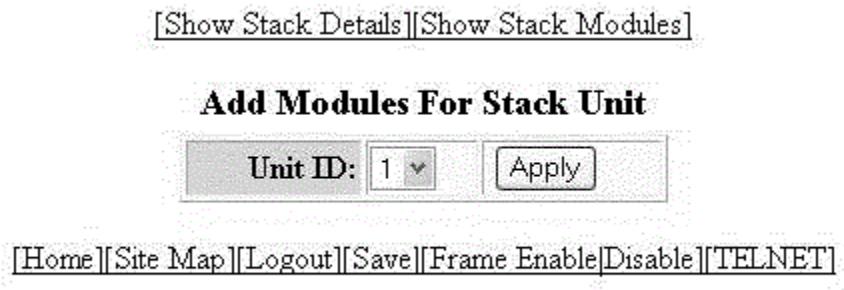
Configuring a stack module

To configure a stack module, perform the following steps.

1. Click **Configure** on the left pane and select **Stack** .
2. Click **Module** .

   The **Add Modules For Stack Unit** window is displayed as shown in the figure below.

   FIGURE 39 Adding modules for a stack unit

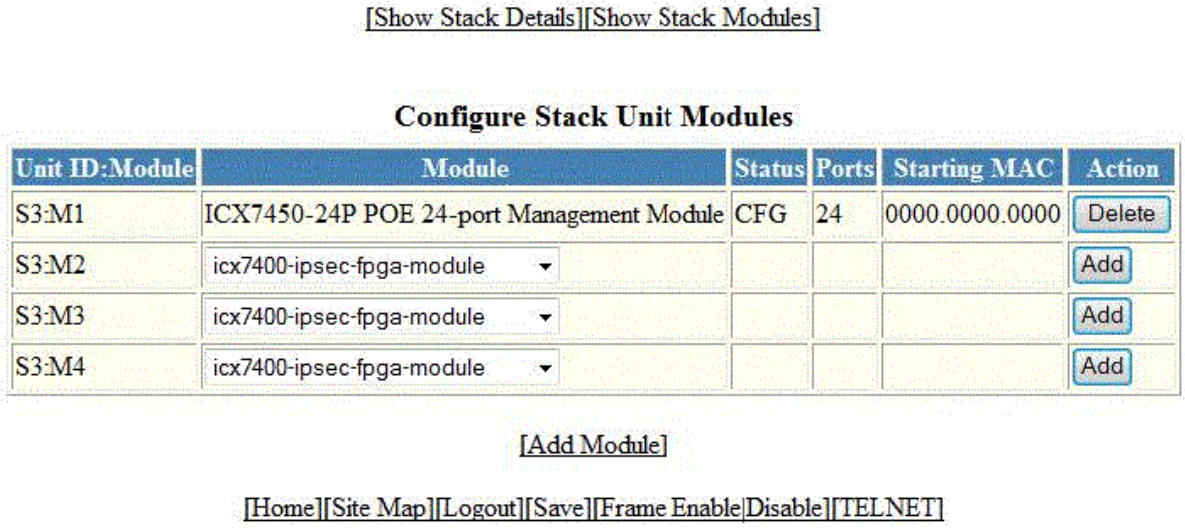


3. Select a stack unit identifier in the **Unit ID** list.

4. Click **Apply** .

   The **Configure Stack Unit Modules** window is displayed as shown in the figure below.

   FIGURE 40 Adding and deleting a stack unit module



5. Select a stack module in the list on the **Module** column and then click **Add** .

   To display current stack details, stack port status, and stack neighbors information, click **Show Stack Details** . For more information, refer to Displaying the stack details on page 33. Click **Delete** to delete a stack unit module. You cannot delete the active modules.

   To display the stack unit modules, click **Show Stack Modules** . For more information, refer to Displaying a stack module on page 35.

Configuring System Components

- Configuring the system clock....99
- Configuring the system DNS....100
- Configuring the general system settings....101
- Configuring the system identification....103
- Configuring the system IP address....104
- Configuring a standard ACL....105
- Configuring an extended ACL....106
- Configuring an IP access group....110
- Configuring the system MAC filter....111
- Configuring the maximum system parameter value....114
- Configuring a system module....115
- Configuring a RADIUS server....117
- Configuring a TACACS/TACACS+ server....119
- Configuring management authentication....120
- Configuring management authorization....121
- Configuring management accounting....122
- Configuring an SNMP community string....123
- Configuring the general management parameters....124
- Configuring a management system log....126
- Configuring a trap....128
- Configuring a trap receiver....129
- Configuring a management user account....131
- Configuring the web management preferences....131

Configuring the system clock

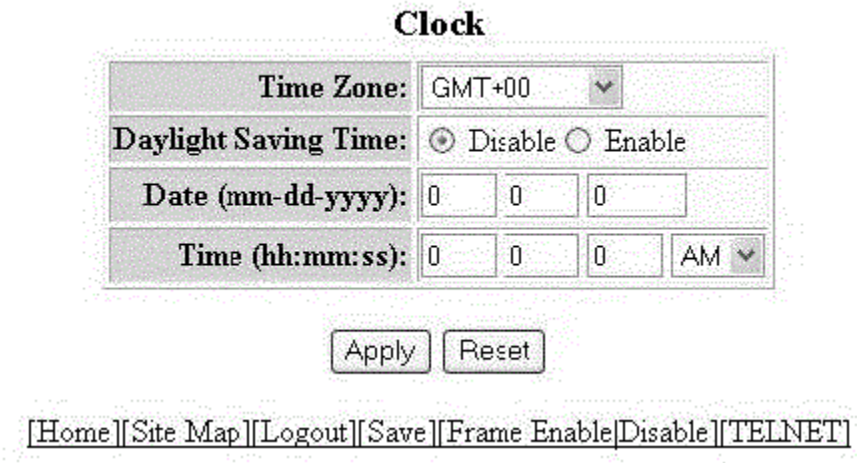
To configure the system clock, perform the following steps.

1. Click **Configure** on the left pane and select **System** .

2. Click **Clock** .

   The **Clock** window is displayed as shown in the figure below.

   FIGURE 41 Configuring the system clock



3. Select the GMT time zone that you want to configure for the device in the **Time Zone** list.
4. Click **Disable** or **Enable** for **Daylight Saving Time** . Daylight Saving Time applies to the US time zone only.
5. Type the date in mm-dd-yyyy format in the **Date (mm-dd-yyyy)** field.
6. Type the time in hh:mm:ss format in the **Time (hh:mm:ss)** field and select **AM** or **PM** in the list.
7. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring the system DNS

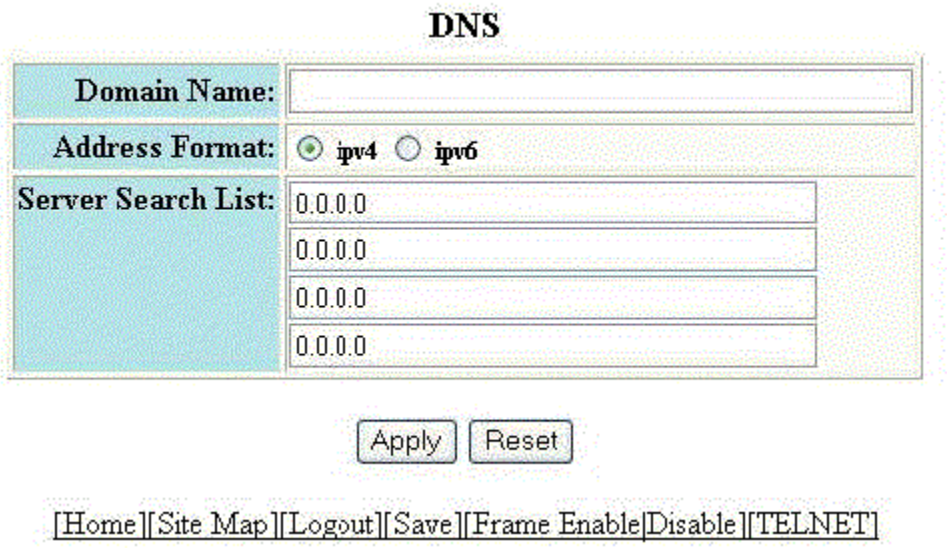
To configure the system Domain Name System (DNS), perform the following steps.

1. Click **Configure** on the left pane and select **System** .

2. Click **DNS** .

   The **DNS** window is displayed as shown in the figure below.

   FIGURE 42 Configuring the system DNS



3. Type the name of the domain that can be used to resolve host names in the **Domain Name** field.
4. Select **ipv4** or **ipv6** for the **Address Format** .
5. Type the server IP addresses in the **Server Search List** fields.

   You can configure a Ruckus device to recognize up to four DNS servers. The first entry serves as the primary default address. If a query to the primary address fails to be resolved after three attempts, the next DNS address is queried (also up to three times). This process continues for each defined DNS address until the query is resolved. The order in which the default DNS addresses are polled is the same as the order in which you enter them.
6. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring the general system settings

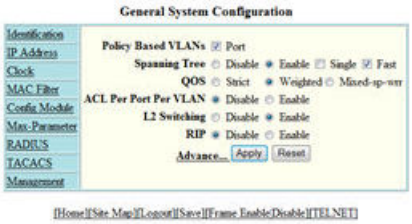
To configure the general system settings, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **General**.

   The **General System Configuration** window is displayed.

   FIGURE 43 Configuring the general system



3. Select the **Port** check box for **Policy based VLANs** to enable configuration of port-based VLANs.
4. Click **Disable** or **Enable** for **Spanning Tree** . If you click **Enable**, select the **Single** or **Fast** check box.
5. Click **Strict** or **Weighted** for **QOS**.
6. Click **Disable** or **Enable** for **ACL Per Port Per VLAN**.
7. Click **Advance** to configure additional system parameters.

   The **System** window is displayed.

   FIGURE 44 Advance system information



8. Type the VLAN tag type in hexadecimal format from 0 through ffff in the **Tag Type** field. The default is 0081.
9. Type the number of seconds a port address remains active in the address table in the **Mac Age Time** field.
10. Type the default VLAN ID number in the **Default VLAN ID** field.
11. Type the interval, in seconds, in which the chassis is polled in the **Chassis Poll Interval (sec)** field.
12. Select a negotiation mode in the **Gig Port Default** list.
13. Click **Disable** or **Enable** for **Route Only**. If you click **Enable** , Layer 2 switching is disabled globally.
14. Click **Disable** or **Enable** for **Jumbo Frame**.

    Jumbo frames are Ethernet frames with more than 1,500 bytes MTU.

15. Click **Apply**.

    The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset**.

    The **General System Configuration** window provides the following links to configure the system parameters:

    - **Identification**
    - **IP Address**
    - **DNS**
    - **DHCP Gateway**
    - **Clock**
    - **MAC Filter**
    - **Module**
    - **Max-Parameter**
    - **RADIUS**
    - **TACACS**
    - **Management**

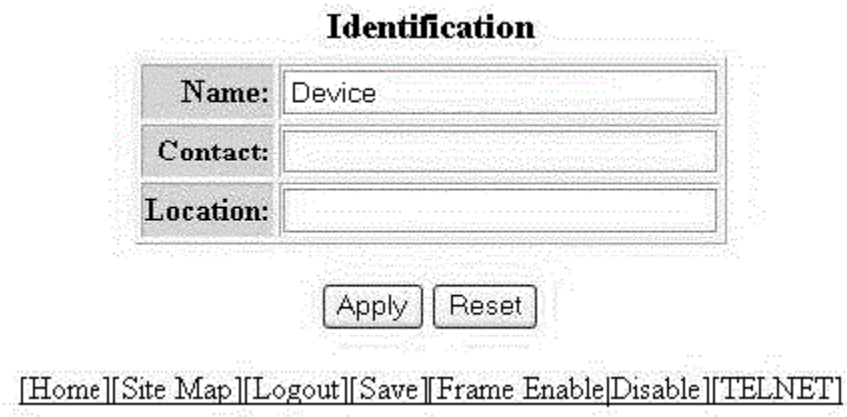
Configuring the system identification

To configure the system identification information, perform the following steps.

1. Click **Configure** on the left pane and select **System** .
2. Click **Identification** .

   The **Identification** window is displayed as shown in the figure below.

   FIGURE 45 Configuring the system identification



3. Type the name of the device in the **Name** field.
4. Type the contact information of the device in the **Contact** field.
5. Type the location of the device in the **Location** field.

6. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

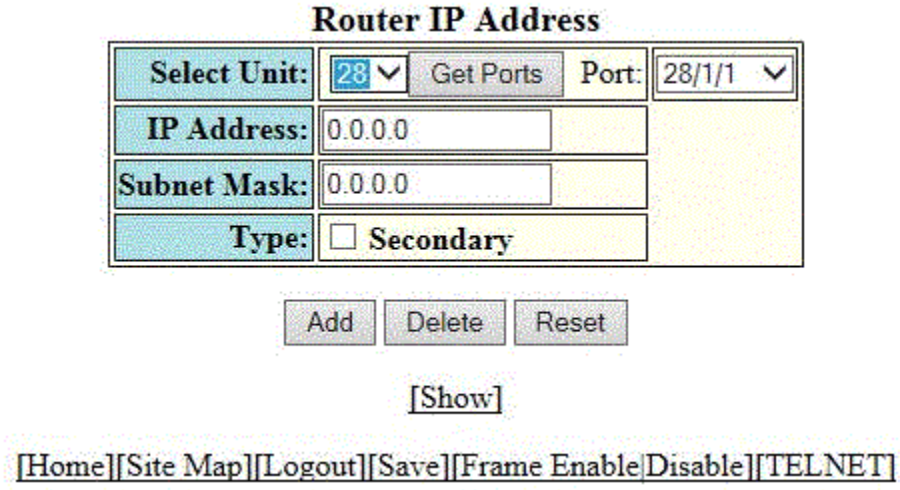
Configuring the system IP address

To configure the IP address of the system, perform the following steps.

1. Click **Configure** on the left pane and select **System** .
2. Click **IP Address** . The **Router IP address** window is displayed.
3. Click **Add IP Address**.

   The **Router IP address** window is displayed as shown in the figure below.

   FIGURE 46 Configuring the system IP address



4. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
5. Select a port from the **Port** list.
6. Type the IP address of the device in the **IP Address** field.
7. Type the network mask for the IP address in the **Subnet Mask** field.
8. Select the **Secondary** check box for **Type** if you have already configured an IP address within the same subnet on the interface.
9. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring a standard ACL

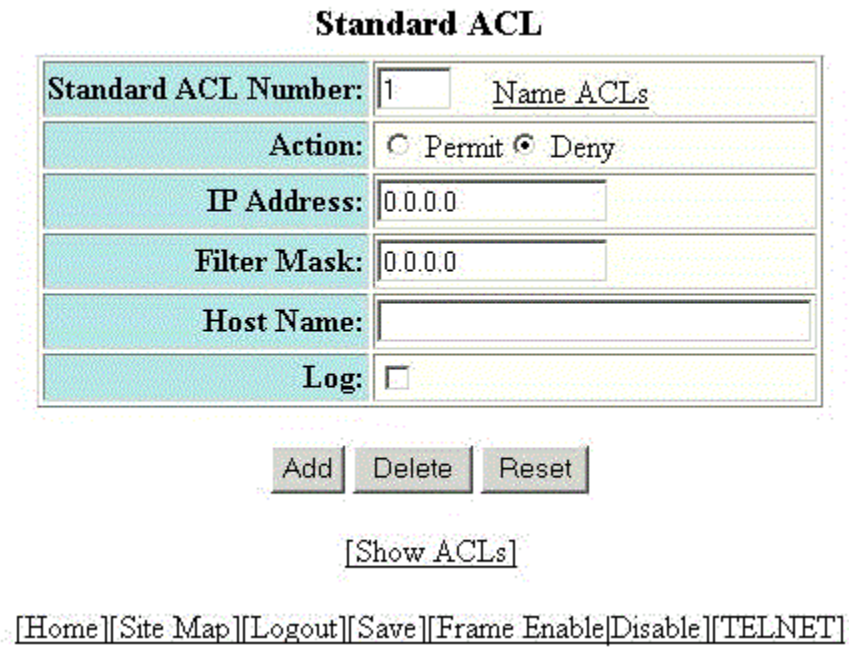
To configure a standard Access Control List (ACL), perform the following steps.

1. Click **Configure** on the left pane and select **System** .
2. Click **Standard ACL** .

   The **Standard ACL** window is displayed as shown in the figure below.

   NOTE
   Web GUI does not have ACL Sequence number support.

   FIGURE 47 Configuring a standard ACL



3. Type the standard ACL number from 1 through 99 in the **Standard ACL Number** field. If you want to type an ACL name, click **Name ACLs** . The field label changes to **Standard ACL Name** .
4. Click **Permit** or **Deny** for **Action** so that the ACL forwards or drops the packets that match the policy in the ACL.
5. Type the IP address of the route's destination in the **IP Address** field.
6. Type the masking bits in the **Filter Mask** field. This allows you to specify a range of IP addresses to include or exclude based on mask matching.
7. Type the host name in the **Host Name** field. The host name enables you to perform Telnet, ping, and trace route commands.
8. Select the **Log** check box to log the entries.
9. Click **Add** .

   The message `The change has been made` is displayed. To display the configured standard ACL, click **Show ACLs** . To delete the configured ACL, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring an extended ACL

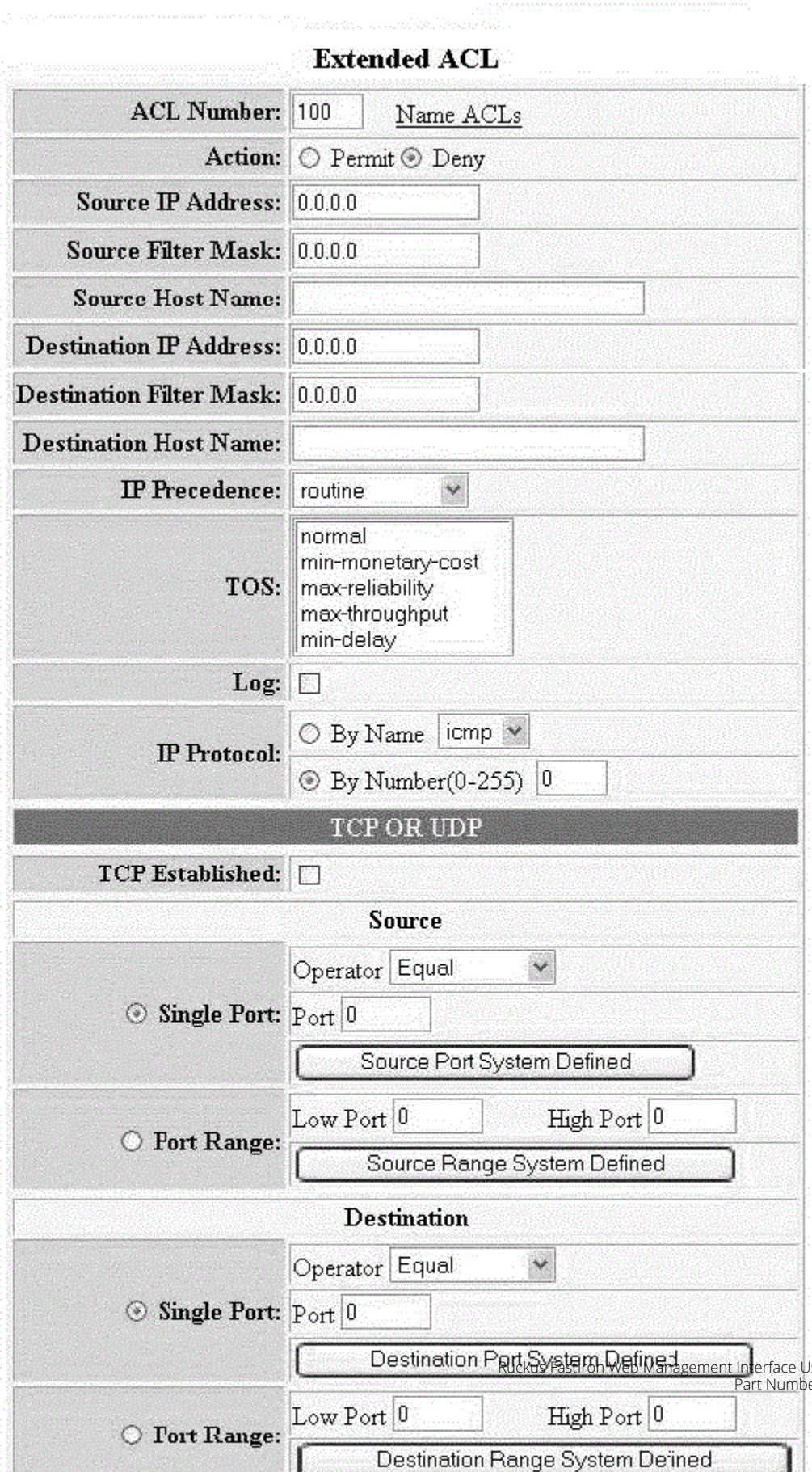
To configure an extended Access Control List (ACL), perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **Extended ACL**.

   The **Extended ACL** window is displayed as shown in the figure below.

FIGURE 48 Configuring an extended ACL



3. Type the extended ACL number (from 100 through 199) in the **ACL Number** field. If you want to specify an extended ACL name, click **Name ACLs**. The field label changes to **ACL Name**.
4. Click **Permit** or **Deny** for **Action** so that the packets that match the policy are forwarded or dropped.
5. Type the source IP address in the **Source IP Address** field.
6. Type the source mask in the **Source Filter Mask** field.
7. Type the source host name in the **Source Host Name** field.
8. Type the destination IP address in the **Destination IP Address** field.
9. Type the destination mask in the **Destination Filter Mask** field.
10. Type the destination host name in the **Destination Host Name** field.
11. Select one of the following options in the **IP Precedence** list:
    - **routine** --The ACL matches packets that have the routine precedence.
    - **priority** --The ACL matches packets that have the priority precedence.
    - **immediate** --The ACL matches packets that have the immediate precedence.
    - **flash** --The ACL matches packets that have the flash precedence.
    - **flash-override** --The ACL matches packets that have the flash override precedence.
    - **critical** --The ACL matches packets that have the critical precedence.
    - **internet** --The ACL matches packets that have the internetwork control precedence.
    - **network** --The ACL matches packets that have the network control precedence.
12. Select one of the following options in the **TOS** list:
    - **normal** --The ACL matches packets that have the normal Type of Service (ToS).
    - **min-monetary-cost** --The ACL matches packets that have the minimum monetary cost ToS.
    - **max-reliability** --The ACL matches packets that have the maximum reliability ToS.
    - **max-throughput** --The ACL matches packets that have the maximum throughput ToS.
    - **min-delay** --The ACL matches packets that have the minimum delay ToS.
13. Select the **Log** check box to enable generation of SNMP traps and syslog messages for packets denied by the ACL.
14. Click **By Name** for I**P Protocol** to select the IP protocol by name or click **By Number** to specify the number (from 0 through 255).
15. Select the **TCP Established** check box so that the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. The policy applies only to the established TCP sessions, not to the new sessions.

    NOTE
    This field applies only to the destination TCP ports, not the source TCP ports.

16. Enter the following information for **Source**:
    a) To configure a single port, click **Single Port**.

       Select one of the following options for **Operator**:

       - **Equal** --The policy applies to the TCP or UDP port number or name you enter.
       - **NotEqual** --The policy applies to all the TCP or UDP port numbers except the port number or port name you enter.
       - **LessThan** --The policy applies to the TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter.
       - **GreaterThan** --The policy applies to the TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter.

       Click **Source Port System Defined**.

    b) To configure a range of ports, click **Port Range**.

       Type the lower port number in the **Low Port** field and the highest port number in the **High Port** field.

       Click **Source Range System Defined**.
17. To configure the destination port settings under **Destination**, follow the procedure explained in step 16 .
18. Click **Add**.

    The message `The change has been made` is displayed. To display the configured extended numbered ACL, click **Show**.

    To delete the configured extended numbered ACL, click **Delete** . To reset the data entered in the configuration pane, click **Reset**.

    NOTE
    Web GUI does not have ACL Sequence number support.

Configuring an IP access group

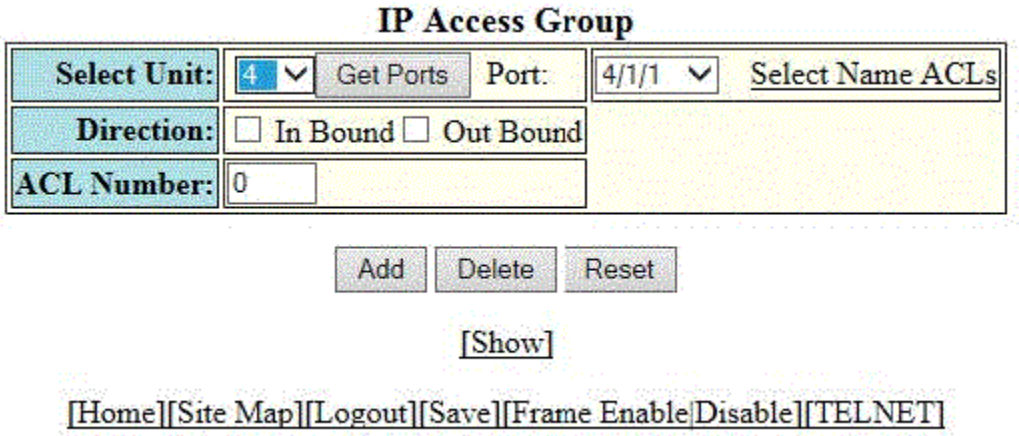
To configure an IP access group, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **IP Access Group**.

   The **IP Access Group** window is displayed as shown in the figure below.

   FIGURE 49 Configuring IP access groups



3. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.

4. Select a port in the **Port** list.
   - stack-unit/slotnum/portnum
5. Select the **In Bound** check box for **Direction** to enable incoming traffic on the interface to which you apply the ACL.
6. Type the ACL number in the **ACL Number** list. If you want to type an ACL name, click **Select Name ACLs**. The field label changes to **ACL Name** . Now, you can type the ACL name up to 256 alphanumeric characters.
7. Click **Add**.

   The message `The change has been made` is displayed. To display the configured IP access group, click **Show**.

   To delete the configured IP access group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring the system MAC filter

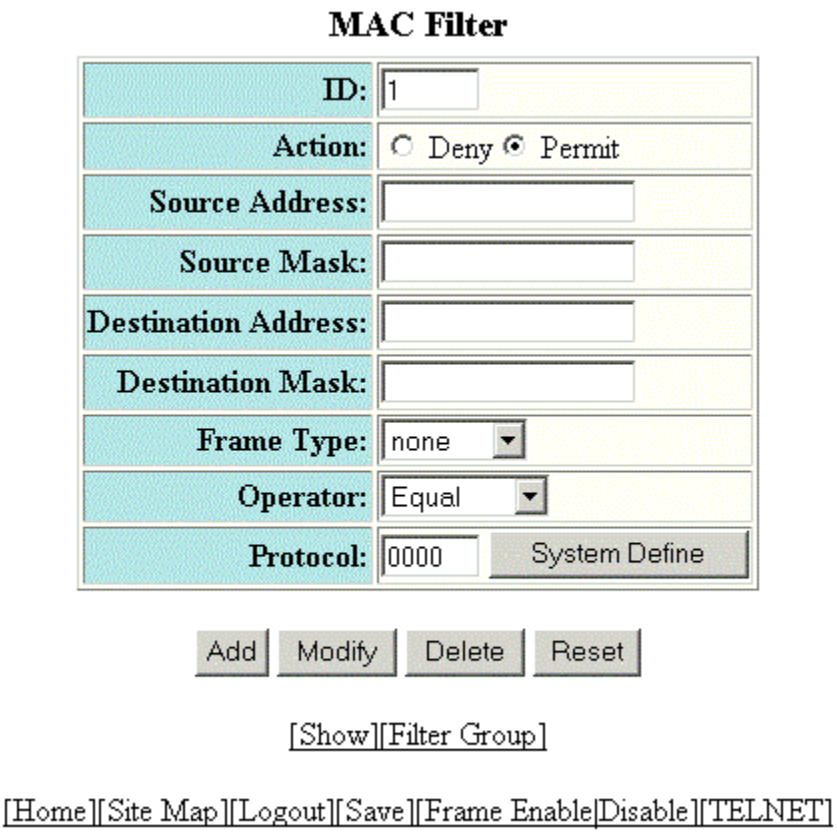
To configure the system MAC filter, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **MAC Filter**.

   The **MAC Filter** window is displayed as shown in the figure below.

   FIGURE 50 Configuring a MAC filter



3. Type the filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action**.
5. Type the source MAC address in xx.xx.xx.xx.xx.xx format in the **Source Address** field.
6. Type the source mask in the **Source Mask** field.
7. Type the destination MAC address in xx.xx.xx.xx.xx.xx format in the **Destination Address** field.
8. Type the destination mask in the **Destination Mask** field.
9. Select the type of frame in the **Frame Type** list.
10. Select the comparison operator in the **Operator** list.
11. Type the protocol identifier in the **Protocol** field. To select the system-defined protocol, click **System Define**.

12. Click **Add**.

    The message `The change has been made` is displayed. To display the configured MAC filter, click **Show**.

    To change the configured MAC filter, click **Modify**. You can also delete the MAC filter by clicking **Delete** . To reset the data entered in the configuration pane, click **Reset**.

    To configure a filter group, click **Filter Group**. For more information on how to configure a filter group, refer to the "Configuring a filter group" section.

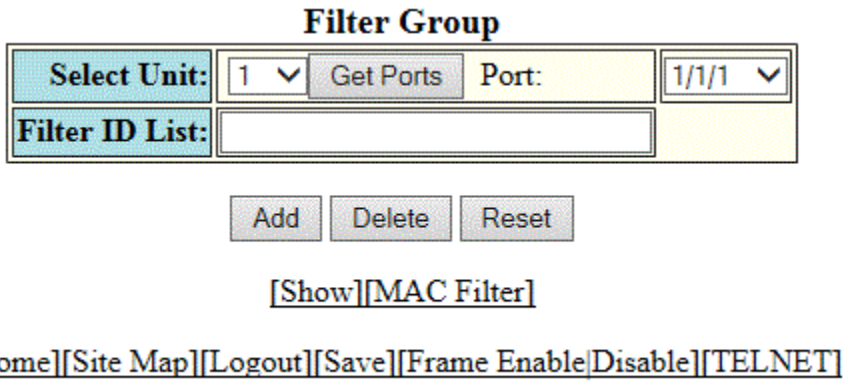
Configuring a filter group

To configure a system filter group, perform the following steps.

1. Click **Filter Group** on the right pane of the **MAC Filter** window.

   The **Filter Group** window is displayed as shown in the figure below.

   FIGURE 51 Configuring a filter group



2. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
3. Select a port number in the **Port** list.
   - stack-unit/slotnum/portnum
4. Type the filter identifier in the **Filter ID List** field.
5. Click **Add**.

   The message `The change has been made` is displayed. To display the configured filter group, click **Show**.

   To delete the configured filter group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

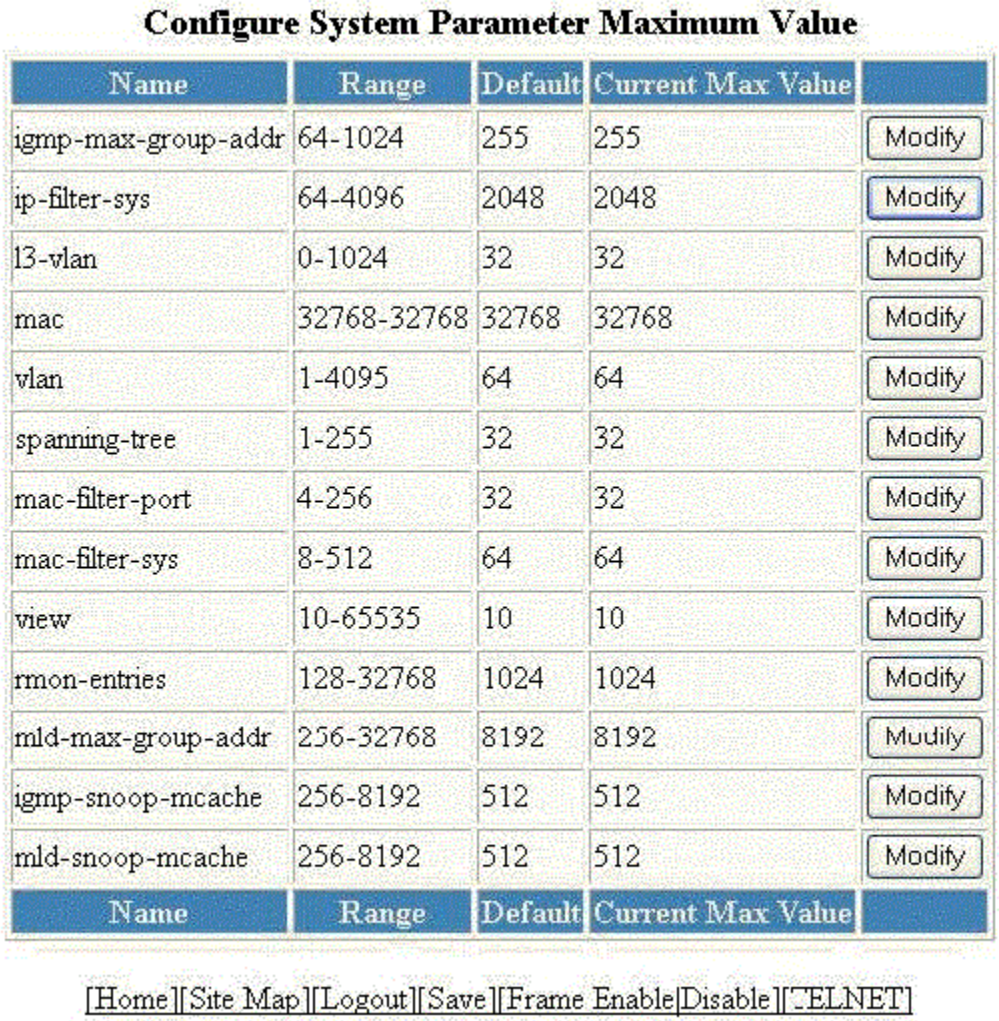
Configuring the maximum system parameter value

To configure the maximum system parameter value, perform the following steps.

1. Click **Configure** on the left pane and select **System** .
2. Click **Max-Parameter** .

   The **Configure System Parameter Maximum Value** window is displayed as shown in the figure below.

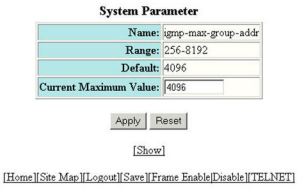
FIGURE 52 Configuring the maximum system parameter



3. To change the values for each system parameter, click **Modify** .

   The **System Parameter** window is displayed as shown in the figure below.

   FIGURE 53 Modifying the maximum parameter value



4. Type the maximum value in the **Current Maximum Value** field.
5. Click **Apply** .

   The message `The change has been made` is displayed. To display the configured maximum system value, click **Show** . To reset the data entered in the configuration pane, click **Reset** .

Configuring a system module

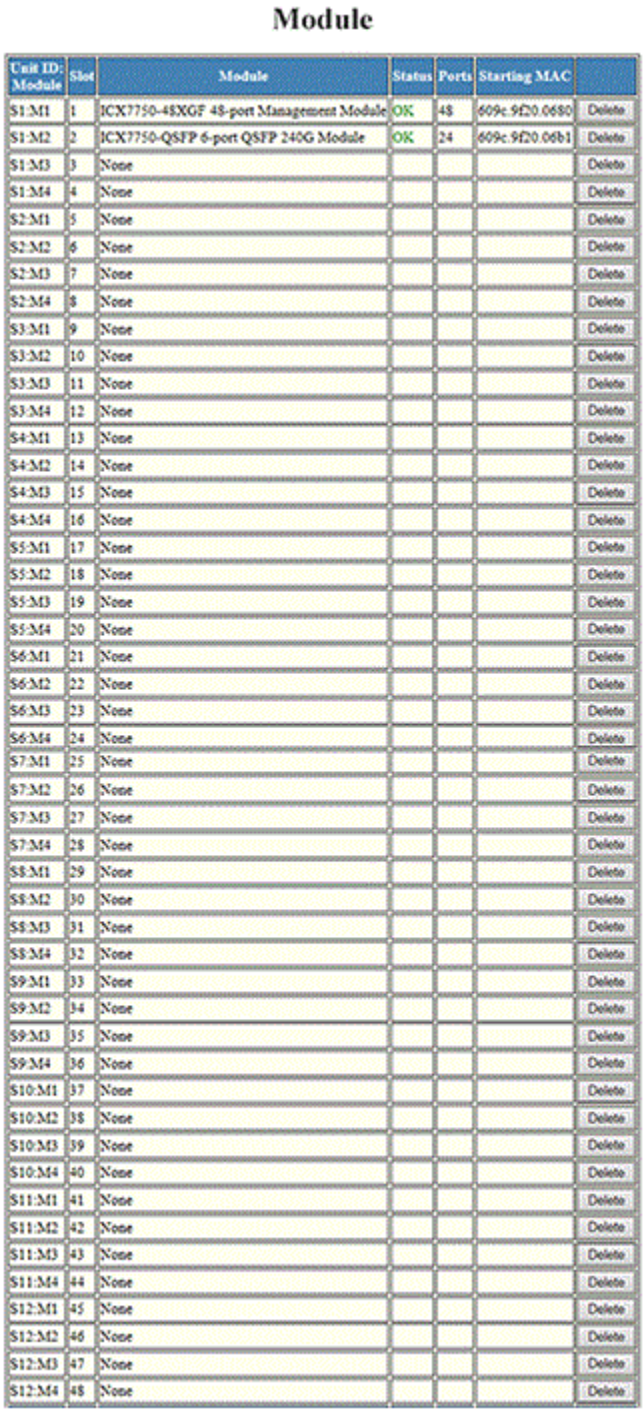
To configure a system module, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **Module**.

   The **Module** window is displayed as shown in the figure below.

FIGURE 54 Configuring system modules



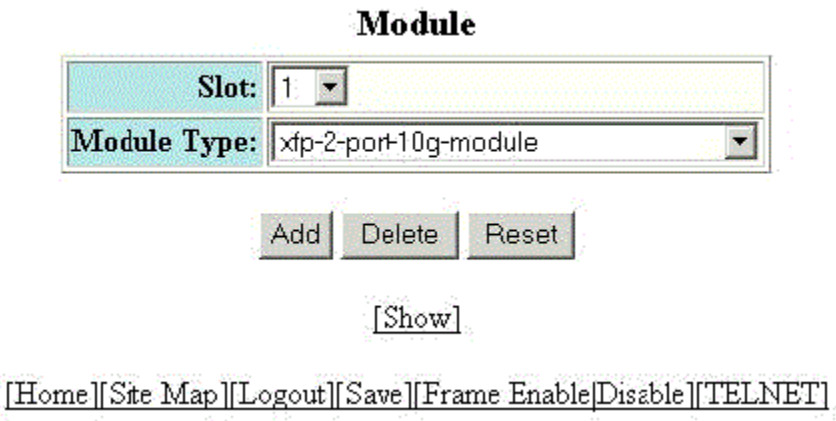
Module

Unit ID: Module	Slot	Module	Status	Ports	Starting MAC	
S1:M1	1	ICX7750-48XGF 48-port Management Module	OK	48	609c.9f20.0680	Delete
S1:M2	2	ICX7750-QSFP 6-port QSFP 240G Module	OK	24	609c.9f20.06b1	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
S9:M1	33	None				Delete
S9:M2	34	None				Delete
S9:M3	35	None				Delete
S9:M4	36	None				Delete
S10:M1	37	None				Delete
S10:M2	38	None				Delete
S10:M3	39	None				Delete
S10:M4	40	None				Delete
S11:M1	41	None				Delete
S11:M2	42	None				Delete
S11:M3	43	None				Delete
S11:M4	44	None				Delete
S12:M1	45	None				Delete
S12:M2	46	None				Delete
S12:M3	47	None				Delete
S12:M4	48	None				Delete

3. Click **Add Module**.

   The **Module** window is displayed as shown in the figure below.

   FIGURE 55 Adding system modules



4. Select a slot number in the **Slot** list.
5. Select a chassis module type in the **Module Type** list.
6. Click **Add**.

   The message `The change has been made` is displayed. To display the configured module, click **Show**.

