

Intel® Gigabit Ethernet Switch AXXSW1GB User Guide

A Guide for System Administrators of Intel® Server Products

Intel Order Number D95362-005

Disclaimer

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other names and brands may be claimed as the property of others.

Copyright © 2007-2008, Intel Corporation. All Rights Reserved.

Safety Information

Important Safety Instructions

Read all caution and safety statements in this document before performing any of the instructions. See also *Intel® Server Boards and Server Chassis Safety Information* at: <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>

Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warnung und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die *el Server Boards and Server Chassis Safety Information* unter: <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>.

Consignes de sécurité

Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction. Consultez *Intel Server Boards and Server Chassis Safety Information* sur le site: <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>

Instrucciones de seguridad importantes

Lea todas las declaraciones de seguridad y precaución de este documento antes de realizar cualquiera de las instrucciones. Vea *Intel Server Boards and Server Chassis Safety Information* en: <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>

重要安全指导

在执行任何指令之前，请阅读本文件中的所有注意事项及安全声明。并参阅 <http://support.intel.com/support/motherboards/server/sb/CS-010770.htm> 上的 *Intel Server Boards and Server Chassis Safety Information*（《Intel 服务器主板与服务器机箱安全信息》）。

Warnings

These warnings and cautions apply whenever you remove the server compute module enclosure cover to access components inside the system. Only a technically qualified person should maintain or configure the system.

Heed safety instructions: Before working with your server product, whether you are using this guide or any other resource as a reference, pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in the region(s) in which the product is sold.

System power on/off: The power button DOES NOT turn off the system AC power. To remove power from the system, you must unplug the AC power cord from the wall outlet or the chassis. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and disconnect the power cord, telecommunications systems, networks, and modems attached to the system before opening it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures in this document only at an ESD workstation. If one is not available, provide some ESD protection by wearing an anti-static wrist strap attached to chassis ground (any unpainted metal surface) on your system when handling parts.

ESD and handling electronic devices: Always handle electronic devices carefully. They can be extremely sensitive to ESD. Do not touch the connector contacts.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle nosed pliers. If your jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool you use to remove a jumper, or you may bend or break the pins on the board.

Reinstalling enclosure cover: To protect internal components and for proper cooling and airflow, the server compute module should not be inserted into the chassis with the cover removed; operating it without the enclosure cover in place can damage system parts.

Preface

The *Embedded Web System* (EWS) is a network management system. The Embedded Web Interface configures, monitors, and troubleshoots network devices from a remote web browser. The Embedded Web Interface web pages are easy-to-use and easy-to-navigate. In addition, The Embedded Web Interface provides real time graphs and RMON statistics to help system administrators monitor network performance.

This preface provides an overview to the Embedded Interface User Guide, and includes the following sections:

- User Guide Overview
- Intended Audience

User Guide Overview

This section provides an overview to the Web System Interface User Guide. The Web System Interface User Guide provides the following sections:

- **Section 1, Getting Started** — Provides information about using the EWS, including The Embedded Web Interface interface, management, and information buttons, as well as information about adding, modifying, and deleting device information.
- **Section 2, Managing Device Information** — Provides information about opening the device zoom view, defining general system information, and enabling Jumbo frames.
- **Section 3, Configuring Device Security** — Provides information about configuring device security for management security, traffic control, and network security.
- **Section 4, Configuring Ports** — Provides information about configuring ports.
- **Section 5, Aggregating Ports** — Provides information about configuring Link Aggregated Groups and LACP.
- **Section 6, Configuring VLANs** — Provides information about configuring and managing VLANs, including information about GARP and GVRP, and defining VLAN groups.
- **Section 7, Defining Forwarding Database** — Provides information about defining Static Forwarding Database Entries and Dynamic Forward Database Entries.
- **Section 8, Configuring Multicast Forwarding** — Provides information about Multicast Forwarding.
- **Section 9, Configuring Spanning Tree** — Provides information about configuring Spanning Tree Protocol and the Rapid Spanning Tree Protocol.
- **Section 10, Configuring Quality of Service** — Provides information about configuring Quality of Service on the device.

- **Section 11, Managing System Logs** — Provides information about enabling and defining system logs.
- **Section 12, Managing Device Diagnostics** — Provides information on Configuring Port Mirroring, Ethernet Ports, and Viewing Optical Transceivers.
- **Section 13, Viewing Statistics** — Provides information about viewing device statistics, including RMON statistics, device history events, and port and LAG utilization statistics.

Intended Audience

This guide is intended for network administrators familiar with IT concepts and terminology.

Table of Contents

Safety Information	iii
Important Safety Instructions	iii
Wichtige Sicherheitshinweise	iii
Consignes de sécurité	iii
Instrucciones de seguridad importantes	iii
Preface	v
User Guide Overview	v
Intended Audience	vi
Chapter 1: Getting Started	1
Starting the Embedded Web Interface	2
Understanding the Embedded Web Interface	3
Using Screen and Table Options	6
Resetting the Device	8
Logging Off the Device	8
Chapter 2: Managing Device Information	9
Viewing System Information	9
Chapter 3: Configuring Device Security	11
Configuring Traffic Control	11
Defining Access Control Lists	17
Chapter 4: Configuring Ports	31
Chapter 5: Aggregating Ports	35
Configuring LAGs	36
Defining LAG Members	40
Configuring LACP	42
Configuring Virtual Trunk Group Failover	44
Chapter 6: Configuring VLANs	47
Defining VLAN Properties	48
Defining VLAN Membership	50
Defining VLAN Interface Settings	53
Defining VLAN Groups	56
Configuring GARP	66
Chapter 7: Defining Forwarding Database	71
Defining Static Forwarding Database Entries	72
Defining Dynamic Forwarding Database Entries	74

Chapter 8: Configuring Multicast Forwarding	77
Defining IGMP Snooping	78
Defining Multicast Groups	80
Defining Multicast Forward All Settings	83
Chapter 9: Configuring Spanning Tree	85
Defining Spanning Tree	86
Defining Spanning Tree Interface Settings	89
Defining Rapid STP	93
Defining Multiple STP	96
Defining Multiple STP Instance To VLAN Settings	97
Chapter 10: Configuring Quality of Service	103
Quality of Service Overview	104
Defining General QoS Settings	105
Configuring Basic QoS Settings	114
Configuring Advanced QoS Settings	117
Chapter 11: Managing System Logs	129
Enabling System Logs	130
Viewing the FLASH Logs	132
Viewing the Device Memory Logs	133
Chapter 12: Managing Device Diagnostics	135
Configuring Port Mirroring	136
Ethernet Ports Diagnostics	138
Copper Cable Extended Feature	139
Viewing the CPU Utilization	141
Chapter 13: Viewing Statistics	143
Viewing Statistics	143
Viewing Interface Statistics	143
Managing RMON Statistics	150
A Troubleshooting	166
B Installation/Assembly Safety Instructions	168
English	168
Deutsch	170
Français	173
Español	175
Italiano	177
C Safety Information	180
English	180
Français	191

List of Tables

Table 1. Additional Information and Software	8
Table 2. Product Certification Markings	42

List of Figures

Figure 1. Embedded Web Interface Home Page	2
Figure 2. Embedded Web Interface Components	3
Figure 3. Device Representation.....	4
Figure 4. Add MAC Based ACL.....	6
Figure 5. Storm Control Settings Page.....	7
Figure 6. Reset Page	8
Figure 7. System Information Page.....	9
Figure 8. Reset Page	10
Figure 9. Storm Control Page.....	12
Figure 10. Storm Control Settings Page.....	13
Figure 11. Port Security Page	14
Figure 12. Edit Port Security Settings Page	16
Figure 13. MAC Based ACL Page.....	18
Figure 14. Add MAC Based ACL and First Rule Page.....	20
Figure 15. Add ACL Rule Page	20
Figure 16. Edit Rule Page	21
Figure 17. IP Based ACL Page	22
Figure 18. Add IP Based ACL and First Rule Page	25
Figure 19. Add IP Based Rule Page	26
Figure 20. Edit Rule Page	27
Figure 21. ACL Binding Page.....	28
Figure 22. Edit ACL Binding Page.....	29
Figure 23. Port Configuration Page.....	31
Figure 24. Port Configuration Settings Page.....	33
Figure 25. LAG Configuration Page	36
Figure 26. LAG Configuration Settings Page	37
Figure 27. LAG Membership Page.....	40
Figure 28. LAG Membership Settings Page.....	41
Figure 29. LACP Parameters Page.....	42
Figure 30. LACP Parameters Settings Page.....	43
Figure 31. Trunk Group Fail Over Page	45
Figure 32. Edit Fail Over Group Page	46
Figure 33. VLAN Properties Page	48
Figure 34. Add VLAN Page	49
Figure 35. VLAN Settings Page	49
Figure 36. VLAN Membership Page.....	50
Figure 37. Edit VLAN Membership Page	52
Figure 38. Interface Settings Page.....	53
Figure 39. VLAN Interface Settings Page	55
Figure 40. VLAN MAC-based Groups Page.....	57
Figure 41. Add VLAN MAC-based Groups Page	58
Figure 42. MAC Groups Settings Page	58

Figure 43. VLAN Subnet-based Groups Page.....	59
Figure 44. Add VLAN Subnet-based Groups Page	60
Figure 45. Subnet-based Group Settings	60
Figure 46. VLAN Protocol Groups Page	61
Figure 47. Add Protocol-based Groups Page	62
Figure 48. Protocol-based Groups Settings Page	63
Figure 49. Mapping Groups to VLAN Page	64
Figure 50. Mapping Groups to VLAN Settings Page	65
Figure 51. GARP Settings Page	66
Figure 52. GARP Parameters Settings Page.....	67
Figure 53. GVRP Parameters Page.....	68
Figure 54. GVRP Parameters Settings Page.....	69
Figure 55. Static Addresses Page	72
Figure 56. Add Static MAC Address Page.....	73
Figure 57. Dynamic Addresses Page	74
Figure 58. IGMP Snooping Page	78
Figure 59. IGMP Snooping Settings Page	79
Figure 60. Multicast Group Page	80
Figure 61. Add Multicast Group Page.....	81
Figure 62. Edit Multicast Group Page	82
Figure 63. Multicast Forward All Page	83
Figure 64. Edit Multicast Forward All Page.....	84
Figure 65. Spanning Tree Properties Page	86
Figure 66. Spanning Tree Interface Settings Page.....	89
Figure 67. Spanning Tree Interface Settings Page.....	92
Figure 68. Rapid STP Page	93
Figure 69. Rapid Spanning Tree Settings Page	95
Figure 70. Multiple STP Properties Page	96
Figure 71. Instance To VLAN Settings Page	97
Figure 72. Instance Settings Page.....	98
Figure 73. Interface Settings Page	100
Figure 74. Interface Table Page	102
Figure 75. CoS Global Settings Page	106
Figure 76. Modify Port Priority Page	107
Figure 77. Queue Page.....	108
Figure 78. Bandwidth Settings Page.....	110
Figure 79. Modify Bandwidth Settings Page	111
Figure 80. CoS to Queue Page.....	112
Figure 81. DSCP to Queue Page.....	113
Figure 82. Basic Mode General Settings Page.....	114
Figure 83. QoS DSCP Rewrite Page	116
Figure 84. Policed DSCP Page.....	118
Figure 85. Class Map Page	119
Figure 86. Add QoS Class Map Page.....	120
Figure 87. Aggregated Policier Page	121
Figure 88. Add Aggregated Policier Page.....	122
Figure 89. Edit QoS Aggregate Policier Page	122

Figure 90. Policy Table Page	124
Figure 91. Add QoS Policy Profile Page	125
Figure 92. Edit QoS Policy Profile Page.....	126
Figure 93. Policy Binding Page	127
Figure 94. Add Qos Policy Binding Page	128
Figure 95. Qos Policy Binding Settings Page.....	128
Figure 96. System Logs Properties Page.....	130
Figure 97. System Flash Logs Page	132
Figure 98. Device Memory Log Page.....	133
Figure 99. Port Mirroring Page	136
Figure 100. Ethernet Ports Page.....	138
Figure 101. Cable Extended Feature Page.....	139
Figure 102. CPU Utilization Page.....	141
Figure 103. Interface Statistics Page	144
Figure 104. Etherlike Statistics Page	146
Figure 105. GVRP Statistics Page	148
Figure 106. RMON Statistics Page	150
Figure 107. RMON History Control Page.....	154
Figure 108. Add History Entry Settings Page.....	155
Figure 109. RMON History Control Settings Page.....	156
Figure 110. RMON History Table Page.....	157
Figure 111. RMON Events Control Page	159
Figure 112. RMON Events Logs Page	161
Figure 113. RMON Alarm Page	162
Figure 114. Add Alarm Entry Page.....	163
Figure 115. RMON Alarms Definition Page.....	164

1 Getting Started

This section provides an introduction to the user interface, and includes the following topics:

- Starting the Embedded Web Interface
- Understanding the Embedded Web Interface
- Using Screen and Table Options
- Resetting the Device
- Logging Off the Device

Starting the Embedded Web Interface

Note: Disable the popup blocker in your internet browser before beginning device configuration using the EWS.

This section contains information on starting the *Embedded Web Interface*.

To access the user interface:

1. Open an internet browser.
2. Ensure that pop-up blockers are disabled. If pop-up blockers are enabled, the edit, add, and device information messages may not open.
3. Enter the device IP address in the address bar and press Enter.

Figure 1. Embedded Web Interface Home Page

The screenshot displays the Embedded Web Interface (EWS) for a Gigabit Ethernet Switch. The interface has a blue header bar with the title "Gigabit Ethernet Switch" on the left and the user information "User: user15" and a "Sign Out" link on the right. Below the header, there is a central area showing a rack of network switches. On the left side, there is a navigation menu with a tree view containing the following items: System, System Information (selected), Reset, Logs, Diagnostics, Network Security, Layer 2, QoS, and Statistics/RMON. The main content area is titled "System Information" and contains a form with the following fields and values:

Field	Value
Model Name	Gigabit Ethernet Switch
System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.6486.800.1.1.2.2.4.1.3
System Up Time	0 days, 0 hours, 0 minutes, 48 seconds
Base MAC Address	00:00:b0:00:00:00
IP Address	10.1.1.100
Mask	255.255.255.0
Hardware Version	1.0.0
Software Version	1.0.0.0
Boot Version	1.0.0.0
Jumbo Frame	☒ Enable ☐ Disable

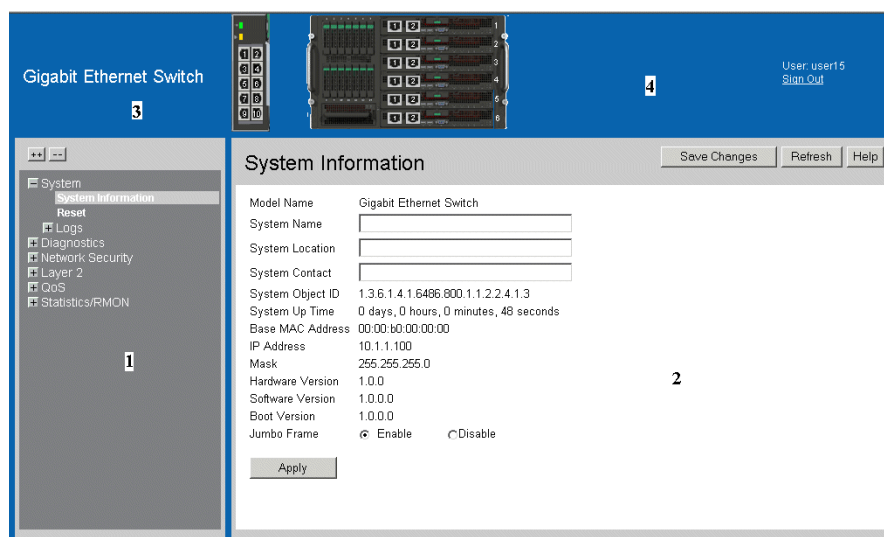
At the bottom of the form, there is an "Apply" button. In the top right corner of the main content area, there are three buttons: "Save Changes", "Refresh", and "Help".

Understanding the Embedded Web Interface

The *Embedded Web Interface Home Page* contains the following views:

- **Port LED Indicators** — Located at the top of the home page, the port LED indicators provide a visual representation of the ports on the front panel.
- **Tab Area** — Located under the LED indicators, the tab area contains a list of the device features and their components.
- **Device View** — Located in the main part of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.

Figure 2. Embedded Web Interface Components



The following table lists the user interface components with their corresponding numbers:

Table 1. Interface Components

View	Description
1 Tree View	Tree View provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
2 Device Information View	Device View provides information about device ports, current configuration and status, table information, and feature components. Device View also displays other device information and dialog boxes for configuring parameters.
3 Zoom View	Provides a graphic of the device on which the Web Interface runs.
4 Web Interface Information Links	Provides user information, and allows users to save the current device configuration, and sign out of the Web Interface.

This section provides the following additional information:

- **Device Representation** — Provides an explanation of the user interface buttons, including both management buttons and task icons.
- **Using the Embedded Web Interface Management Buttons** — Provides instructions for adding, modifying, and deleting configuration parameters.

Device Representation

The *Embedded Web Interface Home Page* contains a graphical panel representation of the device. An explanation of the port settings displays when you move your mouse over the port.

Figure 3. Device Representation

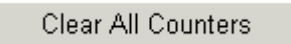
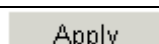
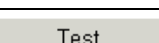
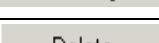


Using the Embedded Web Interface Management Buttons

Configuration Management buttons and icons provide an easy method of configuring device information, and include the following:

Table 2.

Table 1: Web Interface Configuration Buttons

Button	Button Name	Description
	Clear Logs	Clears system logs.
	Clear All Counters	Clears statistics.
	Create	Enables creation of configuration entries.
	Edit	Modifies configuration settings.
	Apply	Applies configuration changes to the device.
	Test	Performs cable tests.
	Advanced	Performs advanced tests.
	Query	Queries the device table.
	Delete	Deletes a configuration entries.
	Reset	Resets configuration to before changes were entered by user.
	Next	Allows viewing the next page in a table.
	Back	Allows to viewing the previous page in a table.
	Help	Opens the online help.

Using Screen and Table Options

This option contains screens and tables for configuring devices. This section contains the following topics:

- Adding Configuration Information
- Modifying Configuration Information
- Deleting Configuration Information

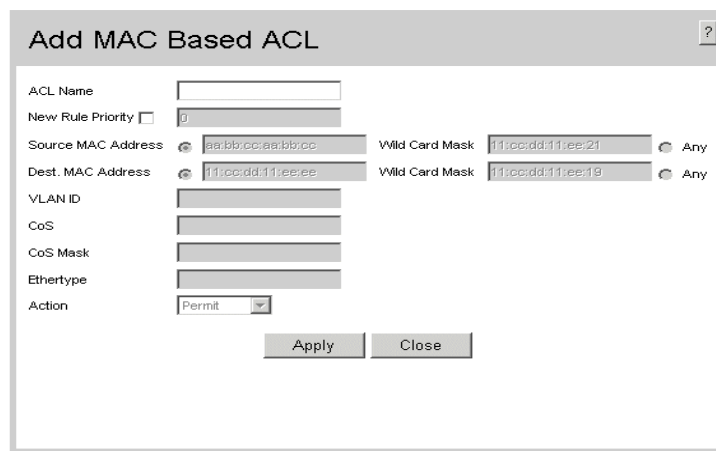
Adding Configuration Information

User-defined information can be added to specific Web Interface pages, by opening a new Add page.

To add information to tables or Web Interface pages:

1. Open an Embedded Web Interface page.
2. Click **Add** . An add page opens, such as the *Add MAC Based ACL*:

Figure 4. Add MAC Based ACL



The screenshot shows a web interface window titled "Add MAC Based ACL" with a help icon (?) in the top right corner. The window contains the following fields and controls:

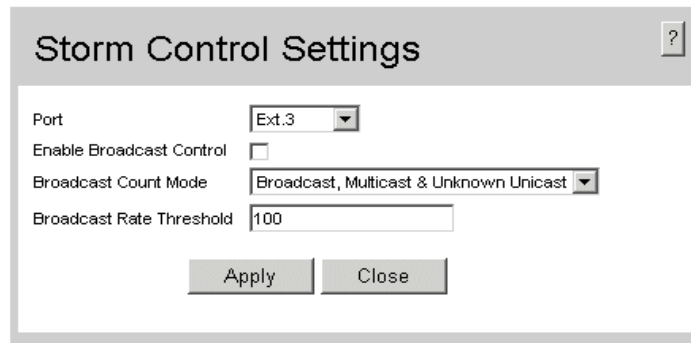
- ACL Name**: A text input field.
- New Rule Priority**: A checkbox followed by a text input field containing the value "9".
- Source MAC Address**: A text input field containing "aa:bb:cc:aa:bb:cc" with a circular icon to its left.
- Wild Card Mask**: A text input field containing "11:cc:dd:11:ee:21" with a circular icon to its left.
- Any**: A radio button.
- Dest. MAC Address**: A text input field containing "11:cc:dd:11:ee:ee" with a circular icon to its left.
- Wild Card Mask**: A text input field containing "11:cc:dd:11:ee:19" with a circular icon to its left.
- Any**: A radio button.
- VLAN ID**: A text input field.
- CoS**: A text input field.
- CoS Mask**: A text input field.
- Ethertype**: A text input field.
- Action**: A dropdown menu currently showing "Permit".
- Buttons**: "Apply" and "Close" buttons at the bottom right.

3. Define the relevant fields.
4. Click **Apply** . The configuration information is saved, and the device is updated.

Modifying Configuration Information

1. Open an Embedded Web Interface page.
2. Select a table entry.
3. Click **Edit**. A modification page, such as the *Storm Control Settings Page* opens:

Figure 5. Storm Control Settings Page



4. Modify the relevant fields.
5. Click **Apply**. The fields are modified, and the information is saved to the device.

Deleting Configuration Information

1. Open The Embedded Web Interface page.
2. Select a table row.
3. Select the *Delete* checkbox.
4. Click **Delete**. The information is deleted, and the device is updated.

Resetting the Device

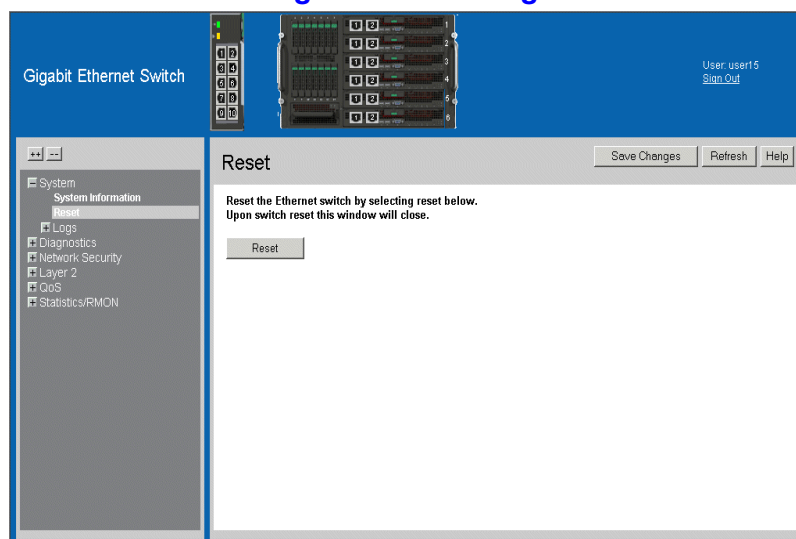
The *Reset Page* enables resetting the device from a remote location.

Note: To prevent the current configuration from being lost, save all changes from the running configuration file to the startup configuration file before resetting the device.

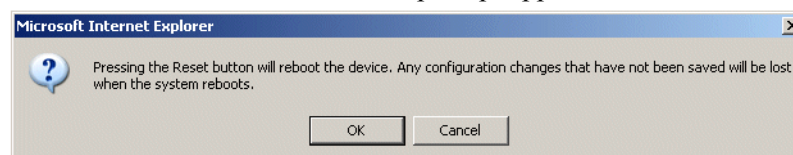
To reset the device:

1. Click **System > Reset**. The *Reset Page* opens.

Figure 6. Reset Page



2. Click **Reset**.
3. The device reboots and a confirmation prompt appears.



4. Click OK. The device is reset, and a prompt for a user name and password is displayed.
5. Enter a user name and password to reconnect to the Web Interface.

Logging Off the Device

1. Click **Sign Out**. The *Embedded Web Interface Home Page* closes.

2 Managing Device Information

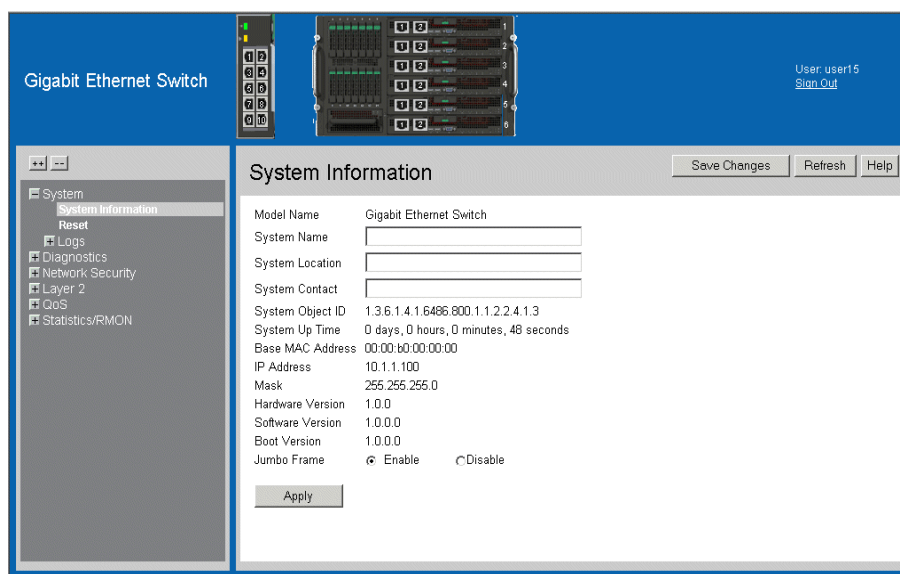
Viewing System Information

The *System Information Page* contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System Up Time, System IP and MAC addresses, and both software and hardware versions.

To view system information:

1. Click **System > System Information**. The *System Information Page* opens:

Figure 7. System Information Page



The screenshot displays the 'System Information' page for a 'Gigabit Ethernet Switch'. The page has a blue header with the device name and a user profile 'User: user15' with a 'Sign Out' link. A left sidebar contains a navigation menu with options like 'System', 'Reset', 'Logs', 'Diagnostics', 'Network Security', 'Layer 2', 'QoS', and 'Statistics/RMON'. The main content area is titled 'System Information' and includes a 'Save Changes' button, a 'Refresh' button, and a 'Help' button. The form contains the following fields and values:

Field	Value
Model Name	Gigabit Ethernet Switch
System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.6486.800.1.1.2.2.4.1.3
System Up Time	0 days, 0 hours, 0 minutes, 48 seconds
Base MAC Address	00:00:b0:00:00:00
IP Address	10.1.1.100
Mask	255.255.255.0
Hardware Version	1.0.0
Software Version	1.0.0.0
Boot Version	1.0.0.0
Jumbo Frame	☒ Enable ☐ Disable

An 'Apply' button is located at the bottom of the form.

The *System Information Page* contains the following fields:

- **Model Name** — Displays the device model number and name.
- **System Name** — Defines the user-defined device name. The field range is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.
- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.

- **System Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes, and 15 seconds.
- **Base MAC Address** — Displays the device MAC address.
- **IP Address** — Displays the IP Address assigned to the switch
- **Mask** — Displays the Mask Address assigned to the switch
- **Hardware Version** — Displays the installed device hardware version number.
- **Software Version** — Displays the installed software version number.
- **Boot Version** — Displays the current boot version running on the device.
- **Jumbo Frames** — Indicates if Jumbo Frames are enabled on the device. The possible field values are:
 - *Enable* — Enables Jumbo Frames on the device.
 - *Disable* — Disables Jumbo Frames on the device

Resetting the Device

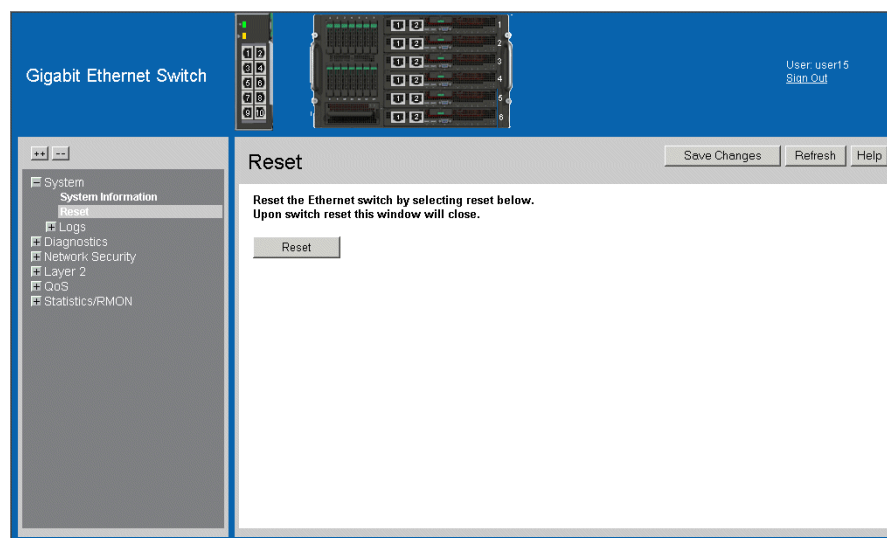
The *Reset Page* enables resetting the device from a remote location.

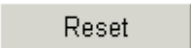
To prevent the current configuration from being lost, save all changes from the running configuration file to the backup configuration file before resetting the device.

To reset the device:

1. Click **System > Reset**. The *Reset Page* opens:

Figure 8. Reset Page



2. Click . The Ethernet switch is reset, and the device is updated.

3 Configuring Device Security

This section provides access to security pages that contain fields for setting security parameters for ports and device management methods. This section contains the following topics:

- Configuring Traffic Control
- Defining Access Control Lists

Configuring Traffic Control

This section contains information for managing both port security and storm control, and includes the following topics:

- Enabling Storm Control
- Managing Port Security

Enabling Storm Control

Storm control limits the amount of Broadcast, Multicast and Unknown Unicast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, Multicast and Unknown Unicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

A Packet Storm is a result of an excessive amount of either Broadcast or Multicast or Unknown Unicast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

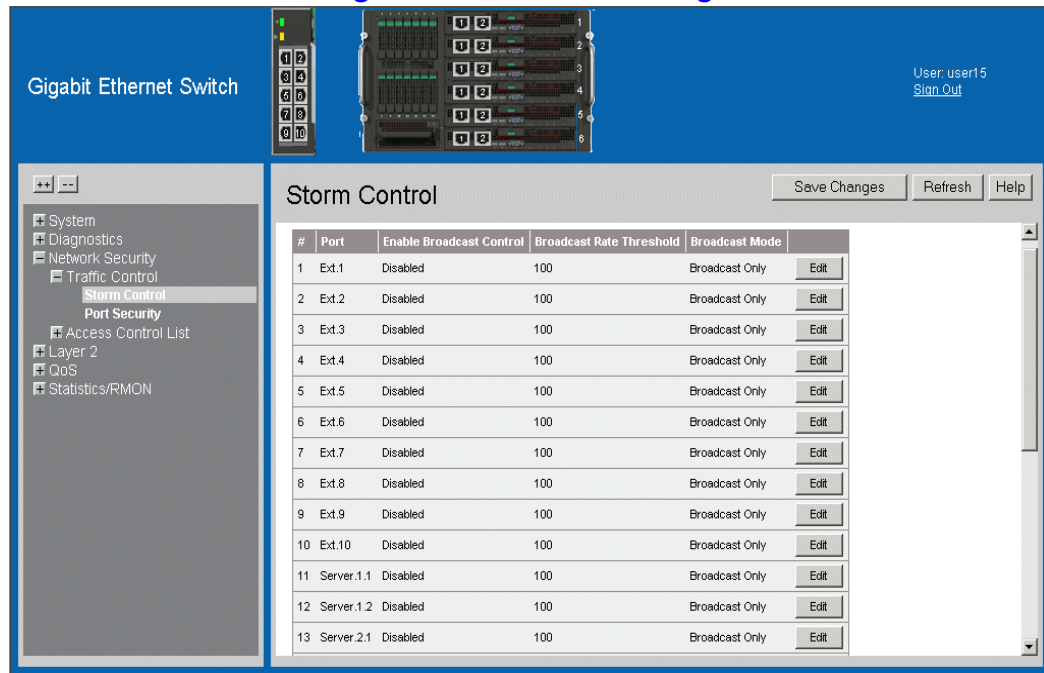
Storm control is enabled for all ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast, Multicast or Unknown Unicast frame rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

The *Storm Control Page* provides fields for configuring packet storm control.

To enable storm control:

1. Click **Network Security > Traffic Control > Storm Control**. The *Storm Control Page* opens.

Figure 9. Storm Control Page

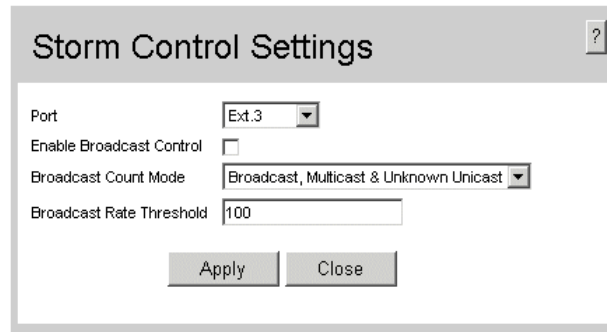


The *Storm Control Page* contains the following fields:

- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — Indicates if forwarding Broadcast packet types is enabled/disabled on the interface. The possible field values are:
 - *Enable* — Enables storm control on the selected port.
 - *Disable* — Disables storm control on the selected port.
- **Broadcast Rate Threshold** — Indicates the maximum rate (kilobits per second) at which packets are forwarded. The range is 3,500 - 1,000,000. The default value is 3,500.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the port. The possible field values are:
 - *Broadcast, Multicast, & Unknown Unicast* — Counts Broadcast, Multicast, and Unicast traffic.
 - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
 - *Broadcast Only* — Counts only Broadcast traffic.

2. Click **Edit** . The *Storm Control Settings Page* opens:

Figure 10. Storm Control Settings Page



The image shows a 'Storm Control Settings' dialog box. It has a title bar with a question mark icon. Inside, there are four settings: 'Port' is a dropdown menu showing 'Ext.3'; 'Enable Broadcast Control' is an unchecked checkbox; 'Broadcast Count Mode' is a dropdown menu showing 'Broadcast, Multicast & Unknown Unicast'; and 'Broadcast Rate Threshold' is a text input field showing '100'. At the bottom, there are two buttons: 'Apply' and 'Close'.

Port	Ext.3
Enable Broadcast Control	☐
Broadcast Count Mode	Broadcast, Multicast & Unknown Unicast
Broadcast Rate Threshold	100

Apply Close

3. Modify the relevant fields.
4. Click **Apply** . Storm control is enabled on the device.

Managing Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- Shuts down the port

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports are activated from the *Port Security Page*.

To define port security:

1. Click **Network Security > Traffic Control > Port Security**. The *Port Security Page* opens.

Figure 11. Port Security Page

The screenshot displays the 'Port Security' configuration page for a Gigabit Ethernet Switch. The page has a blue header with the switch name 'Gigabit Ethernet Switch' and a user status 'User: user15 Sign Out'. A left sidebar contains a navigation menu with options like System, Diagnostics, Network Security, Traffic Control, Storm Control, Port Security (selected), Access Control List, Layer 2, QoS, and Statistics/RMON. The main content area is titled 'Port Security' and includes 'Save Changes', 'Refresh', and 'Help' buttons. Below the title, there are tabs for 'Ports' and 'LAGs'. A table lists 11 ports (Ext.1 to Ext.10 and Server.1.1) with their respective configurations. All ports are 'Unlocked' and use 'Classic Lock' learning mode with 1 max entry. The action is 'Discard' and the trap is 'Disable' with a 10-second frequency. Each row has an 'Edit' button.

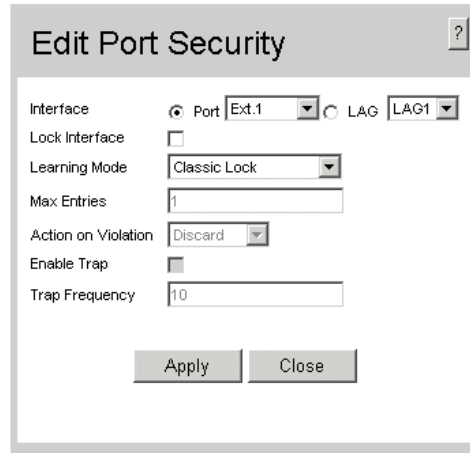
#	Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency (Sec)	
1	Ext.1	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
2	Ext.2	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
3	Ext.3	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
4	Ext.4	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
5	Ext.5	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
6	Ext.6	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
7	Ext.7	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
8	Ext.8	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
9	Ext.9	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
10	Ext.10	Unlocked	Classic Lock	1	Discard	Disable	10	Edit
11	Server.1.1	Unlocked	Classic Lock	1	Discard	Disable	10	Edit

The *Port Security Page* contains the following fields:

- **Ports** — Indicates the port membership.
- **LAGs** — Indicates the LAG membership.
- **Interface** — Displays the port or LAG name.
- **Interface Status** — Indicates the host status. The possible field values are:
 - *Unlocked* — Indicates that the port is unlocked. This is the default value.
 - *Locked* — Indicates that the port is locked.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. The possible field values are:
 - *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
 - *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port (See the Max Entries field). Both relearning and aging MAC addresses are enabled.
- **Max Entries** — Specifies the number of MAC address that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- **Action** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
 - *Discard* — Discards packets from any unlearned source. This is the default value.
 - *Forward* — Forwards packets from an unknown source without learning the MAC address.
 - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
 - *Enable* — Enables traps.
 - *Disable* — Disables traps.
- **Trap Frequency (Sec)** — The amount of time (in seconds) between traps. The range is between 1–1,000,000. The default value is 10 seconds.

2. Click **Edit** . The *Edit Port Security Settings Page* opens:

Figure 12. Edit Port Security Settings Page



The screenshot shows a web-based configuration window titled "Edit Port Security". It contains the following fields and controls:

- Interface:** Two radio buttons, "Port" (selected) and "LAG". The "Port" button is followed by a dropdown menu showing "Ext.1". The "LAG" button is followed by a dropdown menu showing "LAG1".
- Lock Interface:** A checkbox that is currently unchecked.
- Learning Mode:** A dropdown menu showing "Classic Lock".
- Max Entries:** A text input field containing the value "1".
- Action on Violation:** A dropdown menu showing "Discard".
- Enable Trap:** A checkbox that is currently unchecked.
- Trap Frequency:** A text input field containing the value "10".
- Buttons:** "Apply" and "Close" buttons at the bottom.

3. Modify the relevant fields.
4. Click **Apply** . The port security settings are defined, and the device is updated.

Defining Access Control Lists

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. If they are denied entry, the user can disable the port.

For example, an ACL rule is defined that states, port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is dropped. ACLs are composed of access control entries (ACEs) that are rules that determine traffic classifications.

When configuring ACLs consider the following:

- The maximum number of ACEs/rules per a single ACL are 1018.
- The maximum number of ACEs/rules in all ACLs are 1021.
- The maximum number of ACLs applied to a single interface are 256.

