# Intel® Blade Server Ethernet Switch Modules SBCEGBESW1 and SBCEGBESW10 EWS User Guide

**A Guide for System Administrators of Intel® Server Products**

Intel Order Number D67147-002

**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.



This product includes software developed by the OpenSSL Project for use in the Open SSL Toolkit (http://wwww.openssl.org/).

This product includes software developed by the NetBSD Foundation, Inc., and its contributors.

This product includes crytographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SECURE SOCKETS LAYER DELIVERABLE: The Secure Sockets Layer shall constitute “OpenSSL Deliverables” hereunder. The OpenSSL Deliverables are provided to Licensee under the terms of this Agreement and the OpenSSL License Agreement (the “OpenSSL License”), and any use of such OpenSSL Deliverables shall comply with the terms and conditions of the OpenSSL License and this Agreement. A copy of the OpenSSL License is available in the license.txt file accompanying the Deliverables and at http://www.openssl.org/source/license.html.

SSH PROTOCOL SUITE OF NETWORK CONNECTIVITY TOOLS DELIVERABLES: The SSH protocol suite of network connectivity tools shall constitute “Open SSH Deliverables” hereunder. The OpenSSH Deliverables are provided to Licensee under the terms of this Agreement and the BSD License (the “BSD License”), and any use of such OpenSSH Deliverables shall comply with the terms and conditions fo the BSD License and this Agreement. A copy of the BSD License is set forth as below:



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

4. Neither the name of Marvell nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# *Safety Precautions*

## Important Safety Instructions

Read all caution and safety statements in this document before performing any of the instructions.

## Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warnund Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen.

## Consignes de sécurité

Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction.

## Instrucciones de seguridad importantes

Lea todas las declaraciones de seguridad y precaución de este documento antes de realizar cualquiera de las instrucciones.

## 重要安全指导

*在执行任何指令之前，请阅读本文档中的所有注意事项及安全声明。 和/或* 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

**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 system, you must unplug the AC power cord from the wall outlet. 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 server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server 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 chapter only 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.

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
(安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si prečtěte prírůcků bezpecnoštních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet.
- Connect to properly wired outlets any equipment that will be attached to this product.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

| To Connect: | To Disconnect: |
|---|---|
| 1. Turn everything OFF. | 1. Turn everything OFF. |
| 2. First, attach all cables to devices. | 2. First, remove power cords from outlet. |
| 3. Attach signal cables to connectors. | 3. Remove signal cables from connectors. |
| 4. Attach power cords to outlet. | 4. Remove all cables from devices. |
| 5. Turn device ON. | |

Statement 2:

CAUTION

When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

DANGER

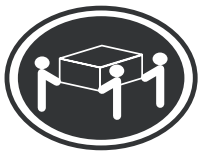
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical

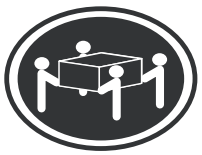
Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaite
Appareil À Laser de Classe 1

Statement 3:

≥ 18 kg (39.7 lb)



≥ 32 kg (70.5 lb)



≥ 55 kg (121.2 lb)

CAUTION:

Use safe practices when lifting.

Statement 4:

CAUTION:

If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to an easily accessible power source.

Statement 5:

CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 6:

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements.

Statement 7:

CAUTION:

Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the following label is attached.

# 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 of this User Guide:

- **Safety Precautions** — Provides safety precautions for using the device. It is recommended to read the safety precautions before using the device.
- **Section 1, Device Description** — Provides a device description, including the port descriptions, supported RFCs and standards, and a brief description of the device features.
- **Section 2, Installing and Removing the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10** — Provides instructions for unpacking and installing the device.
- **Section 3, Information Panel LEDs and External Ports** — Provides a description of device LEDs and external ports.
- **Section 4, 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 5, Managing Device Information** — Provides information about opening the device zoom view, defining general system information, and enabling Jumbo frames.
- **Section 6, Configuring Device Security** — Provides information about configuring device security for management security, traffic control, and network security.
- **Section 7, Configuring Ports** — Provides information about configuring ports.
- **Section 8, Aggregating Ports** — Provides information about configuring Link Aggregated Groups and LACP.

- **Section 9, Configuring VLANs** — Provides information about configuring and managing VLANs, including information about GARP and GVRP, and defining VLAN groups.
- **Section 10, Configuring IP Information** — Provides information about defining device IP addresses, ARP, and Domain Name Servers.
- **Section 11, Defining the Forwarding Database and Static Routes** — Provides information about defining Static Forwarding Database Entries and Dynamic Forward Database Entries.
- **Section 12, Configuring Multicast Forwarding** — Provides information about Multicast Forwarding.
- **Section 13, Configuring Spanning Tree** — Provides information about configuring Spanning Tree Protocol and the Rapid Spanning Tree Protocol.
- **Section 14, Configuring SNMP** — Provides information about defining SNMP v1,v2c, and v3 management, including SNMP filters and notifications.
- **Section 15, Configuring Quality of Service (QoS)** — Provides information about configuring Quality of Service on the device.
- **Section 16, Managing System Files** — Provides information about downloading, uploading, and copying system files.
- **Section 17 Managing System Logs** — Provides information about enabling and defining system logs.
- **Section 18, Managing Device Diagnostics** — Provides information on Configuring Port Mirroring, Ethernet Ports, and Viewing Optical Transceivers.
- **Section 19, Configuring System Time** — Provides information about configuring system time, including Daylight Savings Time parameters and Simple Network Time Protocol (SNTP) parameters.
- **Section 20, Viewing Statistics** — Provides information about viewing device statistics, including RMON statistics, device history events, and port and LAG utilization statistics.
- **Appendix A, Getting Help** — Provides information for getting technical support.
- **Appendix B, Regulatory and Compliance Information** — Provides information about safety compliances, compliance markings, product certifications, electromagnetic compatibility, RoHS, and recycling.
- **Appendix C, Troubleshooting** — Provides information for troubleshooting the device.
- **Appendix D, Intel**® Server Issue Report Form — Provides a customer service form for reporting problems with the device.

# Intended Audience

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

# Contents

**Safety Precautions ..... iii**
Important Safety Instructions ..... iii
Wichtige Sicherheitshinweise ..... iii
Consignes de sécurité ..... iii
Instrucciones de seguridad importantes ..... iii

**Preface ..... ix**
User Guide Overview ..... ix
Intended Audience ..... x

**Device Description ..... 1**
Specifications and Features ..... 1
Ports ..... 1
Standards ..... 1
Network Cable Support ..... 3
Device Features ..... 3

**Installing and Removing the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10 ..... 9**
Overview ..... 9
Package Contents ..... 9
Unpacking the Switch Module ..... 9
Hardware Components ..... 10
Configuration Information Requirements ..... 11
Installation Guidelines ..... 12
System Reliability Considerations ..... 12
Installing the Switch Module ..... 12

**Information Panel LEDs and External Ports ..... 17**
Information Panel ..... 17
LEDs ..... 18

**Getting Started ..... 19**
Starting the Embedded Web Interface ..... 19
Understanding the Embedded Web Interface ..... 21
Device Representation ..... 22
Using the Embedded Web Interface Management Buttons ..... 23
Using Screen and Table Options ..... 24
Adding Configuration Information ..... 24
Modifying Configuration Information ..... 25
Deleting Configuration Information ..... 25

Resetting the Device ..... 26
Logging Off from the Device ..... 26

**Managing Device Information ..... 27**

**Configuring Device Security ..... 29**
Configuring Management Security ..... 29
Configuring Authentication Methods ..... 29
Configuring Passwords ..... 47
Configuring Network Security ..... 52
Network Security Overview ..... 52
Defining Network Authentication Properties ..... 54
Defining Port Authentication ..... 55
Configuring Traffic Control ..... 61
Defining Access Control Lists ..... 66

**Configuring Ports ..... 77**

**Aggregating Ports ..... 81**
Configuring LAGs ..... 82
Defining LAG Members ..... 84
Configuring LACP ..... 86

**Configuring VLANs ..... 89**
Defining VLAN Properties ..... 90
Defining VLAN Membership ..... 92
Defining VLAN Interface Settings ..... 94
Defining VLAN Groups ..... 95
Defining VLAN MAC Based Groups ..... 96
Defining VLAN Subnet Based Groups ..... 98
Defining VLAN Protocol Based Groups ..... 100
Mapping Groups to VLANs ..... 102
Defining GARP ..... 104
Defining GVRP ..... 106

**Configuring IP Information ..... 109**
Configuring IP Interfaces ..... 109
Defining IP Addresses ..... 109
Defining ARP Settings ..... 111
Configuring Domain Name Servers ..... 112
Defining DNS Servers ..... 113
Defining DNS Host Mapping ..... 115

**Defining the Forwarding Database and Static Routes ..... 117**
Defining Static Forwarding Database Entries ..... 117
Defining Dynamic Forwarding Database Entries ..... 119

**Configuring Multicast Forwarding ..... 121**
Defining IGMP Snooping ..... 121
Defining Multicast Groups ..... 123
Defining Multicast Forward All Settings ..... 126

**Configuring Spanning Tree ..... 129**
Defining Classic Spanning Tree ..... 130
Defining Spanning Tree Interface Settings ..... 132
Defining Rapid STP ..... 136
Defining Multiple STP ..... 138
Defining Multiple STP Instance To VLAN Settings ..... 139
Defining Multiple STP Instance Settings ..... 140
Defining Multiple STP Interface Settings ..... 141

**Configuring SNMP ..... 145**
SNMP v1 and v2c ..... 145
SNMP v3 ..... 145
Configuring SNMP Security ..... 146
Defining SNMP Security ..... 146
Defining SNMP Views ..... 148
Defining SNMP Group Profiles ..... 149
Defining SNMP Group Members ..... 152
Defining SNMP Communities ..... 155
Configuring SNMP Notifications ..... 158
Defining SNMP Notification Global Parameters ..... 159
Defining SNMP Notification Recipients ..... 160
Defining SNMP Notification Filters ..... 162

**Configuring Quality of Service (QoS) ..... 165**
Quality of Service Overview ..... 165
VPT Classification Information ..... 165
CoS Services ..... 165
Defining General QoS Settings ..... 166
Configuring CoS General Parameters ..... 166
Restoring Factory Default QoS Interface Settings ..... 168
Defining Queues ..... 169
Configure Bandwidth Settings ..... 170
Configuring QoS Mapping ..... 171
Mapping DSCP Values to Queues ..... 173
Configuring Basic QoS Settings ..... 174
Configuring Basic General Parameters ..... 174
Configuring DSCP Rewrite ..... 175
Configuring Advanced QoS Settings ..... 177
Defining Policy Properties ..... 177
Defining Policy Profiles ..... 182

**Managing System Files ..... 189**
File Management Overview ..... 189
Downloading System Files ..... 190
Firmware Download ..... 191
Configuration Download ..... 191
Uploading System Files ..... 192
Software Image Upload ..... 192
Configuration Upload ..... 193
Copying Files ..... 194
Restoring the Default Configuration File ..... 195
Activating Image Files ..... 196

**Managing System Logs ..... 197**
Enabling System Logs ..... 198
Viewing the FLASH Logs ..... 200
Clearing FLASH Logs ..... 201
Viewing the Device Memory Logs ..... 201
Defining Servers Log Parameters ..... 202

**Managing Device Diagnostics ..... 205**
Configuring Port Mirroring ..... 205
Ethernet Ports Diagnostics ..... 208

**Configuring System Time ..... 211**
Configuring Daylight Savings Time ..... 211
Configuring SNTP ..... 216
Polling for Unicast Time Information ..... 216
Polling for Anycast Time Information ..... 216
Broadcast Time Information ..... 217
Defining SNTP Global Settings ..... 217
Defining SNTP Authentication ..... 221
Adding an SNTP Interface ..... 223

**Viewing Statistics ..... 225**
Viewing Interface Statistics ..... 225
Viewing Device Interface Statistics ..... 225
Resetting Interface Statistics Counters ..... 227
Resetting Etherlike Statistics Counters ..... 229
Resetting GVRP Statistics Counters ..... 231
Viewing EAP Statistics ..... 232
Managing RMON Statistics ..... 233
Resetting RMON Statistics Counters ..... 236
Configuring RMON History ..... 236

**A. Getting Help ..... 247**
World Wide Web ..... 247

Telephone ..... 247

**B. Troubleshooting ..... 251**

Problems following Initial System Installation ..... 251
First Steps Checklist ..... 251
Hardware Diagnostic Testing ..... 251
Verifying Proper Operation of Key System Lights ..... 252
Confirming Loading of the Operating System ..... 252
Specific Problems and Corrective Actions ..... 252
Power Light Does Not Light ..... 252
No Characters Appear on Screen ..... 252
Characters Are Distorted or Incorrect ..... 253
System Cooling Fans Do Not Rotate Properly ..... 253
Cannot Connect to a Server ..... 253
Problems with Network ..... 254
Problems with Application Software that Ran Correctly Earlier ..... 254

**C. Regulatory and Compliance Information ..... 255**

Product Regulatory Compliance ..... 255
Product Safety Compliance ..... 255
Certifications / Registrations / Declarations ..... 256
Product Regulatory Compliance Markings ..... 256
Electromagnetic Compatibility Notices ..... 257
FCC (USA) ..... 257
ICES-003 (Canada) ..... 258
Europe (CE Declaration of Conformity) ..... 258
VCCI (Japan) ..... 258
RRL (Korea) ..... 259
Restriction of Hazardous Substances (RoHS) Compliance ..... 259
End-of-Life / Product Recycling ..... 260

**D. Intel® Server Issue Report Form ..... 261**

**E. Installation/Assembly Safety Instructions ..... 265**

English ..... 265
Deutsch ..... 267
Français ..... 270
Español ..... 272
Italiano ..... 274

**F. Safety Information ..... 277**

English ..... 277
Server Safety Information ..... 277
Safety Warnings and Cautions ..... 277
Intended Application Uses ..... 278
Site Selection ..... 278

Equipment Handling Practices ..... 278
Power and Electrical Warnings ..... 278
System Access Warnings ..... 279
Rack Mount Warnings ..... 280
Electrostatic Discharge (ESD) ..... 280
Other Hazards ..... 281
Sicherheitshinweise für den Server ..... 282
Sicherheitshinweise und Vorsichtsmaßnahmen ..... 282
Zielbenutzer der Anwendung ..... 283
Standortauswahl ..... 283
Handhabung von Geräten ..... 283
Warnhinweise für den Systemzugang ..... 285
Elektrostatische Entladungen (ESD) ..... 286
Andere Gefahren ..... 287
Français ..... 288
Consignes de sécurité sur le serveur ..... 288
Sécurité: avertissements et mises en garde ..... 288
Domaines d'utilisation prévus ..... 289
Sélection d'un emplacement ..... 289
Pratiques de manipulation de l'équipement ..... 289
Décharges électrostatiques (ESD) ..... 292
Autres risques ..... 293
Información de seguridad del servidor ..... 294
Advertencias y precauciones sobre seguridad ..... 294
Aplicaciones y usos previstos ..... 294
Selección de la ubicación ..... 295
Manipulación del equipo ..... 295
Advertencias el acceso al sistema ..... 297
Descarga electrostática (ESD) ..... 298

# 1 Device Description

This document provides basic information on how to install and establish a basic configuration for the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/ SBCEGBESW10. For the latest updates on documentation and software, check the Intel support website at http://support.intel.com.

***Note:*** *Support for a 3rd or 4th Ethernet switch module requires installation of an Intel® Blade Server Ethernet Expansion Card SBGBE.*

The Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10 is installed in one of the I/O module bays of the Intel® Blade Server Chassis SBCE, which is a system that supports up to 14 server modules and up to four Ethernet switch modules.

***Note:*** *Before proceeding, read the release notes for this product. The release notes can be downloaded from the Intel support website at http://support.intel.com.*

For more information about the components of the information panel, see Chapter 3 “Information Panel LEDs and External Ports” on page 17. For more information about the MAC address, see “IP addresses and SNMP community names” on page 21.

## Specifications and Features

### Ports

- Six external 1000BASE-T ports for making 10/100/1000 Mbps connections to a backbone, end stations, and servers
- Fourteen internal full-duplex gigabit ports, one connected to each of the blade servers
- Two internal full-duplex 100 Mbps ports connected to the management modules
- Two XFP10Gbps ports

### Standards

The following standards apply to the switch module.

- Switching Support
- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3 Auto-negotiation
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.3z Gigabit Ethernet

- IEEE 802.3ab 1000BASE-T
- IEEE 802.1Q Tagged VLAN
- IEEE 802.1p Priority
- GARP
- GVRP
- IEEE 802.3ac - VLAN Tagging
- IEEE 802.3ad - Link Aggregation
- IEEE 802.1s - Spanning Tree
- IEEE 802.1w - Rapid Spanning Tree
- IEEE 802.1X - Port Based Authentication
- IEEE 802.3X - Flow Control
- RFC 768 - UDP
- RFC 783 - TFTP
- RFC 791 - IP
- RFC 792 - ICMP
- RFC 793 - TCP
- RFC 826 - ARP
- RFC 2131 - DHCP Client
- RFC 2865 - RADIUS Client
  - RFC 2866 - RADIUS Accounting
  - RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
  - RFC 2869 - RADIUS Extensions
  - RFC 2869bis - RADIUS Support for Extensible Authentication Protocol (EAP)
- Advanced Layer 2 Functionality:
  - Broadcast Storm Recovery
  - Multicast Storm Recovery
  - Port Mirroring
  - IGMP Snooping
  - Static MAC Filtering
- System Facilities
  - Event and Error Logging Facility
  - Run-time and Configuration Download Capability
  - PING Utility
- Quality of Service (QOS) Support

- Bandwidth Provisioning
  - Per Interface
- Access Control Lists
  - Source IP•Destination IP
  - Source L4 Port
  - Destination L4 Port

## Network Cable Support

- 10BASE-T
  - UTP Category 3, 4, 5 (100 meters maximum)
  - 100-ohm STP (100 meters maximum)
- 100BASE-TX
  - UTP Category 5, 5e (100 meters maximum)
  - EIA/TIA-568B 100-ohm STP (100 meters maximum)
  - XFP 10Gbps

## Device Features

The following table contains information regarding the software and hardware features:

| Feature | Description |
|---|---|
| Access Control Lists | *Access Control Lists* (ACL) provides rules for either forwarding or blocking network traffic. Users can define ACLs to enforce security. This is done by defining classification rules and assigning an action per rule. An ACL can be assigned to an ingress interface (port or VLAN). |
| Address Resolution Protocol | IP routing generally utilizes routers and Layer 3 switches to inter-communicate using various routing protocols to discover network topology and define Routing tables. Device Next-Hop MAC addresses are automatically derived by ARP. This includes directly attached end systems. Users can override and supplement this by defining additional ARP Table entries. |
| Automatic Aging for MAC Addresses | *Media Access Control Address* (MAC) addresses from which no traffic is received for a given period are aged out. This prevents the *Bridging Table* from overflowing. |
| Back Pressure Support | On half-duplex links, the receiving port prevents buffer overflows, by occupying the link so that it is unavailable for additional traffic. |
| BootP and DHCP Clients | *Dynamic Host Configuration Protocol* (DHCP) enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension to BootP. |

| Feature | Description |
|---|---|
| BootP Relay | BootP enables a device to solicit and receive configuration data from servers. BootP relies on UDP broadcasts as the underlying transport mechanism. If the intended BootP server is not directly attached to a client's broadcast domain, a BootP relay service enables the client to reach the server. |
| Class Of Service | The IEEE 802.1p signalling technique is an OSI Layer 2 standard for marking and prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is classified and sent to the destination. No bandwidth reservations or limits are established or enforced. 802.1p is a spin-off of the 802.1Q (Vlans) standard. 802.1p establishes eight levels of priority, similar to the IP Precedence IP Header bit-field. |
| Command Line Interface | *Command Line Interface* (CLI) syntax and semantics conform as much as possible to common industry practice. CLI is composed of mandatory and optional elements. The CLI interpreter provides command and keyword completion to assist user and shorten typing. |
| DNS Client | *Domain Name System* (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the name into a numeric IP address. For example, www.ipexample.com is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses. |
| Fast Link | STP can take up to 30-60 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies where forwarding loops do not occur. |
| Flow Control Support (IEEE 802.3X) | Flow control enables lower speed devices to communicate with higher speed devices, requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows. |
| GVRP | *GARP VLAN Registration Protocol* (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the device registers and propagates VLAN membership on all ports that are part of the active underlying Spanning Tree Protocol Features topology. |
| Hardware Watchdog Support | The device enables detection and corrective action for instances where the device software stops responding. |
| ICMP Messages | *Internet Control Message Protocol* (ICMP) messages are used for OOB messages related to network operation or malfunction |
| IGMP Snooping | *Internet Group Management Protocol* (IGMP) Snooping examines IGMP frame contents, when they are forwarded by the device from stations to an upstream Multicast router. From the frame, the device identifies stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames. |

| Feature | Description |
|---|---|
| Link Aggregated Groups | Up to seven Aggregated Links may be defined, each with up to four member ports, to form a single *Link Aggregated Group* (LAG). This enables:<br>• Fault tolerance protection from physical link disruption<br>• Higher bandwidth connections<br>• Improved bandwidth granularity<br>• High bandwidth server connectivity<br>LAG is composed of ports with the same speed, set to full-duplex operation. |
| Link Aggregation and LACP | *Link Aggregation Control Protocol* (LACP) uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds and monitors the port binding to aggregators within the system. |
| Locked Port Support | Locked Port increases network security by limiting access on a specific port only to users with specific MAC addresses. These addresses are either manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked |
| Longest Prefix Match Support | Within the CIDR recommendation, longest prefix matches are used primarily to determine the best next-hop route for a packet based on the destination address contained in the packet header. Since IP addresses are generally assigned in a manner that reflects the topology of the network, the result of a longest prefix match reflects the shortest route to the destination. There may be many entries matching a given address, and the LPM algorithm entails searching for a matching entry with the longest prefix. |
| MAC Address Capacity Support | The device supports up to 16K MAC addresses. The device reserves specific MAC addresses for system use. |
| MAC Multicast Support | Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 multicast service is where a single frame is addressed to a specific multicast address, and copies of the frame transmitted to relevant port are created to receive its packets. |
| MDI/MDIX Support | The device supports auto-detection between crossed and straight-through cables. Standard wiring for end stations is *Media-Dependent Interface* (MDI) and the standard wiring for hubs and switches is known as *Media-Dependent Interface with Crossover* (MDIX). |
| Multiple Spanning Tree | *Multiple Spanning Tree* (MSTP) operation maps VLANs into STP instances. MSTP provides differing load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths |

| Feature | Description |
|---|---|
| Port Based Authentication | Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the *Remote Authentication Dial In User Service* (RADIUS) server using the *Extensible Authentication Protocol* (EAP). |
| Port Based Virtual LANs (VLANs) | Port-based VLANs classify incoming packets to VLANs based on their ingress port. |
| Port Mirroring | Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port. |
| Quality of Service (QoS) Support | Network traffic is usually unpredictable, and the only basic assurance that can be offered is Best Effort traffic delivery. To overcome this challenge, *Quality of Service* (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance. |
| RADIUS | *Remote Authentication Dial In User Service* (RADIUS) is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information. |
| Rapid Spanning Tree | Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forward traffic. Rapid Spanning Tree (RSTP) detects and uses of network topologies to enable faster convergence, without creating forwarding loops |
| Remote Monitoring | *Remote Monitoring* (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network. |
| Self-Learning MAC Addresses | The device enables automatic MAC addresses learning from incoming packets. |
| SNMP Alarms and Trap Logs | The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List. |
| SNMP Version 1 and Version 2 | *Simple Network Management Protocol* (SNMP) over the UDP/IP protocol. To control access to the system, a list of community entries is defined, each of which consists of a community string and its access privileges. There are 3 levels of SNMP security read-only, read-write and super. Only a super user can access the community table. |
| SNMP Version 3 | The SNMPv3 architecture introduces three main features to existing SNMPv1 and SNMPv2 infrastructure: security, access control and sending traps mechanism. It also describes how to apply the access control and the new sending traps mechanism on SNMPv1 and SNMPv2 PDUs. |

| Feature | Description |
|---|---|
| SNTP | The *Simple Network Time Protocol* (SNTP) assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are established by Stratums. Stratums define the distance from the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. |
| Spanning Tree | The *Spanning Tree Protocol* (STP) is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports. Spanning Tree can be enabled in the following modes:<br>• Classic Spanning Tree<br>• Rapid Spanning Tree<br>• Multiple Spanning Tree |
| **SSH** | Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. There are currently two versions of SSH available: version 1 and 2. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a device. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA Public Key cryptography for device connections and authentication |
| Static MAC Entries | User defined static MAC entries are stored in the *Bridging Table*, in addition to the Self Learned MAC addresses. |
| Storm Control | Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device.<br>When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports. |
| TACACS+ | In addition to RADIUS support, the device also supports the *Terminal Access Controller Access Control System* (TACACS+). TACACS+ is a security application implemented in a Client/Server based protocol that provides centralized validation of users attempting to gain access to a router or network access server. |
| TCP | *Transport Control Protocol* (TCP) hides applications errors. TCP connections are defined between 2 ports by an initial synchronization exchange. TCP ports are identified by an IP address and a 16-bit port number. Octets streams are divided into TCP packets, each carrying a sequence number. |
| TFTP Trivial File Transfer Protocol | The device supports boot image, software and configuration upload/download via TFTP |
| UDP Relay | UDP Relay enables the device to forward specific UDP broadcasts from one interface to another. IP broadcast packets from one interface are not generally forwarded to another interface. However, some applications use UDP broadcast to detect the availability of a service. Other services require Broadcast packets to be routed to provide services to clients on another subnet. |

| Feature | Description |
|---|---|
| Virtual Cable Testing (VCT) | VCT detects and reports copper link cabling occurrences, such as open cables and cable shorts. |
| VLAN Support | VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN. |
| VLAN Tagging | IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs and the protocols and algorithms involved in the provision of these services. |
| VLAN-Aware MAC-based Switching | Packets arriving from an unknown source address are sent to the CPU. When source addresses are added to the *Hardware Table*. Packets addressed to or from this address are more efficiently forwarded in the future. |
| Web Based Management | With web based management, the system can be managed from any web browser. The system contains an Embedded Web Server (EWS), which serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings. |

# 2 Installing and Removing the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/ SBCEGBESW10

## Overview

The process of installing an Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10 into an Intel® Blade Server Chassis SBCE consists of both hardware and software instructions. There are two main tasks:

- Physically installing the switch module into the Intel® Blade Server Chassis SBCE.
- Configuring the switch module.