   To delete the configured module, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a RADIUS server

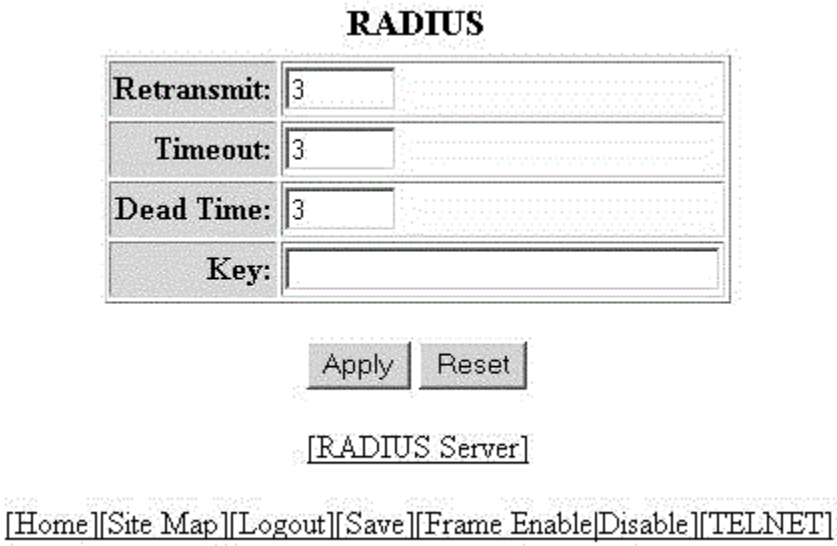
To configure a Remote Authentication Dial In User Service (RADIUS) server, perform the following steps.

1. Click **Configure** on the left pane and select **System** .

2. Click **Radius** .

   The **RADIUS** window is displayed as shown in the figure below.

   FIGURE 56 Configuring a RADIUS server



3. Type the retransmission interval, which specifies how many times the Ruckus device resends an authentication request when the RADIUS server does not respond, in the **Retransmit** field. The range is from 1 through 5 times. The default is 3 times.
4. Type the timeout interval, which specifies how many seconds the Ruckus 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, in the **Timeout** field. The range is from 1 through 15 seconds. The default is 3 seconds.
5. Type the dead interval, which specifies how long the Ruckus device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server, in the **Dead Time** field. The range is from 1 through 5 seconds. The default is 3 seconds.
6. Type the RADIUS key in the **Key** field. This is used to encrypt RADIUS packets before they are sent over the network. The value for the key parameter on the Ruckus device should match the one configured on the RADIUS server. The key can be from 1 through 32 characters in length and cannot include any space characters.
7. Click **Apply** .

   The message `The change has been made` is displayed. To display the configured RADIUS server, click **RADIUS Server** . To reset the data entered in the configuration pane, click **Reset** .

   NOTE
   Web management interface does not support RADIUS configuration using ssl-auth-port.

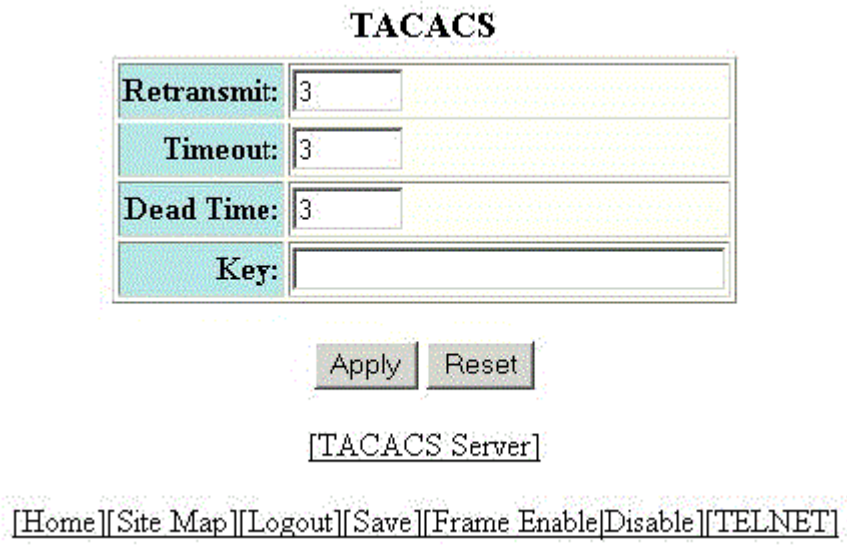
Configuring a TACACS/TACACS+ server

To configure a TACACS/TACACS+ server, perform the following steps.

1. Click **Configure** on the left pane and select **System** .
2. Click **Tacacs** .

   The **TACACS** window is displayed as shown in the figure below.

   FIGURE 57 Configuring a TACACS/TACACS+ server



3. Type the retransmission interval, which specifies how many times the Ruckus device resends an authentication request when the TACACS/TACACS+ server does not respond, in the **Retransmit** field. The range is from 1 through 5 times. The default is 3 times.
4. Type the timeout interval, which specifies how many seconds the Ruckus 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, in the **Timeout** field. The range is from 1 through 15 seconds. The default is 3 seconds.
5. Type the dead interval, which specifies how long the Ruckus device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server, in the **Dead Time** field. The range is from 1 through 5 seconds. The default is 3 seconds.
6. Type the TACACS/TACACS+ key in the **Key** field. This is used to encrypt TACACS/TACACS+ packets before they are sent over the network. The value for the key parameter on the Ruckus device should match the one configured on the TACACS/TACACS+ server. The key can be from 1 through 32 characters in length and cannot include any space characters.
7. Click **Apply** .

   The message `The change has been made` is displayed. To display the configured TACACS/TACACS+ server, click **TACACS Server** . To reset the data entered in the configuration pane, click **Reset** .

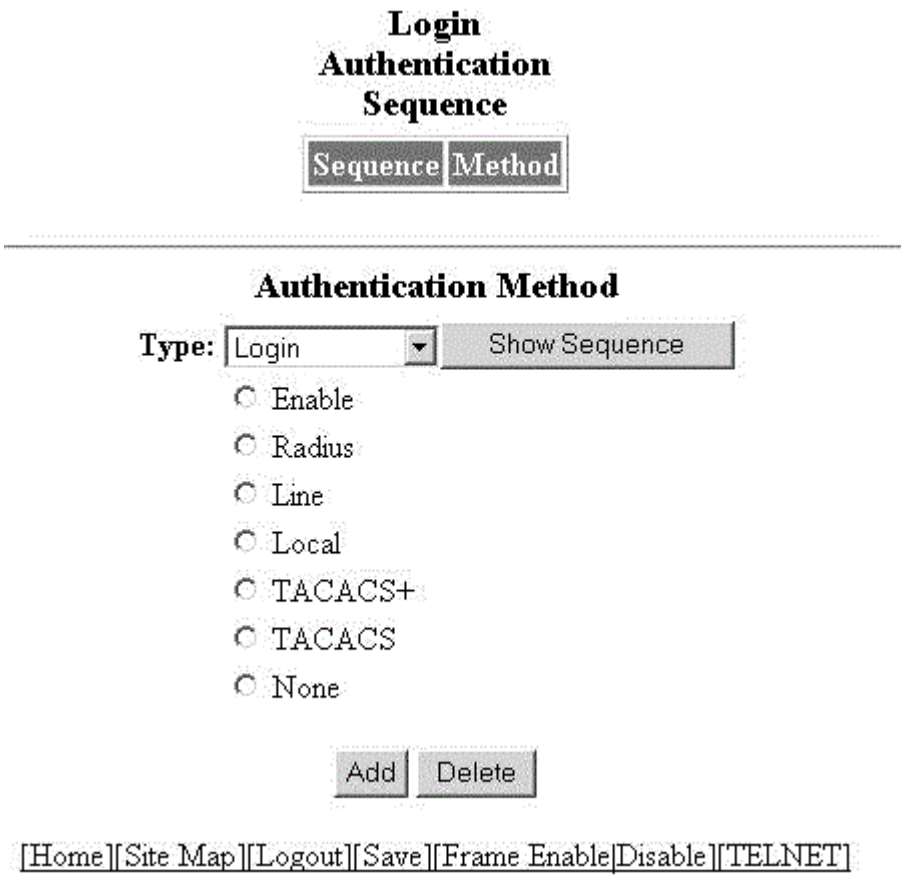
Configuring management authentication

To configure management authentication, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Authentication Methods**.

   The **Authentication Method** window is displayed as shown in the figure below.

   FIGURE 58 Configuring management authentication



3. Select one of the following types of authentication in the **Type** list:
   - **Login**
   - **Enable**
   - **Web Server**
   - **SNMP Server**

4. Click one of the following servers:
   - **Enable**
   - **Radius**
   - **Line**
   - **Local**
   - **TACACS+**
   - **TACACS**
   - **None**
5. Click **Add**.

   The message `The change has been made` is displayed and the configured authentication method is listed in the **Login Authentication Sequence** pane. Click **Show Sequence** to display the list of authentication methods added. To remove the configured management authentication, click **Delete**.

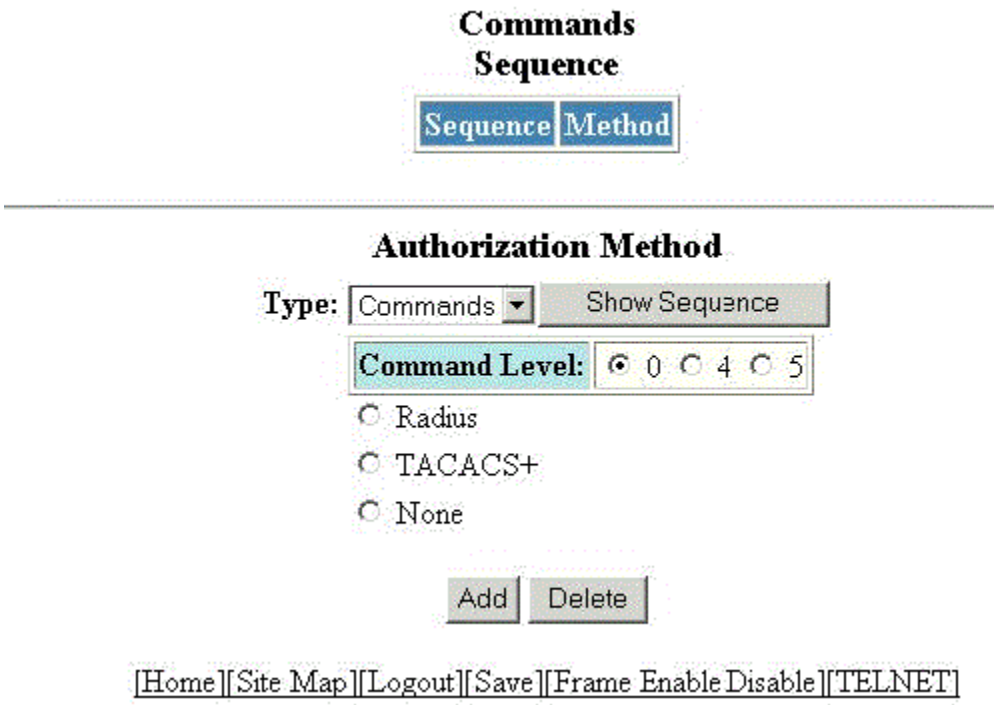
Configuring management authorization

To configure management authorization, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Authorization Methods**.

   The **Authorization Method** window is displayed as shown in the figure below.

FIGURE 59 Configuring management authorization



3. Select either of the following modes of authorization in the **Type** list:
   - **Commands**
   - **Exec**
4. Click **0** or **4** or **5** for **Command Level**.
5. Click one of the following servers:
   - **Radius**
   - **TACACS+**
   - **None**
6. Click **Add**.

   The message `The change has been made` is displayed and the configured authorization method is listed in the **Commands Sequence** pane. Click **Show Sequence** to display the list of authentication methods added. To delete the configured management authorization, click **Delete**.

Configuring management accounting

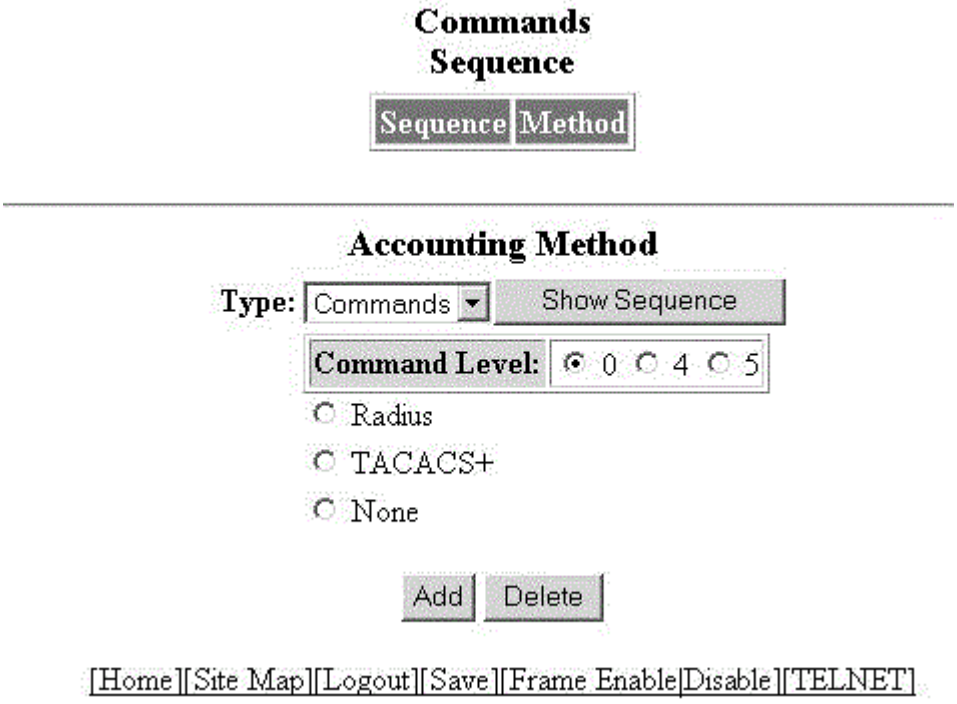
To configure management accounting, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **Management** and select **Accounting Methods**.

   The **Accounting Method** window is displayed as shown in the figure below.

   FIGURE 60 Configuring management accounting methods



3. Select one of the following modes of authorization:
   - **Commands**
   - **Exec**
   - **System**
4. Click **0** or **4** or **5** for **Command Level** .
5. Click one of the following servers:
   - **Radius**
   - **TACACS+**
   - **None**
6. Click **Add**.

   The message `The change has been made` is displayed and the configured accounting method is listed in the **Commands Sequence** pane. To delete the configured accounting method, click **Delete**.

Configuring an SNMP community string

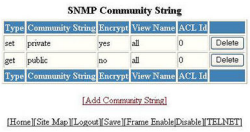
To configure an SNMP community string, perform the following steps.

NOTE
SNMP community string is not supported if FIPS mode is enabled.

1. Click **Configure** on the left pane and select **System** .
2. Click **Management** and select **Community String.**

   The **SNMP Community String** window is displayed as shown in the figure below.

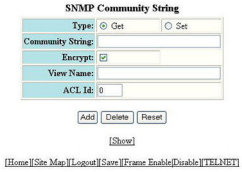
   FIGURE 61 Configuring an SNMP community string



3. Click **Add Community String** .

   The **SNMP Community String** window is displayed as shown in the figure below.

   FIGURE 62 Adding community strings



4. Click **Get** or **Set** for **Type** .
5. Type the user name to open a web management session in the **Community String** field.
6. Select the **Encrypt** check box to enable encryption for a particular string.
7. Type the name of the community string in the **View Name** field.
8. Type the ACL number in the **ACL Id** field.
9. Click **Add** .

   The message `The change has been made` is displayed. To display the configured community string, click **Show** .

   To delete the community string, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring the general management parameters

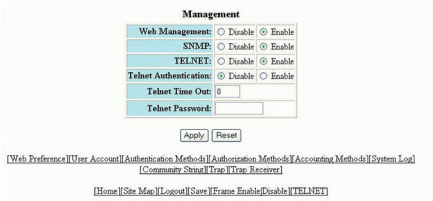
To configure the general management parameters, perform the following steps.

1. Click **Configure** on the left pane and select **System** .

2. Click **Management** and select **General** .

   The **Management** window is displayed as shown in the figure below.

   FIGURE 63 Configuring general management parameters



3. Click **Disable** or **Enable** for **Web Management** .
4. Click **Disable** or **Enable** for **SNMP** .
5. Click **Disable** or **Enable** for **TELNET** .
6. Click **Disable** or **Enable** for **Telnet Authentication** .
7. Type the timeout interval in seconds to wait for a response in the **Telnet Time Out** field.
8. Type an alphanumeric password in the **Telnet Password** field.
9. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

   The **Management** window provides links to configure other management parameters:

   - To configure the web management preferences, click **Web Preference** . For more information, refer to Configuring the web management preferences on page 131.
   - To configure a management user account, click **User Account** . For more information, refer to Configuring a management user account on page 131.
   - To configure management authentication, click **Authentication Methods** . For more information, refer to Configuring management authentication on page 120.
   - To configure management authorization, click **Authorization Methods** . For more information, refer to Configuring management authorization on page 121.
   - To configure management accounting, click **Accounting Methods** . For more information, refer to Configuring management accounting on page 122.
   - To configure a system module, click **System** . For more information, refer to Configuring a system module on page 115.
   - To configure an SNMP community string, click **Community String** . For more information, refer to Configuring a system module on page 115.
   - To configure a trap, click **Trap** . For more information, refer to Configuring a trap on page 128.
   - To configure a trap receiver, click **Trap Receiver** . For more information, refer to Configuring a trap receiver on page 129.

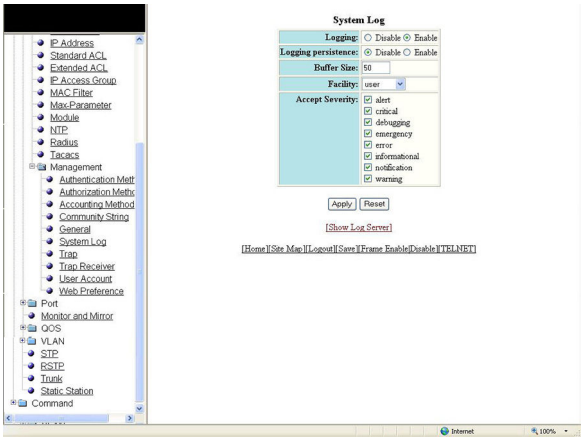
Configuring a management system log

To configure a management system log, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **System Log**.

   The **System Log** window is displayed as shown in the figure below.

   FIGURE 64 Configuring a system log



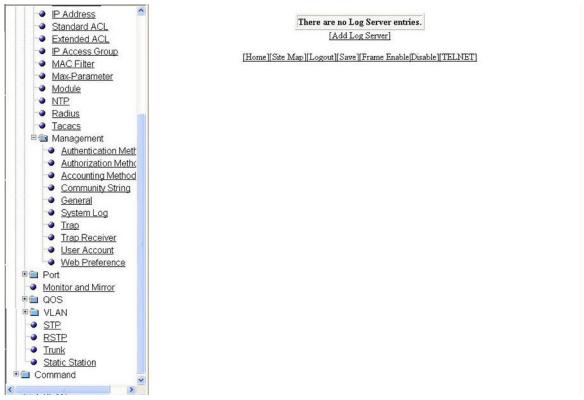
3. Click **Disable** or **Enable** for **Logging**. By default, the syslog buffer is enabled.
4. Click **Disable** or **Enable** for **Logging persistence**. By default, logging persistence is disabled.
5. Type the number of messages in the **Buffer Size** field.
6. Select a facility in the **Facility** list.
7. Select one of the following severity levels for **Accept Severity**:
   - **alert**
   - **critical**
   - **debugging**
   - **emergency**
   - **error**
   - **informational**
   - **notification**
   - **warning**

8. Click **Apply** .

   The message `The change has been made` is displayed. To display log server entries, click **Show Log Server**. To reset the data entered in the configuration pane, click **Reset**.

   If there are no log servers, the message `There are no Log Server entries` is displayed as shown in the figure below.

FIGURE 65 Viewing log server entries



To add extra log servers to your system log configuration, perform the following steps.

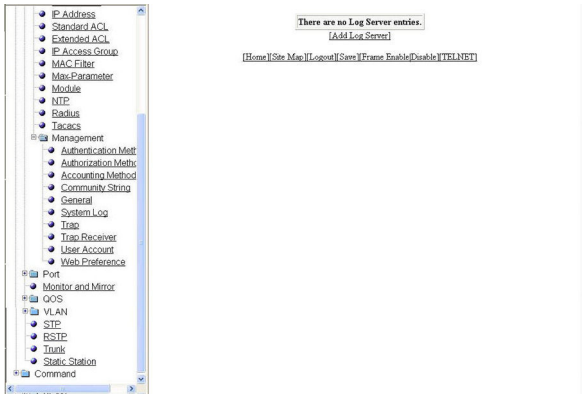
Adding a log server

To add a log sever, perform the following steps.

1. Click **Add Log Server**.

   The **System Log Server** window is displayed as shown in the figure below.

FIGURE 66 Adding a Log Server



2. Click **ipv4** or **ipv6** and then type the IPv4 or IPv6 address in the **Server IP Address** field.
3. Type the application port that can be used for the syslog facility in the **Server Udp Port** field. The default value is 514.

4. Click **Add** .

   The message `The change has been made` is displayed. To display the log server entries, click **Show Log Server** . To display the system log window, click **Show System Log** .

   To delete the changes made, click **Delete**. To reset the data entered in the configuration pane **Reset**.

Configuring a trap

To configure a trap, perform the following steps.

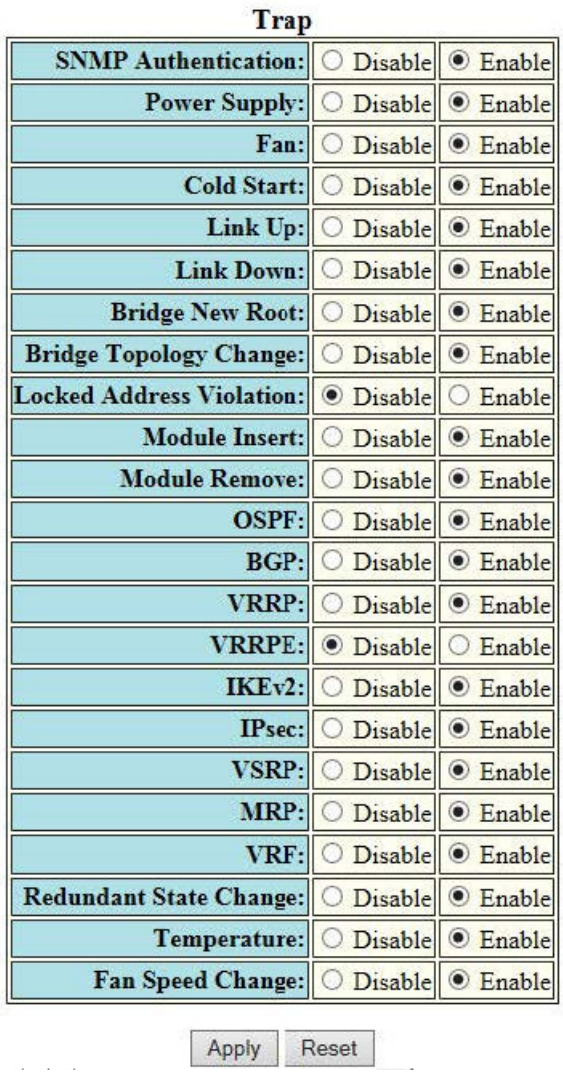
NOTE
Trap cannot be configured if FIPS mode is enabled.

1. Click **Configure** on the left pane and select **System** .

2. Click **Management** and select **Trap** .

   The **Trap** window is displayed as shown in the figure below.

   FIGURE 67 Configuring a trap



3. Click **Disable** or **Enable** for each trap.
4. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring a trap receiver

To configure a trap receiver, perform the following steps.

NOTE
Trap receiver cannot be configured if FIPS mode is enabled.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Trap Receiver**.

   The **Trap Receiver** window is displayed as shown in the figure below.

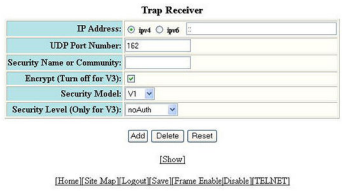
   FIGURE 68 Configuring a trap receiver



3. Click **Add Trap Receiver** to configure a new trap receiver.

   The **Trap Receiver** window is displayed as shown here.

   FIGURE 69 Adding a new trap receiver



4. Click **ipv4** or **ipv6** and then type the IP address of the destination of the route in the **IP Address** field.
5. Type the UDP port number of the host that will receive the trap in the **UDP Port Number** field.
6. Type an arbitrary value made of two five-digit integers joined by a colon in the **Security Name or Community** field. Each string in the community name can be a number from 0 through 65535.
7. Select the **Encrypt (Turn off for V3)** check box to enable or disable encryption for a particular string. It is turned off for V3.
8. Select one of the following options in the **Security Model** list:
   - **V1**
   - **V2C**
   - **V3**
9. For V3 only, select one of the following options in the **Security Level (Only for V3)** list:
   - **noAuth** --Allow all packets.
   - **authNoPriv** --Allow only authenticated packets.
   - **authPriv** --A password is required.
10. Click **Add**.

    The message `The change has been made` is displayed. To view the trap receiver entries, click **Show**.

    To delete the trap receiver, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a management user account

To configure a management user account, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **User Account**.

   The **User Account** window is displayed as shown in the figure below.

   FIGURE 70 Configuring a management user account



3. Type the user identifier in the **Username** field.
4. Type the login password in the **Password** field.
5. Select one of the following options in the **Privilege** list:
   - **0 (Read-Write)**
   - **4 (Port-Config)**
   - **5 (Read-Only)**
6. Click **Add**.

   The message `The change has been made` is displayed. To view the configured user account, click **Show**.

   To delete the configured user account, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring the web management preferences

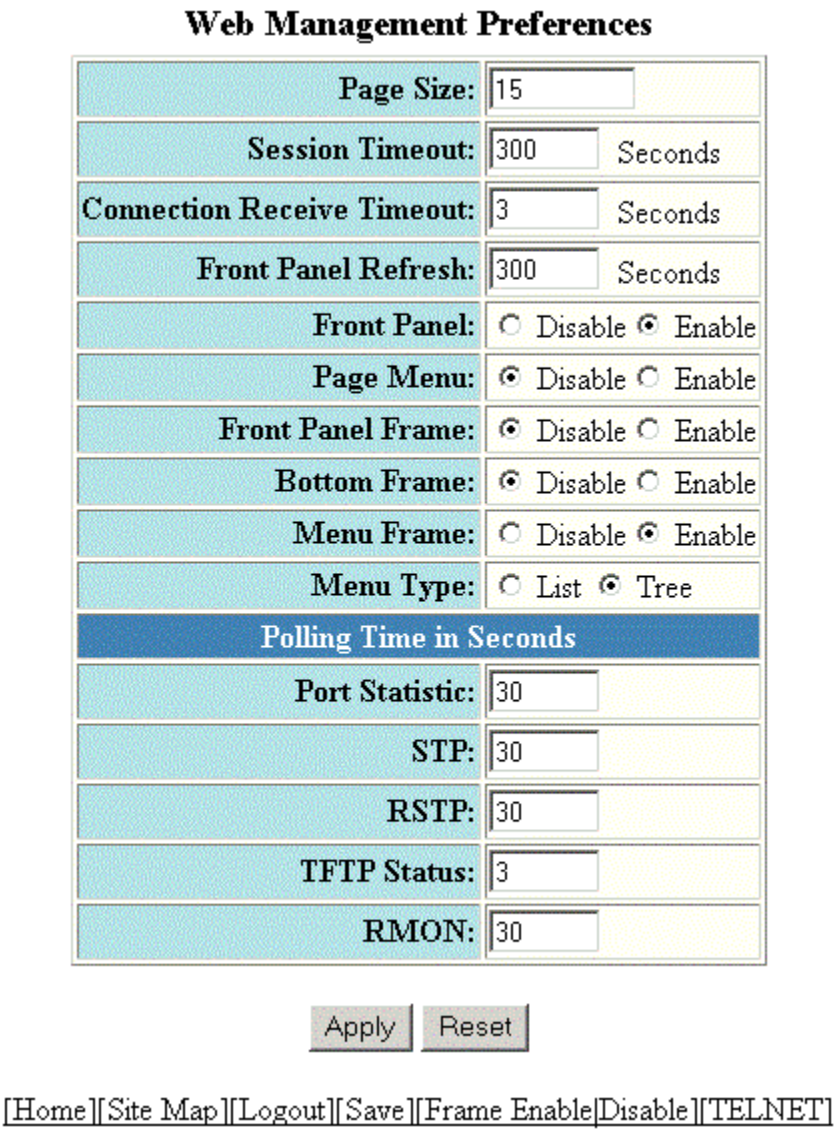
To configure the web management preferences, perform the following steps.

1. Click **Configure** on the left pane and select **System**.

2. Click **Management** and select **Web Preference**.

   The **Web Management Preferences** window is displayed as shown in the figure below.

   FIGURE 71 Configuring the web management preferences



3. Type the page size in the **Page Size** field.
4. Type the console session timeout value in seconds in the **Session Timeout** field.
5. Type the wait time interval after getting disconnected from the application in the **Connection Receive Timeout** field.
6. Type the number of seconds after which the front panel gets refreshed in the **Front Panel Refresh** field.
7. Click **Disable** or **Enable** for **Front Panel**. By default, it is enabled and the ports are labelled on the front panel of the devices.
8. Click **Disable** or **Enable** for **Page Menu**.

9. Click **Disable** or **Enable** for **Front Panel Frame**.
10. Click **Disable** or **Enable** for **Bottom Frame**.
11. Click **Disable** or **Enable** for **Menu Frame**.
12. Click **List** or **Tree** for **Menu Type**.
13. Type the port statistics polling time in the **Port Statistic** field.
14. Type the STP statistics polling time in the **STP** field.
15. Type the TFTP polling time in seconds in the **TFTP Status** field.
16. Type the polling time for Remote Monitoring in the **RMON** field.
17. Click **Apply**.

    The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset**.

Configuring Port Parameters

- Configuring an Ethernet port....135
- Configuring port inline power....138
- Configuring a management port....139
- Configuring the port uplink relative utilization....140

Configuring an Ethernet port

To configure an Ethernet port, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.
2. Click **Ethernet**.

   The **ETHERNET Port Configuration** window is displayed as shown in the figure below.

   FIGURE 72 Configuring an Ethernet port



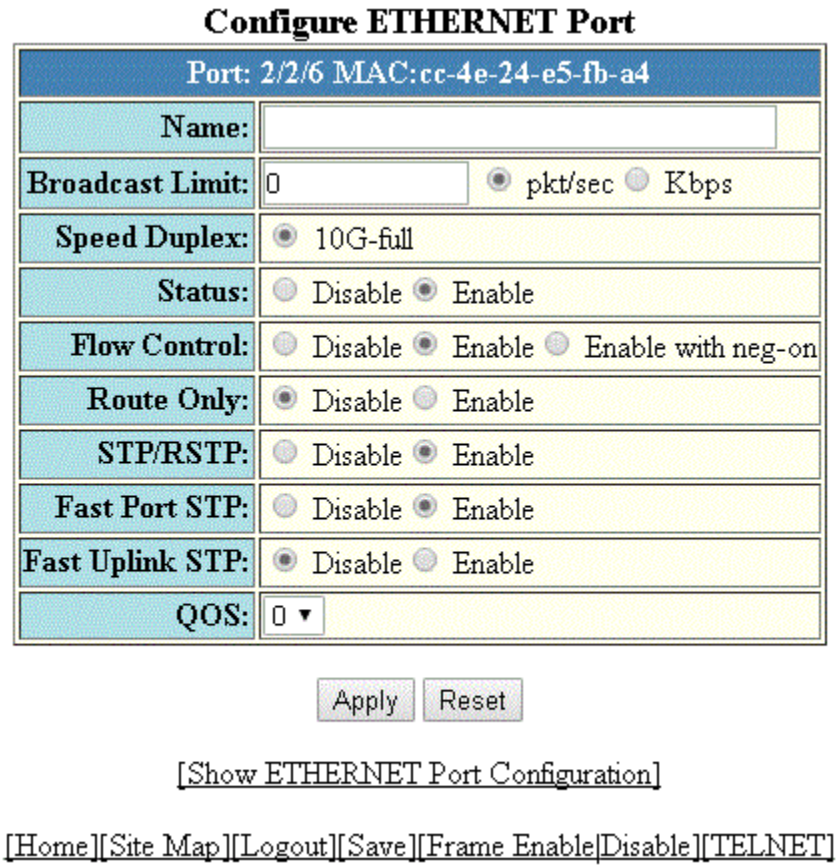
Port	Actual speed/ mode	Configured speed/ mode	QOS	Lock Addr	Tag	STP/RSTP	Fast STP	Fast Uplink	BroadCast limit	Flow Ctrl	Gig Default	Route Only	Trunk	LRM Adapter	
2/1/48	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
2/2/2	None	1G-full-master	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
2/2/4	None	1G-full-master	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
2/2/5	None	1G-full-master	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
2/2/6	10G-full	10G-full	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Enabled	Modify
2/2/7	10G-full	10G-full	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Enabled	Modify
2/2/8	None	1G-full-master	0	Disable	Disabled	Enabled	Enabled	Disabled	0 Packets	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify

   If LRM adapter is present, the status is displayed as **Enabled**.
3. Select a unit ID in the **Select Unit ID** list and click **Display** to display the information about a specific stack unit.

4. Click **Modify** to modify the respective Ethernet port.

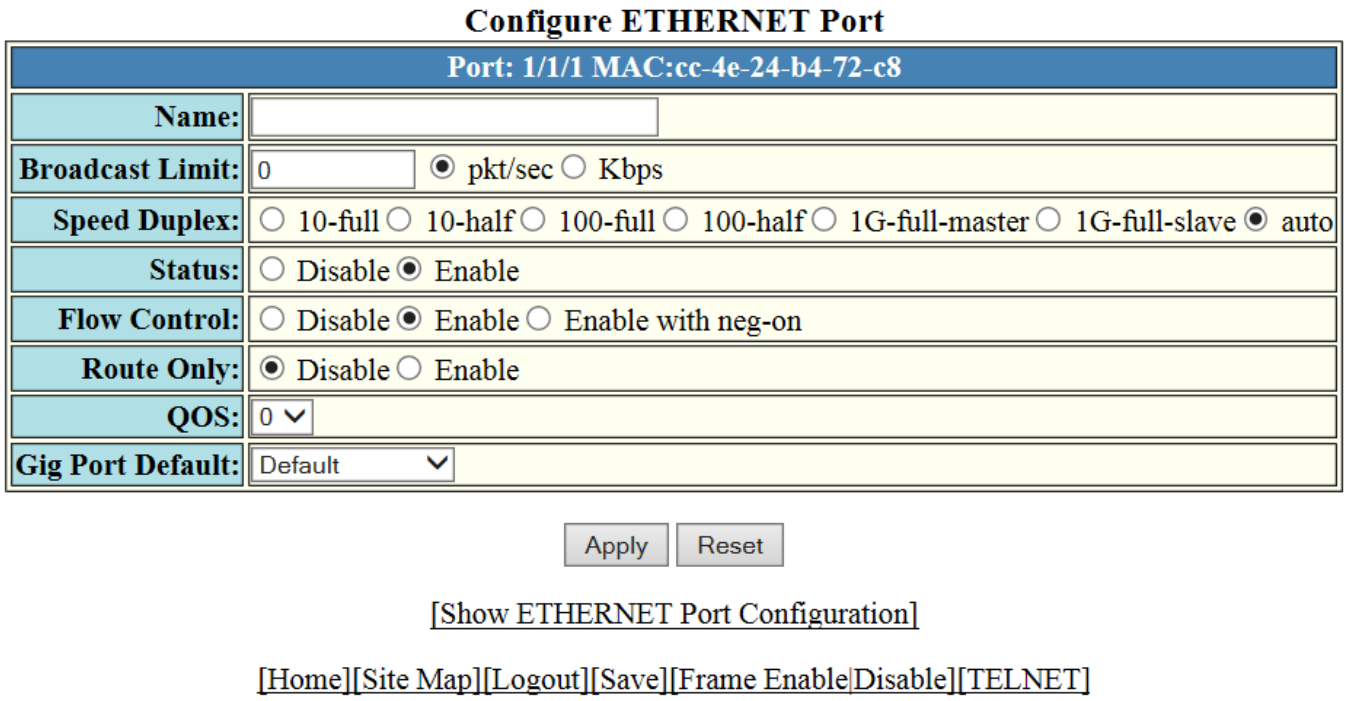
   The **Configure ETHERNET Port** window is displayed as shown in the figure below. The following window is of an Ethernet port for which LRM adapter is enabled.

   FIGURE 73 Modifying the port settings of port with LRM adapter



   For other interfaces, the following window is displayed.

FIGURE 74 Modifying the port settings of an Ethernet port without LRM adapter



5. Type the name of the Ethernet port in the **Name** field.
6. Select the type of the port speed for **Speed Duplex**, which can be one of the following:

   NOTE
   Only 10G-full is supported for Ethernet interface with LRM adapter.

   - **10-full** --10 Mbps, full duplex
   - **10-half** --10 Mbps, half duplex
   - **100-full** --100 Mbps, full duplex
   - **100-half** --100 Mbps, half duplex
   - **1G-full-master** --1 Gbps, full duplex master
   - **1G-full-slave** --1 Gbps, full duplex slave
   - **auto** --Auto-negotiation
7. Click **Disable** or **Enable** for **Status** to disable or enable an Ethernet port.
8. Click **Disable** or **Enable** or **Enable with neg-on** for **Flow Control** . By default, flow control is enabled.
9. Click **Disable** or **Enable** for **Lock Address** . If you click **Enable** , type the number of devices that can have access to a specific port in the **Addr-count** field.
10. Click **Disable** or **Enable** for **Route Only**. If you click **Enable** , Layer 2 switching is disabled globally.
11. Click **Disable** or **Enable** to disable/enable **STP/RSTP**.
12. Click **Disable** or **Enable** to disable/enable **Fast Port STP**.
13. Click **Disable** or **Enable** to disable/enable **Fast Uplink STP**.
14. Select the QoS priority for the port in the **QOS** list.

15. Click **Apply**.

    The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset**.

    To display the **ETHERNET Port Configuration** window, click **Show ETHERNET Port Configuration** .

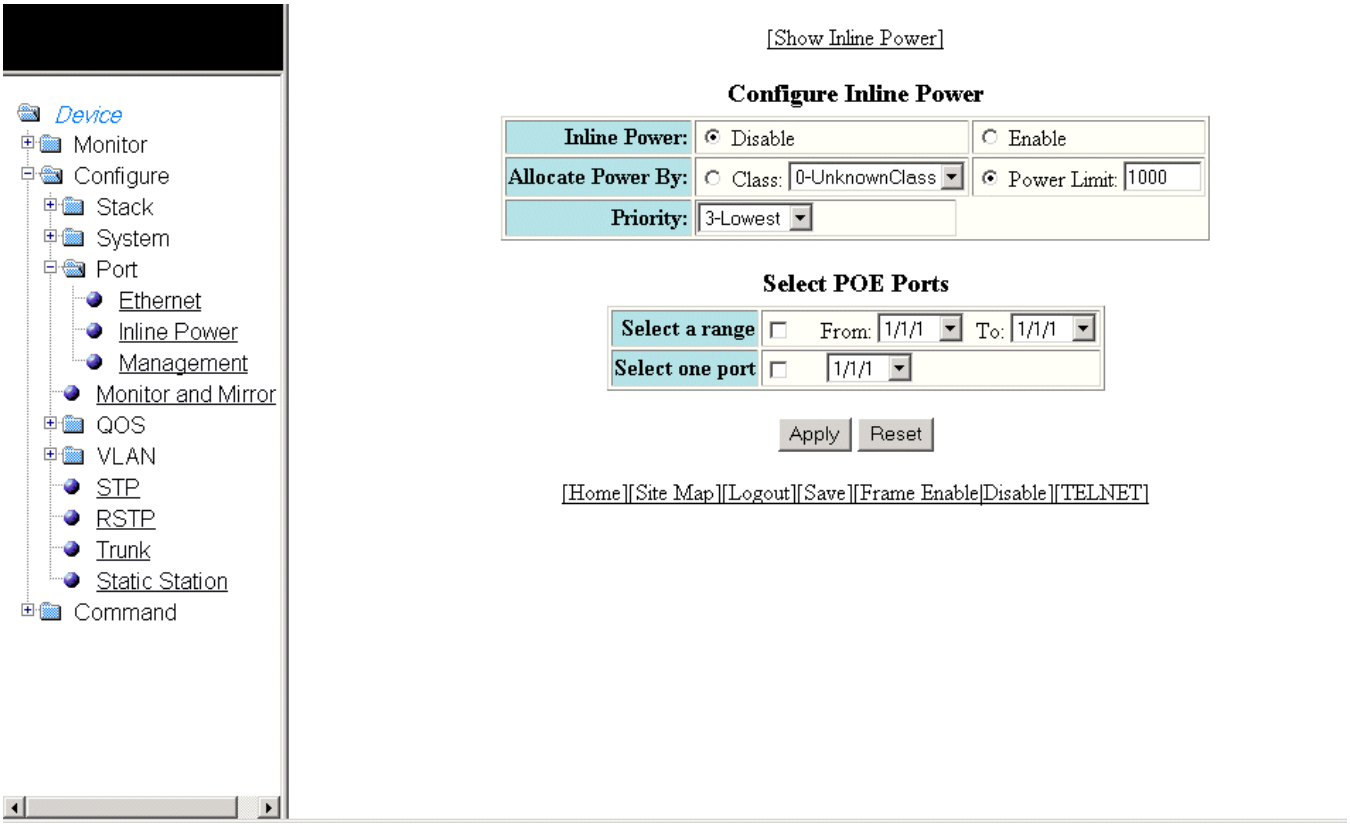
Configuring port inline power

To configure port inline power, perform the following steps.