Stages for configuring ACLs:

1. Define an ACL and the initial ACL Rule.
2. Add additional rules to the ACL.

This section contains the following topics:

- Defining MAC Based Access Control Lists
- Defining IP Based Access Control Lists

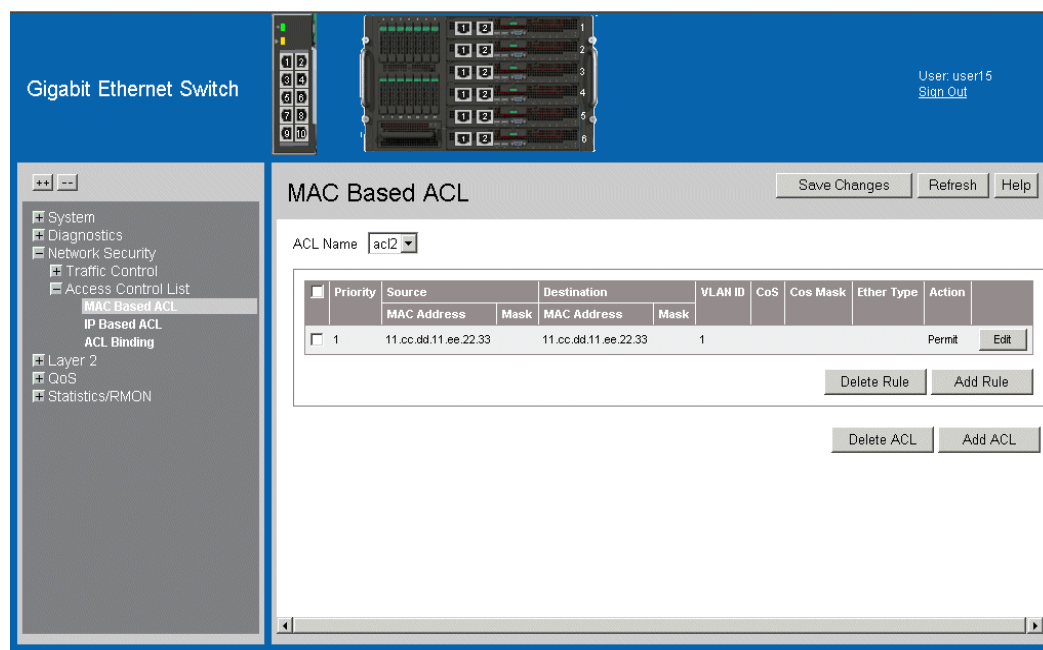
Defining MAC Based Access Control Lists

The *MAC Based ACL Page* allows a MAC-based ACL to be defined. Rules can be added only if the ACL is not bound to an interface.

To define MAC Based ACLs:

1. Click **Network Security > Access Control List > MAC Based ACL**. The *MAC Based ACL Page* opens:

Figure 13. MAC Based ACL Page



The *MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Check box**— Selecting the check box, deletes the MAC based ACLs. The possible field values are:
 - *Checked* — Deletes the selected MAC based ACL.
 - *Unchecked* — Maintains the MAC based ACLs.
- **Priority** — Indicates the Rule Priority, which determines which rule is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Source MAC Address.
 - *MAC Address* — Matches the source MAC Address to which packets are addressed to the rule.
 - *Mask* — Indicates the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source MAC Address. Wildcard masks specify which bits are used and which are ignored. A wildcard mask of FF:FF:FF:FF:FF:FF

indicates that no bit is important. A wildcard of 00.00.00.00.00.00 indicates that all bits are important. For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the last two bits are ignored.

- **Destination** — Destination MAC Address.
 - *MAC Address* — Matches the destination MAC Address to which packets are addressed to the rule.
 - *Mask* — Indicates the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination MAC address. Wildcard masks specify which bits are used and which are ignored. A wildcard mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard mask of 00.00.00.00.00.00 indicates that all bits are important. For example, if the destination MAC address is E0:00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the last two bits are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the rule. The possible field values are 1 to 4093.
- **CoS** — Classifies traffic based on the CoS tag value.
- **CoS Mask** — Defines the Cost of Service mask.
- **Ether Type** — Provides an identifier that differentiates between various types of protocols.
- **Action** — Indicates the ACL forwarding action. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Configuration Page*.

2. Click **Add ACL** . The *Add MAC Based ACL and First Rule Page* opens:

Figure 14. Add MAC Based ACL and First Rule Page

Add MAC Based ACL

ACL Name

New Rule Priority ☐

Source MAC Address Wild Card Mask ☐ Any

Dest. MAC Address Wild Card Mask ☐ Any

VLAN ID

CoS

CoS Mask

Ethertype

Action

Apply **Close**

The *Add MAC Based ACL and First Rule Page* contains the following fields:

- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first match basis.
3. Define the relevant fields.
 4. Click **Apply** . The MAC Based ACLs are defined, and the device is updated.
 5. Click **Add Rule** . The *Add ACL Rule Page* opens:

Figure 15. Add ACL Rule Page

Add MAC Based Rule

ACL Name

New Rule Priority ☐

Source MAC Address Wild Card Mask

Dest. MAC Address Wild Card Mask

VLAN ID

CoS

CoS Mask

Ethertype

Action

Apply **Close**

6. Define the relevant fields.
7. Click **Apply** . The ACL rule is defined, and the device is updated.

To modify a MAC-based rule:

1. Click **Network Security > Access Control List > MAC Based ACL**. The *Edit Rule Page* opens.
2. Click **Edit**. The *Edit Rule Page* opens:

Figure 16. Edit Rule Page

The screenshot shows a web-based configuration interface titled "Edit Rule". It contains several input fields for configuring a MAC-based Access Control List (ACL) rule. The fields are as follows:

- ACL Name:** acl2
- Rule Priority:** 1
- Source MAC Address:** aa:bb:cc:aa:bb:cc (with a radio button selected next to it)
- Wild Card Mask:** 11:cc:dd:11:ee:21 (with a radio button selected next to it)
- Any:** (radio button)
- Dest. MAC Address:** 11:cc:dd:11:ee:ee (with a radio button selected next to it)
- Wild Card Mask:** 11:cc:dd:11:ee:19 (with a radio button selected next to it)
- Any:** (radio button)
- VLAN ID:** 1
- CoS:** (empty field)
- CoS Mask:** (empty field)
- Ethertype:** (empty field)
- Action:** Permit (dropdown menu)

At the bottom right of the form, there are two buttons: "Apply" and "Close".

3. Modify the relevant fields.
4. Click **Apply**. The MAC-based rule is modified, and the device is updated.

Defining IP Based Access Control Lists

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. If they are denied entry, the user can disable the port. ACLs are composed of access control entries (ACEs) which are rules that are made of the filters that determine traffic classifications.

When configuring ACLs consider the following:

- The maximum number of ACEs/rules per a single ACL are 1018.
- The maximum number of ACEs/rules in all ACLs are 1021.
- The maximum number of ACLs applied to a single interface are 256.

The *IP Based ACL Page* contains information for defining IP Based ACLs and rules.

To define IP Based ACLs:

1. Click **Network Security > Access Control List > IP Based ACL**. The *IP Based ACL Page* opens:

Figure 17. IP Based ACL Page

The screenshot shows the 'IP Based ACL' configuration page. The left sidebar contains a navigation menu with the following items: System, Diagnostics, Network Security, Traffic Control, Access Control List, MAC Based ACL, IP Based ACL (selected), ACL Binding, Layer 2, QoS, and Statistics/RMON. The main content area is titled 'IP Based ACL' and includes a 'Save Changes' button, a 'Refresh' button, and a 'Help' button. Below the title, there is a dropdown for 'ACL Name' set to 'acl1'. A note states: '* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.' Below this is a table with the following columns: Priority, Protocol, Flag Set, ICMP Type, ICMP Code, IGMP Type, Source (IP Address, Mask), Destination (IP Address, Mask), Source Port, Destination Port, and DSCP. A single rule is listed with Priority 12, Protocol ICMP, and a 'Dele' button. The top right corner shows 'User: user15' and a 'Sign Out' link.

The *IP Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Delete** — Deletes the IP based ACLs. The possible field values are:
 - *Checked* — Deletes the selected IP based ACL.
 - *Unchecked* — Maintains the IP based ACLs.
- **Priority** — Indicates the Rule priority that determines which rule is matched to a packet based on a first-match basis. The possible field value is 1-2147483647.

- **Protocol** — Creates an rule based on a specific protocol.
 - *Select from List* — Selects from a protocols list on which rule can be based. The possible field values are:
 - ICMP** — *Internet Control Message Protocol* (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
 - IGMP** — *Internet Group Management Protocol* (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.
 - IP** — *Internet Protocol* (IP). Specifies the format of packets and their addressing method. IP addresses packets and forwards the packets to the correct port.
 - TCP** — *Transmission Control Protocol* (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order the are sent.
 - EGP** — *Exterior Gateway Protocol* (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
 - IGP** — *Interior Gateway Protocol* (IGP). Allows for routing information exchange between gateways in an autonomous network.
 - UDP** — *User Datagram Protocol* (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
 - HMP** — *Host Mapping Protocol* (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
 - RDP** — *Remote Desktop Protocol* (RDP). Allows a clients to communicate with the Terminal Server over the network.
 - IDRP** — Matches the packet to the *Inter-Domain Routing Protocol* (IDRP).
 - RVSP** — Matches the packet to the *ReSerVation Protocol* (RSVP).
 - AH** — *Authentication Header* (AH). Provides source host authentication and data integrity.
 - EIGRP** — *Enhanced Interior Gateway Routing Protocol* (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
 - OSPF** — The *Open Shortest Path First* (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).
 - IPIP** — *IP over IP* (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensures that the IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
 - PIM** — Matches the packet to *Protocol Independent Multicast* (PIM).
 - L2TP** — Matches the packet to *Layer 2 Internet Protocol* (L2IP).
 - ISIS** — *Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks

Any — Matches the protocol to any protocol.

— *Protocol ID* — Adds user-defined protocols by which packets are matched to the rule. Each protocol has a specific protocol number which is unique. The possible field range is 0-255.

- **Flag Set** — Displays the TCP flag that can be triggered.
- **ICMP Type** — Specifies an ICMP message type for filtering ICMP packets.
- **ICMP Code** — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP Type** — Displays the IGMP message type. IGMP packets can be filtered by IGMP message type.
- **Source IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
- **Source Mask** — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination IP Address** — Matches the destination IP address to which packets are addressed to the rule.
- **Destination Mask** — Indicates the destination IP Address wildcard mask. Wildcards are used to mask all or part of a destination IP Address. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that no bit is important. A wildcard of 00.00.00.00 indicates that all the bits are not important. For example, if the destination IP address is 149.36.184.198 and the wildcard mask is 255.255.255.00, the last three digits in the IP address are checked while the first 3 sets are ignored.
- **Source Port** — Defines the TCP/UDP source port to which the rule is matched. This field is active only if 800/6-TCP or 800/17-UDP are selected in the *Select from List* drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the *Select from List* drop-down menu. The possible field range is 0 - 65535.
- **DSCP** — Matches the destination port IP address to which packets are addressed to the rule.
- **IP - Prec.** — Defines the destination IP address wildcard mask. Select either *Match DSCP* or *Match IP Precedence*:
 - *Match DSCP* — Matches the packet DSCP value to the rule. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-63.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the rule. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.

- **Action** — Indicates the ACL forwarding action. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Configuration Page*.

2. Click **Add ACL** . The *Add IP Based ACL and First Rule Page* opens:

Figure 18. Add IP Based ACL and First Rule Page

3. Define the relevant fields.
4. Click **Apply** . The IP based ACL and first rule are defined, and the device is updated.

To add an IP based Rule to the ACL:

1. Click **Network Security > Access Control List > IP Based ACL**. The *IP Based ACL Page* opens.
2. Click **Add Rule**. The *Add IP Based Rule Page* opens:

Figure 19. Add IP Based Rule Page

The screenshot shows the 'Add IP Based Rule' configuration window. The fields are as follows:

- ACL Name: acl1
- New Rule Priority: 0
- Protocol: Select from List ANY, Protocol ID: 1
- Source Port: Any
- Destination Port: Any
- TCP Flags: URG, ACK, PUSH, RST, SYN, FIN (all Set)
- ICMP: Select from List Echo-Reply, ICMP Type: Any
- ICMP Code:
- ICMP: Select from List DVMRP, ICMP Type: Any
- Source IP Address: Wild Card Mask: Any
- Dest. IP Address: Wild Card Mask: Any
- Match DSCP:
- Match IP Precedence:
- Action: Permit

Buttons: Apply, Close

3. Define the relevant fields.
4. Click **Apply**. The IP based rules are defined, and the device is updated.

To modify an IP based Rule:

1. Click **Network Security > Access Control List > IP Based ACL**. The *IP Based ACL Page* opens.
2. Select an ACL.
3. Click **Edit** . The *Edit Rule Page* opens:

Figure 20. Edit Rule Page

The screenshot shows the 'Edit Rule' configuration window. The fields are as follows:

- ACL Name: acl2
- New Rule Priority: 11
- Protocol: ICMP
- TCP Flags: ☐ Urg ☐ Set ☐ Ack ☐ Set ☐ Psh ☐ Set ☐ Rst ☐ Set ☐ Syn ☐ Set ☐ Fin ☐ Set
- ICMP: ☐ ☐ Select from List Echo-Reply ☐ ICMP Type ☐ Any
- ICMP Code: ☐
- IGMP: ☐ ☐ Select from List DVMRP ☐ IGMP Type ☐ Any
- Source IP Address: ☐ Wild Card Mask ☐ Any
- Dest. IP Address: ☐ Wild Card Mask ☐ Any
- Match DSCP: ☐
- Match IP Precedence: ☐
- Source Port:
- Destination Port:
- Action: Permit

Buttons: Apply, Close

4. Modify the relevant fields.
5. Click **Apply** . The IP based rule is defined, and the device is updated.

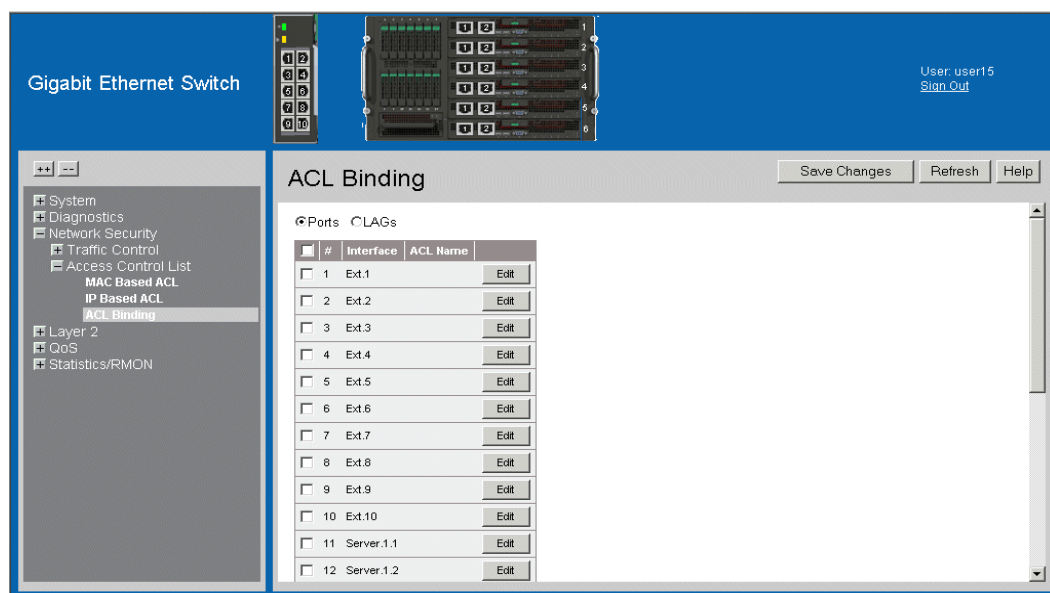
Binding Device Security ACLs

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets.

To bind ACLs to interfaces:

1. Click **Network Security > Access Control List > ACL Binding**. The *ACL Binding Page* opens:

Figure 21. ACL Binding Page

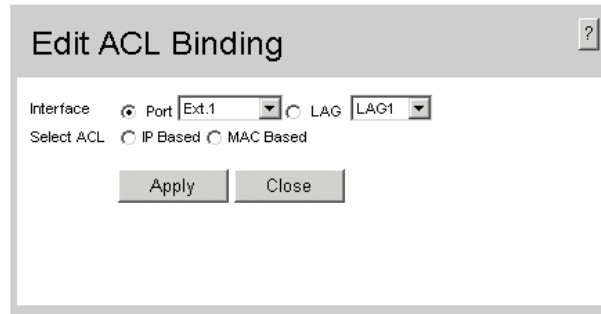


The *ACL Binding Page* contains the following fields:

- **Check Box** — Selecting the check box, selects the ACL binding entry. The possible field values are:
 - *Checked* — Selects the MAC based ACL.
 - *Unchecked* — Maintains the MAC based ACLs.
- **Ports** — Indicates the port membership.
- **LAGs** — Indicates the LAG membership.
- **Interface** — Indicates the interface to which the ACL is bound.
- **ACL Name** — Indicates the ACL which is bound the interface.

2. Select an interface.
3. Click **Edit** . The *Edit ACL Binding Page* opens:

Figure 22. Edit ACL Binding Page



The screenshot shows a dialog box titled "Edit ACL Binding" with a help icon (?) in the top right corner. Inside the dialog, there are two sections. The first section, labeled "Interface", contains two radio buttons: "Port" (which is selected) and "LAG". Next to "Port" is a dropdown menu showing "Ext.1", and next to "LAG" is a dropdown menu showing "LAG1". The second section, labeled "Select ACL", contains two radio buttons: "IP Based" (which is selected) and "MAC Based". At the bottom of the dialog, there are two buttons: "Apply" and "Close".

4. Define the relevant fields.
- Click **Apply** . The ACL is bound the interface, and the device is updated.

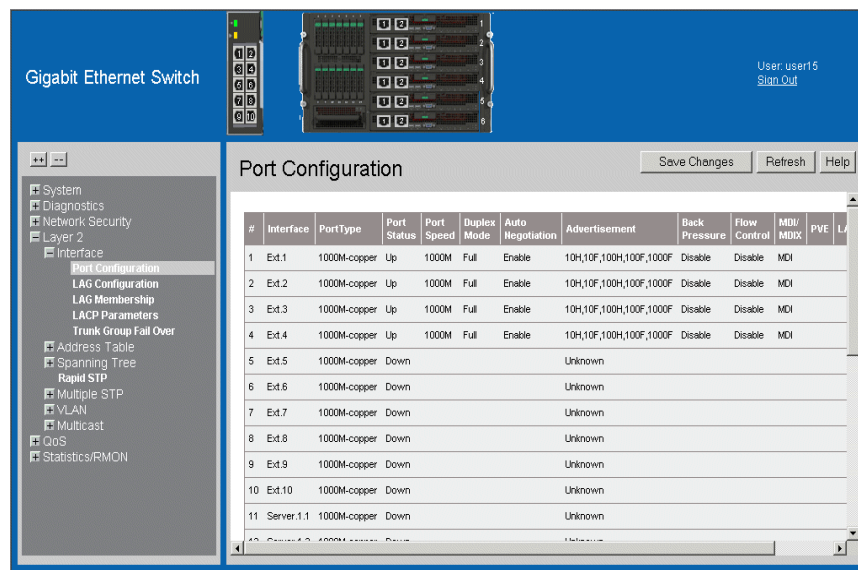
4 Configuring Ports

The *Port Configuration Page* contains fields for defining port parameters.

To define port parameters:

1. Click **Layer 2 > Interface > Port Configuration**. The *Port Configuration Page* opens.

Figure 23. Port Configuration Page



The *Port Configuration Page* contains the following fields:

- **Interface** — Displays the port number.
- **PortType** — Displays the port type. The possible field values are:
 - *1000M-Copper* — Indicates the port has a copper port connection.
- **Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
 - *Up* — Indicates the port is currently operating.
 - *Down* — Indicates the port is currently not operating.
- **Port Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. The possible field values are:
 - *10* — Indicates the port is currently operating at 10 Mbps.
 - *100* — Indicates the port is currently operating at 100 Mbps.
 - *1000* — Indicates the port is currently operating at 1000 Mbps.
 - *10G* — Indicates the port is currently operating at 10 Gbps.

- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
 - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
- **Auto Negotiation** — Displays the auto negotiation status on the port. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner.
- **Advertisement** — Defines the auto negotiation setting the port advertises. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and duplex mode settings are accepted.
 - *10 Half* — Indicates that the port advertises for a 10 Mbps speed port and half duplex mode setting.
 - *10 Full* — Indicates that the port advertises for a 10 Mbps speed port and full duplex mode setting.
 - *100 Half* — Indicates that the port advertises for a 100 Mbps speed port and half duplex mode setting.
 - *100 Full* — Indicates that the port advertises for a 100 Mbps speed port and full duplex mode setting.
 - *1000 Full* — Indicates that the port advertises for a 1000 Mbps speed port and full duplex mode setting.
- **Back Pressure** — Displays the back pressure mode on the Port. Back pressure mode is used with half duplex mode to disable ports from receiving messages.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode. The possible field values are:
 - *Enable* — Enables the flow control.
 - *Disable* — Disables the flow control.
 - *Auto-Negotiation* — Detects the flow control and automatically configures the highest performance mode.
- **MDI/MDIX** — Displays the MDI/MDIX status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
 - *MDIX (Media Dependent Interface with Crossover)* — Use for hubs and switches.
 - *MDI (Media Dependent Interface)* — Use for end stations.
 - *AUTO* — Use to automatically detect the cable type.

- **PVE** — Defines the port as a *Private VLAN Edge* (PVE) port. PVE is configured on the port level and indicates that all traffic received on the port will be redirected to an uplink port. The PVE associated Uplinks ports are defined on the *Port Configuration Settings Page*.
 - **LAG** — Indicates whether the port is part of a *Link Aggregation Group* (LAG).
2. Define the relevant fields.
 3. Click **Apply** . The port configuration settings are defined, and the device is updated.

To modify the port configuration:

1. Click **Edit** . The *Port Configuration Settings Page* opens:

Figure 24. Port Configuration Settings Page

In addition the fields appearing on the *Port Configuration Page*, the *Port Configuration Settings Page* contains the following fields:

- **Description** — Provides a user-defined port description.
- **Admin Status** — Displays the port operational status. Changes to the port state are active only after the device is reset. The possible field values are:
 - *Up* — Indicates that the port is currently operating.
 - *Down* — Indicates that the port is currently not operating.
- **Current Port Status** — Displays the current status of the port.
- **Reactivate Suspended Port** — Reactivates a port if the port has been disabled through the locked port security option.

- **Operational Status** — Indicates the port operational status. Possible field values are:
 - *Suspended* — Indicates the port is currently active, and is not receiving or transmitting traffic.
 - *Active* — Indicates the port is currently active and is receiving and transmitting traffic.
 - *Disable* — Indicates the port is currently disabled, and is not receiving or transmitting traffic.
 - **Admin Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available.
 - **Current Port Speed** — Displays the actual synchronized port speed (bps).
 - **Admin Duplex** — Indicates port duplex mode can be either **Full** or **Half**. **Full** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half** indicates that the interface supports transmission between the device and the client in only one direction at a time.
 - **Current Duplex Mode** — Displays the currently configured port duplex mode.
 - **Current Duplex Mode** — Displays the current Duplex Mode.
 - **Current Auto Negotiation** — Displays the current Auto Negotiation Mode.
 - **Admin Advertisement** — Defines the auto-negotiation setting the port advertises. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and Duplex mode settings are accepted.
 - *10 Full* — Indicates that the port advertises for a 10 mbps speed port and full duplex mode setting.
 - *100 Full* — Indicates that the port advertises for a 100 mbps speed port and full duplex mode setting.
 - *1000 Full* — Indicates that the port advertises for a 1000 mbps speed port and full duplex mode setting.
 - **Current Advertisement** — The port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the **Admin advertisement** field.
 - **Neighbor Advertisement** — Indicates the neighboring port's advertisement settings. The field values are identical to the **Admin Advertisement** field values.
 - **Current Back Pressure** — Displays the current Back Pressure setting.
 - **Current Flow Control** — Displays the current Flow Control setting.
 - **Current MDI/MDIX** — Displays the current MDI/MDIX setting. Define the relevant fields.
2. Click  . The port configuration settings are defined, and the device is updated.

5 Aggregating Ports

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

The device supports both static LAGs and *Link Aggregation Control Protocol* (LACP) LAGs. LACP LAGs negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them. Ensure the following:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to 10 LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.
- Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.
- LAGs can be configured only on external ports.

This section contains the following topics:

- Configuring LAGs
- Defining LAG Members
- Configuring LACP
- Configuring Virtual Trunk Group Failover

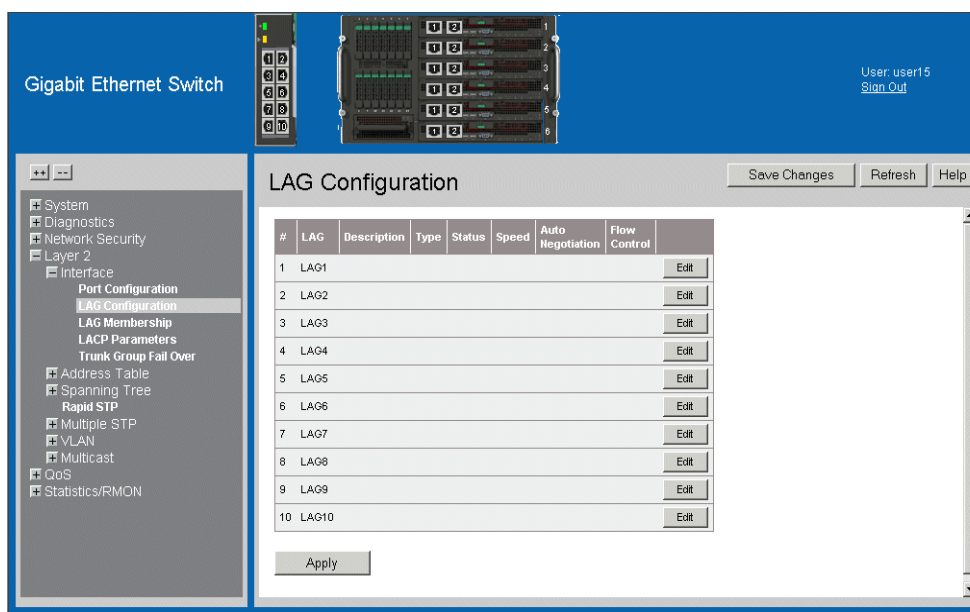
Configuring LAGs

The *LAG Configuration Page* contains information for configured LAGs.

To view LAG information:

1. Click **Layer 2 > Interface > LAG Configuration**. The *LAG Configuration Page* opens:

Figure 25. LAG Configuration Page



The *LAG Configuration Page* contains the following fields:

- **LAG** — Indicates the LAG for which the information is displayed.
- **Description** — Provides a user-defined LAG description.
- **Type** — Displays the port types included in the LAG.
- **Status** — Indicates if traffic forwarding via the LAG is enabled. The possible field values are:
 - *Up* — Indicates that the LAG is currently forwarding network traffic.
 - *Down* — Indicates that the LAG is not currently forwarding network traffic.
- **Speed** — Displays the LAG speed.
- **Auto Negotiation** — Indicates if auto-negotiation is enabled on the LAG. The possible field values are:
 - *Enable* — Indicates that auto-negotiation is enabled on the LAG.
 - *Disable* — Indicates that auto-negotiation is disabled on the LAG.

- **Flow Control** — Indicates if flow control auto-negotiation is enabled on the LAG. The possible field values are:
 - *Enable* — Indicates that flow control is enabled on the LAG.
 - *Disable* — Indicates that flow control is disable on the LAG.
 - *Auto Negotiation* — Detects the flow control and automatically configures the highest performance mode.
2. Define the relevant fields.
 3. Click **Apply** . The LAG configuration settings are saved, and the device is updated.

To modify the LAG configuration:

1. Click **Edit** . The *LAG Configuration Settings Page* opens:

Figure 26. LAG Configuration Settings Page

The screenshot shows the 'LAG Configuration Settings' dialog box. The fields are as follows:

LAG	2
Description	
Type	
Admin Status	Up
Current Status	
Reactivate Suspended	☐
Operational Status	Active
Admin Auto Negotiation	Enable
Current Auto Negotiation	
Admin Advertisement	☒ Max Capability ☐ 10 Full ☐ 100 Full ☐ 1000 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Admin Speed	
Current Speed	
Admin Flow Control	Disable
Current Flow Control	

At the bottom of the dialog are two buttons: **Apply** and **Close**.

In addition the fields appearing on the *LAG Configuration Page*, the *LAG Configuration Settings Page* contains the following fields:

- **Admin Status** — Displays the LAG operational status. Changes to the LAG state are active only after the device is reset. The possible field values are:
 - *Up* — Indicates that the LAG is currently operating.
 - *Down* — Indicates that the LAG is currently not operating.
- **Current Status** — Displays the current status of the LAG.
- **Reactivate Suspended** — Reactivates a port if the port has been disabled through the locked port security option.
- **Operational Status** — Indicates the port operational status. Possible field values are:
 - *Suspended* — The port is currently active, and is not receiving or transmitting traffic.
 - *Active* — The port is currently active and is receiving and transmitting traffic.
 - *Disable* — The port is currently disabled, and is not receiving or transmitting traffic.
- **Admin Auto Negotiation** — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.
- **Admin Advertisement** — Defines the auto-negotiation setting the port advertises. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and Duplex mode settings are accepted.
 - *10 Full* — Indicates that the port advertises for a 10 mbps speed port and full duplex mode setting.
 - *100 Full* — Indicates that the port advertises for a 100 mbps speed port and full duplex mode setting.
 - *1000 Full* — Indicates that the port advertises for a 1000 mbps speed port and full duplex mode setting.
- **Current Advertisement** — The port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the **Admin advertisement** field.
- **Neighbor Advertisement** — Indicates the neighboring port's advertisement settings. The field values are identical to the **Admin Advertisement** field values.
- **Admin Speed** — The configured rate for the port. The port type determines what speed setting options are available. Admin speed can only be designated when the **Admin Auto Negotiation** field is disabled.
- **Current Speed** — The actual synchronized port speed (bps).
- **Admin Flow Control** — Enables/disables flow control, or enables the auto negotiation of flow control on the LAG. Flow Control mode is effective on the ports operating in Full Duplex in the LAG.

- **Current Flow Control** — The current Flow Control setting.
 2. Define the relevant fields.
 3. Click  . The LAG configuration is saved, and the device is updated.

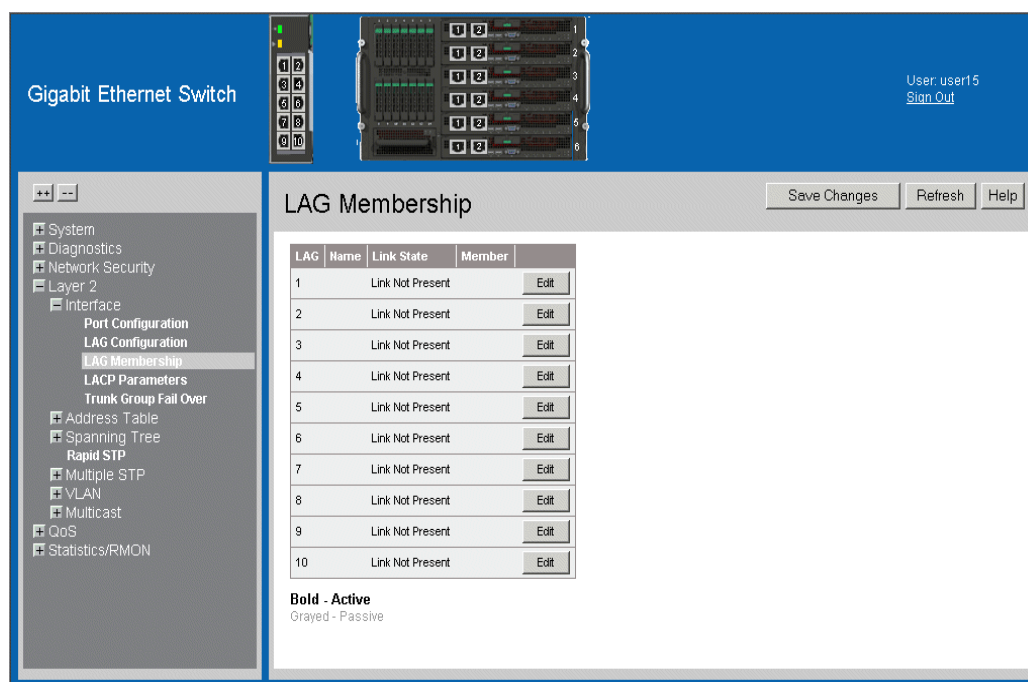
Defining LAG Members

The *LAG Membership Page* contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and ten LAGs per system. LAGs can be configured only on external ports.

To define LAG parameters:

1. Click **Layer 2 > Interface > LAG Membership**. The *LAG Membership Page* opens.

Figure 27. LAG Membership Page



The *LAG Membership Page* contains the following fields:

- **LAG** — Displays the ports which can be assigned to the LAG.
 - **Name** — Indicates the LAG name.
 - **Link State** — Displays the status of the link.
 - **Member** — Displays the ports which are currently configured to the LAG.
2. Define the relevant fields.
 3. Click [Apply](#). The LAG membership settings are saved, and the device is updated.

To modify the LAG membership:

1. Click **Edit** . The *LAG Membership Settings Page* opens:

Figure 28. LAG Membership Settings Page

LAG Membership Settings

LAG: 1

LAG Name:

LACP: ☐

Port List

Ext.1
Ext.2
Ext.3
Ext.4
Ext.5
Ext.6
Ext.7
Ext.8

Lag Members

Apply Close

In addition the fields appearing on the *LAG Membership Page*, the *LAG Membership Settings Page* contains the following fields:

- **LACP** — Enables LACP on the selected LAG.
2. Define the relevant fields.
 3. Click **Apply** . The LAG configuration is saved, and the device is updated.

Configuring LACP

LAG ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed. The *LACP Parameters Page* contains fields for configuring LACP LAGs.

To configure LACP for LAGs:

1. Click **Layer 2 > Interface > LACP Parameters**. The *LACP Parameters Page* opens:

Figure 29. LACP Parameters Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

Save Changes Refresh Help

LACP Parameters

LACP System Priority:

#	Port	Port-Priority	LACP Timeout	
1	Ext.1	1	Long	Edit
2	Ext.2	1	Long	Edit
3	Ext.3	1	Long	Edit
4	Ext.4	1	Long	Edit
5	Ext.5	1	Long	Edit
6	Ext.6	1	Long	Edit
7	Ext.7	1	Long	Edit
8	Ext.8	1	Long	Edit
9	Ext.9	1	Long	Edit
10	Ext.10	1	Long	Edit
11	10G.XC	1	Long	Edit
12	10G.SC	1	Long	Edit

System
Diagnostics
Network Security
Layer 2
Interface
Port Configuration
LAG Configuration
LAG Membership
LACP Parameters
Trunk Group Fail Over
Address Table
Spanning Tree
Rapid STP
Multiple STP
VLAN
Multicast
QoS
Statistics/RMON

The *LACP Parameters Page* contains the following fields:

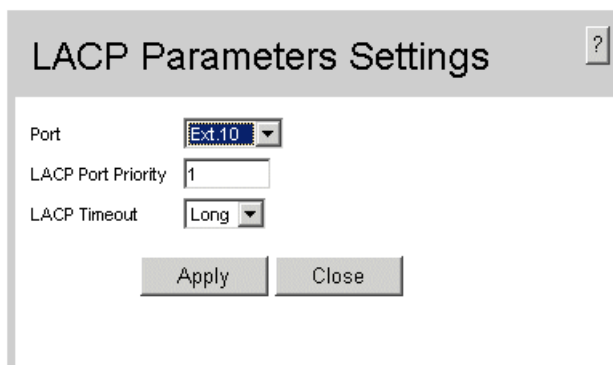
- **LACP System Priority** — Specifies system priority value. The field range is 1-65535. The field default is 1.
- **Port** — Displays the port number to which timeout and priority values are assigned.
- **Port-Priority** — Displays the LACP priority value for the port. The field range is 1-65535. The field default is 1.
- **LACP Timeout** — Displays the administrative LACP timeout. The possible field values are:
 - *Long* — Specifies the long timeout value.
 - *Short* — Specifies the short timeout value.

2. Define the relevant fields.
3. Click **Apply** . The LACP parameters are saved, and the device is updated.

To modify the LACP parameters:

1. Click **Edit** . The *LACP Parameters Settings Page* opens:

Figure 30. LACP Parameters Settings Page



The screenshot shows a dialog box titled "LACP Parameters Settings" with a help icon (?) in the top right corner. Inside the dialog, there are three configuration fields: "Port" with a dropdown menu showing "Ext 10", "LACP Port Priority" with a text input field containing the value "1", and "LACP Timeout" with a dropdown menu showing "Long". At the bottom of the dialog, there are two buttons: "Apply" and "Close".

2. Modify the relevant fields.
3. Click **Apply** . The LACP parameters are saved, and the device is updated.

Configuring Virtual Trunk Group Failover

The *Trunk Group Fail Over Page* enables a network administrator to define a *Virtual Trunk Group Failover* feature. The Trunk Group Failover increases network stability by ensuring that if a trunk group fails, a different trunk begins to forward the failed trunk's traffic. A Virtual Trunk Group Failover is comprised of user defined port groups that include:

- **Uplink Ports** — Connects the switch and external network to the associated internal ports and server NIC.
- **Associated Ports** — Associated with an Uplink port. Uplinks ports forward host traffic associated ports to the external network. Although an associated port typically connects to a Device. External switch ports can also be an Associated port. For example, a server connected to an external switch port as well as to a dependent group of ports on an Uplink port that forwards traffic to the external network.

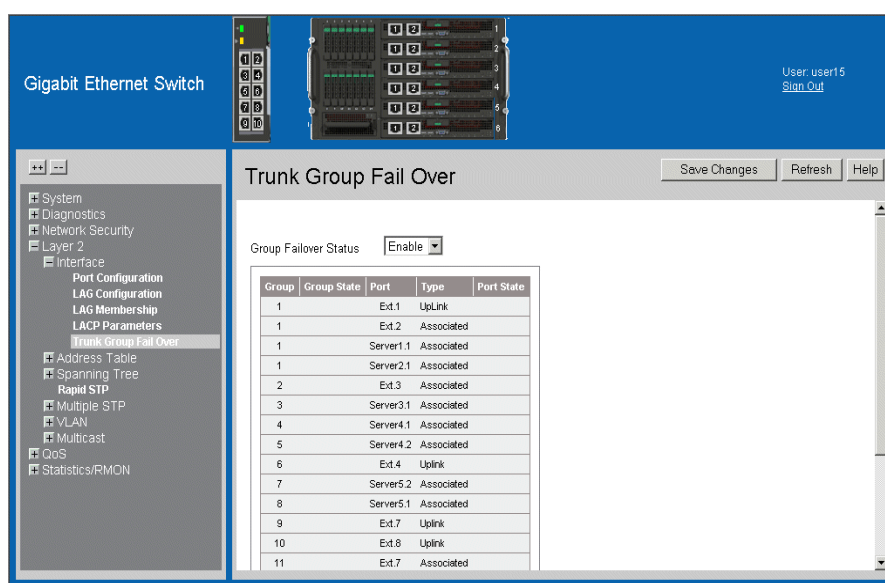
Ensure the following when configuring Virtual Trunk Groups:

- The minimum number of Virtual Trunk Groups is one, whereas the maximum is 12.
- A port cannot be a member of more than one Virtual Trunk Group.
- Virtual Trunk Group Failover is globally enabled.
- The *Virtual Trunk Group Failover* feature cannot be defined on LAGs. However, individual ports within a LAG can be added to a Virtual Trunk Group.
- One Virtual Trunk group can have one or more Uplink ports, and one or more Associated ports.
- Only one Uplink port within the Virtual Trunk Group is required to go up in order for all the associated ports to go up.
- The Associated ports are deactivated within 500ms from the time that the last Uplink port in the Virtual Trunk group fails. The Associated ports reactivate within 500ms whenever a single Uplink port within the group is restored.
- Before the administrator shuts down an Associated port, the administrator must exclude the Associated port from any Virtual Failover group.
- The Associated ports which have been shut down administratively cannot be added to any failover group by the administrator.
- Failover groups can be configured any time regardless of the feature state.
- When Virtual Trunk Group Failover is disabled, all Associated ports disabled by the Virtual Trunk Group Failover feature are re-enabled.
- When Virtual Trunk Group Failover is enabled, all configured failover groups are scanned to update the Associated port status.
- A log message is generated and sent to the system log and stored when an Associated port goes UP or Down.