The initial configuration process consists of setting the user name and password, configuring the static IP address, and configuring the SNMP read/write access and community strings.

After the IP address is set, the switch module can be managed through the network via Telnet, SNMP, or Web interfaces.

## Package Contents

While unpacking the switch module, ensure that the following items are included:

- The switch module
- Resource CD
- Safety and Regulatory Information Document

## Unpacking the Switch Module

To unpack the switch module:

***Note:*** *Before unpacking the switch module, inspect the packaging and report any evidence of damage immediately to Intel.*

***Note:*** *An ESD strap is not provided; however, it is recommended to wear one for the following procedure.*

1. Open the container.

2. Carefully remove the switch module from the container and place it on a secure, stable and clean surface.
3. Remove all packing material.
4. Inspect the switch module for damage. Report any damage immediately to Intel.

# Hardware Components

## Switch Module Components

***Note:*** *The illustrations in this document might differ slightly from the actual switch module and blade server chassis.*

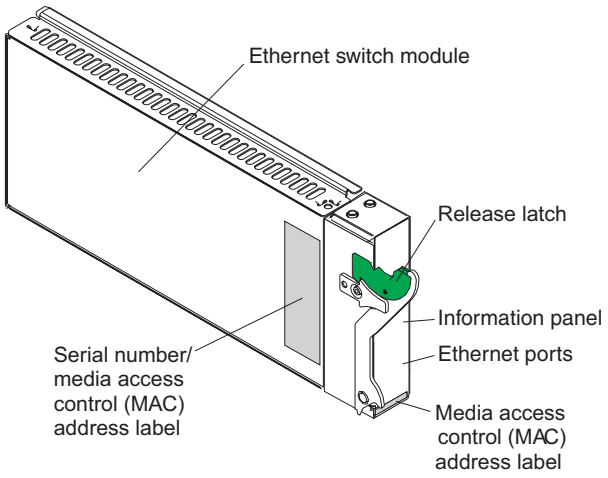



**Figure 1. Switch Module Components**

## Intel® Blade Server Chassis SBCE Architecture

The following illustration shows the four bays reserved for I/O modules.

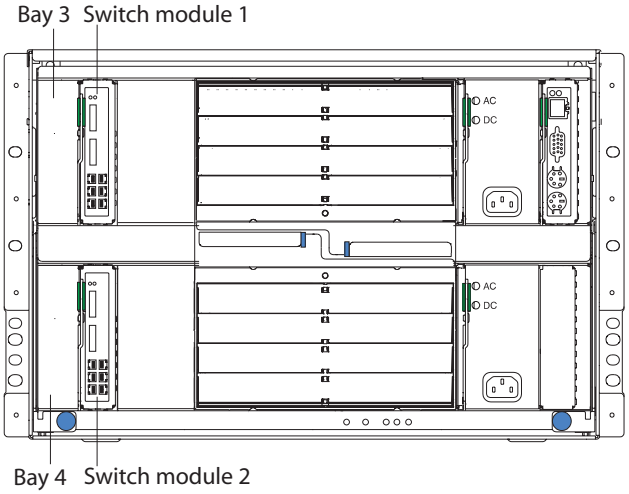



**Figure 2. Chassis I/O Module Bay Locations**

The four I/O module bays are located at the rear panel of the Intel® Blade Server Chassis SBCE. Although the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/ SBCEGBESW10 can be inserted in any of the I/O module bays it is important to understand that not all bays are necessarily intended for switch modules. The usage of the bays is dependent on the system I/O requirements.

Specifically, I/O module bays 1 and 2 are intended to house the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10. Bays 3 and 4 should only be populated with an Intel® Blade Server Ethernet Switch Module SBCEGBESW1/ SBCEGBESW10 if an Intel® Blade Server Ethernet Expansion Card SBGBE is installed as an option on the supported blade. For details of the Ethernet expansion card options, refer to the applicable user guide that shipped with your blade server. The Intel® Blade Server Chassis SBCE user guide also provides additional details on I/O expansion card options.

# Configuration Information Requirements

Before applying the initial configuration procedure to the switch module, the following information must be obtained from the network administrator:

- The IP address to be assigned to a VLAN through which the switch module is managed.
- The IP subnet mask for the network.
- The default gateway IP address.

- The SNMP community.

## Installation Guidelines

Before beginning to install the switch module in the Intel® Blade Server Chassis SBCE, read the following information:

- Review and become familiar with the safety and handling guidelines specified in Appendix E, "Installation/Assembly Safety Instructions" and Appendix F, "Safety Information".
- The Intel® Blade Server Chassis SBCE does not need to be powered down to install or replace any of the hot-swap modules.
- For a list of supported options for your Intel® Blade Server Chassis SBCE, go to http://support.intel.com.

# System Reliability Considerations

***Note:*** *To help ensure proper cooling and system reliability, make sure that:*

*To maintain proper system cooling, each I/O module bay must contain either a module or a filler module.*

*A removed hot-swap module must be replaced with an identical module or a filler module within 1 minute of removal.*

# Installing the Switch Module

***Note:*** *Neither the blade servers nor the Intel® Blade Server Chassis SBCE needs to be powered down to install an Intel® Blade Server Ethernet Switch Module SBCEGBESW1/ SBCEGBESW10.*

***Note:*** *The initial simple configuration uses the following assumptions:*

*The switch module was never configured before and is in the same state as when it was received.*

*The switch module is configured with a default user name and password.*

This section applies only to additional or replacement switch modules not included in the initial system order.

To install a switch module into an Intel® Blade Server Chassis SBCE perform the following:

1. Remove the acoustic attenuation module, if installed, from the rear of the Intel® Blade Server Chassis SBCE. The following illustration shows how to remove the acoustic attenuation module.

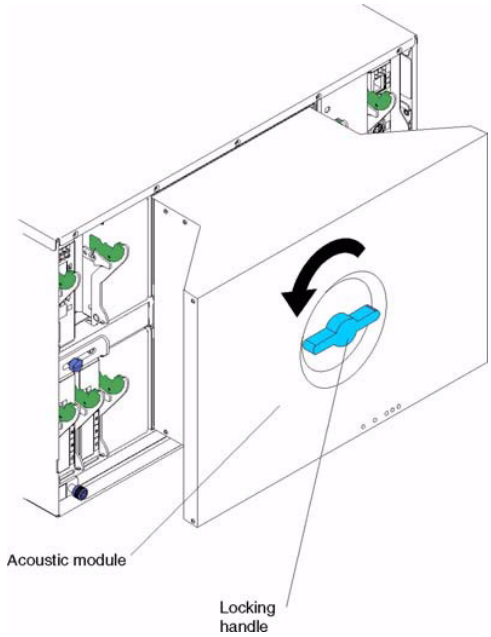



**Figure 3. Removing the Acoustic Attenuation Module**

2. Select an I/O module bay in which to install the switch module. In this example, a switch module is being installed in I/O module bay 1.
3. Remove the filler module from the selected bay. Store the filler module for future use.
4. If not already done, touch the static-protective package that contains the switch module to an unpainted metal part of Intel® Blade Server Chassis SBCE for at least two seconds.
5. Remove the switch module from its static-protective package.
6. Ensure that the release latch on the switch module is in the open position (perpendicular to the module).
7. Slide the switch module into the appropriate bay until it stops.

8. Push the release latch on the front of the switch module to the closed position.

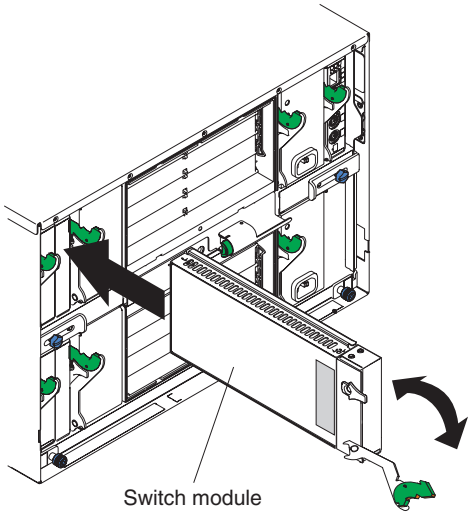



**Figure 4. Inserting a Switch Module into the Intel® Blade Server Chassis SBCE**

9. Replace the acoustic attenuation module if you removed it in Step 1. The following illustration shows how to replace the acoustic attenuation module in the Intel® Blade Server Chassis SBCE

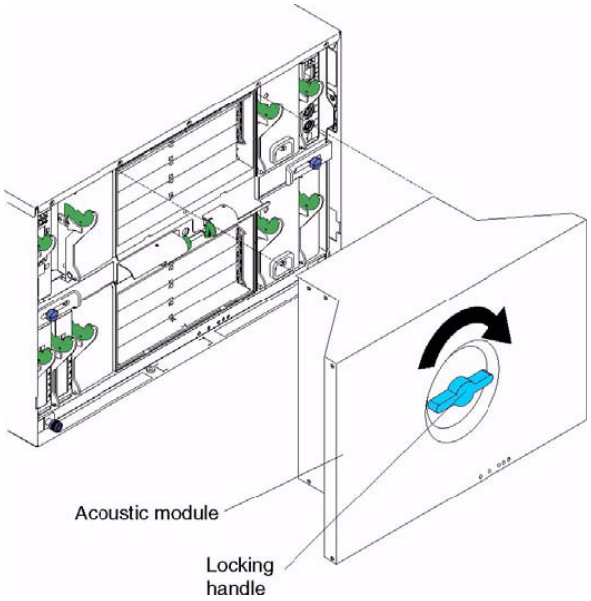



**Figure 5. Replacing the Acoustic Attenuation Module**

# Removing the Switch Module

Complete the following steps to remove the switch module.

1. Remove the acoustic attenuation module, if installed, from the rear of the Intel® Blade Server Chassis SBCE. The following illustration shows how to remove the acoustic attenuation module.

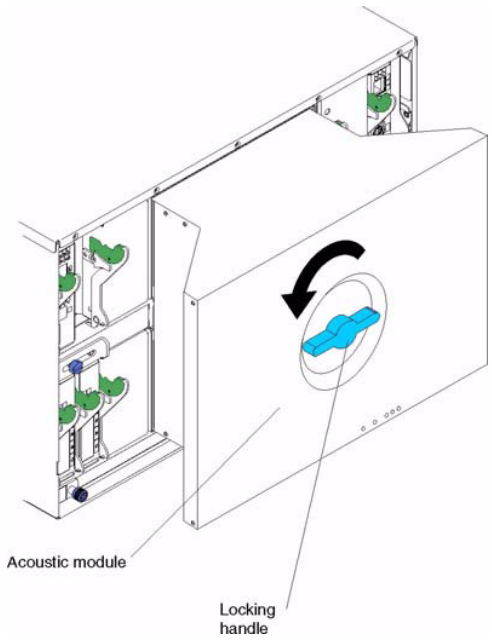



**Figure 6. Removing the Acoustic Attenuation Module**

2. Unplug any cables from the selected switch module.
3. For the Intel® Blade Server Chassis SBCE, pull the release latch toward the side of the switch module. The module moves out of the I/O module bay about 0.64 cm (0.25 inch).
4. Slide the switch module out of the I/O module bay and set it aside.
5. Place either another switch module or a filler module in the I/O module bay within 1 minute.
6. If you placed another switch module in the I/O module bay, reconnect any cables that you unplugged in Step 2.
7. Replace the acoustic attenuation module option if you removed it in Step 1.

# 3 Information Panel LEDs and External Ports

This chapter describes the information panel and LEDs (also known as indicators) on the Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10. This chapter also identifies the external ports on the information panel.

## Information Panel

The information panel of the switch module consists of LEDs, six external 1000BASE-T ports and two XFP ports as shown in the following illustration.

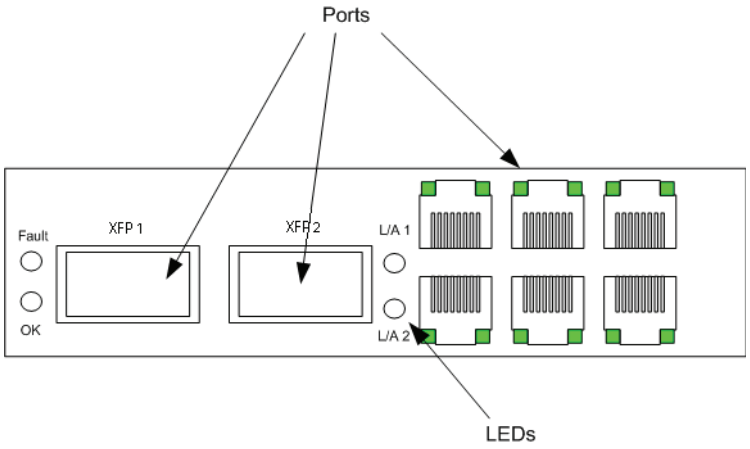



**Figure 7. Ports and LED Locations**

The Intel® Blade Server Ethernet Switch Module SBCEGBESW1/SBCEGBESW10 contains:

- Comprehensive LEDs, which display the status of the switch module and the network (see “LEDs”).
- Fourteen internal ports, one connected to each of the processor blades.
- Two internal full-duplex 100 Mbps ports connected to the management module.
- Six external 1000BASE-T Ethernet ports for 10/100/1000 Mbps connections to external Ethernet devices such as backbones, end stations and servers. These ports are identified as Ext1, Ext2, Ext3, Ext4, Ext5 and Ext6 in the switch configuration menus.
- Two XFP 10Gbps ports. These ports are identified on the switch module as XFP1 and XFP2.

# LEDs

The LEDs on the information panel of the switch module include OK, Fault, Ethernet link, and Ethernet activity. The following illustration shows the LEDs on the switch module. A description of each LED follows the illustration.

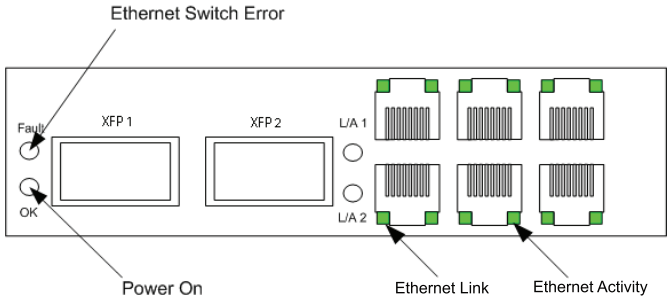



**Figure 8. LED Indicators**

***Note:*** *1.The illustrations in this document may differ slightly from your hardware.*

*2.An amber LED illuminates when a system error or event has occurred. To identify the error or event, check the LEDs on the information panel of the switch module.*

**OK (power-on)**: This green LED is located above the six external 10/100/1000 Mbps ports on the information panel. When this LED is on, it indicates that the switch module has passed the Power-On Self-Test (POST) and is operational.

**Fault** (Ethernet switch error): This amber LED is located next to the OK (power-on) LED on the information panel. This LED indicates that the switch module has a fault. If the switch module fails the POST, this fault LED will be lit.

**Ethernet link**: This green link status LED is located at the top of each external 10/100/1000 Mbps port. When this LED is lit on a port, it indicates that there is a connection (or link) to a device on that port.

**Ethernet activity:** This green activity LED is located at the bottom of each external 10/100/1000 Mbps port. When this LED blinks on a port, it indicates that data is being received or transmitted (that is, activity is occurring) on that port. The blink frequency is proportional to the amount of traffic on that port.

# 4 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 from 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. The *Enter Network Password Page* opens:

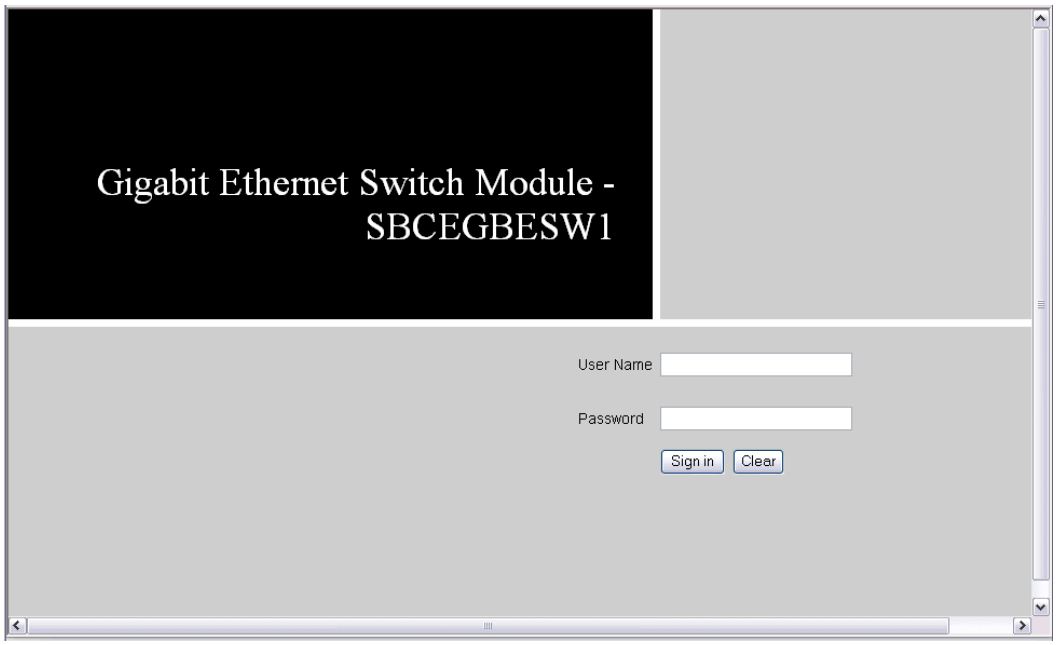



**Figure 9. Enter Network Password Page**

4. Enter your user name and password.

***Note:***

- The device is pre-configured with the user name “USERID” and password “PASSW0RD”.
- Passwords are case sensitive.

5. Click Sign in. The *Embedded Web Interface Home Page* opens:

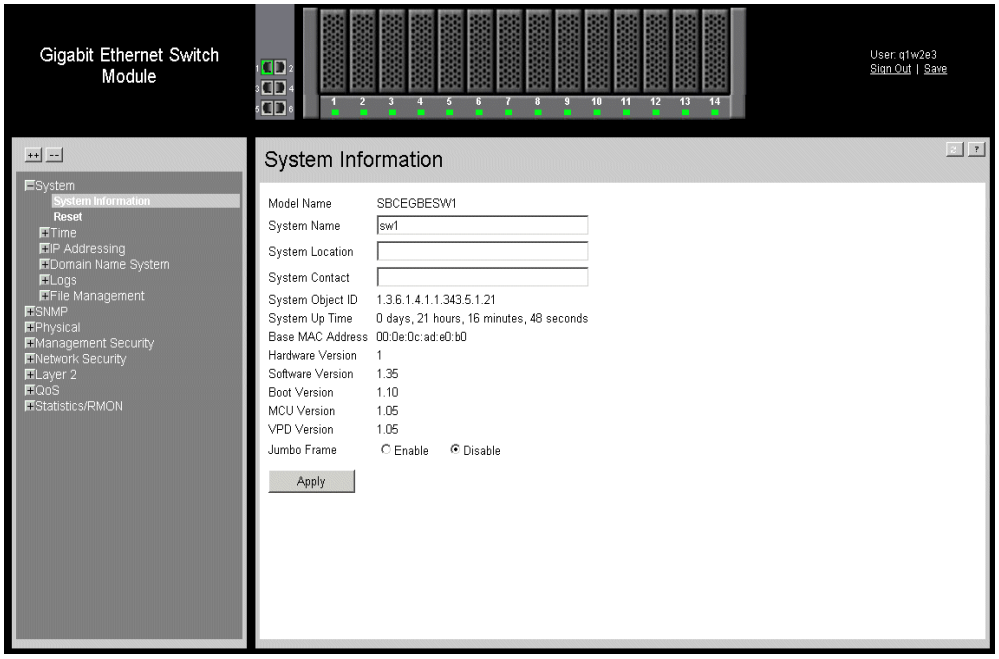



**Figure 10. Embedded Web Interface Home Page**

# 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.

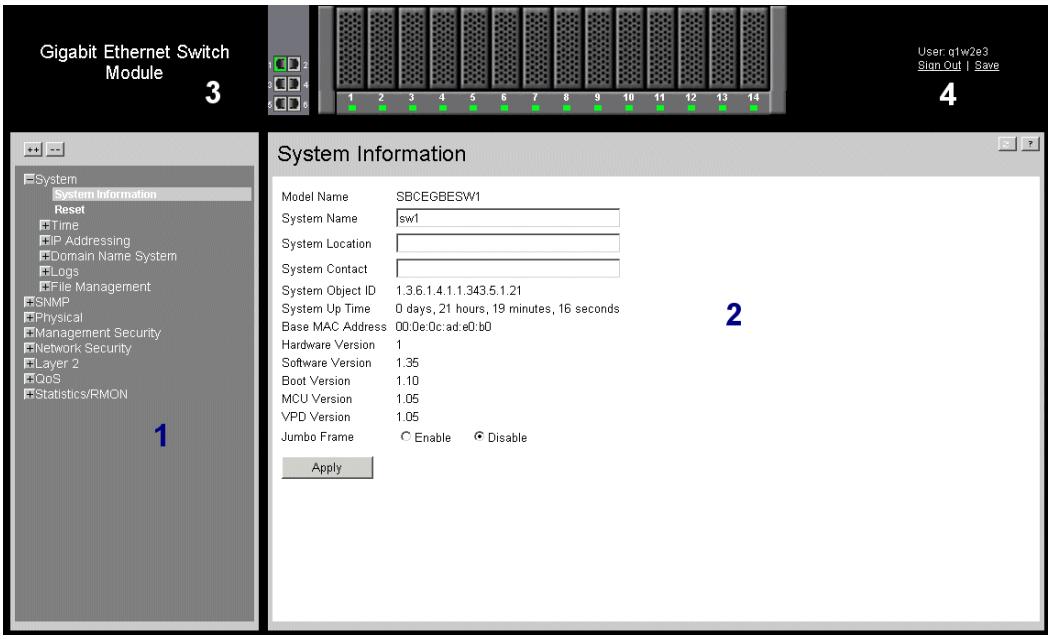



**Figure 11. Embedded Web Interface Components**

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.