1. Click **Configure** on the left pane and select **Port** .
2. Click **Inline Power** .

   The **Configure Inline Power** window is displayed as shown in the figure below.

   FIGURE 75 Configuring port inline power



3. Click **Disable** or **Enable** for **Inline Power** .
4. Click **Class** for **Allocate Power By** and then select a power class in the **Class** list, or click **Power Limit** and then type the maximum power level for a power-consuming device in the **Power Limit** field.
5. Select an inline power priority for a Power over Ethernet (PoE) port in the **Priority** list.
6. To select the PoE ports, select the **Select a range** check box and select the range of ports in the **From** and **To** lists, or select the **Select one port** check box and select the port in the list.

7. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

   To display the inline power statistics and details, click **Show Inline Power** . For more information, refer to Displaying port inline power for Ruckus ICX devices on page 52.

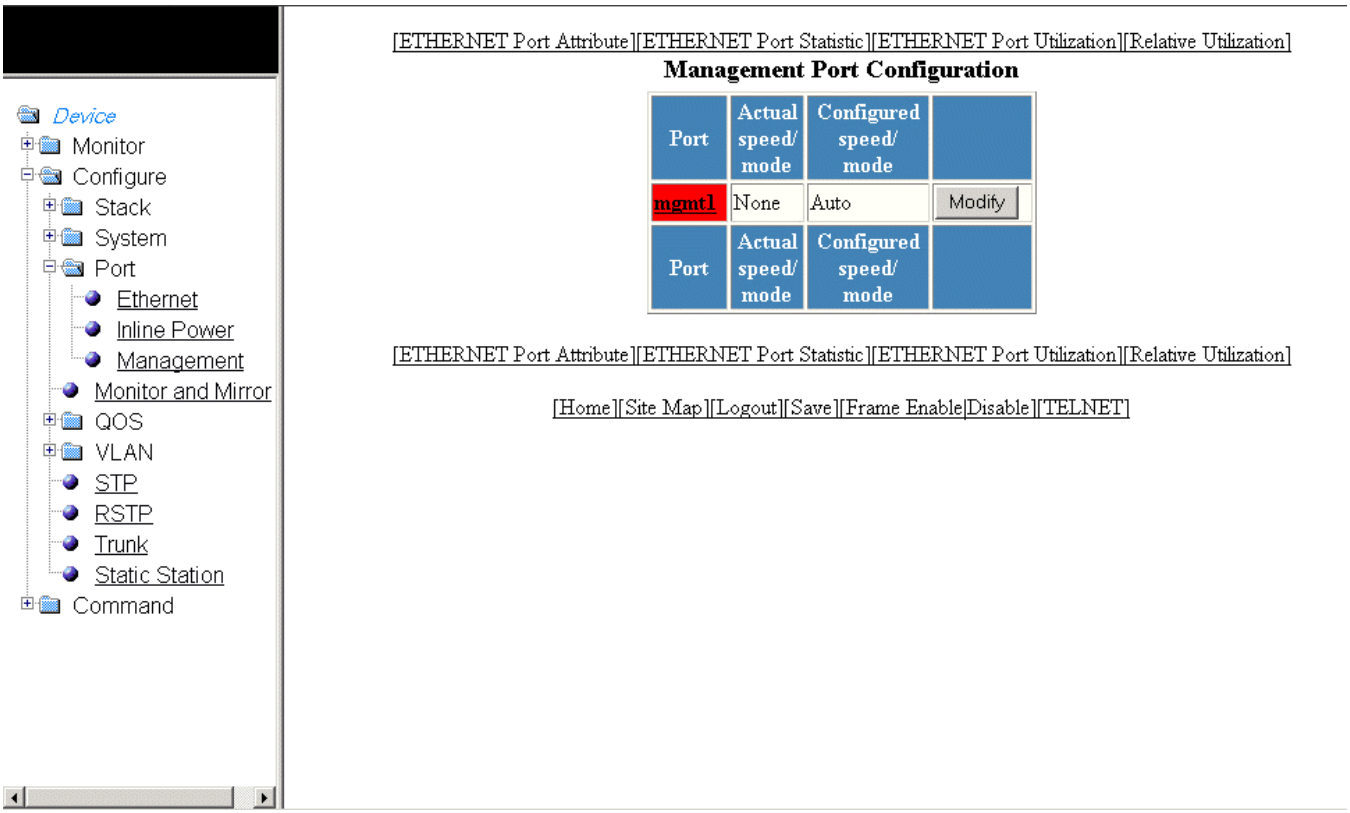
Configuring a management port

To configure a management port, perform the following steps.

1. Click **Configure** on the left pane and select **Port** .
2. Click **Management** .

   The **Management Port Configuration** window is displayed as shown in the figure below.

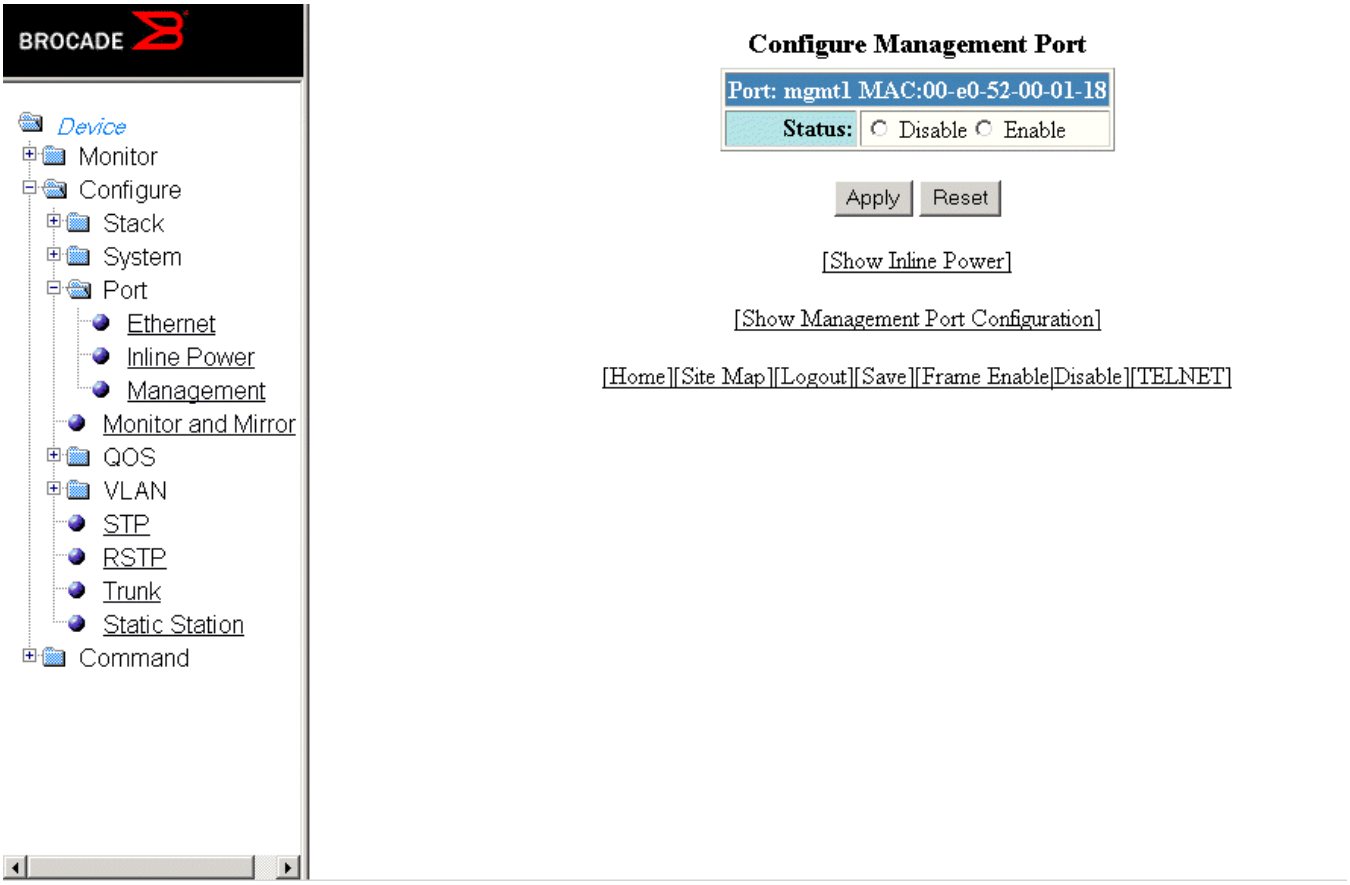
FIGURE 76 Management port configuration



3. Click **Modify** .

   The **Configure Management Port** window is displayed as shown in the figure below.

   FIGURE 77 Configuring a management port



4. Click **Disable** or **Enable** for **Status** .
5. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

   To display the configured management port information, click **Show Management Port Configuration** .

   To display the inline power statistics and details, click **Show Inline Power** . For more information, refer to Displaying port inline power for Ruckus ICX devices on page 52.

Configuring the port uplink relative utilization

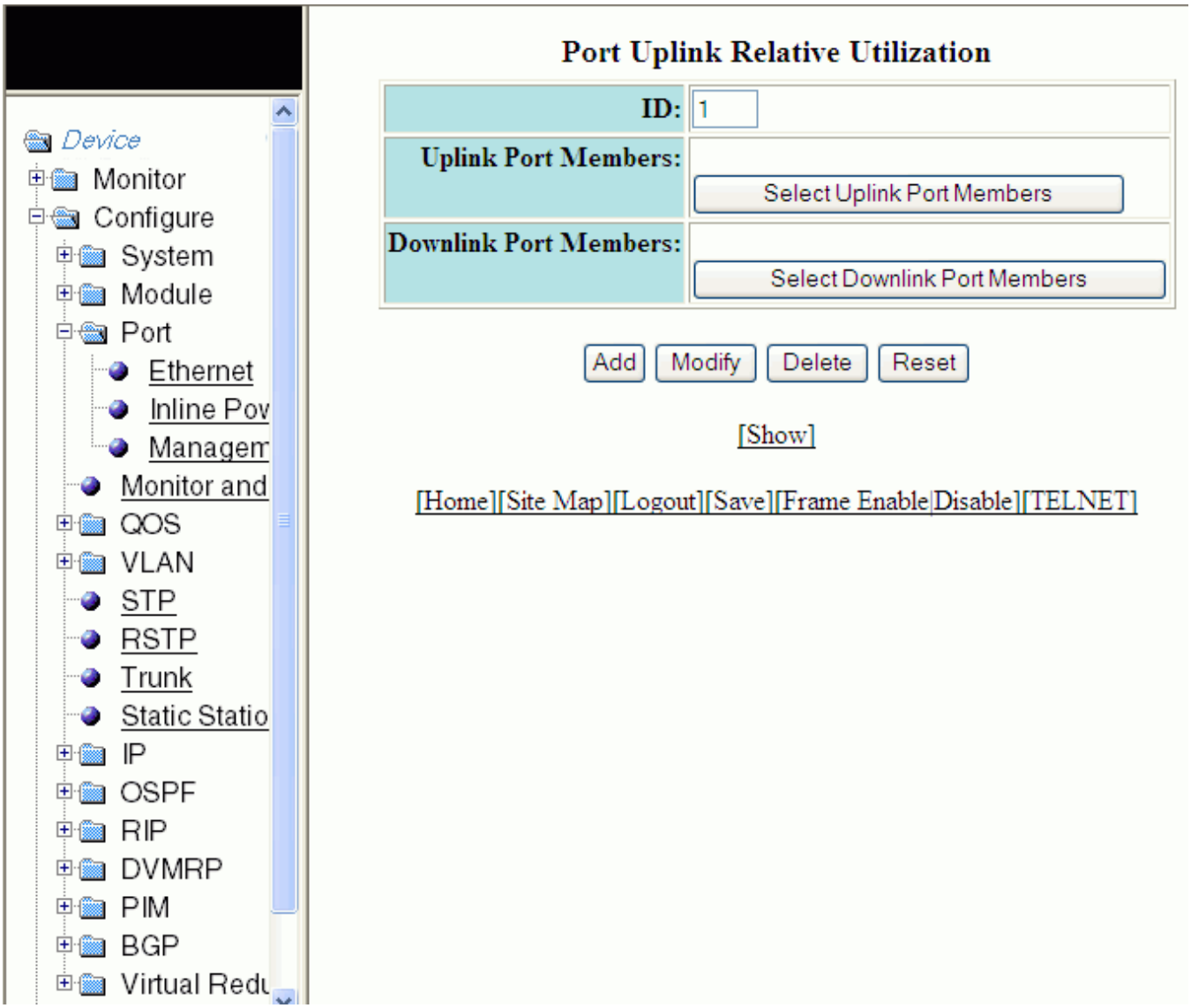
To configure the port uplink utilization list, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.

2. Click **Relative Utilization** on the **ETHERNET Port Configuration**, **Configure Inline Power**, or **Management Port Configuration** window.

   The **Port Uplink Relative Utilization** window is displayed as shown in the figure below.

FIGURE 78 Configuring the port uplink relative utilization



3. Type the uplink utilization list number (from 1 through 4) in the **ID** field.
4. Click **Select Uplink Port Members** to select the uplink ports.
5. Click **Select Downlink Port Members** to select the downlink ports.
   - stack-unit/slotnum/portnum

6. Click **Add**.

   The message `The change has been made` is displayed. To display the configured port uplink utilization list, click **Show**.

   To modify the configured port uplink utilization list, click **Modify**. You can also delete the configured port uplink utilization list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring Monitor and Mirror Port

- Configuring a mirror port....143
- Configuring a monitor port....145

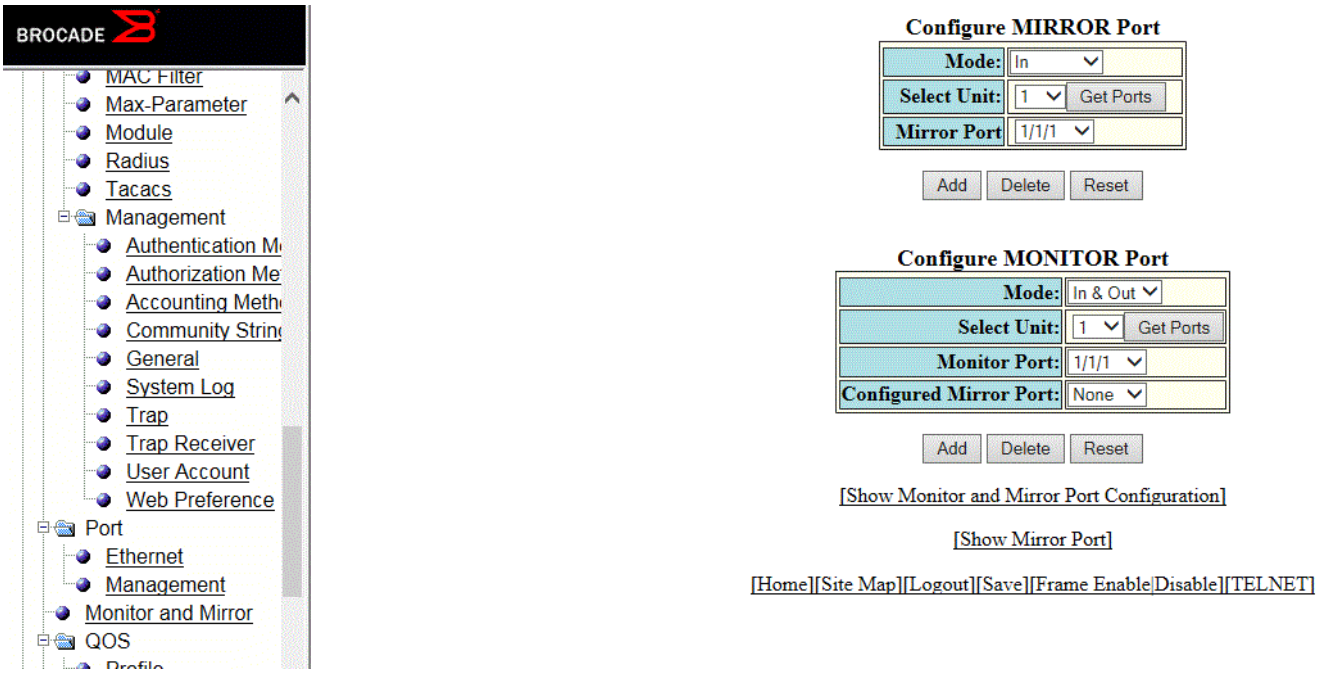
Configuring a mirror port

To configure port monitoring, first configure the mirror port. The mirror port is the port to which the monitored traffic is copied. To configure a mirror port, perform the following steps.

1. Click **Configure** on the left pane and select **Monitor and Mirror**.

   The **Configure MIRROR Port** window is displayed as shown in the figure below.

   FIGURE 79 Configuring a mirror port



2. Select the mode in which the port operates in the **Mode** list, which can be one of the following:
   - **In**
   - **Out**
   - **In & Out**
3. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

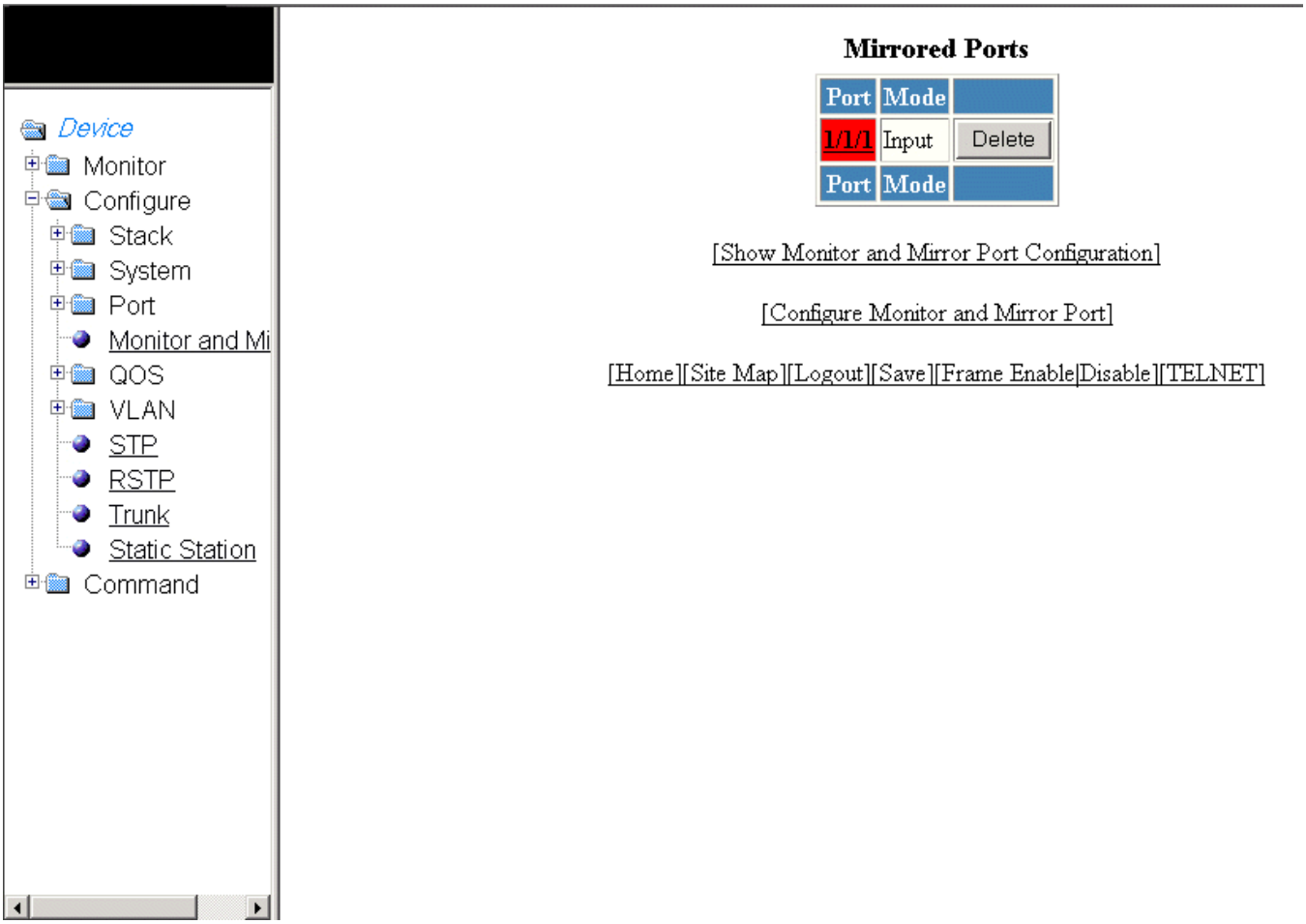
   A message is displayed to indicate that the operation does not change the running configuration.
4. Select a port to which the monitored traffic must be copied in the **Mirror Port** list.
   - stack-unit/slotnum/portnum

5. Click **Add** .

   The message `The change has been made` is displayed. To display the configured mirror port, click **Show Mirror Port**. The figure below shows the **Mirrored Ports** window with the configured mirror port information.

   To delete the configured mirror port, click **Delete**. To reset the data entered in the configuration pane, click **Reset** .

FIGURE 80 Monitoring mirror ports



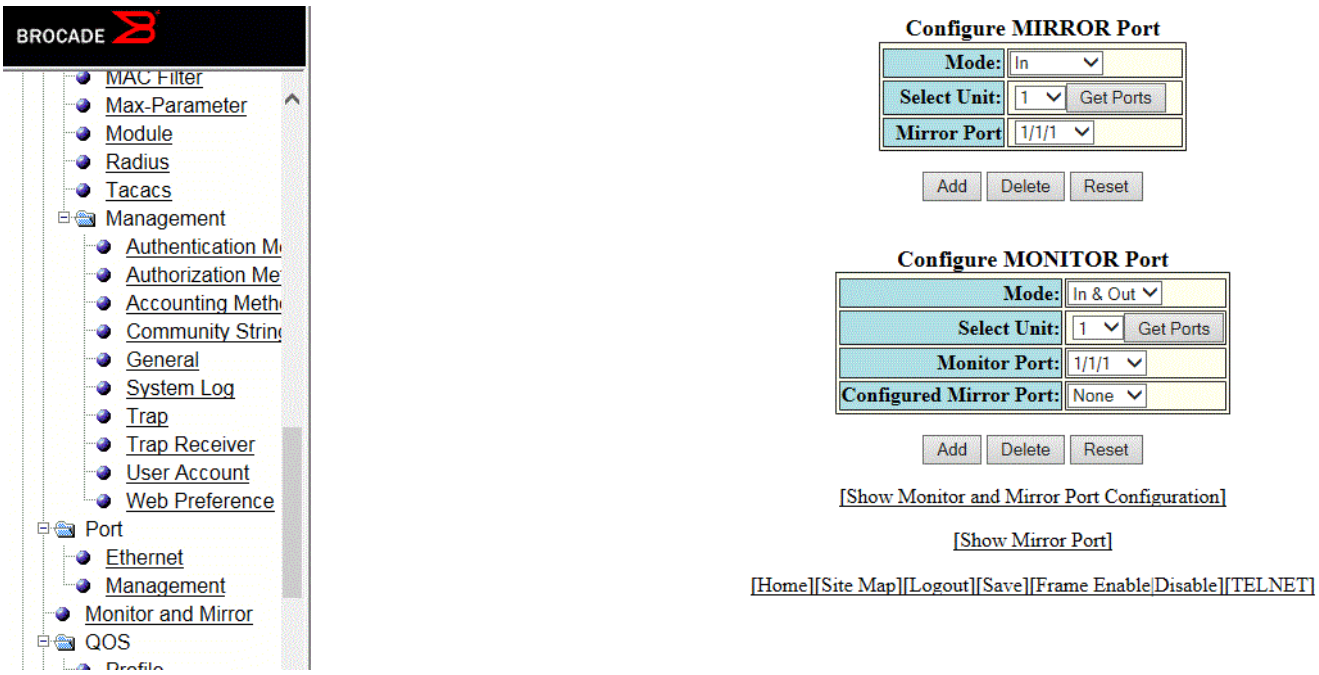
Configuring a monitor port

To configure port monitoring on an individual port on a Ruckus ICX device, perform the following steps.

1. Click **Configure** on the left pane and select **Monitor and Mirror**.

   The **Configure MONITOR Port** window is displayed as shown in the figure below.

   FIGURE 81 Configuring the monitor port



2. Select one of the following modes in which the port operates in the **Mode** list:
   - **In**
   - **Out**
   - **In & Out**
3. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
4. Select a port for which you want to monitor the traffic in the **Monitor Port** list.
   - – stack-unit/slotnum/portnum
5. Select a mirror port that you have configured in the **Configured Mirror Port** list.
6. Click **Add**.

   The message `The change has been made` is displayed. To display the configured monitor port, click **Show Monitor and Mirror Port Configuration**. To display the mirror port, click **Show Mirror Port**.

   To delete the configured monitor port, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring QoS

- Configuring the QoS profile..... 147
- Configuring the QoS profile bind..... 148

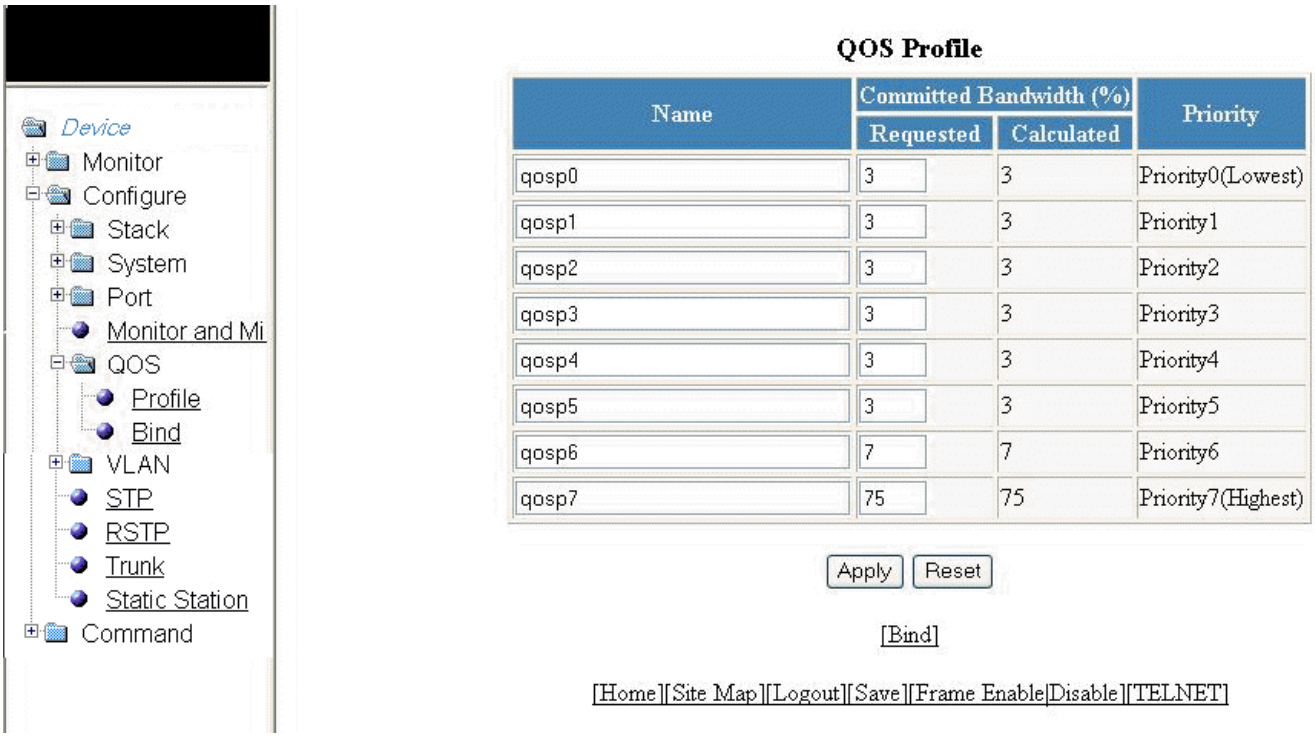
Configuring the QoS profile

To configure the Quality of Service (QoS) profile, perform the following steps.

1. Click **Configure** on the left pane and select **QOS** .
2. Click **Profile** .

   The **QOS Profile** window is displayed as shown in the figure below.

   FIGURE 82 Configuring a QoS profile



3. The default queue names are **qosp0** , **qosp1** , **qosp2** , **qosp3** , **qosp4** , **qosp5** , **qosp6** , and **qosp7** . You can change one or more of the names, if desired. Type the QoS name in the **Name** field.

4. The **Committed Bandwidth (%)** is the percentage of the device outbound bandwidth that is allocated to the queue. Ruckus QoS queues require a minimum bandwidth of 3 percent for each priority. Type the percentage of bandwidth you want for the queue in the **Requested** field.

   NOTE
   The total of the percentages you enter must be equal to 100. The Ruckus device does not adjust the bandwidth percentages you enter.

5. Click **Apply** .

   The message `The change has been made` is displayed and the committed bandwidth is changed to the configured value in the **Calculated** field. The **Priority** field shows the default priority of the individual QoS from lowest to highest (0 through 7).

   To clear the entered data in the fields, click **Reset** . To configure the QoS profile bind, click **Bind** . For more information on how to configure a QoS profile bind, refer to Configuring the QoS profile bind on page 148.

Configuring the QoS profile bind

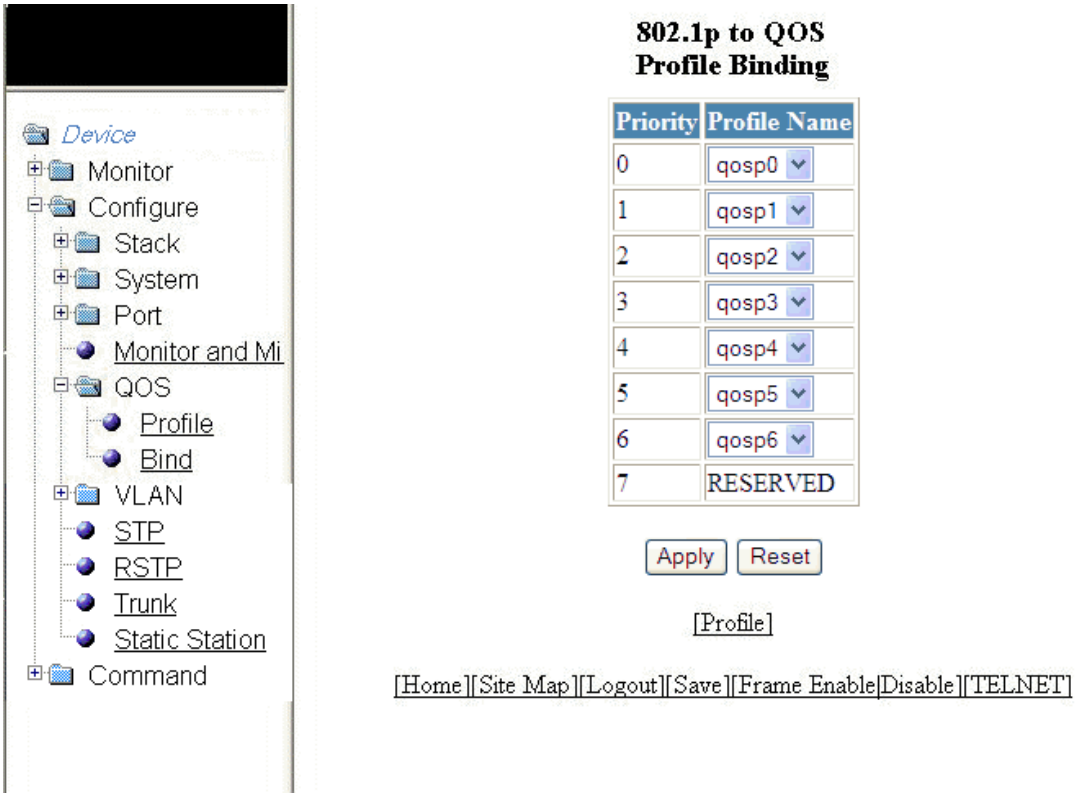
To bind an 802.1p priority to a hardware forwarding queue, perform the following steps.

1. Click **Configure** on the left pane and select **QOS** .

2. Click **Bind** .

   The **802.1p to QOS Profile Binding** window is displayed as shown in the figure below.

   FIGURE 83 802.1p to QoS profile binding



3. Select a hardware forwarding queue to which you are reassigning the priority in the **Profile Name** lists.
4. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

   To configure the Quality of Service (QoS) profile, click **Profile** . For more information, refer to Configuring the QoS profile on page 147.

Configuring VLAN

- Configuring a port VLAN.....151
- Modifying a port VLAN.....155

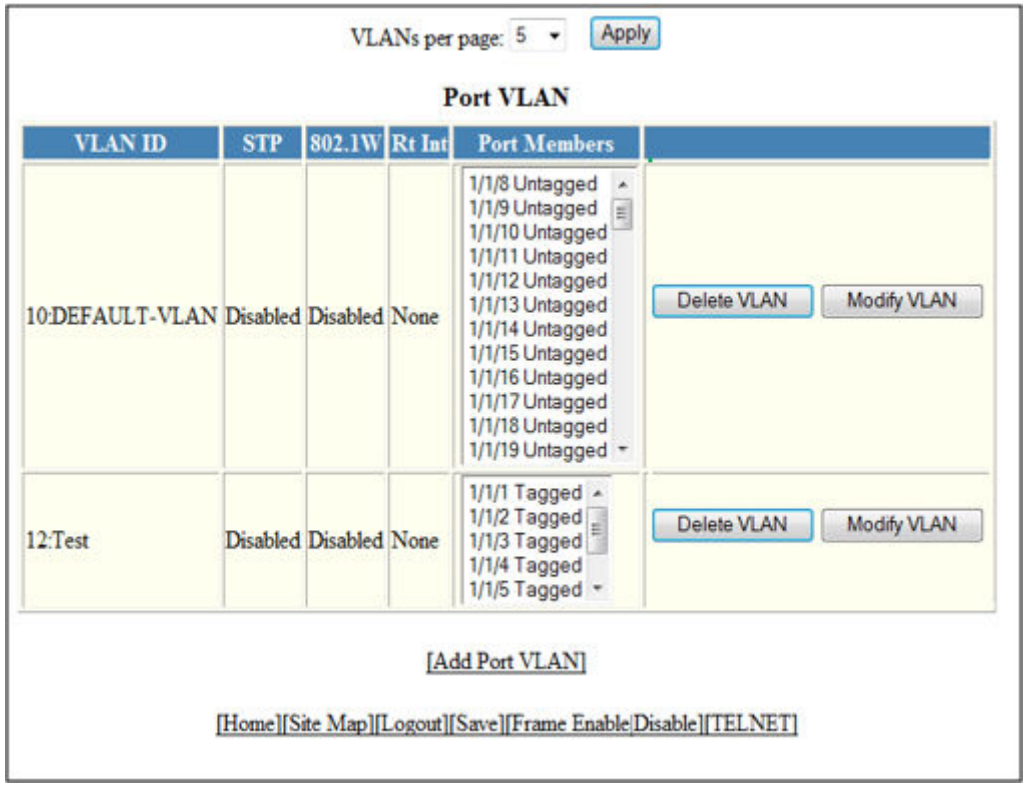
Configuring a port VLAN

To configure a port-based Virtual LAN (VLAN), perform the following steps.

1. Click **Configure** on the left pane and select **VLAN** .
2. Click **Port** .

   The **Port VLAN** window is displayed as shown in the figure below. You can limit the number of VLANs displayed per page using the **VLANs per page** list.

   FIGURE 84 Configuring port VLANs



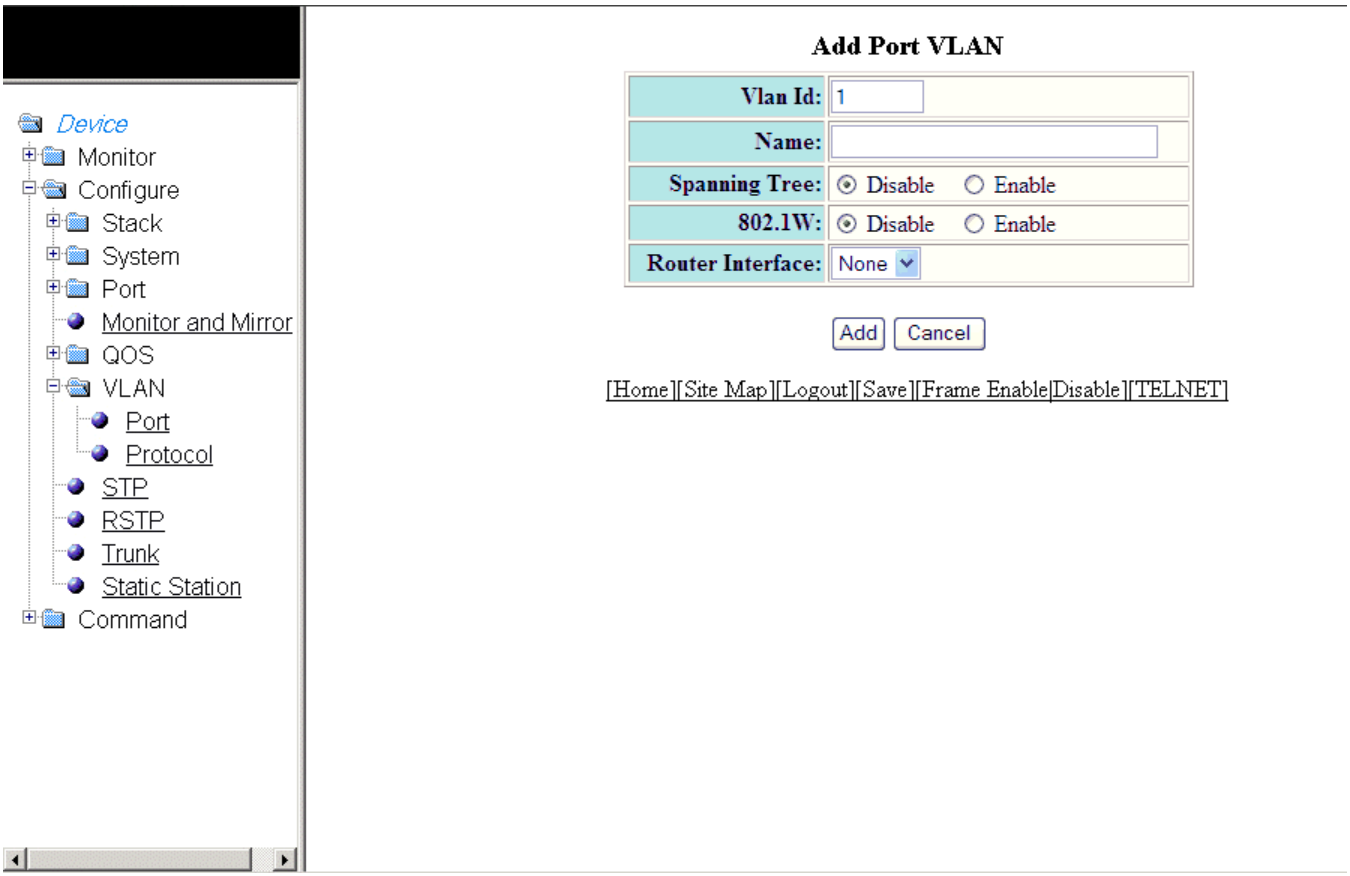
3. Click **Add Port VLAN** .

   The **Add Port VLAN** window is displayed as shown in the figure below.

   NOTE
   Port-based VLAN cannot be configured, if the VLAN does not have any ports assigned to it.

   NOTE
   Web management interface displays only the active VLANs with port members.