To configure Trunk Group Failover:

1. Click **Layer 2 > Interface > Trunk Group Fail Over**. The *Trunk Group Fail Over Page* opens:

Figure 31. Trunk Group Fail Over Page



The *Trunk Group Fail Over Page* contains the following fields:

- **Group Failover Status** — Enables the Trunk Group Failover feature on the device. The possible field values are:
 - *Enable* — Enables Trunk Group Failover on the device.
 - *Disable* — Disables Trunk Group Failover on the device.
- **Group** — Displays the Trunk Group number.
- **Group State** — Indicates the Trunk Group state. The possible field values are:
 - *Up* — Indicates the group state is active.
 - *Down* — Indicates the group state is inactive.
- **Port** — Displays the port added to the specific Trunk Group.
- **Type** — Displays the port type. The possible field values are:
 - *Uplink* — Ports that connect the switch and external network to the associated internal ports and server NIC.
 - *Associated* — Ports that are associated with an Uplink port.
- **Port State** — Indicates the port state within the Trunk Group. The possible field values are:
 - *Up* — Indicates the port is in the **Up** state.
 - *Down* — Indicates the port is in the **Down** state.

To modify the Fail Over Group:

1. Click **Edit** . The *Edit Fail Over Group Page* opens:

Figure 32. Edit Fail Over Group Page

Edit Fail Over Group ?

Pressing the Arrow button assigns the port to the Fail Over Group.

Fail Over Group **1**

Ports

Uplink Ports

Ext.1
Ext.2
Ext.3
Ext.4
Ext.5
Ext.6
Ext.7
Ext.8
Ext.9
Ext.10
Server.1.
Server.1.
Server.2.
Server.2.
Server.3.
Server.3.
Server.4.
Server.4.
Server.5.
Server.5.

Associated Ports

Close

2. Select a Fail Over Group to be defined.
3. Define the Ext. or Server ports as a Uplink or Associated port.
4. Click **Apply** . The Group Fail Over groups are defined, and the device is updated.

6 Configuring VLANs

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router working at a protocol level is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

Combining VLANs and *Generic Attribute Registration Protocol* (GARP) allows network managers to define network nodes into Broadcast domains.

This section contains the following topics:

- Defining VLAN Properties
- Defining VLAN Membership
- Defining VLAN Interface Settings
- Configuring GARP

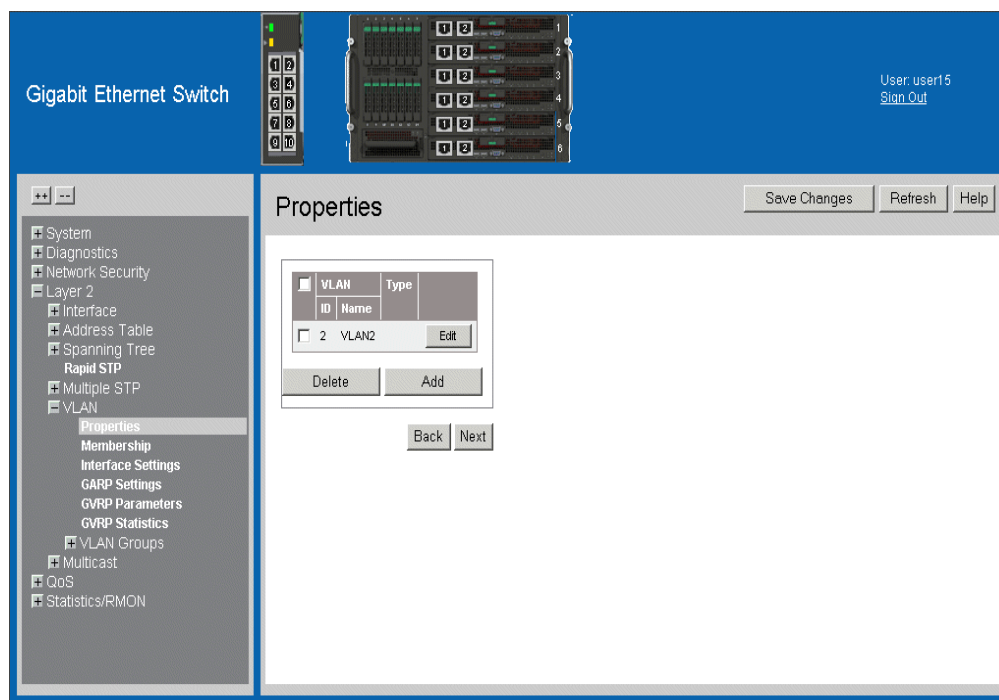
Defining VLAN Properties

The *VLAN Properties Page* provides information and global parameters for configuring and working with VLANs.

To define VLAN properties:

1. Click **Layer 2 > VLAN > Properties**. The *VLAN Properties Page* opens.

Figure 33. VLAN Properties Page



The *VLAN Properties Page* contains the following fields:

- **Delete** — Deletes VLANs. The possible field values are:
 - *Checked* — Deletes the selected VLAN.
 - *Unchecked* — Maintains VLANs.
- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Displays the user-defined VLAN name.
- **Type** — Displays the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GARP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.

- **Back** — Allows you to view the previous page in a table.
 - **Next** — Allows you to view the next page in a table when there are more than 20 entries.
2. Click **Add** . The *Add VLAN Page* opens:

Figure 34. Add VLAN Page

3. Define the relevant fields.
4. Click **Apply** . The VLAN ID is defined, and the device is updated.

To modify the VLAN ID:

1. Click **Layer 2 > VLAN > Properties**. The *VLAN Properties Page* opens.
2. Click **Edit** . The *VLAN Settings Page* opens:

Figure 35. VLAN Settings Page

3. Modify the relevant fields.
4. Click **Apply** . The VLAN Name is defined, and the device is updated.

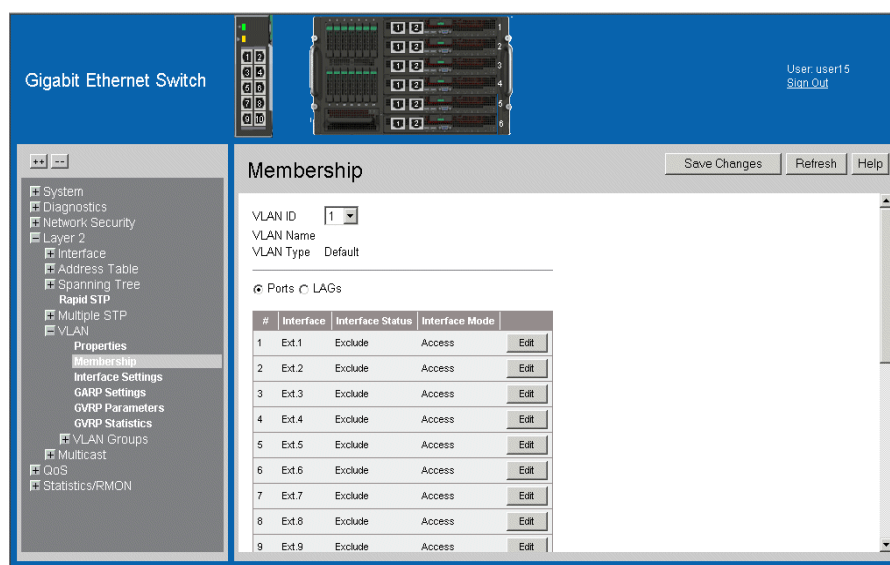
Defining VLAN Membership

The *VLAN Membership Page* contains a table that maps VLAN parameters to ports/LAGs. Interfaces are assigned VLAN membership by toggling through the Port Control settings.

To define VLAN membership:

1. Click **Layer 2 > VLAN > Membership**. The *VLAN Membership Page* opens.

Figure 36. VLAN Membership Page



The *VLAN Membership Page* contains the following fields:

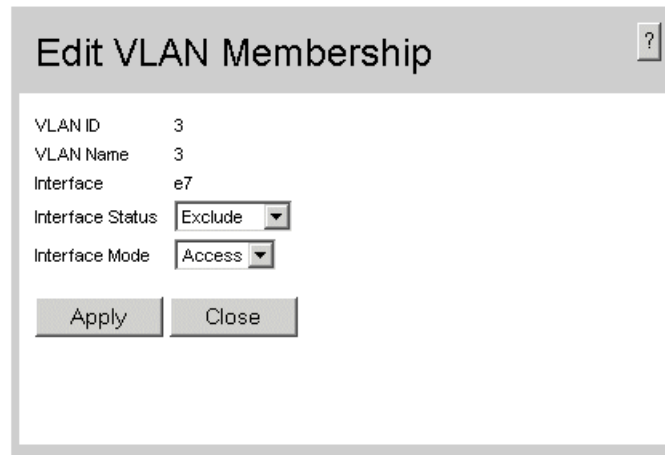
- **VLAN ID** — Displays the user-defined VLAN ID.
- **VLAN Name** — Displays the name of the VLAN
- **VLAN Type** — Indicates the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GARP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Ports** — Indicates the port membership.
- **LAGs** — Indicates the LAG membership.
- **Interface** — Displays the VLAN interfaces.

- **Interface Status** — Indicates the port status. The possible field values are:
 - *Excluded* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
 - *Forbidden* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.
 - *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
 - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
 - **Interface Mode** — Displays the interface mode. The possible field values are:
 - *General* — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode). This is the default value.
 - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that can be untagged.
 - *Access* — Indicates a port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled or disabled on an access port.
2. Define the relevant fields.
 3. Click Apply. The VLAN membership is defined, and the device is updated.

To modify the VLAN membership:

1. Click **Edit** . The *Edit VLAN Membership Page* opens:

Figure 37. Edit VLAN Membership Page



Edit VLAN Membership ?

VLAN ID	3
VLAN Name	3
Interface	e7
Interface Status	Exclude ▼
Interface Mode	Access ▼

Apply Close

2. Modify the relevant fields.
3. Click **Apply** . The VLAN membership is modified

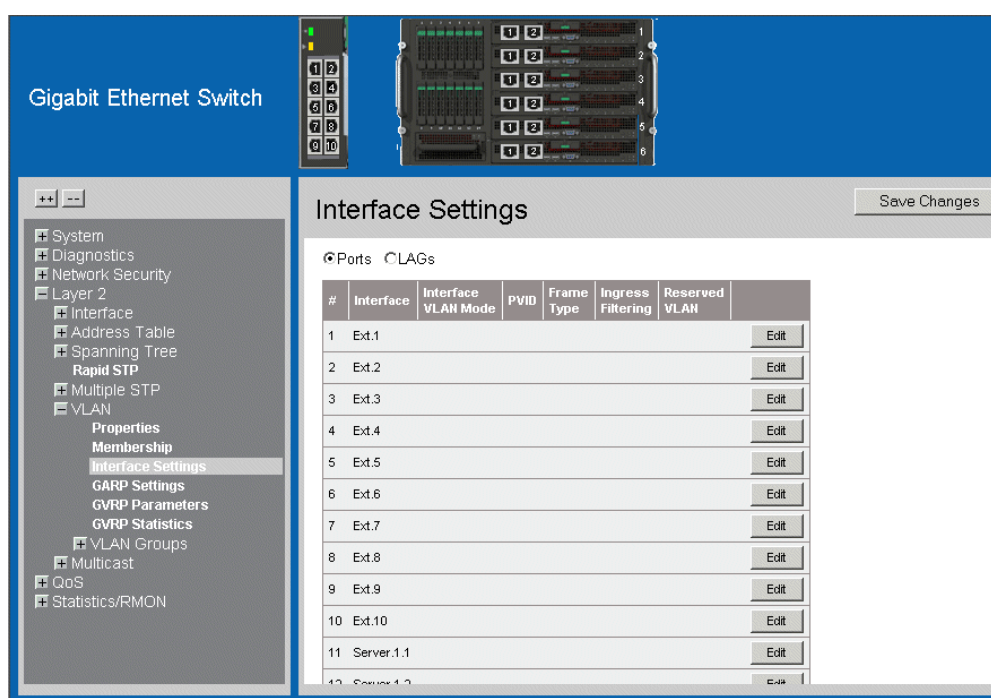
Defining VLAN Interface Settings

The *Interface Settings Page* contains fields for managing ports/LAGs that are part of a VLAN. The *Port Default VLAN ID (PVID)* is configured on the *Interface Settings Page*. All untagged packets arriving at the device are tagged with the port PVID.

To define VLAN interfaces:

1. Click **Layer 2 > VLAN > Interface Settings**. The *Interface Settings Page* opens.

Figure 38. Interface Settings Page



The *Interface Settings Page* contains the following fields:

- **Ports** — Indicates the port membership.
- **LAGs** — Indicates the LAG membership.
- **Interface** — Displays the interface number included in the VLAN.
- **Interface VLAN Mode** — Displays the interface mode. The possible values are:
 - *General* — Indicates the interface belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
 - *Access* — Indicates a interface belongs to a single untagged VLAN. When an interface is in Access mode, the packet types which are accepted on the port

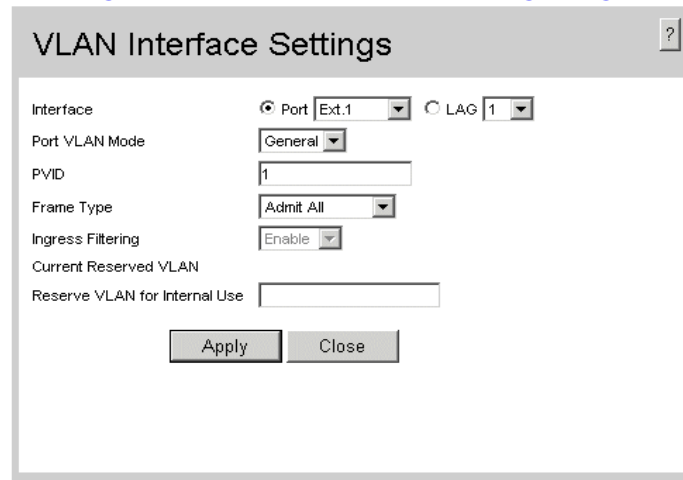
cannot be designated. Ingress filtering cannot be enabled or disabled on an access port.

- *Trunk* — Indicates the interface belongs to VLANs in which all VLANs are tagged, except for one VLAN that can be untagged.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1-4094 except VLAN 4080. VLAN 4095 is defined as per standard and industry practice as the Discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Specifies the packet type accepted on the interface. The possible field values are:
 - *Admit All* — Both tagged and untagged packets are accepted on the interface.
 - *Admit Tag Only* — Only tagged packets are accepted on the interface.
- **Ingress Filtering** — Indicates whether ingress filtering is enabled on the interface. The possible field values are:
 - *Enable* — Enables ingress filtering on the interface. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.
 - *Disable* — Disables ingress filtering on the interface.
- **Reserved VLAN** — Indicates the VLAN selected by the user to be the reserved VLAN if not in use by the system.

To modify the VLAN interface settings:

1. Click **Edit** . The *Interface Settings Page* opens:

Figure 39. VLAN Interface Settings Page



The screenshot shows a dialog box titled "VLAN Interface Settings" with a help icon (?) in the top right corner. The dialog contains the following fields and controls:

- Interface:** Two radio buttons, "Port" (selected) and "LAG". The "Port" button has a dropdown menu showing "Ext.1". The "LAG" button has a dropdown menu showing "1".
- Port VLAN Mode:** A dropdown menu showing "General".
- PVID:** A text input field containing the value "1".
- Frame Type:** A dropdown menu showing "Admit All".
- Ingress Filtering:** A dropdown menu showing "Enable".
- Current Reserved VLAN:** A text input field.
- Reserve VLAN for Internal Use:** A text input field.
- Buttons:** "Apply" and "Close" buttons at the bottom.

In addition the fields appearing on the *Interface Settings Page*, the *VLAN Interface Settings Page* contains the following fields:

- **Current Reserved VLAN** — Displays the current reserved VLAN on the interface.
 - **Reserve VLAN for Internal Use** — Indicates the VLAN selected by the user to be the reserved VLAN if not in use by the system.
2. Modify the relevant fields.
 3. Click **Apply** . The VLAN membership is modified

Defining VLAN Groups

VLAN groups increase network flexibility and portability. For example, network users grouped by MAC address can log on to the network from multiple locations without moving between VLANs.

VLANs can be grouped by MAC address, Subnets, and Protocols. Once a user logs on, the system attempts to classify the user by MAC address. If the user cannot be classified by MAC address, the system attempts to classify the user by Subnet. If the subnet classification is unsuccessful, the system attempts to classify the user by protocol. If the protocol classification is unsuccessful, the user is classified by PVID.

VLAN groups allow network managers to define VLAN groups based on specific criteria, including MAC addresses, network subnets, and protocols. This section contains the following topics:

- Defining VLAN MAC Based Groups
- Defining VLAN Subnet Based Groups
- Defining VLAN Protocol Based Groups
- Mapping Groups to VLANs

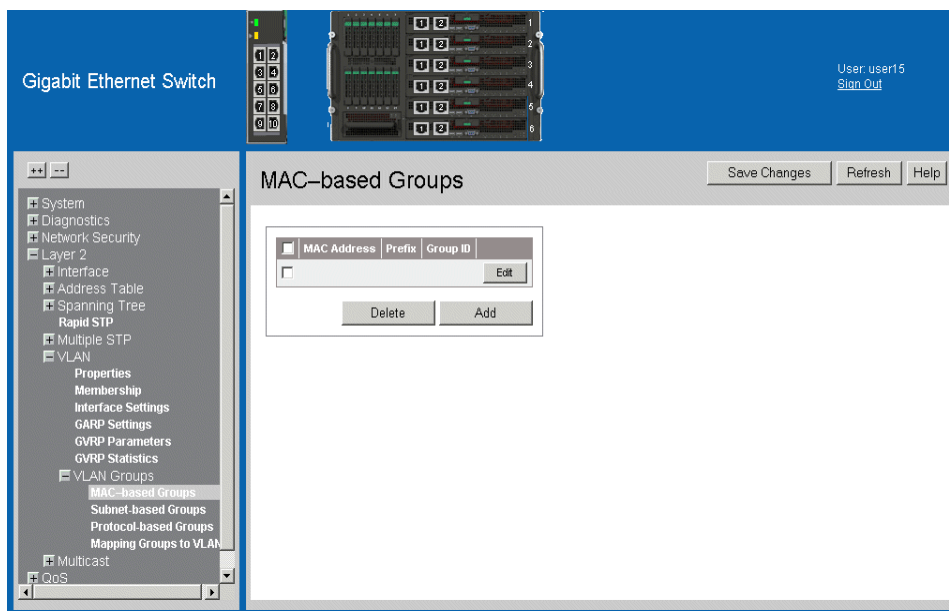
Defining VLAN MAC Based Groups

The *VLAN MAC-based Groups Page* allows network managers to group VLANs based on the VLAN MAC address.

To define VLAN MAC Based Groups:

1. Click **Layer 2 > VLAN > VLAN Groups > MAC-based Groups**. The *VLAN MAC-based Groups Page* opens:

Figure 40. VLAN MAC-based Groups Page

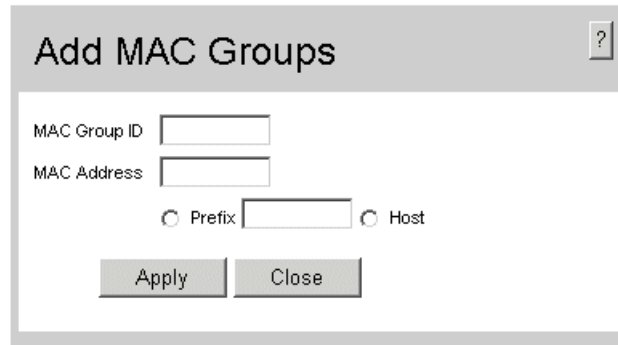


The *VLAN MAC-based Groups Page* contains the following fields:

- **MAC Address** — Displays the MAC address associated with the VLAN group.
- **Prefix** — Displays the MAC prefix associated with the VLAN group.
- **Group ID** — Displays the VLAN Group ID.

2. Click **Add**. The *Add VLAN MAC-based Groups Page* opens:

Figure 41. Add VLAN MAC-based Groups Page

A dialog box titled "Add MAC Groups" with a help icon in the top right corner. It contains three input fields: "MAC Group ID", "MAC Address", and a radio button selection between "Prefix" and "Host". The "Prefix" radio button is selected. Below the fields are "Apply" and "Close" buttons.

MAC Group ID

MAC Address

☒ Prefix ☐ Host

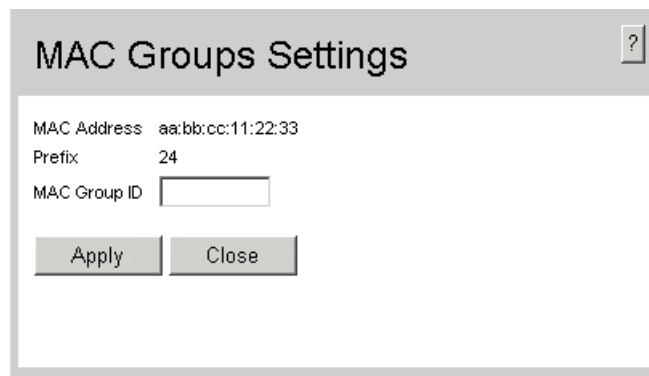
In addition to the fields in the *VLAN MAC-based Groups Page*, the *Add VLAN MAC-based Groups Page* contains the following additional fields:

- **MAC Group ID** — Defines the Group ID associated with the VLAN group.
 - **Prefix** — Defines the MAC prefix associated with the VLAN group.
 - **Host** — Defines the specified MAC address as the only address associated with the VLAN group.
3. Define the fields.
 4. Click . The MAC based VLAN group is defined, and the device is updated.

To modify a MAC Based VLAN Group:

1. Click **Layer 2 > VLAN > VLANS Groups > MAC-based Groups**. The *VLAN MAC-based Groups Page* opens.
2. Click . The *MAC Groups Settings Page* opens:

Figure 42. MAC Groups Settings Page

A dialog box titled "MAC Groups Settings" with a help icon in the top right corner. It displays the current settings: "MAC Address" as "aa:bb:cc:11:22:33", "Prefix" as "24", and "MAC Group ID" in an empty text box. Below the fields are "Apply" and "Close" buttons.

MAC Address aa:bb:cc:11:22:33

Prefix 24

MAC Group ID

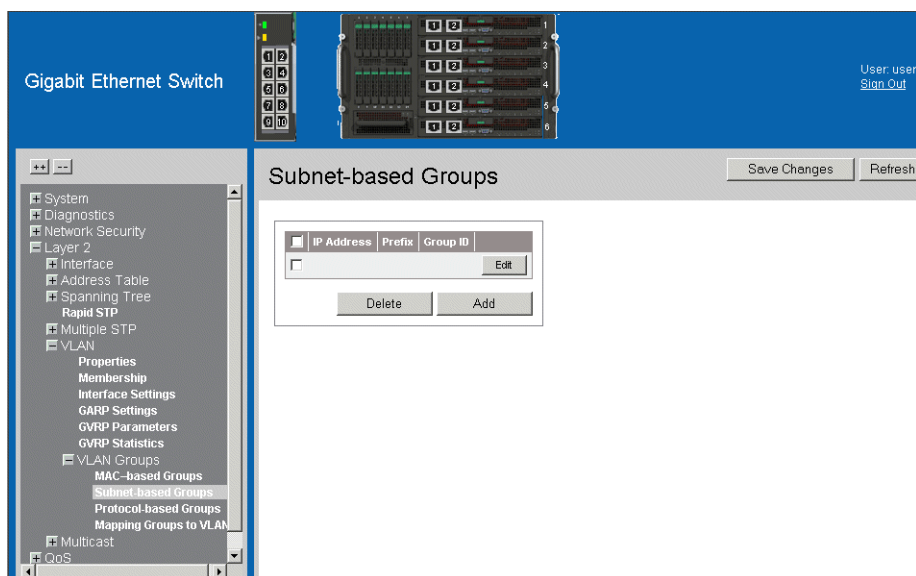
3. Modify the fields.
4. Click . The MAC based VLAN group is modified, and the device is updated.

Defining VLAN Subnet Based Groups

The *Subnet-based Group Settings* allows network managers to group VLANs based on their subnet. To define VLAN Subnet-based Groups:

1. Click **Layer 2 > VLAN > VLAN Groups > Subnet-based Groups**. The *VLAN Subnet-based Groups Page* opens:

Figure 43. VLAN Subnet-based Groups Page

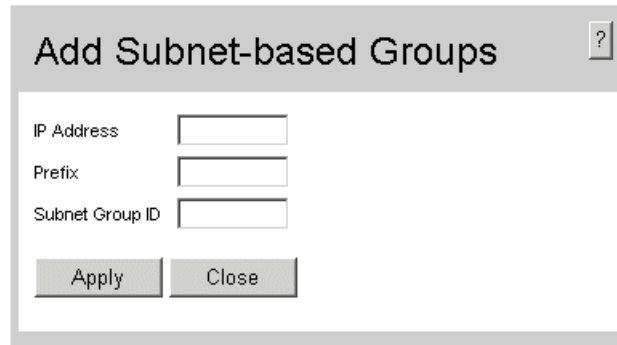


The *VLAN Subnet-based Groups Page* contains the following fields:

- **IP Address** — Displays the IP address associated with the VLAN subnet group.
- **Prefix** — Displays the network prefix associated with the VLAN group.
- **Group ID** — Displays the VLAN group ID associated with the VLAN subnet group.

2. Click **Add**. The *Add VLAN Subnet-based Groups Page* opens:

Figure 44. Add VLAN Subnet-based Groups Page



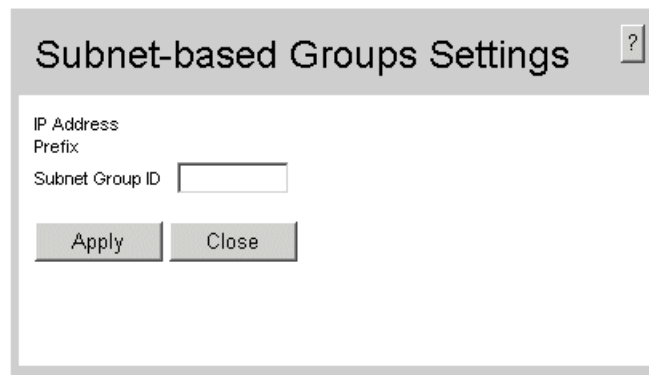
A dialog box titled "Add Subnet-based Groups" with a help icon (?) in the top right corner. It contains three input fields: "IP Address", "Prefix", and "Subnet Group ID". Below the fields are two buttons: "Apply" and "Close".

3. Define the fields.
4. Click **Apply**. The Subnet based VLAN group is defined, and the device is updated.

To modify a Subnet VLAN Group:

1. Click **Layer 2 > > VLAN > VLAN Groups > Subnet-based Groups**. The *VLAN Subnet-based Groups Page* opens.
2. Click **Edit**. The *Subnet-based Group Settings* opens.

Figure 45. Subnet-based Group Settings



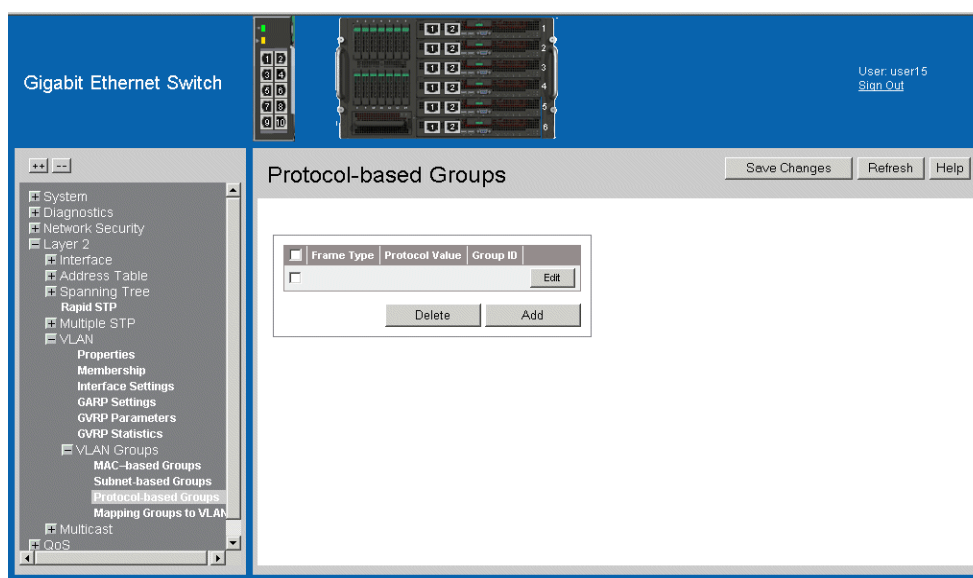
A dialog box titled "Subnet-based Groups Settings" with a help icon (?) in the top right corner. It contains three input fields: "IP Address", "Prefix", and "Subnet Group ID". Below the fields are two buttons: "Apply" and "Close".

Defining VLAN Protocol Based Groups

The *VLAN Protocol Groups Page* contains information regarding protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface. The classification places the interface into a protocol group. To define protocol based VLANs

1. Click **Layer 2 >> VLAN > VLAN Groups > Protocol-based Groups**. The *VLAN Protocol Groups Page* opens:

Figure 46. VLAN Protocol Groups Page



The *VLAN Protocol Groups Page* contains the following fields:

- **Frame Type** — Displays the packet type. Possible field values are **Ethernet**, **RFC1042**, and **LLC Other**.
- **Protocol Value** — Displays the user-defined protocol name.
- **Group ID** — Displays the ID number assigned to frames containing specified protocol value. The possible field range is 1 - 2147483647.

2. Click **Add**. The *Add Protocol-based Groups Page* opens:

Figure 47. Add Protocol-based Groups Page

The screenshot shows a dialog box titled "Add Protocol-based Groups". It contains the following fields and controls:

- Frame Type:** A dropdown menu currently showing "Ethernet".
- Protocol Value:** A radio button that is selected.
- Ethernet-Based Protocol Value:** A radio button that is not selected.
- Protocol Group ID:** A text input field.
- Buttons:** "Apply" and "Close" buttons at the bottom.

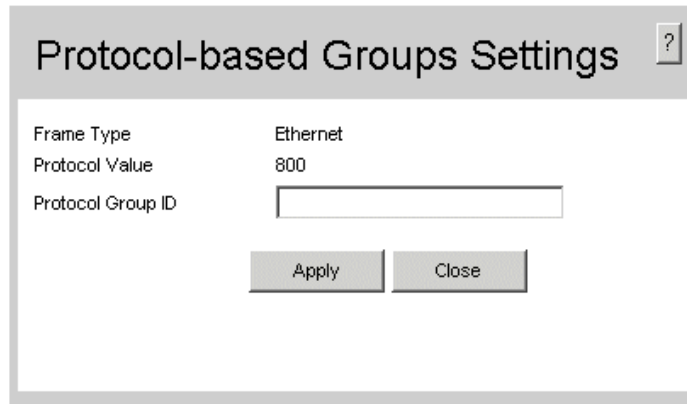
In addition to the fields in the *VLAN Protocol Groups Page*, the *Add Protocol-based Groups Page* contains the following additional fields:

- **Frame Type** — Displays the packet type. Possible field values are **Ethernet**, **RFC1042**, and **LLC Other**.
 - **Protocol Value** — Displays the protocol group type. The possible field values are:
 - *IP* — *IP Internet Protocol* (IP).
 - *IPX* — *Internet Packet Exchange* (IPX).
 - *ARP* — The *Address Resolution Protocol* (ARP) converts IP addresses into physical addresses and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known.
 - **Ethernet-Based Protocol Value** — Displays the Ethernet protocol value.
3. Define the fields.
 4. Click **Apply** . The protocol based VLAN group is defined, and the device is updated.

To Modify a Protocol Based VLAN Group:

1. Click **Layer 2 > VLAN > VLAN Groups > Protocol Based Groups**. The *VLAN Protocol Groups Page* opens.
2. Click **Edit** . The *Protocol-based Groups Settings Page* opens:

Figure 48. Protocol-based Groups Settings Page



The image shows a dialog box titled "Protocol-based Groups Settings" with a help icon (?) in the top right corner. Inside the dialog, there are three labels on the left and their corresponding values or input fields on the right: "Frame Type" with the value "Ethernet", "Protocol Value" with the value "800", and "Protocol Group ID" with an empty text input field. At the bottom of the dialog, there are two buttons: "Apply" and "Close".

Frame Type	Ethernet
Protocol Value	800
Protocol Group ID	

Apply Close

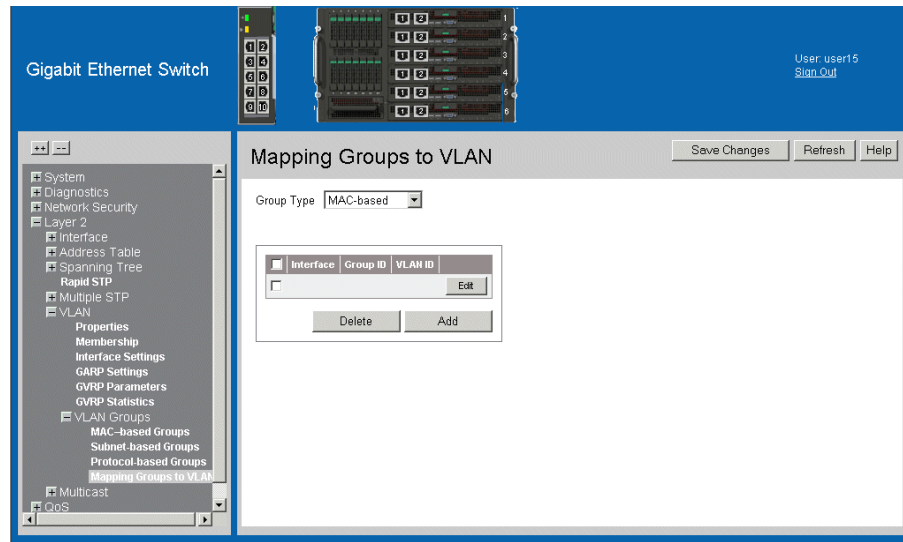
3. Modify the fields.
4. Click **Apply** . The protocol based VLAN group is defined, and the device is updated. au

Mapping Groups to VLANs

The *Mapping Groups to VLAN Page* allows network managers to assign specific interfaces to specific VLAN groups. To map interfaces to VLAN groups:

1. Click **Layer 2 > VLANS > VLAN Groups > Mapping Groups to VLAN**. The *Mapping Groups to VLAN Page* opens:

Figure 49. Mapping Groups to VLAN Page

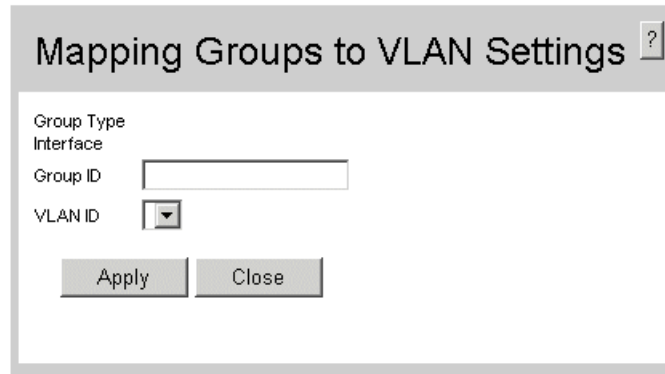


The *Mapping Groups to VLAN Page* contains the following fields:

- **Group Type** — Displays the VLAN Group type to which the interface is attached. The possible field values are:
 - *MAC-based* — Indicates the interface is attached to a MAC based VLAN group.
 - *Subnet-based* — Indicates the interface is attached to a Subnet based VLAN group.
 - *Protocol-based* — Indicates the interface is attached to a Protocol based VLAN group.
- **Interface** — Displays the interface attached to the VLAN group.
- **Group ID** — Displays the VLAN Group ID.
- **VLAN ID** — Displays the VLAN ID.

2. Click **Add**. The *Mapping Groups to VLAN Settings Page Mapping Groups to VLAN Settings Page* opens:

Figure 50. Mapping Groups to VLAN Settings Page



Mapping Groups to VLAN Settings ?

Group Type
Interface
Group ID
VLAN ID

3. Modify the fields.
4. Click **Apply**. The interfaces mappings are modified, and the device is updated.

Configuring GARP

This section contains information for configuring *Generic Attribute Registration Protocol* (GARP). This section includes the following topics:

- Defining GARP
- Defining GVRP

Defining GARP

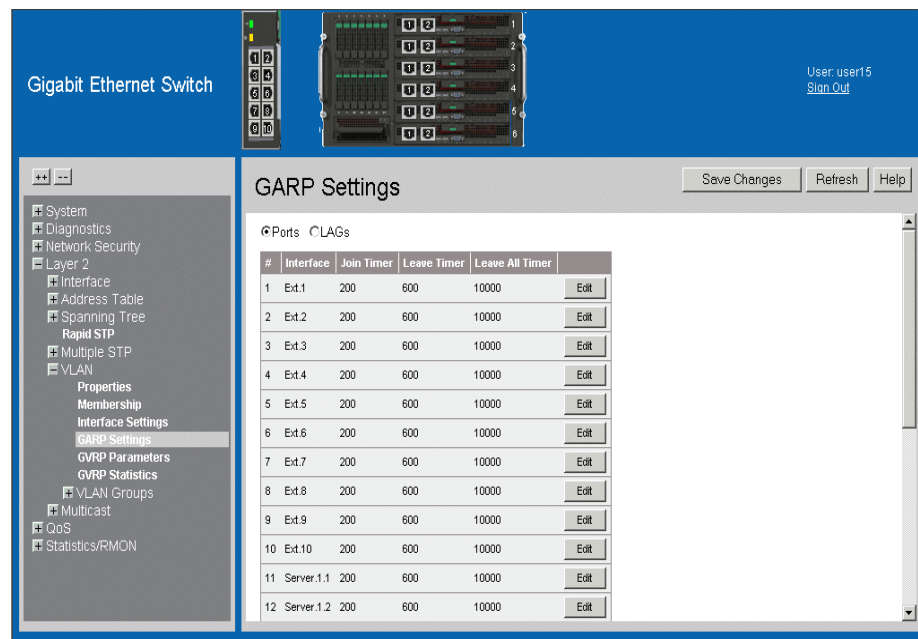
The *Generic Attribute Registration Protocol* (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address. When configuring GARP, ensure the following:

- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, the GARP application does not operate successfully.