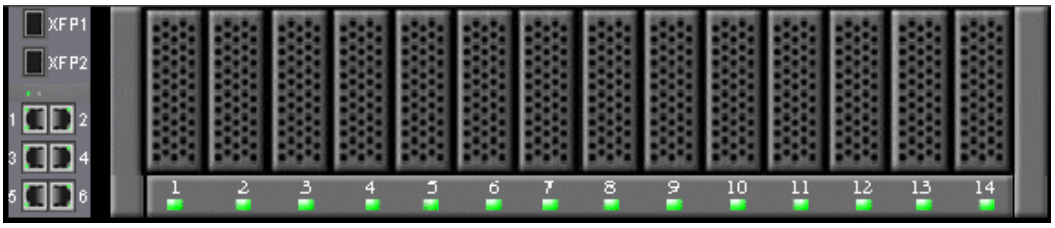



**Figure 12. Device Representation**

# 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. Web Interface Configuration Buttons**

| Button | Button Name | Description |
|---|---|---|
| Clear Logs | Clear Logs | Clears system logs. |
| Clear All Counters | Clear All Counters | Clears statistics. |
| Add | Create | Enables creation of configuration entries. |
| Edit | Edit | Modifies configuration settings. |
| Apply | Apply | Applies configuration changes to the device. |
| Test | Test | Performs cable tests. |
| Advanced | Advanced | Performs advanced tests. |
| Query | Query | Queries the device table. |
| Delete | Delete | Deletes a configuration entries. |
| Reset | Reset | Resets configuration to before changes were entered by user. |
| Next | Next | Allows you to view the next page in a table. |
| Back | Back | Allows you to view 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 SNMP Community Page*:

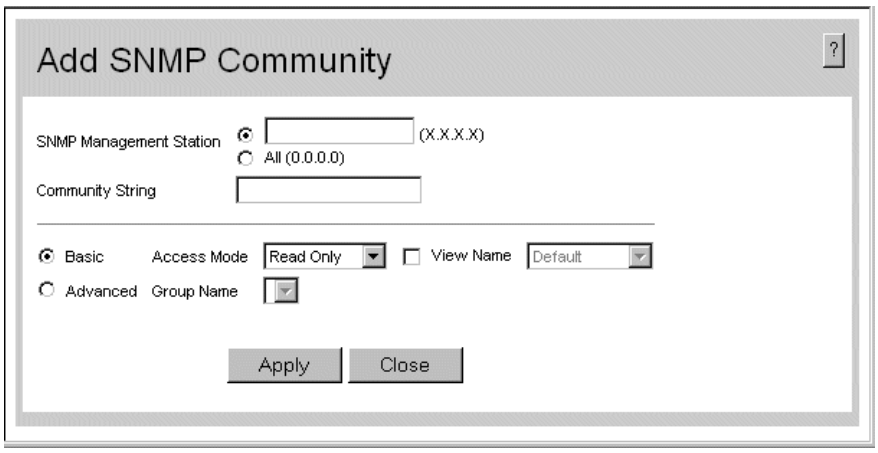



**Figure 13. Add SNMP Community Page**

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 *Bind ACL Page* opens:

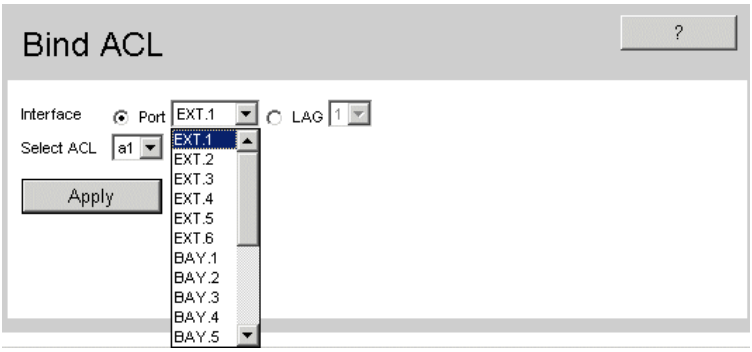



**Figure 14. Bind ACL Page**

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 *Remove* checkbox.
4. Click Delete . The information is deleted, and the device is updated.

# Resetting the Device

The  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  opens.

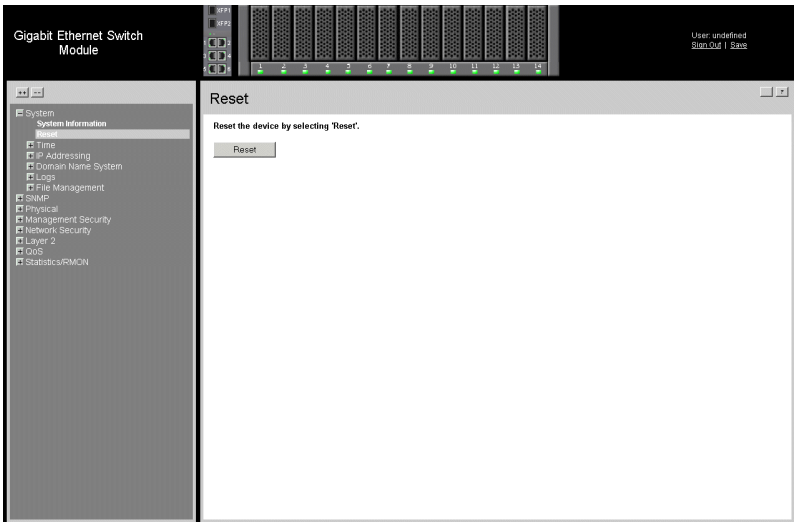



**Figure 15. Reset Page**

2. Click Reset .
   The device reboots and a confirmation prompt appears.
3. Click OK. The device is reset, and a prompt for a user name and password is displayed.
4. Enter a user name and password to reconnect to the Web Interface.

# Logging Off from the Device

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

# 5 Managing Device 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 define the general system information:

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

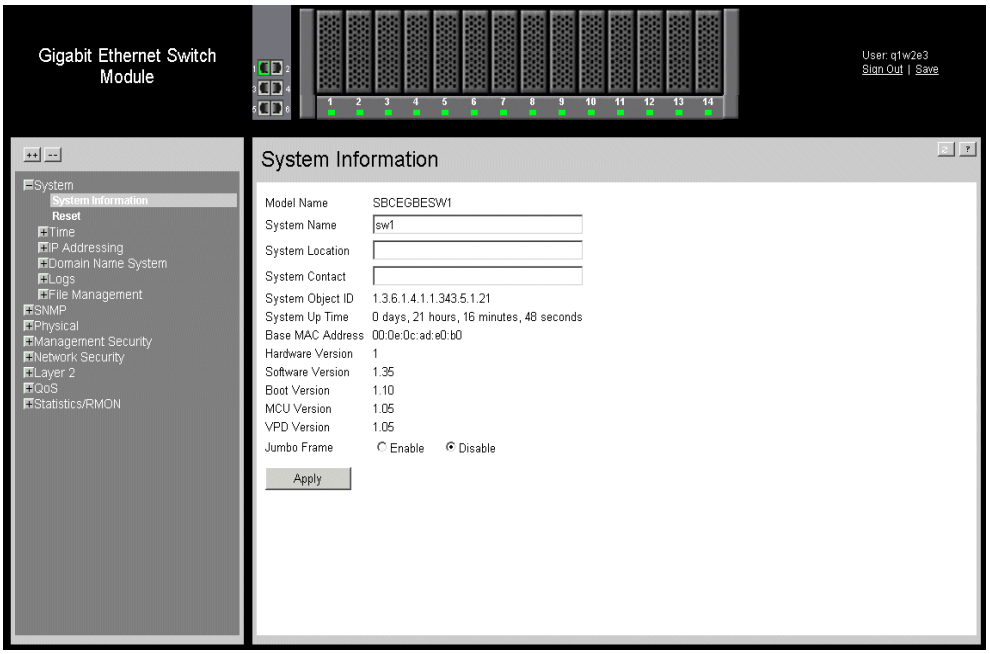



**Figure 16. System Information Page**

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.
- **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.
- **MCU Version** — Displays the Multicontroller Unit (MCU) version number.
- **VPD Version** — Displays the version of the VPD (Vital Product Data) EEPROM used. The VPD stores information about a device that allows the device to be administered at a system or network level. Typical VPD information includes a product model number, a unique serial number, MAC address, Firmware and Hardware revisions, and other information specific to the device type.
- **Jumbo Frames** — Indicates if Jumbo Frames are enabled on the device. The possible field values are:
  - *Selected* — Enables Jumbo Frames on the device.
  - *Unselected* — Disables Jumbo Frames on the device

# 6 Configuring Device Security

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

- Configuring Management Security
- Configuring Network Security

## Configuring Management Security

This section provides information for configuring device management security. This section includes the following topics:

- Configuring Authentication Methods
- Configuring Passwords
- Defining Access Control Lists

### Configuring Authentication Methods

This section provides information for configuring device authentication methods. This section includes the following topics:

- Defining Access Profiles
- Defining Profile Rules
- Defining Authentication Profiles
- Mapping Authentication Methods
- Defining TACACS+ Authentication
- Defining RADIUS Settings

## Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The *Access Profiles Page* contains the currently configured access profiles and their activity status. Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

To configure access profiles:

1. Click **Management Security > Access Method > Access Profiles**. *The Access Profiles Page opens:*

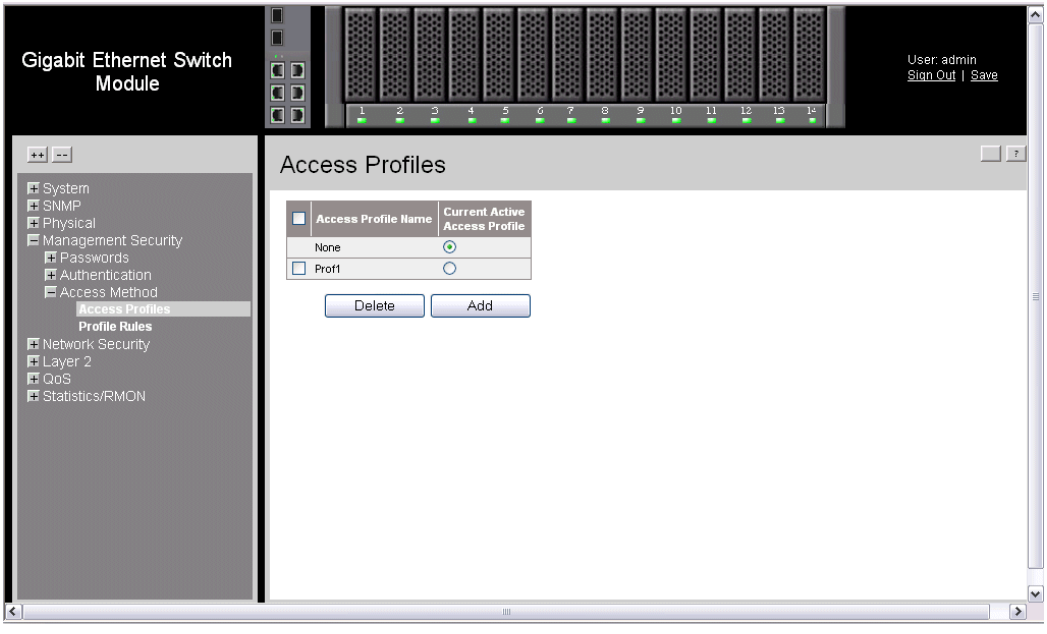



**Figure 17. Access Profiles Page**

The *Access Profiles Page* contains the following fields:

- **Remove** — Removes the selected access profile. The possible field values are:
  - *Checked* — Removes the selected access profile. Access Profiles cannot be removed when Active.
  - *Unchecked* — Maintains the access profiles.
- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Current Active Access Profile** — Defines the access profile currently active**.**

2. Click Add . The *Add Access Profile Page* opens:

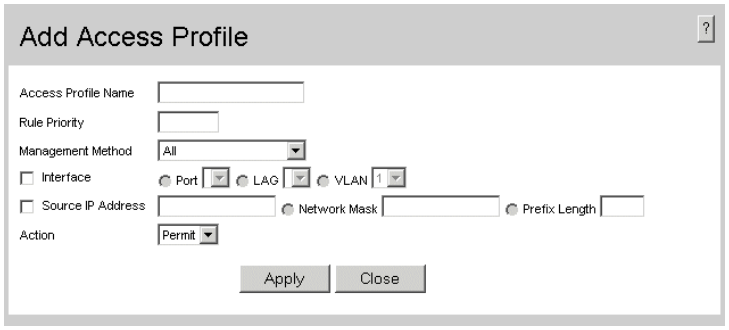



**Figure 18. Add Access Profile Page**

The *Add Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the *Profile Rules Page*.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.

- *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
- *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.

- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port* — Specifies the port on which the access profile is defined.
  - *LAG* — Specifies the LAG on which the access profile is defined.
  - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnet work.
- **Network Mask** — Indicates the interface network mask to which the packet is matched.
- **Prefix Length** — Indicates the prefix length to which the packet is matched.
- **Action** — Defines the action taken. The possible field values are:
  - *Permit* — Permits the addition of the access profile.
  - *Deny* — Denies the addition of the access profile.

3. Define the relevant fields.
4. Click Apply. The access profile is created, and the device is updated.

## Defining Profile Rules

Access profiles can contain up to 128 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- Source IP Address
- Prefix Length
- Forwarding Action

The rule order is essential as packets are matched on a first-fit basis.

To define profile rules:

1. Click **Management Security > Access Methods > Profile Rules**. The *Profile Rules Page* opens:

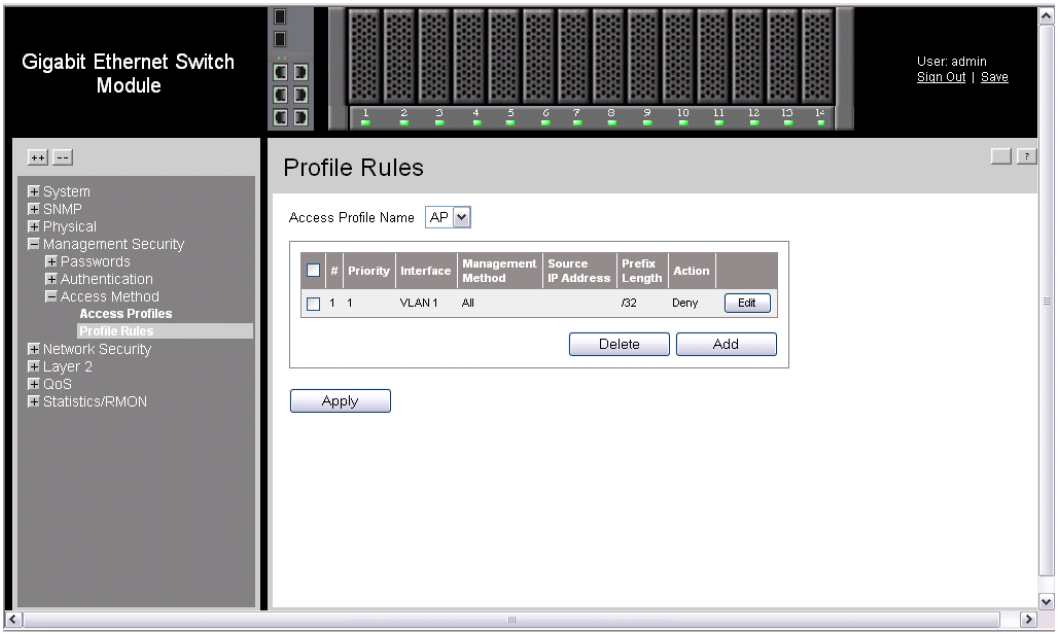



**Figure 19. Profile Rules Page**

The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile (AP) to which the rule is attached.
- **Remove** — Removes rules from the selected access profiles. The possible field values are:
  - *Checked* — Removes the selected rule from the access profile.
  - *Unchecked* — Maintains the rules attached to the access profile.
- **Unit No.** — Displays the unit number.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
  - *Port* — Attaches the rule to the selected port.
  - *LAG* — Attaches the rule to the selected LAG.
  - *VLAN* — Attaches the rule to the selected VLAN.

- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** —Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

2. Click Add . The *Add Profile Rule Page* opens:

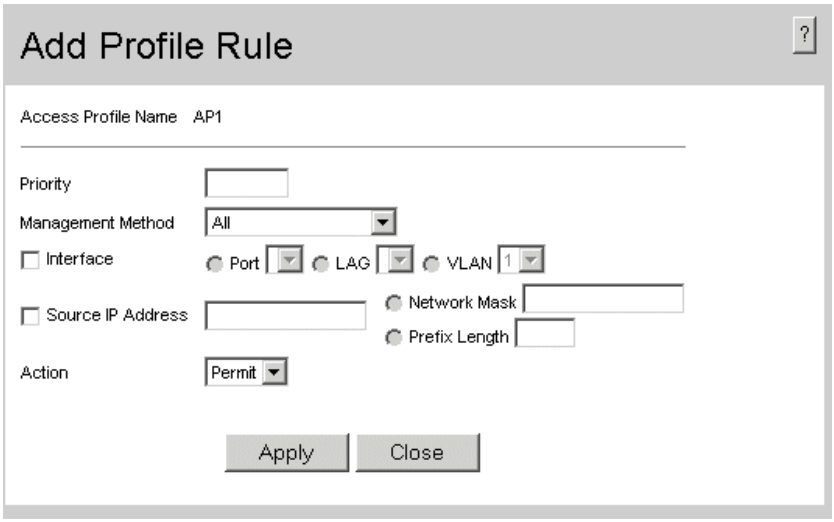



**Figure 20. Add Profile Rule Page**

3. Define the relevant fields.
4. Click Apply . The profile rule is added to the access profile, and the device is updated.

To modify a profile rule:

1. Click **Management Security > Access Method > Profile Rules**. The *Access Profiles Page* opens
2. Click Edit . The *Profile Rules Setting Page* opens.
3. Modify the desired fields.
4. Click Apply . The profile rule is modified, and the device is updated.

## Defining Authentication Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed either locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

To define authentication profiles:

1. Click **Management Security > Authentication > Authentication Profiles**. The *Authentication Profiles Page* opens:

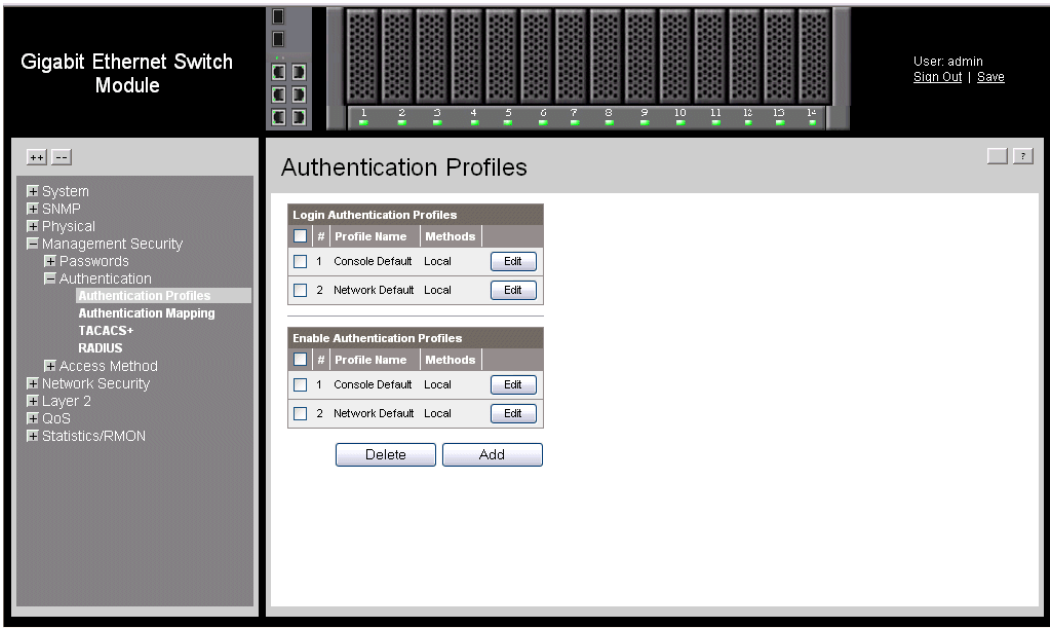



**Figure 21. Authentication Profiles Page**

The *Authentication Profiles Page* is separated into two tables, Login Authentication Profiles and Enable Authentication Profiles, and contains the following fields:

- **Remove** — Removes the selected authentication profile. The possible field values are:
  - — *Checked* — Removes the selected authentication profile.
  - — Unchecked — Maintains the authentication profiles.
- **Unit No.** — Displays the unit number.
- **Profile Name** — Contains a list of user-defined authentication profile lists to which user-defined authentication profiles are added.
- **Methods** — Defines the user authentication methods. The possible field values are:
  - — *None* — Assigns no authentication method to the authentication profile.
  - — *Line* — Authenticates the user using a line password.
  - — *Enable* — Authenticates the user using an enabled password.
  - — *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
  - — *RADIUS* — Authenticates the user at the RADIUS server.
  - — *TACACS+* — Authenticates the user at the TACACS+

2. Click Add . The *Add Authentication Profile Page* opens:

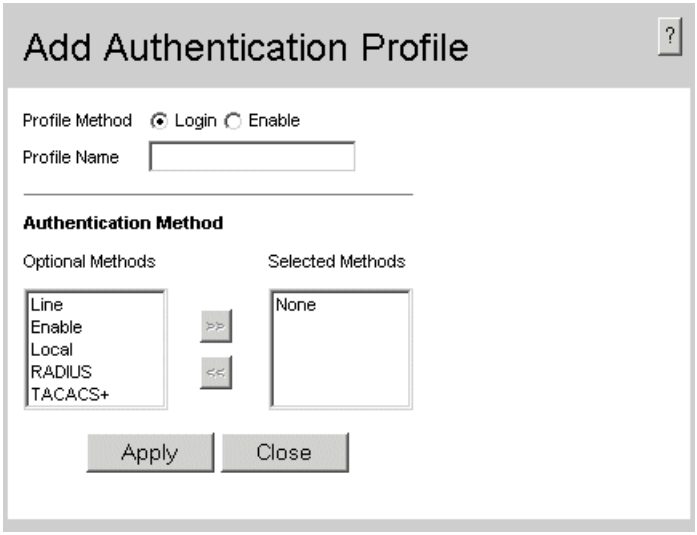



**Figure 22. Add Authentication Profile Page**

3. Define the relevant fields.
4. Click Apply . The authentication profile is defined, and the device is updated.

To modify an authentication profile:

1. Click **Management Security > Authentication > Authentication Profiles**. The *Authentication Profiles Page* opens.
2. Click Edit . The *Authentication Mapping Page* opens.
3. Select an authentication method from the *Optional Methods* list.
4. Click Apply . The authentication method is selected, and the device is updated.