FIGURE 85 Adding port VLANs

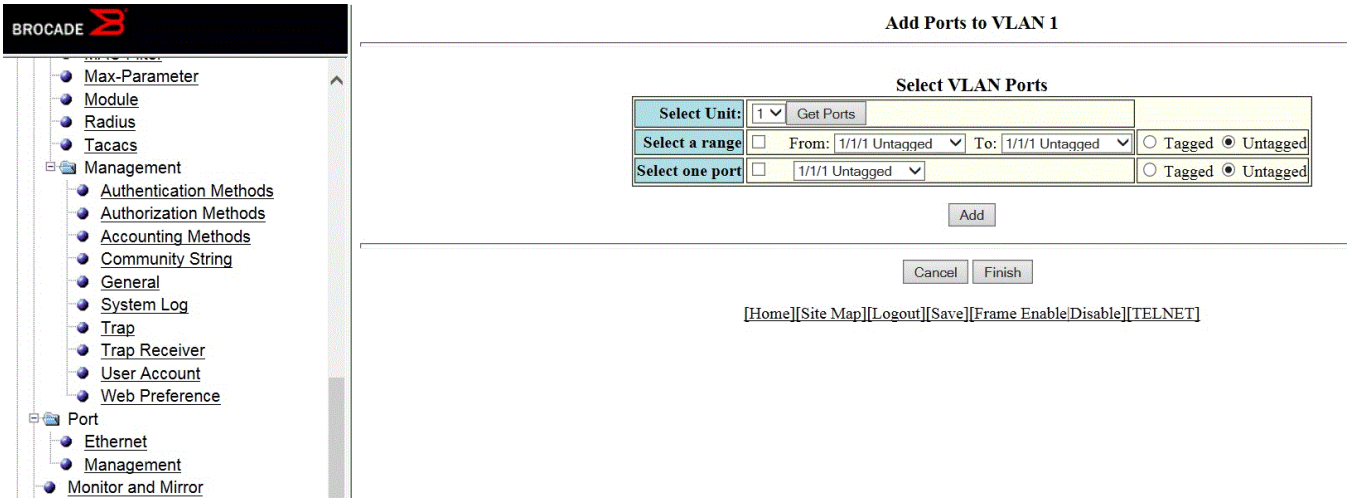


4. Type the VLAN identifier of the port in the **Vlan Id** field.
5. Type the port VLAN name in the **Name** field.
6. Click **Disable** or **Enable** for **Spanning Tree** .
7. Click **Disable** or **Enable** for **802.1W** .
8. Select a virtual routing interface in the **Router Interface** list.

9. Click **Add** .

   The **Add Ports to VLAN** window is displayed as shown in the figure below.

   FIGURE 86 Adding ports to VLANs



10. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

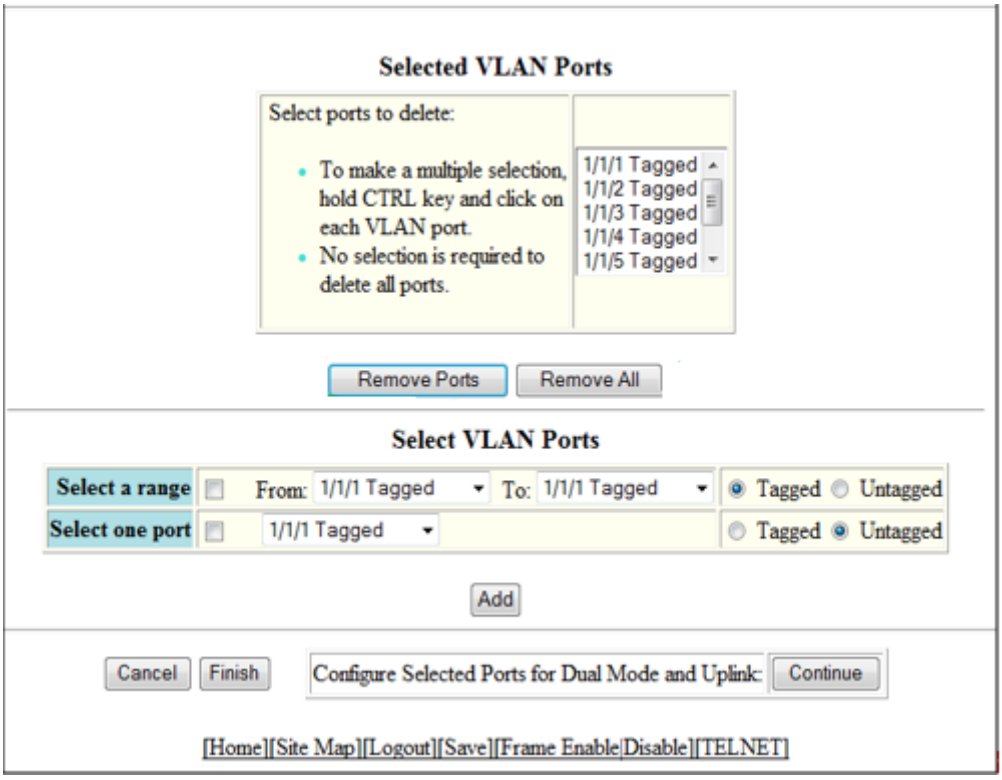
    A message is displayed to indicate that the operation does not change the running configuration.

11. To select the VLAN ports, select the **Select a range** check box, select the range of VLAN ports in the **From** and **To** lists, and click **Tagged** or **Untagged** , or select the **Select one port** check box, select a port-based VLAN in the list, and click **Tagged** or **Untagged** .

12. Click **Add** .

    The **Selected VLAN Ports** window is displayed as shown in the figure below.

    FIGURE 87 Selected VLAN ports



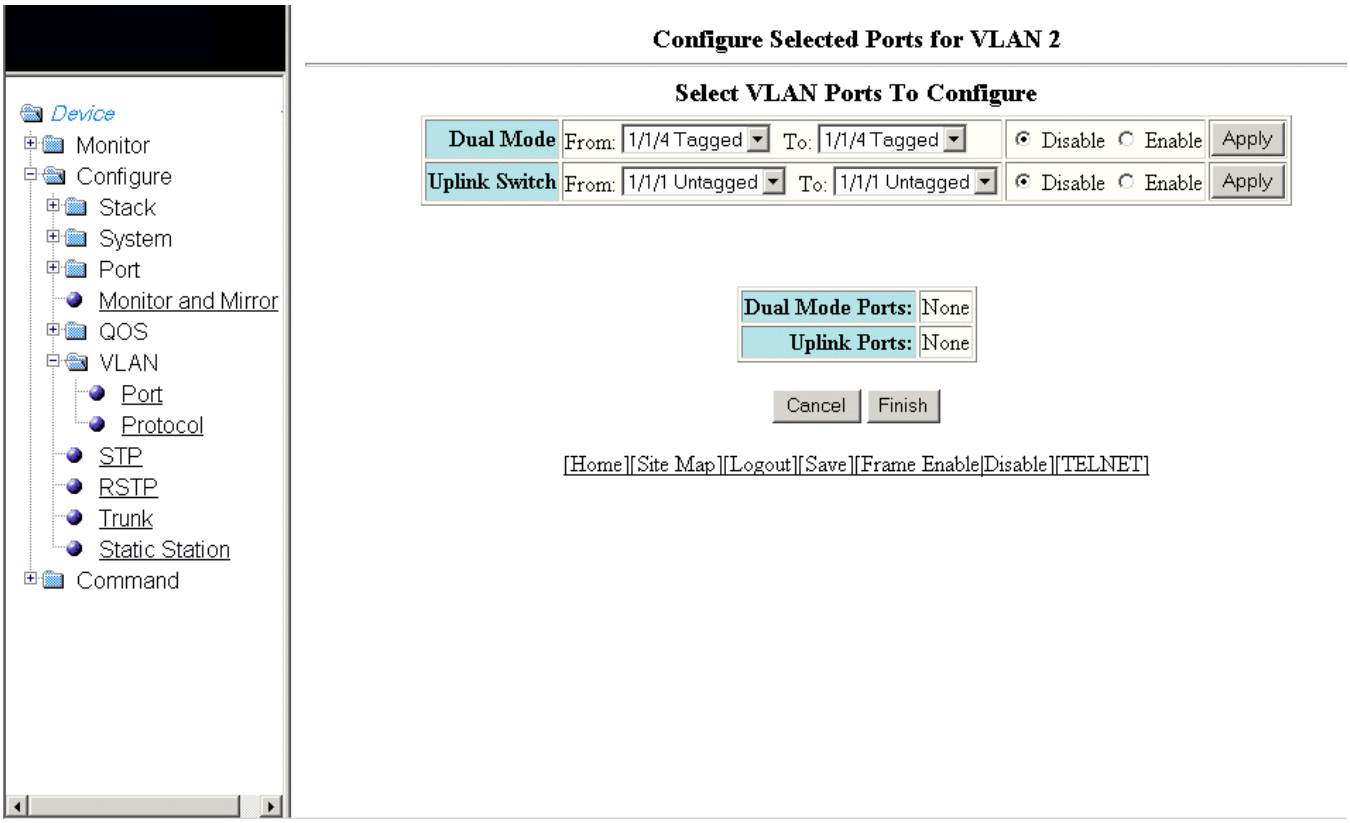
13. The selected VLAN ports are displayed in the **Selected VLAN Ports** list. Click **Remove Ports** or **Remove All** to delete the VLAN ports.

    NOTE
    The VLAN configuration is retained even if the last port member is deleted.

14. You can add more VLAN ports from the **Select VLAN Ports** pane. To do so, complete step 10 and step 11.

15. Click **Finish** to return to the **Port VLAN** window with the configured port-based VLAN displayed, or click **Continue** to configure selected ports for dual mode and uplink. The **Configure Selected Ports for VLAN** window is displayed as shown in the figure below.

FIGURE 88 Configuring dual mode and uplink for ports



16. To configure dual mode and uplink for the ports, perform the following steps.
    a) Select the ports for which you want to configure the dual mode in the **From** and **To** lists for **Dual Mode** . Click **Disable** or **Enable** and then click **Apply** . The configured ports are displayed in the **Dual Mode Ports** list.
    b) Select the ports for which you want to configure uplink in the **From** and **To** lists for **Uplink Switch** . Click **Disable** or **Enable** and then click **Apply** . The configured ports are displayed in the **Uplink Ports** list.
    c) Click **Finish** .

    The configured port VLAN is displayed in the **Port VLAN** window. To cancel the VLAN port configuration and return to the **Port VLAN** window, click **Cancel** .

Modifying a port VLAN

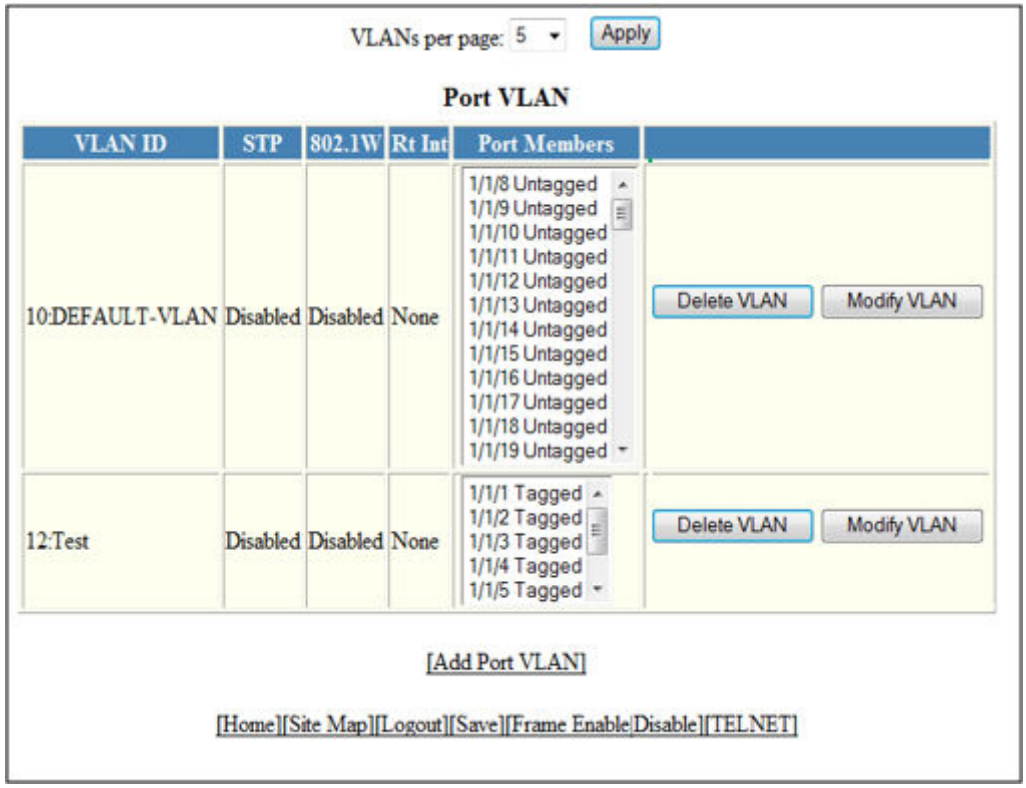
To modify a port VLAN, perform the following steps.

1. Click **Configure** on the left pane and select **VLAN** .

2. Click **Port** .

   The **Port VLAN** window is displayed as shown in the figure below.

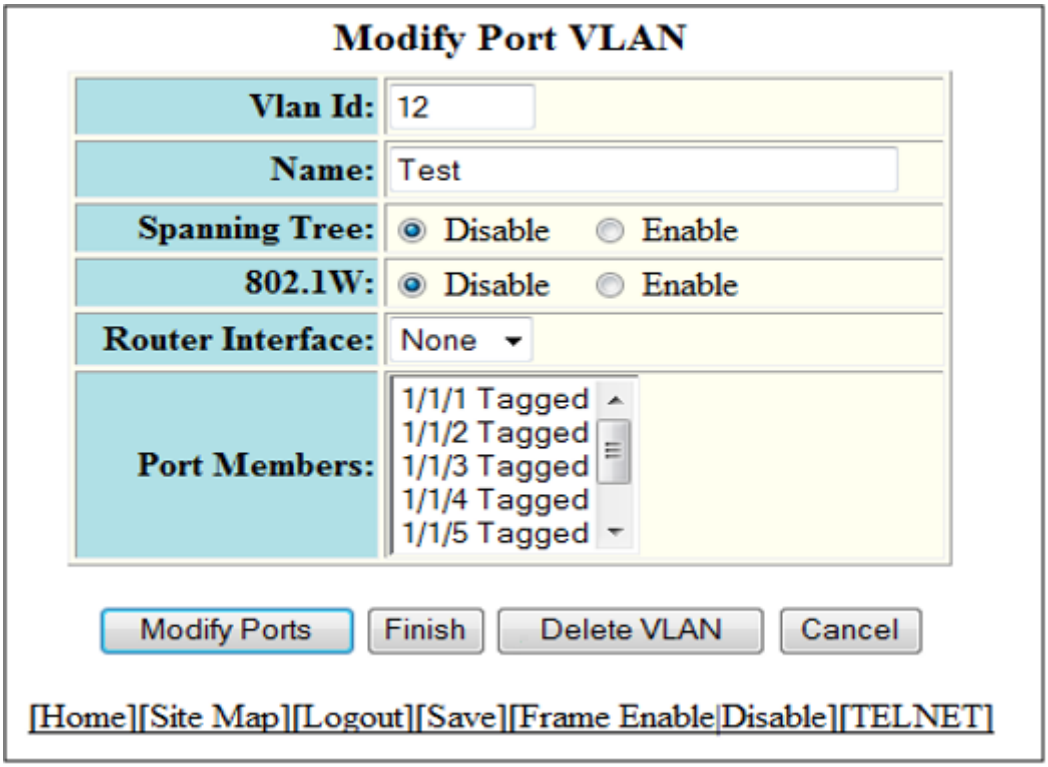
FIGURE 89 Configuring port VLANs



3. Click **Modify** .

   The **Modify Port VLAN** window is displayed as shown in the figure below .

   FIGURE 90 Modifying port VLANs

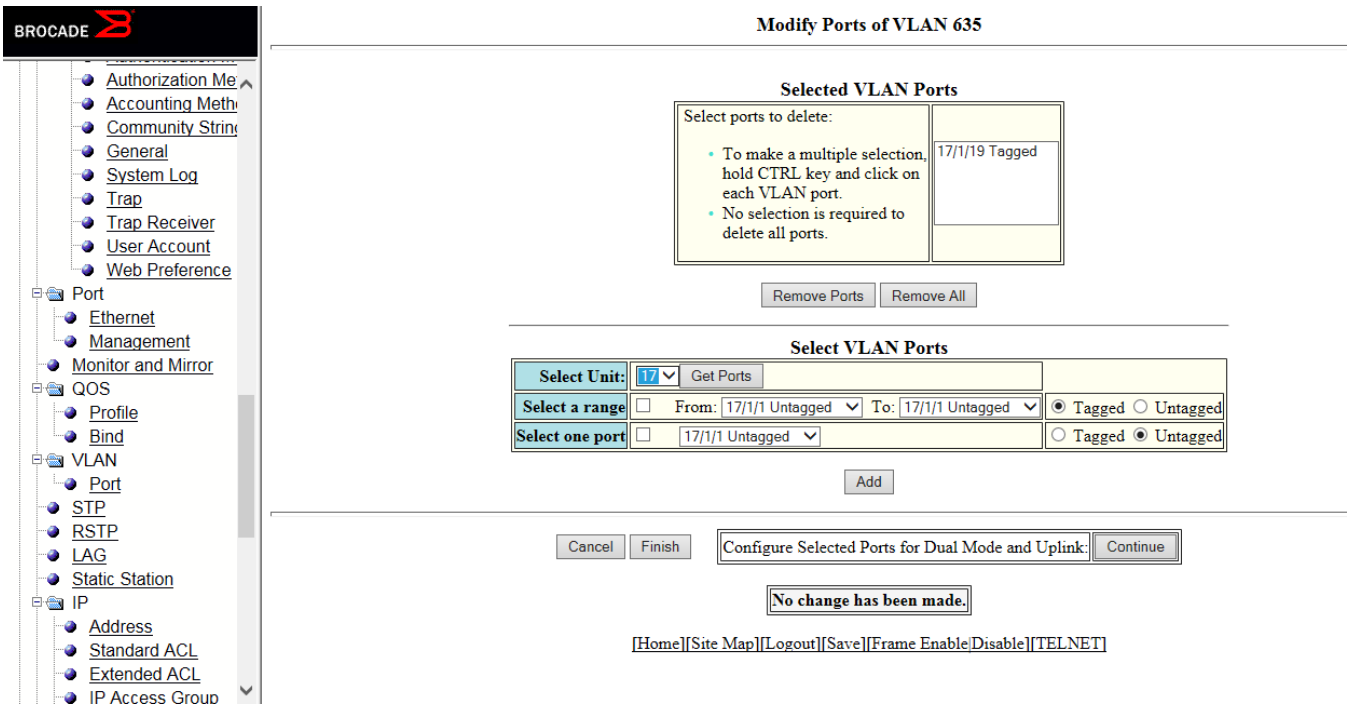


4. Type the VLAN identifier of the port in the **Vlan Id** field.
5. Type the port VLAN name in the **Name** field.
6. Click **Disable** or **Enable** for **Spanning Tree** .
7. Click **Disable** or **Enable** for **802.1W** .
8. Select the VLAN ports in the **Port Members** list.
9. To delete the configured port VLAN, click **Delete VLAN** . To undo your changes and go back to the **Port VLAN** window, click **Cancel** .

10. Click **Modify Ports** to modify VLAN ports.

    The **Modify Ports of VLAN** window is displayed as shown in the figure below .

    FIGURE 91 Modify Ports of the selected VLAN



11. The selected VLAN ports are displayed in the **Selected VLAN Ports** list. Click **Remove Ports** or **Remove All** to delete the VLAN ports.

    NOTE
    The VLAN configuration is retained even if the last port member is deleted.

12. You can add more VLAN ports from the **Select VLAN Ports** pane.
13. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

    A message is displayed to indicate that the operation does not change the running configuration.
14. To select the VLAN ports, select the **Select a range** check box, select the range of VLAN ports in the **From** and **To** lists, and click **Tagged** or **Untagged** , or select the **Select one port** check box, select a port-based VLAN in the list, and click **Tagged** or **Untagged** .
15. Click **Add** to add more VLAN ports.
16. Click **Finish** to return to the **Modify Port VLAN** window with the configured port-based VLAN displayed, or click **Continue** to configure selected ports for dual mode and uplink.
17. Click **Finish** to complete the port modifying operation.

Configuring STP

- Configuring STP parameters..... 159

Configuring STP parameters

Ruckus ICX Layer 2 switches and Layer 3 switches support standard Spanning Tree Protocol (STP) as described in the IEEE 802.1D specification.

Each port-based VLAN on a Ruckus device runs a separate spanning tree. A Ruckus device has one port-based VLAN (VLAN 1) that contains all the device ports. However, if you configure additional port-based VLANs on a Ruckus device, then each of those VLANs on which STP is enabled and the VLAN 1 run separate spanning trees.

If you configure a port-based VLAN on the device, the VLAN has the same STP state as the default STP state on the device. Thus, by default on Layer 2 switches, new VLANs have STP enabled and on Layer 3 switches, new VLANs have STP disabled. You can enable or disable STP in each VLAN separately and also on individual ports.

Using the Web Management Interface, you can change the default STP bridge and port parameters.

Changing STP bridge parameters

The table below lists the default STP bridge parameters.

TABLE 29 Default STP bridge parameters

Parameter	Default value
Forward Delay	15 seconds
Maximum Age	20 seconds
Hello Time	2 seconds
Priority	32768

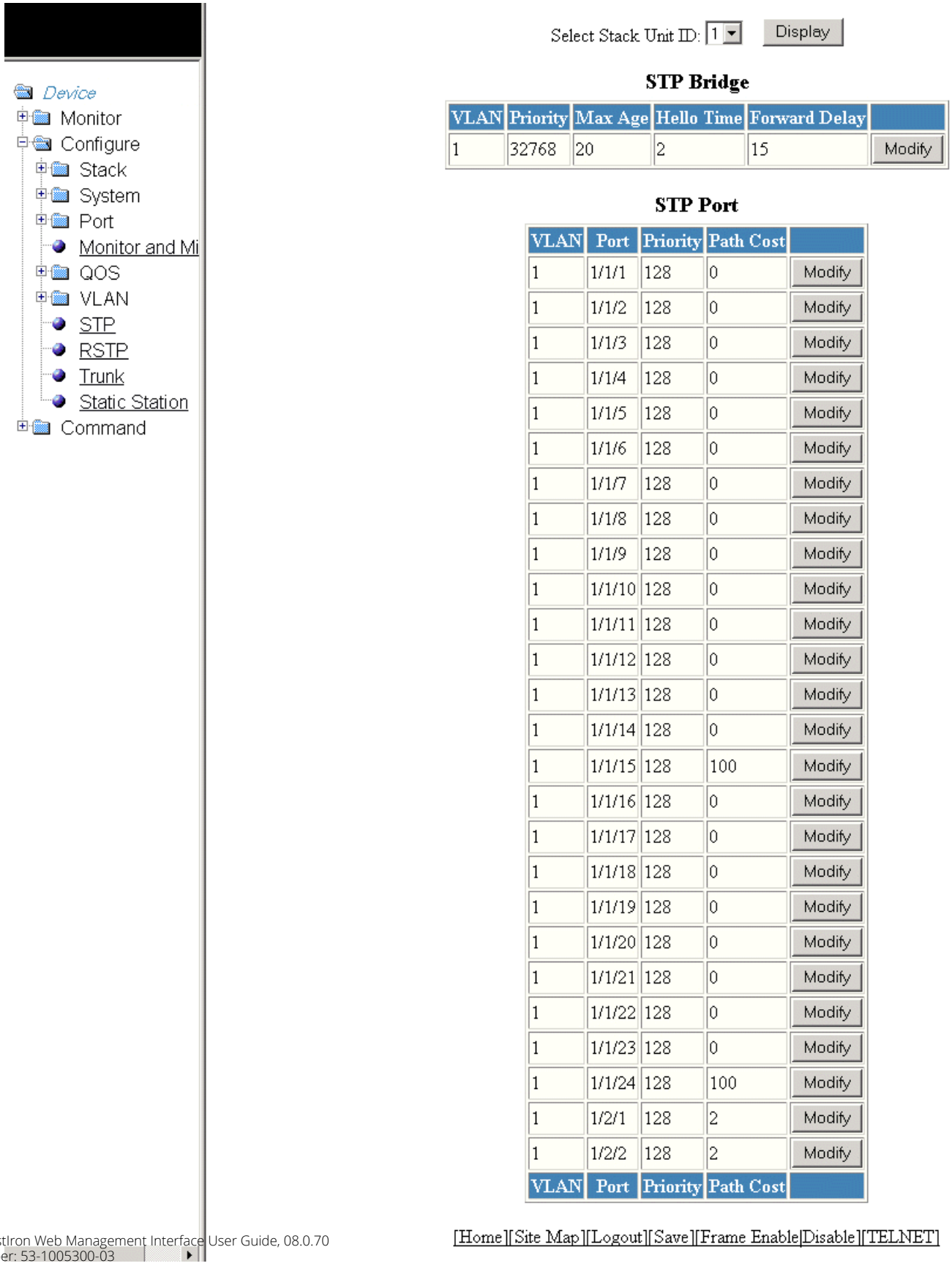
NOTE
To change STP bridge timers, you must stay within the following ranges:2 * (Forward Delay-1) >= Maximum Age >= 2 * (Hello Time +1)

To change the default STP bridge values, perform the following steps.

1. Click **Configure** on the left pane and select **STP** .

   The **STP Bridge** window is displayed as shown in the figure below.

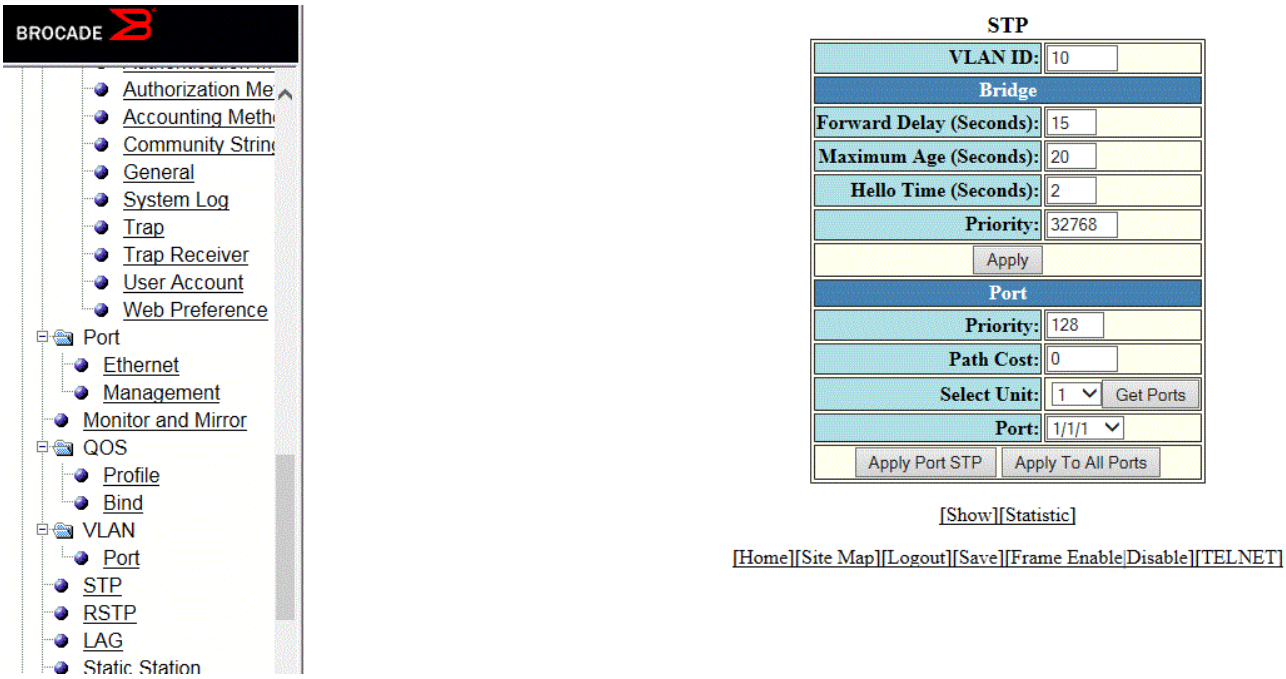
FIGURE 92 Configuring the STP bridge



2. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to display the information about a specific stack unit.
3. To change the default values of the STP bridge, click **Modify** .

   The **STP** window is displayed as shown in the figure below.

FIGURE 93 Configuring STP bridge parameters



4. Type the VLAN identifier of the port in the **VLAN ID** field.
5. Type the forward delay time, which is the period of time spent by a port in the listening and learning state before moving on to the learning or forwarding state, in the **Forward Delay (Seconds)** field. The range is from 4 through 30 seconds.
6. Type the maximum amount of time the device waits before a topology change in the **Maximum Age (Seconds)** field. The range is from 6 through 40 seconds.
7. Type the hello time, which is the interval of time between each configuration BPDU sent by the root bridge, in the **Hello Time (Seconds)** field. The range is from 1 through 10 seconds.
8. Type the priority used to identify the root bridge in a spanning tree in the **Priority** field. The range is from 0 through 65535.
9. Click **Apply** .

   The message `The change has been made` is displayed and the configured values are displayed in the **STP Bridge** window. To display the **STP Bridge** window, click **Show** . To display STP information, click **Statistic** . For more information on the field descriptions, refer to Displaying STP information on page 59.

Changing STP port parameters

The table below lists the default STP port parameters.

TABLE 30 Default STP port parameters

Parameter	Default value
Priority	128
Path Cost	The default path cost depends on the port type. • 10 Mbps - 100 • 100 Mbps - 19 • 1 Gbps - 4 • 10 Gbps - 2

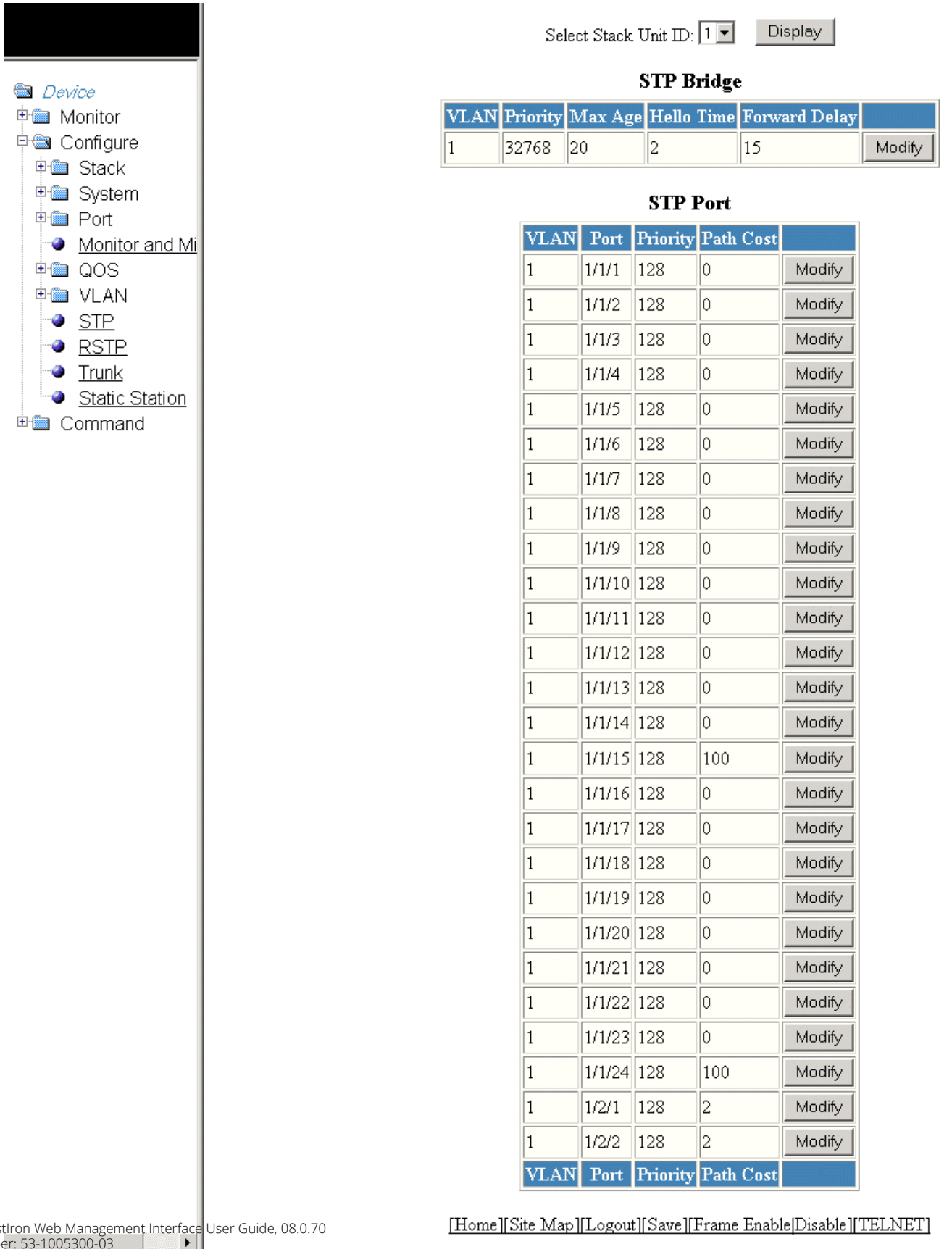
To change the default STP port values, perform the following steps.

1. Click **Configure** on the left pane and select **STP**.

   The **STP Port** window is displayed as shown in the figure below.

2. Select a unit ID in the **Select Stack Unit ID** list and click **Display** to display the information about a specific stack unit.

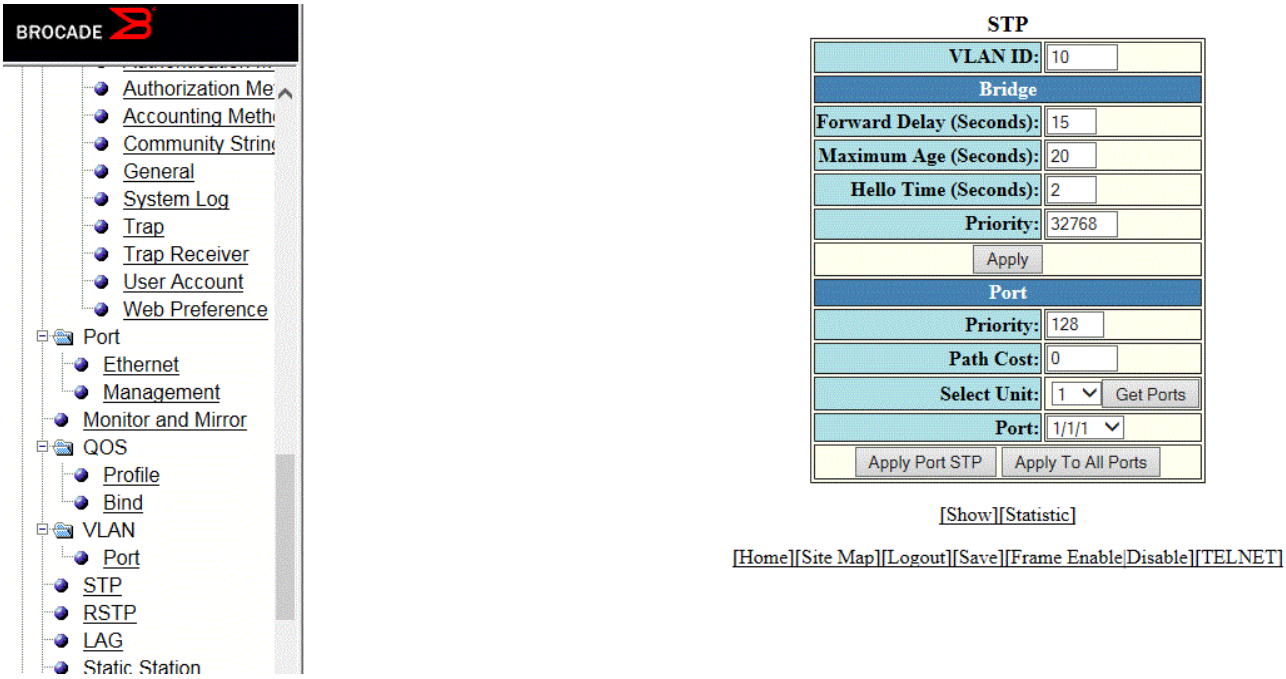
FIGURE 94 Configuring the STP port



3. Click **Modify** to change the default values of individual STP ports.

   The **STP** window is displayed.

FIGURE 95 Configuring STP port parameters



4. Type the VLAN identifier of the port in the **VLAN ID** field.
5. Type the preference that STP should give to this port relative to other ports for forwarding traffic out of the spanning tree in the **Priority** field. The range is from 0 through 240.
6. Type the cost of using the port to reach the root bridge in the **Path Cost** field. The range is from 0 through 65535.
7. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
8. Select a port number in the **Port** list.
   - stack-unit/slotnum/portnum
9. Click **Apply Port STP** to configure the entered values only to the specified port. Click **Apply To All Ports** to configure the entered values to all the ports.

   The message `The change has been made` is displayed and the configured values are displayed in the **STP Port** window. To display the **STP Port** window, click **Show**.

   To display STP information, click **Statistic**. For more information on the field descriptions, refer to the “Displaying STP information” section.

Configuring RSTP

- Configuring RSTP parameters.....167

Configuring RSTP parameters

You can change the RSTP default bridge and port parameters using the Web Management Interface.

Changing RSTP bridge parameters

The table below lists the default RSTP bridge parameters.

TABLE 31 Default RSTP bridge parameters

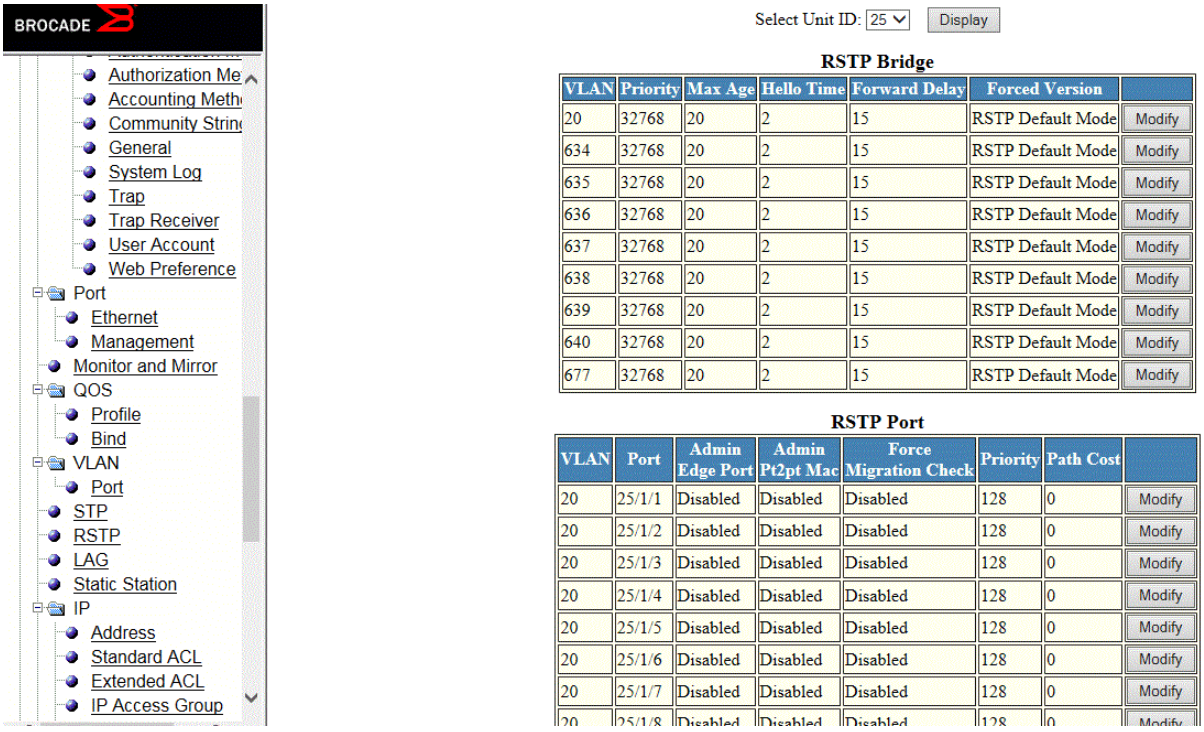
Parameter	Default value
Forward Delay	15 seconds
Maximum Age	20 seconds
Hello Time	2 seconds
Priority	32768
Force Version	RSTP Default Mode

To change the default RSTP bridge values, perform the following steps.

1. Click **Configure** on the left pane and select **RSTP**.

   The **RSTP Bridge** window is displayed as shown in the figure below.