To define the GARP settings on the device:

1. Click **Layer 2 > VLAN > GARP Settings**. The *GARP Settings Page* opens:

Figure 51. GARP Settings Page



The *GARP Settings Page* contains the following fields:

- **Ports** — Displays the Port GARP settings.
- **LAGs** — Displays the LAG GARP settings.
- **Interface** — Displays the port or LAG on which GARP is enabled.
- **Join Timer** — Indicates the amount of time, in milliseconds, that PDUs are transmitted. The default value is 200 milliseconds.
- **Leave Timer** — Indicates the amount of time lapse, in milliseconds, that the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The default value is 600 milliseconds.
- **Leave All Timer** — Indicates the amount of time lapse, in milliseconds, that all devices waits before leaving the GARP state. The leave all time must be greater than the leave time. The default value is 10,000 milliseconds.

2. Click **Edit**. The *GARP Parameters Settings Page* opens:

Figure 52. GARP Parameters Settings Page

GARP Parameters Settings

Interface ☒ Port Ext.1 ☐ LAG LAG1

GARP Timers

Join Timer 200 (msec)

Leave Timer 600 (msec)

Leave All Timer 10000 (msec)

Apply Close

3. Define the relevant fields.
4. Click **Apply**. The GARP parameters are defined, and the device is updated.

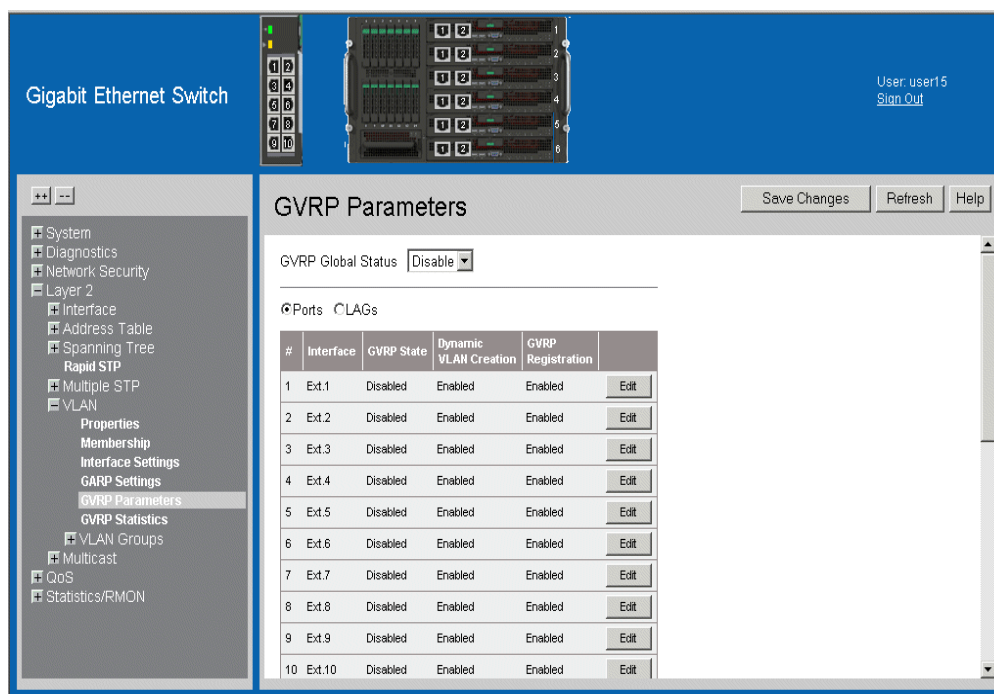
Defining GVRP

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

To define the GVRP parameters on the device:

1. Click **Layer 2 > VLAN > GVRP Parameters**. The *GVRP Parameters Page* opens:

Figure 53. GVRP Parameters Page



The *GVRP Parameters Page* is divided into Port and LAG parameters. The field definitions are the same. The *GVRP Parameters Page* contains the following fields:

- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
 - *Enable* — Enables GVRP on the device.
 - *Disable* — Disables GVRP on the device.
- **Ports** — Displays the Port GVRP settings.
- **LAGs** — Displays the LAG GVRP settings.
- **Interface** — Displays the port or LAG on which GVRP is enabled.

- **GVRP State** — Indicates if GVRP is enabled on the interface. The possible field values are:
 - *Enable* — Enables GVRP on the selected interface.
 - *Disable* — Disables GVRP on the selected interface.
 - **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
 - *Enable* — Enables Dynamic VLAN creation on the interface.
 - *Disable* — Disables Dynamic VLAN creation on the interface.
 - **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the interface. The possible field values are:
 - *Enable* — Enables GVRP registration on the interface.
 - *Disable* — Disables GVRP registration on the interface.
2. Define the relevant fields.
 3. Click **Apply** . The GVRP parameters are defined, and the device is updated.

To modify the GVRP parameters:

1. Click **Edit** . The *GVRP Parameters Settings Page* opens:

Figure 54. GVRP Parameters Settings Page

The screenshot shows a window titled "GVRP Parameters Settings". Inside the window, there are four rows of configuration options:

- Interface:** Two radio buttons are present. The first is labeled "Port" and is selected (indicated by a filled circle). Next to it is a dropdown menu showing "Ext.1". The second radio button is labeled "LAG" and is not selected. Next to it is a dropdown menu showing "LAG1".
- GVRP State:** A dropdown menu is shown with "Disable" selected.
- Dynamic VLAN Creation:** A dropdown menu is shown with "Enable" selected.
- GVRP Registration:** A dropdown menu is shown with "Enable" selected.

At the bottom of the window, there are two buttons: "Apply" and "Close".

2. Define the relevant fields.
3. Click **Apply** . The GVRP Interface parameters are sent, and the device is updated.

7 Defining Forwarding Database

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The Dynamic MAC Address Table can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

An address becomes associated with a port by learning the port from the frame's source address, but if a frame that is addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

This section contains information for defining both static and dynamic forwarding database entries, and includes the following topics:

- Defining Static Forwarding Database Entries
- Defining Dynamic Forwarding Database Entries

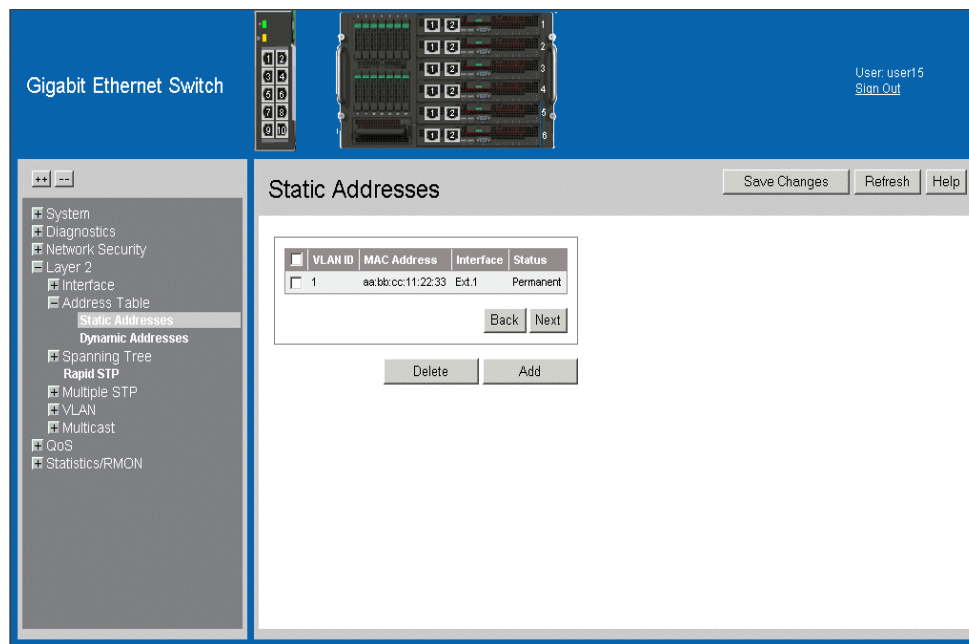
Defining Static Forwarding Database Entries

The *Static Addresses Page* contains parameters for defining the age interval on the device. To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked.

To configure the static forwarding database:

1. Click **Layer 2 > Address Table > Static Addresses**. The *Static Addresses Page* opens.

Figure 55. Static Addresses Page



The *Static Addresses Page* contains the following fields:

- **Delete** — Deletes the entry. The possible field values are:
 - *Checked* — Deletes the selected entry.
 - *Unchecked* — Maintains the current static forwarding database.
- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
 - *Port* — The specific port number to which the forwarding database parameters refer.
 - *LAG* — The specific LAG number to which the forwarding database parameters refer.

- **Status** — Displays how the entry was created. The possible field values are:
 - *Permanent* — The MAC address is permanent.
 - *Delete on Reset* — The MAC address is deleted when the device is reset.
 - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
 - *Secure* — The MAC Address is defined for locked ports.

Note: To prevent static MAC addresses from being deleted when the device is reset, make sure that the port attached to the MAC address is locked.

2. Click **Add**. The *Add Static MAC Address Page* opens:

Figure 56. Add Static MAC Address Page

In addition to the fields in the *Static Addresses Page*, the *Add Static MAC Address Page* contains the following additional field:

- **VLAN Name** — Displays the user-defined VLAN name.

3. Define the relevant fields.
4. Click **Apply**. The Static MAC Addresses are defined, and the device is updated.

Defining Dynamic Forwarding Database Entries

The *Dynamic Addresses Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN and MAC Address.

To configure the Dynamic MAC Address table:

1. Click **Layer 2 > Address Table > Dynamic Addresses**. The *Dynamic Addresses Page* opens.

Figure 57. Dynamic Addresses Page

The screenshot shows the 'Dynamic Addresses' configuration page for a Gigabit Ethernet Switch. The left sidebar contains a navigation tree with options like System, Diagnostics, Network Security, Layer 2, Interface, Address Table, Static Addresses, Dynamic Addresses (selected), Spanning Tree, Rapid STP, Multiple STP, VLAN, Multicast, QoS, and Statistics/RMON. The main content area has a 'Dynamic Addresses' title with 'Save Changes', 'Refresh', and 'Help' buttons. Below the title are fields for 'Aging Interval' (set to 300 Sec), 'Clear Table' (checkbox), and 'Query by' options (Interface, Port, MAC Address, VLAN ID). The 'Address Table Sort Key' is set to 'VLAN'. A 'Query' button is located below the query options. At the bottom, a table displays the current Dynamic MAC Address Table entries.

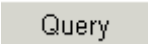
#	VLAN ID	MAC	Interface
1	VLAN 1	000000145412	Ext.1
2	VLAN 1	0000b012800	Ext.2
3	VLAN 1	00010308e947	Ext.3
4	VLAN 1	0001030e8110	Ext.4

The *Dynamic Addresses Page* contains the following fields:

- **Aging Interval (Sec)** — Specifies the amount of time the MAC Address remains in the Dynamic Address Table before it times out. The default value is 300 seconds.
- **Clear Table** — Clears the current Address Table entries.
- **Query by:** — Sorts the addresses table by:
 - *Interface* — Displays the interface to for which the dynamic address is defined.
 - *MAC Address* — Specifies the MAC address for which the table is queried.
 - *VLAN ID* — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** — Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by MAC address, VLAN or interface.

2. Define the fields.
3. Click . The *Dynamic Address Aging* field is defined, and the device is updated.

To query the Dynamic MAC Address Table:

1. Click **Layer 2 > Address Table > Dynamic Addresses**. *The Dynamic Addresses Page* opens.
2. Select an *Address Table Sort Key*.
3. Click . The Dynamic MAC Address Table is queried, and the results are displayed.

8 Configuring Multicast Forwarding

This section contains information for configuring Multicast forwarding, and includes the following sections:

- Defining IGMP Snooping
- Defining Multicast Groups
- Defining Multicast Forward All Settings

Defining IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.

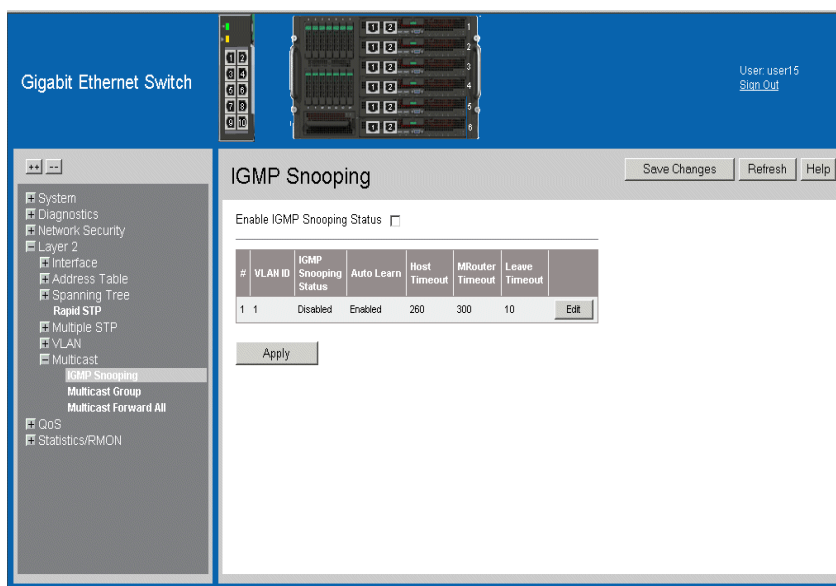
Hosts on ports join a specific Multicast group by sending an IGMP report, learned by the bridge. This results in the creation of the Multicast filtering database.

Note: Ensure that Bridge Multicast filtering is enabled before enabling IGMP Snooping (see *Defining Multicast Groups*).

To enable IGMP Snooping:

1. Click **Layer 2 > Multicast > IGMP Snooping**. The *IGMP Snooping Page* opens:

Figure 58. IGMP Snooping Page



The *IGMP Snooping Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
 - *Checked* — Enables IGMP Snooping on the device.
 - *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.

- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
 - *Enable* — Enables IGMP Snooping on the VLAN.
 - *Disable* — Disables IGMP Snooping on the VLAN.
 - **Auto Learn** — Indicates if Auto Learn is enabled on the VLAN. If Auto Learn is enabled, the device automatically learns about the existing multicast routers. The possible field values are:
 - *Enable* — Enables auto learn.
 - *Disable* — Disables auto learn.
 - **Host Timeout** — Indicates the amount of time the host waits to receive a message before timing out. If an IGMP report for a multicast group wasn't received on the port from any host (located on the port), the port is deleted from the membership list of that group. The default time is 260 seconds.
 - **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. If any MRouter message (IGMP query or any other multicast router message), wasn't received on the port, the port is deleted from the MRouter membership port list. The default value is 300 seconds.
 - **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.
2. Check the *Enable IGMP Snooping Status* checkbox.
 3. Click **Edit** . The *IGMP Snooping Settings Page* opens:

Figure 59. IGMP Snooping Settings Page

The screenshot shows the 'IGMP Snooping Settings' dialog box. It contains the following fields and controls:

- VLAN ID:** A dropdown menu currently showing '1'.
- IGMP Status Enable:** A dropdown menu currently showing 'Disable'.
- Auto-Learn:** A dropdown menu currently showing 'Enable'.
- Host Timeout:** A text input field containing the value '260'.
- MRouter Timeout:** A text input field containing the value '300'.
- Leave Timeout:** A section with two options: a selected radio button next to '10' and an unselected radio button next to 'Immediate Leave'.
- Buttons:** 'Apply' and 'Close' buttons at the bottom.

4. Modify the relevant fields.
5. Click **Apply** . The IGMP global parameters are sent, and the device is updated.

Defining Multicast Groups

The *Multicast Group Page* displays the ports and LAGs attached to the Multicast service group in the Ports and LAGs tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports and LAGs can be added either to existing groups or to new Multicast service groups. The *Multicast Group Page* permits new Multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific Multicast service address group.

Bridge multicast groups are defined according to MAC addresses. In cases where the Bridge Multicast Address is an IP Address it is required to be mapped to a MAC address. Multiple IP address can be mapped to a single MAC address and are presented in the form of an IP Address range (see *Edit Multicast Group Page*). The MAC address for the multicast group is created as a result of mapping the last 23 bits of the IP Address to the Last 23 bits of the MAC address and this allows multiple IP addresses to be mapped to one MAC address. The first three octets of such a mapped MAC address have the standard form of **01:00:5E:XX:XX:XX**.

To define multicast groups:

1. Click **Layer 2 > Multicast > Multicast Group**. The *Multicast Group Page* opens:

Figure 60. Multicast Group Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

Multicast Group [Save Changes] [Refresh] [Help]

Enable Bridge Multicast Filtering ☐

VLAN ID: 1

Bridge Multicast Address: 01005e010101

[Delete] [Add]

☒ Ports ☐ LAGs

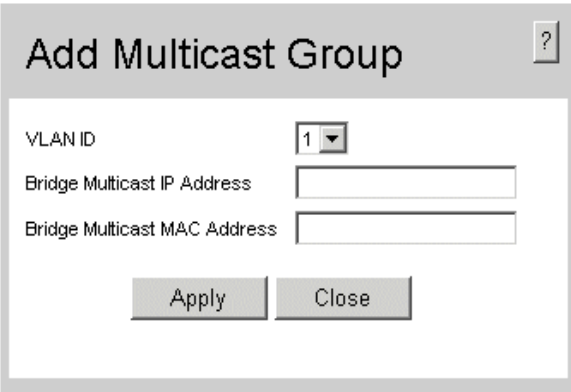
#	Interface	Interface Status	
1	Ext.1	Exclude	[Edit]
2	Ext.2	Forbidden	[Edit]
3	Ext.3	Exclude	[Edit]
4	Ext.4	Exclude	[Edit]
5	Ext.5	Exclude	[Edit]
6	Ext.6	Exclude	[Edit]

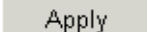
The *Multicast Group Page* contains the following fields:

- **Enable Bridge Multicast Filtering** — Indicate if bridge Multicast filtering is enabled on the device. The possible field values are:
 - *Checked* — Enables multicast filtering on the device.
 - *Unchecked* — Disables multicast filtering on the device. If multicast filtering is disabled, multicast frames are flooded to all ports in the relevant VLAN. Disabled is the default value.
- **VLAN ID** — Identifies a VLAN and contains information about the multicast group address.
- **Bridge Multicast Address** — Identifies the multicast group MAC address/IP address.
- **Ports** — Displays port that can be added to a multicast service.
- **LAGs** — Displays LAGs that can be added to a multicast service.
- **Interface** — Displays the interface used to manage the device.
- **Interface Status** — Indicates the port/LAG status in relation to the Multicast group.
 - *Static* — Attaches the port/LAG to the Multicast group as static member.
 - *Dynamic* — Dynamically joins the port/LAG to the multicast group in the Current Row.
 - *Forbidden* — Indicates the port/LAG is not included in the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
 - *Exclude* — Indicates the port/LAG is not part of a Multicast group.

2. Click . The *Add Multicast Group Page* opens:

Figure 61. Add Multicast Group Page

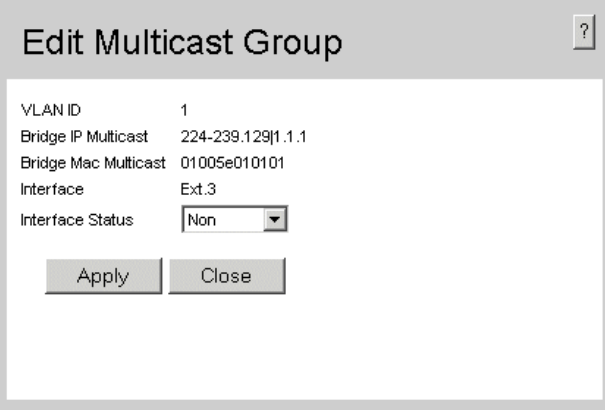


3. Define the relevant fields.
4. Click . The Multicast group is defined, and the device is updated.

To modify the multicast group:

1. Click **Edit**. The *Edit Multicast Group Page* opens:

Figure 62. Edit Multicast Group Page



VLAN ID	1
Bridge IP Multicast	224-239.129 1.1.1
Bridge Mac Multicast	01005e010101
Interface	Ext.3
Interface Status	Non

Apply Close

2. Modify the relevant fields.
3. Click **Apply**. The Multicast group is defined, and the device is updated.

Defining Multicast Forward All Settings

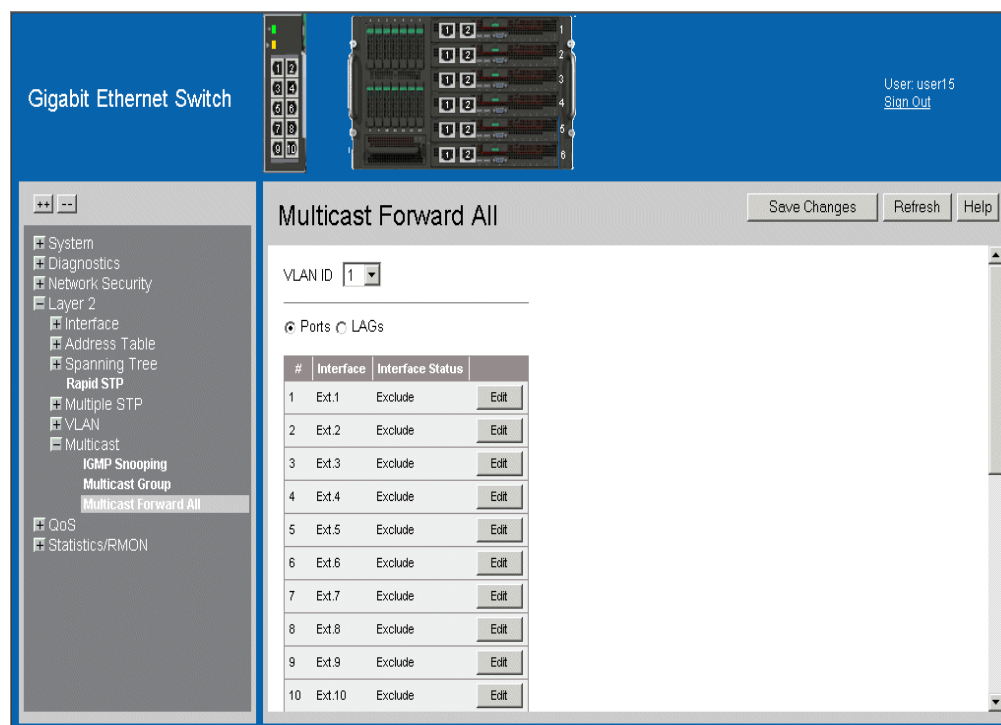
The *Multicast Forward-ALL Page* allows users to define the ports which are filtered by the IGMP snooping protocol. The IGMP Snooping protocol filters ports during the forwarding process to a neighboring Multicast router or switch. Ports can either be defined as:

- *Forbidden* — Excluded from *IGMP Learned Port List*.
- *Forwarded* — Added to the *IGMP Learned Port List*. The IGMP snooping interprets *Forward* (static) ports as statically configured Multicast ports that propagates IGMP reports and data. The *Forward* also adds the *Multicast Group Forward (static)* ports to the *Forward-All Forward (static)* ports list.

To define multicast forward all settings:

1. Click **Layer 2 > Multicast > Multicast Forward All**. The *Multicast Forward All Page* opens:

Figure 63. Multicast Forward All Page



The *Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN for which multicast parameters are displayed.
- **Ports** — Displays port that can be added to a multicast service.
- **LAGs** — Displays LAGs that can be added to a multicast service.

- **Interface** — Displays the interface used to manage the device.
- **Interface Status** — Indicates the port/LAG status. The possible field values are:
 - *Static* — Attaches the port/LAG to the Multicast group as static member.
 - *Dynamic* — Dynamically joins ports/LAG to the multicast group in the Current Row.
 - *Forbidden* — Indicates the port/LAG is not included in the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
- 2. *Exclude* — Indicates the port/LAG is not part of a Multicast group. Select a VLAN in the *VLAN ID* drop-down box.
- 3. Define the VLAN port settings.
- 4. Click **Apply** . The Multicast Forward All settings are defined, and the device is updated.

To modify the Multicast Forward All settings:

1. Click **Edit** . The *Multicast Forward All Page* opens:

Figure 64. Edit Multicast Forward All Page

The screenshot shows a window titled "Edit Multicast Forward All". Inside the window, there are three fields: "VLAN ID" set to "1", "Interface" set to "Ext.6", and "Interface Status" set to "Excluded" (with a dropdown arrow). At the bottom of the window, there are two buttons: "Apply" and "Close".

2. Define the relevant fields.
3. Click **Apply** . The Multicast Forward All settings are defined, and the device is updated.

9 Configuring Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides a single path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following STP versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. *Defining Spanning Tree*
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops. For more information on configuring Rapid STP, see *Defining Rapid STP*.
- **Multiple STP** — Provides various load balancing scenarios. For example, if port A is blocked in one STP instance, the same port can be placed in the *Forwarding State* in another STP instance. For more information on configuring Multiple STP, see *Defining Multiple STP*.

Defining Spanning Tree

The *Spanning Tree Properties Page* contains parameters for enabling STP on the device.

To enable STP on the device:

1. Click **Layer 2 > Spanning Tree > Properties**. The *Spanning Tree Properties Page* opens:

Figure 65. Spanning Tree Properties Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

Properties

Save Changes Refresh Help

Global Settings

Spanning Tree State:

STP Operation Mode:

BPDU Handling:

Path Cost Default Values:

Bridge Settings

Priority:

☐ Hello Time: (Sec)

☐ Max Age: (Sec)

☐ Forward Delay: (Sec)

Designated Root

Bridge ID: 32768-00:00:00:00:00:00

Root Bridge ID: 32768-00:00:00:00:00:00

Root Port: 0

Root Path Cost: 0

The *Spanning Tree Properties Page* contains the following fields:

Global Settings

- **Spanning Tree State** — Indicates whether STP is enabled on the device. The possible field values are:
 - *Enable* — Enables STP on the device.
 - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Specifies the STP mode that is enabled on the device. The possible field values are:
 - *Classic STP* — Enables Classic STP on the device.
 - *Rapid STP* — Enables Rapid STP on the device. This is the default value.
 - *Multiple STP* — Enables Multiple STP on the device.

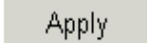
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
 - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface. This is the default value.
 - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface.
- **Path Cost Default Values** — Specifies the method used to assign default path cost to STP ports. The possible field values are:
 - *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
 - *Long* — Specifies 1 through 200,000,000 range for port path cost. The default path cost assigned to an interface varies according to the selected method (*Hello Time*, *Max Age*, or *Forward Delay*).

Bridge Settings

- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The possible field range is 0 - 61440 seconds. The default value is 32768. The bridge priority value is provided in increments of 4096.
- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root Bridge waits between configuration messages. The possible field range is 1-10 seconds. The default is 2 seconds.
- **Max Age** — Specifies the device Maximum Age Time. The Maximum Age Time is the amount of time in seconds a bridge waits before sending configuration messages. The possible field range is 6 - 40 seconds. The default Maximum Age Time is 20 seconds.
- **Forward Delay** — Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The possible field range is 4 -30. The default is 15 seconds.

Designated Root

- **Bridge ID** — Identifies the Bridge priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. This field is significant when the bridge is not the Root Bridge. The default is zero.
- **Root Path Cost** — Specifies the cost of the path from this bridge to the Root Bridge.
- **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change that occurred. The time is displayed in a day-hour-minute-second format, such as 2 days 5 hours 10 minutes and 4 seconds.

2. Define the relevant fields.
3. Click . STP is enabled, and the device is updated.

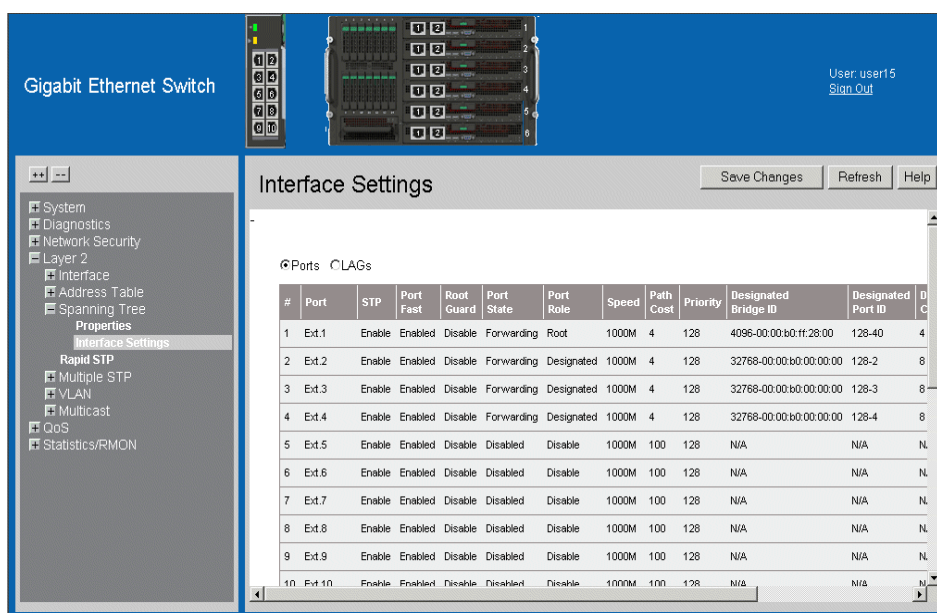
Defining Spanning Tree Interface Settings

Network administrators can assign STP settings to specific interfaces using the *Spanning Tree Interface Settings Page*. The Global LAGs section displays the STP information for Link Aggregated Groups.

To assign STP settings to an interface:

1. Click **Layer 2 > Spanning Tree > Interface Settings**. The *Spanning Tree Interface Settings Page* opens:

Figure 66. Spanning Tree Interface Settings Page



The *Spanning Tree Interface Settings Page* contains the following fields:

- **Ports** — Displays the port on which STP is enabled.
- **LAGs** — Displays the LAG on which STP is enabled.

If *Ports* are selected, the following fields are displayed:

- **Port** — Displays the port for which the information is displayed.
- **LAG** — Displays the LAG for which the information is displayed
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
 - *Enabled* — Indicates that STP is enabled on the port.
 - *Disabled* — Indicates that STP is disabled on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port

link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. The possible field values are:

- *Enabled* — Port Fast is enabled.
- *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
- *Disabled* — Port Fast is disabled.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Forwarding* — Indicates that the port can forward traffic or learn MAC addresses.
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Discarded* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root switch.
 - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
 - *Disable* — The port is not participating in the Spanning Tree.
- **Speed** — Indicates the speed at which the port is operating.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is re-routed.
- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is determined in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

- **Forward Transitions** — Indicates the number of times the port has changed from *Discarding* state to *Forwarding* state.
- **LAG** — Indicates the LAG to which the port belongs.

If *LAGs* are selected, the following fields are displayed:

- **LAG** — Indicates the LAG to which the port belongs.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
 - *Enabled* — Indicates that STP is enabled on the port.
 - *Disabled* — Indicates that STP is disabled on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. The possible field values are:
 - *Enabled* — Port Fast is enabled.
 - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
 - *Disabled* — Port Fast is disabled.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root.
- **State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Forwarding* — Indicates that the port can forward traffic or learn MAC addresses.
 - *Discarding* - Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root switch.
 - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
 - *Disable* — The port is not participating in the Spanning Tree.

- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is re-routed.
- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is determined in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Indicates the number of times the port has changed from *Discarding* state to *Forwarding* state.

2. Click **Edit**. The *Spanning Tree Interface Settings Page* opens:

Figure 67. Spanning Tree Interface Settings Page

The screenshot shows a window titled "Interface Settings" with a help icon in the top right corner. The window contains the following fields and controls:

- Port:** A dropdown menu showing "Ext.1".
- STP:** A dropdown menu showing "Enable".
- Port Fast:** A dropdown menu showing "Enabled".
- Enable Root Guard:** An unchecked checkbox.
- Port State:** A text field showing "Forwarding".
- Speed:** A text field.
- Path Cost:** A text field showing "100".
- Default Path Cost:** An unchecked checkbox.
- Priority:** A text field showing "128".
- Designated Bridge ID:** A text field.
- Designated Port ID:** A text field.
- Designated Cost:** A text field.
- Forward Transitions:** A text field.
- LAG:** A dropdown menu showing "LAG1".
- Buttons:** "Apply" and "Close" buttons at the bottom.

3. Select *Enable* in the *STP* field.
4. Define the relevant fields.
5. Click **Apply**. STP is enabled on the interface, and the device is updated.

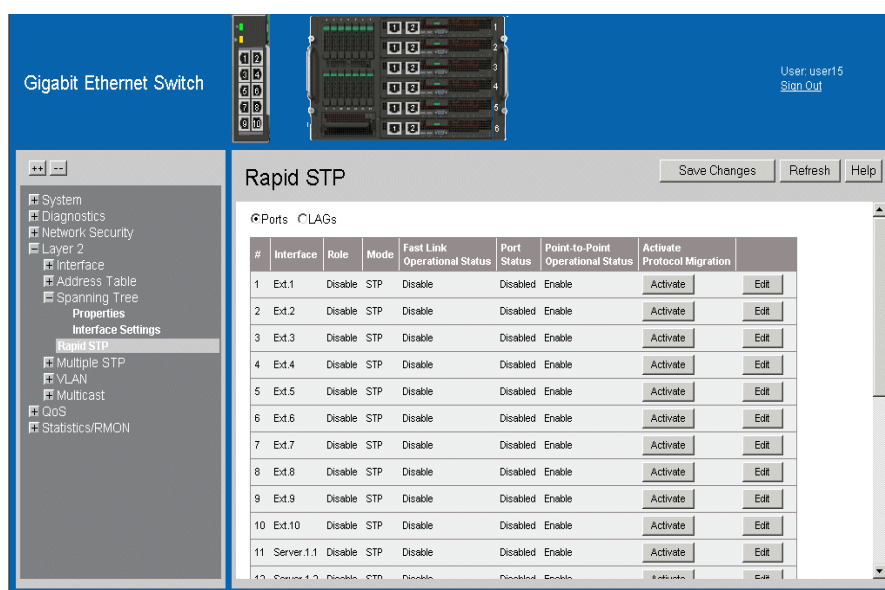
Defining Rapid STP

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. *Rapid Spanning Tree Protocol* (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops. The Global System LAG information displays the same field information as the ports, but represents the LAG RSTP information.

To define Rapid STP on the device:

1. Click **Layer 2 > Spanning Tree > Rapid STP**. The *Rapid STP Page* opens:

Figure 68. Rapid STP Page



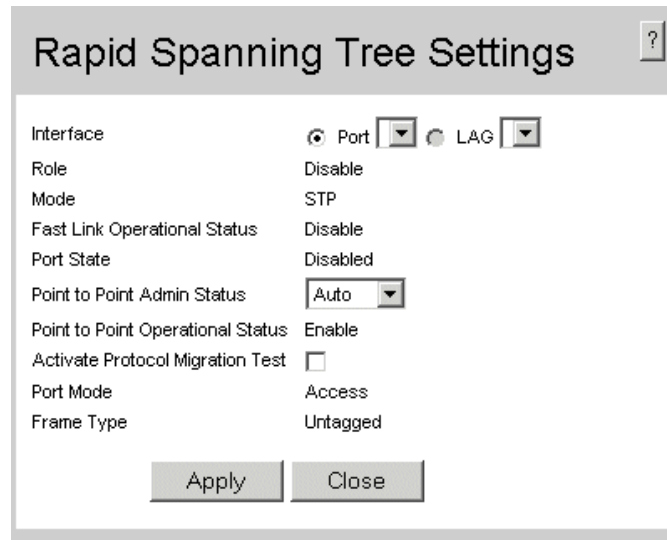
The *Rapid STP Page* contains the following fields:

- **Ports** — Displays the port on which RSTP is enabled.
- **LAGs** — Indicates the LAG to which the port belongs.
- **Interface** — Displays the port or LAG for which the information is displayed.

- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root switch.
 - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — The port is not participating in the Spanning Tree.
- **Mode**—Displays the current STP mode. The STP mode is selected in the *Rapid STP Page*. The possible field values are:
 - *STP* — Classic STP is enabled on the device.
 - *Rapid STP* — Rapid STP is enabled on the device.
 - *Multiple STP* — Multiple STP is enabled on the device.
- **Fast Link Operational Status** — Indicates whether Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Port Status** — Displays the current RSTP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Forwarding* — Indicates that the port can forward traffic or learn MAC addresses.
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Discarding* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses
- **Point-to-Point Operational Status** — Displays the point-to-point operating state.
- **Activate Protocol Migration** — Indicates whether sending Link Control Protocol (LCP) packets to configure and test the data link is enabled.

2. Click **Edit** . The *Rapid Spanning Tree Settings Page* opens:

Figure 69. Rapid Spanning Tree Settings Page



The image shows a dialog box titled "Rapid Spanning Tree Settings" with a help icon (?) in the top right corner. The dialog contains a list of configuration options for a network interface. The options are arranged in two columns. The first column lists the settings, and the second column shows the current values. At the bottom of the dialog are two buttons: "Apply" and "Close".

Setting	Value
Interface	☒ Port ☐ LAG
Role	Disable
Mode	STP
Fast Link Operational Status	Disable
Port State	Disabled
Point to Point Admin Status	Auto
Point to Point Operational Status	Enable
Activate Protocol Migration Test	☐
Port Mode	Access
Frame Type	Untagged

3. Define the relevant fields.
4. Click **Apply** . Rapid STP is defined for the interface, and the device is updated.

Defining Multiple STP

Multiple Spanning Tree (MSTP) provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the *Forwarding* state in another STP instance. The *Multiple STP Properties Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

To define MSTP:

1. Click **Layer 2 > Multiple STP > Properties**. The *Multiple STP Properties Page* opens:

Figure 70. Multiple STP Properties Page

The screenshot shows the web interface of a Gigabit Ethernet Switch. The top header is blue with the text 'Gigabit Ethernet Switch' on the left and 'User: user15 Sign Out' on the right. Below the header is a navigation tree on the left with categories like System, Diagnostics, Network Security, Layer 2, and Layer 3. Under Layer 2, 'Multiple STP' is expanded, showing 'Properties' as the selected option. The main content area is titled 'Properties' and contains four input fields: 'Region Name' (00:00:b0:00:00:00), 'Revision' (0), 'Max Hops' (20), and 'IST Master' (32768-00:00:b0:00:00:00). There are 'Save Changes', 'Refresh', and 'Help' buttons at the top right of the form, and an 'Apply' button at the bottom.

The *Multiple STP Properties Page* contains the following fields:

- **Region Name** — User-defined STP region name.
 - **Revision** — An unsigned 16-bit number that identifies the revision of the current MSTP configuration. The revision number is required as part of the MSTP configuration. The possible field range is 0-65535.
 - **Max Hops** — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.
 - **IST Master** — Identifies the Spanning Tree Master instance. The IST Master is the specified instance root. The IST Master identifies the Bridge priority and the MAC address.
2. Define the relevant fields.
 3. Click **Apply**. The Multiple STP properties are defined, and the device is updated.

Defining Multiple STP Instance To VLAN Settings

The *Instance To VLAN Settings Page* enables mapping VLANs to MSTP Instances. Network administrators can define the Multiple STP Instance To VLAN settings using the *Instance To VLAN Settings Page*.