## Mapping Authentication Methods

After authentication profiles are defined, they can be applied to management access methods.

Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

To map authentication methods:

1. Click **Management Security > Authentication > Authentication Mapping**. The *Authentication Mapping Page* opens:

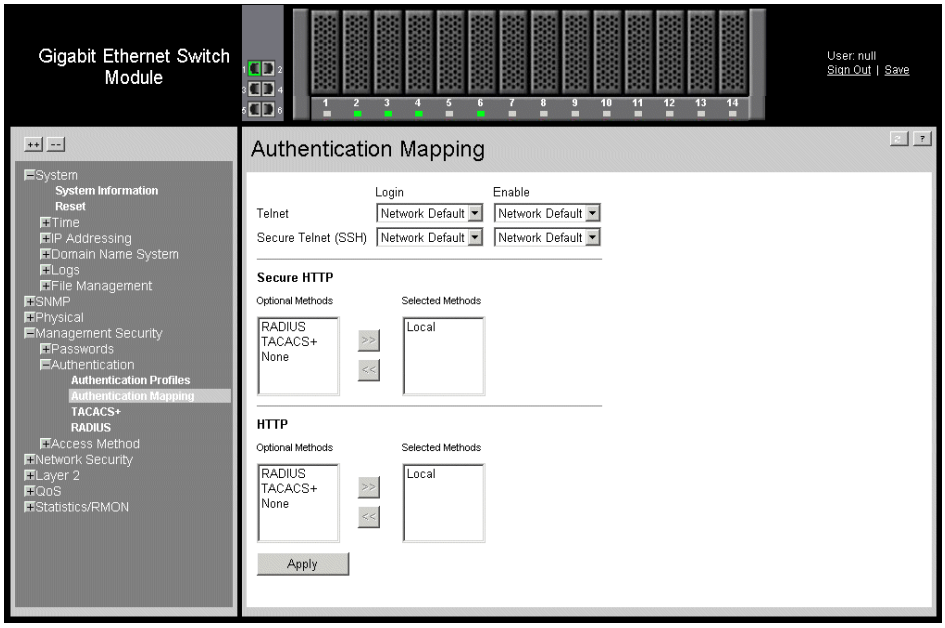



**Figure 23. Authentication Mapping Page**

The *Authentication Mapping Page* contains the following fields:

- **Telnet** — Indicates that authentication profiles are used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Indicates that authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.
- **Secure HTTP** — Indicates that authentication methods used for Secure HTTP access. Possible field values are:
  - *RADIUS (Optional)* — Indicates that authentication occurs at the RADIUS server.
  - *TACACS+(Optional)* — Indicates that authentication occurs at the TACACS+.
  - *None (Optional)* — Indicates that no authentication method is used for access.

— *Local* (*Selected*) — Indicates that the authentication method is on the device's local user database.

- **HTTP** — Indicates that Authentication methods are used for HTTP access. Possible field values are:
  - — *RADIUS (Optional)* — Indicates that authentication occurs at the RADIUS server.
  - — *TACACS+(Optional)* — Indicates that authentication occurs at the TACACS+.
  - — *None — (Optional)* Indicates that no authentication method is used for access.
  - — *Local* (*Selected*) — Indicates that the authentication method is on the device's local user database.

2. Define the relevant fields.
3. Map the respective authentication methods.
4. Click Apply . The authentication mapping is saved, and the device is updated.

## Defining TACACS+ Authentication

*Terminal Access Controller Access Control System* (TACACS+) provides centralized security user access validation. The system supports up-to 4 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server.

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers.

To define TACACS+ authentication settings:

1. Click **Management Security > Authentication > TACACS+**. The *TACACS+ Page* opens:

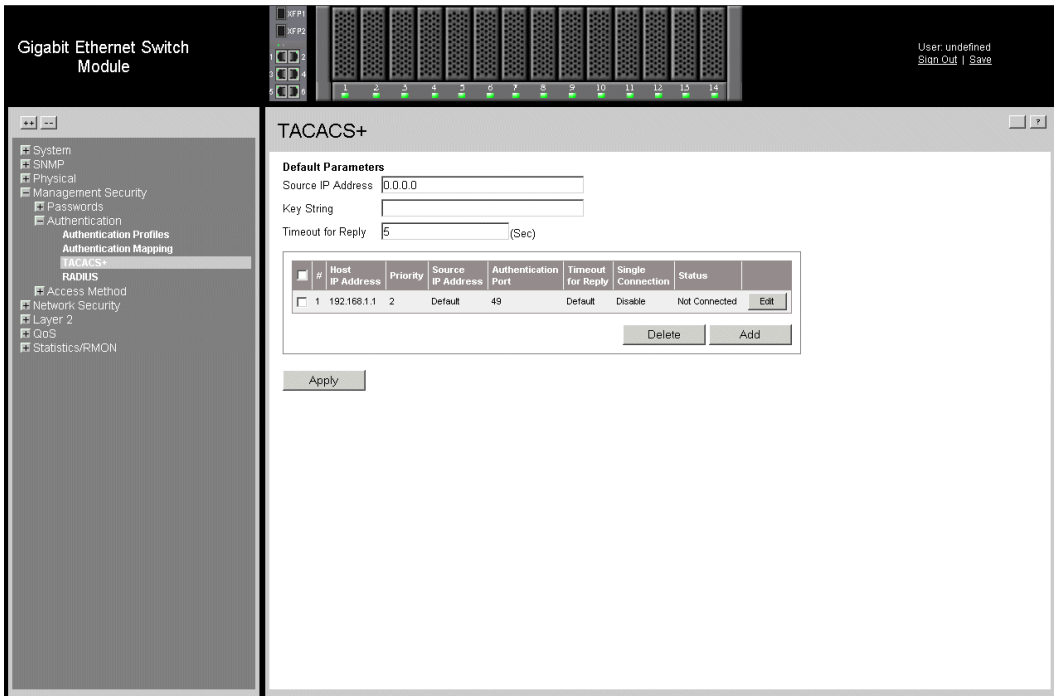



**Figure 24. TACACS+ Page**

The **Default Parameters** section contains the following fields:

- **Source IP Address** — Defines the default device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout for Reply** — Defines the default time that passes before the connection between the device and the TACACS+ times out. The default is 5.

The *TACACS+ Page* also contains the following fields:

- **Remove** — Removes TACACS+ server. The possible field values are:
  - *Checked* — Removes the selected TACACS+ server.
  - *Unchecked* — Maintains the TACACS+ servers.
- **Unit No.** — Displays the unit number.
- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The field range is 0-65535. The default is 0.

- **Source IP Address** — Defines the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port** — Defines the port number via which the TACACS+ session occurs. The field range is 0-65535. The default port is port 49.
- **Timeout for Reply**— Defines the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server. The possible field values are:
  - *Checked* — Enables a single connection.
  - *Unchecked* — Disables a single connection.
- **Status** — Indicates the connection status between the device and the TACACS+ server. The possible field values are:
  - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — Indicates there is not currently a connection between the device and the TACACS+ server.

2. Click Add . The *Add TACACS+ Host Page.* opens.

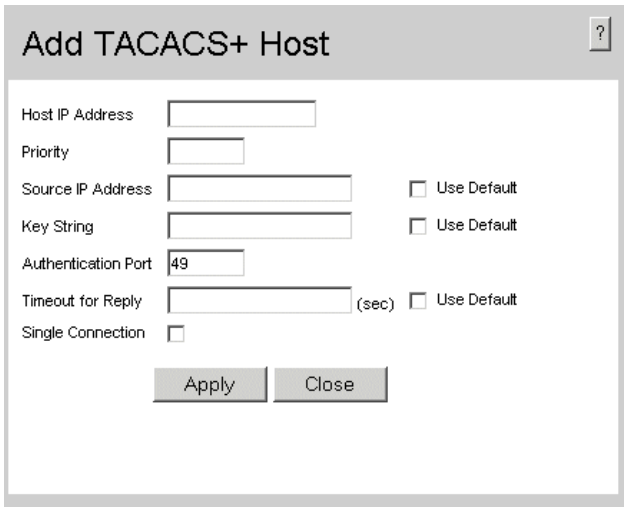



**Figure 25. Add TACACS+ Host Page.**

3. Define the relevant fields.
4. Click Apply . The TACACS+ server is define, and the device is updated.

To modify the TACACS+ server settings:

1. Click **Management Security >Authentication > TACACS+**. The *TACACS+ Page* opens.
2. Select TACACS+ server entry.
3. Click Edit . The *TACACS+ Host Settings Page* opens:

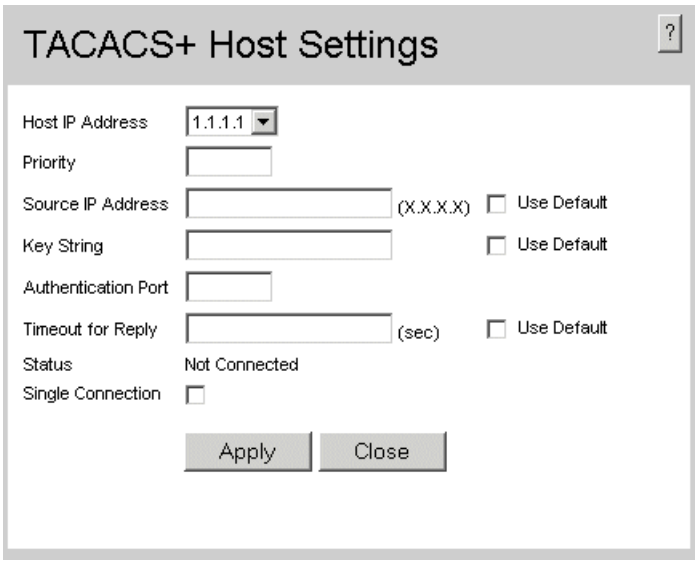



**Figure 26. TACACS+ Host Settings Page**

4. Modify the relevant fields.
5. Click Apply . The TACACS+ host settings are saved, and the device is updated.

## Defining RADIUS Settings

*Remote Authorization Dial-In User Service* (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To configure RADIUS servers:

1. Click **Management Security > Authentication > RADIUS**. The *RADIUS Page* opens:

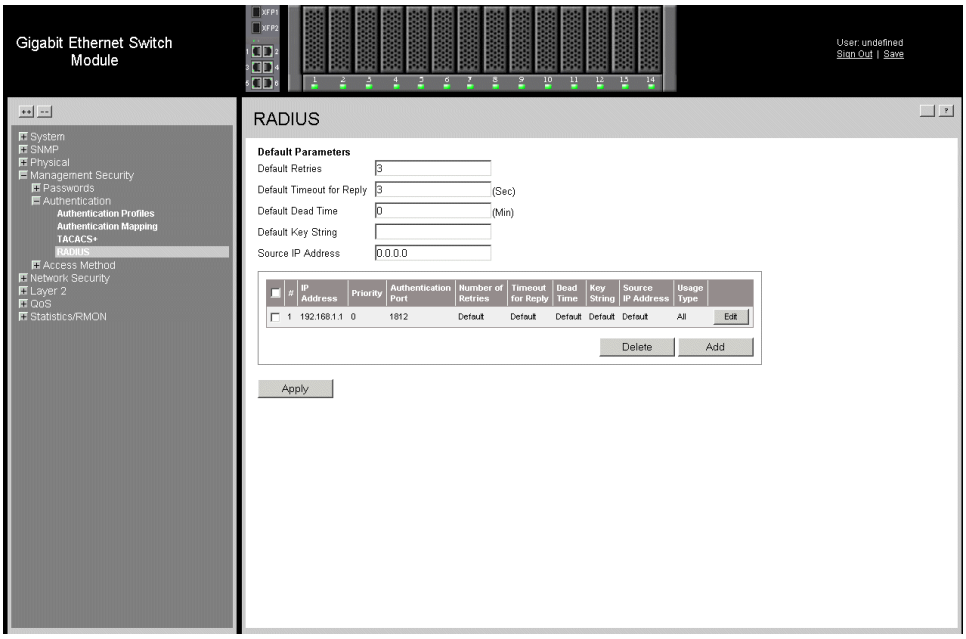



**Figure 27. RADIUS Page**

The *RADIUS Page* **Default Parameters** section contains the following fields:

- **Default Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default value is 3.
- **Default Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Possible field values are 1-30. The default value is 3.
- **Default Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default value is 0.
- **Default Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Source IP Address** — Defines the default IP address of a device accessing the RADIUS server.

The *RADIUS Page* also contains the following fields:

- **Remove**— Removes a RADIUS server. The possible field values are:
  - *Checked* — Removes the selected RADIUS server.
  - *Unchecked* — Maintains the RADIUS servers.

- **IP Address —** Lists the RADIUS server IP addresses.
- **Priority** — Displays the RADIUS server priority. The possible values are 1-65535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1-10. Three is the default value.
- **Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1-30. Three is the default value.
- **Dead Time** — Defines the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is *All*. The possible field values are:
  - *Log in* — Indicates the RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — Indicates the RADIUS server is used for 802.1X authentication.
  - *All* — Indicates the RADIUS server is used for authenticating user names and passwords, and 802.1X port authentication.

2. Click 

. The *Add RADIUS Server Page* opens:

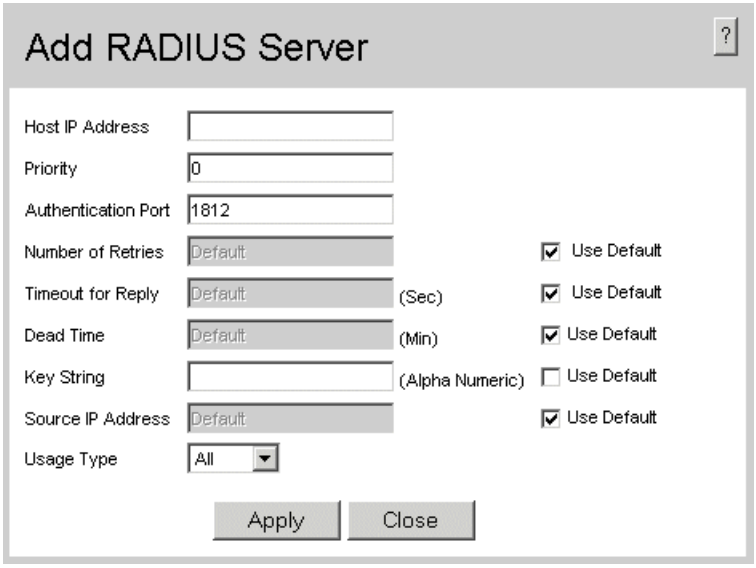



**Figure 28. Add RADIUS Server Page**

3. Define the relevant fields.
4. Click Apply. The RADIUS server is added, and the device is updated.

To modify RADIUS Server Settings:

1. Click **Management Security > Authentication > RADIUS**. The *RADIUS Page* opens.
2. Click Edit . The *RADIUS Server Settings Page* opens:

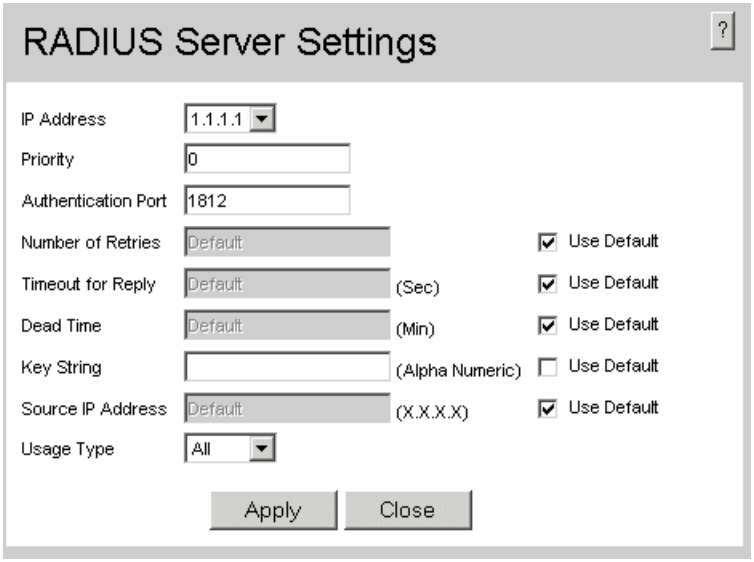



**Figure 29. RADIUS Server Settings Page**

3. Modify the relevant fields.
4. Click Apply . The RADIUS server settings are saved, and the device is updated.

# Configuring Passwords

This section contains information for defining device passwords, and includes the following topics.

- Defining Local Users
- Defining Line Passwords
- Defining Enable Passwords

## Defining Local Users

Network administrators can define users, passwords, and access levels for users using the *Local Users Page*.

To define local users:

1. Click **Management Security > Passwords > Local Users**. The *Local Users Page* opens:

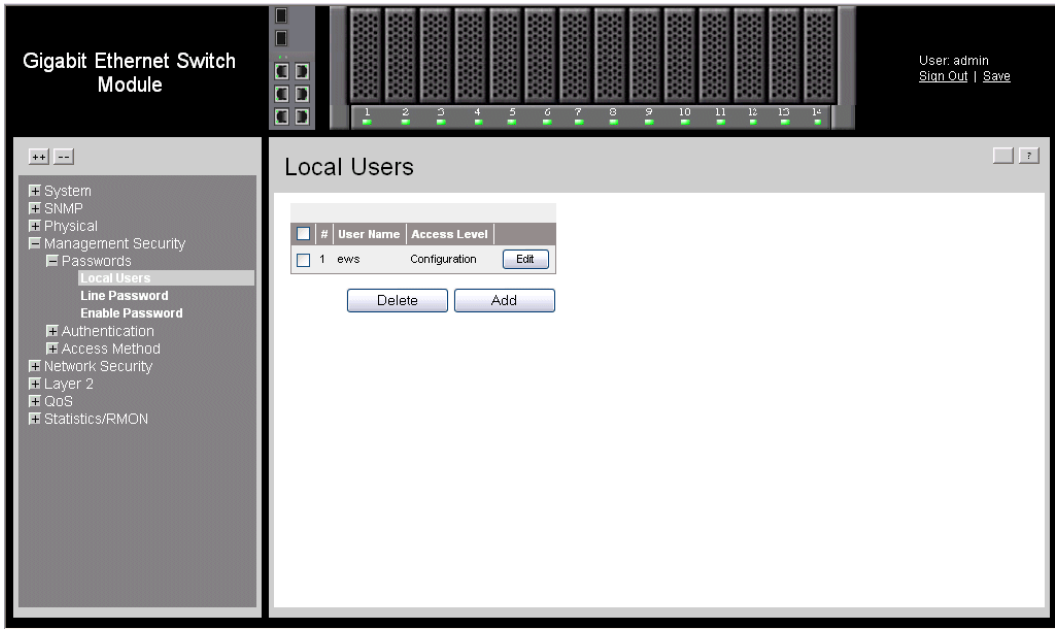



**Figure 30. Local Users Page**

The *Local Users Page* contains the following fields:

- **Remove** — Removes the user from the *User Name* list. The possible field values are:
  - *Checked* — Removes the selected local user.
  - *Unchecked* — Maintains the local users.
- **Unit No.** — Displays the unit number.

- **User Name** — Displays the user name.
- **Access Level** — Displays the user access level. The lowest user access level is 1 and the highest is 15. Users with access level 15 are Privileged Users.

2. Click Add . The *Add Local User Page* opens:

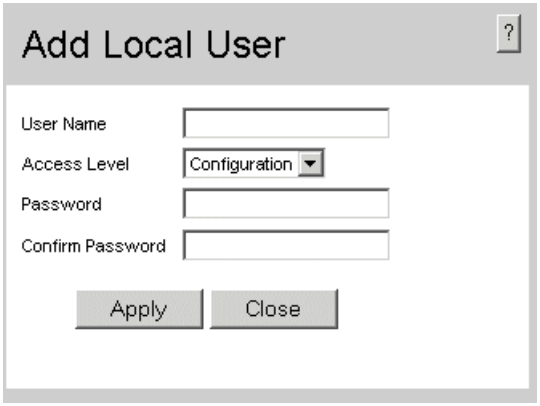



**Figure 31. Add Local User Page**

In addition to the fields in the *Local Users Page*, the *Add Local User Page* contains the following fields:

- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **Confirm Password** — Verifies the password.

To modify the settings for a local user:

1. Click **Management Security > Passwords > Local Users**. The *Local Users Page* opens.
2. Click Edit . The *Local User Settings Page* opens:

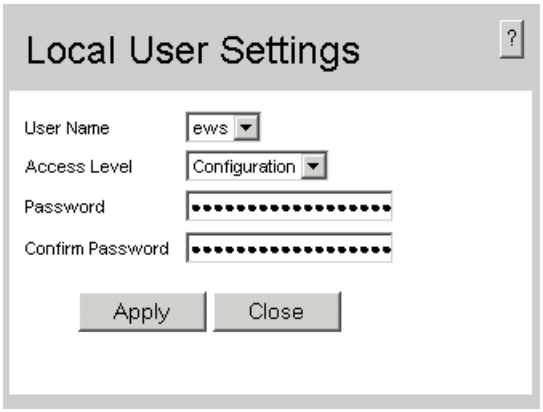



**Figure 32. Local User Settings Page**

3. Modify the relevant fields.
4. Click Apply . The local user passwords settings are saved, and the device is updated.

## Defining Line Passwords

Network administrators can define line passwords in the *Line Password Page*. After the line password is defined, a management method is assigned to the password. The device can be accessed using the following methods:

- Telnet Line Passwords
- Secure Telnet Line Passwords

To define line passwords:

1. Click **Management Security > Passwords > Line Password**. The *Line Password Page* opens:

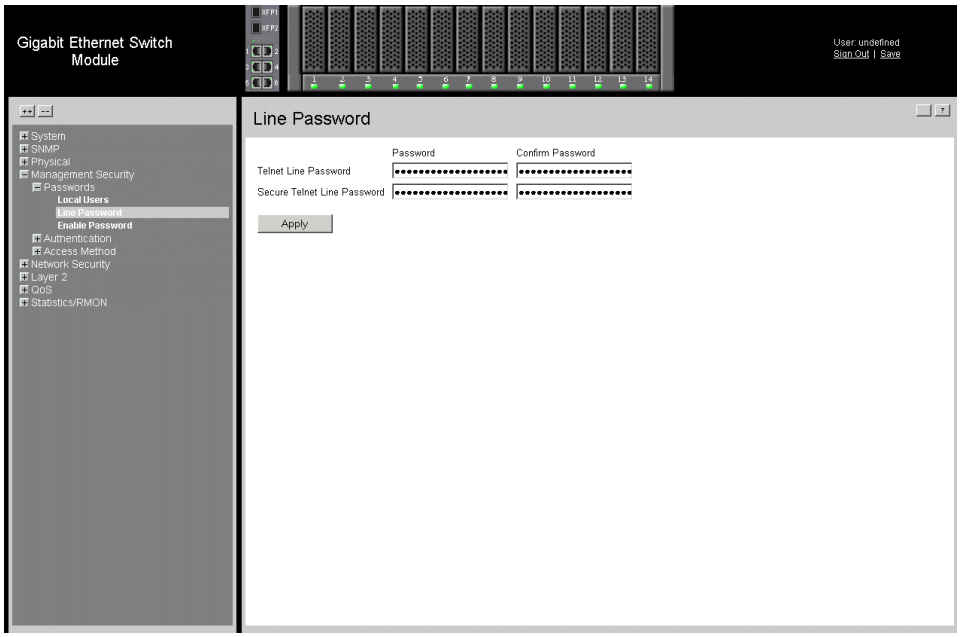



**Figure 33. Line Password Page**

The *Line Password Page* contains the following fields:

- **Telnet Line Password** — Defines the line password for accessing the device via a Telnet session. Passwords can contain a maximum of 159 characters.
- **Secure Telnet Line Password** — Defines the line password for accessing the device via a secure Telnet session. Passwords can contain a maximum of 159 characters.