   FIGURE 96 Configuring RSTP parameters

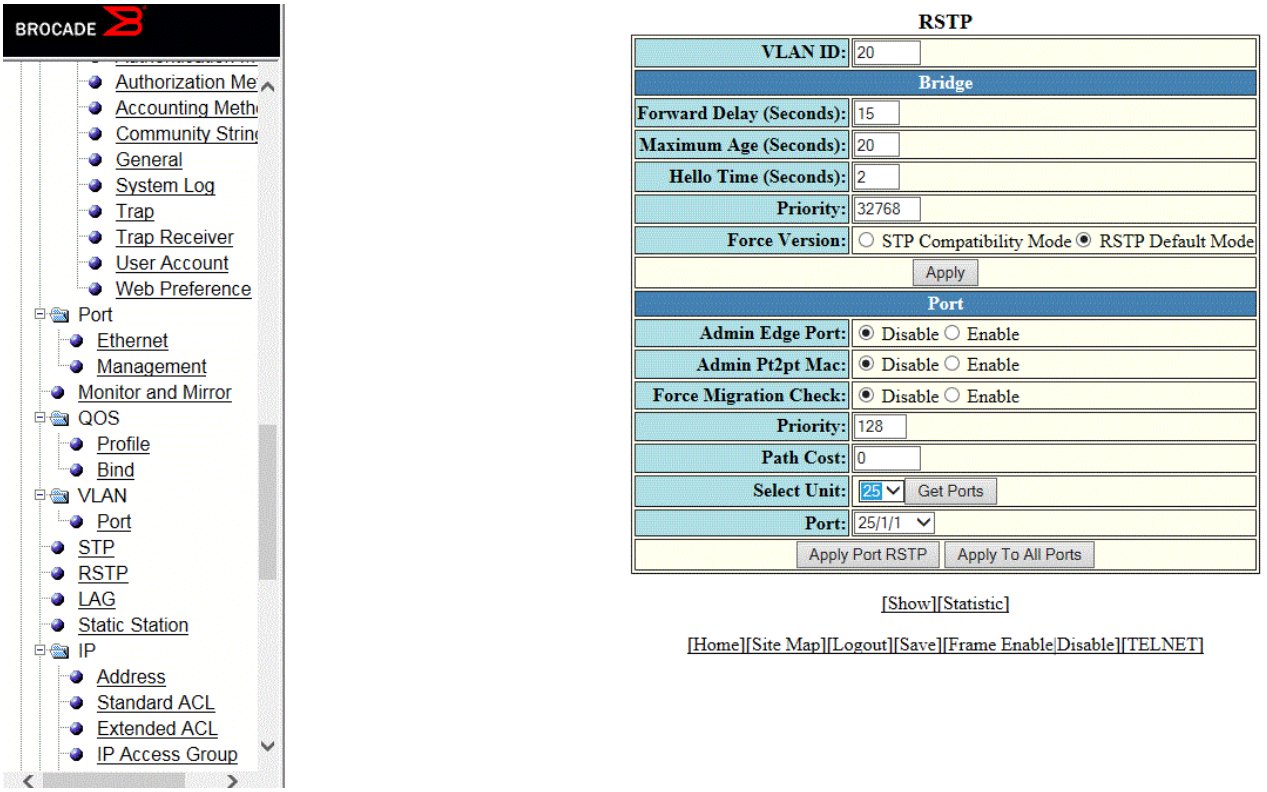


2. Select a Unit ID from the **Select Unit ID** list and click **Display** to view the ports configured with RSTP.

3. Click **Modify**.

   The **RSTP** window is displayed as shown in the figure below.

FIGURE 97 Changing RSTP bridge values



4. Type the VLAN identifier of the port in the **VLAN ID** field.
5. Type the forward delay, which specifies how long a port waits before it forwards an RST BPDU after a topology change, in the **Forward Delay (Seconds)** field. The range is from 4 through 30 seconds.
6. Type the maximum age, which specifies the amount of time the device waits to receive a Hello packet before it starts a topology change, in the **Maximum Age (Seconds)** field. The range is from 6 through 40 seconds.
7. Type the hello time, which specifies the interval between two Hello packets, in the **Hello Time (Seconds)** field. The range is from 1 through 10 seconds.
8. Type the priority of the bridge in the **Priority** field. The range is from 0 through 65535.
9. Click **STP Compatibility Mode** or **RSTP Default Mode** for **Force Version** . By default, **RSTP Default Mode** is enabled.
10. Click **Apply**.

    The message `The change has been made` is displayed and the configured values are shown in the **RSTP Bridge** window.

Changing RSTP port parameters

The table below lists the default RSTP port parameters.

TABLE 32 Default RSTP port parameters

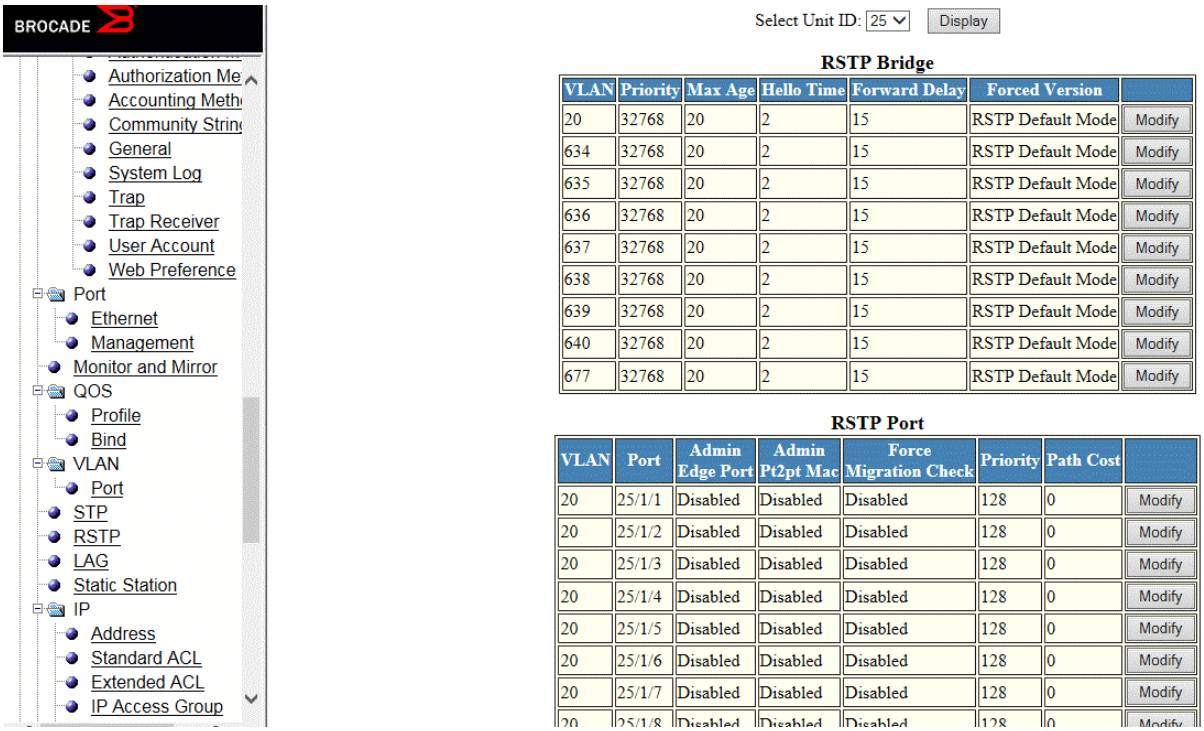
Parameter	Default value
Admin Edge Port	Disable
Admin Pt2pt Mac	Disable
Force Migration Check	Disable
Priority	128
Path Cost	0

To change the default RSTP port values, perform the following steps.

1. Click **Configure** on the left pane and select **RSTP**

   The **RSTP Port** window is displayed as shown in the figure below.

   FIGURE 98 Configuring RSTP ports

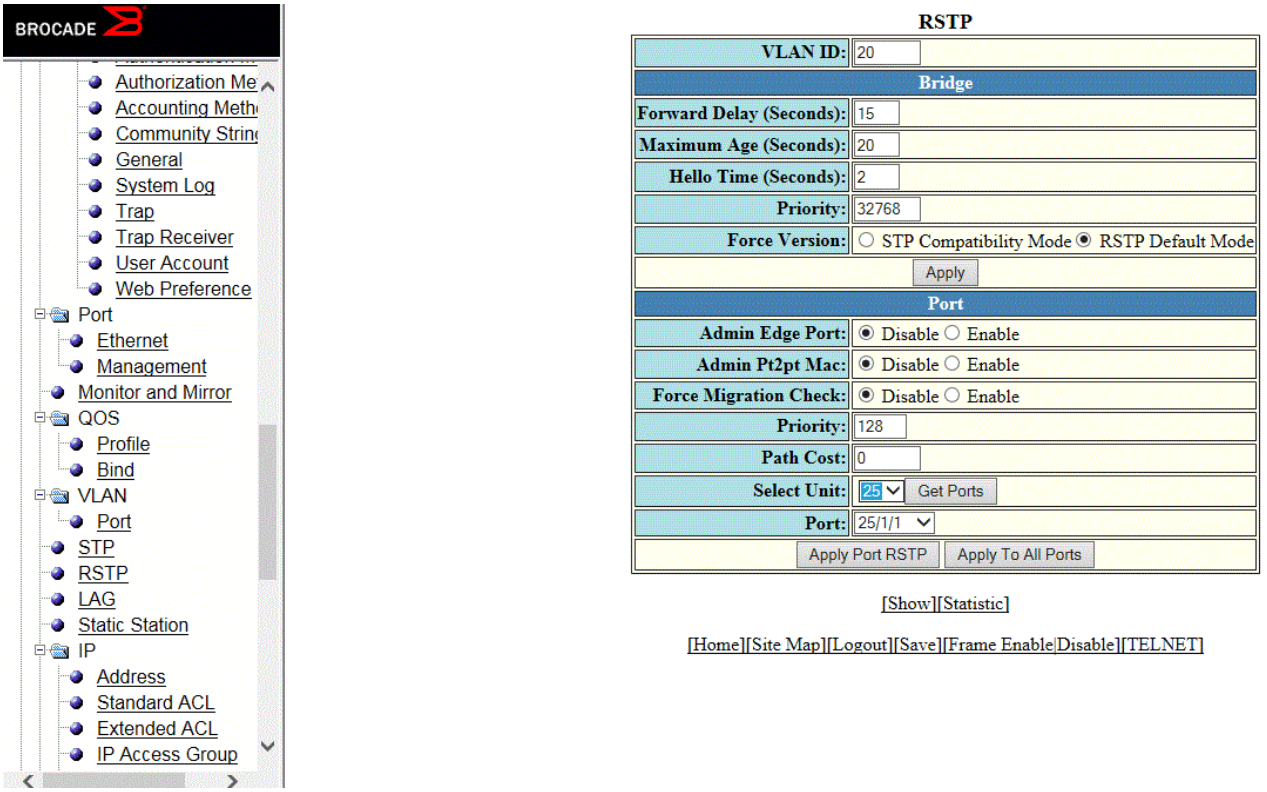


2. Select a Unit ID from the **Select Unit ID** list and click **Display** to view the ports configured with RSTP.

3. Click **Modify** to change the default values for an individual RSTP ports.

   The **RSTP** window is displayed as shown in the figure below.

FIGURE 99 Changing RSTP port values



4. Click **Disable** or **Enable** for **Admin Edge Port**. If you click **Enable** , the port becomes an edge port in the domain.
5. Click **Disable** or **Enable** for **Admin Pt2pt Mac**. If you click **Enable**, a port will be connected to another port through a point-to-point link.
6. Click **Disable** or **Enable** for **Force Migration Check**. If you click **Enable**, the specified port will be forced to send one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port returns to sending STP BPDUs.
7. Type the priority, which is the preference that RSTP gives to this port relative to other ports for forwarding traffic out of the topology, in the **Priority** field. The range is from 0 through 240.
8. Type the cost of the port path to the root bridge in the **Path Cost** field. The range is from 1 through 20,000,000.
9. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
10. Select a port from the **Port** list.
    - stack-unit/slotnum/portnum
11. Click **Apply Port RSTP** to configure the values only to the specified port, or click **Apply To All Ports** to configure the values to all the ports.

    The message `The change is made` is displayed and the configured RSTP port values are reflected in the **RSTP Port** window.

Configuring LAGs

- Configuring a static, dynamic, or keep-alive LAG..... 173
- Displaying a configured LAG..... 177

Configuring a static, dynamic, or keep-alive LAG

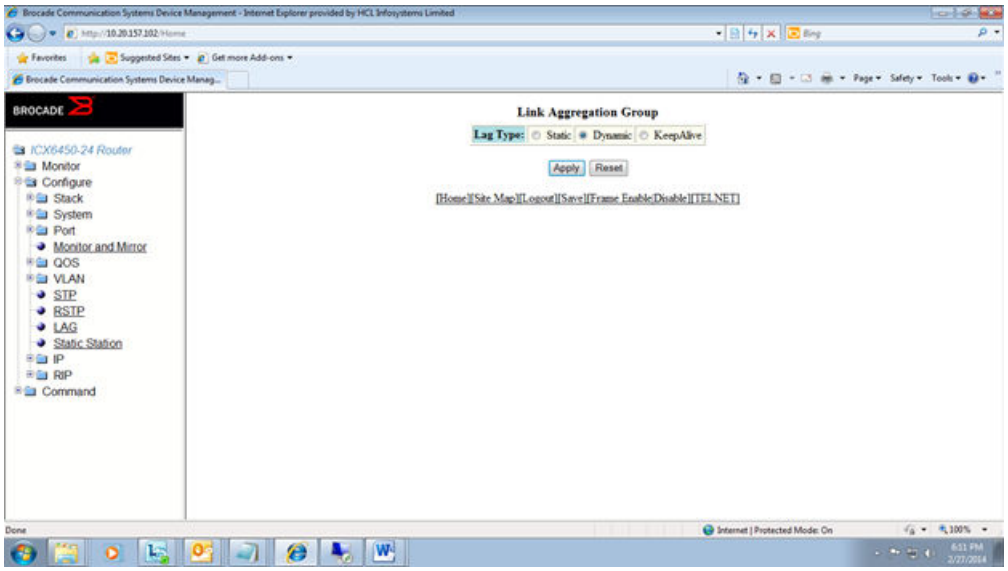
You can configure a static, dynamic, or keep-alive link aggregation group (LAG).

NOTE
sFlow and rate-limiting commands are not supported in the Web Management interface.

To configure a LAG, perform the following steps.

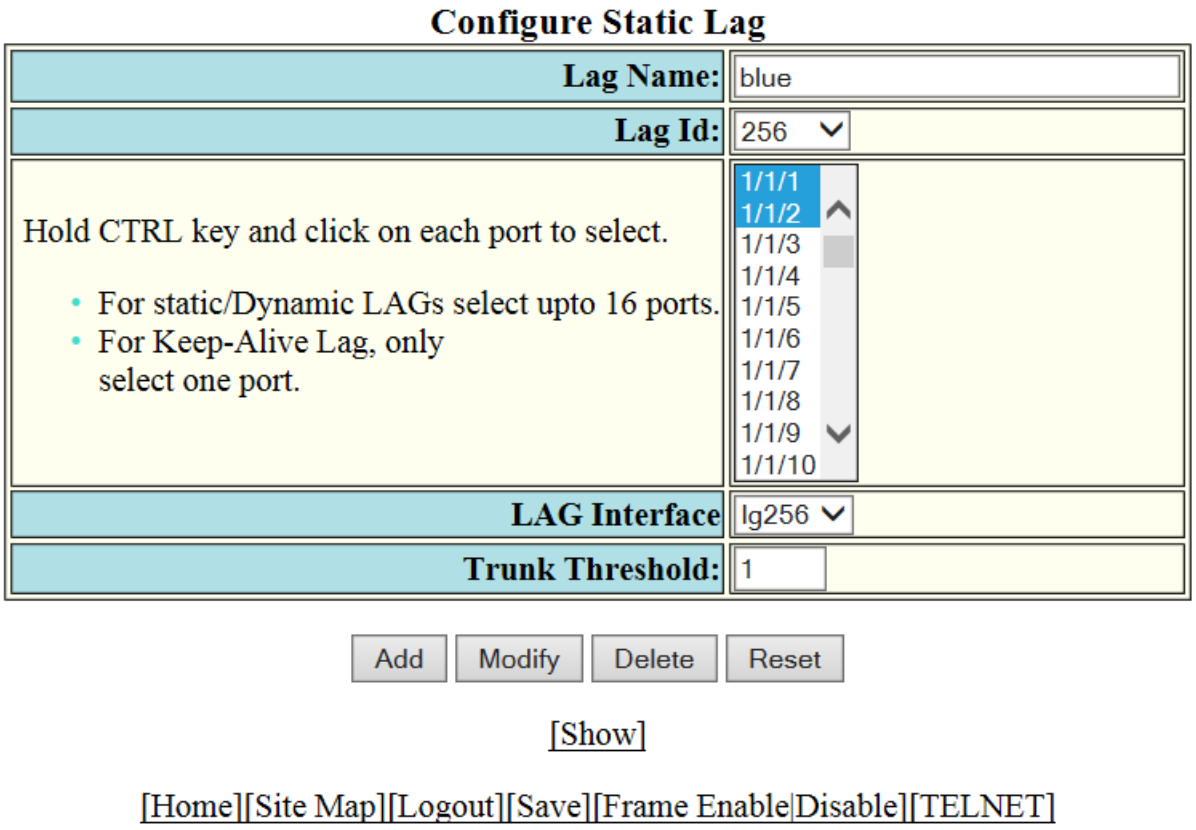
1. Click **Configure** on the left pane and select **LAG**.

   The **Link Aggregation Group** window is displayed.

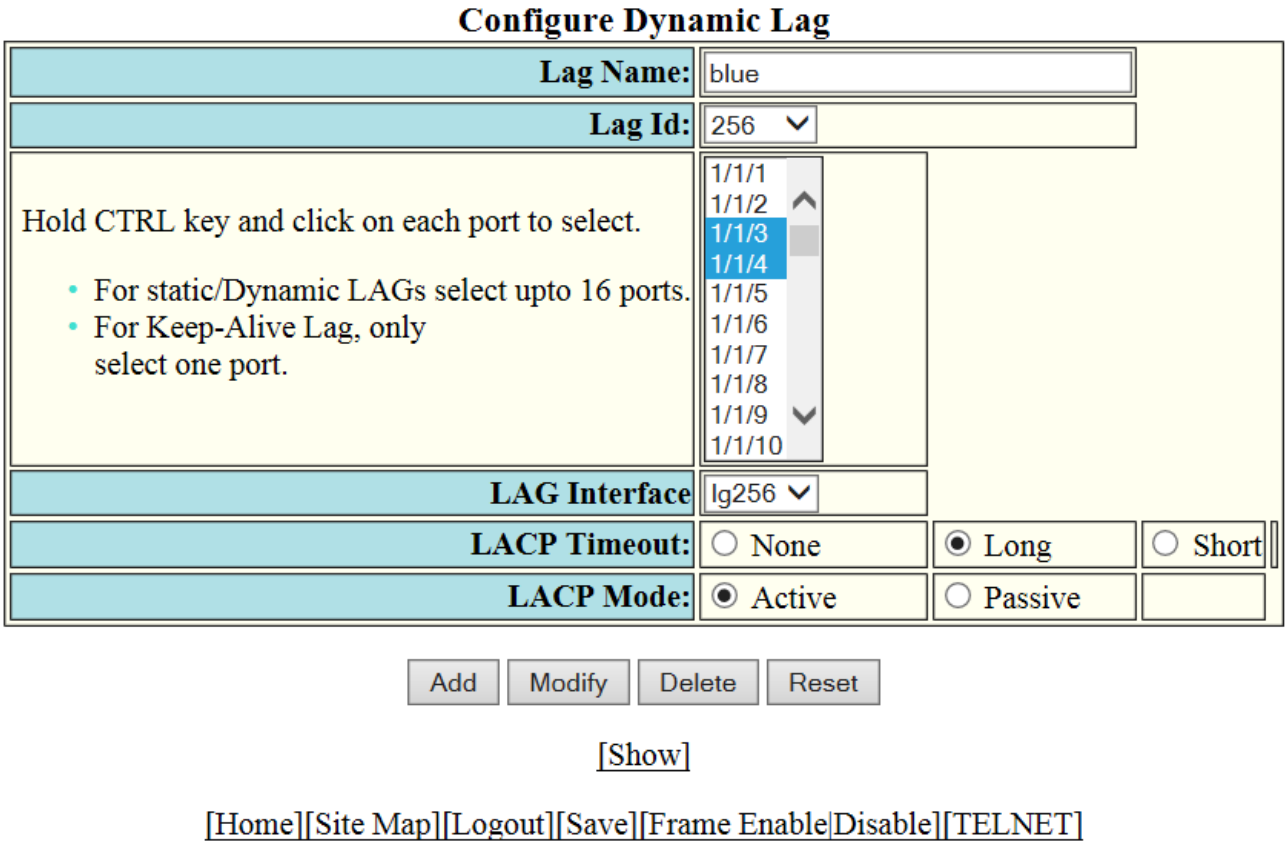


   You can select among the LAG types: static, dynamic, or keep-alive.

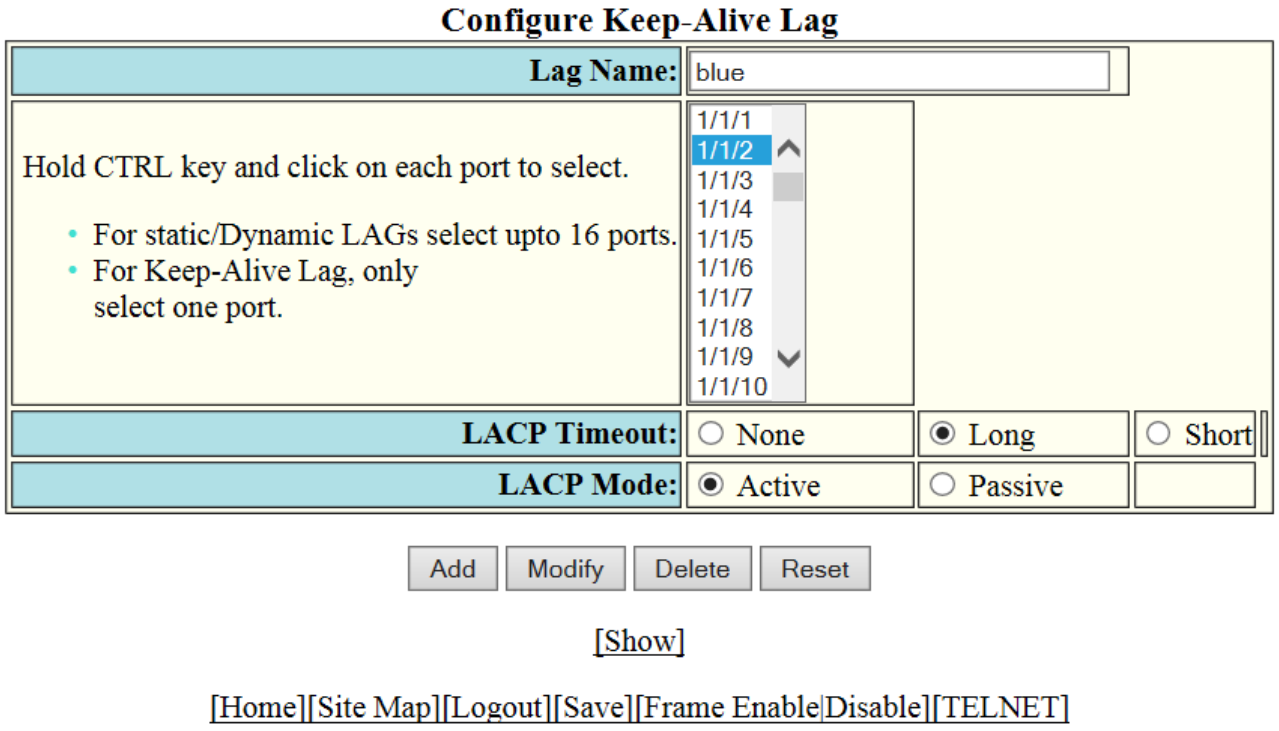
2. Click **Apply**.
   - If you select a static LAG, this window is displayed:



   - If you select a dynamic LAG, this window is displayed:



- If you select a keep-alive LAG, this window is displayed:



3. Enter the LAG name in the **Lag Name** field.

   You can enter up to 64 alphanumeric characters.

4. Enter the LAG ID in the **Lag Id** field.

   Hold down the CTRL key and, for static and dynamic LAGs only, select ports from the list. The number of ports you can select for static and dynamic LAGs depends on the platform. You can select only one port for keep-alive LAGs.

   NOTE
   If you do not select a LAG ID, an ID is automatically generated.

5. **NOTE**
   This step applies only to static and dynamic LAGs.

   Select the LAG virtual interface.

   The **LAG Interface** list displays a list of LAG virtual interface names. The interface name is of the format **lg**<*id*>, where *id* is the configured LAG ID.

6. **NOTE**
   This step applies only to static LAGs.

   Configure the trunk threshold.

7. **NOTE**
   This step applies only to dynamic and keep-alive LAGs.

   Configure the LACP timeout.

8. **NOTE**
   This step applies only to dynamic and keep-alive LAGs.

   Configure the LACP mode as **Active** or **Passive**. By default, the LACP operation mode is **Active**.
9. Click **Add**.

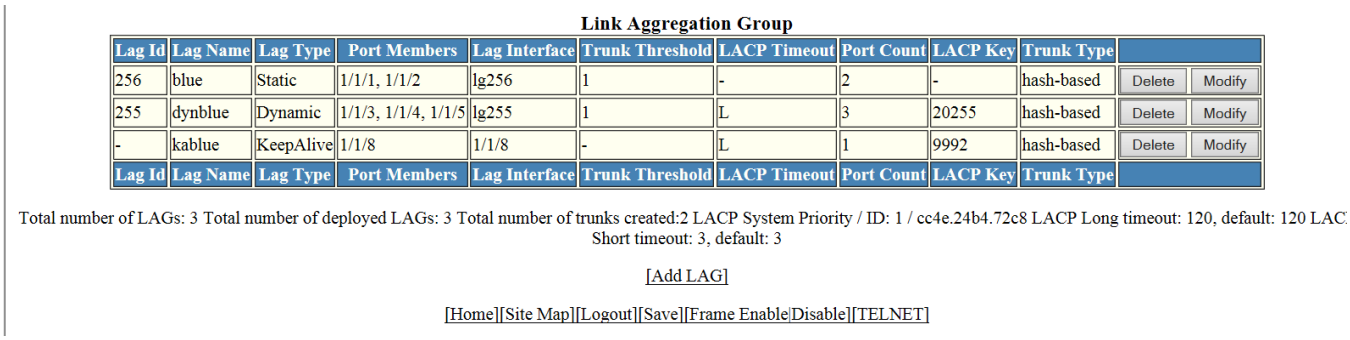
   The LAG is added.

Displaying a configured LAG

You can display information for a configured link aggregation group (LAG). You can also deploy, undeploy, modify, or delete configured LAGs.

To display LAG information, perform the following step.

Click **Show** in the **Configure LAG** window.



Link Aggregation Group

Lag Id	Lag Name	Lag Type	Port Members	Lag Interface	Trunk Threshold	LACP Timeout	Port Count	LACP Key	Trunk Type	
256	blue	Static	1/1/1, 1/1/2	lg256	1	-	2	-	hash-based	Delete Modify
255	dynblue	Dynamic	1/1/3, 1/1/4, 1/1/5	lg255	1	L	3	20255	hash-based	Delete Modify
-	kablue	KeepAlive	1/1/8	1/1/8	-	L	1	9992	hash-based	Delete Modify
Lag Id	Lag Name	Lag Type	Port Members	Lag Interface	Trunk Threshold	LACP Timeout	Port Count	LACP Key	Trunk Type	

Total number of LAGs: 3 Total number of deployed LAGs: 3 Total number of trunks created:2 LACP System Priority / ID: 1 / cc4e.24b4.72c8 LACP Long timeout: 120, default: 120 LAC
Short timeout: 3, default: 3

[Add LAG]

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

This window has information fields for all LAG types; the fields are populated according to the LAG type, as follows:

- For static LAGs, the **LACP Timeout** and **LACP Key** fields display "–" because these parameters do not apply to static LAGs.
- For dynamic LAGs, the **Trunk Threshold** field displays "–" because this parameter does not apply to dynamic LAGs.

You can perform the following actions in this window:

- You can select the **Modify** button to display the **Link Aggregation Group** configuration window.
- You can select the **Add LAG** link to configure a new LAG.

Configuring a Static Station

- Adding a static station..... 179
- Modifying a static station..... 180

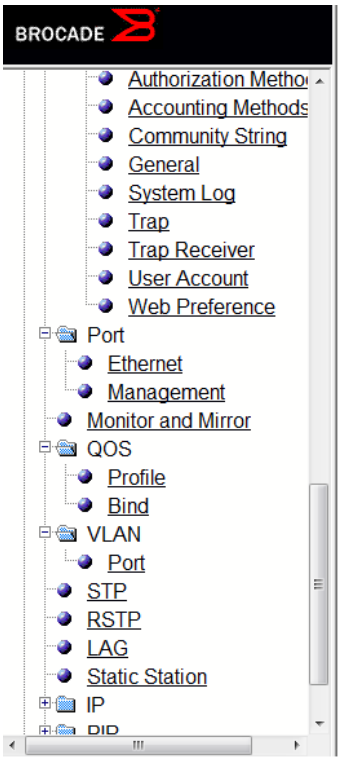
Adding a static station

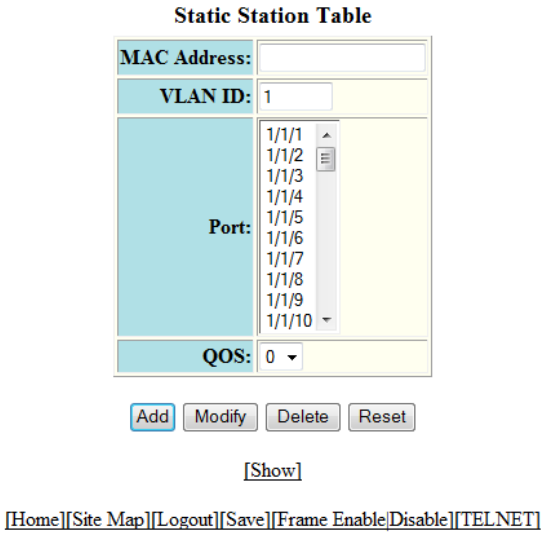
To configure a static MAC entry and assign the traffic priority (QoS) and VLAN membership (VLAN ID) to the entry, perform the following steps.

1. Click **Configure** on the left pane and select **Static Station**.

   The **Static Station Table** window is displayed as shown in the figure below.

   FIGURE 100 Configuring the static station





2. Type the MAC address of the device in *xx-xx-xx-xx-xx-xx* format in the **MAC Address** field.
3. Type the port-based VLAN identifier in the **VLAN ID** field. VLAN 1 is the default VLAN.
4. Select a port number or multiple port numbers in the **Port** list.
5. Select a QoS priority in the **QOS** list. A static MAC entry can be assigned a priority from 0 through 7.

6. Click **Add**.

   The message `The change has been made` is displayed. To display the configured static station, click **Show**.

   To reset the data entered in the configuration pane, click **Reset**. You can also delete the configured static station entry by clicking **Delete**.

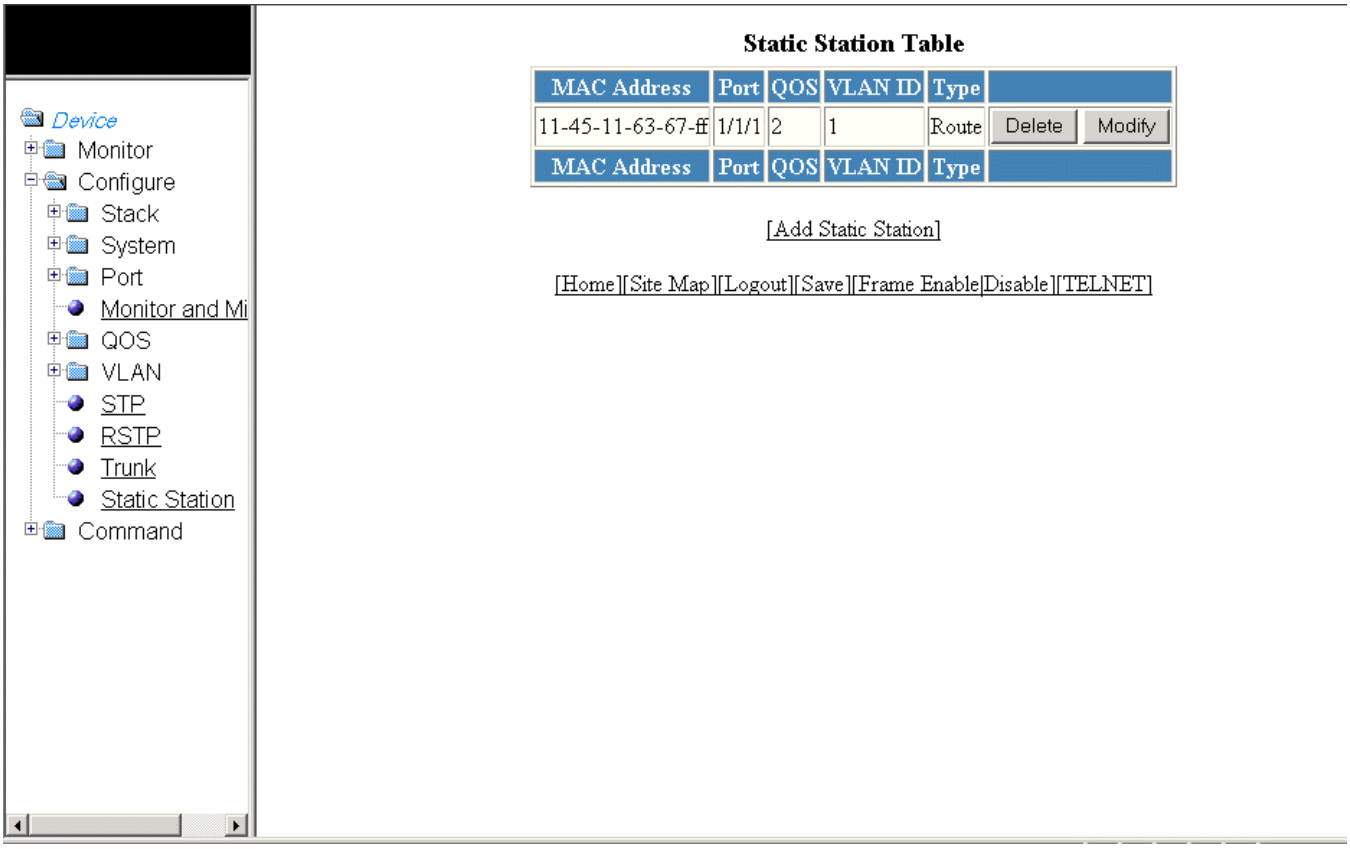
Modifying a static station

After you configure a static station, you can modify the port number, QoS priority, VLAN ID, and device type of the entry by performing the following steps.

1. Click **Configure** on the left pane and select **Static Station**.

   The **Static Station Table** window is displayed as shown in the figure below.

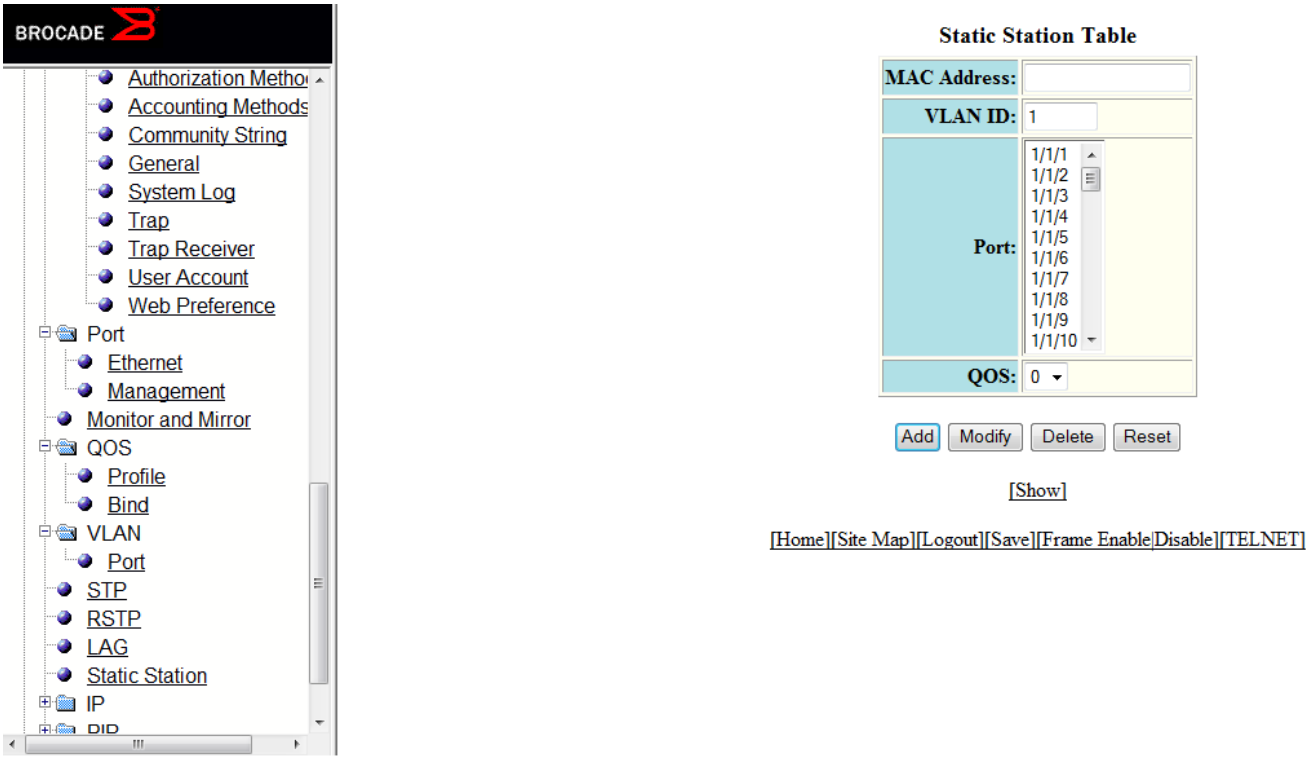
FIGURE 101 Modifying the static station



2. Click **Modify** .

   The **Static Station Table** window is displayed as shown in the figure below.

   FIGURE 102 Modifying the static station



3. Type the port-based VLAN identifier in the **VLAN ID** field. VLAN 1 is the default VLAN.
4. Select a port number or multiple port numbers in the **Port** list.
5. Select a QoS priority in the **QOS** list. A static MAC entry can be assigned a priority from 0 through 7.
6. Click **Modify**.

   The message `The change has been made` is displayed and the configured values are reflected in the **Static Station** window. To display the modified static station, click **Show**.

   To reset the data entered in the configuration pane, click **Reset** . You can also delete the static station entry by clicking **Delete**.

Configuring IP

- Configuring the router IP address....183
- Configuring a standard ACL....185
- Configuring an extended ACL....186
- Configuring an IP access group....190
- Configuring an IP Autonomous System-path access list....192
- Configuring an IP community list....193
- Configuring an IP prefix list....194
- Configuring a DNS entry....196
- Configuring the general IP settings....197
- Configuring IP interfaces....199
- Configuring a static ARP....201
- Configuring a static RARP....202
- Configuring a UDP helper....204

The IP feature is specific to Ruckus ICX devices running Layer 3 code.

NOTE
The terms "Layer 3 switch" and "router" are used interchangeably in this chapter.

Configuring the router IP address

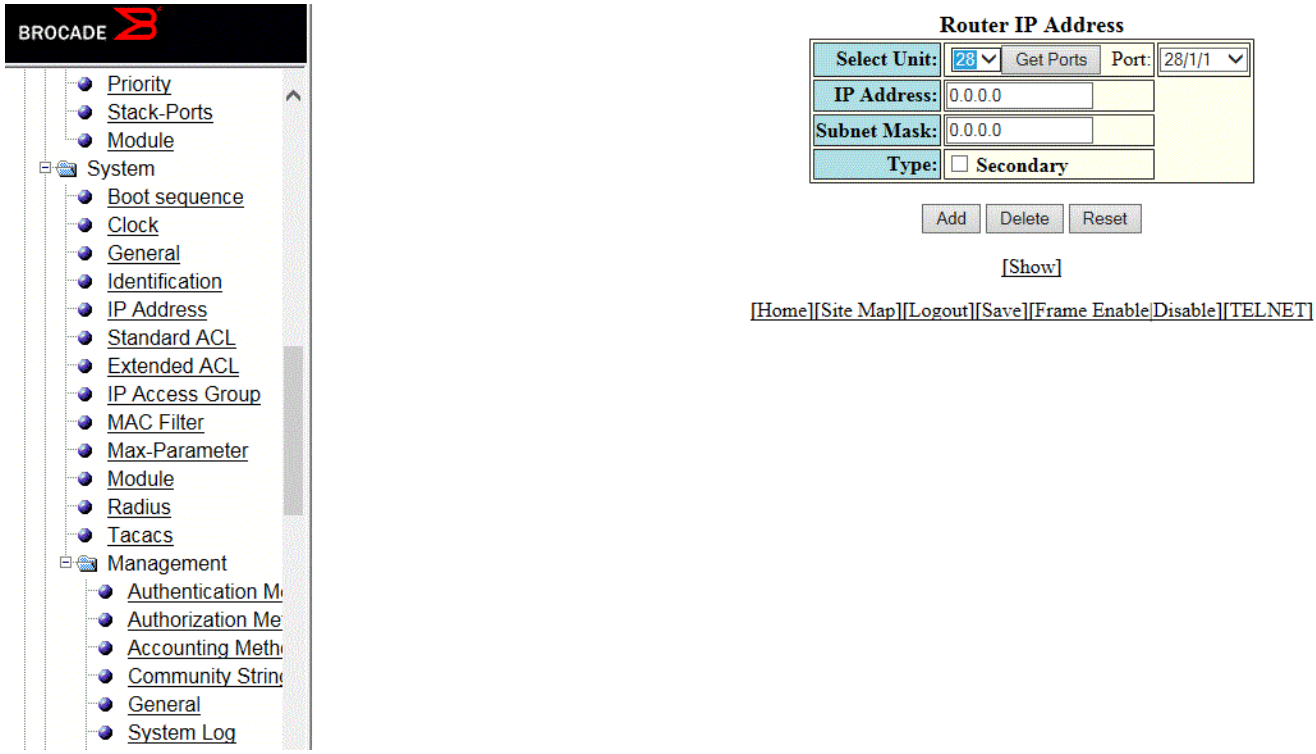
To configure an IP address to an interface, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Address**. The **Router IP Address** window is displayed.