To define the instance to VLAN settings:

1. Click **Layer 2 > Multiple STP > Instance To VLAN Settings**. The *Instance To VLAN Settings Page* opens:

Figure 71. Instance To VLAN Settings Page

The screenshot displays the 'Instance To VLAN' configuration page. On the left is a sidebar with a tree view containing: System, Diagnostics, Network Security, Layer 2 (expanded), Interface, Address Table, Spanning Tree, Rapid STP, Multiple STP (expanded), Properties, Instance To VLAN (selected), Instance Settings, Interface Settings, VLAN, Multicast, QoS, and Statistics/RMON. The top header shows 'Gigabit Ethernet Switch' and a user profile 'User: user15' with a 'Sign Out' link. The main area is titled 'Instance To VLAN' and contains three tables, each with 'VLAN' and 'Instance ID (0-7)' columns. The first table lists VLAN0-VLAN7, the second lists VLAN8-VLAN17, and the third lists VLAN18-VLAN24. Each 'Instance ID' cell contains a dropdown menu. At the bottom right are 'Back' and 'Next' buttons. At the bottom center is an 'Apply' button. At the top right of the main area are 'Save Changes', 'Refresh', and 'Help' buttons.

The *Instance To VLAN Settings Page* contains the following fields:

- **VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
 - **Instance ID (0-7)** — Specifies the VLAN group to which the interface is assigned.
2. Define the relevant fields.
 3. Click **Apply**. The *Instance To VLAN Settings Page* is defined, and the device is updated.

Defining Multiple STP Instance Settings

Multiple STP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring Multiple STP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

Network administrators can define the Multiple STP instance settings using the *Instance Settings Page*.

To define the Instance settings:

1. Click **Layer 2 > Multiple STP > Instance Settings**. The *Instance Settings Page* opens:

Figure 72. Instance Settings Page

The screenshot shows the 'Instance Settings' page for a Gigabit Ethernet Switch. The page has a blue header with the switch name 'Gigabit Ethernet Switch' and a user status 'User: user15 Sign Out'. A navigation tree on the left includes System, Diagnostics, Network Security, Layer 2 (with sub-items Interface, Address Table, Spanning Tree, Rapid STP, Multiple STP, Properties, Instance To VLAN, Instance Settings, and Interface Settings), VLAN, Multicast, QoS, and Statistics/RMON. The 'Instance Settings' page contains fields for Instance ID (a dropdown menu showing '1'), Included VLAN (a list box), Bridge Priority (a text box with '32768'), Designated Root Bridge ID (32768-00:00:b0:00:00:00), Root Port (0), Root Path Cost (0), Bridge ID (32768-00:00:b0:00:00:00), and Remaining Hops (20). Buttons for 'Save Changes', 'Refresh', 'Help', and 'Apply' are present.

The *Instance Settings Page* contains the following fields:

- **Instance ID** — Specifies the VLAN group to which the interface is assigned.
- **Included VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440. The default value is 32768. The bridge priority value is determined in increments of 4096.

- **Designated Root Bridge ID** — Indicates the ID of the bridge with the lowest path cost to the instance ID.
 - **Root Port** — Indicates the selected instance's root port.
 - **Root Path Cost** — Indicates the selected instance's path cost.
 - **Bridge ID** — Indicates the bridge ID of the selected instance.
 - **Remaining Hops** — Indicates the number of hops remaining to the next destination.
2. Define the relevant fields.
 3. Click . The *Instance Settings Page* is defined, and the device is updated.

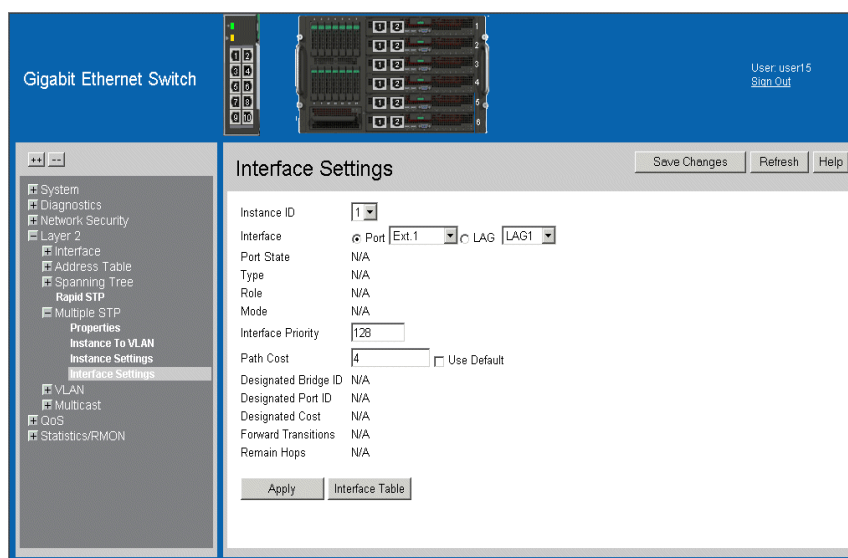
Defining Multiple STP Interface Settings

Network Administrators can assign Multiple STP Interface Settings in the *Interface Settings Page*.

To define Interface settings:

1. Click **Layer 2 > Multiple STP > Interface Settings**. The *Interface Settings Page* opens:

Figure 73. Interface Settings Page



The *Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-7.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
 - *Port* — Specifies the port for which the MSTP settings are displayed.
 - *LAG* — Specifies the LAG for which the MSTP settings are displayed.
- **Port State** — Indicates whether the port is enabled for the specific instance. The possible field values are:
 - *Enabled* — Enables the port for the specific instance.
 - *Disabled* — Disables the port for the specific instance.
- **Type** — Indicates whether the port is a Boundary, Master or an internal port. The possible field values are:
 - *Boundary Port* — Indicates that the port is a Boundary port. A Boundary port attaches MST bridges to LANs in an outlying region. If the port is a Boundary

port, this field also indicates whether the device on the other side of the link is working in RSTP or STP mode

- *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
- *Internal Port* — Indicates the port is within the same MSTP region.
- **Role** — Indicates the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root device.
 - *Designated* — Indicates the port or LAG through which the designated device is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root device from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link or when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the STP mode by which STP is enabled on the device. The possible field values are:
 - *Classic STP* — Classic STP is enabled on the device.
 - *Rapid STP* — Rapid STP is enabled on the device. This is the default value.
 - *Multiple STP* — Multiple STP is enabled on the device.
- **Interface Priority** — Defines the interface priority for the specified instance. The default value is 128. Priority should be defined between 0 and 240 in steps of 16.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000. The default value is 4.
- **Designated Bridge ID** — Displays the ID of the bridge that connects the link or shared LAN to the root.
- **Designated Port ID** — Displays the ID of the port on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Forward Transitions** — Indicates the number of times the port or LAG has been changed from a *Forwarding* state to a *Discarding* state.
- **Remain Hops** — Indicates the hops remaining to the next destination.

- Click **Interface Table**. The *Interface Table Page* opens.

Figure 74. Interface Table Page

Interface Table ?											
Instance 1											
☒ Port ☐ LAG											
#	Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Remain Hops
1	Ext.1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
2	Ext.2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
3	Ext.3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
4	Ext.4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
5	Ext.5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
6	Ext.6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
7	Ext.7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
8	Ext.8	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
9	Ext.9	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
10	Ext.10	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
11	Server.1.1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
12	Server.1.2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
13	Server.2.1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
14	Server.2.2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
15	Server.3.1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
16	Server.3.2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
17	Server.4.1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A

- Define the relevant fields.
- Click **Apply**. The *Interface Settings Page* is defined, and the device is updated.

10 Configuring Quality of Service

This section contains information for configuring QoS, and includes the following topics:

- Quality of Service Overview
- Defining General QoS Settings
- Configuring Basic QoS Settings
- Configuring Advanced QoS Settings

Quality of Service Overview

Quality of Service (QoS) provides the ability to implement QoS and priority queuing within a network. For example, certain types of traffic that require minimal delay, such as Voice, Video, and real-time traffic can be assigned a high priority queue, while other traffic can be assigned a lower priority queue. The result is an improved traffic flow for traffic with high demand. QoS is defined by:

- **Classification** — Specifies which packet fields are matched to specific values. All packets matching the user-defined specifications are classified together.
- **Action** — Defines traffic management where packets are forwarded are based on packet information, and packet field values such as *VLAN Priority Tag* (VPT) and *DiffServ Code Point* (DSCP).

VPT Classification Information

VLAN Priority Tags (VPT) are used to classify packets by mapping packets to one of the egress queues. VPT-to-queue assignments are user-definable. Packets arriving untagged are assigned a default VPT value, which is set on a per-port basis. The assigned VPT is used to map the packet to the egress queue.

CoS Services

After packets are assigned to a specific egress queue, CoS services can be assigned to the queue. Egress queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded. Strict Priority (SP) allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications. For example, under SP, voice over IP (VoIP) traffic can be prioritized so that it is forwarded before FTP or e-mail (SMTP) traffic.
- **Weighted Round Robin** — Ensures that a single application does not dominate the device forwarding capacity. Weighted Round Robin (WRR) forwards entire queues in a round robin order. SP queues are serviced before WRR queues. If the traffic flow is minimal, and SP queues do not occupy the whole bandwidth allocated to a port, the WRR queues can share the bandwidth with the SP queues. This ensures that the remaining bandwidth is distributed according to the weight ratio. If WRR is selected, the following weights are assigned to the queues: 1, 2, 4, 8.

Defining General QoS Settings

This section contains information for defining general QoS settings and includes the following topics:

- Configuring CoS General Parameters
- Configure Bandwidth Settings
- Defining Queues

Configuring CoS General Parameters

The *CoS Global Settings Page* contains information for enabling QoS globally and on specific interfaces. After QoS has been configured, the original device QoS default settings can be reassigned to the interface in the *CoS Global Settings Page*.

To enable QoS:

1. Click **QoS > General > CoS**. The *CoS Global Settings Page* opens:

Figure 75. CoS Global Settings Page

#	Interface	Default CoS	Restore Defaults
1	Ext.1	0	☐
2	Ext.2	0	☐
3	Ext.3	0	☐
4	Ext.4	0	☐
5	Ext.5	0	☐
6	Ext.6	0	☐
7	Ext.7	0	☐
8	Ext.8	0	☐
9	Ext.9	0	☐
10	Ext.10	0	☐

The *CoS Global Settings Page* contains the following:

- **QoS Mode** — Determines whether QoS is enabled on the device. The possible values are:
 - *Disable* — Disables QoS on the device.
 - *Basic* — Enables CoS Basic mode on the device.
 - *Advanced* — Enables Advanced CoS mode on the device.
- **Ports** — Displays the ports on which CoS is enabled.
- **LAGs** — Displays the LAGs on which CoS is enabled.
- **Interface** — Displays the interface for which the global QoS parameters are defined.
 - *Port* — Selects the port for which the global QoS parameters are defined.
 - *LAG* — Selects the LAG for which the global QoS parameters are defined.
- **Default CoS** — Determines the default CoS value for incoming packets for which a VLAN priority is not defined. The possible field values are **0-7**. The default CoS is **0**.

- **Restore Defaults** — Restores the QoS Interface factory defaults.
2. Define the relevant fields.
 3. Click **Apply** . *Quality of Service* is enabled on the device.

To modify the QoS:

1. Click **Edit** . The *Modify Port Priority Page* opens:

Figure 76. Modify Port Priority Page

In addition to the fields in the *CoS Global Settings Page*, the *Modify Port Priority Page* contains the following field:

- **Set Default User Priority** — Sets the default user priority. The possible field values are 0-7. The default CoS value is 0. With the default settings, 0 is the lowest and 7 is the highest priority.
2. Modify the relevant fields.
 3. Click **Apply** . The *Port Priority* settings are saved to interface, and the device is updated.

Restoring Factory Default QoS Interface Settings

1. Click **QoS > General > CoS**. The *CoS Global Settings Page* opens.
2. Check the Restore Defaults checkbox next to the corresponding Interface.
3. Click **Apply** . The factory defaults are restored on the interface.

Defining Queues

The *Queue Page* contains fields for defining the QoS queue forwarding types. The *Queue Page* allows network managers to define scheduling types. WRR Weights are defined once the WRR option has been selected for a specific QoS service queue. Modifying queue scheduling affects the queue settings globally.

To set the queue settings:

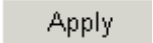
1. Click **QoS > General > Queue**. The *Queue Page* opens.

Figure 77. Queue Page

Queue	Scheduling	WRR Weight	% of WRR Bandwidth
	Strict Priority	WRR	
1	☒	☐	1
2	☒	☐	2
3	☒	☐	3
4	☒	☐	4
5	☒	☐	5
6	☒	☐	6
7	☒	☐	7
8	☒	☐	8

The *Queue Page* contains the following fields:

- **Queue** — Displays the number of queues for which the scheduling type and WRR weights are defined.
- **Scheduling** — Indicates the scheduling type by which the bandwidth is allocated to queues. The system supports selecting up to two group entries. Group entries must be selected in consecutive order. The possible field values are:
 - *Strict Priority* — Specifies whether traffic scheduling is based strictly on the queue priority.
 - *WRR* — Assigns the WRR scheduling type to the queue.
- **WRR Weight** — Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode. If a queue is set to 0 weight, the queue is not operational. Each queue has a weight range, queues 1-7 have the range 0-255, and queue 8 has the range 1-255.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the QoS queue.

2. Define the relevant fields.
3. Click . The *Queue* settings are set, and the device is updated.

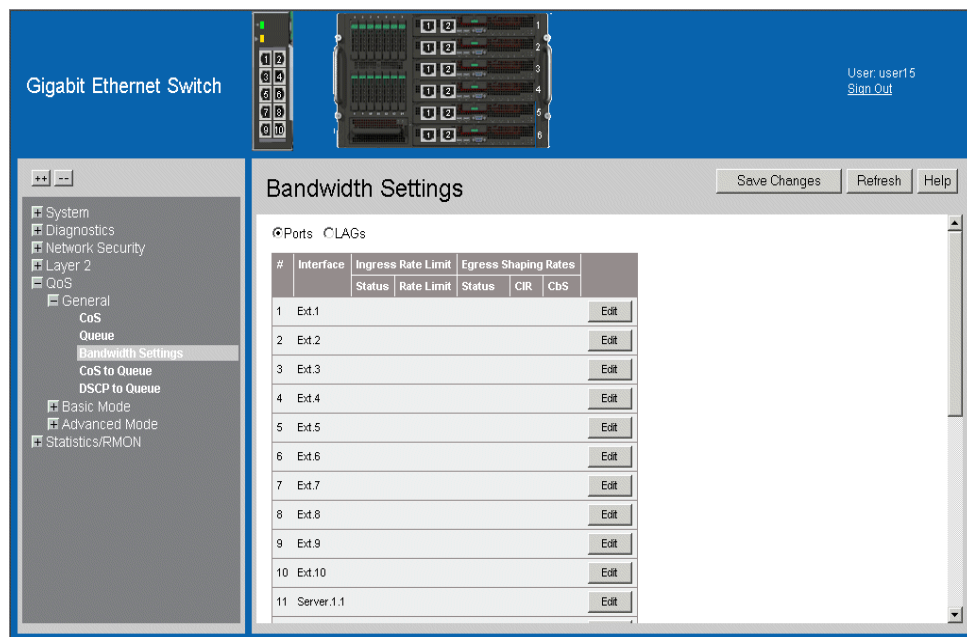
Configure Bandwidth Settings

The *Bandwidth Settings Page* allows network managers to define the bandwidth settings for a specified interface. Queue shaping can be based per interface. The queue shaping type is selected in the *Bandwidth Settings Page*.

To define bandwidth settings:

1. Click **QoS > General > Bandwidth Setting**. The *Bandwidth Settings Page* opens:

Figure 78. Bandwidth Settings Page



The *Bandwidth Settings Page* contains the following fields:

- **Ports** — Displays the port table for which the bandwidth settings are defined.
- **LAGs** — Displays the LAG table for which the bandwidth settings are defined.
- **Interface** — Displays the interface list for which the bandwidth settings are defined.
- **Ingress Rate Limit** — Indicates the traffic limit for the port.
 - *Status* — Indicates if Ingress Rate Limit is enabled on the interface.
 - *Rate Limit* — Defines the rate limit at which network traffic is forwarded.

- **Egress Shaping Rates** — Configures the traffic shaping type for selected interfaces. The possible field values are:
 - *Status* — Indicates if Egress Shaping Rate is enabled on the interface. The possible range is 1 to 10000000.
 - *CIR* — Defines CIR as the queue shaping type. The possible field value is 64 - 10,000,000 bits per second.
 - *CbS* — Defines CbS as the queue shaping type. The possible field value is 1 *kbps* -10,000,000 *bytes*.
2. Select an interface.
 3. Click **Edit**. The *Modify Bandwidth Settings Page* opens.

Figure 79. Modify Bandwidth Settings Page

4. Modify the relevant fields.
5. Click **Apply**. The *Bandwidth Settings* are saved to interface, and the device is updated.

Configuring QoS Mapping

This section contains information for mapping CoS values to queues. The *CoS to Queue Page* contains fields for mapping CoS values to traffic queues.

To map CoS values to queues:

1. Click **QoS > General > CoS to Queue**. The *CoS to Queue Page* opens.

Figure 80. CoS to Queue Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

CoS to Queue

Save Changes Refresh Help

Restore Defaults ☐

#	Class of Service	Queue
1	0	2
2	1	1
3	2	1
4	3	3
5	4	4
6	5	5
7	6	6
8	7	7

Apply

The *CoS to Queue Page* contains the following fields:

- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.
 - **Class of Service** — Specifies the CoS values, where zero is the lowest and 7 is the highest.
 - **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Eight traffic priority queues are supported.
2. Define the queue number in the *Queue* field next to the required CoS value.
 3. Click **Apply**. The CoS value is mapped to a queue, and the device is updated.

Mapping DSCP Values to Queues

The *DSCP to Queue Page* contains fields for mapping DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2.

To map CoS values to queues:

1. Click **QoS > General > DSCP to Queue**. The *DSCP to Queue Page* opens.

Figure 81. DSCP to Queue Page

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	13	1	26	1	39	1	52	1
1	1	14	1	27	4	40	1	53	1
2	1	15	1	28	1	41	1	54	1
3	1	16	1	29	1	42	1	55	1
4	1	17	1	30	1	43	5	56	1
5	1	18	1	31	1	44	1	57	1
6	1	19	3	32	1	45	1	58	1
7	1	20	1	33	1	46	1	59	0
8	1	21	1	34	1	47	1	60	1
9	1	22	1	35	5	48	1	61	1
10	1	23	1	36	1	49	1	62	1
11	2	24	1	37	1	50	1	63	1

The *DSCP to Queue Page* contains the following fields:

- **Restore Defaults** — Restores the device factory defaults for mapping DSCP values to a forwarding queue.
 - **DSCP In** — Displays the incoming packet's DSCP value.
 - **Queue** — Specifies the traffic forwarding queue to which the DSCP priority is mapped. Eight traffic priority queues are supported.
2. Define the queue number in the *Queue* field next to the required DSCP value.
 3. Click **Apply**. The DSCP value is mapped to a queue, and the device is updated.

Configuring Basic QoS Settings

This section contains information for defining basic QoS settings and includes the following topics:

- Configuring Basic General Parameters
- Configuring DSCP Rewrite

Configuring Basic General Parameters

The *Basic Mode General Settings Page* contains parameters for enabling the Basic QoS Mode on the device.

To configure QoS general parameters:

1. Click **QoS > Basic Mode > General**. The *Basic Mode General Settings Page* opens:

Figure 82. Basic Mode General Settings Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

++ --

- System
- Diagnostics
- Network Security
- Layer 2
- QoS
 - General
 - Basic Mode
 - General
 - DSCP Rewrite
 - Advanced Mode
 - Statistics/RMON

General

Trust Mode: CoS

Always Rewrite DSCP: ☐

Ports: C LAGs

#	Interface	Disable Trust Mode
1	Ext.1	☐
2	Ext.2	☐
3	Ext.3	☐
4	Ext.4	☐
5	Ext.5	☐
6	Ext.6	☐
7	Ext.7	☐
8	Ext.8	☐
9	Ext.9	☐
10	Ext.10	☐
11	Server.1.1	☐

Save Changes Refresh Help

The *Basic Mode General Settings Page* contains the following fields:

- **Ports** — Displays the basic mode general settings in the port table.
 - **LAGs** — Displays the basic mode general settings in the LAG table.
 - **Trust Mode** — Defines which packet fields to use for classifying packets entering the device. The possible Trust Mode field values are:
 - *CoS* — Classifies traffic based on the CoS tag value.
 - *DSCP* — Classifies traffic based on the DSCP values.
 - **Always Rewrite DSCP** — Indicates if the DSCP value is always reassigned based on values displayed in the DSCP Rewrite table. The possible field values are:
 - *Checked* — Enables reassigning the DSCP value.
 - *Unchecked* — Disables reassigning the DSCP value. This is the default value.
 - **Interface** — Indicates the Interface on which the Trust Mode is disabled.
 - **Disable Trust Mode** — When checked, Trust Mode is disabled.
2. Define the relevant fields.
 3. Click . The *QoS General Settings* are configure, and the device is updated.

Configuring DSCP Rewrite

DSCP Mutation map allows network managers to redefine DSCP values between DSCP-in and DSCP-out packets.

To configure the DSCP rewrite:

1. Click **QoS > Basic Mode > DSCP Rewrite**. The *QoS DSCP Rewrite Page* opens:

Figure 83. QoS DSCP Rewrite Page

Gigabit Ethernet Switch

User: user15
Sion Out

Save Changes Refresh Help

DSCP Rewrite

DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	12	12	24	24	36	36	48	48	60	60
1	1	13	13	25	25	37	37	49	49	61	61
2	2	14	14	26	26	38	38	50	50	62	62
3	3	15	15	27	27	39	39	51	51	63	63
4	4	16	16	28	28	40	40	52	52		
5	5	17	17	29	29	41	41	53	53		
6	6	18	18	30	30	42	42	54	54		
7	7	19	19	31	31	43	43	55	55		
8	8	20	20	32	32	44	44	56	56		
9	9	21	21	33	33	45	45	57	57		
10	10	22	22	34	34	46	46	58	58		
11	11	23	23	35	35	47	47	59	59		

Apply

The *QoS DSCP Rewrite Page* contains the following fields:

- **DSCP In** — Displays the incoming packet's DSCP value.
- **DSCP Out** — Reassigns the DSCP value on incoming packets.

2. Define the relevant fields.

3. Click **Apply**. The *QoS DSCP Rewrite Settings* are configure, and the device is updated.

Configuring Advanced QoS Settings

This section contains information for configuring advanced QoS features, and includes the following topics:

- Defining Policy Properties
- Defining Policy Profiles

Defining Policy Properties

This section contains information for configuring advanced policy properties, and includes the following topics:

- Mapping DSCP Values
- Creating Class Maps
- Aggregating Policies

Mapping DSCP Values

When traffic exceeds user-defined limits, use the *Policed DSCP Page* to configure the DSCP tag to use in place of the incoming DSCP tags.

To define advance QoS DSCP mapping:

1. Click **QoS > Advance Mode > Policed DSCP**. The *Policed DSCP Page* opens.

Figure 84. Policed DSCP Page

Gigabit Ethernet Switch

User: user15
[Sign Out](#)

Policed DSCP

DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	12	12	24	24	36	36	48	48	60	60
1	1	13	13	25	25	37	37	49	49	61	61
2	2	14	14	26	26	38	38	50	50	62	62
3	3	15	15	27	27	39	39	51	51	63	63
4	4	16	16	28	28	40	40	52	52		
5	5	17	17	29	29	41	41	53	53		
6	6	18	18	30	30	42	42	54	54		
7	7	19	19	31	31	43	43	55	55		
8	8	20	20	32	32	44	44	56	56		
9	9	21	21	33	33	45	45	57	57		
10	10	22	22	34	34	46	46	58	58		
11	11	23	23	35	35	47	47	59	59		

Apply

Save Changes Refresh Help

The *Policed DSCP Page* contains the following fields:

- **DSCP In** — Displays the incoming packet's DSCP value.
- **DSCP Out** — Reassigns the DSCP value on incoming packets.

2. Define the relevant values.
3. Click **Apply**. The *Policed DSCP* value is mapped to a queue, and the device is updated.

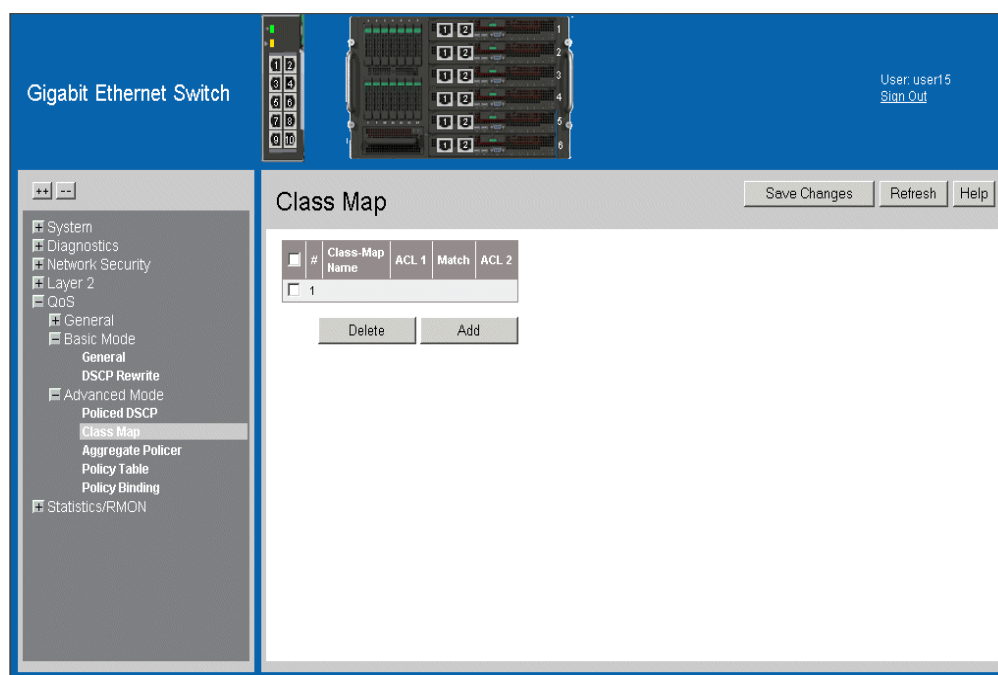
Creating Class Maps

One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

To define class maps:

1. Click **QoS > Advanced Mode > Class Map**. The *Class Map Page* opens:

Figure 85. Class Map Page



The *Class Map Page* contains the following fields:

- **Delete** — Deletes Class Maps. The possible field values are:
 - *Checked* — Deletes the selected Class Maps.
 - *Unchecked* — Maintains the current Class Maps.
- **Class-Map Name** — Displays the user-defined name of the class map.
- **ACL 1** — Contains a list of the user defined ACLs.
- **Match** — Indicates the criteria used to match ACLs filters within the class maps for incoming packets. Possible values are:
 - *And* — Matches both ACL 1 and ACL 2 to the packet.
 - *Or* — Matches either ACL 1 or ACL 2 to the packet.
- **ACL 2** — Contains a list of the user defined ACLs.

2. Click **Add** . The *Add QoS Class Map Page* opens:

Figure 86. Add QoS Class Map Page

The screenshot shows a window titled "Add QoS Class Map" with a help icon in the top right corner. The window contains the following fields and controls:

- Class Map Name:** A text input field.
- Preferred ACL:** A dropdown menu currently showing "IP Based ACL".
- IP ACL:** A checkbox that is checked, followed by a small dropdown menu.
- Match:** A label followed by a dropdown menu currently showing "And".
- MAC ACL:** An unchecked checkbox, followed by a dropdown menu currently showing "acl2".
- Buttons:** "Apply" and "Close" buttons at the bottom.

In addition to the fields in the *Class Map Page*, the *Add QoS Class Map Page* contains the following fields:

- **Preferred ACL** — Indicates if packets are first matched to an IP based ACL or a MAC based ACL.
- **IP ACL** — Contains a list of IP defined ACLs.
- **MAC ACL** — Contains a list of MAC defined ACLs.

3. Define the relevant fields.
4. Click **Apply** . The *Class Map* is defined, and the device is updated.

Aggregating Policiers

After a packet is classified, the policing process begins. A policier specifies the bandwidth limit for incoming traffic on the classified flow and actions are defined for packets that exceed the limits. These actions include forwarding packets, dropping packets, or remarking packets with a new DSCP value. The device supports per flow and aggregate policiers.

Aggregate policers enforce limits on a group of flows. An aggregate policer cannot be deleted if it is being used in a policy map. The *Aggregated Policier Page* contains information for defining the bandwidth limits and define actions to take on packets that do not meet the requirements.

To configure Aggregated Policiers:

1. Click **QoS > Advanced Mode > Aggregated Policier**. The *Aggregated Policier Page* opens:

Figure 87. Aggregated Policier Page

#	Aggregate Policier Name	Ingress CIR	Ingress CBS	Exceed Action
1	APN1	3	300	Remark DSCP

The *Aggregated Policier Page* contains the following fields:

- **Delete** — Deletes Aggregated Policy. The possible field values are:
 - *Checked* — Deletes the selected Aggregated Policy.
 - *Unchecked* — Maintains the current Aggregated Policy.
- **Aggregate Policier Name** — Specifies the aggregate policier name.
- **Ingress CIR** — Defines the CIR in kbits per second.

- **Ingress CBS** — Defines the CBS in bytes per second.
- **Exceed Action** — Indicates the action assigned to incoming information exceeds the traffic limits. Possible values are:
 - *None* — Packets exceeding the limits are forwarded.
 - *Drop* — Packets exceeding the limits are dropped.
 - *Remark DSCP* — Packets exceeding the limits are forwarded with a flagged/remarked DSCP value.

2. Click **Add** . The *Add Aggregated Policier Page* opens.

Figure 88. Add Aggregated Policier Page

The screenshot shows a dialog box titled "Add QoS Aggregate Policier". It has a help icon (?) in the top right corner. The form contains the following fields:

- Aggregate Policier Name**: An empty text input field.
- Ingress Committed Information Rate (CIR)**: A text input field containing the value "3", with "(Kbits per Second)" as a label to its right.
- Ingress Committed Burst Size (CBS)**: A text input field containing the value "3000", with "(Bytes per Second)" as a label to its right.
- Exceed Action**: A dropdown menu currently showing "None".

 At the bottom of the dialog are two buttons: "Apply" and "Close".

3. Define the relevant fields.

4. Click **Apply** . The *Aggregated Policier* is defined, and the device is updated.

To modify Aggregated Policiers:

1. Click **Edit** . The *Edit QoS Aggregate Policier Page* opens:

Figure 89. Edit QoS Aggregate Policier Page

The screenshot shows a dialog box titled "Edit QoS Aggregate Policier". It has a help icon (?) in the top right corner. The form contains the following fields:

- Aggregate Policier Name**: A text input field containing the value "agPol1".
- Ingress Committed Information Rate (CIR)**: A text input field containing the value "3", with "(Kbits per Second)" as a label to its right.
- Ingress Committed Burst Size (CBS)**: A text input field containing the value "3000", with "(Bytes per Second)" as a label to its right.
- Exceed Action**: A dropdown menu currently showing "None".

 At the bottom of the dialog are two buttons: "Apply" and "Close".

2. Modify the relevant fields.

3. Click **Apply** . The *Aggregated Policier* is defined, and the device is updated.

Defining Policy Profiles

This section contains information for configuring policy profiles, and includes the following topics:

- Defining Policies

Defining Policies

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

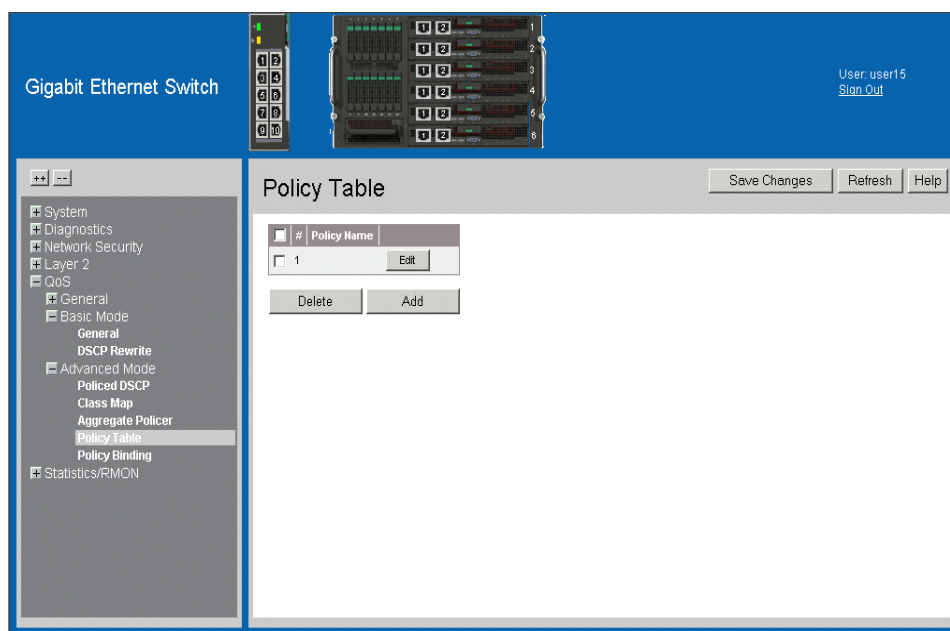
Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To define policies:

1. Click **QoS > Advanced Mode > Policy Table**. The *Policy Table Page* opens:

Figure 90. Policy Table Page

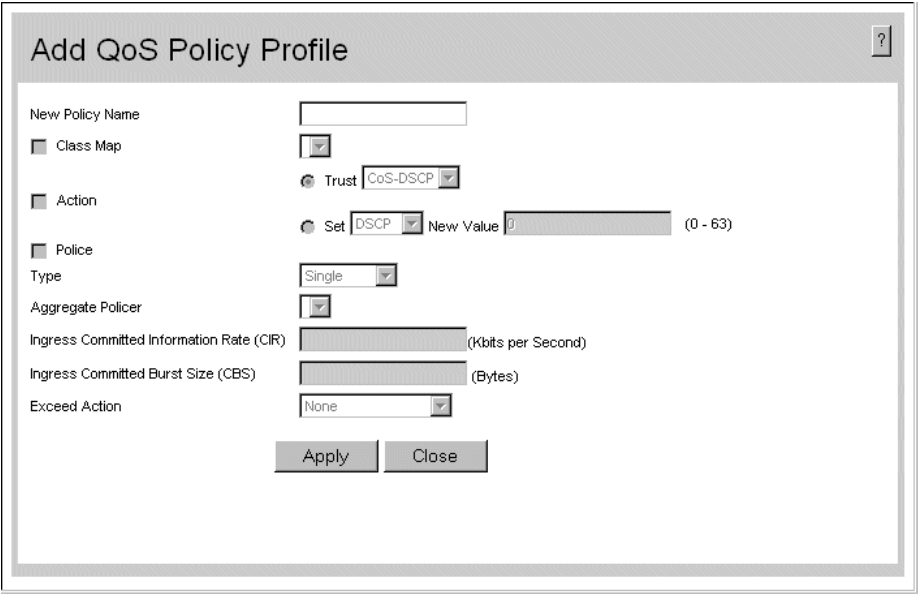


The *Policy Table Page* contains the following fields:

- **Delete** — Deletes policies. The possible field values are:
 - *Checked* — Deletes the selected policy.
 - *Unchecked* — Maintains policies.
- **Policy Name** — Displays the user-defined policy name.

2. Click  . The *Add QoS Class Map Page* opens:

Figure 91. Add QoS Policy Profile Page



In addition to the fields in the *Policy Table Page*, the *Add QoS Class Map Page* contains the following fields:

- **Class Map** — Selects a class map for the policy.
- **Action** — Indicates the action performed on incoming packets matching the policy profile. The possible field values are:
 - *Trust* — Applies the selected Trust settings. If an incoming packet contain both CoS and DSCP, the DSCP value takes precedence.
 - *Set* — Redefines the DSCP, Queue, CoS settings for incoming traffic.
 - *New Value* — Assigns the new value to the selected DSCP, Queue or CoS Setting.
- **Police** — Policer type for the class. Possible values are:
 - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
 - *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — User-defined aggregate policers.
- **Ingress Committed Information Rate (CIR)** — CIR in kilobits per second. This field is only relevant when the **Police** value is **Single**.

- **Ingress Committed Burst Size (CBS)** — CBS in bytes per second. This field is only relevant when the **Police** value is **Single**.
 - **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the **Police** value is **Single**. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP* — Remarks packets' DSCP values exceeding the defined CIR value according to Policed DSCP table.
 - *None* — Packets exceeding the limits are forwarded.
3. Define the relevant fields.
 4. Click **Apply** . The policy is defined, and the device is updated.

To modify policies:

1. Click **Edit** . The *Edit QoS Policy Profile Page* opens:

Figure 92. Edit QoS Policy Profile Page

Edit QoS Policy Profile

Policy Name
☐ Class Map

Action
☐

Police
☐ Type

Aggregate Policer

Ingress Committed Information Rate (CIR) (3-12,582,912) (Kbits per Second)

Ingress Committed Burst Size (CBS) (3,000-19,173,960) (Bytes)

Exceed Action
 None

#	Class-Map	Trust	Set Attribute	Set Value	Type	Aggregate Policer Name	CIR	CBS	Exceed Action
1									

Apply **Close**

2. Modify the relevant fields.
3. Click **Apply** . The policies are defined, and the device is updated.

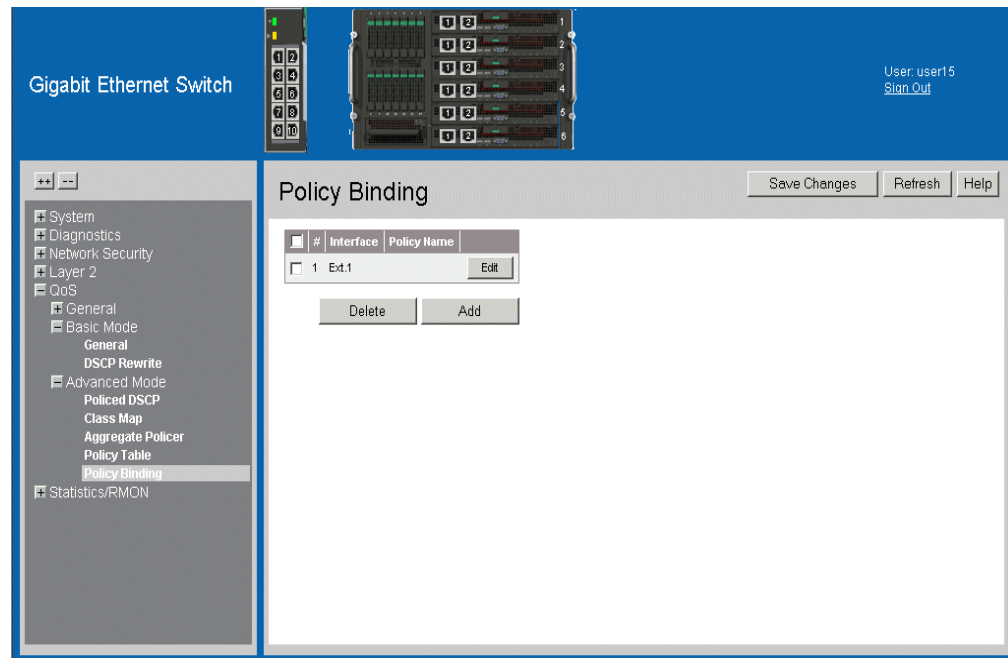
Attaching Policies to Interfaces

The *Policy Binding Page* contains information for attaching policies on interfaces and allows the user to modify policy binding to interfaces.