2. Define the relevant fields.
3. Redefine the *Confirm Password* field for each of the passwords defined in the previous steps to verify the passwords.
4. Click Apply. The line passwords are saved, and the device is updated.

## Defining Enable Passwords

The *Enable Password Page* sets a local password for a particular access level.

To enable passwords:

1. Click **Management Security > Passwords > Enable Password**. The *Enable Password Page* opens:

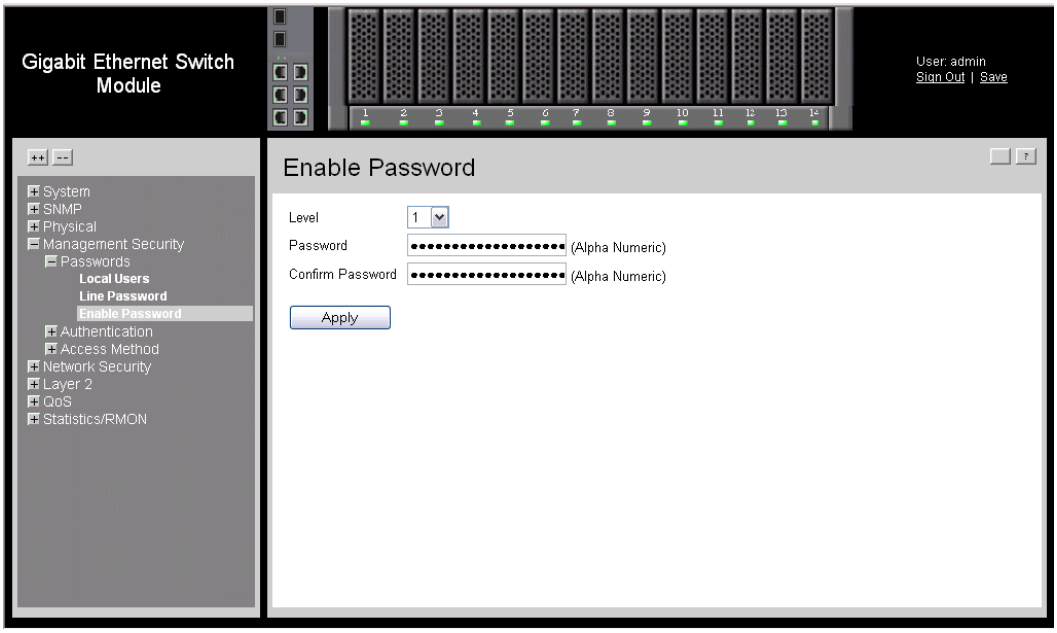



**Figure 34. Enable Password Page**

The *Enable Password Page* contains the following fields:

- **Level** — Defines the access level associated with the enable password. Possible field values are 1-15.
- **Password** — Defines the enable password.
- **Confirm Password** — Confirms the new enable password. The password is hidden and appears in the ***** format.

2. Define the relevant fields.
3. Click Apply. The enable password is defined, and the device is updated.

# Configuring Network Security

Network security manages both access control lists and locked ports. This section contains the following topics:

- Network Security Overview
- Defining Network Authentication Properties
- Defining Port Authentication
- Configuring Traffic Control

## Network Security Overview

This section provides an overview of network security and contains the following topics:

- Port-Based Authentication
- Advanced Port-Based Authentication

### Port-Based Authentication

Port-based authentication authenticates users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the *Extensible Authentication Protocol* (EAP). Port-based authentication includes:

- **Authenticators** — Specifies the device port which is authenticated before permitting system access.
- **Supplicants** — Specifies the host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port-based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports port-based authentication via RADIUS servers.

## Advanced Port-Based Authentication

Advanced port-based authentication enables multiple hosts to be attached to a single port. Advanced port-based authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized, all attached hosts are denied access to the network.

Advanced port-based authentication also enables user-based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced port-based authentication is implemented in the following modes:

- **Single Host Mode** — Allows port access only to the authorized host.
- **Multiple Host Mode** — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Guest VLANs** — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant internet access to unauthorized users.
- **Unauthenticated VLANS** — Are available to users, even if the ports attached to the VLAN are defined as unauthorized.

# Defining Network Authentication Properties

The *802.1x Properties Page* allows network managers to configure network authentication parameters. In addition, Guest VLANs are enabled from the *802.1x Properties Page*.

To define the network authentication properties:

1. Click **Network Security > 802.1x > Properties**. The *802.1x Properties Page* opens.


**Figure 35. 802.1x Properties Page**

The *802.1x Properties Page* contains the following fields:

- **Port-based Authentication State** — Indicates if Port Authentication is enabled on the device. The possible field values are:
  - *Enable* — Enables port-based authentication on the device.
  - *Disable* — Disables port-based authentication on the device.
- **Authentication Method** — Specifies the authentication method used for port authentication. The possible field values are:
  - RADIUS, None — Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
  - *RADIUS* — Provides port authentication using the RADIUS server.
  - *None* — Indicates that no authentication method is used to authenticate the port.

- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - *Enable* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
  - *Disable* — Disables port-based authentication on the device. This is the default.
- **Guest VLAN ID** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

2. Define the relevant fields.
3. Click Apply . The network authentication properties are set, and the device is updated.

# Defining Port Authentication

The *Port Authentication Page* allows network managers to configure port-based authentication global parameters.

To define the port-based authentication global properties:

1. Click **Network Security > 802.1x > Port Authentication**. The *Port Authentication Page* opens:

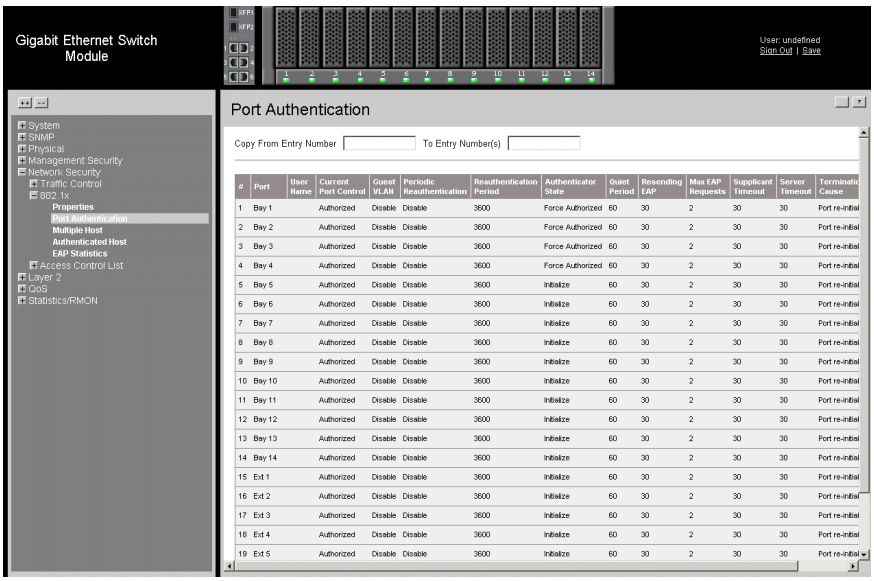



**Figure 36. Port Authentication Page**

The *Port Authentication Page* contains the following fields:

- **Copy From Entry Number** — Copies port authentication information from the selected port.

- **To Entry Number(s)** — Copies port authentication information to the selected port.
- **Unit No**. — Indicates the unit number.
- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.
- **Current Port Control** — Displays the current port authorization state.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - *Enable* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
  - *Disable* — Disables port-based authentication on the device. This is the default.
- **Periodic Reauthentication** — Permits immediate port reauthentication. The possible field values are:
  - *Enable* — Enables immediate port reauthentication. This is the default value.
  - *Disable* — Disables port reauthentication.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.
  - *Reauthenticate Now* — Reauthenticates all selected ports immediately.
- **Authenticator State** — Displays the current authenticator state.
- **Quiet Period** — Indicates the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the amount of time (in seconds) that lapses before EAP requests are resent to the supplicant. The field default is 30 seconds.
- **Server Timeout** — Displays the amount of time (in seconds) that lapses before the device re-sends a request to the authentication server. The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

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

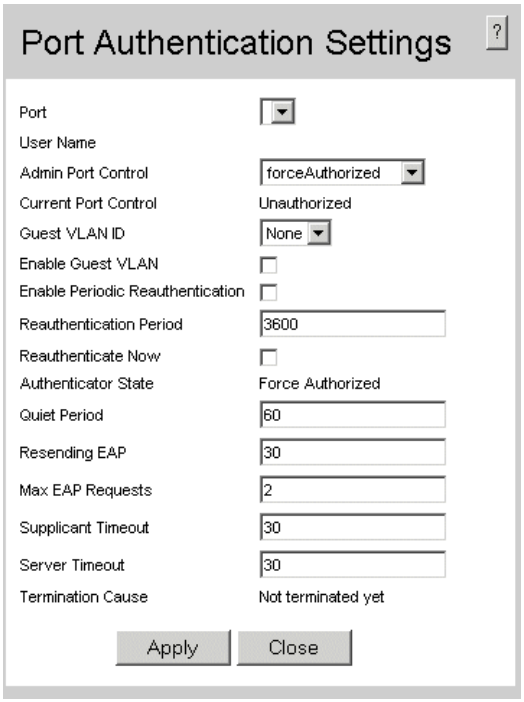



**Figure 37. Port Authentication Settings Page**

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

## Configuring Multiple Hosts

The *Multiple Host Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs. For more information on advanced port-based authentication, see *Advanced Port-Based Authentication*.

To define the network authentication global properties:

1. Click **Network Security > 802.1x > Multiple Host**. The *Multiple Host Page* opens.

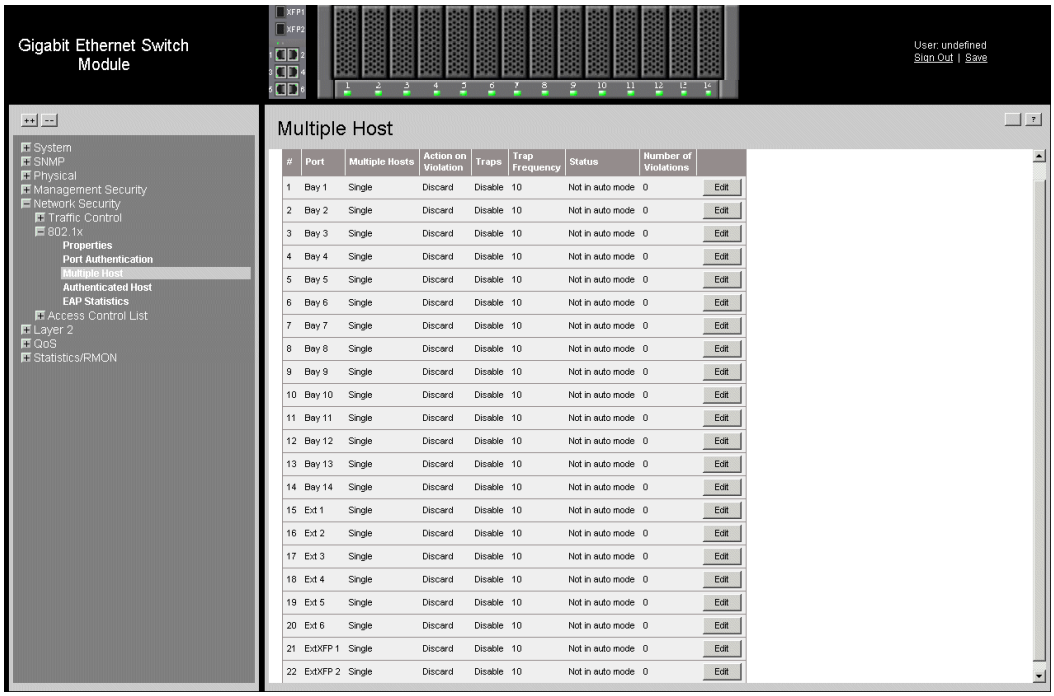



**Figure 38. Multiple Host Page**

- The *Multiple Host Page* contains the following fields:
- **Unit No**. — Indicates the unit number.
- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Multiple Hosts** — Indicates whether multiple hosts are enabled. Multiple hosts must be enabled to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
  - — *Multiple* — Multiple hosts are enabled.
  - — *Single*— A single host is enabled.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - — *Forward* — Forwards the packet.
  - — *Discard* — Discards the packets. This is the default value.
  - — *Shutdown* — Discards the packets and shuts down the port. The port remains shut down until reactivated, or until the device is reset.

- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - *Enable* — Indicates that traps are enabled for Multiple hosts.
  - *Disable* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- **Status** — Indicates the host status. If there is an asterisk (*), the port is either not linked or is down. The possible field values are:
  - *Unauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
  - *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.
  - *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.
  - *No Single Host* — Indicates that Multiple Host is enabled.
- **Number of Violations** — Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

2. Click Edit . The *Multiple Host Settings Page* opens:

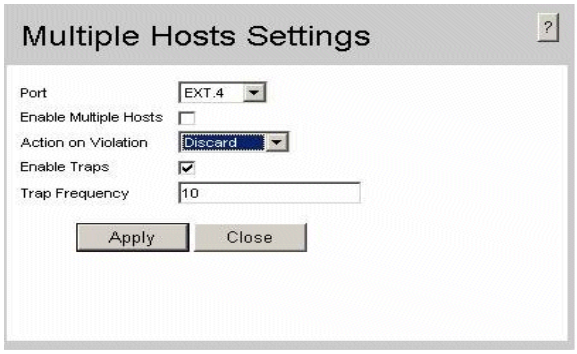



**Figure 39. Multiple Host Settings Page**

3. Modify the relevant fields.
4. Click Apply . The multiple host settings are modified, and the device is updated.

## Defining Authentication Hosts

The *Authenticated Host Page* contains a list of authenticated users.

To define authenticated users:

1. Click **Network Security > 802.1x > Authenticated Host**. The *Authenticated Host Page* opens:

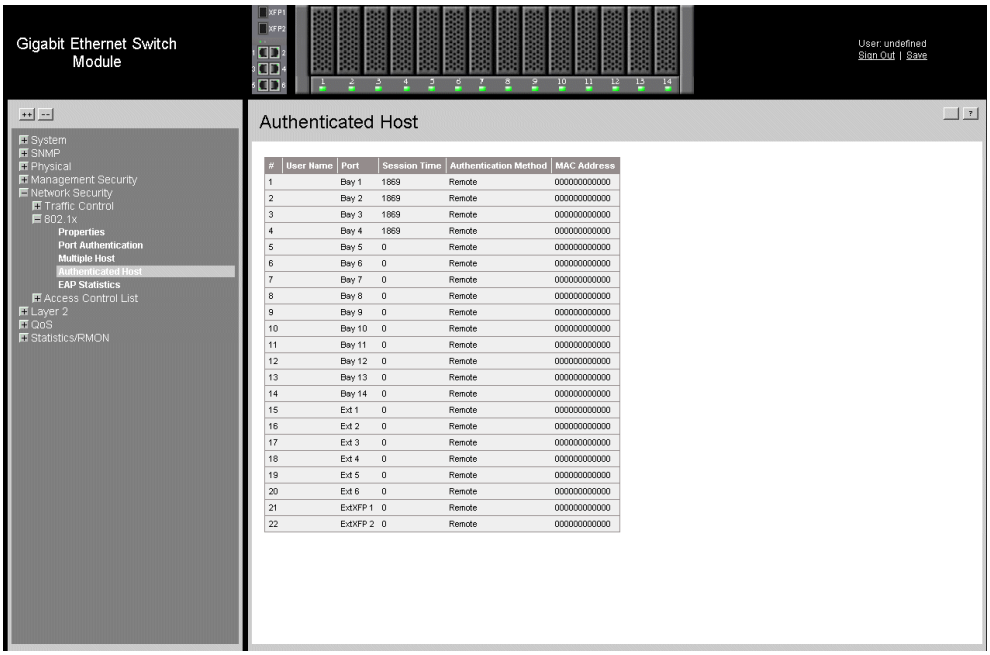



**Figure 40. Authenticated Host Page**

The *Authenticated Host Page* contains the following fields:

- **Unit No**. — Indicates the unit number.
- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- **Session Time** — Displays the amount of time (in seconds) the supplicant was logged on the port.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
  - *Remote* — 802.1x authentication is not used on this port (port is forced-authorized).
  - *None* — The supplicant was not authenticated.
  - *RADIUS* — The supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

# 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 Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

A Broadcast Storm is a result of an excessive amount of broadcast 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 Gigabit ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast 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 broadcast storm control.

To enable storm control:

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

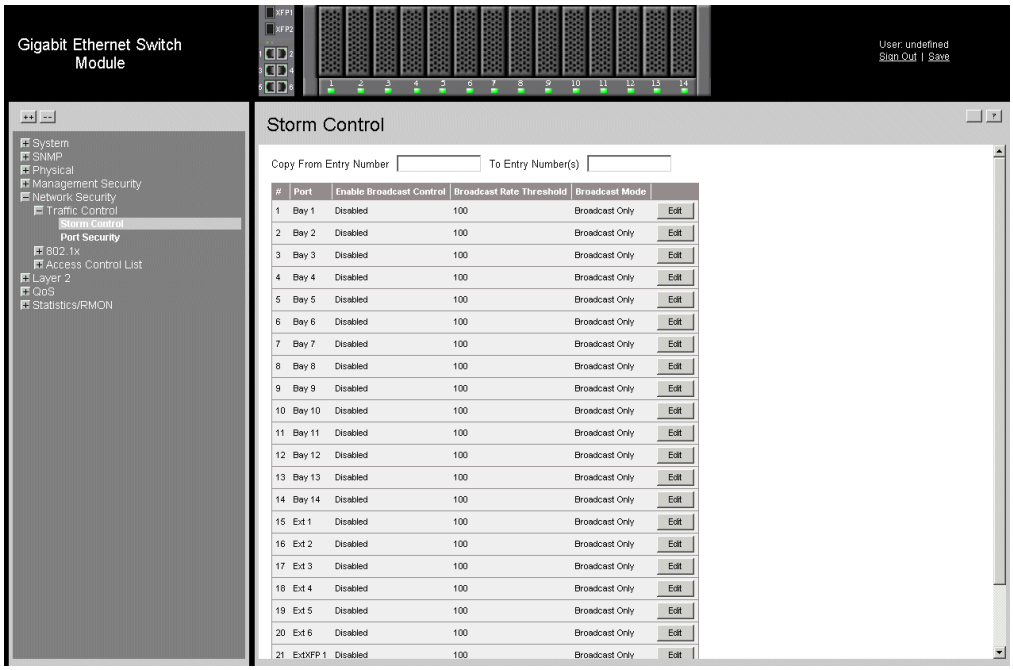



**Figure 41. Storm Control Page**

The *Storm Control Page* contains the following fields:

- **Copy From Entry Number** — Copies the storm control parameters from the selected port.
- **To Entry Number(s)** — Copies the storm control parameters to the selected port.
- **Unit No**. — Indicates the unit number.
- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control —** Indicates if forwarding Broadcast packet types 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 unknown packets are forwarded. The range is 70-1,000,000. The default value is 3500 and it is not possible to set the value lower than 3500.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  - — *Broadcast, Multicast, & Unknown Unicast* — Counts Unicast, Multicast, and Broadcast traffic.

— *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.

— *Broadcast Only* — Counts only Broadcast traffic.

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

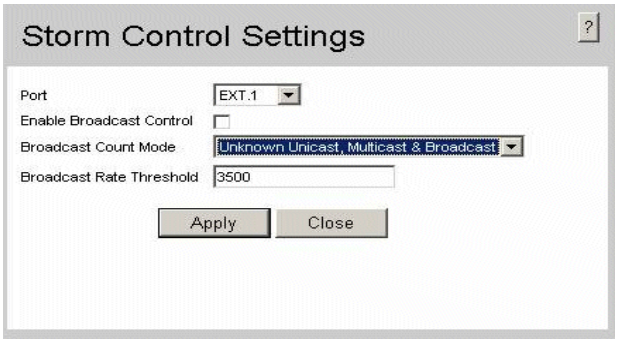



**Figure 42. Storm Control Settings Page**

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.

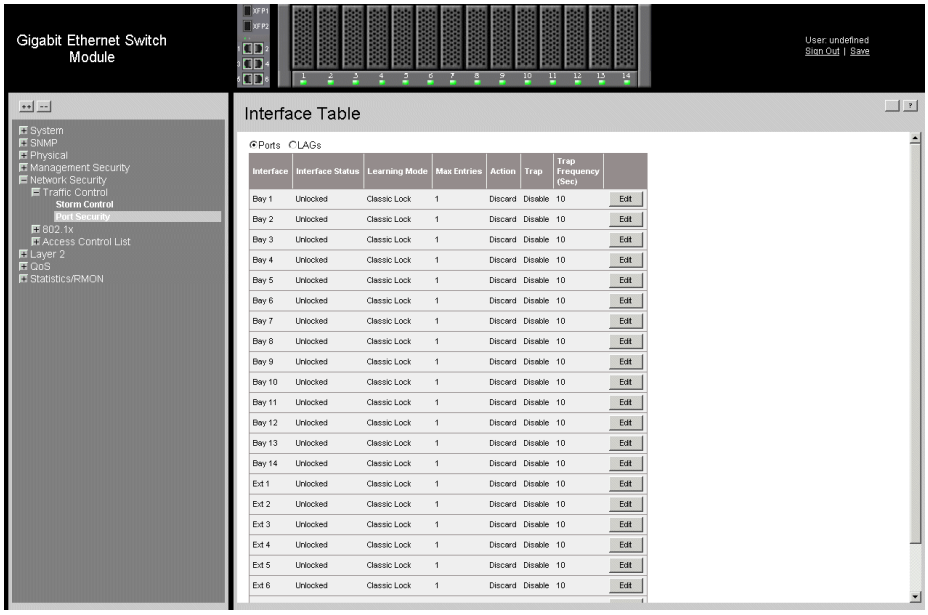



**Figure 43. Port Security Page**

The *Port Security Page* contains the following fields:

- **Port** — 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 Set Port 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. 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 Set Port 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 default value is 10 seconds.