3. Click **Add IP Address**.

   The **Router IP Address** window is displayed as shown in the figure below.

   FIGURE 103 Configuring router IP addresses



4. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.

5. Select a port in the **Port** list.
   - stack-unit/slotnum/portnum
6. Type the IP address of the device in the **IP Address** field.
7. Type the IP subnet mask in the **Subnet Mask** field.
8. Select the **Secondary** check box for **Type** if you have already configured an IP address within the same subnet on the interface.
9. Click **Add**.

   The message `The change has been made` is displayed and the specified IP address is assigned to the interface. To display the configured router IP address, click **Show**.

   To delete the configured IP address, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a standard ACL

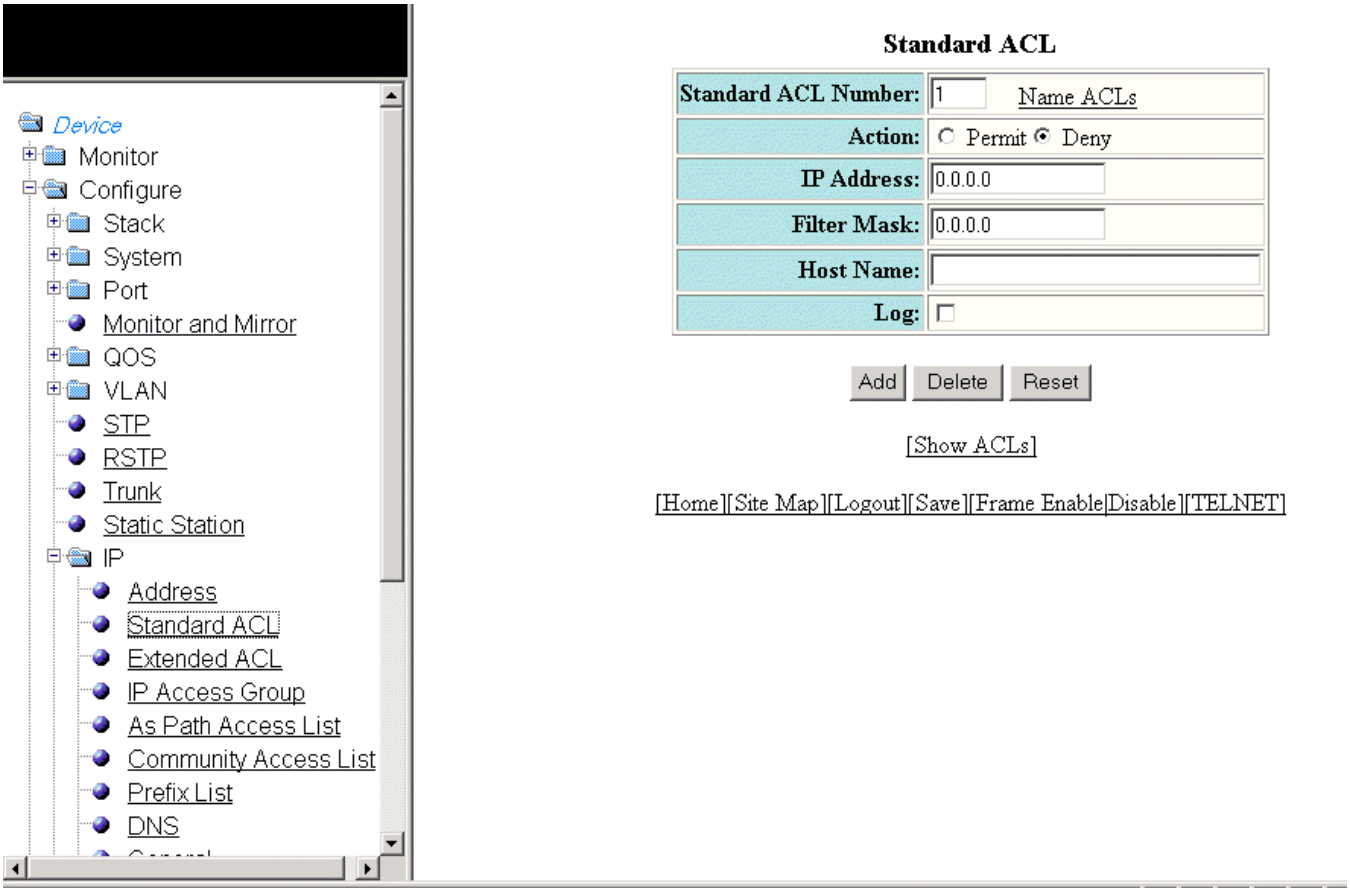
To configure a standard ACL, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .
2. Click **Standard ACL** .

   The **Standard ACL** window is displayed as shown in the figure below.

   NOTE
   Web GUI does not have ACL Sequence number support.

FIGURE 104 Configuring standard ACLs



3. Type the ACL number from 1 through 99 in the **Standard ACL Number** field. If you want to type an ACL name, click **Name ACLs** . The field label changes to **Standard ACL Name** . Now you can type an ACL name up to 256 alphanumeric characters in length.
4. Click **Permit** or **Deny** for **Action** so that the packets that match a policy in the ACL can be permitted (forwarded) or denied (dropped).
5. Type the host IP address in the **IP Address** field.
6. Type the IP subnet mask in the **Filter Mask** field.
7. Type the host name in the **Host Name** field.

8. Select the **Log** check box so that the device generates syslog entries and SNMP traps for the packets that are denied by the access policy.
9. Click **Add** .

   The message `The change has been made` is displayed and the ACL is added. To display the configured ACL, click **Show ACLs** .

   To delete the configured ACL, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring an extended ACL

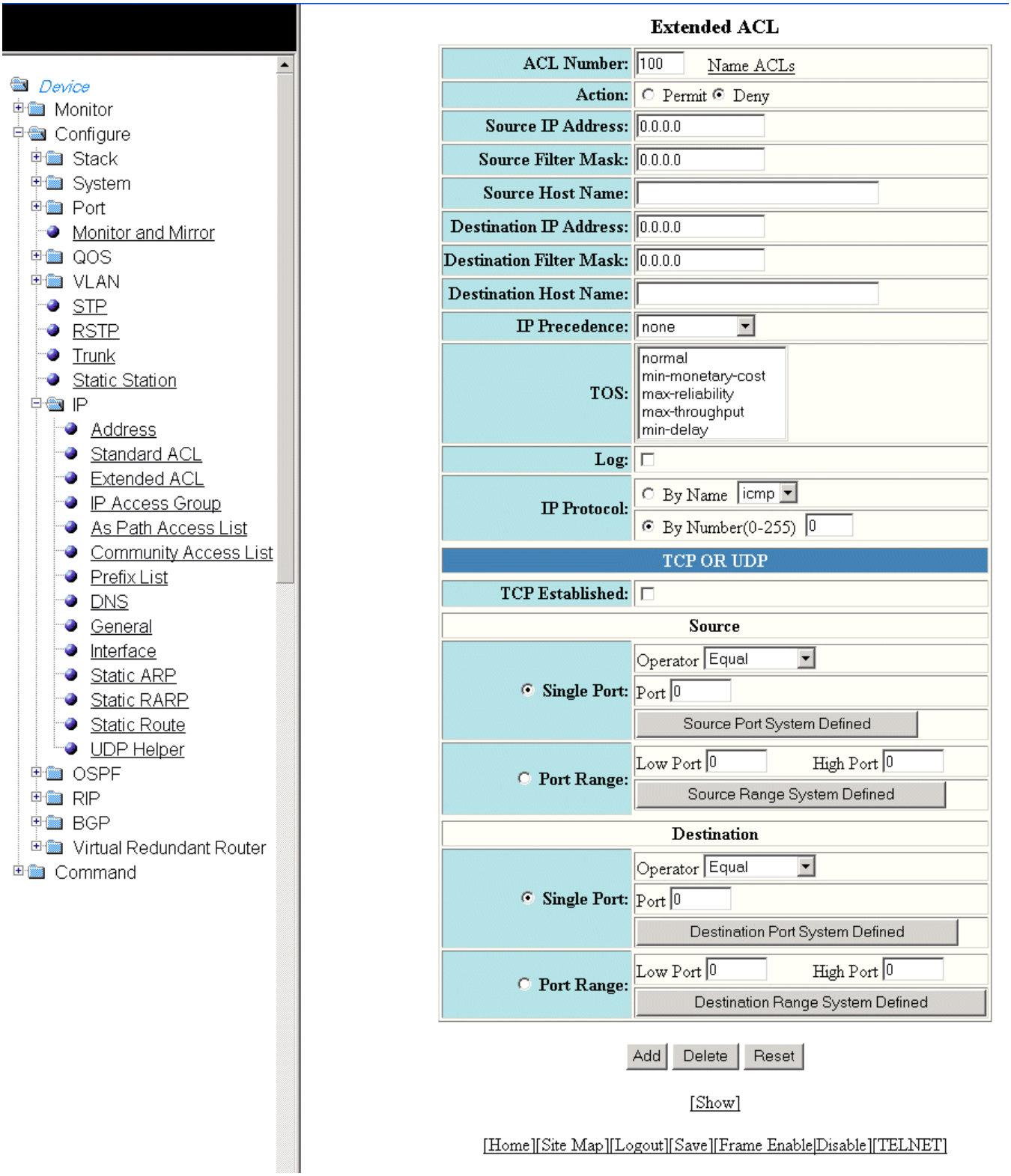
To configure an extended numbered ACL, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **Extended ACL** .

   The **Extended ACL** window is displayed as shown in the figure below.

FIGURE 105 Configuring an extended ACL



3. Type the extended ACL number from 100 through 199 in the **ACL Number** field. If you want to specify the extended ACL name, click **Name ACLs** . The field label is changed to **ACL Name** .
4. Click **Permit** or **Deny** for **Action** so that the packets that match the policy can be forwarded or dropped.
5. Type the source IP address in the **Source IP Address** field.
6. Type the source mask in the **Source Filter Mask** field.
7. Type the source host name in the **Source Host Name** field.
8. Type the destination IP address in the **Destination IP Address** field.
9. Type the destination mask in the **Destination Filter Mask** field.
10. Type the destination host name in the **Destination Host Name** field.
11. Select one of the following options in the **IP Precedence** list:
    - **routine** --The ACL matches packets that have the routine precedence.
    - **priority** --The ACL matches packets that have the priority precedence.
    - **immediate** --The ACL matches packets that have the immediate precedence.
    - **flash** --The ACL matches packets that have the flash precedence.
    - **flash-override** --The ACL matches packets that have the flash override precedence.
    - **critical** --The ACL matches packets that have the critical precedence.
    - **internet** --The ACL matches packets that have the internetwork control precedence.
    - **network** --The ACL matches packets that have the network control precedence.
12. Select one of the following options in the **TOS** list:
    - **normal** --The ACL matches packets that have the normal ToS.
    - **min-monetary-cost** --The ACL matches packets that have the minimum monetary cost ToS.
    - **max-reliability** --The ACL matches packets that have the maximum reliability ToS.
    - **max-throughput** --The ACL matches packets that have the maximum throughput ToS.
    - **min-delay** --The ACL matches packets that have the minimum delay ToS.
13. Select the **Log** check box to enable generation of SNMP traps and syslog messages for packets denied by the ACL.
14. Click **By Name** for **IP Protocol** to select the IP protocol by name or click **By Number** to specify the number (from 0 through 255).
15. Select the **TCP Established** check box so that the policy applies to the TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. The policy applies only to the established TCP sessions, not to the new sessions.

    NOTE
    This field applies only to the destination TCP ports, not the source TCP ports.

16. Enter the following information for **Source** :
    a) To configure a single port, click **Single Port** .

       Select one of the following for **Operator** :

       - **Equal** --The policy applies to the TCP or UDP port name or number you enter.
       - **NotEqual** --The policy applies to all the TCP or UDP port numbers except the port number or port name you enter.
       - **LessThan** --The policy applies to the TCP or UDP port numbers that are less than the port number or the numeric equivalent to the port name you enter.
       - **GreaterThan** --The policy applies to the TCP or UDP port numbers greater than the port number or the numeric equivalent to the port name you enter.

       Click **Source Port System Defined**

    b) To configure a range of ports, click **Port Range** .

       Type the lower port number in the **Low Port** field and the highest port number in the **High Port** field.

       Click **Source Range System Defined** .
17. To configure the destination port settings under **Destination** , follow the procedure explained in step 16 .
18. Click **Add** .

    The message `The change has been made` is displayed. To display the configured extended numbered ACL, click **Show** .

    To delete the configured extended numbered ACL, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

    NOTE
    Web GUI does not have ACL Sequence number support.

Configuring an IP access group

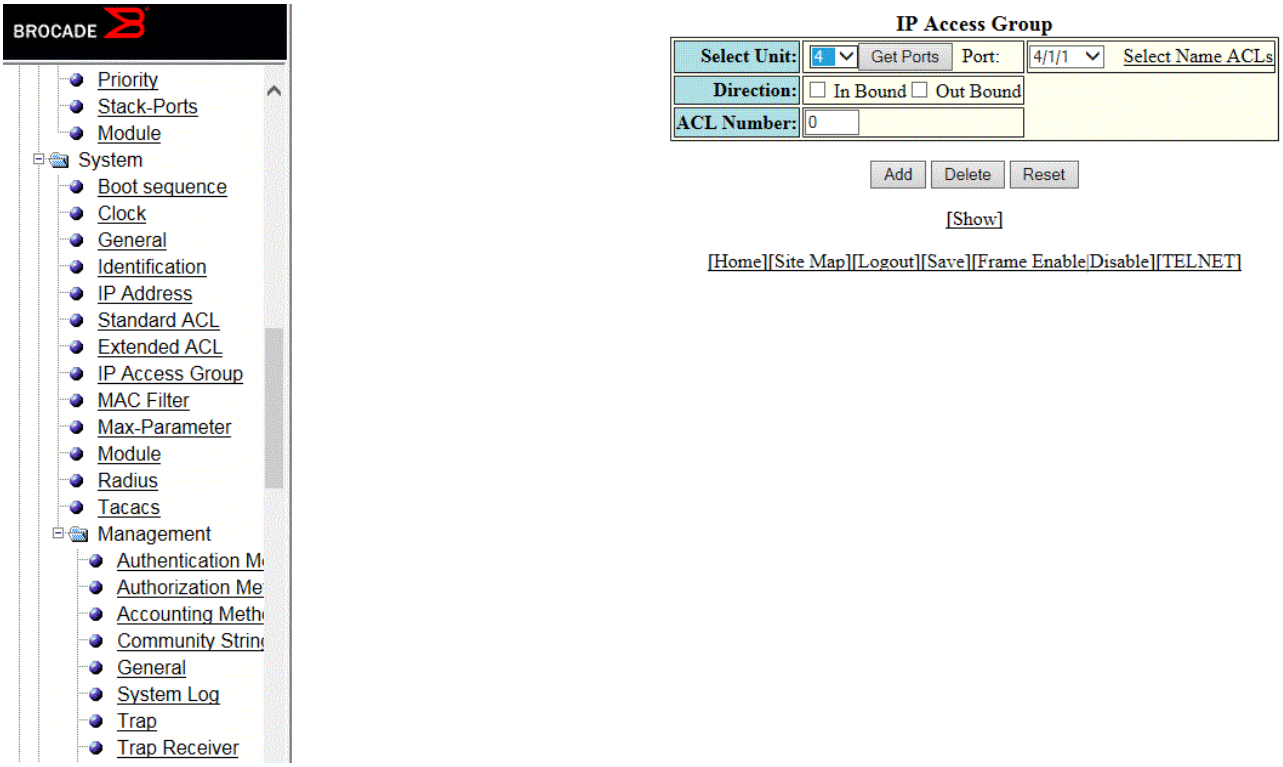
To configure an IP access group, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **IP Access Group** .

   The **IP Access Group** window is displayed as shown in the figure below.

FIGURE 106 Configuring IP access groups



3. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.

4. Select a port in the **Port** list.
   - – stack-unit/slotnum/portnum
5. Select the **In Bound** check box for **Direction** to enable incoming traffic on the interface to which you apply the ACL.
6. Type the ACL number in the **ACL Number** field. If you want to type an ACL name, click **Select Name ACLs** . The field label changes to **ACL Name** . Now you can type the ACL name up to 256 alphanumeric characters in length.
7. Click **Add** .

   The message `The change has been made` is displayed. To display the configured IP access group, click **Show** .

   To delete the configured IP access group, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

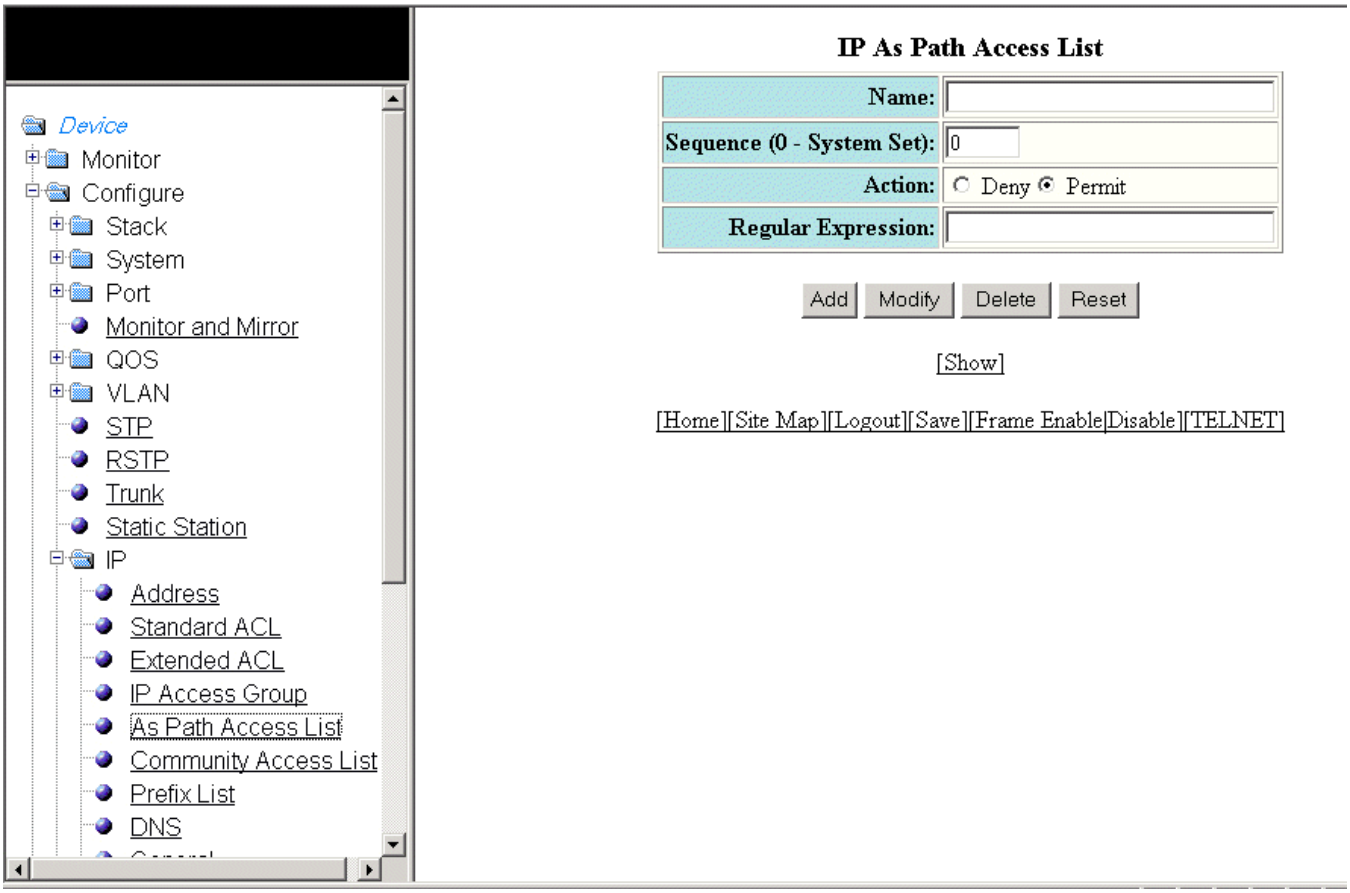
Configuring an IP Autonomous System-path access list

To configure an Autonomous System-path access list, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .
2. Click **Autonomou System Path Access List** .

   The **IP Autonomous System Path Access List** window is displayed as shown in the figure below.

   FIGURE 107 Configuring the IP Autonomous System-path access list



3. Type the ACL name in the **Name** field.
4. Type the Autonomous System-path list sequence number in the **Sequence (0 - System Set)** field. You can configure up to 199 entries in an Autonomous System-path list.

   If you do not specify a sequence number, the software numbers the entries in increments of five, beginning with number 5. The software interprets the entries in an Autonomous System-path list in numerical order, beginning with the lowest sequence number.
5. Click **Deny** or **Permit** for **Action** .

6. Type the Autonomous System-path information you want to permit or deny to routes that match any of the match statements within the ACL in the **Regular Expression** field.
7. Click **Add** .

   The message `The change has been made` is displayed. To display the configured Autonomous System-path list, click **Show** .

   To modify the Autonomous System-path list, click **Modify** . You can also delete the Autonomous System-path list by clicking **Delete** . To reset the data entered in the configuration pane, click **Reset** .

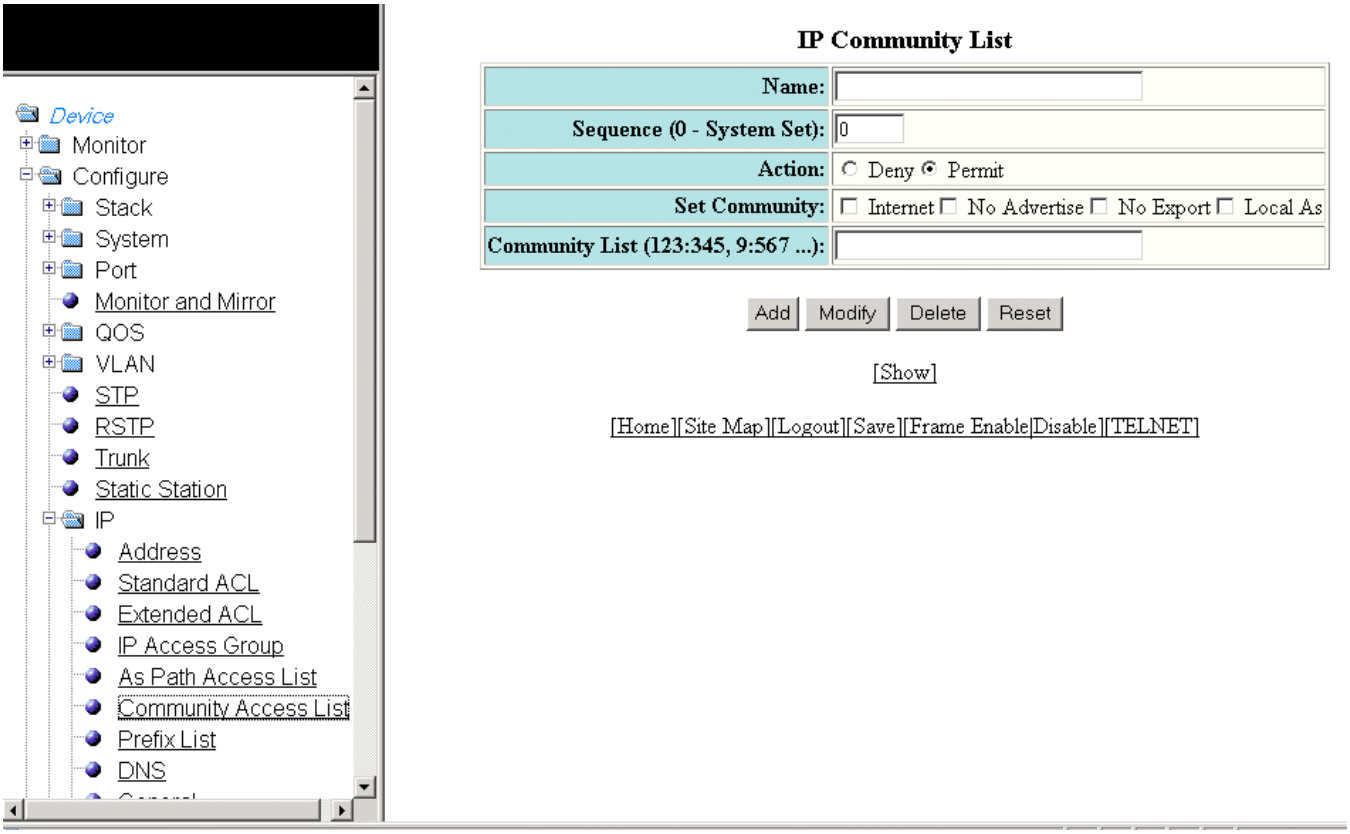
Configuring an IP community list

To configure an IP community list, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .
2. Click **Community Access List** .

   The **IP Community List** window is displayed as shown in the figure below.

   FIGURE 108 Configuring the IP community list



3. Type the ACL name in the **Name** field.

4. Type the community list sequence number in the **Sequence (0 - System Set)** field. You can configure up to 199 entries in a community list.

   If you do not specify a sequence number, the software numbers the entries in increments of five, beginning with number 5. The software interprets the entries in a community list in numerical order, beginning with the lowest sequence number.
5. Click **Deny** or **Permit** for **Action** .
6. Select one of the following options for **Set Community** :
   - **Internet** --The Internet community.
   - **No Advertise** --Routes with this community cannot be advertised to any other BGP Layer 3 switches.
   - **No Export** --The community of sub-Autonomous Systems within a confederation. Routes with this community can be exported to other sub-Autonomous Systems within the same confederation but cannot be exported outside the confederation to other Autonomous Systems or otherwise sent to EBGP neighbors.
   - **Local Autonomous System** --The local sub-Autonomous System within the confederation. Routes with this community can be advertised only within the local sub-Autonomous System.
7. Type the community number in *num* :*num* format in the **Community List** field.
8. Click **Add** .

   The message `The change has been made` is displayed. To display the configured community list, click **Show** .

   To modify the community list, click **Modify** . You can also delete the community list by clicking **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring an IP prefix list

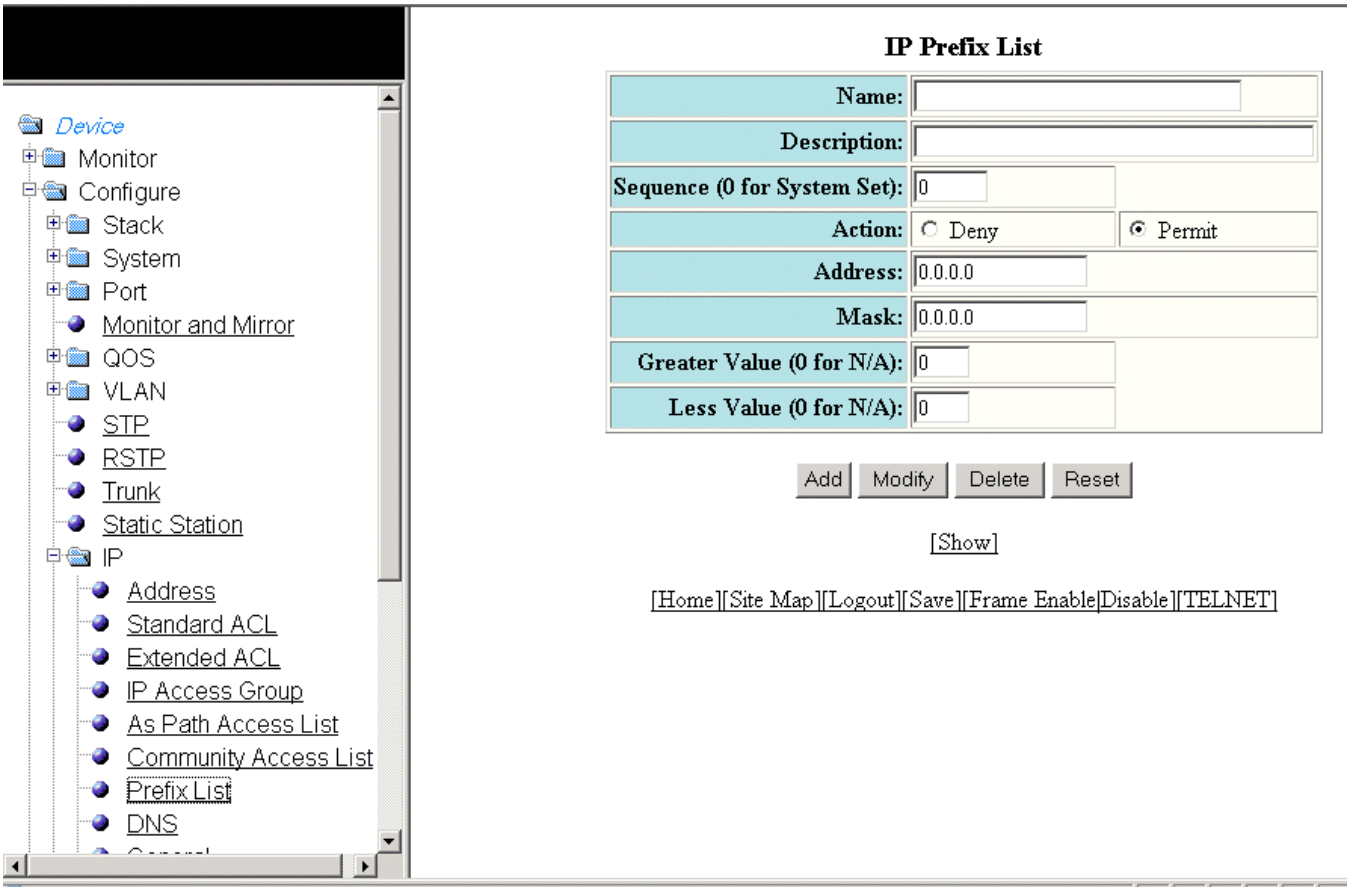
To configure an IP prefix list, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **Prefix List** .

   The **IP Prefix List** window is displayed as shown in the figure below.

FIGURE 109 Configuring IP prefix lists



3. Type the prefix list name in the **Name** field.
4. Type a text string describing the prefix list in the **Description** field.
5. Type the IP prefix list sequence number in the **Sequence (0 for System Set)** field. You can configure up to 100 prefix list entries.

   If you do not specify a sequence number, the software numbers the entries in increments of five, beginning with prefix list entry 5. The software interprets the prefix list entries in numerical order, beginning with the lowest sequence number.
6. Click **Deny** or **Permit** for **Action** .
7. Type the network IP address in the **Address** field.
8. Type the network mask address in the **Mask** field.
9. Type the maximum value of the mask length in the **Greater Value (0 for N/A)** field.

10. Type the least value of the mask length in the **Less Value (0 for N/A)** field.

    NOTE
    The **Greater Value (0 for N/A)** or **Less Value (0 for N/A)** values you specify must meet the following condition:Length < Greater Value <= Less Value <= 32

11. Click **Add** .

    The message `The change has been made` is displayed. To display the configured IP prefix list, click **Show** .

    To modify the IP prefix list, click **Modify** . You can also delete the IP prefix list by clicking **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring a DNS entry

You can configure the Ruckus device to recognize up to four Domain Name System (DNS) servers. The first entry serves as the primary default address. If a query to the primary address fails to be resolved after three attempts, the next DNS address is queried (also up to three times). This process continues for each defined DNS address until the query is resolved. The order in which the default DNS addresses are polled is the same as the order in which you enter them.

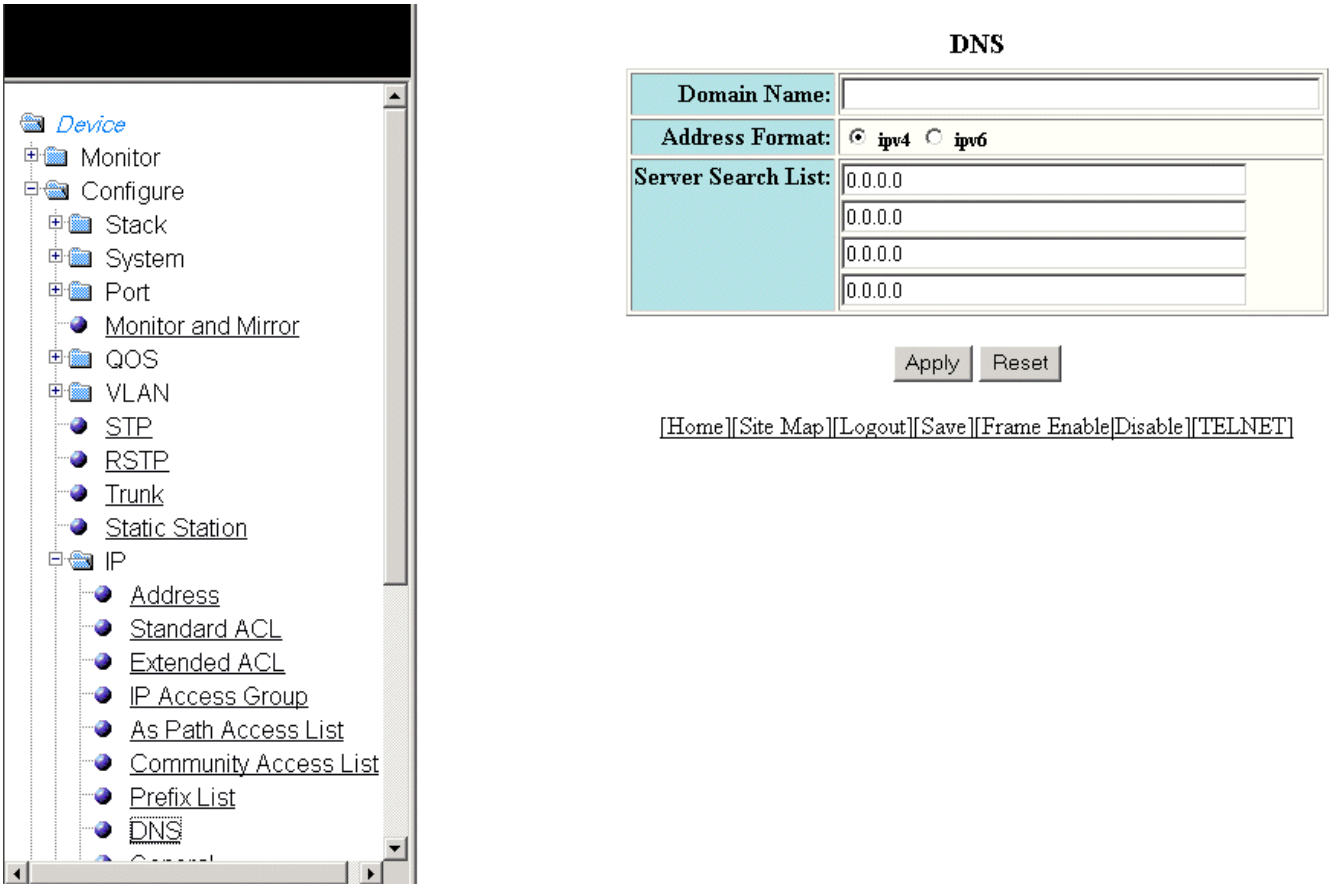
To configure DNS, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **DNS** .

   The **DNS** window is displayed as shown in the figure below.

   FIGURE 110 Configuring a DNS entry



3. Type the domain name in the **Domain Name** field.
4. Click **ipv4** or **ipv6** for **Address Format** .
5. Type the IPv4 or IPv6 address of the DNS in the **Server Search List** fields.
6. Click **Apply** .

   The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring the general IP settings

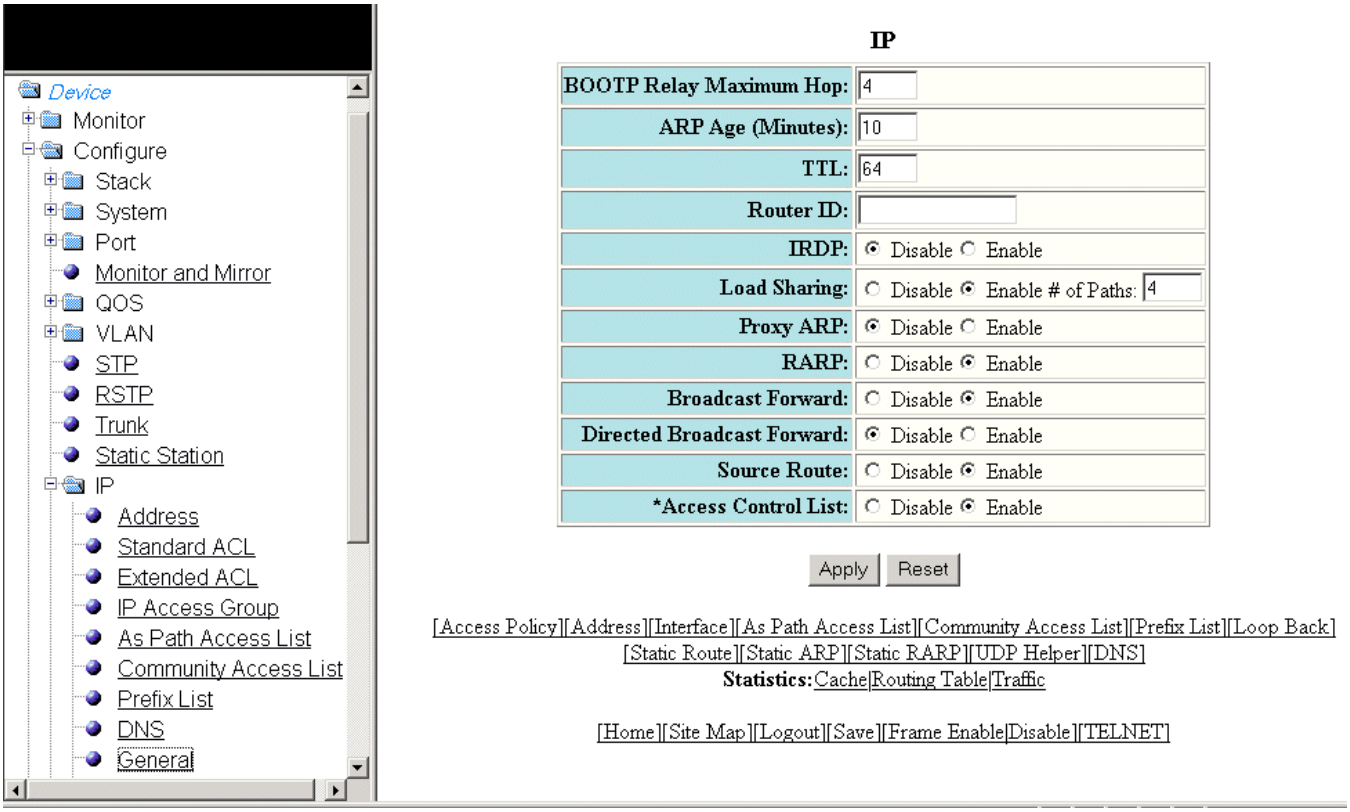
To configure the general IP settings, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **General** .

   The **IP** window is displayed as shown in the figure below.

FIGURE 111 Configuring the general IP settings



3. Type the maximum number of hops away a BootP server can be located from a Layer 3 switch and still be used by the router clients for network booting in the **BOOTP Relay Maximum Hop** field. The range is from 1 through 15. The default value is 4 hops.
4. Type the amount of time the device should keep a MAC address learned through ARP in the device ARP cache in the **ARP Age (Minutes)** field. The range is from 0 through 240 minutes. The default is 10 minutes.
5. Type the maximum number of Layer 3 switches (hops) through which a packet can pass before being discarded in the **TTL** field. The range is from 1 through 255 hops. The default is 64 hops.
6. Type the Layer 3 switch identifier in the **Router ID** field.
7. Click **Disable** or **Enable** for **IRDP** . By default, this protocol is disabled.

   ICMP Router Discovery Protocol (IRDP) is an IP protocol a Layer 3 switch can use to advertise the IP addresses of its interfaces to the directly attached hosts.
8. Click **Disable** or **Enable** for **Load Sharing** . If you click **Enable** , type the number of load sharing paths in the **# of Paths** field.
9. Click **Disable** or **Enable** for **Proxy ARP** .

   Proxy ARP is an IP mechanism a Layer 3 switch can use to answer an ARP request on behalf of a host, by replying with the Layer 3 switch's own MAC address instead of the host.