To attach a policy to an interface:

1. Click **QoS > Advanced Mode > Policy Binding**. The *Policy Binding Page* opens:

Figure 93. Policy Binding Page

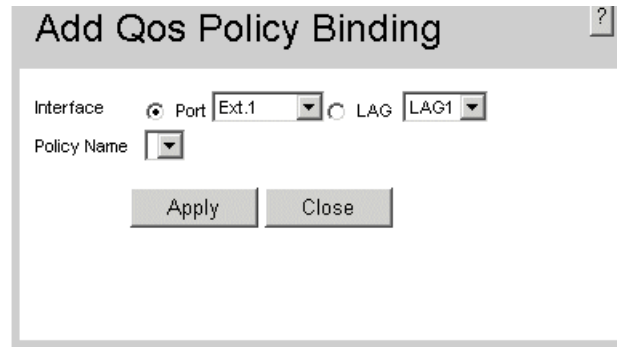


The *Policy Binding Page* contains the following fields:

- **Delete** — Deletes policies.
 - *Checked* — Deletes the selected policies.
 - *Unchecked* — Maintains the policies.
- **Interface** — Selects an interface.
- **Policy Name** — Contains a list of user-defined policies that can be attached to the interface.

2. Click **Add** . The *Add Qos Policy Binding Page* opens.

Figure 94. Add Qos Policy Binding Page

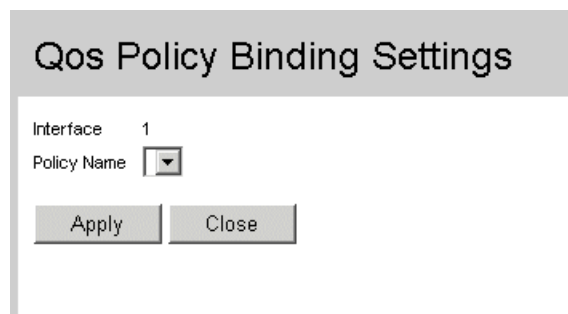


3. Define the relevant fields.
4. Click **Apply** . The *Add Qos Policy Binding Page* is defined, and the device is updated.

To modify the QoS policy binding settings:

1. Click **Edit** . The *Qos Policy Binding Settings Page* opens:

Figure 95. Qos Policy Binding Settings Page



2. Modify the relevant fields.
3. Click **Apply** . The *Qos Policy Binding Settings Page* is defined, and the device is updated.

11 Managing System Logs

This section provides information for managing system logs. The system logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors and informational messages.

Event messages have a unique format, as per the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event message.

The following table lists the log severity levels:

System Log Severity Levels

Severity	Level	Message
Emergency	Highest (0)	The system is not functioning.
Alert	1	The system needs immediate attention.
Critical	2	The system is in a critical state.
Error	3	A system error has occurred.
Warning	4	A system warning has occurred.
Notice	5	The system is functioning properly, but a system notice has occurred.
Informational	6	Provides device information.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

This section includes the following topics:

- Enabling System Logs
- Viewing the FLASH Logs
- Viewing the Device Memory Logs

Enabling System Logs

The *System Logs Properties Page* contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. Log messages are listed from the highest severity to the lowest severity level.

To define system log parameters:

1. Click **System > Logs > Properties**. The *System Logs Properties Page* opens.

Figure 96. System Logs Properties Page

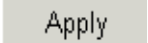
Severity	Memory Logs	Log Flash
Emergency	☒	☒
Alert	☒	☒
Critical	☒	☒
Error	☒	☒
Warning	☒	☐
Notice	☒	☐
Informational	☒	☐
Debug	☐	☐

The *System Logs Properties Page* contains the following fields:

- **Enable Logging** — Indicates if device global logs for Cache and File Logs are enabled. The possible field values are:
 - *Checked* — Enables device logs.
 - *Unchecked* — Disables device logs.
- **Severity** — The following are the available log severity levels for Memory Logs and Log Flash:
 - *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
 - *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
 - *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.

- *Error* — A device error has occurred.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- *Notice* — Provides device information.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

Note: *When a severity level is selected, all severity level choices above the selection are selected automatically.*

- **Memory Logs** — Defines the minimum severity level from which logs are sent to the RAM Log kept in RAM (Cache).
 - **Log Flash** — Defines the minimum severity level from which logs are sent to the log file kept in FLASH memory.
2. Define the relevant fields.
 3. Click  . The global log parameters are set, and the device is updated.

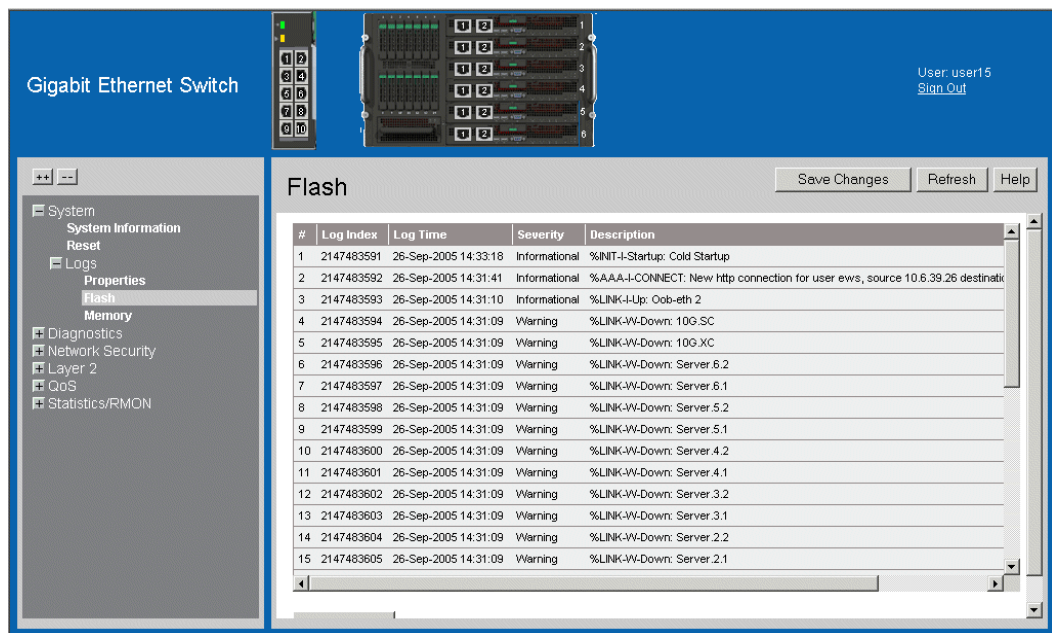
Viewing the FLASH Logs

The *System Flash Logs Page* contains information about log entries saved to the log file in Flash, including the time the log was generated, the log severity, and a description of the log message. The message log is available after reboot.

To view the message logs:

1. Click **System > Logs > Flash**. The *System Flash Logs Page* opens:

Figure 97. System Flash Logs Page



The *System Flash Logs Page* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

Clearing FLASH Logs

Message logs can be cleared from the *System Flash Logs Page*.

To clear message logs:

1. Click **System > Logs > Flash**. The *System Flash Logs Page* opens.
2. Click **Clear Logs**. The message logs are cleared.

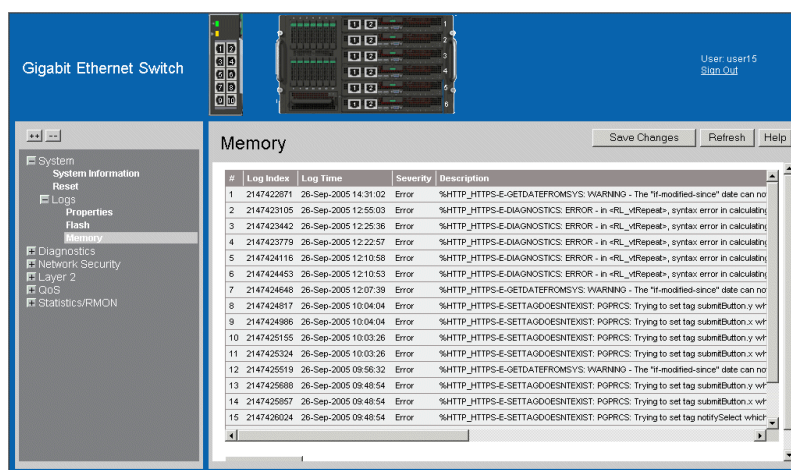
Viewing the Device Memory Logs

The *Device Memory Log Page* contains all system logs in a chronological order that are saved in RAM (Cache).

To open the *Device Memory Log Page*:

1. Click **System > Logs > Memory**. The *Device Memory Log Page* opens.

Figure 98. Device Memory Log Page



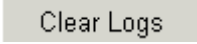
The *Device Memory Log Page* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

Clearing Device Memory Logs

Message logs can be cleared from the *Device Memory Log Page*.

To clear message logs:

1. Click **System > Logs > Memory**. The *Device Memory Log Page* opens.
2. Click . The message logs are cleared.

12 Managing Device Diagnostics

This section contains the following topics:

- Configuring Port Mirroring
- Ethernet Ports Diagnostics
- Viewing the CPU Utilization

Configuring Port Mirroring

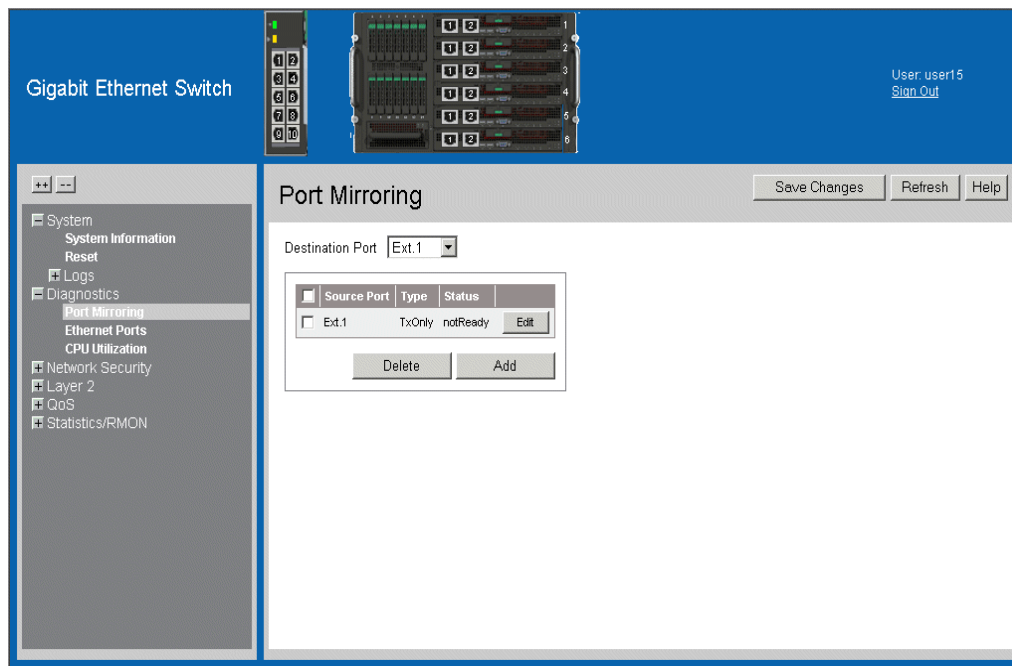
Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators can configure port mirroring by selecting a specific port from which to copy all packets, and other ports to which the packets copied.

To enable port mirroring:

1. Click **Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens:

Figure 99. Port Mirroring Page



The *Port Mirroring Page* contains the following fields:

- **Destination Port** — Defines the port number to which port traffic is copied.
- **Check box** — Selecting the check box, deletes the port mirroring session. The possible field values are:
 - *Checked* — Deletes the selected port mirroring sessions.
 - *Unchecked* — Maintains the port mirroring session.
- **Source Port** — Indicates the port from which the packets are mirrored.

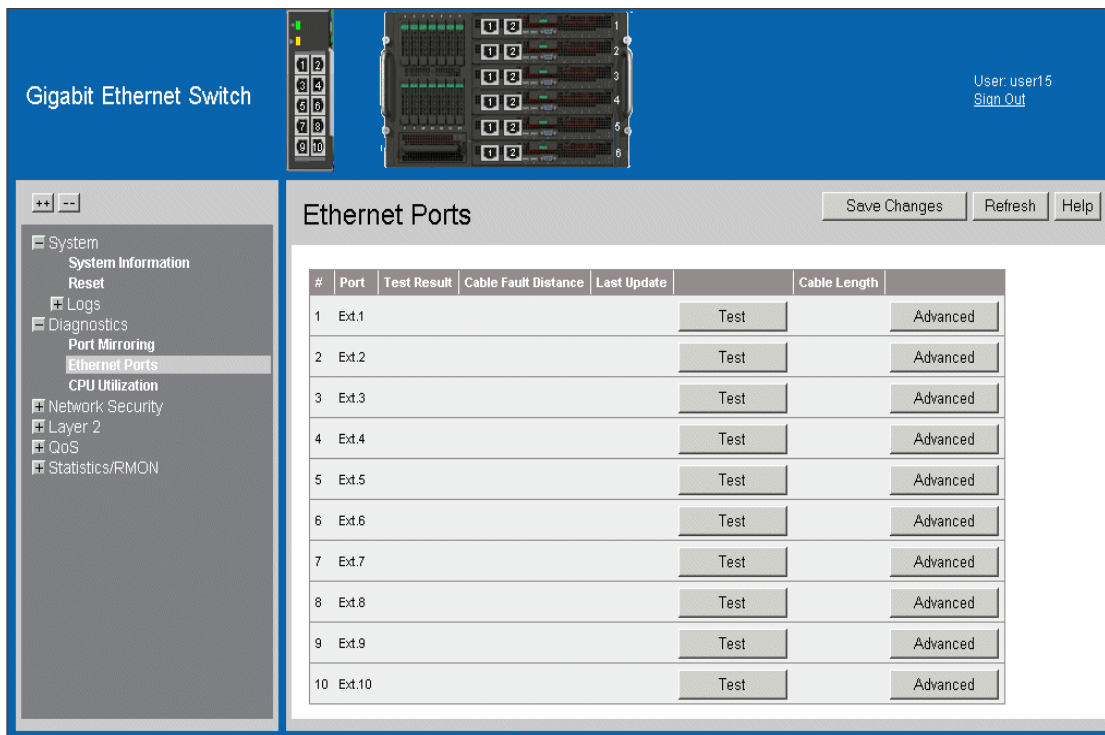
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
 - *Rx Only* — Defines the port mirroring on receiving ports.
 - *Tx Only* — Defines the port mirroring on transmitting ports.
 - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports. This is the default value.
- **Status** — Indicates if the port is currently monitored. The possible field values are:
 - *Active* — Indicates the port is currently monitored.
 - *Ready* — Indicates the port is not currently monitored.

Ethernet Ports Diagnostics

To test ethernet ports:

1. Click **Diagnostics > Ethernet Ports**. The *Ethernet Ports Page* opens:

Figure 100. Ethernet Ports Page



The *Ethernet Ports Page* contains the following fields:

- **Port** — Selects the port to be configured.
 - **Test Result** — Displays the cable test results. Possible values are:
 - *No Cable* — Indicates that there is not a cable connected to the port.
 - *Open Cable* — Indicates that the cable is open.
 - *Short Cable* — Indicates that a short has occurred in the cable.
 - *OK* — Indicates that the cable passed the test.
 - *Fiber Cable* — Indicates that a fiber cable is connected to the port.
 - **Cable Fault Distance** — Displays the distance from the port where the cable error occurred.
 - **Last Update** — Specifies the last time the port was tested.
 - **Cable Length** — Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.
2. Click . The ethernet port is tested.

Copper Cable Extended Feature

The Advanced button opens the *Cable Extended Feature Page*.

To perform an advance test on the ethernet port:

1. Click **Diagnostics > Ethernet Ports**. The *Ethernet Ports Page* opens.
2. Select a port and click **Advanced**. The *Cable Extended Feature Page* opens.

Figure 101. Cable Extended Feature Page

Copper Cable Extended Feature

Port

Ext 1

Cable Status

Bad Cable

Speed

1000 MB/s

Link Status

Up

Pair	Distance to Fault	Status	Cable Length	Channel	Polarity	Pair Skew
1-2			78M	B	Normal	8 ns
3-6			73M	A	Normal	8 ns
4-5			75M	D	Normal	8 ns
7-8			75M	C	Normal	0 ns

Close

The *Cable Extended Feature Page* contains the following fields:

- **Port** — Displays the port being tested.
- **Cable Status** — Displays the cable status.
- **Speed** — Indicates the speed at which the cable is transmitting packets. The possible field values are:
 - *10* — Indicates the port is currently operating at 10 Mbps.
 - *100* — Indicates the port is currently operating at 100 Mbps.
 - *1000* — Indicates the port is currently operating at 1000 Mbps.
- **Link Status** — Displays the current link status. The possible field values are:
 - *Up* — Indicates the port is currently active.
 - *Down* — Indicates the port is currently inactive.
- **Pair** — The pair of cables under test.
- **Distance to Fault** — Indicates the distance from the port where the cable error occurred.
- **Status** — Displays the cable status.
- **Channel** — Displays the cable's channel.

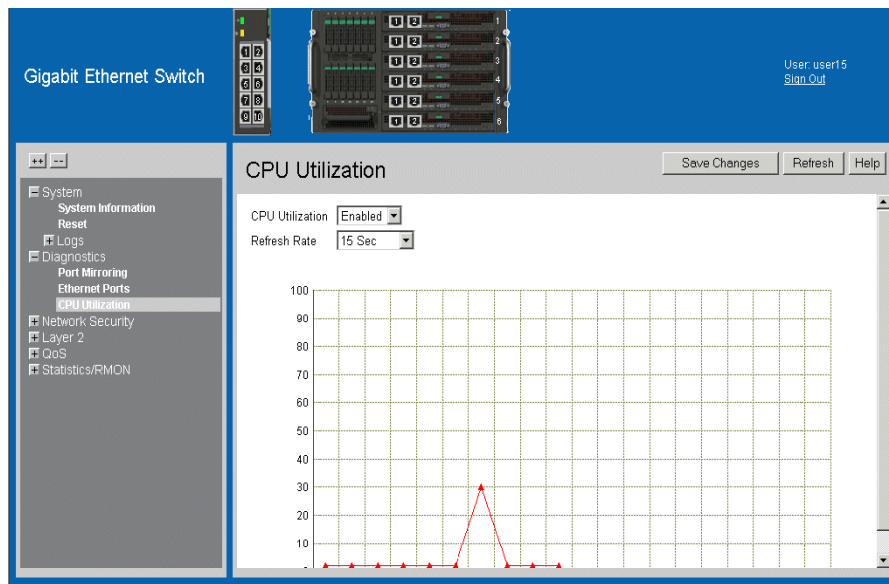
- **Polarity** — Automatic polarity detection and correction permits on all RJ-45 ports for automatic adjustment of wiring errors.
 - **Pair Skew** — Reaction or transmission time in nanoseconds for the selected cable pair and given cable length.
3. Click  . The ethernet port is tested.

Viewing the CPU Utilization

The *CPU Utilization Page* contains information about the system's CPU utilization. To view the CPU Utilization:

1. Click **System > CPU > CPU Utilization**. The *CPU Utilization Page* opens:

Figure 102. CPU Utilization Page



The *CPU Utilization Page* contains the following fields:

- **CPU Utilization** — Displays CPU resource utilization information. The possible field values are:
 - *Enabled* — Enables viewing CPU utilization information. This is the default value.
 - *Disabled* — Disables viewing the CPU utilization information.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed.

13 Viewing Statistics

Viewing Statistics

This section provides device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics. This section contains the following topics:

- Viewing Interface Statistics
- Managing RMON Statistics

Viewing Interface Statistics

This section contains the following topics:

- Viewing Device Interface Statistics
- Viewing Etherlike Statistics
- Viewing GVRP Statistics

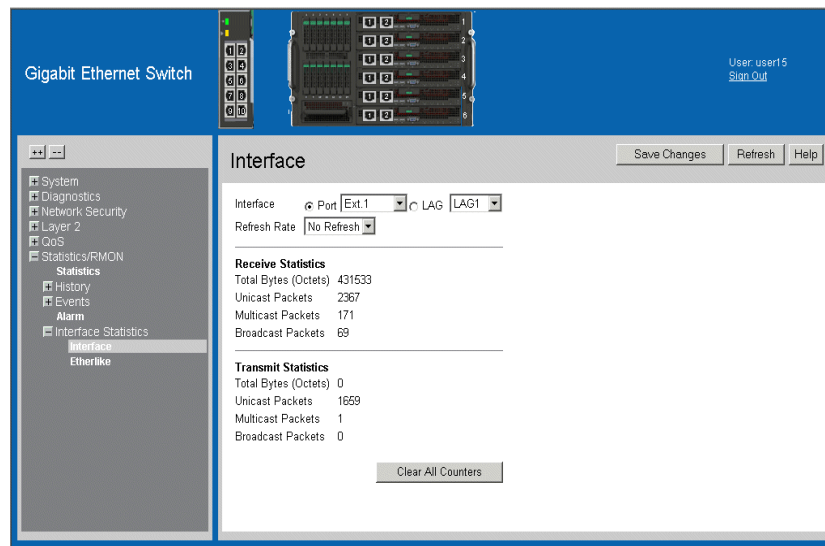
Viewing Device Interface Statistics

The *Interface Statistics Page* contains statistics for both received and transmitted packets.

To view interface statistics:

1. Click **Statistics/RMON > Interface Statistics > Interface**. The *Interface Statistics Page* opens.

Figure 103. Interface Statistics Page



The *Interface Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which interface statistics are displayed.
 - *LAG* — Defines the specific LAG for which interface statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *No Refresh*—Indicates that the Interface statistics are not refreshed.
 - *15 Sec*—Indicates that the Interface statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the Interface statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the Interface statistics are refreshed every 60 seconds.

Receive Statistics

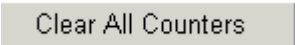
- **Total Bytes (Octets)** — Displays the number of octets received on the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets received on the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets received on the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the number of octets transmitted from the selected interface.
 - **Unicast Packets** — Displays the number of Unicast packets transmitted from the selected interface.
 - **Multicast Packets** — Displays the number of Multicast packets transmitted from the selected interface.
 - **Broadcast Packets** — Displays the number of Broadcast packets transmitted from the selected interface.
2. Select an interface in the *Interface* field. The interface statistics are displayed.

Resetting Interface Statistics Counters

To reset the Interface statistics counters:

1. Open the *Interface Statistics Page*.
2. Click . The interface statistics counters are cleared.

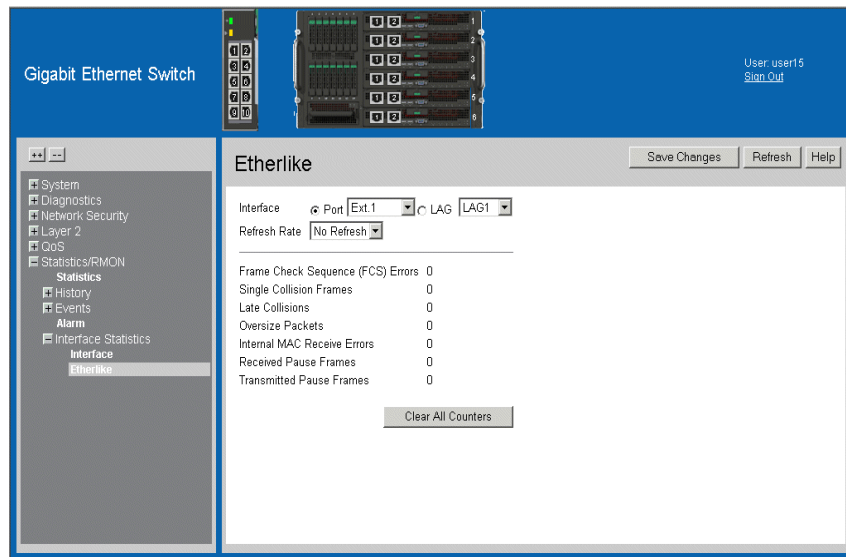
Viewing Etherlike Statistics

The *Etherlike Statistics Page* contains interface statistics.

To view Etherlike Statistics:

1. Click **Statistics/RMON > Interfaces Statistics > Etherlike**. The *Etherlike Statistics Page* opens.

Figure 104. Etherlike Statistics Page



The *Etherlike Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which Etherlike statistics are displayed.
 - *LAG* — Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the etherlike statistics are refreshed. The possible field values are:
 - *No Refresh*—Indicates that the Etherlike statistics are not refreshed.
 - *15 Sec*—Indicates that the Etherlike statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the Etherlike statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the Etherlike statistics are refreshed every 60 seconds.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.

- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
 - **Oversize Packets** — Displays the number of oversized packet errors on the selected interface.
 - **Internal MAC Receive Errors** — Number of internal MAC received errors on the selected interface.
 - **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
 - **Transmitted Pause Frames** — Displays the number of paused frames transmitted from the selected interface.
2. Select an interface in the *Interface* field. The Etherlike statistics are displayed.

Resetting Etherlike Statistics Counters

To reset the Etherlike statistics counters:

1. Open the *Etherlike Statistics Page*.
2. Click . The Etherlike statistics counters are cleared.

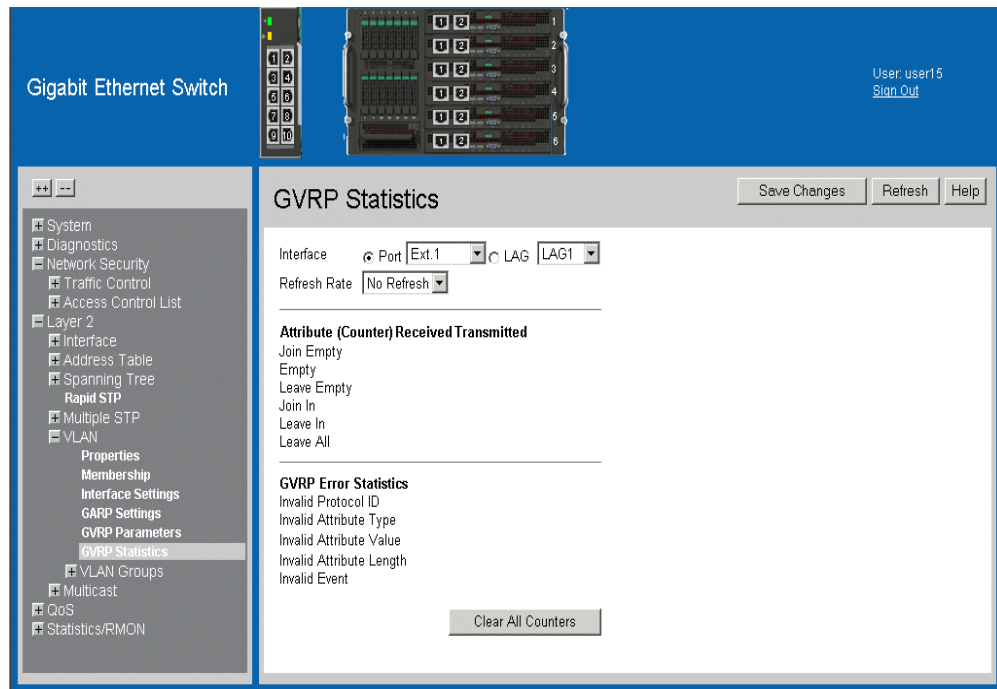
Viewing GVRP Statistics

The *GVRP Statistics Page* contains interface statistics for GVRP.

To view GVRP statistics:

1. Click **Layer 2 > VLAN > GVRP Statistics**. The *GVRP Statistics Page* opens.

Figure 105. GVRP Statistics Page



The *GVRP Statistics Page* contains the following fields:

- **Interface** — Specifies the interface type for which the statistics are displayed.
 - *Port* — Indicates port statistics are displayed.
 - *LAG* — Indicates LAG statistics are displayed.
- **Refresh Rate** — Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the GVRP statistics are not refreshed.
 - *15 Sec* — Indicates that the GVRP statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the GVRP statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the GVRP statistics are refreshed every 60 seconds.

Attribute (Counter) Received Transmitted

- **Join Empty** — Displays the device GVRP Join Empty statistics.
- **Empty** — Displays the device GVRP Empty statistics.
- **Leave Empty** — Displays the device GVRP Leave Empty statistics.
- **Join In** — Displays the device GVRP Join In statistics.
- **Leave In** — Displays the device GVRP Leave in statistics.
- **Leave All** — Displays the device GVRP Leave all statistics.

GVRP Error Statistics

- **Invalid Protocol ID** — Displays the device GVRP Invalid Protocol ID statistics.
 - **Invalid Attribute Type** — Displays the device GVRP Invalid Attribute ID statistics.
 - **Invalid Attribute Value** — Displays the device GVRP Invalid Attribute Value statistics.
 - **Invalid Attribute Length** — Displays the device GVRP Invalid Attribute Length statistics.
 - **Invalid Event** — Displays the device GVRP Invalid Event statistics.
2. Select an interface in the *Interface* field. The GVRP statistics are displayed.

Resetting GVRP Statistics Counters

To reset the GVRP statistics counter:

1. Open the *GVRP Statistics Page*.
2. Click **Clear All Counters**. The GVRP statistics counters are cleared.

Managing RMON Statistics

This section contains the following topics:

- Viewing RMON Statistics
- Configuring RMON History
- Configuring RMON Events
- Defining RMON Alarms

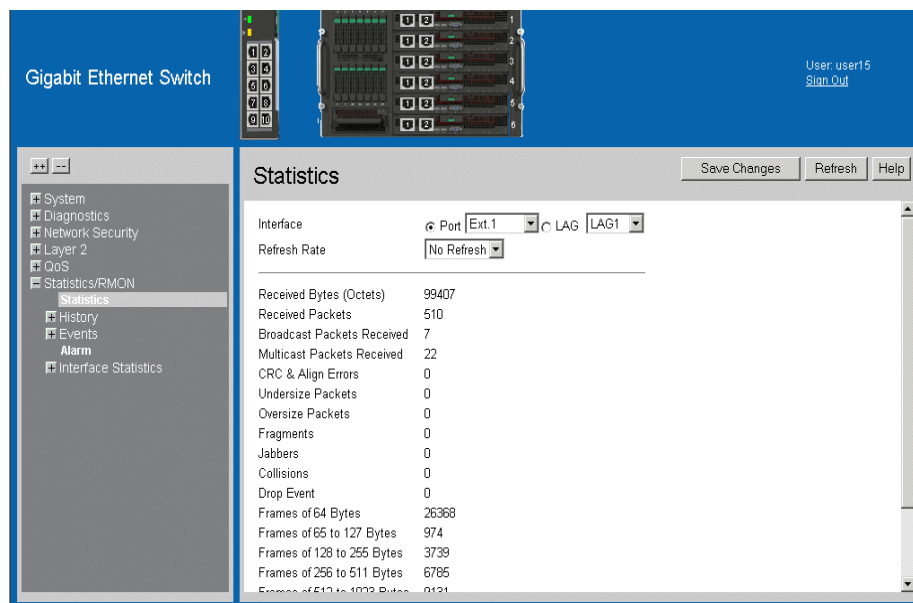
Viewing RMON Statistics

The *Viewing RMON Statistics* contains fields for viewing information about device utilization and errors that occurred on the device.

To view RMON statistics:

1. Click **Statistics/RMON > Statistics**. The *RMON Statistics Page* opens.

Figure 106. RMON Statistics Page



The *RMON Statistics Page* contains the following fields:

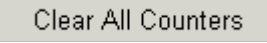
- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which RMON statistics are displayed.
 - *LAG* — Defines the specific LAG for which RMON statistics are displayed.

- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the Interface statistics are not refreshed.
 - *15 Sec* — Indicates that the Interface statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the Interface statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the Interface statistics are refreshed every 60 seconds.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Drop Event** — Displays the number of dropped events that have occurred on the interface since the device was last refreshed.
- **Frames of 64 Bytes** — Number of 64-byte frames received on the interface since the device was last refreshed.
- **Frames of 65 to 127 Bytes** — Number of 65 to 127 byte frames received on the interface since the device was last refreshed.
- **Frames of 128 to 255 Bytes** — Number of 128 to 255 byte frames received on the interface since the device was last refreshed.

- **Frames of 256 to 511 Bytes** — Number of *256 to 511* byte frames received on the interface since the device was last refreshed.
 - **Frames of 512 to 1023 Bytes** — Number of *512 to 1023* byte frames received on the interface since the device was last refreshed.
 - **Frames of 1024 to 1522 Bytes** — Number of *1024 to 1522* byte frames received on the interface since the device was last refreshed.
2. Select an interface in the *Interface* field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

To reset the RMON statistics counters:

1. Open the *RMON Statistics Page*.
2. Click . The RMON statistics counters are cleared.

Configuring RMON History

This section contains the following topics:

- Defining RMON History Control
- Viewing the RMON History Table
- Configuring RMON Events

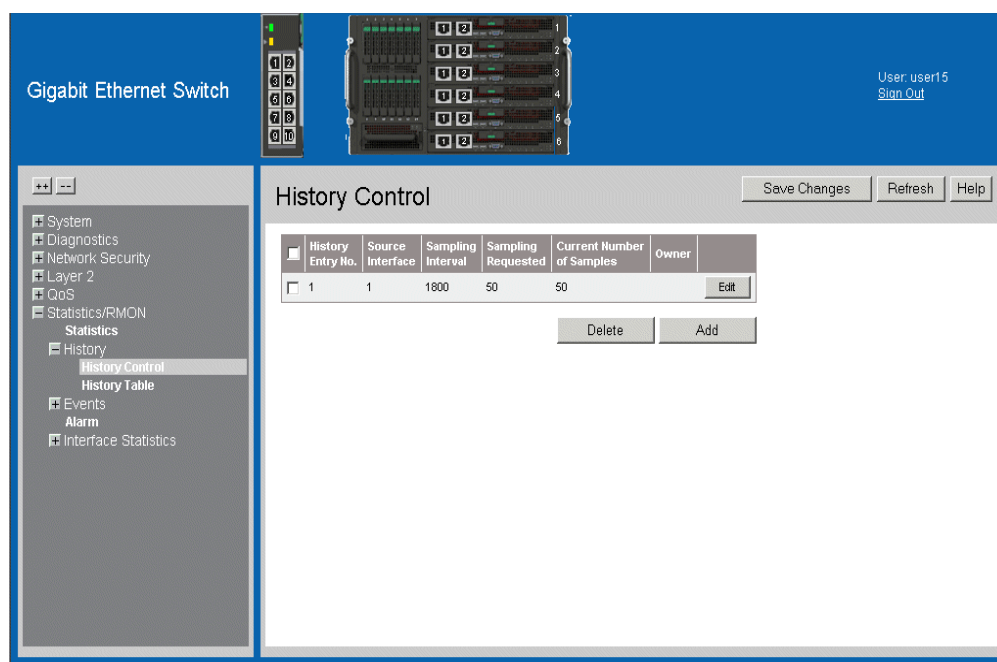
Defining RMON History Control

The *RMON History Control Page* contains information about the History Table and it's associated with the History table entry, and defines how the table is created. For example: The samples may include number of samples to be saved or the sampling interval.

To view RMON history information:

1. Click **Statistics/RMON > History > History Control**. The *RMON History Control Page* opens.

Figure 107. RMON History Control Page



The *RMON History Control Page* contains the following fields:

- **Delete** — Deletes History Control entries. The possible field values are:
 - *Checked* — Deletes the selected History Control entry.
 - *Unchecked* — Maintains the current History Control entries.
- **History Entry No.** — Displays the current history table number.
- **Source Interface** — Displays the interface from which the history samples were taken. The possible field values are:
 - *Port* — Specifies the port from which the RMON information was taken.
 - *LAG* — Specifies the port from which the RMON information was taken.
- **Sampling Interval** — Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

- **Sampling Requested**— Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
 - **Current Number of Samples**— Displays the current number of samples taken.
 - **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
2. Click **Add** . The *Add History Entry Settings Page* opens:

Figure 108. Add History Entry Settings Page

The screenshot shows a window titled "Add History Entry" with a help icon in the top right corner. The window contains the following fields and controls:

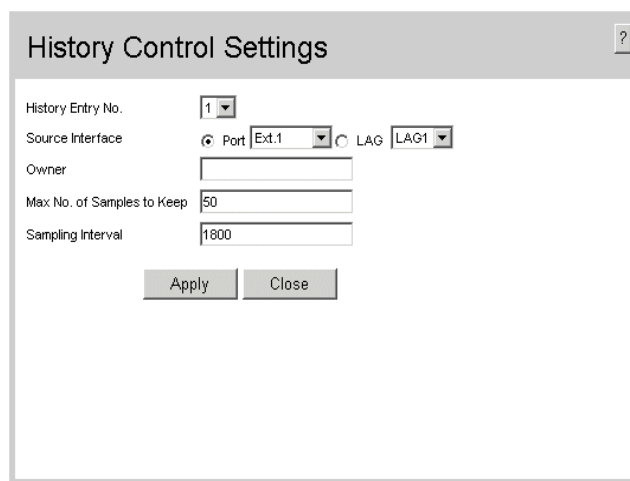
- New History Entry:** A text field containing the value "1".
- Source Interface:** Two radio buttons. The "Port" radio button is selected, and its dropdown menu shows "Ext.1". The "LAG" radio button is unselected, and its dropdown menu shows "LAG1".
- Owner:** An empty text input field.
- Max No. of Samples to Keep:** A text input field containing the value "50".
- Sampling Interval:** A text input field containing the value "1800".
- Buttons:** "Apply" and "Close" buttons at the bottom center.

3. Define the relevant fields.
4. Click **Apply** . The entry is added to the *Add History Entry Settings Page*, and the device is updated.

To modify the RMON History Control Settings:

1. Click **Edit** . The *RMON History Control Settings Page* opens:

Figure 109. RMON History Control Settings Page



The screenshot shows a dialog box titled "History Control Settings" with a help icon (?) in the top right corner. The dialog contains the following fields and controls:

- History Entry No.:** A dropdown menu with the value "1" selected.
- Source Interface:** Two radio buttons. The "Port" radio button is selected, and its dropdown menu shows "Ext.1". The "LAG" radio button is unselected, and its dropdown menu shows "LAG1".
- Owner:** A text input field.
- Max No. of Samples to Keep:** A text input field with the value "50".
- Sampling Interval:** A text input field with the value "1800".
- Buttons:** "Apply" and "Close" buttons at the bottom.

2. Modify the relevant fields.
3. Click **Apply** . The entry is added to the *RMON History Control Settings Page*, and the device is updated.

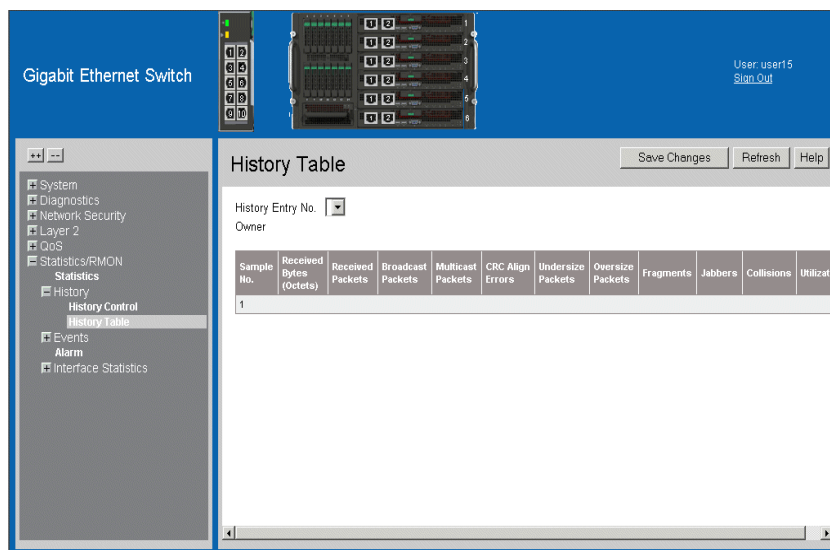
Viewing the RMON History Table

The *RMON History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To view the RMON History Table:

1. Click **Statistics/RMON > History > History Table**. The *RMON History Table Page* opens.

Figure 110. RMON History Table Page



The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.

- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
 - **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
 - **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
 - **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
 - **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
 - **Utilization** — Displays the percentage of the interface utilized.
2. Select an entry in the *History Entry No.* field. The Statistics are displayed.

Configuring RMON Events

This section includes the following topics:

- Defining RMON Events Control
- Viewing the RMON Events Logs

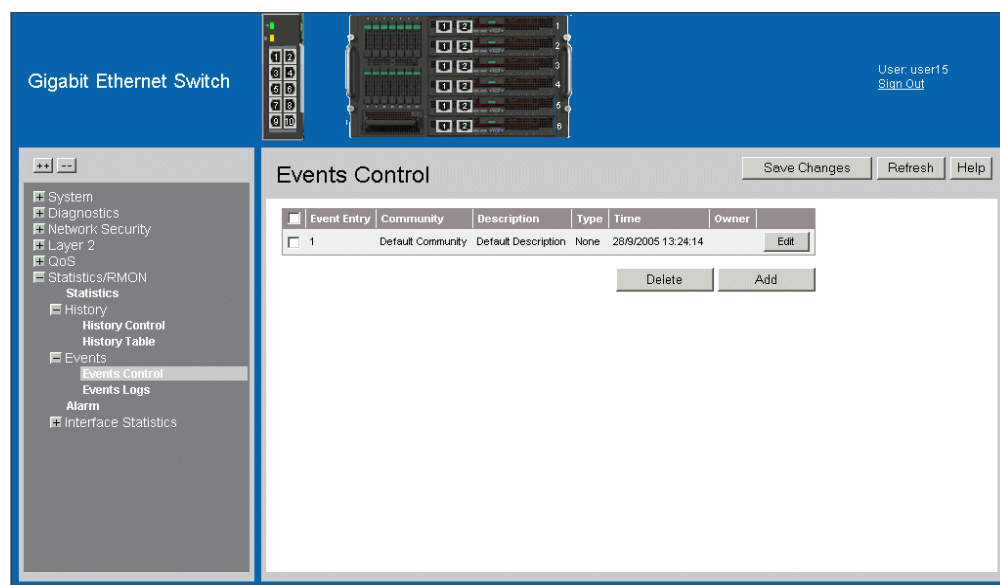
Defining RMON Events Control

The *RMON Events Control Page* contains fields for defining RMON events.

To view RMON events:

1. Click **Statistics/RMON > Events > Events Control**. The *RMON Events Control Page* opens.

Figure 111. RMON Events Control Page



The *RMON Events Control Page* contains the following fields:

- **Delete** — Deletes a RMON event. The possible field values are:
 - *Checked* — Deletes a selected RMON event.
 - *Unchecked* — Maintains RMON events.
- **Event Entry** — Displays the event.
- **Community** — Displays the community to which the event belongs.
- **Description** — Displays the user-defined event description.

- **Type** — Describes the event type. Possible values are:
 - *None* — Indicates that no event occurred.
 - *Log* — Indicates that the event is a log entry.
 - *Trap* — Indicates that the event is a trap.
 - *Log and Trap* — Indicates that the event is both a log entry and a trap.
- **Time** — Displays the time that the event occurred.
- **Owner** — Displays the device or user that defined the event.

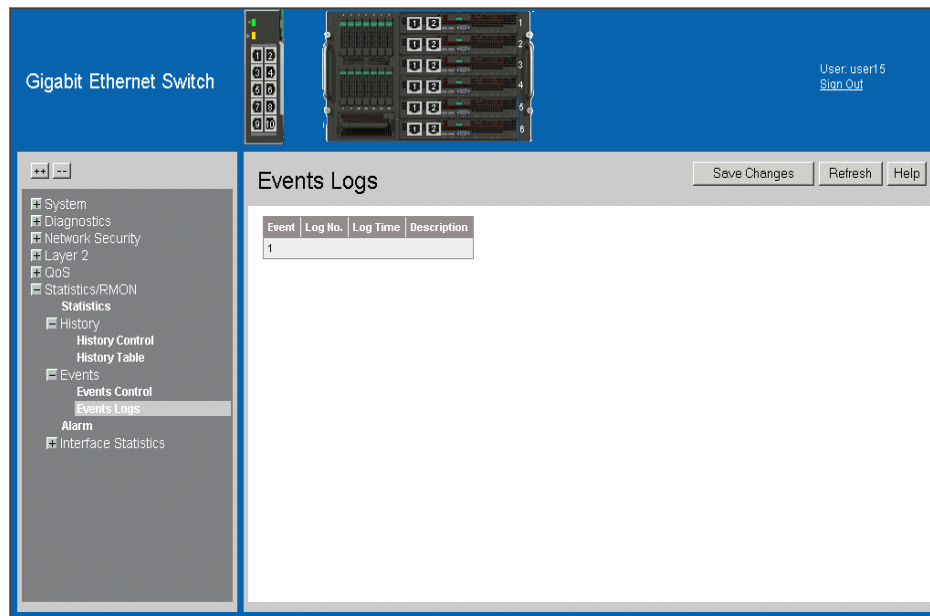
Viewing the RMON Events Logs

The *RMON Events Logs Page* contains a list of RMON events.

To view RMON event logs:

1. Click **Statistics/RMON > Events > Events Logs**. The *RMON Events Logs Page* opens.

Figure 112. RMON Events Logs Page



The *RMON Events Logs Page* contains the following fields:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

Defining RMON Alarms

The *RMON Alarm Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To set RMON alarms:

1. Click **Statistics/RMON > Alarm**. The *RMON Alarm Page* opens.

Figure 113. RMON Alarm Page

Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event
☐ 1		LAG 2	0	Absolute	100	1 - Default Description	20	1 - Default Description

The *RMON Alarm Page* contains the following fields:

- **Delete** — Deletes the RMON Alarms Table entry. The possible field values are:
 - *Checked* — Deletes a selected RMON Alarms Table entry.
 - *Unchecked* — Maintains RMON Alarms Table entry.
- **Alarm Entry** — Indicates a specific alarm.
- **Counter Name** — Displays the selected MIB variable.
- **Interface** — Displays interface for which RMON statistics are displayed. The possible field values are:
 - *Port* — Displays the RMON statistics for the selected port.
 - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Value** — Displays the selected MIB variable value.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

- *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.
 - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
 - **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
 - **Rising Event** — Displays the user-defined description of the event.
 - **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
 - **Falling Event** — Displays the user-defined description of the event.
 - **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
 - **Interval (sec)** — Defines the alarm interval time in seconds.
 - **Owner** — Displays the device or user that defined the alarm.
2. Click **Add**. The *Add Alarm Entry Page* opens:

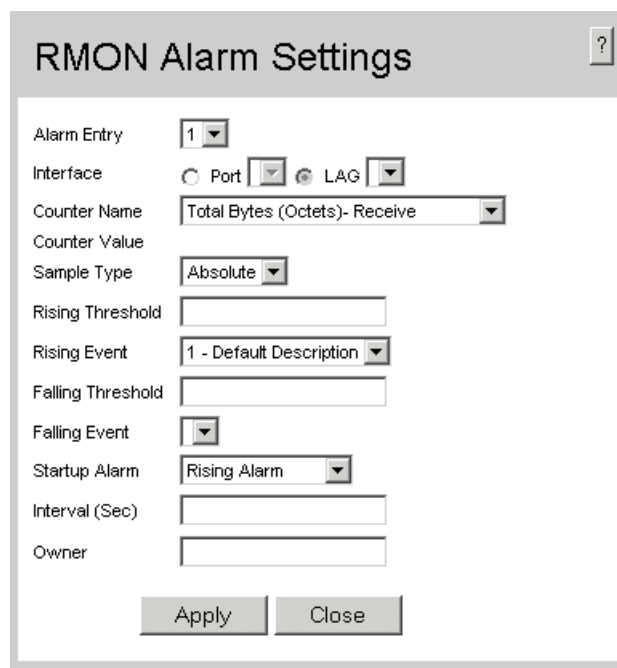
Figure 114. Add Alarm Entry Page

3. Define the relevant fields.
4. Click **Apply**. The entry is added to the *Add Alarm Entry Page*, and the device is updated.

To edit RMON alarms:

1. Click **Edit** . The RMON Alarms Definition Page opens:

Figure 115. RMON Alarms Definition Page



The screenshot shows a window titled "RMON Alarm Settings" with a help icon in the top right corner. The window contains the following fields and controls:

- Alarm Entry:** A dropdown menu with the value "1".
- Interface:** Radio buttons for "Port" and "LAG", each followed by a dropdown menu. "Port" is selected.
- Counter Name:** A dropdown menu with the value "Total Bytes (Octets)- Receive".
- Counter Value:** A text input field.
- Sample Type:** A dropdown menu with the value "Absolute".
- Rising Threshold:** A text input field.
- Rising Event:** A dropdown menu with the value "1 - Default Description".
- Falling Threshold:** A text input field.
- Falling Event:** A dropdown menu.
- Startup Alarm:** A dropdown menu with the value "Rising Alarm".
- Interval (Sec):** A text input field.
- Owner:** A text input field.

At the bottom of the window are two buttons: "Apply" and "Close".

2. Define the relevant fields.
3. Click **Apply** . The RMON alarm is added, and the device is updated.

A Troubleshooting

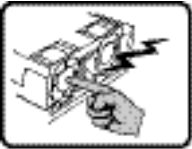
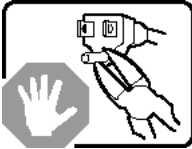
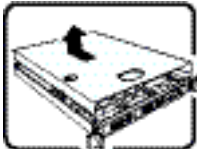
This chapter helps you identify and solve problems that might occur while you are using the system.

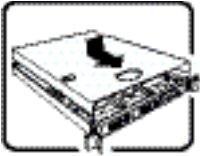
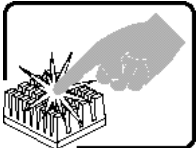
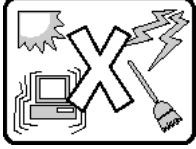
Symptoms / Problems	Possible Causes	Solutions
Switch's green power LED does not blink on switch restart or insertion.	Switch was not inserted properly or handle was not closed.	Pull the switch out and re-insert it into the chassis slot. Ensure that it is plugged in properly.
	Power cables are not connected to the chassis.	Ensure that the power cables are properly connected. Replace cables if defective.
Switch's green power LED does not change from blinking to solid ON after 300 seconds following switch restart or insertion.	Fatal hardware or software problem.	Pull the switch out and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem persists, consult your technical support representative.
Switch's amber fault LED is solid on.	Fatal hardware or software problem.	Pull the switch out and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem repeats, replace the faulty switch.
"Advanced UI" in the chassis management module GUI is not available on the "Switch 1/2 Actions" tab.	Connection between the switch and the management module is broken.	Pull out the management module/switch and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem repeats, replace the faulty switch. If the problem persists, consult your technical support representative.
Clicking on the "Advanced UI" action in the chassis management module GUI does not open web browser of the switch.	Connection between the switch and management module is broken.	Pull out the management module/switch and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem repeats, replace the faulty switch. If the problem persists, consult your technical support representative.

Symptoms / Problems	Possible Causes	Solutions
Switch web browser cannot display pages.	Web browser settings are not configured properly.	Ensure that the web browser settings are configured correctly (cookies, pop-ups, JavaScript enabled, proxy, etc.) according to the installation guide.
	Connection between the switch and management module is broken.	Pull out the management module/switch and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem repeats, replace the faulty switch. If the problem persists, consult your technical support representative.
An external port is connected, but the corresponding link LED is not ON or flashing.	Incorrect Ethernet cable - crossed, rather than straight cable, or vice versa, or split pair (incorrect twisting of pairs)	Check pin-out and replace if necessary.
	Bad cable.	Replace with a known good cable.
	Wrong cable type.	Replace with a known good cable of the proper type.
	The switch is not active, or the switch is in a fault state.	Pull out the switch and re-insert it into the chassis slot. Ensure that it is plugged in properly. If the problem repeats, replace the faulty switch. If the problem persists, consult your technical support representative.
	The other side is not configured with the same attributes as the switch's port.	Ensure both sides have the same port configuration settings (speed, duplex, auto-negotiation, etc.)

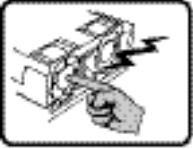
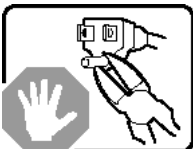
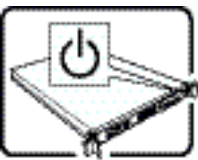
B Installation/Assembly Safety Instructions

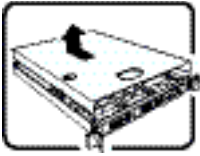
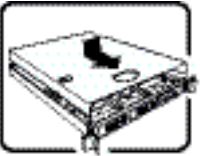
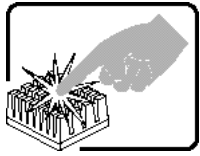
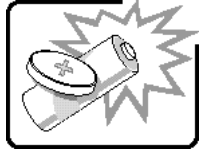
English

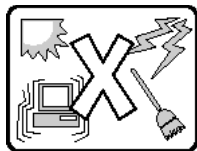
	The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified personnel.
	Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.
	The power button on the system does not turn off system AC power. To remove AC power from the system, you must unplug each AC power cord from the wall outlet or power supply. The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into shall be installed near the equipment and shall be easily accessible.
	SAFETY STEPS: Whenever you remove the chassis covers to access the inside of the system, follow these steps: 1. Turn off all peripheral devices connected to the system. 2. Turn off the system by pressing the power button. 3. Unplug all AC power cords from the system or from wall outlets. 4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system. 5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system-any unpainted metal surface-when handling components. 6. Do not operate the system with the chassis covers removed.
	After you have completed the six SAFETY steps above, you can remove the system covers. To do this: 1. Unlock and remove the padlock from the back of the system if a padlock has been installed. 2. Remove and save all screws from the covers. 3. Remove the cover(s).

	For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers: 1. Check first to make sure you have not left loose tools or parts inside the system. 2. Check that cables, add-in boards, and other components are properly installed. 3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly. 4. Insert and lock the padlock to the system to prevent unauthorized access inside the system. 5. Connect all external cables and the AC power cord(s) to the system.
	A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.
	Danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer's instructions.
	The system is designed to operate in a typical office environment. Choose a site that is: • Clean and free of airborne particles (other than normal room dust). • Well ventilated and away from sources of heat including direct sunlight. • Away from sources of vibration or physical shock. • Isolated from strong electromagnetic fields produced by electrical devices. • In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm. • Provided with a properly grounded wall outlet. • Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect.

Deutsch

	Benutzer können am Netzgerät dieses Produkts keine Reparaturen vornehmen. Das Produkt enthält möglicherweise mehrere Netzgeräte. Wartungsarbeiten müssen von qualifizierten Technikern ausgeführt werden.
	Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht genau um den erforderlichen Typ handelt. Ein Produkt mit mehreren Netzgeräten hat für jedes Netzgerät ein eigenes Netzkabel.
	Der Wechselstrom des Systems wird durch den Ein-/Aus-Schalter für Gleichstrom nicht ausgeschaltet. Ziehen Sie jedes Wechselstrom-Netzkabel aus der Steckdose bzw. dem Netzgerät, um den Stromanschluß des Systems zu unterbrechen.
	SICHERHEISSMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten: 1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus. 2. Schalten Sie das System mit dem Hauptschalter aus. 3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose. 4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab. 5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden. 6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.

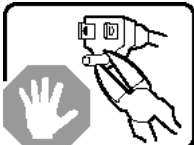
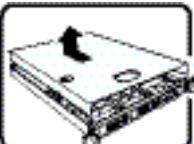
	SICHERHEISSMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten: 1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus. 2. Schalten Sie das System mit dem Hauptschalter aus. 3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose. 4. Auf der Rückseite des Systems beschrifteten und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab. 5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden. 6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.
	Zur ordnungsgemäßen Kühlung und Lüftung muß die Gehäuseabdeckung immer wieder vor dem Einschalten installiert werden. Ein Betrieb des Systems ohne angebrachte Abdeckung kann Ihrem System oder Teile darin beschädigen. Um die Abdeckung wieder anzubringen: 1. Vergewissern Sie sich, daß Sie keine Werkzeuge oder Teile im Innern des Systems zurückgelassen haben. 2. Überprüfen Sie alle Kabel, Zusatzkarten und andere Komponenten auf ordnungsgemäßen Sitz und Installation. 3. Bringen Sie die Abdeckungen wieder am Gehäuse an, indem Sie die zuvor gelösten Schrauben wieder anbringen. Ziehen Sie diese gut an. 4. Bringen Sie die Verschlusseinrichtung (Padlock) wieder an und schließen Sie diese, um ein unerlaubtes Öffnen des Systems zu verhindern. 5. Schließen Sie alle externen Kabel und den AC Stromanschlußstecker Ihres Systems wieder an.
	Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.
	Bei falschem Einsetzen einer neuen Batterie besteht Explosionsgefahr. Die Batterie darf nur durch denselben oder einen entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt werden. Entsorgen Sie verbrauchte Batterien den Anweisungen des Herstellers entsprechend.

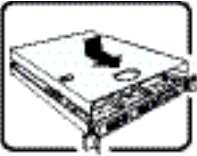
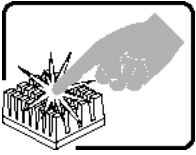
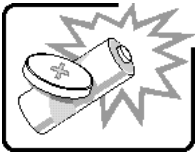
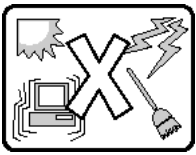


Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der Standort sollte:

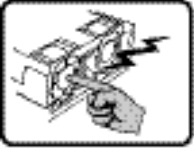
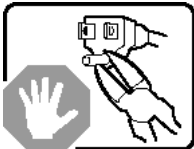
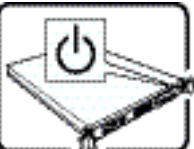
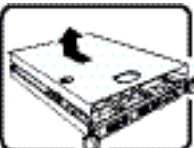
- "sauber und staubfrei sein (Hausstaub ausgenommen);
- "gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- "keinen Erschütterungen ausgesetzt sein;
- "keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- "in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- "mit einer geerdeten Wechselstromsteckdose ausgerüstet sein;
- "über ausreichend Platz verfügen, um Zugang zu den Netzkabeln zu gewährleisten, da der Stromanschluß des Produkts hauptsächlich über die Kabel unterbrochen wird

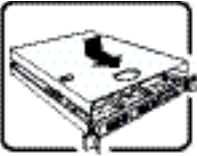
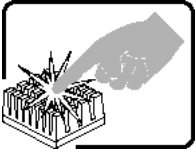
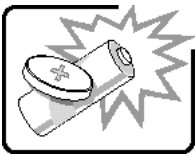
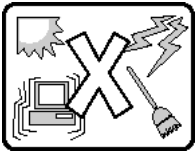
Français

	Le bloc d'alimentation de ce produit ne contient aucune pièce pouvant être réparée par l'utilisateur. Ce produit peut contenir plus d'un bloc d'alimentation. Veuillez contacter un technicien qualifié en cas de problème.
	Ne pas essayer d'utiliser ni modifier le câble d'alimentation CA fourni, s'il ne correspond pas exactement au type requis. Le nombre de câbles d'alimentation CA fournis correspond au nombre de blocs d'alimentation du produit.
	Notez que le commutateur CC de mise sous tension /hors tension du panneau avant n'éteint pas l'alimentation CA du système. Pour mettre le système hors tension, vous devez débrancher chaque câble d'alimentation de sa prise.
	CONSIGNES DE SÉCURITÉ -Lorsque vous ouvrez le boîtier pour accéder à l'intérieur du système, suivez les consignes suivantes: 1. Mettez hors tension tous les périphériques connectés au système. 2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir). 3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales. 4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système. 5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez une bande antistatique pour poignet et reliez-la à la masse du système (toute surface métallique non peinte du boîtier). 6. Ne faites pas fonctionner le système tandis que le boîtier est ouvert.
	Une fois TOUTES les étapes précédentes accomplies, vous pouvez retirer les panneaux du système. Procédez comme suit: 1. Si un cadenas a été installé sur à l'arrière du système, déverrouillez-le et retirez-le. 2. Retirez toutes les vis des panneaux et mettez-les dans un endroit sûr. 3. Retirez les panneaux.

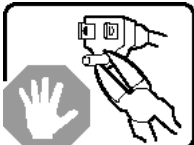
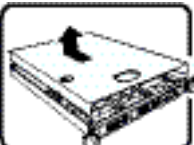
	Afin de permettre le refroidissement et l'aération du système, réinstallez toujours les panneaux du boîtier avant de mettre le système sous tension. Le fonctionnement du système en l'absence des panneaux risque d'endommager ses pièces. Pour installer les panneaux, procédez comme suit: 1. Assurez-vous de ne pas avoir oublié d'outils ou de pièces démontées dans le système. 2. Assurez-vous que les câbles, les cartes d'extension et les autres composants sont bien installés. 3. Revissez solidement les panneaux du boîtier avec les vis retirées plus tôt. 4. Remettez le cadenas en place et verrouillez-le afin de prévenir tout accès non autorisé à l'intérieur du système. 5. Rebranchez tous les cordons d'alimentation c. a. et câbles externes au système.
	Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.
	Danger d'explosion si la batterie n'est pas remontée correctement. Remplacer uniquement avec une batterie du même type ou d'un type équivalent recommandé par le fabricant. Disposez des piles usées selon les instructions du fabricant.
	Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être: • "Propre et dépourvu de poussière en suspension (sauf la poussière normale). • "Bien aéré et loin des sources de chaleur, y compris du soleil direct. • "A l'abri des chocs et des sources de vibrations. • "Isolé de forts champs électromagnétiques géénérés par des appareils électriques. • "Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage. • "Muni d'une prise murale correctement mise à la terre. • "Suffisamment spacieux pour vous permettre d'accéder aux câbles d'alimentation (ceux-ci étant le seul moyen de mettre le système hors tension).

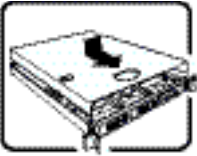
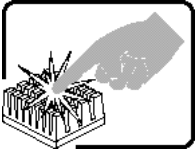
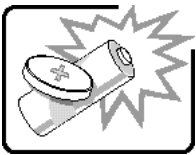
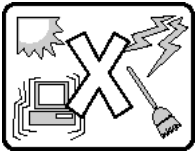
Español

	El usuario debe abstenerse de manipular los componentes de la fuente de alimentación de este producto, cuya reparación debe dejarse exclusivamente en manos de personal técnico especializado. Puede que este producto disponga de más de una fuente de alimentación
	No intente modificar ni usar el cable de alimentación de corriente alterna, si no corresponde exactamente con el tipo requerido. El número de cables suministrados se corresponden con el número de fuentes de alimentación de corriente alterna que tenga el producto
	Nótese que el interruptor activado/desactivado en el panel frontal no desconecta la corriente alterna del sistema. Para desconectarla, deberá desenchufar todos los cables de corriente alterna de la pared o desconectar la fuente de alimentación.
	INSTRUCCIONES DE SEGURIDAD: Cuando extraiga la tapa del chasis para acceder al interior del sistema, siga las siguientes instrucciones: 1. Apague todos los dispositivos periféricos conectados al sistema. 2. Apague el sistema presionando el interruptor encendido/apagado. 3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna. 4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema. 5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujeta a la toma de tierra del chasis - o a cualquier tipo de superficie de metal sin pintar. 6. No ponga en marcha el sistema si se han extraído las tapas del chasis.
	Después de completar las seis instrucciones de SEGURIDAD mencionadas, ya puede extraer las tapas del sistema. Para ello: 1. Desbloquee y extraiga el bloqueo de seguridad de la parte posterior del sistema, si se ha instalado uno. 2. Extraiga y guarde todos los tornillos de las tapas. Extraiga las tapas.

	Para obtener un enfriamiento y un flujo de aire adecuados, reinstale siempre las tapas del chasis antes de poner en marcha el sistema. Si pone en funcionamiento el sistema sin las tapas bien colocadas puede dañar los componentes del sistema. Para instalar las tapas: 1. Asegúrese primero de no haber dejado herramientas o componentes sueltos dentro del sistema. 2. Compruebe que los cables, las placas adicionales y otros componentes se hayan instalado correctamente. 3. Incorpore las tapas al chasis mediante los tornillos extraídos anteriormente, tensándolos firmemente. 4. Inserte el bloqueo de seguridad en el sistema y bloquéelo para impedir que pueda accederse al mismo sin autorización. 5. Conecte todos los cables externos y los cables de alimentación CA al sistema.
	Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.
	Existe peligro de explosión si la pila no se cambia de forma adecuada. Utilice solamente pilas iguales o del mismo tipo que las recomendadas por el fabricante del equipo. Para deshacerse de las pilas usadas, siga igualmente las instrucciones del fabricante.
	El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar: • "Limpio y libre de partículas en suspensión (salvo el polvo normal). • "Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa. • "Alejado de fuentes de vibración. • "Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos. • "En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas. • "Provisto de una toma de tierra correctamente instalada. • "Provisto de espacio suficiente como para acceder a los cables de alimentación, ya que éstos hacen de medio principal de desconexión del sistema.

Italiano

	Rivolgersi ad un tecnico specializzato per la riparazione dei componenti dell'alimentazione di questo prodotto. È possibile che il prodotto disponga di più fonti di alimentazione.
	Non modificare o utilizzare il cavo di alimentazione in c.a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto. Ad ogni fonte di alimentazione corrisponde un cavo di alimentazione in c.a. separato.
	L'interruttore attivato/disattivato nel pannello anteriore non interrompe l'alimentazione in c.a. del sistema. Per interromperla, è necessario scollegare tutti i cavi di alimentazione in c.a. dalle prese a muro o dall'alimentazione di corrente.
	PASSI DI SICUREZZA: Qualora si rimuovano le coperture del telaio per accedere all'interno del sistema, seguire i seguenti passi: 1. Spegner tutti i dispositivi periferici collegati al sistema. 2. Spegner il sistema, usando il pulsante spento/acceso dell'interruttore del sistema. 3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche. 4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema. 5. Qualora si tocchino i componenti, proteggersi dallo scarico elettrostatico (SES), portando un cinghia anti-statica da polso che è attaccata alla presa a terra del telaio del sistema - qualsiasi superficie non dipinta - . 6. Non far operare il sistema quando il telaio è senza le coperture.
	Dopo aver seguito i sei passi di SICUREZZA sopracitati, togliere le coperture del telaio del sistema come segue: 1. Aprire e rimuovere il lucchetto dal retro del sistema qualora ve ne fosse uno installato. 2. Togliere e mettere in un posto sicuro tutte le viti delle coperture. 3. Togliere le coperture.

	Per il giusto flusso dell'aria e raffreddamento del sistema, rimettere sempre le coperture del telaio prima di riaccendere il sistema. Operare il sistema senza le coperture al loro proprio posto potrebbe danneggiare i componenti del sistema. Per rimettere le coperture del telaio: 1. Controllare prima che non si siano lasciati degli attrezzi o dei componenti dentro il sistema. 2. Controllare che i cavi, dei supporti aggiuntivi ed altri componenti siano stati installati appropriatamente. 3. Attaccare le coperture al telaio con le viti tolte in precedenza e avvitarle strettamente. 4. Inserire e chiudere a chiave il lucchetto sul retro del sistema per impedire l'accesso non autorizzato al sistema. 5. Ricollegare tutti i cavi esterni e le prolunghe AC del sistema.
	Se il sistema è stato a lungo in funzione, il microprocessore e il dissipatore di calore potrebbero essere surriscaldati. Fare attenzione alla presenza di piedini appuntiti e parti taglienti sulle schede e sul telaio. È consigliabile l'uso di guanti di protezione.
	Esiste il pericolo di un'esplosione se la pila non viene sostituita in modo corretto. Utilizzare solo pile uguali o di tipo equivalente a quelle consigliate dal produttore. Per disfarsi delle pile usate, seguire le istruzioni del produttore.
	Il sistema è progettato per funzionare in un ambiente di lavoro tipo. Scegliere una postazione che sia: • "Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente). • "Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta. • "Al riparo da urti e lontana da fonti di vibrazione. • "Isolata dai forti campi magnetici prodotti da dispositivi elettrici. • "In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem. • "Dotata di una presa a muro correttamente installata. • "Dotata di spazio sufficiente ad accedere ai cavi di alimentazione, i quali rappresentano il mezzo principale di scollegamento del sistema.

C Safety Information

English

Server Safety Information

This document applies to Intel® server boards, Intel® server chassis and installed peripherals. To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read this document and observe all warnings and precautions in this guide before installing or maintaining your Intel® server product.

In the event of a conflict between the information in this document and information provided with the product or on the website for a particular product, the product documentation takes precedence.

Your server should be integrated and serviced only by technically qualified persons.

You must adhere to the guidelines in this guide and the assembly instructions in your server manuals to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL Listing and other regulatory approvals of the product, and may result in noncompliance with product regulations in the region(s) in which the product is sold.

Safety Warnings and Cautions

To avoid personal injury or property damage, before you begin installing the product, read, observe, and adhere to all of the following safety instructions and information. The following safety symbols may be used throughout the documentation and may be marked on the product and / or the product packaging.

CAUTION	Indicates the presence of a hazard that may cause minor personal injury or property damage if the CAUTION is ignored.
WARNING	Indicates the presence of a hazard that may result in serious personal injury if the WARNING is ignored.
	Indicates potential hazard if indicated information is ignored.
	Indicates shock hazards that result in serious injury or death if safety instructions are not followed.
	Indicates hot components or surfaces.
	Indicates do not touch fan blades, may result in injury.
	Indicates to unplug all AC power cord(s) to disconnect AC power
	Please recycle battery

Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments (such as medical, industrial, residential, alarm systems, and test equipment), other than an ITE application, may require further evaluation.

Site Selection

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean, dry, and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat including direct sunlight and radiators.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect.

Equipment Handling Practices

Reduce the risk of personal injury or equipment damage:

- Conform to local occupational health and safety requirements when moving and lifting equipment.
- Use mechanical assistance or other suitable assistance when moving and lifting equipment.
- To reduce the weight for easier handling, remove any easily detachable components.

Power and Electrical Warnings

Caution: *The power button, indicated by the stand-by power marking, DOES NOT completely turn off the system AC power, 5V standby power is active whenever the system is plugged in. To remove power from system, you must unplug the AC power cord from the wall outlet. Your system may use more than one AC power cord. Make sure all AC power cords are*

unplugged. Make sure the AC power cord(s) is/are unplugged before you open the chassis, or add or remove any non hot-plug components.

Do not attempt to modify or use an AC power cord if it is not the exact type required. A separate AC cord is required for each system power supply.

Some power supplies in Intel® servers use Neutral Pole Fusing. To avoid risk of shock use caution when working with power supplies that use Neutral Pole Fusing.

The power supply in this product contains no user-serviceable parts. Do not open the power supply. Hazardous voltage, current and energy levels are present inside the power supply. Return to manufacturer for servicing.

When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing it from the server.

To avoid risk of electric shock, turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it.

Power Cord Warnings

If an AC power cord was not provided with your product, purchase one that is approved for use in your country.

Caution: *To avoid electrical shock or fire, check the power cord(s) that will be used with the product as follows:*

- *Do not attempt to modify or use the AC power cord(s) if they are not the exact type required to fit into the grounded electrical outlets*
- *The power cord(s) must meet the following criteria:*
- *The power cord must have an electrical rating that is greater than that of the electrical current rating marked on the product.*
- *The power cord must have safety ground pin or contact that is suitable for the electrical outlet.*
- *The power supply cord(s) is/are the main disconnect device to AC power. The socket outlet(s) must be near the equipment and readily accessible for disconnection.*
- *The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground.*

System Access Warnings

Caution: *To avoid personal injury or property damage, the following safety instructions apply whenever accessing the inside of the product:*

- *Turn off all peripheral devices connected to this product.*
- *Turn off the system by pressing the power button to off.*
- *Disconnect the AC power by unplugging all AC power cords from the system or wall outlet.*

- *Disconnect all cables and telecommunication lines that are connected to the system.*
- *Retain all screws or other fasteners when removing access cover(s). Upon completion of accessing inside the product, refasten access cover with original screws or fasteners.*
- *Do not access the inside of the power supply. There are no serviceable parts in the power supply. Return to manufacturer for servicing.*
- *Power down the server and disconnect all power cords before adding or replacing any non hot-plug component.*
- *When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing the power supply from the server.*

Caution: *If the server has been running, any installed processor(s) and heat sink(s) may be hot. Unless you are adding or removing a hot-plug component, allow the system to cool before opening the covers. To avoid the possibility of coming into contact with hot component(s) during a hot-plug installation, be careful when removing or installing the hot-plug component(s).*

Caution: *To avoid injury do not contact moving fan blades. If your system is supplied with a guard over the fan, do not operate the system without the fan guard in place.*

Rack Mount Warnings

The equipment rack must be anchored to an unmovable support to prevent it from tipping when a server or piece of equipment is extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.

Install equipment in the rack from the bottom up, with the heaviest equipment at the bottom of the rack.

Extend only one piece of equipment from the rack at a time.

You are responsible for installing a main power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server(s).

To avoid risk of potential electric shock, a proper safety ground must be implemented for the rack and each piece of equipment installed in it.

Electrostatic Discharge (ESD)

Caution: *ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground -- any unpainted metal surface -- on your server when handling parts.*

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a

conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Other Hazards

Battery Replacement

Caution: *There is the danger of explosion if the battery is incorrectly replaced. When replacing the battery, use only the battery recommended by the equipment manufacturer.*

Dispose of batteries according to local ordinances and regulations.

Do not attempt to recharge a battery.

Do not attempt to disassemble, puncture, or otherwise damage a battery.

Cooling and Airflow

Caution: *Carefully route cables as directed to minimize airflow blockage and cooling problems.*

For proper cooling and airflow, operate the system only with the chassis covers installed. Operating the system without the covers in place can damage system parts. To install the covers:

- *Check first to make sure you have not left loose tools or parts inside the system.*
- *Check that cables, add-in boards, and other components are properly installed.*
- *Attach the covers to the chassis according to the product instructions.*

Laser Peripherals or Devices

Caution: *To avoid risk of radiation exposure and/or personal injury:*

- *Do not open the enclosure of any laser peripheral or device*
- *Laser peripherals or devices have are not user serviceable*
- *Return to manufacturer for servicing*

Deutsch

Sicherheitshinweise für den Server

Das vorliegende Dokument bezieht sich auf Intel® Serverplatinen, Intel® Servergehäuse (Standfuß und Rack) sowie installierte Peripheriegeräte. Es enthält Warnungen und Vorsichtsmaßnahmen zur Vermeidung von Gefahren durch Verletzung, Stromschlag, Feuer und Beschädigungen von Geräten. Lesen Sie diese Dokument daher sorgfältig, bevor Sie Ihr Intel® Serverprodukt installieren oder warten.

Bei Widersprüchen zwischen den hier vorliegenden Angaben und den Informationen im Lieferumfang des Produkts oder auf der Website des betreffenden Produkts hat die Produktdokumentation Vorrang.

Die Integration und Wartung des Servers darf nur durch technisch qualifizierte Personen erfolgen.

Um die Einhaltung der vorhandenen Zulassungen und Genehmigungen für das Produkt zu gewährleisten, sind die Richtlinien in diesem Handbuch sowie die Montageanleitungen in den Serverhandbüchern zu beachten. Verwenden Sie nur die beschriebenen, zugelassenen Komponenten, die im vorliegenden Handbuch angegeben werden. Die Verwendung anderer Produkte oder Komponenten führt zum Erlöschen der UL-Zulassung und anderer Genehmigungen für das Produkt. Dadurch kann das Produkt gegen Produktbestimmungen verstoßen, die im Verkaufsland gelten.

Sicherheitshinweise und Vorsichtsmaßnahmen

Um Verletzungen und Beschädigungen zu vermeiden, sollten Sie vor dem Beginn der Produktinstallation die nachfolgend aufgeführten Sicherheitshinweise und -informationen sorgfältig lesen und befolgen. In dem vorliegenden Handbuch sowie auf dem Produkt und auf der Verpackung werden folgende Sicherheitssymbole verwendet:

VORSICHT	Weist auf eine Gefahrenquelle hin, die bei Nichtbeachtung des VORSICHTSHINWEISES zu leichten Verletzungen bzw. Sachbeschädigungen führen kann.
WARNUNG	Weist auf eine Gefahrenquelle hin, die bei Nichtbeachtung der WARNUNG zu schweren Verletzungen führen kann.
	Weist auf potentielle Gefahr bei Nichtbeachtung der angezeigten Informationen hin.
	Weist auf die Gefahr eines Stromschlags hin, der bei Nichtbeachtung der Sicherheitshinweise zu schweren oder tödlichen Verletzungen führen kann.
	Weist auf Verbrennungsgefahr an heißen Bauteilen bzw. Oberflächen hin.
	Weist darauf hin, daß das Anfassen des Gebläses zu Verletzungen führen kann.
	Bedeutet, alle Netzkabel abzuziehen und das Gerät von der Netzspannung zu trennen.
	Bereiten Sie bitte Batterie auf

Zielbenutzer der Anwendung

Dieses Produkt wurde in seiner Eigenschaft als IT-Gerät getestet, das in Büros, Schulen, Computerräumen und ähnlichen öffentlichen Räumlichkeiten installiert werden kann. Die Eignung dieses Produkts für andere Einsatzbereiche als IT (z. B. Medizin, Industrie, Alarmsysteme oder Prüfgeräte) kann u. U. weitere Tests erfordern.

Standortauswahl

Das System ist für den Betrieb innerhalb normaler Büroumgebungen geeignet. Wählen Sie einen Standort, der folgenden Kriterien entspricht:

- Sauber, trocken und frei von Partikeln in der Luft (außer dem normalen Raumstaub).
- Gut belüftet, nicht in der Nähe von Wärmequellen und keiner direkten Sonnenbestrahlung ausgesetzt.
- Nicht in der Nähe von Vibrations- oder Erschütterungsquellen.
- Abgeschirmt von starken elektromagnetischen Feldern, die durch elektrische Geräte erzeugt werden.
- In gewittergefährdeten Gebieten sollten Sie das System an einen Überspannungsschutz anschließen und bei einem Gewitter die Telekommunikationskabel zum Modem abziehen.
- Eine ordnungsgemäß geerdete Wandsteckdose muß vorhanden sein.
- Ausreichender Freiraum für den Zugang zu den Netzkabeln, da diese die Hauptvorrichtung zum Trennen des Produkts von der Stromversorgung sind.

Handhabung von Geräten

Beachten Sie zur Vermeidung von Verletzungen oder Beschädigungen an den Geräten die folgenden Hinweise:

- Halten Sie beim Transportieren und Anheben von Geräten die örtlichen Gesundheits- und Sicherheitsvorschriften ein.
- Verwenden Sie mechanische oder andere geeignete Hilfsmittel zum Transportieren oder Anheben von Geräten.
- Entfernen Sie alle Komponenten, die sich leicht abnehmen lassen, um das Gewicht zu reduzieren und die Handhabung zu erleichtern.