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

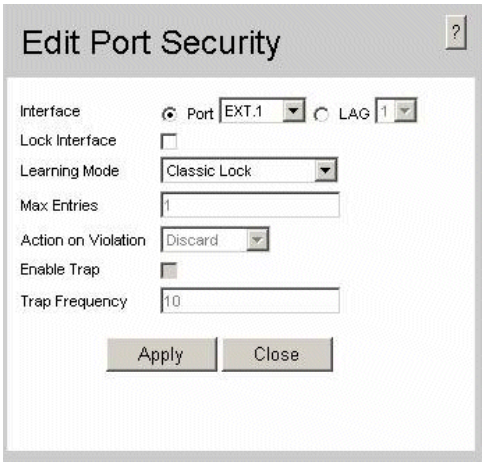



**Figure 44. Edit Port Security Settings Page**

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 and the ingress port is disabled. 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 made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 1024. The following filters can be defined as ACEs:

- **Source Port IP Address and Wildcard Mask** — Filters the packets by the Source port IP address and wildcard mask.
- **Destination Port IP Address and Wildcard Mask** — Filters the packets by the Source port IP address and wildcard mask.
- **ACE Priority** — Filters the packets by the ACE priority.
- **Protocol** — Filters the packets by the IP protocol.
- **DSCP** — Filters the packets by the DiffServ Code Point (DSCP) value.
- **IP Precedence** — Filters the packets by the IP Precedence.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. 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.

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* page allows a MAC-based ACL to be defined. ACEs 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:

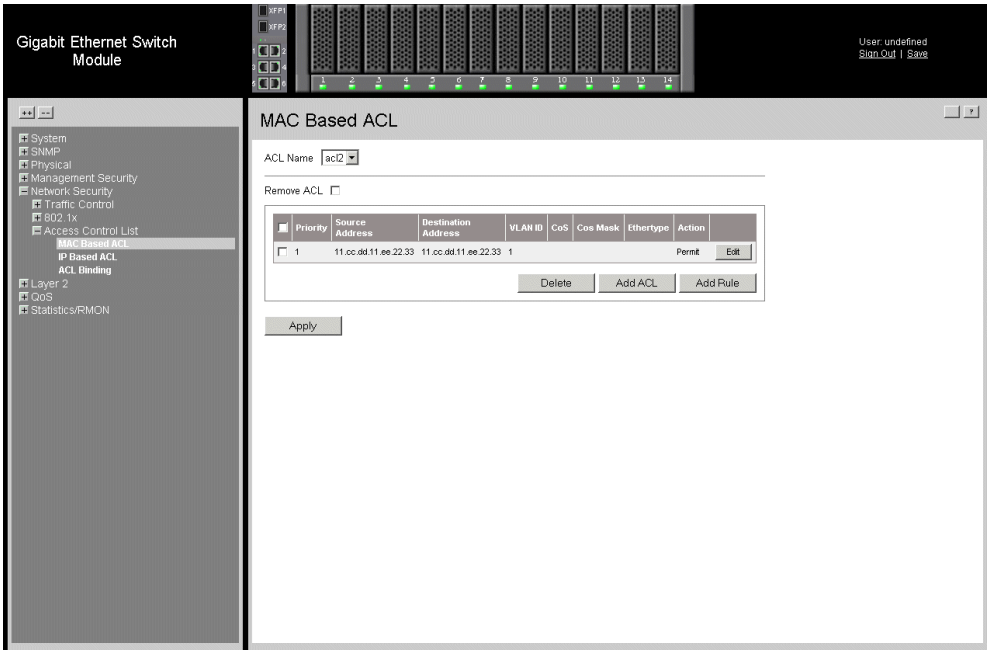



**Figure 45. MAC Based ACL Page**

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

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Remove** — Removes the IP based ACLs. The possible field values are:
  - *Checked* — Removes the selected MAC based ACL.
  - *Unchecked* — Maintains the MAC based ACLs.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source Address** — Matches the source MAC address to which packets are addressed to the ACE.
- **Source Mask** — Masks all or parts of the source IP address.
- **Destination Address** — Matches the destination MAC address to which packets are addressed to the ACE.
- **Destination Mask** — Masks all or parts of the destination IP address.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **CoS** — Classifies traffic based on the CoS tag value.
- **CoS Mask** — Defines the Cost of Service mask.

- **Ethertype** — Provides an identifier that differentiates between various types of protocols.
- **Action** — Indicates the ACL forwarding action. Possible field values are:
  - — *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 *Interface Configuration Page*.

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

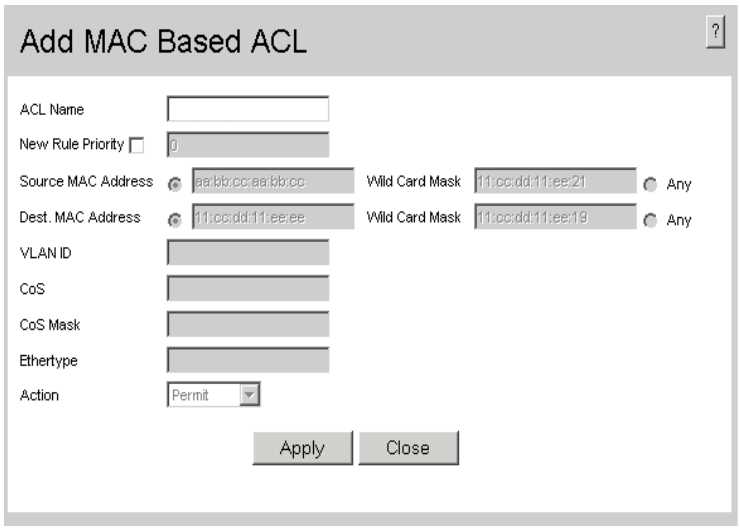



**Figure 46. Add MAC Based ACL Page**

3. Define the relevant fields.
4. Click Apply . The MAC Based ACLs are defined, and the device is updated.

To modify an IP-based ACL:

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

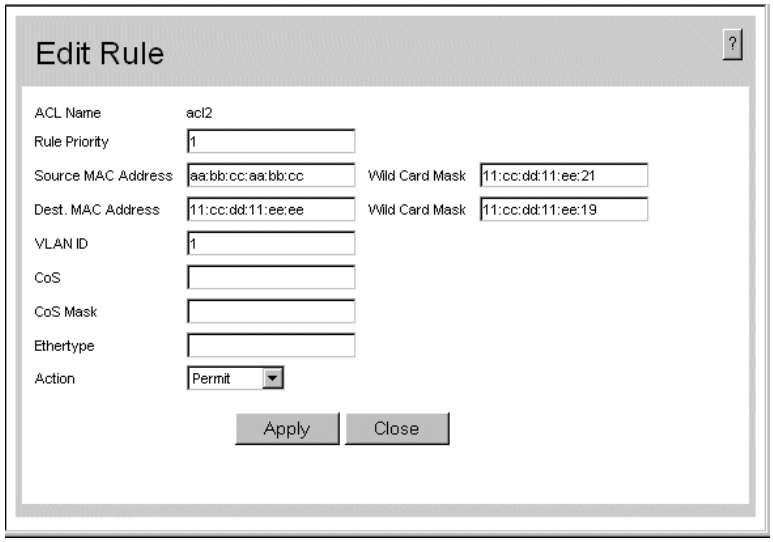



**Figure 47. Edit Rule Page**

3. Modify the relevant fields.
4. Click Apply . The MAC based protocol is defined, and the device is updated.

## Defining IP Based Access Control Lists

The *IP Based ACL Page* contains information for defining IP Based ACLs, including defining the ACEs defined for IP Based ACLs.

To define IP Based ACLs:

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

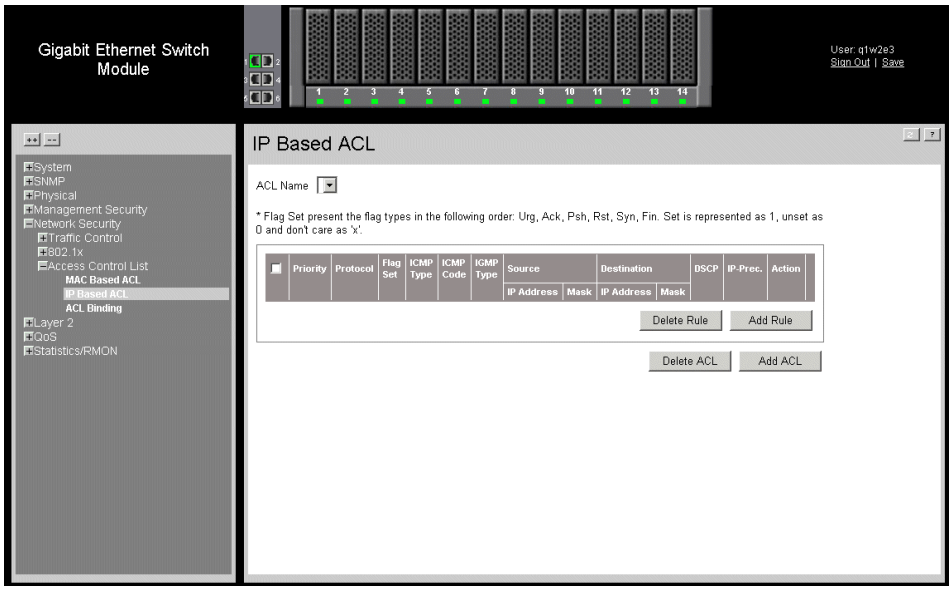



**Figure 48. IP Based ACL Page**

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

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Remove** — Removes the IP based ACLs. The possible field values are:
  - — *Checked* — Removes the selected IP based ACL.
  - — *Unchecked* — Maintains the IP based ACLs.
- **Priority** — Indicates the ACE priority that determines which ACE is matched to a packet based on a first-match basis. The possible field value is 1-2147483647.
- **Protocol** — Creates an ACE based on a specific protocol.
  - — *Select from List* — Selects from a protocols list on which ACE 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.

**IPV6** — *Internet Routing Protocol version 6* (IPv6). Provides a newer version of the Internet Protocol, and follows IP version 4 (IPv4). IPv6 increases the IP address size from 32 bits to 128 bits. In addition, IPv6 support more levels of addressing hierarchy, more addressable nodes, and supports simpler auto-configuration of addresses.

**IPV6:ROUTE** — Matches packets to the *IPv6 Route* through a Gateway (IPV6:ROUTE).

**IPV6:FRAG** — Matches packets to the *IPv6 Fragment Header* (IPV6:FRAG).

**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.

**IPV6:ICMP** — Matches packets to the  Matches packets to the IPv6 and Internet Control Message Protocol.

**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) Tunnelling 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 to access 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 To Match*— Adds user-defined protocols by which packets are matched to the ACE. 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 wild card 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 ACE.
- **Destination Mask** —Indicates the destination IP Address wild card mask. Wild cards are used to mask all or part of a destination IP Address. Wild card masks specify which bits are used and which bits are ignored. A wild card 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 important. For example, if the destination IP address 149.36.184.198 and the wildcard mask are 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.
- **Source Port** — Defines the TCP/UDP source port to which the ACE 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 ACE.
- **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 ACE. 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 ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.

- **Action** — The ACL forwarding action. Possible values are:
  - — *Permit* — Forwards packets which meet the ACL criteria.
  - — *Deny* — Drops packets which meet the ACL criteria.
  - — *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed.

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

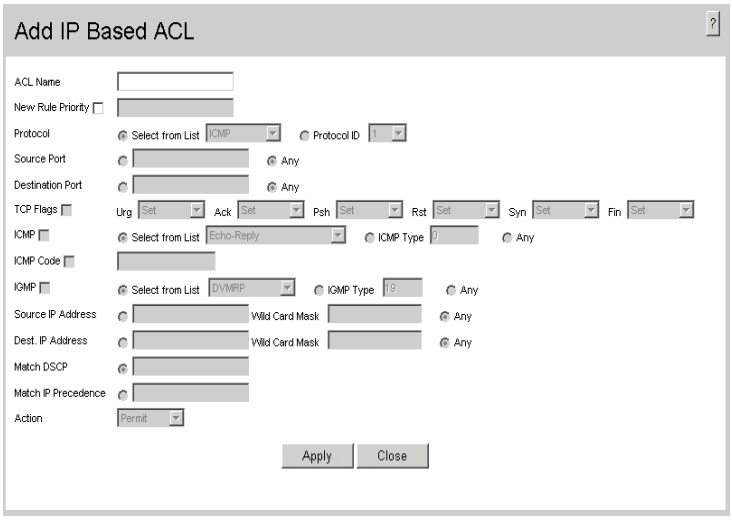



**Figure 49. Add IP Based ACL Page**

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

To modify an IP-based ACL:

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

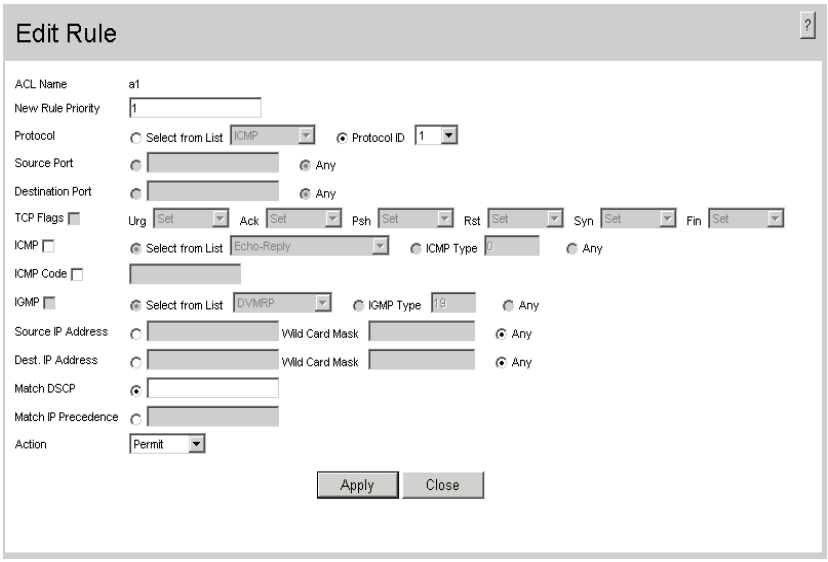



**Figure 50. IP Based ACL Settings Page**

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

## Binding Device Security ACLs

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface.Whenever an ACL is assigned on a port, LAG or, VLAN, 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:

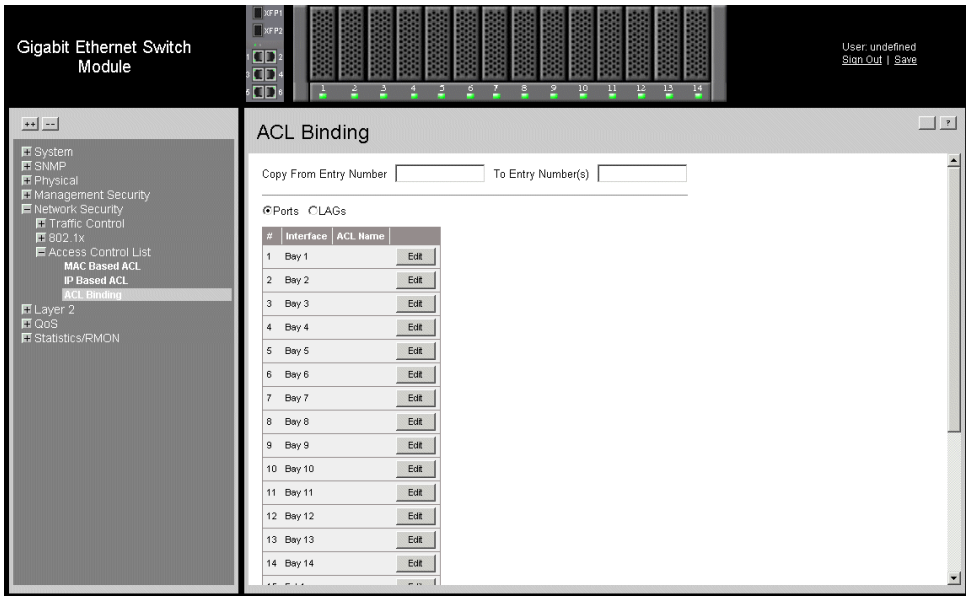



**Figure 51. ACL Binding Page**

The *ACL Binding Page* contains the following fields:

- **Copy from Entry Number** — Copies the ACL information from the defined interface.
- **To Entry Number(s)** — Copies the ACL information to the defined interface.
- **Ports** — Indicates the port membership.
- **LAGs** — Indicates the LAG membership.
- **Unit No**. — Indicates the unit number.
- **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 *Bind ACL Settings Page* opens:

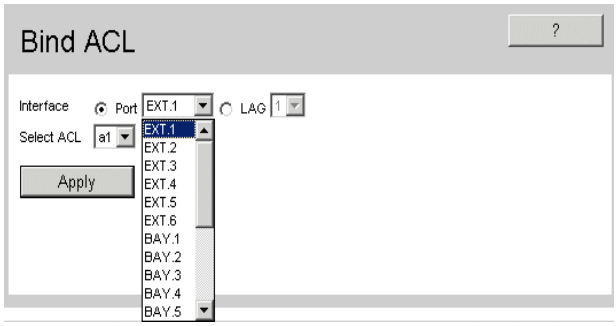



**Figure 52. Bind ACL Settings Page**

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

# 7 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.

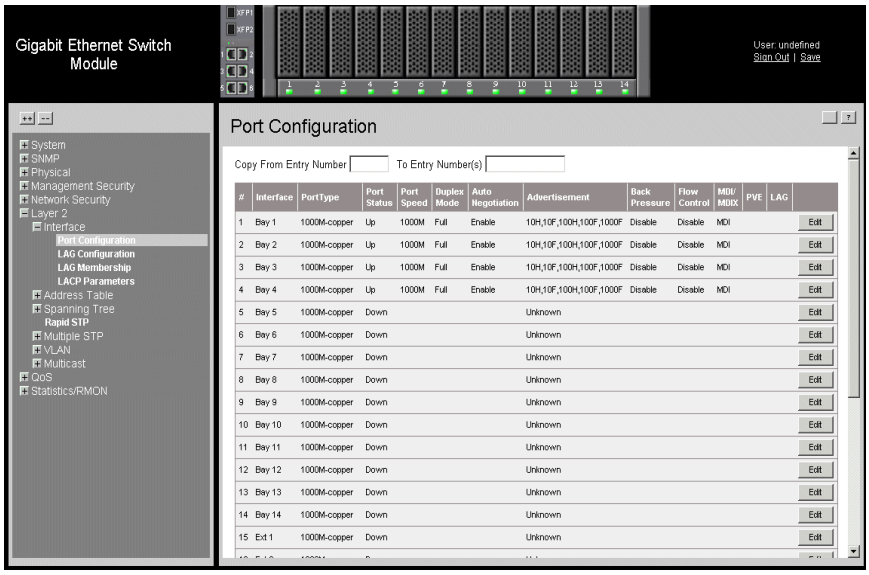



**Figure 53. Port Configuration Page**

The *Port Configuration Page* contains the following fields:

- **Copy From Entry Number** — Copies port authentication information from the selected port.
- **To Entry Number(s)** — Copies port authentication information to the selected port(s).
- **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.
  - *10G-FiberOptics* — Indicates the port has a fiber optic 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.
  - *10G* — Indicates the port is currently operating at 10 Gbps.
  - *100* — Indicates the port is currently operating at 100 Mbps.
  - *1000* — Indicates the port is currently operating at 1000 Mbps.
- **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** — Indicates the Private VLAN Edge.
- **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:

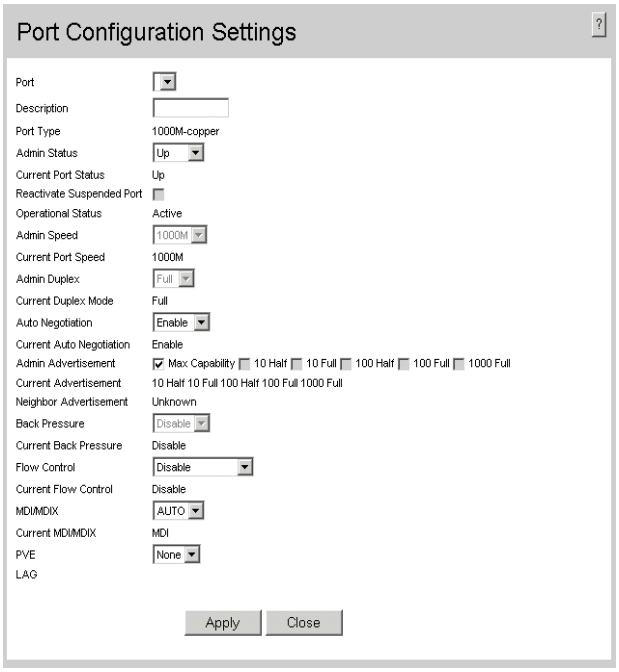



**Figure 54. Port Configuration Settings Page**

2. Modify the relevant fields.
3. Click Apply . The port configuration settings are defined, and the device is updated.

# 8 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.
- Auto-negotiation mode is not configured on the port.
- 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 back pressure and 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 64 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.

This section contains the following topics:

- Configuring LAGs
- Defining LAG Members
- Configuring LACP

# 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:

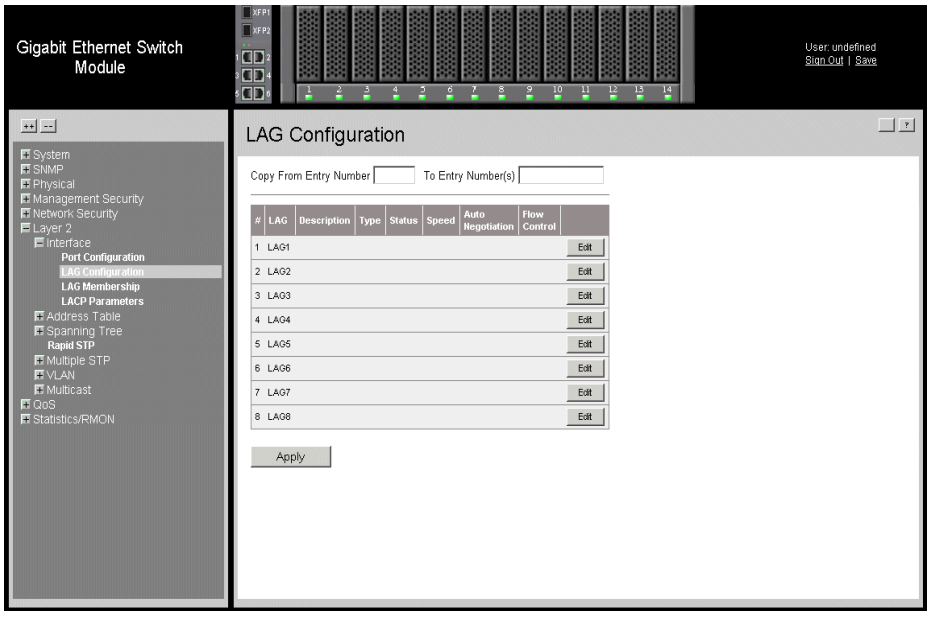



**Figure 55. LAG Configuration Page**

The *LAG Configuration Page* contains the following fields:

- **Copy From Entry Number** — Copies LAG configuration information from the selected port.
- **To Entry Number(s)** — Copies LAG configuration information to the selected port.
- **Unit No**. — Indicates the unit number.
- **LAG** — Indicate 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 disable 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.