10. Click **Disable** or **Enable** for **RARP** .

    Reverse ARP (RARP) is an IP mechanism a host can use to request an IP address from a directly attached Layer 3 switch when the host boots.
11. Click **Disable** or **Enable** for **Broadcast Forward** .
12. Click **Disable** or **Enable** for **Directed Broadcast Forward** .

    A directed broadcast is a packet containing all ones (or in some cases, all zeros) in the host portion of the destination IP address. When a Layer 3 switch forwards such a broadcast, it sends a copy of the packet to each of its enabled IP interfaces.
13. Click **Disable** or **Enable** for **Source Route** .
14. Click **Disable** or **Enable** for **Access Control List** .
15. Click **Apply** .

    The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

Configuring IP interfaces

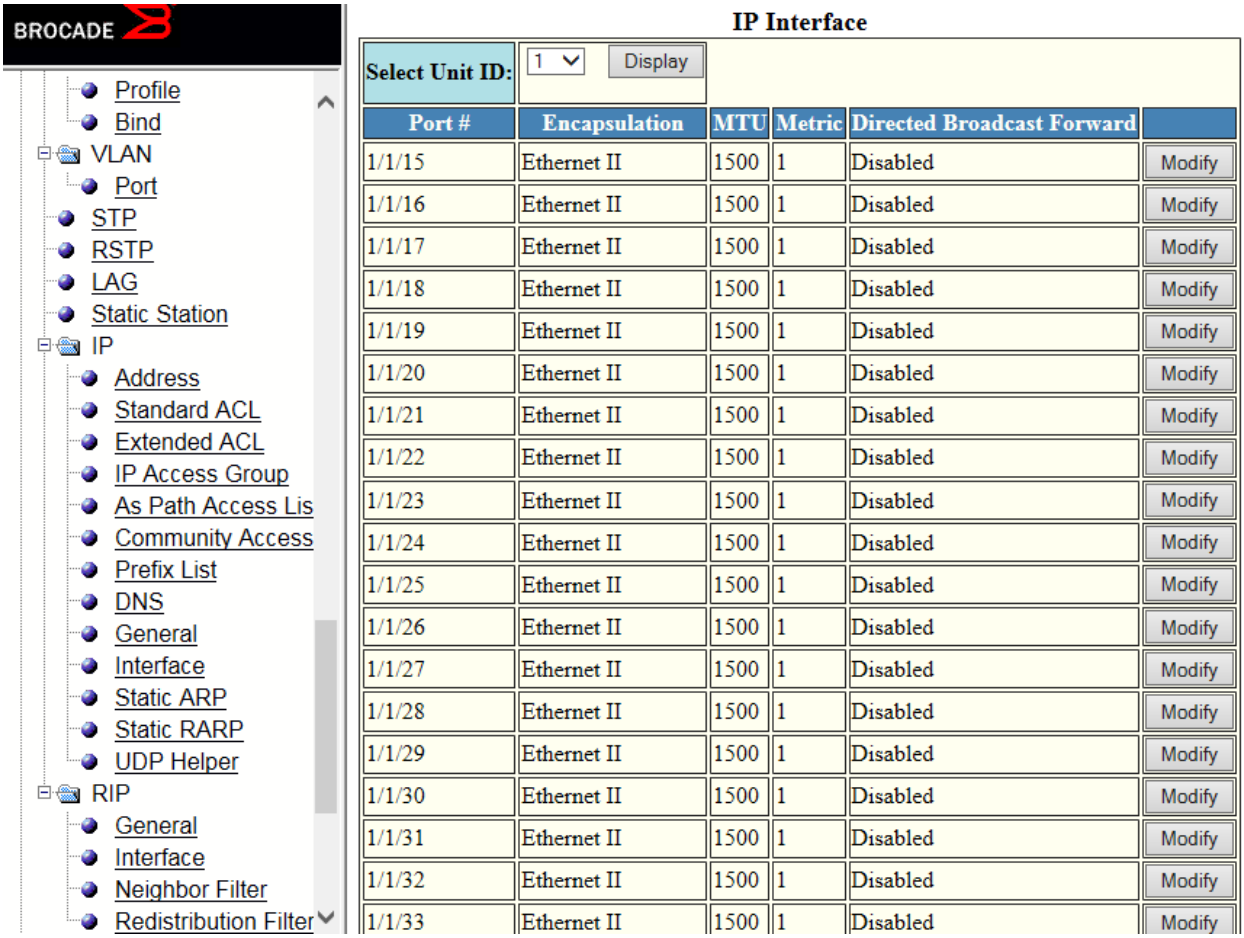
To configure an IP interface, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .

2. Click **Interface** .

   The **IP Interface** window is displayed as shown in the figure below.

FIGURE 112 IP Interface window

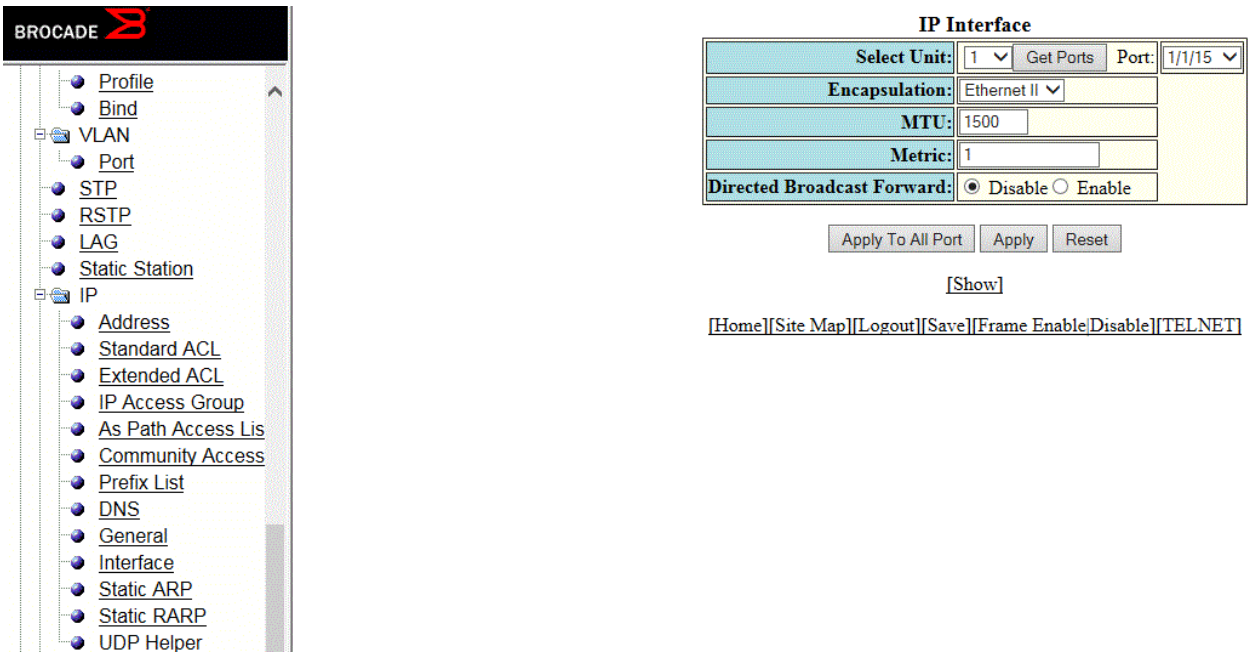


3. Select a Unit ID from the **Select Unit ID** list and click **Display** to view the IP properties table.

4. Click **Modify**.

   The **IP Interface** window is displayed in which stack unit and ports can be specified.

   FIGURE 113 Configuring an IP interface



5. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
6. Select the format of the Layer 2 packets in the **Encapsulation** list.
7. Type the maximum size of the IP packet when encapsulated in a Layer 2 packet, in the **MTU** field.
8. Type the cost in the **Metric** field.
9. Click **Disable** or **Enable** for **Directed Broadcast Forward** .
10. Click **Apply** to configure the IP interface to the specified port or click **Apply To All Ports** to configure the IP interface on all the ports.

    The message `The change has been made` is displayed. To display the configured IP interface, click **Show** . To reset the data entered in the configuration pane, click **Reset** .

Configuring a static ARP

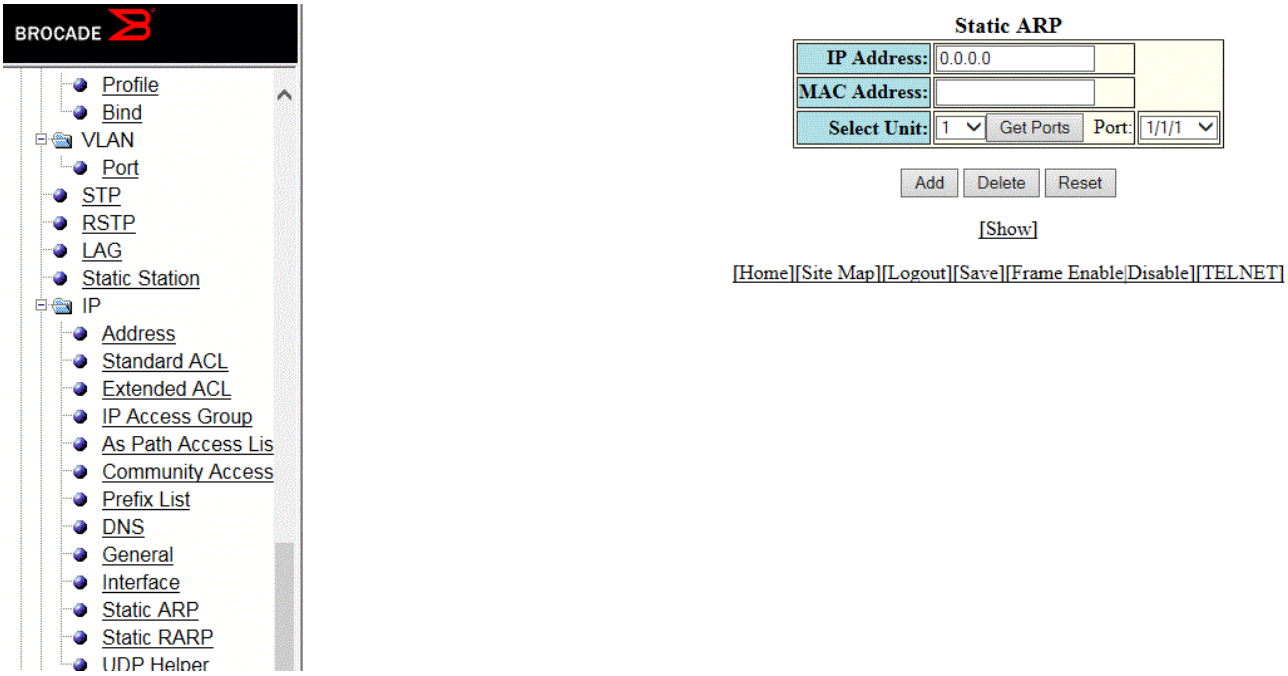
To configure a static Address Resolution Protocol (ARP) entry, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.

2. Click **Static ARP**.

   The **Static ARP** window is displayed as shown in the figure below.

FIGURE 114 Configuring static ARP



3. Type the IP address of the directly connected device in the **IP Address** field.
4. Type the MAC address of the device in *xx-xx-xx-xx-xx-xx* format in the **MAC Address** field.
5. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
6. Select a port from the **Port** list.
7. Click **Add** .

   The message `The change has been made` is displayed. To display the configured static ARP entry, click **Show** .

   To reset the data entered in the configuration pane, click **Reset** .

> **NOTE**
> The delete operation is not supported in 08.0.20 and later releases.

Configuring a static RARP

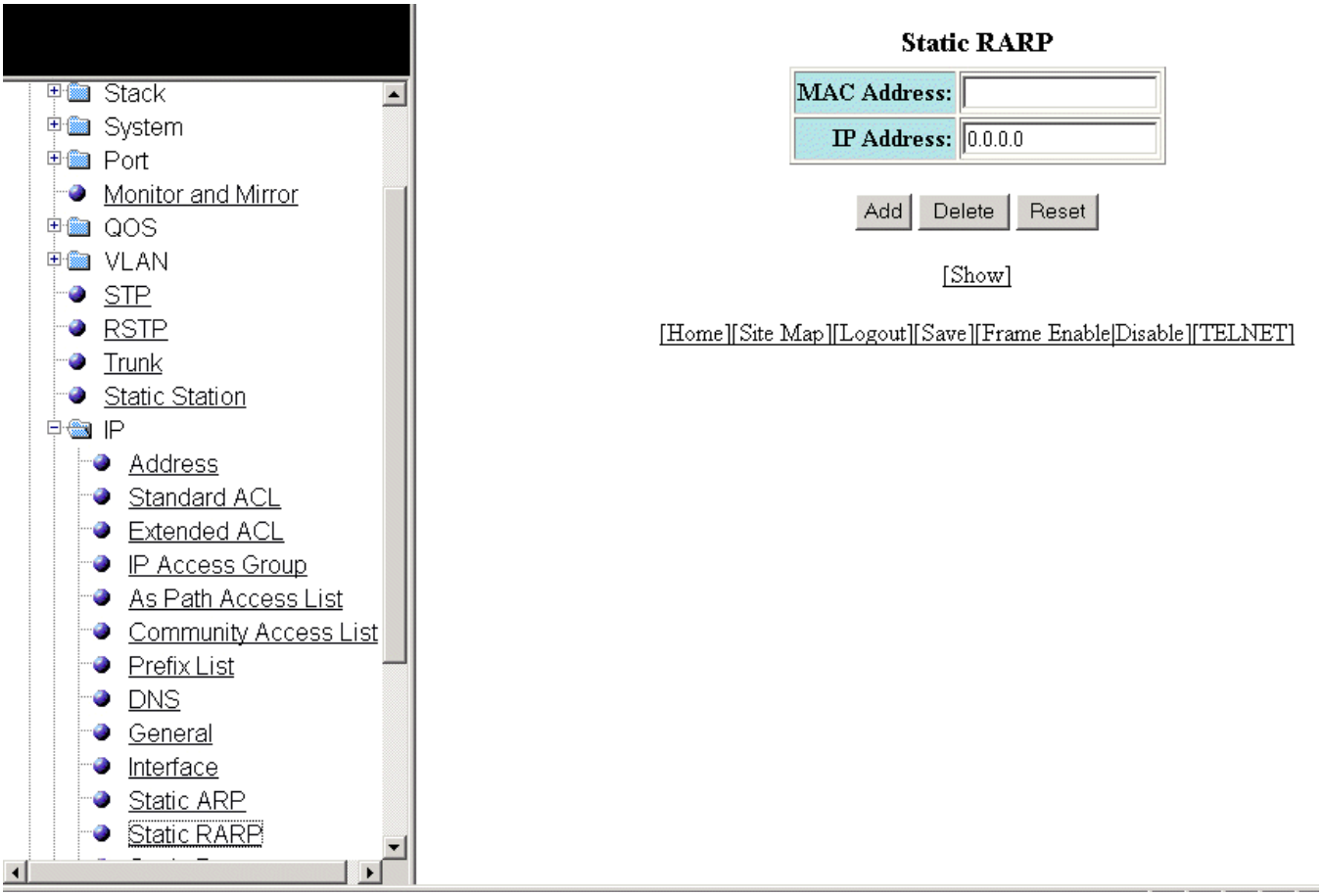
The Reverse Address Resolution Protocol (RARP) provides a simple mechanism for directly attached IP hosts to boot over the network. RARP allows an IP host that does not have a means of storing its IP address across power cycles or software reloads to query a directly attached Layer 3 switch for an IP address.

To configure a static IP RARP entry for static routes on a Ruckus ICX Layer 3 switch, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .
2. Click **Static RARP** .

   The **Static RARP** window is displayed as shown in the figure below.

   FIGURE 115 Configuring static RARP



3. Type the MAC address of the boot client in *xx-xx-xx-xx-xx-xx* format in the **MAC Address** field.
4. Type the IP address you want the Layer 3 switch to give to the client in the **IP Address** field.
5. Click **Add** .

   The message `The change has been made` is displayed. To display the configured static IP RARP entry, click **Show** .

   To delete the configured static IP RARP entry, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

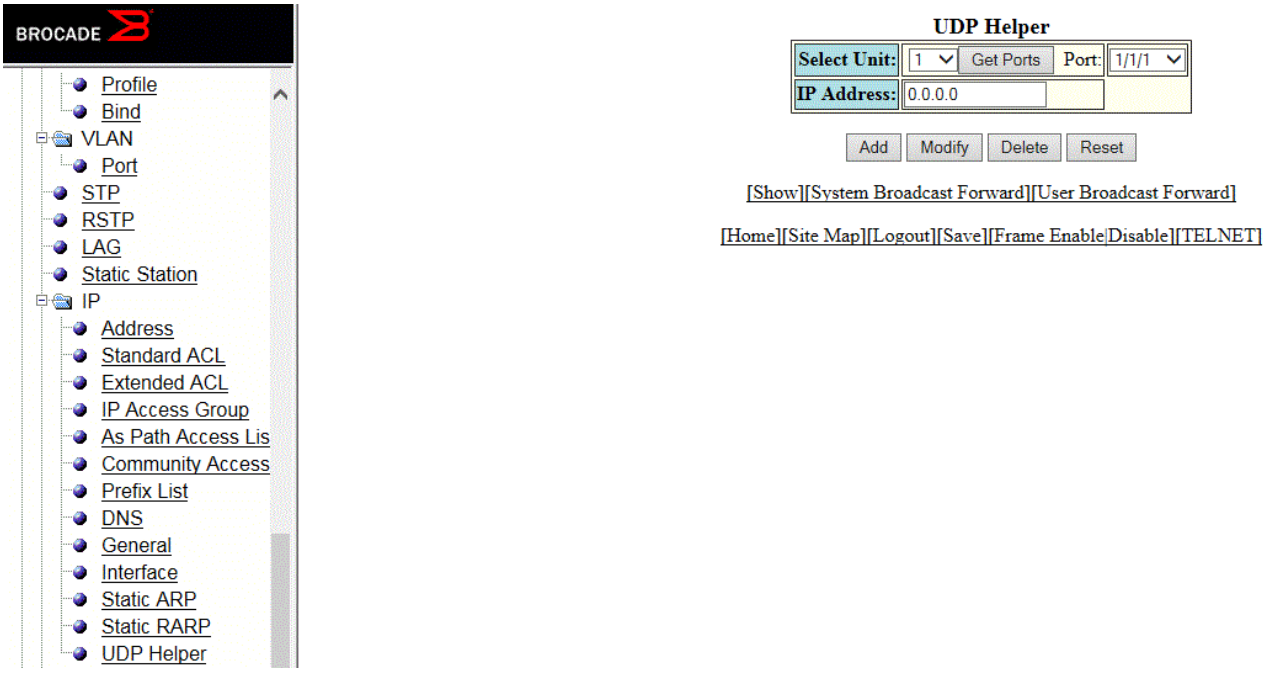
Configuring a UDP helper

To configure a helper address on the interface connected to the clients, perform the following steps.

1. Click **Configure** on the left pane and select **IP** .
2. Click **UDP Helper** .

   The **UDP Helper** window is displayed as shown in the figure below.

   FIGURE 116 Configuring UDP helper



3. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
4. Select an Ethernet port in the **Port** list.
5. Type the server IP address or the subnet directed broadcast address of the IP subnet the server belongs to in the **IP Address** field.
6. Click **Add** .

   The message `The change has been made` is displayed. To display the configured UDP helper, click **Show** .

   To modify the configured UDP helper, click **Modify** . You can also delete the UDP helper by clicking **Delete** . To reset the data entered in the configuration pane, click **Reset** .

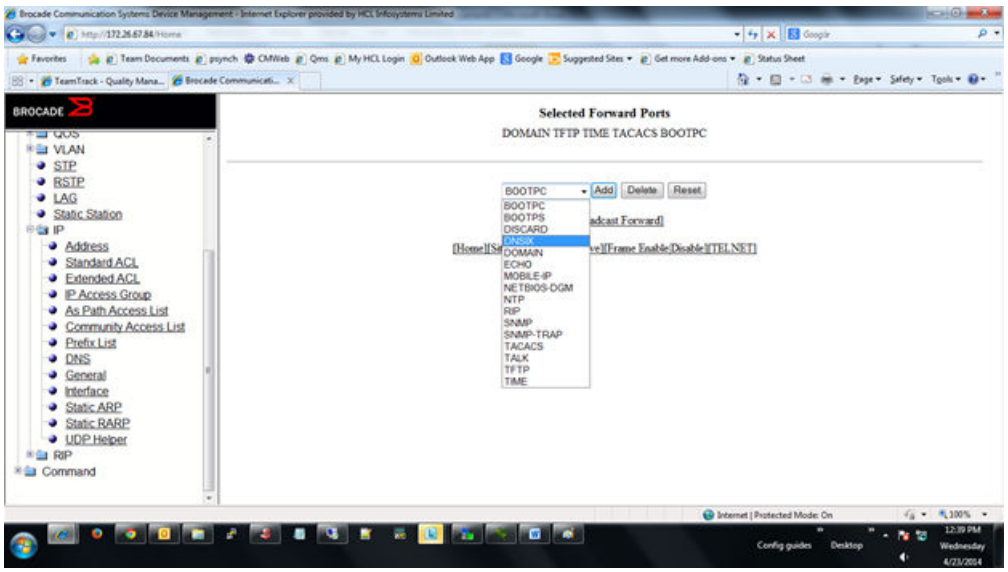
Enabling forwarding for a UDP application

To specify a UDP application by using an application name, perform the following steps.

1. Click **System Broadcast Forward** on the **UDP Helper** window.

   The system broadcast forward window is displayed as shown in this figure.

   FIGURE 117 Enabling forwarding for a UDP application



2. Select one of the following forward ports in the list:

   - **BOOTPC**
   - **BOOTPS**
   - **DISCARD**
   - **DNSIX**
   - **DOMAIN**
   - **ECHO**
   - **MOBILE-IP**
   - **NETBIOS-DGM**
   - **RIP**
   - **SNMP**
   - **SNMP-TRAP**
   - **TACACS**
   - **TALK**
   - **TFTP**
   - **TIME**

3. Click **Add** .

   The added port is displayed in the **Selected Forward Ports** pane, which displays the application ports that are enabled by default. To delete the forwarding port, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

   To specify the UDP application by using an application UDP port number, perform the following steps.

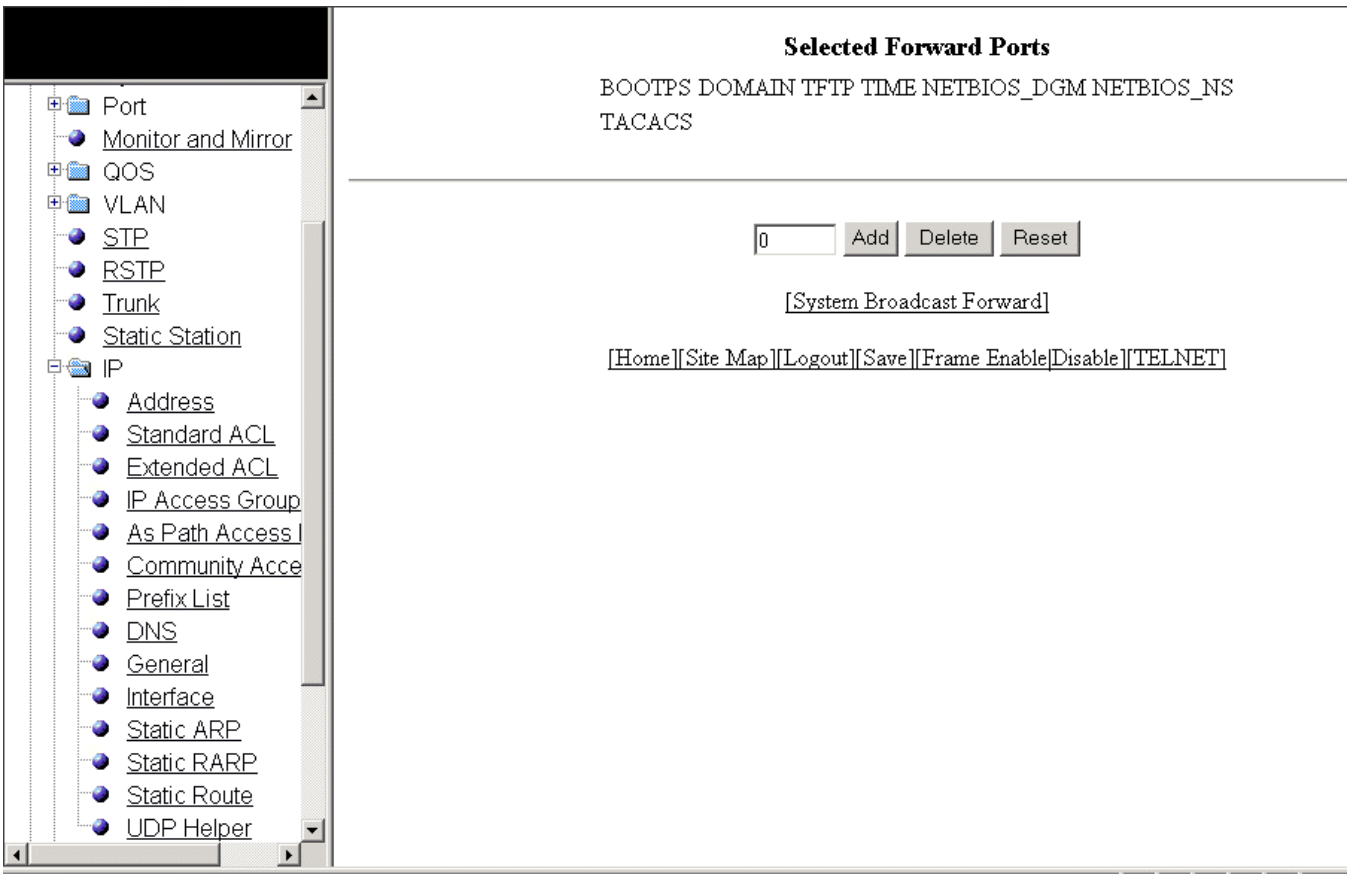
Specifying the UDP application

To specify the UDP application by using an application UDP port number, perform the following steps.

1. Click **User Broadcast Forward** on the **UDP Helper** window.

   The user broadcast forward window is displayed as shown in the figure below.

   FIGURE 118 Enabling user broadcast forward



2. Type the UDP port number in the field.
3. Click **Add**.

   The added port is displayed in the **Selected Forward Ports** pane, which displays the application ports that are enabled by default. To delete the forwarding port, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Configuring RIP

- Configuring the general RIP settings.....207
- Configuring a RIP interface..... 208
- Configuring a RIP neighbor filter.....212
- Configuring a RIP redistribution filter.....214

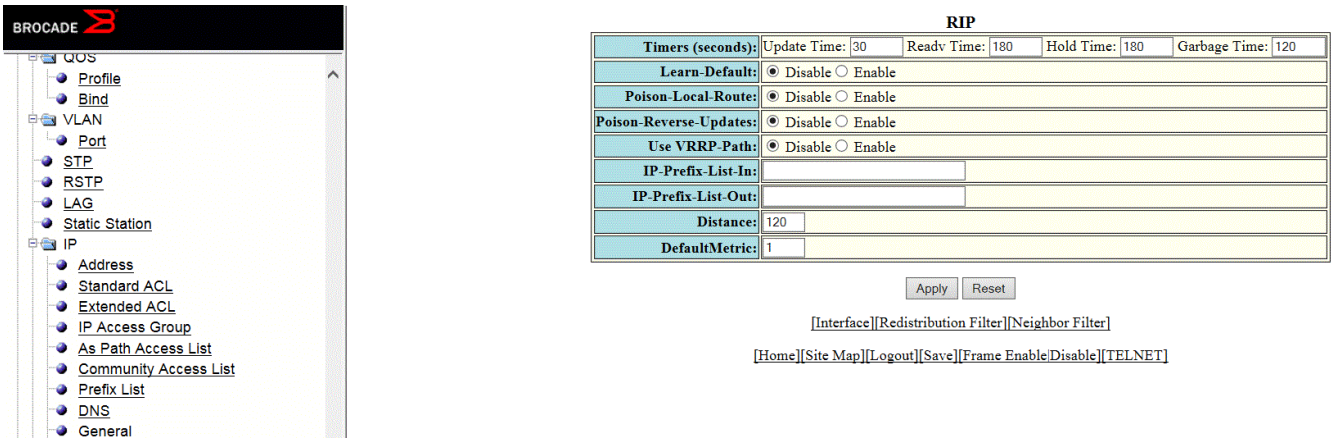
Configuring the general RIP settings

To configure the general RIP settings, perform the following steps.

1. Click **Configure** on the left pane and select **RIP** .
2. Click **General** .

   The **RIP** window is displayed as shown in the figure below.

   FIGURE 119 Configuring the general RIP settings



3. Configure the timer settings in the **Timers (seconds)**.
   - **Update Time**: Sets the amount of time between RIP routing updates. The default is 30 seconds. Possible values are 3 through 21845 seconds.
   - **Hold Time**: Sets the amount of time during which information about other paths is ignored. The default is 180 seconds. Possible values are 0 through 65535 seconds.
   - **Garbage Time**: Sets the amount of time after which a route is removed from the RIP routing table. The default is 120 seconds. Possible values are 0 through 65535.
4. Click **Disable** or **Enable** for the **Learn-Default** parameter that determines learning of default RIP routes.
5. Click **Disable** or **Enable** for the **Poison-Local-Route** parameter that determines avoiding routing loops by advertising local RIP routes with a cost of 16 ("infinite" or "unreachable") when these routes go down.
6. Click **Disable** or **Enable** for the **Poison-Reverse-Updates** parameter that determines poison reverse loop prevention, by assigning by assigning an "unreachable" cost to a route before advertising it on the interface where the route was learned.

7. Click **Disable** or **Enable** for the **Use VRRP-Path** parameter that suppresses RIP route advertisement on a VRRP or VRRPE backup interface.
8. Specify the prefix list to be applied to the routes, the device learns from its neighbors in the **IP-Prefix-List-In** field.
9. Specify the prefix list to be applied to the routes, the device advertises to its neighbors in the **IP-Prefix-List-out** field.
10. Specify the administrative distance that the RIP router adds to routes in the **Distance** field. By default, the RIP router assigns the default RIP administrative distance (120) to RIP routes.
11. Change the RIP metric the router assigns by default to redistributed routes in the **DefaultMetric** field. By default, a metric of 1 is assigned to each route that is redistributed into RIP.
12. Click **Apply** .

    The message `The change has been made` is displayed. To reset the data entered in the configuration pane, click **Reset** .

    The **RIP** window provides links to configure other RIP parameters:

    - To configure a RIP interface, click **Interface** . For more information, refer to Configuring a RIP interface on page 208.
    - To configure a RIP neighbor filter, click **Neighbor Filter** . For more information, refer to Configuring a RIP neighbor filter on page 212.

Configuring a RIP interface

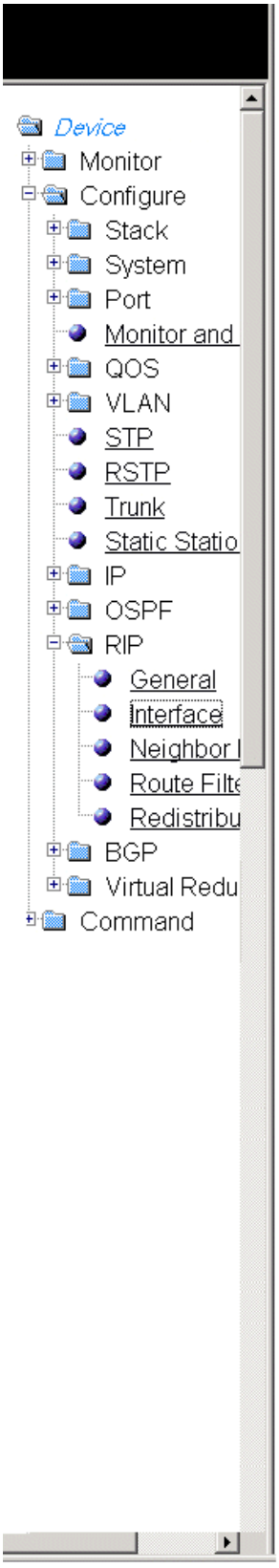
To configure a RIP interface, perform the following steps.

1. Click **Configure** on the left pane and select **RIP** .

2. Click **Interface** .

   The **RIP Interface** window is displayed as shown in the figure below.

FIGURE 120 RIP interface



RIP Interface

Port	Version	Poison Reverse	
1/1/1	Disabled	Enabled	Modify
1/1/2	Disabled	Enabled	Modify
1/1/3	Disabled	Enabled	Modify
1/1/4	Disabled	Enabled	Modify
1/1/5	Disabled	Enabled	Modify
1/1/6	Disabled	Enabled	Modify
1/1/7	Disabled	Enabled	Modify
1/1/8	Disabled	Enabled	Modify
1/1/9	Disabled	Enabled	Modify
1/1/10	Disabled	Enabled	Modify
1/1/11	Disabled	Enabled	Modify
1/1/12	Disabled	Enabled	Modify
1/1/13	Disabled	Enabled	Modify
1/1/14	Disabled	Enabled	Modify
1/1/15	Disabled	Enabled	Modify
1/1/16	Disabled	Enabled	Modify
1/1/17	Disabled	Enabled	Modify
1/1/18	Disabled	Enabled	Modify
1/1/19	Disabled	Enabled	Modify
1/1/20	Disabled	Enabled	Modify
1/1/21	Disabled	Enabled	Modify
1/1/22	Disabled	Enabled	Modify
1/1/23	Disabled	Enabled	Modify
1/1/24	Disabled	Enabled	Modify
mgmt1	Disabled	Enabled	Modify
1/2/1	Disabled	Enabled	Modify
1/2/2	Disabled	Enabled	Modify
Port	Version	Poison Reverse	

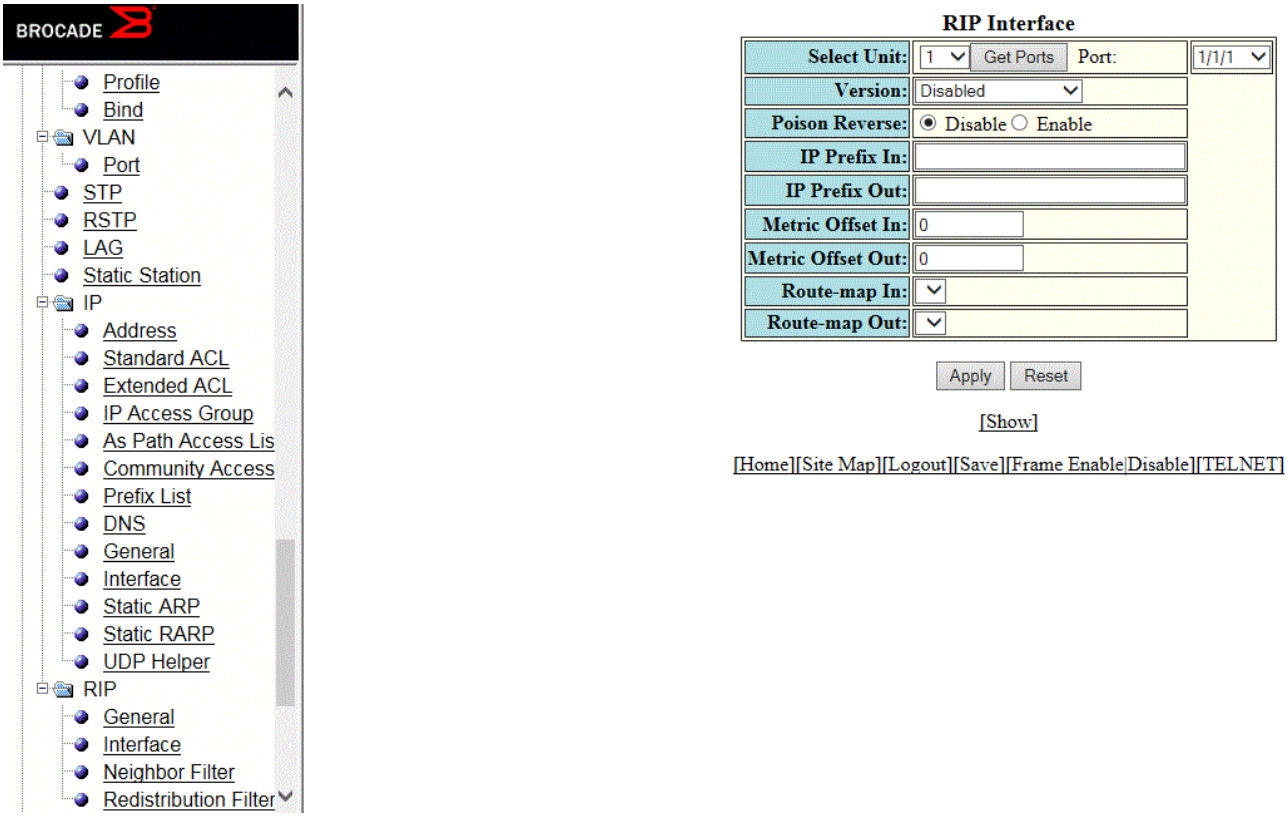
[Configure RIP Interface]

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

3. Click **Configure RIP Interface** or **Modify** to change the RIP interface parameters for the respective port.

   The **RIP Interface** window is displayed as shown in the figure below.

FIGURE 121 Configuring a RIP interface



4. Select a Unit ID from the **Select Unit** list and click **Get Ports** to retrieve the list of ports corresponding to the selected Unit ID.

   A message is displayed to indicate that the operation does not change the running configuration.
5. Select a port from the **Port** list.
6. Select one of the following options for **Version** :
   - **Disabled**
   - **V1 Only**
   - **V2 Only**
   - **V1-Compatible-V2**
7. Click **Disable** or **Enable** for **Poison Reverse** .

   Poison reverse is the method a Layer 3 switch uses to prevent routing loops caused by advertising a route on the same interface as the one on which the Layer 3 switch learned the route.
8. Enter the prefix list to be applied to the learned RIP routes in the **IP Prefix In** field.
9. Enter the prefix list to be applied to the advertised RIP routes in the **IP Prefix Out** field.
10. Enter the cost metric to be applied to the learned RIP routes in the **Metric Offset In** field.
11. Enter the cost metric to be applied to the advertised RIP routes in the **Metric Offset Out** field.

12. Specify the route map to be applied on the interface to filter the learned RIP routes in the **Route-map In** field.
13. Specify the route map to be applied on the interface to filter the advertised RIP routes in the **Route-map Out** field.
14. Click **Apply** to configure the RIP interface to the specified port or click **Apply All Port** to configure the RIP interface on all the ports.

    The message `The change has been made` is displayed. To display the configured RIP interface, click **Show** . To reset the data entered in the configuration pane, click **Reset** .

Configuring a RIP neighbor filter

By default, a Ruckus Layer 3 switch learns RIP routes from all its RIP neighbors. Neighbor filters allow you to specify the neighbor Layer 3 switches from which the Ruckus device can receive RIP routes. Neighbor filters apply globally to all ports.

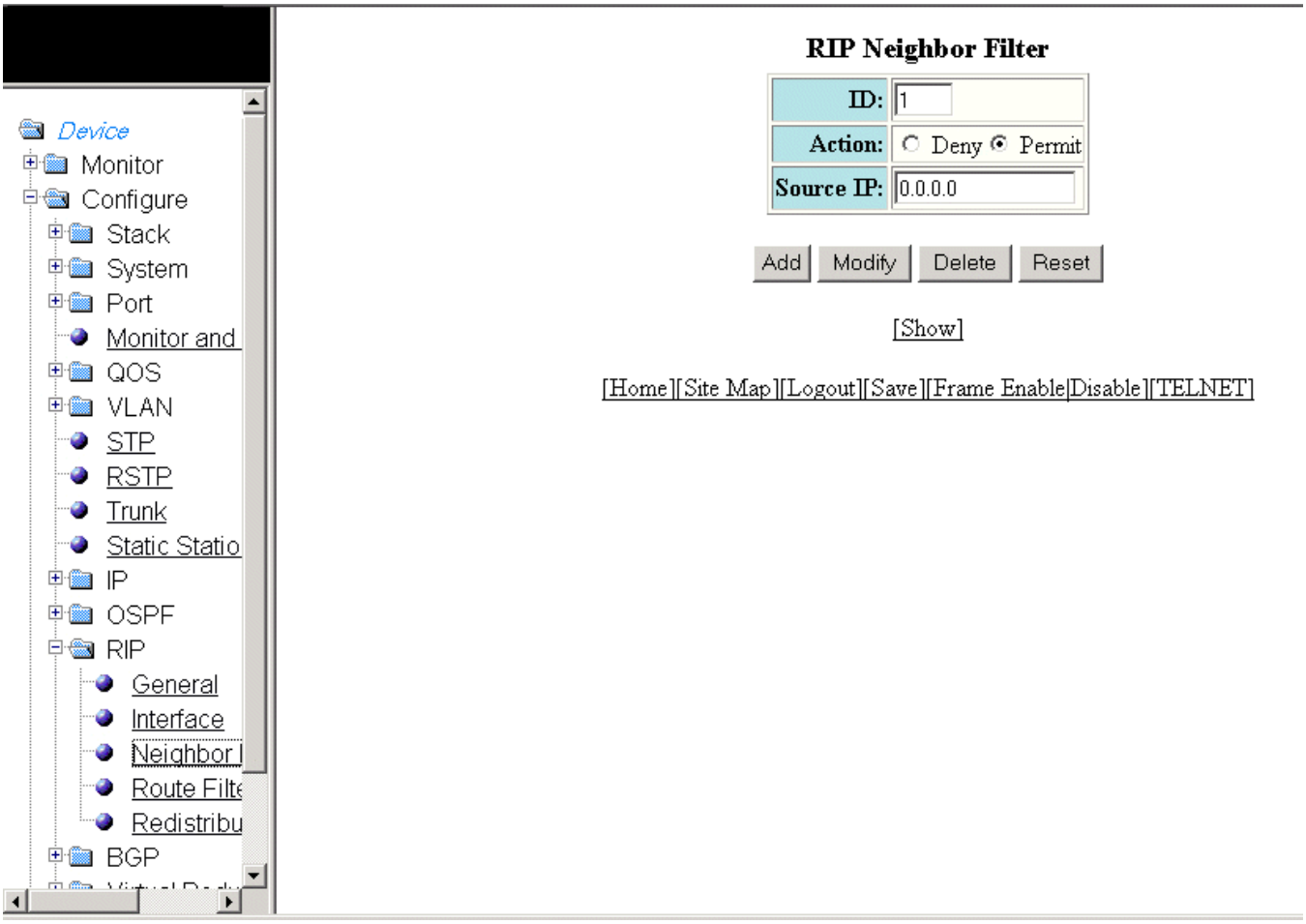
To configure a RIP neighbor filter, perform the following steps.