Warnungen zu Netzspannung und Elektrizität

Vorsicht: Durch Betätigen der mit dem Standby-Symbol gekennzeichneten Netztaste wird das System NICHT vollständig vom Netz getrennt. Es sind weiterhin 5 V aktiv, solange das System eingesteckt ist. Um das System vollständig vom Strom zu trennen, muß das Netzkabel aus der Steckdose abgezogen werden. Das System verfügt möglicherweise über mehrere Netzkabel. Vergewissern Sie sich in diesem Fall, daß alle Netzkabel abgezogen sind. Wenn Sie Komponenten ein- oder ausbauen möchten, die nicht hot-plug-fähig sind, stellen Sie sicher, daß zuvor alle Netzkabel abgezogen sind.

Nehmen Sie keine Änderungen am Netzkabel vor, und verwenden Sie kein Kabel, das nicht genau dem geforderten Typ entspricht. Jedes Netzteil im System muß über ein eigenes Netzkabel angeschlossen werden.

Einige Netzteile von Intel Servern verwenden Nullleitersicherungen. Vorsicht ist geboten im Umgang mit Netzteilen, welche Nullleitersicherungen verwenden, um das Risiko eines elektrischen Schlages zu vermeiden

Das Netzteil in diesem Produkt enthält keine Teile, die vom Benutzer gewartet werden können. Öffnen Sie das Netzteil nicht. Im Netzteil bestehen gefährliche Spannungen, Ströme und Energiequellen. Schicken Sie das Gerät für Wartungsarbeiten an den Hersteller zurück.

Wenn Sie ein hot-plug-fähiges Netzteil austauschen, ziehen Sie dessen Netzkabel ab, bevor Sie es aus dem Server ausbauen.

Zur Vermeidung von Stromschlägen schalten Sie den Server aus, und trennen Sie vor dem Öffnen des Geräts das Netzkabel sowie alle an den Server angeschlossene Telekommunikationssysteme, Netzwerke und Modems.

Hinweis für Netzkabel

Wenn kein Netzkabel mit dem Produkt geliefert wurde, kaufen Sie ein Kabel, das für die

Vorsicht: Prüfen Sie zur Vermeidung von Stromschlag- oder Feuergefahr die mit dem Produkt zu verwendenden Netzkabel wie folgt:

- Nehmen Sie keine Änderungen an einem Netzkabel vor, und benutzen sie es nicht, wenn es nicht genau in die geerdeten Netzsteckdosen paßt.
- Netzkabel müssen die folgenden Anforderungen erfüllen:
- Die Nennbelastbarkeit des Netzkabels muß mindestens so hoch sein wie die am Produkt angegebenen Nennstromaufnahme.
- Das Netzkabel muß einen zur Netzsteckdose passenden Schutzkontakt besitzen.
- Die Netzkabel sind die Hauptvorrichtung zum Trennen des Geräts vom Stromnetz. Die Steckdose muß in der Nähe der Anlage angebracht und gut erreichbar sein.
- Netzkabel müssen an eine ordnungsgemäß geerdete Steckdose angeschlossen sein.

Warnhinweise für den Systemzugang

Vorsicht: Um Verletzungen und Beschädigungen zu vermeiden, sollten Sie vor Arbeiten im Produktinneren folgende Sicherheitsanweisungen beachten:

- Schalten Sie alle am Produkt angeschlossenen Peripheriegeräte aus.
- Schalten Sie das System mit dem Netzschalter aus.
- Trennen Sie das Gerät von der Stromquelle, indem Sie alle Netzkabel vom System bzw. aus der Steckdose ziehen.
- Ziehen Sie alle Kabel und alle an das System angeschlossenen Telekommunikationsleitungen ab.
- Bewahren Sie alle Schrauben und anderen Befestigungselemente gut auf, nachdem Sie die Gehäuseabdeckung entfernt haben. Wenn Sie Ihre Arbeiten im Systeminneren beendet haben, befestigen Sie die Gehäuseabdeckung mit den Originalschrauben bzw. -befestigungselementen.
- Führen Sie keine Arbeiten im Netzteil aus. Das Netzteil enthält keine für den Benutzer wartungsbedürftigen Teile. Schicken Sie das Gerät für Wartungsarbeiten an den Hersteller zurück.
- Schalten Sie den Server aus, und ziehen Sie alle Netzkabel ab, bevor Sie Komponenten ein- oder ausbauen, die nicht hot-plug-fähig sind.
- Wenn Sie ein hot-plug-fähiges Netzteil austauschen, ziehen Sie dessen Netzkabel ab, bevor Sie es aus dem Server ausbauen.

Vorsicht: War Ihr Server in Betrieb, können die installierten Prozessoren und Kühlkörper heiß sein. Sofern Sie keine Hot-Plug-Komponenten ein- oder ausbauen, warten Sie mit dem Abnehmen der Abdeckungen, bis das System abgekühlt ist. Gehen Sie beim Aus- oder Einbauen von Hot-Plug-Komponenten sorgfältig vor, um nicht mit heißen Komponenten in Berührung zu kommen.

Vorsicht: Berühren Sie nicht die rotierenden Lüfterflügel, um Verletzungen zu vermeiden. Falls Ihr System mit einer Lüfterabdeckung besitzt, darf es nicht ohne diese Abdeckung betrieben werden.

Warnhinweise für Racks

Das Geräte-Rack muß auf einer geeigneten, festen Unterlage verankert werden, um ein Umkippen zu vermeiden, wenn ein Server oder andere Geräte herausgezogen werden. Bei der Installation des Racks müssen die Anweisungen des Rack-Herstellers beachtet werden.

Gehen Sie bei der Installation von Geräten im Rack immer von unten nach oben vor, und bauen Sie das schwerste Gerät an der untersten Position im Rack ein.

Ziehen Sie jeweils immer nur ein Gerät aus dem Rack heraus.

Sie müssen für die gesamte Rack-Einheit einen Netztrennschalter einrichten. Dieser Netztrennschalter muß leicht zugänglich sein und über eine Kennzeichnung verfügen, die besagt, daß er die Stromzufuhr zur gesamten Einheit steuert und nicht nur zu den Servern.

Zur Vermeidung von Stromschlaggefahr müssen das Rack selbst und alle darin eingebauten Geräte ordnungsgemäß geerdet sein.

Elektrostatische Entladungen (ESD)

Vorsicht: *Elektrostatische Entladungen können zur Beschädigung von Festplatten, Platinen und anderen Komponenten führen. Daher sollten Sie alle Arbeiten an einer ESD-Workstation ausführen. Steht ein solcher Arbeitsplatz nicht zur Verfügung, erzielen Sie einen gewissen Schutz vor elektrostatischen Entladungen durch Tragen einer Antistatik-Manschette, die Sie während der Arbeit zur Erdung an einem beliebigen unlackierten Metallteil des Computergehäuses befestigen.*

Gehen Sie bei der Handhabung von Platinen immer mit größter Vorsicht vor. Sie können äußerst empfindlich gegenüber elektrostatischer Entladung sein. Halten Sie Platinen nur an den Kanten fest. Legen Sie die Platinen nach dem Auspacken aus der Schutzhülle oder nach dem Ausbau aus dem Server mit der Bauelementseite nach oben auf eine geerdete, statisch entladene Unterlage. Verwenden Sie dazu, sofern verfügbar, eine leitfähige Schaumstoffunterlage, aber nicht die Schutzhülle der Platine. Ziehen Sie die Platine nicht über eine Fläche.

Andere Gefahren

Batterieaustausch

Vorsicht: Wird die Batterie unsachgemäß ausgetauscht, besteht Explosionsgefahr. Verwenden Sie als Ersatz nur die vom Gerätehersteller empfohlene Batterie.

Beachten Sie bei der Entsorgung von Batterien die gültigen Bestimmungen.

Versuchen Sie nicht, eine Batterie aufzuladen.

Versuchen Sie nicht, eine Batterie zu öffnen oder sonstwie zu beschädigen.

Kühlung und Luftstrom

Vorsicht: Verlegen Sie Kabel sorgfältig entsprechend der Anleitung, um Störungen des Luftstroms und Kühlungsprobleme zu vermeiden.

Zur Gewährleistung des ordnungsgemäßen Kühlungs- und Luftstromverhaltens darf das System nur mit angebrachten Gehäuseabdeckungen betrieben werden. Die Inbetriebnahme des Systems ohne Abdeckung kann zur Beschädigung von Systemkomponenten führen. So bringen Sie die Abdeckung wieder an:

- Vergewissern Sie sich zunächst, daß Sie keine Werkzeuge oder Teile im Gehäuse vergessen haben.
- Prüfen Sie, ob Kabel, Erweiterungskarten sowie weitere Komponenten ordnungsgemäß angebracht sind.
- Befestigen Sie die Abdeckungen am Gehäuse des Produkts, wie in dessen Anleitung beschrieben.

Laser-Peripheriegeräte oder -Komponenten

Vorsicht: Beachten Sie zur Vermeidung von Strahlung und Verletzungen die folgenden Hinweise:

- Öffnen Sie keinesfalls das Gehäuse von Laser-Peripheriegeräten oder Laser-Komponenten.
- Laser-Peripheriegeräte oder -Komponenten besitzen keine für den Benutzer wartungsbedürftigen Teile.
- Schicken Sie das Gerät für Wartungsarbeiten an den Hersteller zurück.

Français

Consignes de sécurité sur le serveur

Ce document s'applique aux cartes serveur Intel®, au châssis de serveur Intel® (sur pieds et sur rack) et aux périphériques installés. Pour réduire les risques de dommages corporels, d'électrocution, d'incendie et de dommages matériels, lisez ce document et respectez tous les avertissements et précautions mentionnés dans ce guide avant d'installer ou de mettre à jour votre produit serveur Intel®.

En cas de conflit entre les informations fournies dans ce document et celles livrées avec le produit ou publiées sur le site Web pour un produit particulier, la documentation du produit prime.

Votre serveur doit être intégré et entretenu uniquement par des techniciens qualifiés.

Vous devez suivre les informations de ce guide et les instructions d'assemblage des manuels de serveur pour vérifier et maintenir la conformité avec les certifications et approbations de produit existantes. Utilisez uniquement les composants décrits et réglementés spécifiés dans ce guide. L'utilisation d'autres produits/composants annulera la liste UL et les autres approbations réglementaires du produit, et le produit peut ne pas être conforme aux autres lois et réglementations locales applicables au produit.

Sécurité: avertissements et mises en garde

Pour éviter de vous blesser ou d'endommager votre équipement, lisez et respectez toutes les informations et consignes de sécurité avant de commencer l'installation du produit. Les symboles de sécurité suivants peuvent être utilisés tout au long de cette documentation et peuvent figurer sur le produit ou sur son emballage.

ATTENTION	Indique la présence d'un risque pouvant entraîner des blessures physiques mineures ou endommager légèrement le matériel si la mise en garde n'est pas prise en compte.
AVERTISSEMENT	Indique la présence d'un risque pouvant entraîner des blessures corporelles graves si l'avertissement n'est pas pris en compte.
	Indique un risque potentiel si les informations signalées ne sont pas prises en compte.
	Indique des risques d'électrocution pouvant entraîner des blessures corporelles graves ou mortelles si les consignes de sécurité ne sont pas respectées.
	Signale des composants ou des surfaces soumis à des températures élevées.
	Indique de ne pas toucher aux pales de ventilateur, car cela peut entraîner des blessures.
	Indique de débrancher tous les cordons d'alimentation secteur pour déconnecter l'alimentation.
	Veuillez réutiliser la batterie

Domaines d'utilisation prévus

Ce produit a été testé comme équipement informatique (ITE) et peut être installé dans des bureaux, des écoles, des salles informatiques et des endroits commerciaux similaires. L'utilisation du présent produit dans des catégories et environnements de produits et domaines d'application (par exemple, le domaine médical, industriel, résidentiel, les systèmes d'alarme et les appareils de contrôle) autres qu'ITE doit faire l'objet d'évaluations supplémentaires.

Sélection d'un emplacement

Le système est conçu pour fonctionner dans un environnement standard de bureau. Choisissez un emplacement respectant les conditions suivantes :

- Propre, sec et exempt de particules en suspension (autres que la poussière normale d'une pièce).
- Bien ventilé et à l'écart des sources de chaleur telles que la lumière directe du soleil et les radiateurs.
- À l'écart des sources de vibration ou des chocs physiques.
- Isolé des champs électromagnétiques importants produits par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques, nous vous recommandons de brancher votre système à un suppresseur de surtension et de déconnecter les lignes de télécommunication de votre modem pendant les orages.
- Équipé d'une prise murale reliée à la terre.
- Équipé d'un espace suffisant pour accéder aux cordons d'alimentation secteur, car ils servent de disjoncteur principal d'alimentation du produit.

Pratiques de manipulation de l'équipement

Réduisez le risque de dommages personnels ou matériels :

- Conformez-vous aux exigences de médecine du travail et de sécurité lorsque vous déplacez et soulevez le matériel.
- Utilisez l'assistance mécanique ou toute autre assistance appropriée lorsque vous déplacez et soulevez le matériel.
- Pour réduire le poids en vue de faciliter la manipulation, retirez tout composant amovible.

Alimentation et avertissements en matière d'électricité

Attention: Le bouton d'alimentation, indiqué par le symbole de mise en veille, NE COUPE PAS complètement l'alimentation secteur du système car le courant de veille 5 V reste actif lorsque le système est sous tension. Pour couper l'alimentation du système, vous devez débrancher le cordon d'alimentation secteur de la prise murale. Votre système peut utiliser plusieurs cordons d'alimentation secteur. Assurez-vous que tous les cordons d'alimentation sont débranchés. Vous devez les débrancher avant d'ouvrir le châssis, d'ajouter ou de supprimer un composant non connectable à chaud.

Les alimentations de certains serveurs Intel sont munies de doubles fusibles pôle/neutre: veuillez observer les précautions d'usage afin d'éviter tout risque d'électrocution.

N'essayez pas de modifier ou d'utiliser un cordon d'alimentation secteur s'il ne s'agit pas du type exact requis. Un cordon secteur est requis pour chaque alimentation système.

Le bloc d'alimentation de ce produit ne contient aucun composant réparable par l'utilisateur. N'ouvrez pas le bloc d'alimentation. L'intérieur de celui-ci est soumis à des niveaux dangereux de tension, de courant et d'énergie. Renvoyez-le au fabricant en cas de problème.

Lorsque vous remplacez un bloc d'alimentation à chaud, débranchez le cordon du bloc d'alimentation en cours de remplacement avant de le retirer du serveur.

Pour éviter tout risque d'électrocution, mettez le système hors tension et débranchez les cordons d'alimentation ainsi que les systèmes de télécommunication, réseaux et modems reliés au système avant d'ouvrir ce dernier.

Avertissements sur le cordon d'alimentation

Si aucun cordon d'alimentation secteur n'a été fourni avec votre produit, vous devez vous en procurer un qui soit approuvé pour une utilisation dans votre pays.

Attention: Pour éviter tout risque d'électrocution ou d'incendie, vérifiez les cordons d'alimentation qui seront utilisés avec le produit comme suit:

- N'essayez pas d'utiliser ou de modifier les cordons d'alimentation en CA s'ils ne correspondent pas exactement au type requis pour les prises électriques reliées à la terre.
- Les cordons d'alimentation doivent répondre aux critères suivants :
- Le cordon d'alimentation doit supporter une intensité supérieure à celle indiquée sur le produit.
- Le cordon d'alimentation doit posséder une broche ou un contact de mise à la terre approprié à la prise électrique.
- Les cordons d'alimentation électrique représentent le principal dispositif de déconnexion raccordé à l'alimentation secteur. Les prises de courant doivent se trouver à proximité de l'équipement et être facilement accessibles pour une déconnexion.
- Les cordons d'alimentation doivent être branchés sur des prises électriques correctement reliées à la terre.

Avertissements sur l'accès au système

Attention: Pour éviter de vous blesser ou d'endommager votre équipement, les consignes de sécurité suivantes s'appliquent chaque fois que vous accédez à l'intérieur du produit:

- Mettez hors tension tous les périphériques connectés à ce produit.
- Éteignez le système en appuyant sur le bouton d'alimentation.
- Déconnectez l'alimentation secteur en débranchant tous les cordons d'alimentation secteur du système ou de la prise murale.
- Déconnectez l'ensemble des câbles et lignes de télécommunication qui sont connectés au système.
- Mettez toutes les vis ou autres attaches de côté lorsque vous retirez les panneaux d'accès. Une fois que vous avez terminé d'accéder à l'intérieur du produit, refixez le panneau d'accès avec les vis ou attaches d'origine.
- N'essayez pas d'accéder à l'intérieur du bloc d'alimentation. Il ne contient aucune pièce réparable. Renvoyez-le au fabricant en cas de problème.
- Mettez le serveur hors tension et débranchez tous les cordons d'alimentation avant d'ajouter ou de remplacer tout composant non connectable à chaud.
- Lorsque vous remplacez le bloc d'alimentation à chaud, débranchez le cordon du bloc d'alimentation en cours de remplacement avant de retirer le bloc du serveur.

Attention: Si le serveur a été utilisé, les processeurs et dissipateurs de chaleur installés peuvent être chauds. À moins que vous n'ajoutiez ou ne retiriez un composant connectable à chaud, laissez le système refroidir avant d'ouvrir les panneaux. Pour éviter tout risque d'entrer en contact avec un composant chaud lors d'une installation à chaud, prenez toutes les précautions nécessaires lorsque vous retirez ou installez des composants connectables à chaud.

Attention: Pour éviter de vous blesser, ne touchez pas les pales de ventilateur en mouvement. Si votre système est fourni avec une protection sur le ventilateur, ne mettez pas le système en route sans la protection en place.

Avertissements sur le montage en rack

Le rack doit être fixé à un support inamovible pour éviter qu'il ne bascule lors de l'extension d'un serveur ou d'un élément de l'équipement. Le rack doit être installé conformément aux instructions du fabricant.

Installez les équipements dans le rack en partant du bas, en plaçant le plus lourd en bas du rack.

N'étendez qu'un seul élément de l'équipement à partir du rack à la fois.

Vous êtes responsable de l'installation d'un disjoncteur principal d'alimentation pour la totalité du rack. Ce disjoncteur principal doit être rapidement accessible et doit être étiqueté comme contrôlant toute l'unité, et pas uniquement le ou les serveurs.

Pour éviter tout risque d'électrocution, le rack et chaque élément de l'équipement installé dans le rack doivent être correctement reliés à la terre.

Décharges électrostatiques (ESD)

Attention: *Les décharges électrostatiques (ESD) peuvent endommager les lecteurs de disque dur, les cartes et d'autres pièces. Il est fortement conseillé d'effectuer l'ensemble des procédures décrites à un poste de travail protégé contre les ESD. Au cas où aucun poste de ce type ne serait disponible, protégez-vous contre les ESD en portant un bracelet antistatique relié à la masse du châssis (n'importe quelle surface métallique non peinte) de votre serveur lorsque que vous manipulez les pièces.*

Manipulez toujours les cartes avec précaution. Elles peuvent être extrêmement sensibles aux ESD. Ne tenez les cartes que par leurs bords. Après avoir retiré une carte de son emballage de protection ou du serveur, placez-la sur une surface reliée à la terre, exempte de charge statique, composants orientés vers le haut. Utilisez si possible un tapis de mousse conducteur, mais pas l'emballage de la carte. Veillez à ce que la carte ne glisse sur aucune surface.

Autres risques

Remplacement de la pile

Attention: Il existe un risque d'explosion si la pile n'est pas correctement remplacée. Lors du remplacement de la pile, utilisez uniquement celle recommandée par le fabricant du matériel.

Mettez la pile au rebut en vous conformant aux réglementations locales.

N'essayez pas de recharger une pile.

N'essayez pas de démonter, de percer ou d'endommager la pile d'une quelconque façon.

Refroidissement et ventilation

Attention: Routez les câbles avec précaution comme indiqué pour minimiser les blocages de circulation d'air et les problèmes de refroidissement.

Afin de permettre une ventilation et un refroidissement corrects, ne mettez le système en marche que lorsque les panneaux du châssis sont en place. L'utilisation du système sans les panneaux peut endommager les composants système. Pour installer les panneaux :

- Vérifiez tout d'abord que vous n'avez pas oublié d'outils ou de composants détachés à l'intérieur du système.
- Vérifiez que les câbles, les cartes d'extension et les autres composants sont correctement installés.
- Fixez les panneaux au châssis en suivant les instructions du produit.

Périphériques laser

Attention: Pour éviter tout risque d'exposition aux rayonnements et/ou de dommage personnel:

- N'ouvrez pas l'enceinte d'un périphérique laser.
- Les périphériques laser ne sont pas réparables par l'utilisateur.
- Retournez-les au fabricant en cas de problème.

Español

Información de seguridad del servidor

Este documento se aplica a las tarjetas de servidor de Intel[®], los gabinetes de servidor de Intel[®] (montaje en rack y en pedestal) y los dispositivos periféricos. Para reducir el riesgo de daños corporales, descargas eléctricas, fuego y en el equipo, lea este documento y preste atención a todas las advertencias y precauciones de esta guía antes de instalar o mantener el producto de servidor de Intel[®].

En el caso de que haya diferencias entre la información para un producto en particular contenida en este documento y la información proporcionada con dicho producto o en el sitio Web, la documentación del producto es la que prevalece.

Sólo personal técnico calificado debe montar y prestar los servicios para el servidor.

Debe ceñirse a las directrices de esta guía y a las instrucciones de montaje de los manuales del servidor para asegurar y mantener el cumplimiento con las certificaciones y homologaciones existentes de los productos. Utilice sólo los componentes descritos y homologados que se especifican en esta guía. El uso de otros productos o componentes anulará la homologación UL y otras certificaciones oficiales del producto, pudiendo dejar de ser compatible con las normativas locales de los países en los que se comercializa.

Advertencias y precauciones sobre seguridad

Para reducir la posibilidad de que se produzcan lesiones personales o daños en la propiedad, antes de empezar a instalar el producto, lea, observe y cumpla toda la información e instrucciones de seguridad siguientes. Puede que se utilicen los siguientes símbolos de seguridad en la documentación y es posible que aparezcan en el producto o en su embalaje.

PRECAUCIÓN	Indica la existencia de un riesgo que podría causar lesiones personales o daños en la propiedad leves si no se tiene en cuenta la PRECAUCIÓN.
ADVERTENCIA	Indica la existencia de un riesgo que podría causar lesiones personales graves si no se tiene en cuenta la ADVERTENCIA.
	Indica un riesgo potencial si no se tiene en cuenta la información indicada.
	Indica riesgo de descargas eléctricas que podrían causar lesiones graves o la muerte si no se siguen las instrucciones de seguridad.
	Indica componentes o superficies calientes.
	Indica que no se deben tocar las aspas de los ventiladores, ya que de lo contrario se podrían producir lesiones.
	Indica que es necesario desenchufar los cables de alimentación de CA para desconectar la alimentación de CA
	Recicle por favor la batería

Aplicaciones y usos previstos

Este producto ha sido evaluado como equipo de tecnología informática (ITE) que puede instalarse en oficinas, escuelas, salas de equipos informáticos o lugares de ámbito comercial similares. Es posible que sea necesario llevar a cabo una evaluación adicional para comprobar si este producto es apropiado para otras categorías de productos y entornos además de las aplicaciones informáticas (por ejemplo, soluciones médicas, industriales, residenciales, sistemas de alarma y equipos de pruebas).

Selección de la ubicación

El sistema se ha diseñado para funcionar en un entorno normal de oficinas. Seleccione una ubicación que esté:

- Limpia, seca y libre de macropartículas en suspensión en el aire (que no sean el polvo habitual de la habitación).
- Bien ventilada y alejada de fuentes de calor, incluida la luz solar directa y los radiadores.
- Alejada de fuentes de vibración o de golpes físicos.
- Aislada de campos electromagnéticos producidos por dispositivos eléctricos.
- En zonas propensas a tormentas eléctricas, se recomienda que conecte el servidor a un supresor de sobretensiones y desconecte las líneas de telecomunicaciones al módem durante una tormenta eléctrica.
- Provista de una toma de corriente alterna correctamente conectada a tierra.
- Provista de espacio suficiente para acceder a los cables de la fuente de alimentación ya que constituyen la desconexión principal de la alimentación.

Manipulación del equipo

Reduzca el riesgo de daños personales o en el equipo:

- Respete los requisitos de sanidad y seguridad laborales de su país cuando traslade y levante el equipo.
- Utilice medios mecánicos u otros que sean adecuados al trasladar o levantar el equipo.
- Para que el peso sea menor para manipularlo con más facilidad, extraiga los componentes que sean de fácil extracción.

Advertencias de alimentación y eléctricas

Precaución: El botón de encendido, indicado con la marca del modo de reposo o stand-by, NO DESCONECTA completamente la alimentación de CA del sistema, ya que el modo de reposo de 5 V sigue activo mientras el sistema está enchufado. Para desconectar el sistema debe desenchufar el cable de alimentación de CA de la toma de la pared. Puede usar más de un cable de alimentación de CA con el sistema. Asegúrese de que todos los cables de alimentación de CA estén desenchufados. Asegúrese de que los cables de alimentación de CA estén desenchufado antes de abrir el gabinete, agregar o extraer cualquier componente que no es de conexión en funcionamiento.

Algunas fuentes de alimentación de electricidad de los servidores de Intel utilizan el polo neutral del fuselaje. Para evitar riesgos de choques eléctricos use precauciones al trabajar con las fuentes de alimentación que utilizan el polo neutral de fuselaje.

No intente modificar ni utilizar un cable de alimentación de CA si no es del tipo exacto requerido. Se necesita un cable de CA para cada fuente de alimentación del sistema.

La fuente de alimentación de este producto no contiene piezas que puedan ser reparadas por el usuario. No abra la fuente de alimentación. Dentro de la fuente de alimentación puede haber niveles de tensión, corriente y energía peligrosos. Devuélvala al fabricante para repararla.

Al reemplazar una fuente de alimentación de conexión en funcionamiento, desenchufe el cable de alimentación de la fuente de alimentación que va a reemplazar antes de extraerla del servidor.

Para evitar el riesgo de descargas eléctricas, antes de abrir el servidor, apáguelo, desconecte el cable de alimentación, los sistemas de telecomunicaciones, las redes y los módems conectados al mismo.

Advertencias sobre el cable de alimentación

Si no se ha proporcionado con el producto ningún cable de alimentación de CA, adquiera alguno cuyo uso esté aprobado en su país.

Precaución: Para evitar descargas eléctricas o fuego, revise los cables de alimentación que usará con el producto tal y como se describe a continuación:

- No intente modificar ni utilizar los cables de alimentación de CA si no son exactamente del modelo especificado para ajustarse a las tomas de corriente conectadas a tierra
- Los cables de alimentación deben reunir los siguientes requisitos:
- El cable de alimentación debe disponer de una capacidad nominal de corriente eléctrica mayor que la capacidad especificada en el producto.
- El cable de alimentación debe disponer de una patilla o contacto de conexión a tierra que sea apto para la toma de corriente.
- Los cables de la fuente de alimentación son los dispositivos de desconexión principales a la corriente alterna. El enchufe o enchufes de zócalo deben encontrarse cerca del equipo y el acceso a ellos debe poderse efectuar de forma inmediata con el fin de desconectarlos.

- Los cables de la fuente de alimentación deben estar conectados a los enchufes con una toma de tierra adecuada.

Advertencias el acceso al sistema

Precaución: Para evitar lesiones personales o daños en la propiedad, se aplican las siguientes instrucciones de seguridad siempre que se acceda al interior del producto:

- Apague todos los dispositivos periféricos conectados a este producto.
- Pulse el botón de alimentación para apagar el sistema.
- Desconecte la alimentación de CA desenchufando los cables de alimentación de CA del sistema o de la toma de corriente alterna.
- Desconecte todos los cables y líneas de telecomunicación que estén conectados al sistema.
- Guarde todos los tornillos o elementos de fijación cuando retire las cubiertas de acceso. Cuando termine de operar en el interior del producto, vuelva a colocar los tornillos o los elementos de fijación originales de la cubierta de acceso.
- No acceda al interior de la fuente de alimentación. No hay elementos en la fuente de alimentación que usted pueda reparar y utilizar. Devuélvala al fabricante para repararla.
- Apague el servidor y desconecte todos los cables de alimentación antes de agregar o reemplazar cualquier componente que no es de conexión en funcionamiento.
- Al reemplazar una fuente de alimentación de conexión en funcionamiento, desenchufe el cable de alimentación de la fuente de alimentación que va a reemplazar antes de extraerla del servidor.

Precaución: Si el servidor se ha estado ejecutando, los procesadores y disipadores de calor estarán recalentados. A no ser que esté instalando o extrayendo un componente de conexión en funcionamiento, deje que el sistema se enfríe antes de abrir las cubiertas. Para que no llegue a tocar los componentes que estén calientes cuando esté realizando una instalación de conexión en funcionamiento, tenga cuidado al extraer o instalar los componentes de conexión en funcionamiento.

Precaución: Para evitar posibles daños, no toque las aspas en movimiento de los ventiladores. Si el sistema se le ha suministrado con una protección para el ventilador, asegúrese de que cuando esté funcionando el sistema la protección esté en su sitio.

Advertencias sobre el montaje en rack

El rack para el equipo se debe sujetar con un soporte fijo para evitar que se caiga cuando se extraiga un servidor o una pieza del mismo. El rack debe instalarse siguiendo las instrucciones del fabricante del bastidor.

Instale el equipo en el rack comenzando desde la parte de abajo, con el equipo más pesado en la parte inferior del rack.

Extraiga las piezas del equipo del rack de una a una.

El usuario es el responsable de la instalación de un dispositivo de desconexión de la alimentación principal para toda la unidad del rack. El acceso a este dispositivo de desconexión deberá ser de fácil acceso y deberán incluirse indicaciones que lo identifiquen como el control de alimentación eléctrica de toda la unidad, no sólo de los servidores.

Para evitar el riesgo de descargas eléctricas, deberá instalar una conexión a tierra apropiada para el rack y para cada pieza del equipo instalada en el mismo.

Descarga electrostática (ESD)

Precaución: Las descargas electrostáticas pueden dañar las unidades de disco, las tarjetas y otros componentes. Recomendamos que realice todos los procedimientos en una estación de trabajo protegida contra descargas electrostáticas. En caso de que no haya una disponible, protéjase de alguna forma contra las descargas llevando un brazalete antiestático conectado a la toma de tierra de la carcasa (cualquier superficie de metal que no esté pintada) del servidor cuando manipule las piezas.

Manipule siempre las tarjetas con el máximo cuidado. Pueden ser sumamente sensibles a las descargas electrostáticas. Sujételas sólo por los bordes. Una vez extraída la tarjeta de su envoltorio de protección o del servidor, colóquela con el lado de los componentes hacia arriba sobre una superficie con toma de tierra y sin carga estática. Utilice una almohadilla de espuma conductora si dispone de ella, pero nunca el envoltorio de la tarjeta. No deslice la tarjeta sobre ninguna superficie.

Sustitución de la batería

Precaución: Existe el peligro de explosión si la batería no se reemplaza correctamente. Al reemplazar la batería, utilice sólo la batería recomendada por el fabricante del equipo.

Deseche las baterías respetando la normativa local.

No intente recargar la batería.

No intente desmontar, pinchar o causar cualquier otro desperfecto a una batería.

Enfriamiento y circulación de aire

Precaución: El tendido de los cables debe realizarse cuidadosamente tal y como se le indica para reducir al mínimo los problemas de obstrucción de la ventilación y de refrigeración.

Para conseguir una refrigeración y corriente de aire adecuadas, compruebe que cuando sistema esté funcionando, las cubiertas de la carcasa están instaladas. Si utiliza el sistema sin las cubiertas, podría dañar sus componentes. Para instalar las cubiertas:

- *Compruebe primero que no ha dejado herramientas o piezas sueltas dentro del sistema.*
- *Compruebe que los cables, tarjetas adicionales y otros componentes están instalados correctamente.*
- *Sujete las cubiertas a la carcasa siguiendo las instrucciones del producto.*

Periféricos o dispositivos láser

Precaución: Para evitar el riesgo de la exposición a radiaciones o de daños personales:

- *No abra la caja de ningún periférico o dispositivo láser*
- *Los periféricos o dispositivos láser no pueden ser reparados por el usuario*
- *Haga que el fabricante los repare.*

简体中文

服务器安全信息

本文档适用于 Intel® 服务器主板、Intel® 服务器机箱（基座和机架固定件）和已安装的外设。为减少人身伤害、电击、火灾以及设备毁坏的危险，请在安装或维护 Intel® 服务器产品之前阅读本文档并遵循本指南中的所有警告和预防措施。

如果本文档中的信息与特定产品的随附信息或 Web 站点信息之间存在不一致，请以产品文档为准。

服务器须由合格的技术人员进行集成和维护。

必须遵守本指南的规定和服务器手册的装配指导，以确保符合现有的产品认证和审批。仅使用本指南中描述和规定的指定组件。使用其他产品 / 组件将使产品的 UL 认证和其他管理审批无效，并可能导致产品不符合销售地的产品法规。

安全警告与注意事项

为避免人身伤害与财产损失，安装本产品之前，请阅读以下所有安全指导和信息。下面所列的安全符号可能在整个文档中使用并可能标注于产品和 / 或产品包装之上。

注意	表示如果无视此“ ??? 项” ?????? 轻微人身伤害或财产损失的危险。
警告	表示如果无视此“ ?? ” ?????? 严重人身伤害的危险。
	表示如果无视所示信息，即存在潜在的危险。
	表示如果不遵守安全指导，存在可导致严重伤害或死亡的电击危险。
	表示灼热组件或表面。
	表示请勿触摸风机叶片，否则可能致伤。
	表示拔下所有交流电线，断开交流电源

预期应用使用

根据评估，本产品为信息技术设备（ITE），可安装在办公室、学校、计算机房和类似的商业场所。本产品对于非 ITE 应用的其他产品种类和环境（如医疗、工业、住宅、报警系统和测试设备）的适用性尚有待进一步的评估。

场地选择

本系统专为在典型办公环境运行而设计。请选择符合以下条件的地点：

- 清洁、干燥，无气载微粒（而非一般的室内尘埃）。
- 通风良好，远离热源（包括直接日晒和散热器）。
- 远离振动源或物理震动。
- 与电气设备产生的强大电磁场隔离。
- 在易受闪电袭击的地区，我们建议将系统插入电涌抑制器并在闪电期间断开通信线路与调制解调器之间的连接。
- 提供正确接地的墙壁插座。
- 提供足够的空间，以便拿取电源供应线，因为这是本产品的主要电源断开器。

设备操作规范

减少人身伤害或设备受损的危险：

- 移举设备时遵守当地的职业健康与安全要求。
- 借助机械手段或其他合适的手段移举设备。
- 拆除一切易分离组件，以降低重量并方便操作。

电源与电气警告

注意事项

电源按钮（如待机电源标记所示）并不能完全关闭系统的交流电源，只要系统已接通电源，就存在 5V

待机电源。要从系统切断电源，须从墙壁电源插座中拔下交流电线。您的系统可能不止使用一根交流电线。请确保所有的交流电线都已拔下。打开机箱或增加或删除任何热插拔组件之前，确保交流电线已拔下。

若非所需的确切类型，请勿尝试修改或使用交流电线。系统的每个电源供应设备都需要一根单独的交流电线。

本产品的电源供应设备包含非用户维修部件。请勿打开电源供应设备。电源供应设备包含非常危险的电压级、电流级和能量级。请与生产商联系维修事宜。

替换热插拔电源供应设备时，请先拔下需替换的电源供应设备上的电源线，再将其从服务器上移除。

为避免电击，请在打开服务器之前，关闭服务器并断开服务器上连接的电源线、电信系统、网络 and 调制解调器。

电源线警告

如果产品未提供交流电线，请购买一根您所在国家批准使用的交流电线。

注意事项

为避免电击或火灾危险，请按如下所述对产品所用的电源线进行检查：

- 若非所需的符合接地插座的确切类型，请勿尝试修改或使用交流电线
- 电源线须符合以下标准：
 - 电源线的电气额定值须大于产品上标注的电流额定值。
 - 电源线须拥有适合插座的安全接地插头或触点。
- 电源线为交流电源的主要断开设备。插座须靠近设备并可随时断开。
- 电源线须插入所提供的拥有合适接地的插座。

系统使用警告

注意事项

为避免人身伤害或财产损失，无论何时检查产品内部，以下安全指导都适用：

- 关闭所有与本产品相连的外设。
- 按下电源按钮至关闭状态，关闭系统。
- 从系统或墙壁插座上拔下所有交流电线，断开交流电源。
- 断开与系统相连的所有线缆和通信线路。
- 卸除舱口盖时，保留所有螺钉及其他紧固件。完成产品内部检查之后，请用螺钉或紧固件重新固定舱口盖。
- 请勿打开电源供应设备。电源供应设备内没有可维修部件。请与生产商联系维修事宜。
- 增加或替换任何非热插拔组件之前，请关闭服务器电源并断开所有电源线。
- 替换热插拔电源供应设备时，请先拔下需替换的电源供应设备上的电源线，然后再从服务器上移除电源供应设备。

注意事项

如果服务器一直在运行，任何已安装的处理器和吸热设备都可能很热。除非要增加或移除热插拔组件，否则请待系统冷却后再开盖。为避免在热插拔组件安装过程中接触灼热组件，移除或安装热插拔组件时务须小心。

注意事项

为避免受伤，请勿触摸运转的风机叶片。如果系统的风机上配有防护装置，请勿卸下风机防护装置运行系统。

机架固定件警告

设备的机架须固定在稳固的支座上，以防从中安装服务器或设备时倒塌。须按照机架生产商提供的安装说明进行安装。

从下往上将设备安装在机架上，最重的设备安装在机架的最底层。

一次只从机架上安装一件设备。

您须负责安装整个机架装置的主要电源断开设备。此主要断开设备须随时可用，且须标明为控制整个装置（而不仅限于服务器）的电源。

为避免潜在的电击危险，须对机架及其上所安装的每一件设备实行正确的安全接地。

静电放电（ESD）

注意事项

ESD 会损坏磁盘驱动器、主板及其他部件。我们建议您执行 ESD 工作站的所有步骤。如果没有 ESD

工作站，则采取一些静电放电保护措施，操作部件时，戴上与服务器上的机箱接地或任何未喷漆金属表面连接的防静电腕带。

操作主板时始终保持小心。它们可能对 ESD

非常敏感。拿持主板时只接触边缘。从保护包装中或从服务器上取出主板后，请将主板组件侧面朝上放置于无静电的接地表面上。请使用导电泡沫垫（若有），不要使用主板包装。请勿将主板在任何表面上滑动。

其他危险

替换电池



注意事项

不正确替换电池可能导致爆炸危险。替换电池时，请只使用设备生产商推荐使用的电池。

请按当地法规处置电池。

请勿对电池充电。

请勿拆卸、刺穿或以其他方式损坏电池。

冷却和气流



注意事项

按照说明小心布置线缆，尽量减少气流阻塞和冷却问题。

为保证适当的冷却和气流，运行系统时请确保机箱盖已安装。未安装机箱盖即运行系统可能导致系统部件受损。安装机箱盖的步骤如下：

- 首先检查并确保系统内没有遗留的未固定工具或部件。
- 检查线缆、内插板和其他组件已正确安装。
- 按产品说明安装机箱盖。

激光外设或激光设备



注意事项

为避免幅射暴露和 / 或人身伤害：

- 请勿打开任何激光外设或激光设备的外壳
- 激光外设或激光设备为非用户维修设备

请与生产商联系维修事宜