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:

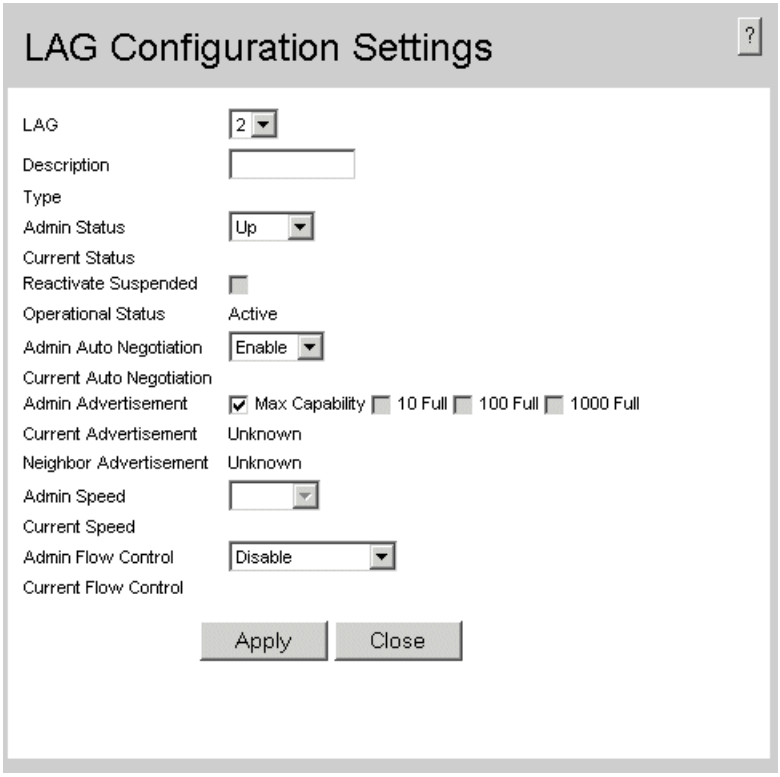



**Figure 56. LAG Configuration Settings Page**

2. Define the relevant fields.
3. Click Apply . 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 eight LAGs per system.

To define LAG parameters:

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

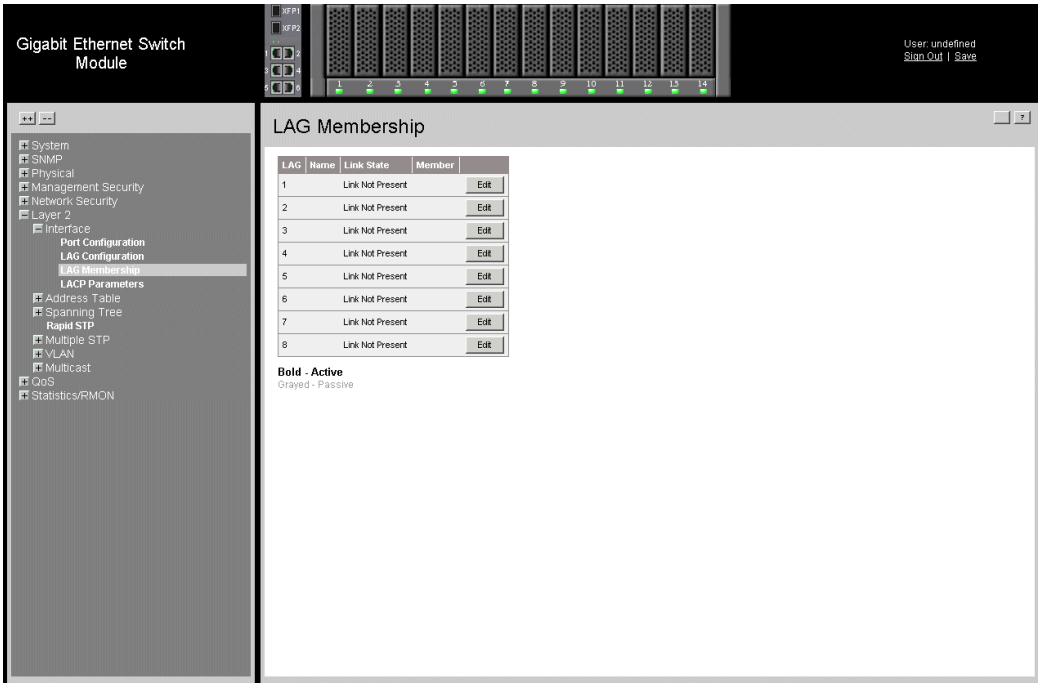



**Figure 57. LAG Membership Page**

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:

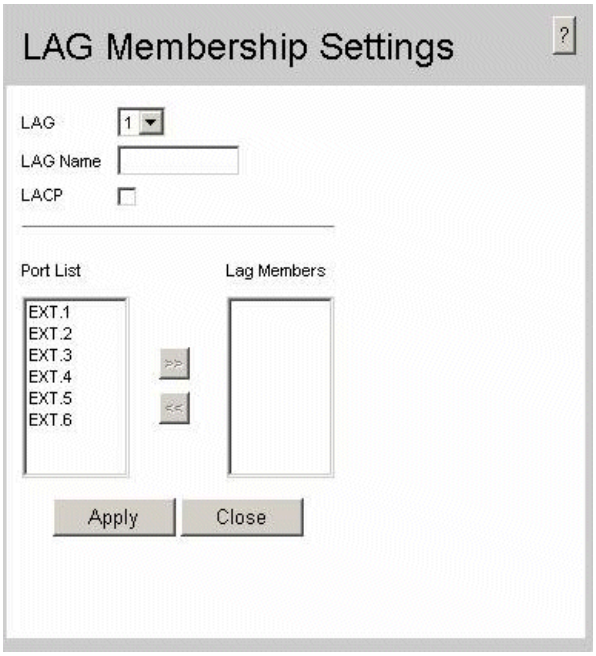



**Figure 58. LAG Membership Settings Page**

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** tab. The *LACP Parameters Page* opens:

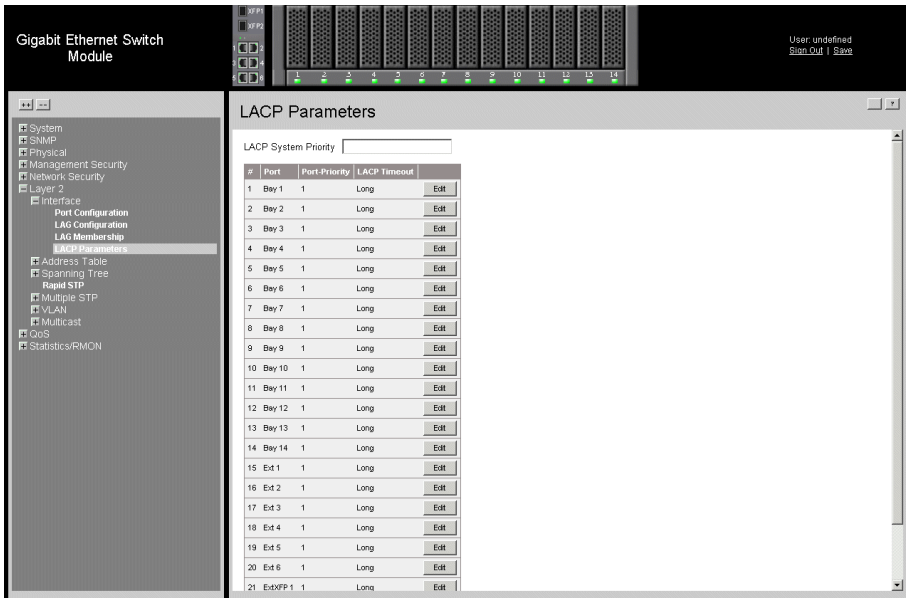



**Figure 59. LACP Parameters Page**

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.
- **Unit No**. — Indicates the unit number.
- **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.
- **LACP Timeout** — Displays the administrative LACP timeout. The possible field values are:
  - *Long* — Specifies the long timeout value. (Range: 1 - 200,000,000)
  - *Short* — Specifies the short timeout value. (Range: 1 - 65,535)

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:

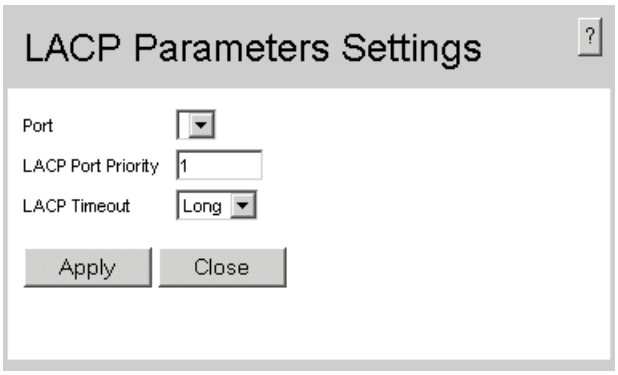



**Figure 60. LACP Parameters Settings Page**

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

# 9 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, and can be created per unit, per device, or through any other logical connection combination, 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 GARP (Generic Attribute Registration Protocol) 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.

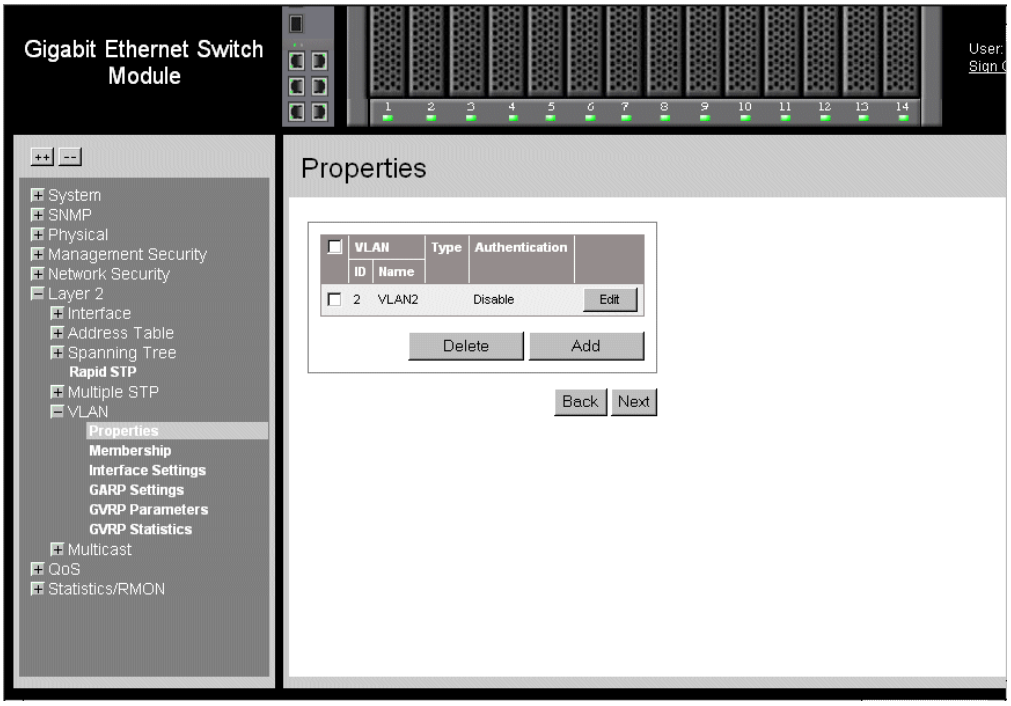



**Figure 61. VLAN Properties Page**

The *VLAN Properties Page* contains the following fields:

- **Remove**— Removes VLANs. The possible field values are:
  - *Checked* — Removes 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.

- **Authentication** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - — *Enable* — Enables unauthorized users to use the Guest VLAN.
  - — *Disable* — Disables unauthorized users from using the Guest 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:

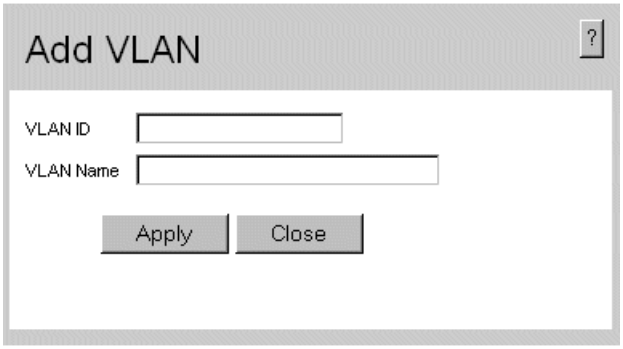



**Figure 62. Add VLAN Page**

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 Edit . The *Authentication VLAN Settings Page* opens:

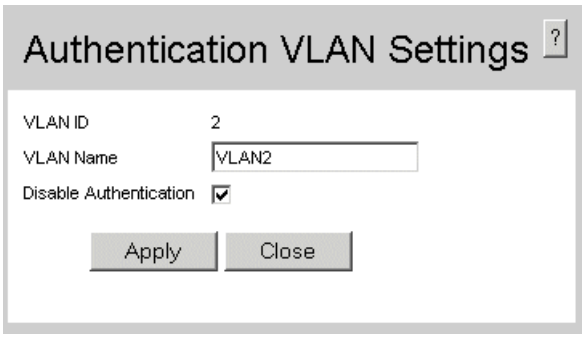



**Figure 63. Authentication VLAN Settings Page**

2. Modify the relevant fields.
3. Click Apply . The VLAN ID is defined, and the device is updated.

# Defining VLAN Membership

The *VLAN Membership Page* contains a table that maps VLAN parameters to ports. Ports 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.

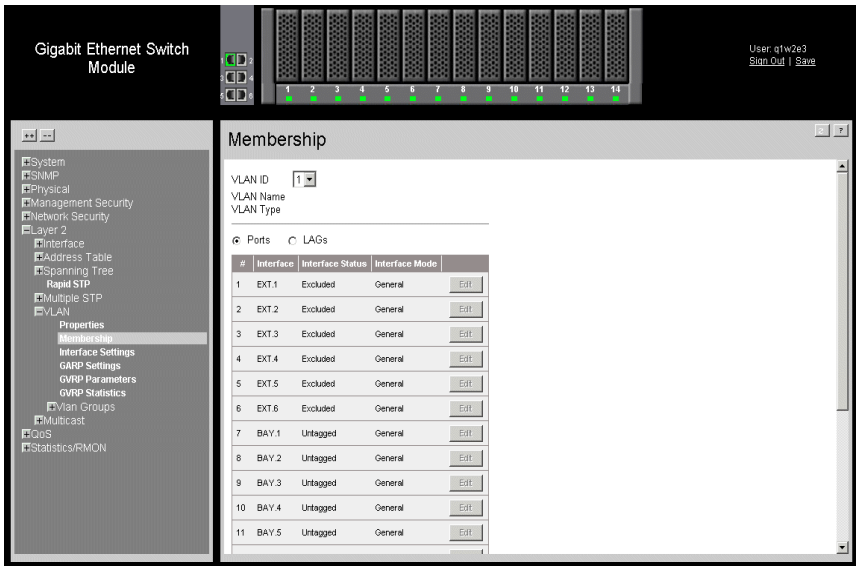



**Figure 64. VLAN Membership Page**

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.
- **Unit No**. — Displays the unit number.
- **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.

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:

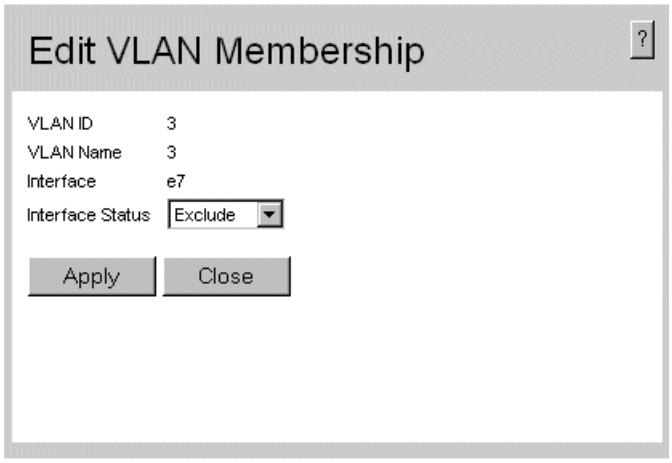



**Figure 65. Edit VLAN Membership Page**

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

# Defining VLAN Interface Settings

The *VLAN Interface Settings Page* contains fields for managing ports that are part of a VLAN. The *Port Default VLAN ID* (PVID) is configured on the *VLAN 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 *VLAN Interface Settings Page* opens.

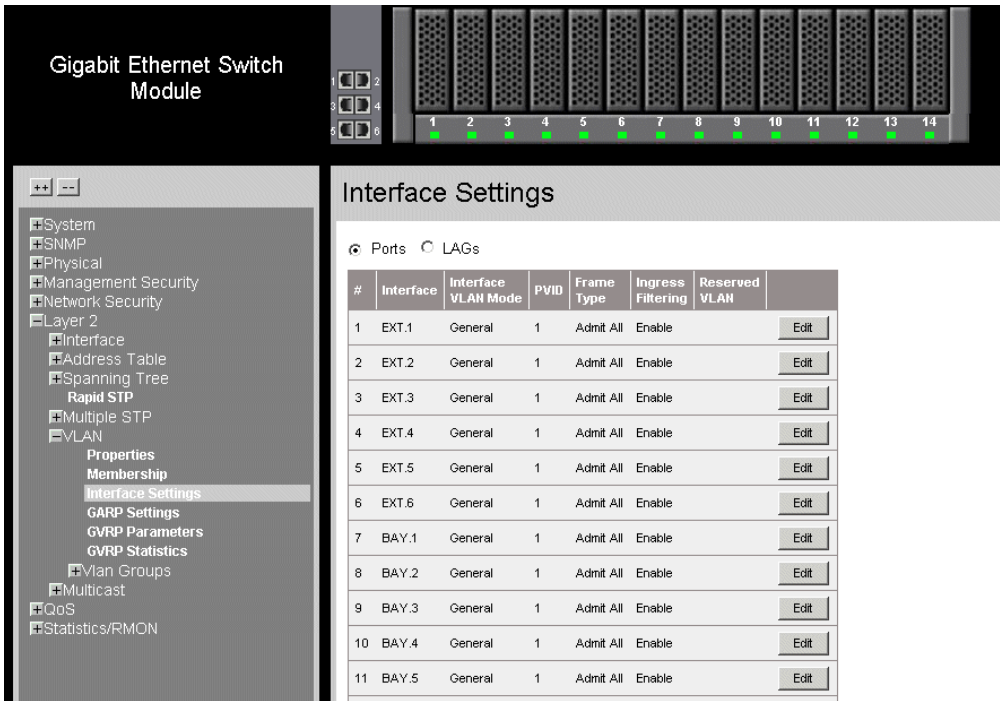



**Figure 66. VLAN Interface Settings Page**

The *VLAN Interface Settings Page* contains the following fields:

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

  - *Trunk* — Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.

- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1-4094. 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 port. The possible field values are:
  - *Admit All* — Both tagged and untagged packets are accepted on the port.
  - *Admit Tag Only* — Only tagged packets are accepted on the port.
- **Ingress Filtering**— Indicates whether ingress filtering is enabled on the port. The possible field values are:
  - *Enable* — Enables ingress filtering on the device. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.
  - *Disable* — Disables ingress filtering on the device.
- **Reserve VLAN** — Indicates the VLAN selected by the user to be the reserved VLAN if not in use by the system.

# 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 Interface Settings 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 Interface Settings Page* opens:

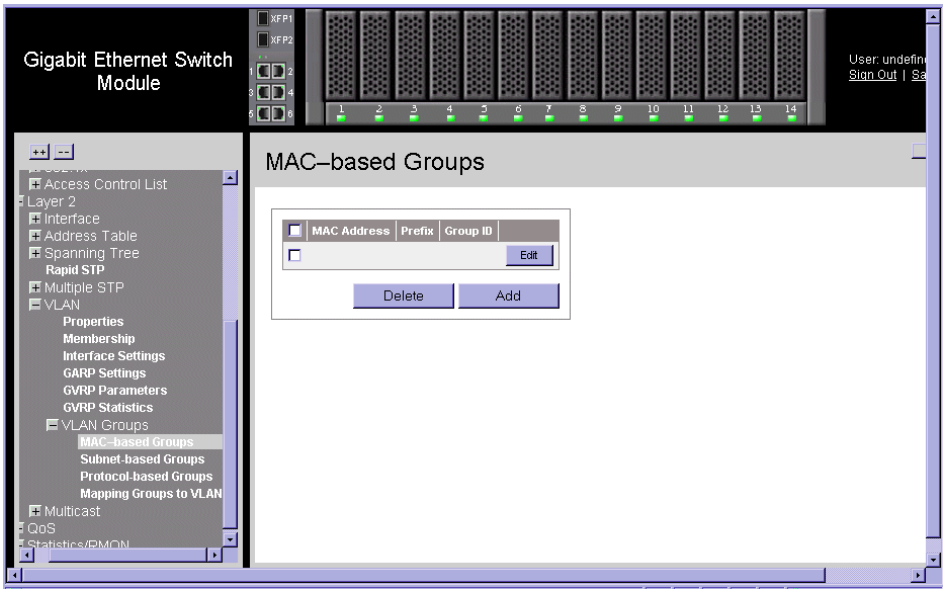



**Figure 67. VLAN MAC-based Groups Page**

The *VLAN Interface Settings Page* contains the following fields:

- **MAC Address** — Displays the MAC address associated with the VLAN group.
- **Prefix** — Displays the network prefix associated with the VLAN group. Prefix matches determine the best next-hop route for a packet based solely on the destination address contained in the packet header.
- **Group ID** — Displays the VLAN Group ID.