1. Click **Configure** on the left pane and select **RIP** .

2. Click **Neighbor Filter** .

   The **RIP Neighbor Filter** window is displayed as shown in the figure below.

   FIGURE 122 Configuring a RIP neighbor filter



3. Type a filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action** .
5. Type a source IP address in the **Source IP** field.
6. Click **Add** .

   The message `The change has been made` is displayed. To display the configured RIP neighbor filter, click **Show** .

   To modify the configured RIP neighbor filter, click **Modify** . To reset the data entered in the configuration pane, click **Reset** . You can also delete the configured RIP neighbor filter by clicking **Delete** .

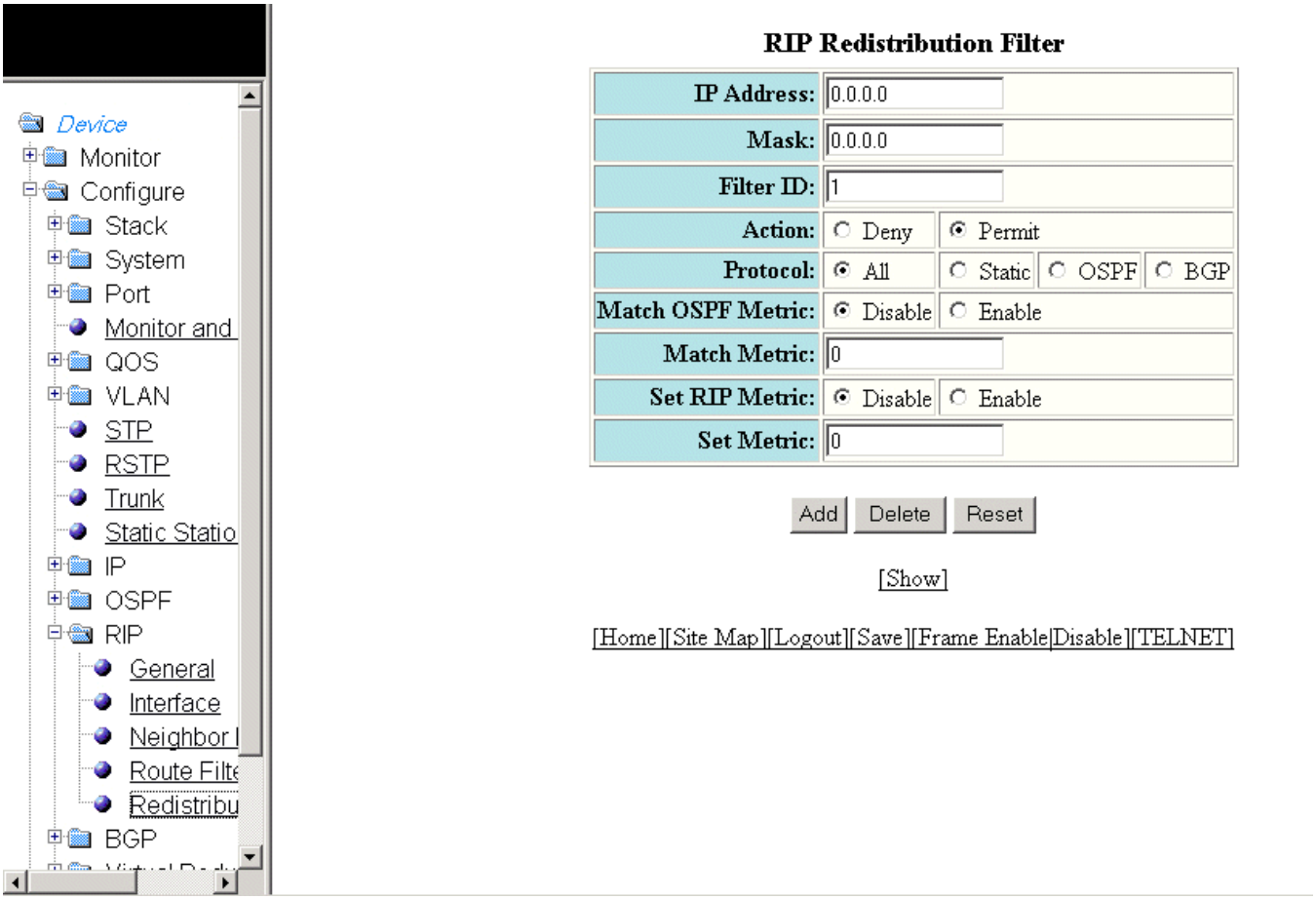
Configuring a RIP redistribution filter

To configure a RIP redistribution filter, perform the following steps.

1. Click **Configure** on the left pane and select **RIP** .
2. Click **Redistribution Filter** .

   The **RIP Redistribution Filter** window is displayed as shown in the figure below.

FIGURE 123 Configuring the RIP redistribution filter



3. Type a network IP address in the **IP Address** field.
4. Type an IP subnet mask in the **Mask** field.
5. Type a redistribution filter identifier in the **Filter ID** field.
6. Click **Deny** or **Permit** for **Action** .
7. Select one of the following options for **Protocol** :

- **All** --Applies redistribution to all route types.
- **Static** --Applies redistribution to IP static routes only.
- **OSPF** --Applies redistribution to OSPF routes only.
- **BGP** --Applies redistribution to BGP routes only.

8. Click **Disable** or **Enable** for **Set OSPF Metric** .
9. Type the match metric value from 1 through 15 in the **Match Metric** field. The match metric parameter applies the redistribution filter only to those routes with the specified metric value.
10. Click **Disable** or **Enable** for **Set RIP Metric** .
11. Type the RIP metric value in the **Set Metric** field.
12. Click **Add** .

    The message `The change has been made` is displayed. To display the configured RIP redistribution filter, click **Show** .

    To delete the configured RIP redistribution filter, click **Delete** . To reset the data entered in the configuration pane, click **Reset** .

Basic Device Commands

- Clearing information for a Layer 2 switch....217
- Clearing information for a Layer 3 switch....218
- Disabling or enabling the menu view....219
- Logging out....220
- Reloading units in a stack....221
- Saving the configuration to flash....222
- Switching over to the active role....223
- Accessing the Telnet command prompt....223
- Performing a trace....225

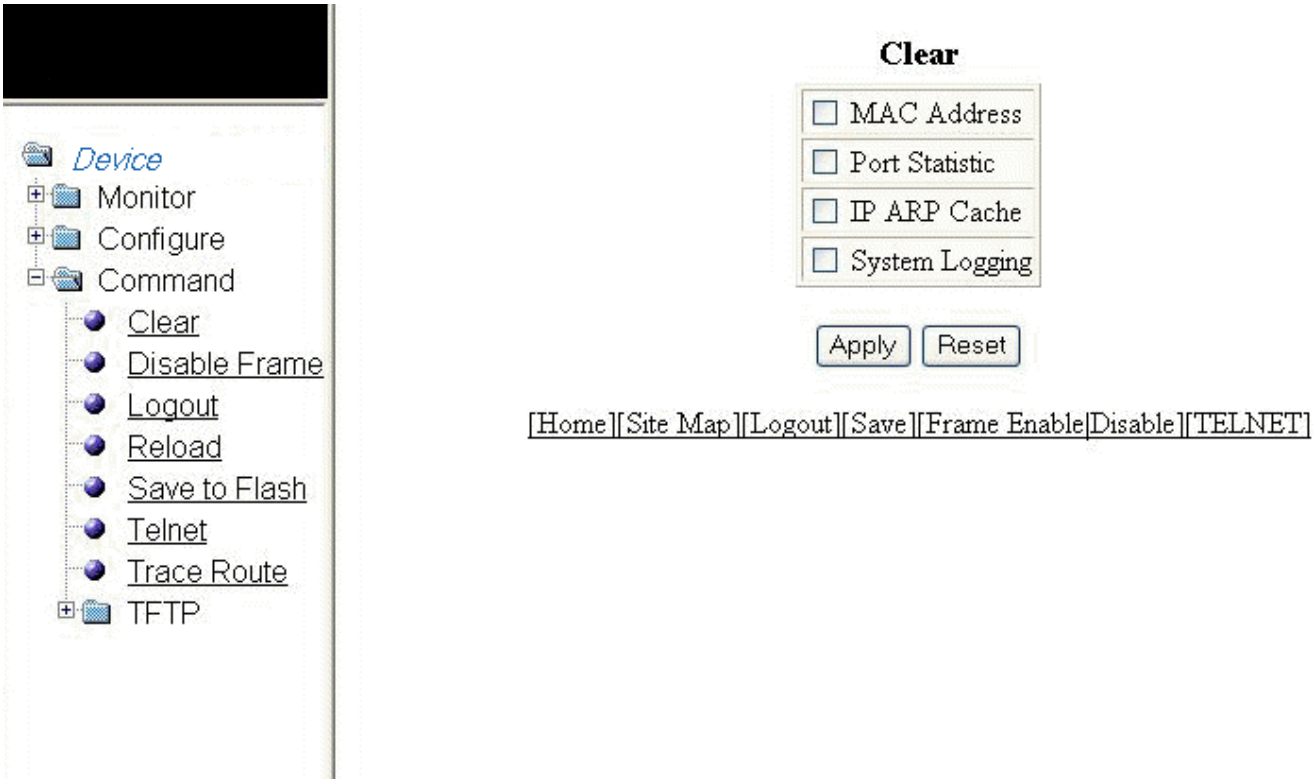
Clearing information for a Layer 2 switch

To clear specific data related to a Layer 2 switch, perform the following steps.

1. Click **Command** on the left pane and select **Clear.**

   The **Clear** window is displayed as shown in the figure below.

FIGURE 124 Clear window



2. Select the following check boxes to clear information:
   - **MAC Address**
   - **Port Statistic**
   - **IP ARP Cache**
   - **System Logging**
3. Click **Apply** .

   All the current entries will be deleted.

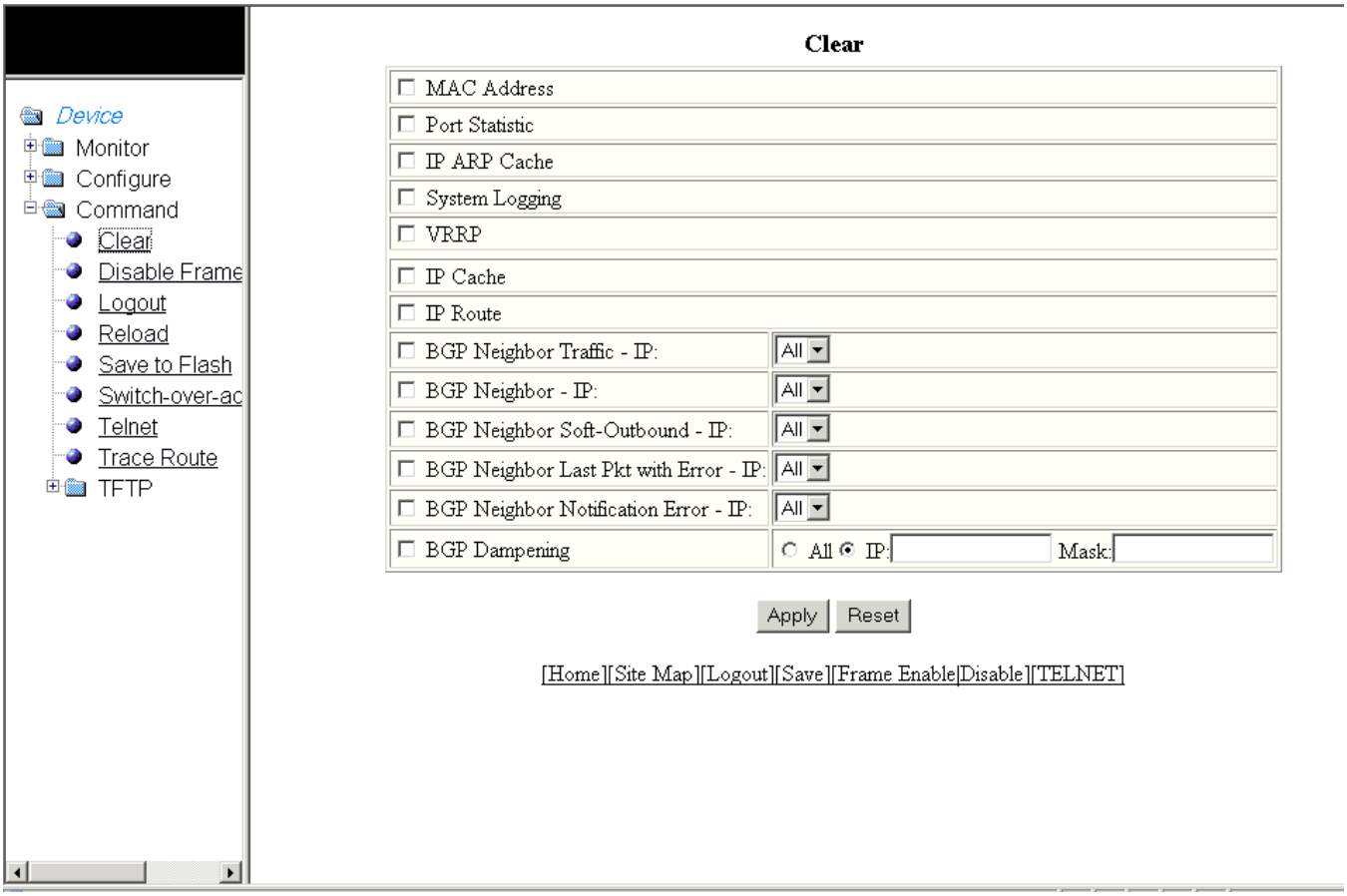
Clearing information for a Layer 3 switch

To clear specific data related to a Layer 3 switch, perform the following steps.

1. Click **Command** on the left pane and select **Clear**.

   The **Clear** window is displayed as shown in the figure below .

FIGURE 125 Clear window



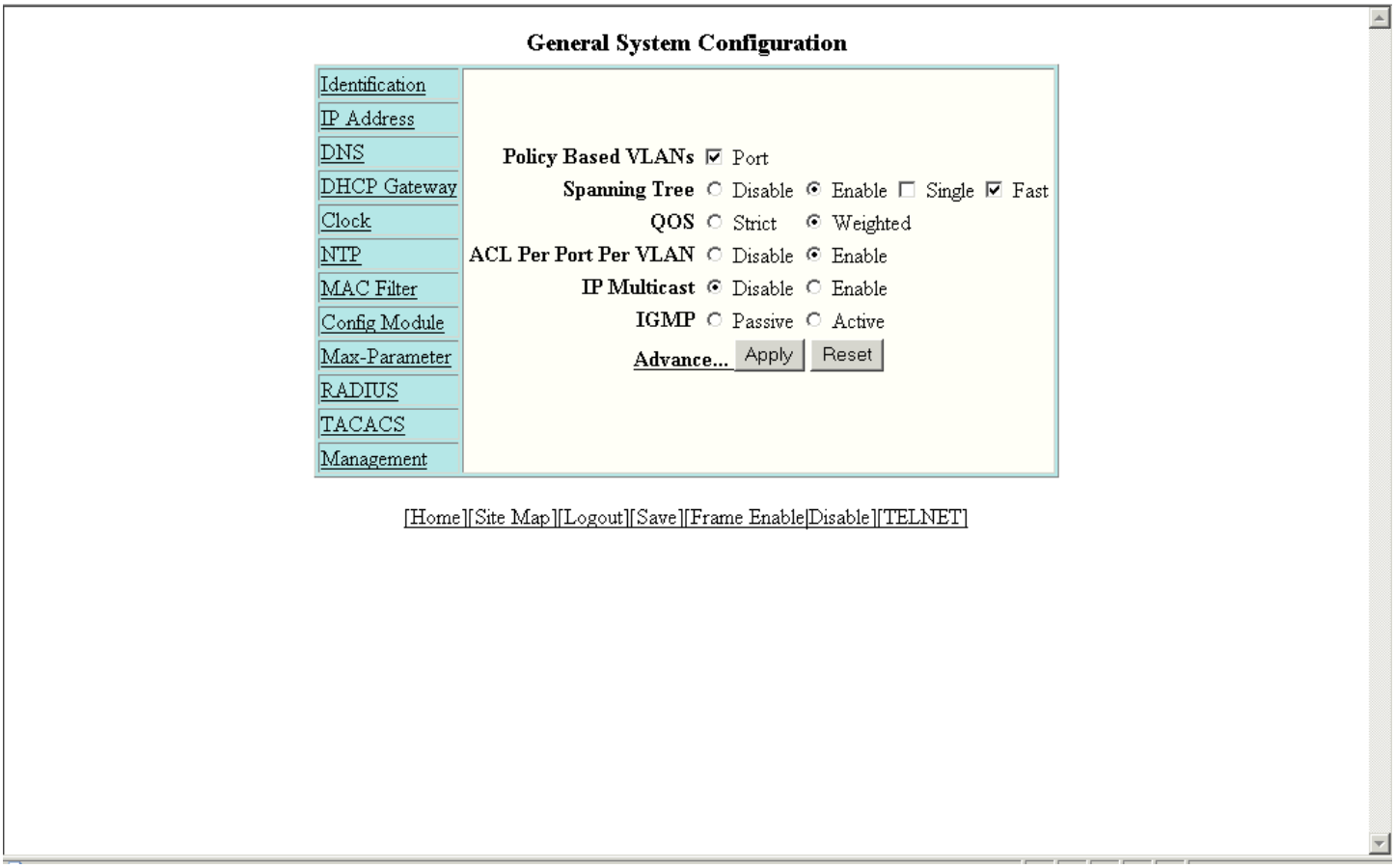
2. Select the following check boxes to clear information:
   - **MAC Address**
   - **Port Statistic**
   - **IP ARP Cache**
   - **System Logging**
   - **VRRP**
   - **IP Cache**
   - **IP Route**
   - **BGP Neighbor Traffic - IP** --Select **All** in the list to clear the BGP message counter for all neighbors.
   - **BGP Neighbor - IP** --Select **All** in the list to close all neighbor sessions and clear all the routes exchanged by the Layer 3 switch and the neighbors.
   - **BGP Neighbor Soft-Outbound - IP** --Select **All** in the list to update all outbound routes by applying the new or changed filters.
   - **BGP Neighbor Last Pkt with Error - IP** --Select **All** in the list to clear the last packet from the neighbors that contained an error.
   - **BGP Neighbor Notification Error - IP** --Select **All** in the list to clear the buffer for all neighbors containing the last NOTIFICATION message sent or received.
   - **BGP Dampening** --Perform one of the following tasks:
     - Click **All** to clear all the route dampening statistics.
     - Click **IP** and type the network IP address in the **IP** field and the network mask in the **Mask** field.
3. Click **Apply**.

   All the current entries will be deleted.

Disabling or enabling the menu view

To enable or disable the menu view, click **Command** on the left pane and select **Disable Frame.** The menu tree from the left panel is hidden as shown in the figure below. Click **Frame Enable** to view the menu tree.

FIGURE 126 Disabling the menu tree



Logging out

To exit the Web Management Interface, click **Command** on the left pane and select **Logout** . The login window is displayed as shown in the figure below. To re-log in, click **Login** on the window.

FIGURE 127 Logging out



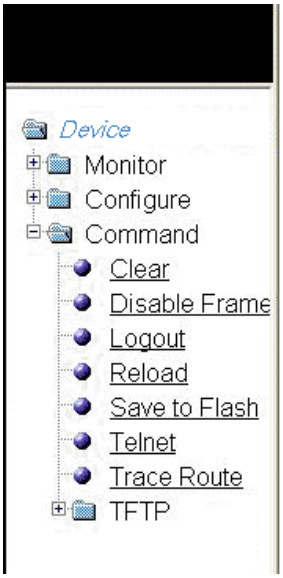
Reloading units in a stack

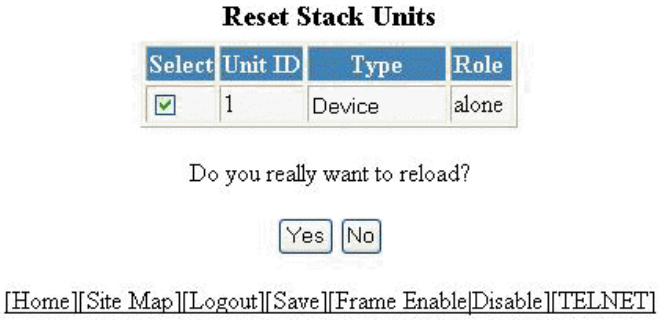
To reload any or all of the units within a device, perform the following steps.

1. Click **Command** on the left pane and select **Reload** .

   The **Reset Stack Units** window is displayed as shown in the figure below.

   FIGURE 128 Reloading the units





2. Click **Yes** to start the process.

NOTE
If the Active Controller is reset or removed from the stack, the entire stack reloads and Active Controller and Standby Controller elections are started. 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 the Active Controller, the existing Standby Controller waits 30 seconds and then assumes the role of the Active Controller.If both the Active Controller and the Standby Controllers are removed, the rest of the stack continues to function. The stack members will not be able to learn any new addresses.

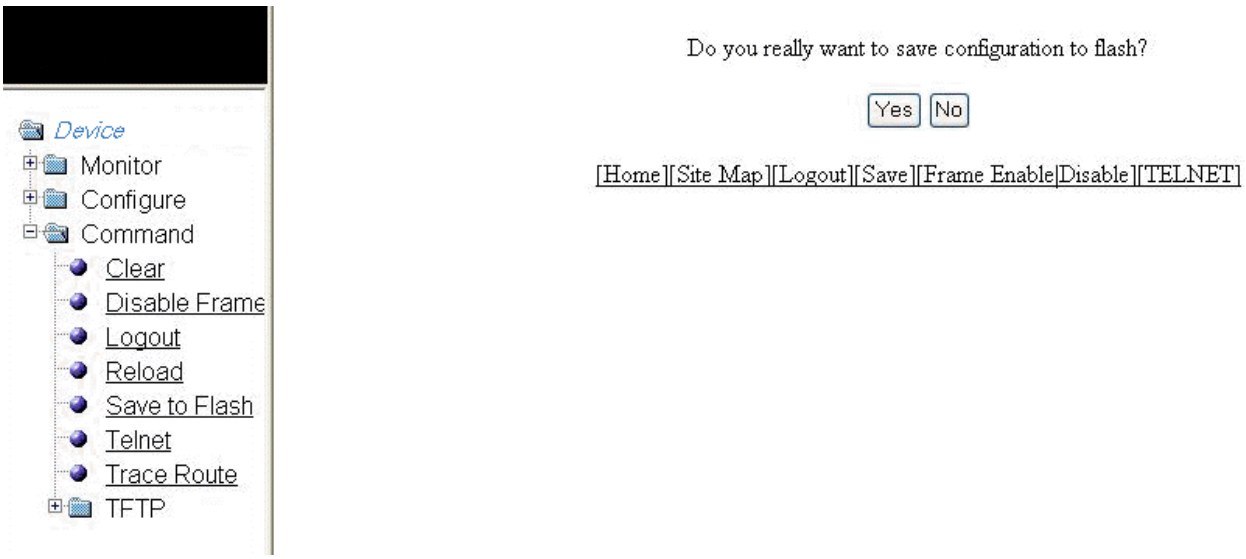
Saving the configuration to flash

To save the configuration changes to flash, perform the following tasks.

1. Click **Command** on the left pane and select **Save To Flash** .

   The save configuration window is displayed as shown in the figure below.

   FIGURE 129 Saving the configuration to flash



2. Click **Yes** to confirm saving the configuration.

   NOTE
   To apply the changes to memory allocation, reload the software after you save the changes to the startup-configuration file.

Switching over to the active role

To switch a standby module to become an Active Controller, perform the following steps.

1. Click **Command** on the left pane and select **Switch-over-active-controller** .

   The switch over window is displayed as shown in the figure below.

   FIGURE 130 Switching over to an Active Controller



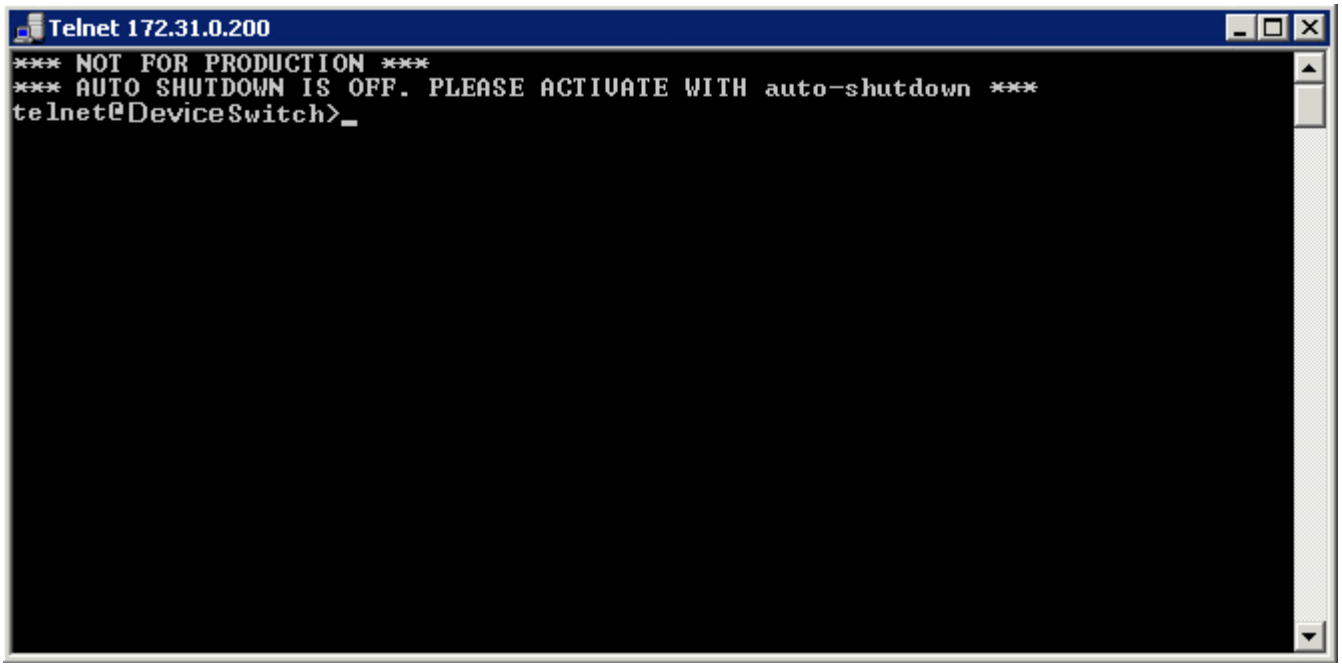
2. Click **Yes** to switch the standby module to become an Active Controller or click **No** to cancel the operation.

Accessing the Telnet command prompt

To open a Telnet CLI window, click **Command** on the left pane and select **Telnet** .

The **Telnet** window is displayed as shown in the figure below.

FIGURE 131 Accessing Telnet



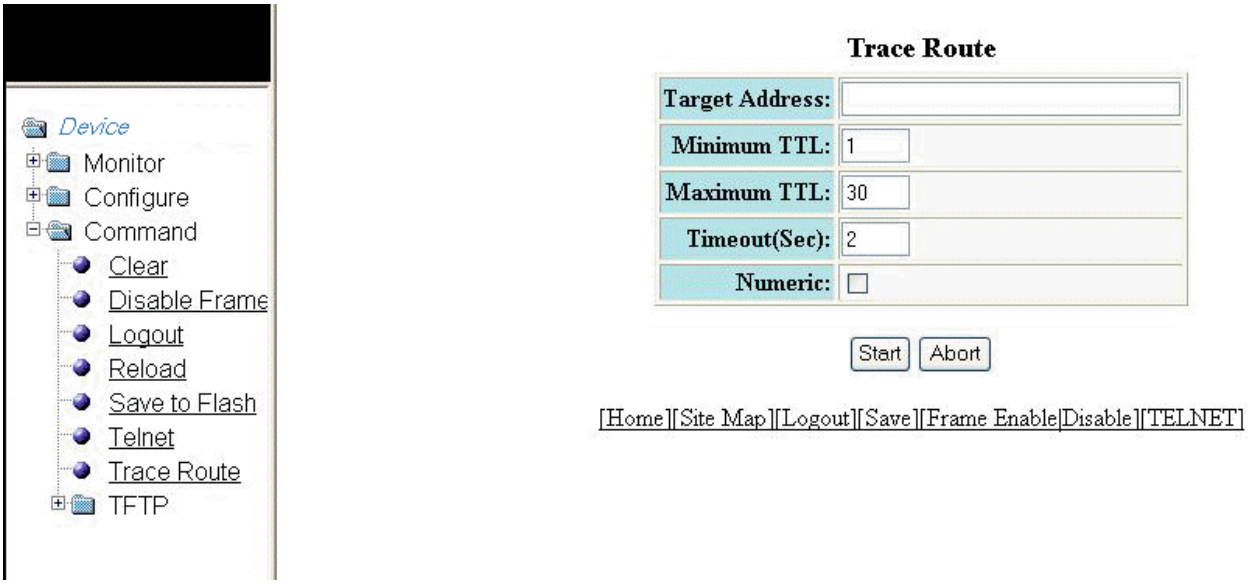
Performing a trace

Trace Route allows you to trace a path from the Ruckus device to an IPv4 host. Trace route requests show all responses to a minimum Time To Live (TTL) of 1 second and a maximum TTL of 30 seconds. In addition, if there are multiple equal-cost routes to the destination, the Ruckus device displays up to three responses. To run a trace, perform the following steps.

1. Click **Command** on the left pane and select **Trace Route** .

   The **Trace Route** window is displayed as shown in the figure below.

   FIGURE 132 Performing a trace



2. Type the IP address of the host at the other end of the route in the **Target Address** field.
3. Type the minimum value of TTL in the **Minimum TTL** field. The default is 1.
4. Type the maximum value of TTL in the **Maximum TTL** field. The default is 30.
5. Type the number of seconds the router waits for a reply from the pinged device in the **Timeout (Sec)** field.
6. Select the **Numeric** check box so that, 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.
7. Click **Start** to begin the trace process or click **Abort** to exit without performing the trace.

Using TFTP

- Configuring TFTP..... 227
- Configuring a TFTP image..... 229

Configuring TFTP

When the device reboots, or the auto-configuration feature has been disabled and then re-enabled, the device uses information from the Dynamic Host Configuration Protocol (DHCP) server to contact the Trivial File Transfer Protocol (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 in the following order:

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

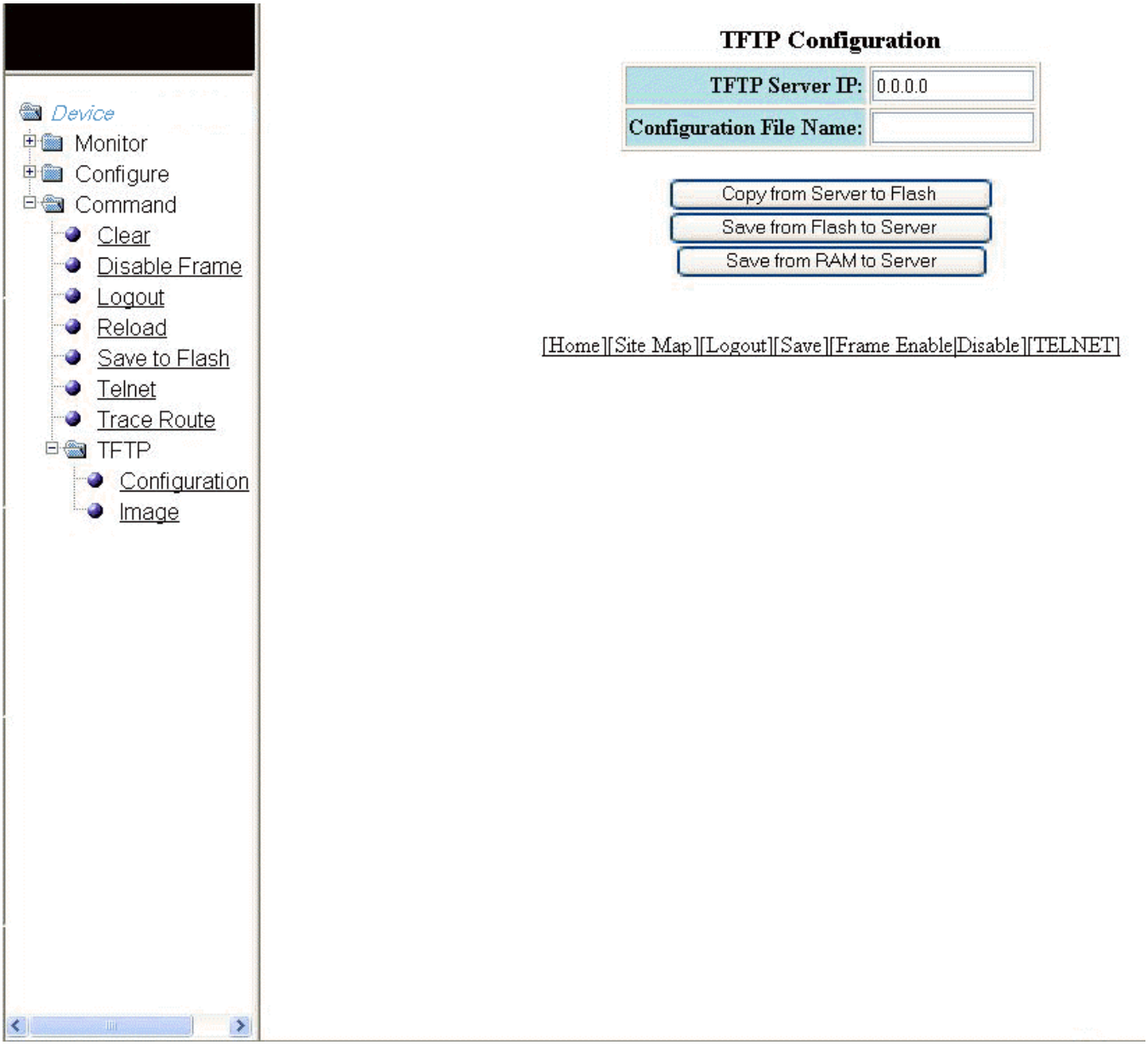
To access the TFTP configuration, perform the following steps.

1. Click **Command** on the left pane and select **TFTP** .

2. Click **Configuration** .

   The **TFTP Configuration** window is displayed as shown in the figure below.

FIGURE 133 Configuring TFTP



3. Type 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) in the **TFTP Server IP** field.
4. Type the name under which the startup-config file of the Layer 2 switch or Layer 3 switch was uploaded or downloaded during the most recent TFTP access in the **Configuration File Name** field.

5. You can perform one of the following tasks with the configuration file:
   - Click **Copy from Server to Flash** to copy the file from a TFTP server to the device flash memory.
   - Click **Save from Flash to Server** to save the file from the device flash memory to a TFTP server.
   - Click **Save from RAM to Server** to save the file from the device RAM memory to a TFTP server.

Configuring a TFTP image

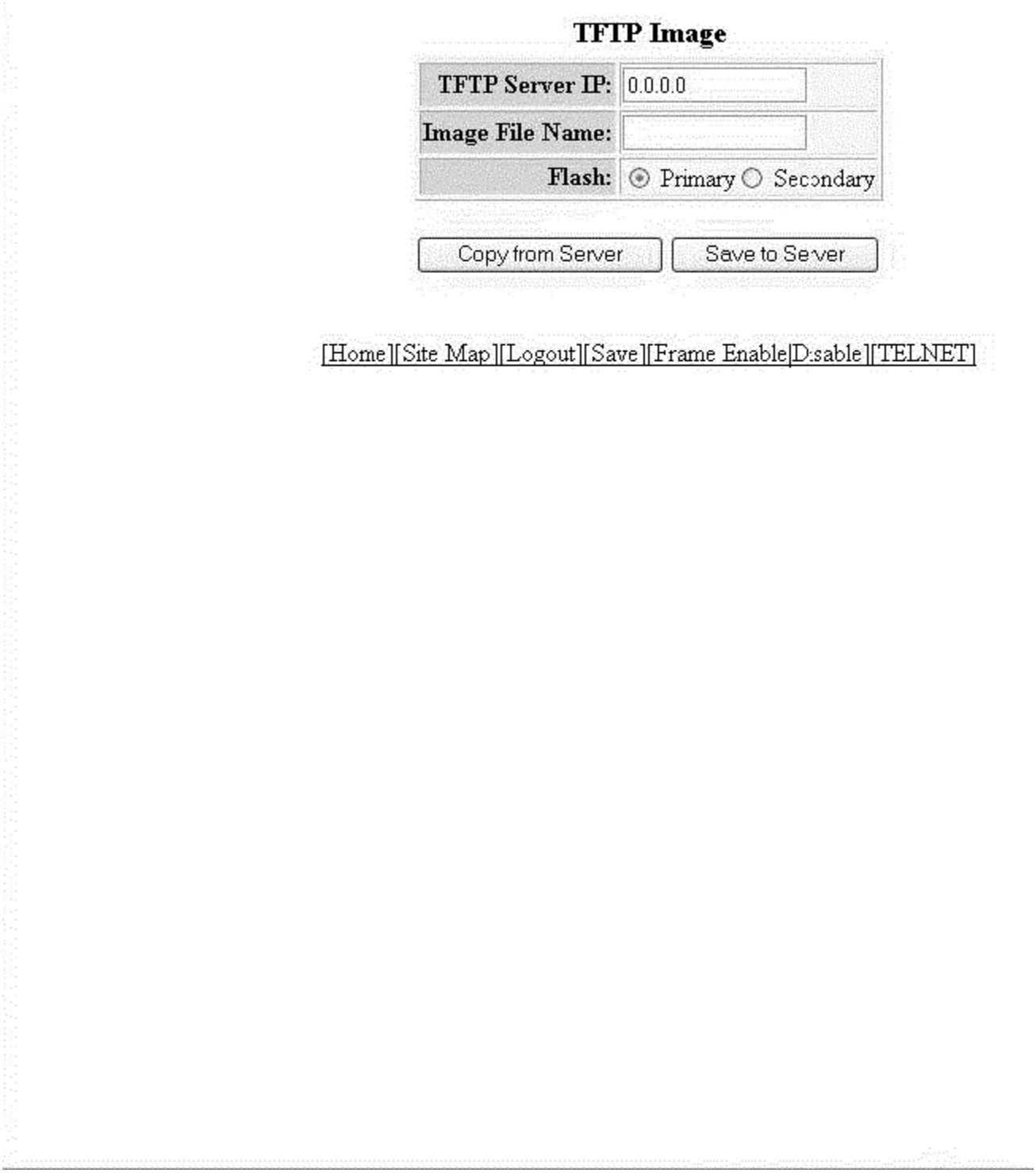
To access a TFTP image, perform the following steps.

1. Click **Command** on the left pane and select **TFTP** .

2. Click **Image** .

   The **TFTP Image** window is displayed as shown in the figure below.

   FIGURE 134 Configuring a TFTP image



3. Type 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) in the **TFTP Server IP** field.
4. Type the name of the Layer 2 switch or Layer 3 switch flash image (system software file) that was uploaded or downloaded during the most recent TFTP access in the **Image File Name** field.
5. Click one of the following for **Flash** :
   - *Primary* --The default local storage device for image files and configuration files.
   - *Secondary* --The 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.
6. You can perform one of the following tasks with the TFTP image:
   - Click **Copy from Server** to copy a boot image from a TFTP server to the primary or secondary storage location in the device flash memory.
   - Click **Save to Server** to save the boot image from the primary or secondary storage location of the device flash memory to a TFTP server.



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com