2. Click Add. The *VLAN Interface Settings Page* opens:

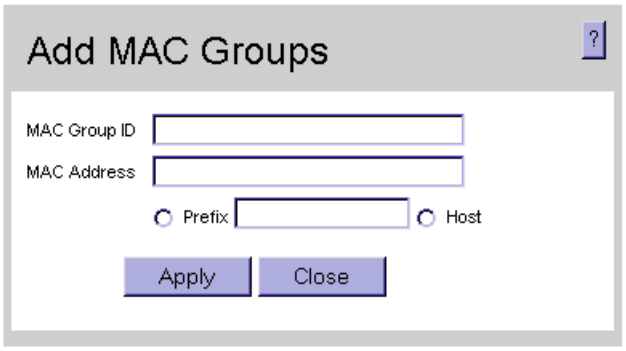



**Figure 68. Add VLAN MAC-based Groups Page**

In addition to the fields in the *VLAN Interface Settings Page*, the *VLAN Interface Settings Page* contains the following additional fields:

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

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

To modify a MAC Based VLAN Group:

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

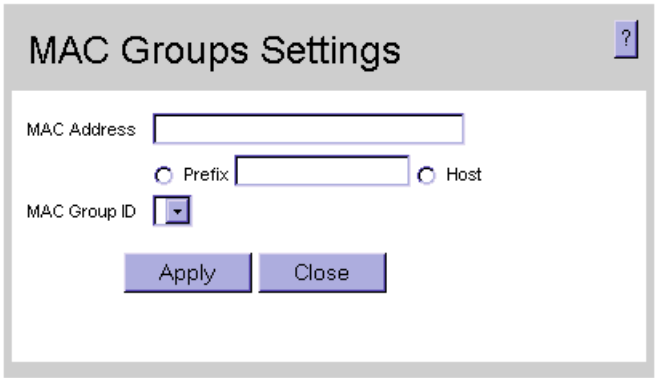



**Figure 69. MAC Groups Settings Page**

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

# Defining VLAN Subnet Based Groups

The *VLAN Interface Settings Page* allows network managers to group VLANs based on their subnet. To define VLAN MAC Based Groups:

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

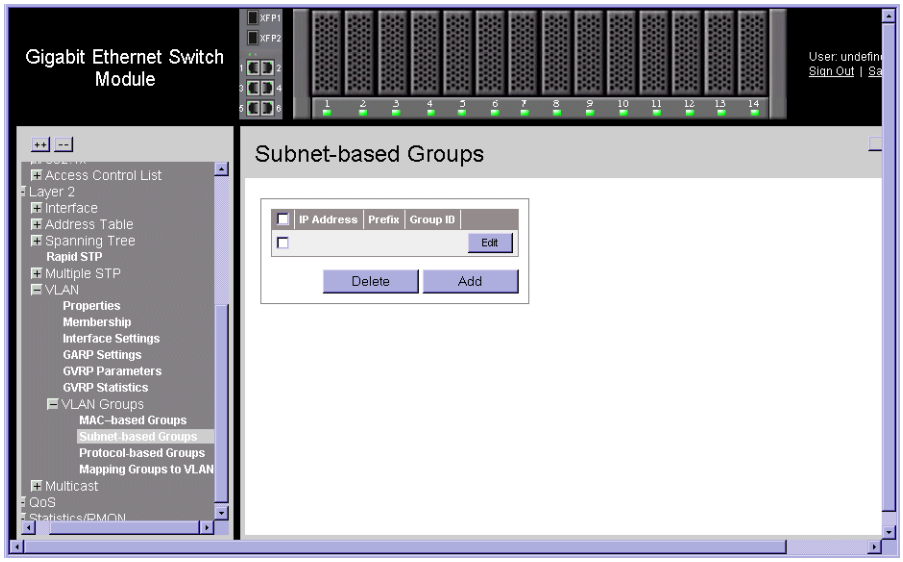



**Figure 70. VLAN Subnet-based Groups Page**

The *VLAN Interface Settings Page* contains the following fields:

- **MAC Address** — Displays the MAC address associated with the VLAN subnet group.
- **Prefix** — Displays the network prefix associated with the VLAN group. Prefix matches determine the best next-hop route for a packet based solely on the destination address contained in the packet header.
- **Group ID** — Displays the VLAN group ID associated with the VLAN subnet group.

2. Click Add. The *VLAN Interface Settings Page* opens:

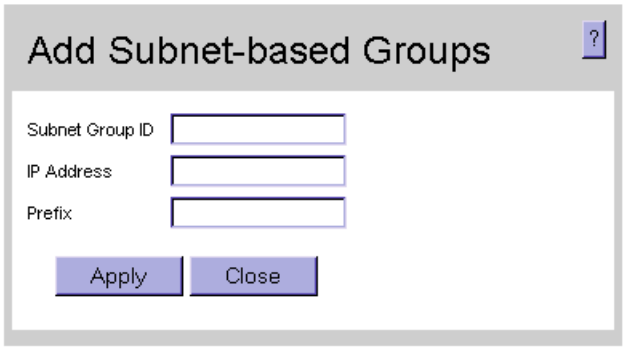



**Figure 71. Add VLAN Subnet-based Groups Page**

In addition to the fields in the *VLAN Interface Settings Page*, the *VLAN Interface Settings Page* contains the following additional field:

- **IP Address** — Displays the IP address associated with the VLAN subnet group.

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 Interface Settings Page* opens.
2. Click Edit. The *Subnet-based Group Settings* opens.

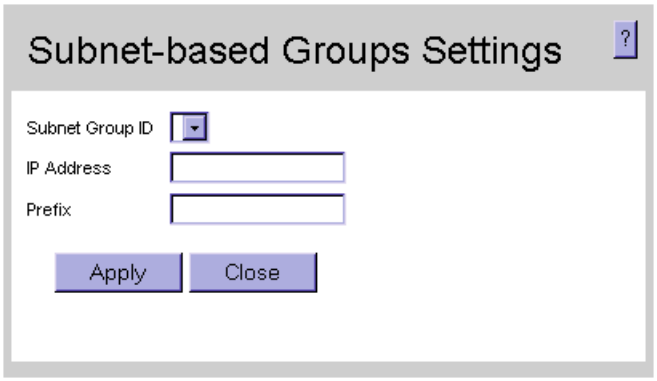



**Figure 72. Subnet-based Group Settings**

# 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 Interface Settings Page* opens:

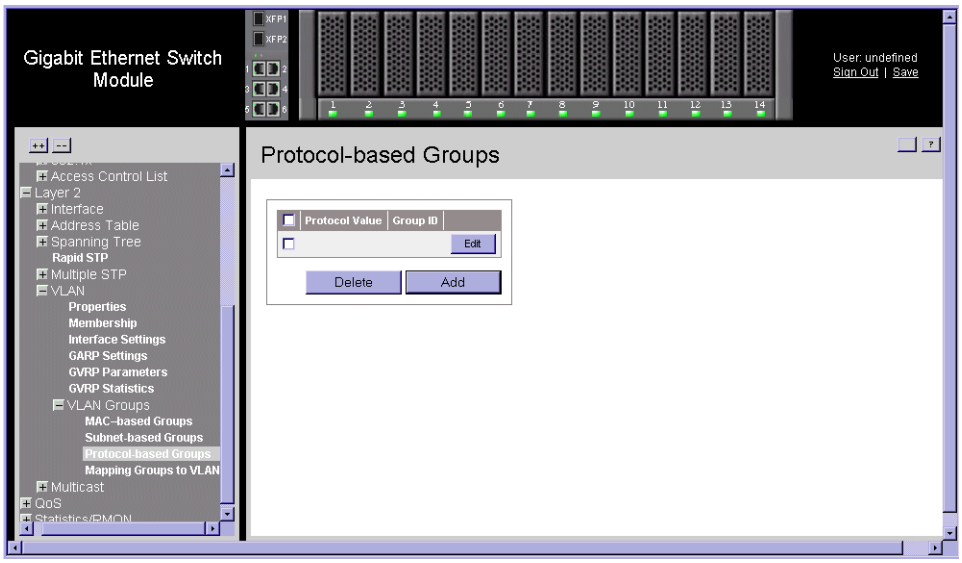



**Figure 73. VLAN Protocol Groups Page**

The *VLAN Interface Settings Page* contains the following fields:

- **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 *VLAN Interface Settings Page* opens:

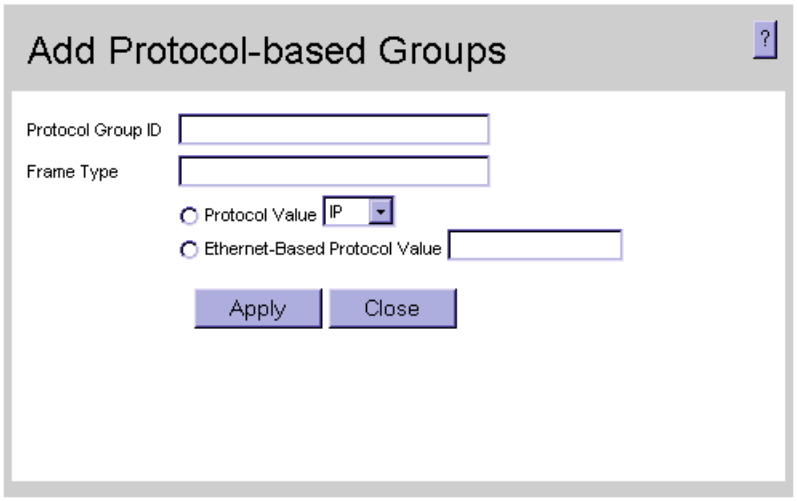



**Figure 74. Add Protocol-based Groups Page**

In addition to the fields in the *VLAN Interface Settings Page*, the *VLAN Interface Settings Page* contains the following additional fields:

- **Protocol Value** — Displays the protocol group type. The possible field values are:
  - *IP*
  - *IPX*
  - *IPv6*
  - *ARP*
- **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 Interface Settings Page* opens.
2. Click Edit. The *Protocol-based Groups Settings Page* opens:

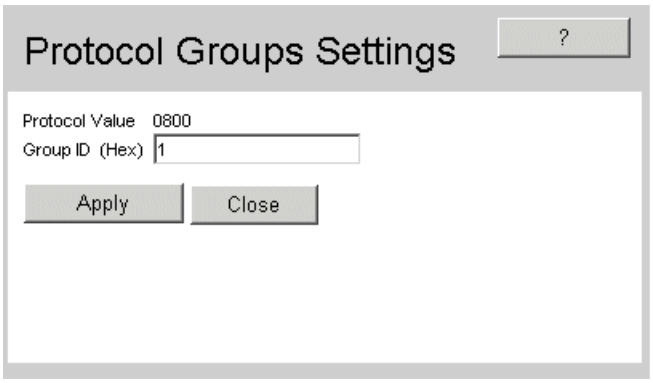



**Figure 75. Protocol-based Groups Settings Page**

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

# Mapping Groups to VLANs

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

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

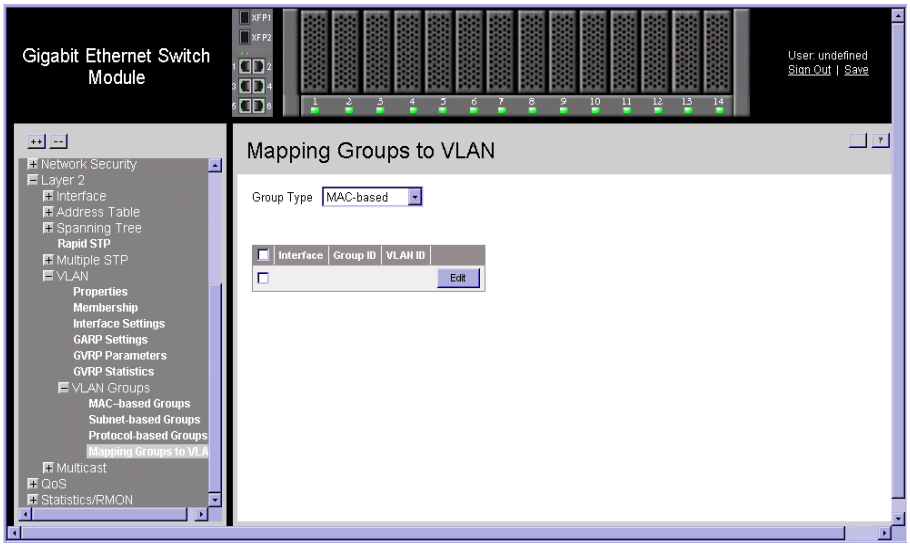



**Figure 76. Mapping Groups to VLAN Page**

The *VLAN Interface Settings 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. The possible field values are:
  - — *Checked* — Indicates the VLAN is attached to the selected VLAN group.
  - — *Unchecked* — Indicates the VLAN is not attached to the selected VLAN group.
- **Group ID** — Displays the VLAN Group ID.
- **VLAN ID** — Displays the VLAN ID.

2. Select a port.
3. Click Edit . The *VLAN Interface Settings Page* opens:

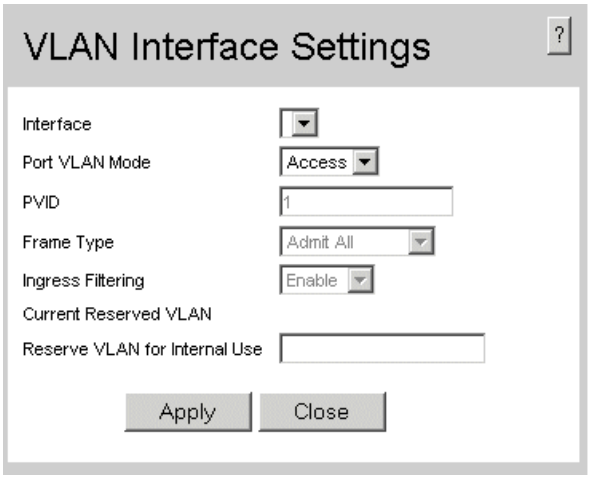



**Figure 77. VLAN Interface Settings Page**

4. Define the relevant fields.
5. Click Apply . The VLAN interface settings 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

*Generic Attribute Registration Protocol* (GARP) protocol 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:

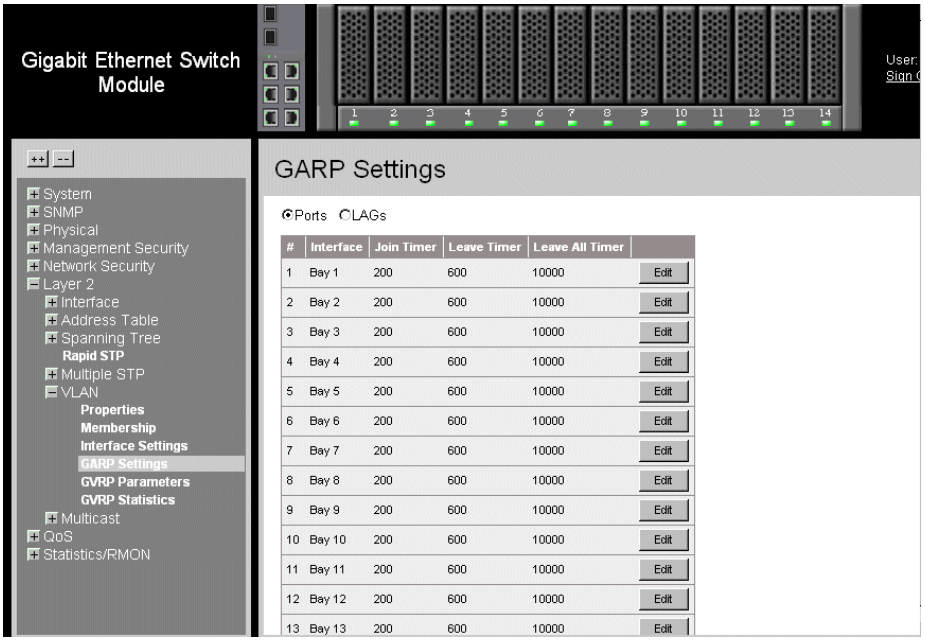



**Figure 78. GARP Settings Page**

The *GARP Settings Page* contains the following fields:

- **Ports** — Displays the Port GARP settings.
- **LAGs** — Displays the LAG GARP settings.
- **Unit No**. — Indicates the unit number.
- **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 device 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:

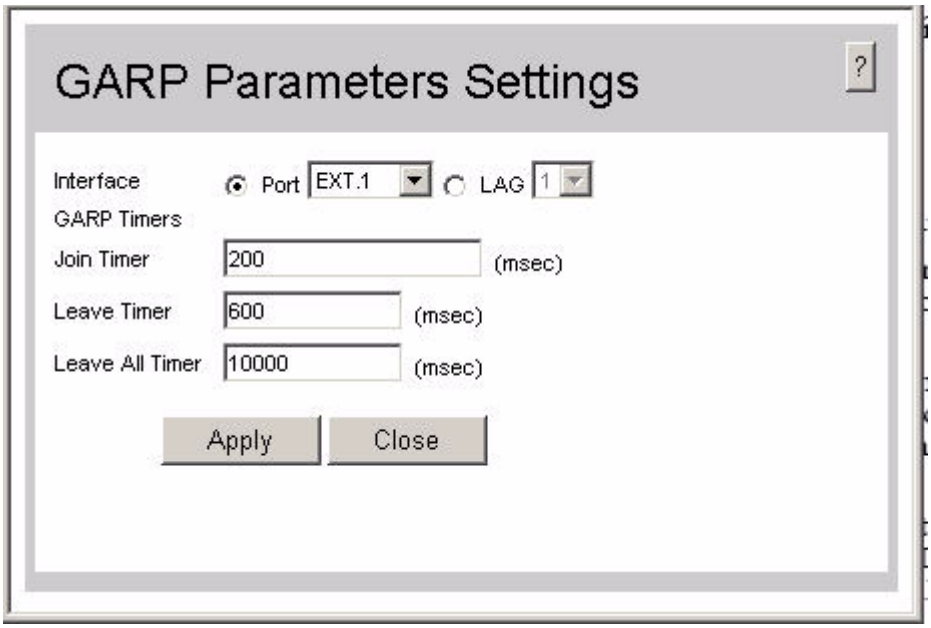



**Figure 79. GARP Parameters Settings Page**

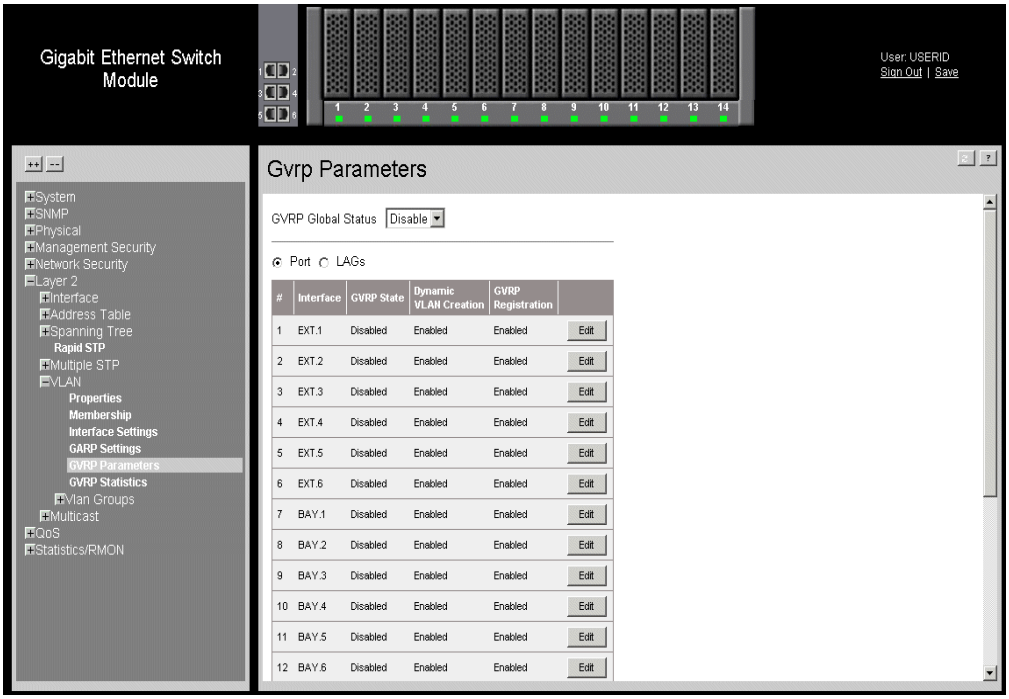
3. Define the relevant fields.
4. Click Apply . The GARP parameters are defined, and the device is updated.

# 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:




| # | Interface | GVRP State | Dynamic VLAN Creation | GVRP Registration | |
|---|---|---|---|---|---|
| 1 | EXT.1 | Disabled | Enabled | Enabled | Edit |
| 2 | EXT.2 | Disabled | Enabled | Enabled | Edit |
| 3 | EXT.3 | Disabled | Enabled | Enabled | Edit |
| 4 | EXT.4 | Disabled | Enabled | Enabled | Edit |
| 5 | EXT.5 | Disabled | Enabled | Enabled | Edit |
| 6 | EXT.6 | Disabled | Enabled | Enabled | Edit |
| 7 | BAY.1 | Disabled | Enabled | Enabled | Edit |
| 8 | BAY.2 | Disabled | Enabled | Enabled | Edit |
| 9 | BAY.3 | Disabled | Enabled | Enabled | Edit |
| 10 | BAY.4 | Disabled | Enabled | Enabled | Edit |
| 11 | BAY.5 | Disabled | Enabled | Enabled | Edit |
| 12 | BAY.6 | Disabled | Enabled | Enabled | Edit |

**Figure 80. 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 selected device.
  - — *Disable* — Disables GVRP on the selected device.
- **Ports** — Displays the Port GVRP settings.
- **LAGs** — Displays the LAG GVRP settings.
- **Unit No.** — Indicates the row number from which GVRP parameters are copied.
- **Interface** — Displays the port or LAG on which GVRP is enabled.

- **GVRP State**— Indicates if GVRP is enabled on the port. The possible field values are:
  - *Enable* — Enables GVRP on the selected port.
  - *Disable* — Disables GVRP on the selected port.
- **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 device. The possible field values are:
  - *Enable* — Enables GVRP registration on the device.
  - *Disable* — Disables GVRP registration on the device.

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:

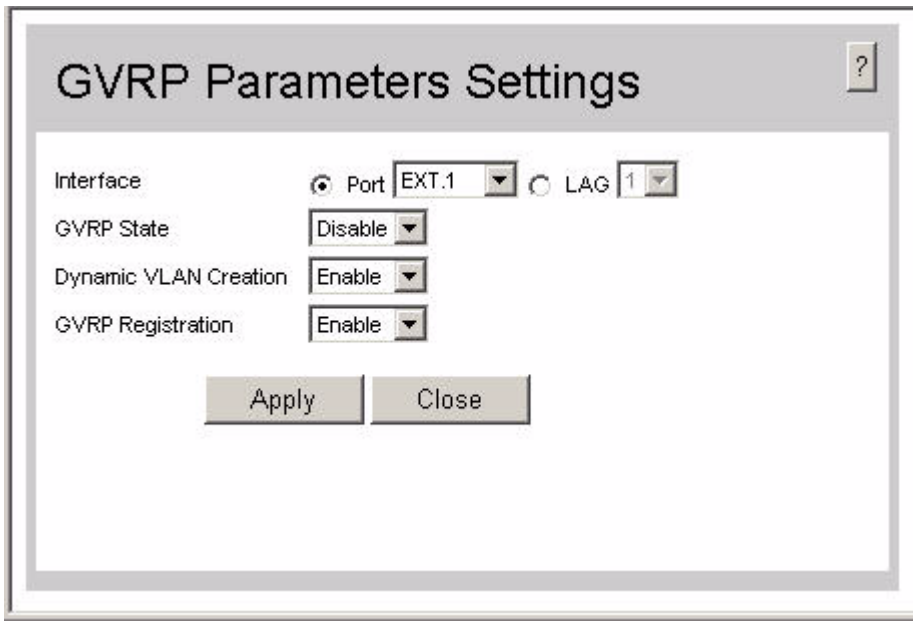



**Figure 81. GVRP Parameters Settings Page**

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

# 10 Configuring IP Information

This section provides information for defining device IP addresses, and includes the following topics:

- Configuring IP Interfaces
- Configuring Domain Name Servers

## Configuring IP Interfaces

This section contains information for defining IP interfaces and ARP settings, and includes the following sections:

- Defining IP Addresses
- Defining ARP Settings

### Defining IP Addresses

The *IP Interface Page* contains fields for assigning IP addresses. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces. Packets are forwarded to the default IP when frames are sent to a remote network via the default gateway. The configured IP address must belong to the same subnet of one of the IP interfaces. The *Dynamic Host Configuration Protocol* (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

To define an IP interface:

1. Click **System > IP Addressing > IP Interface.** The *IP Interface Page* opens:

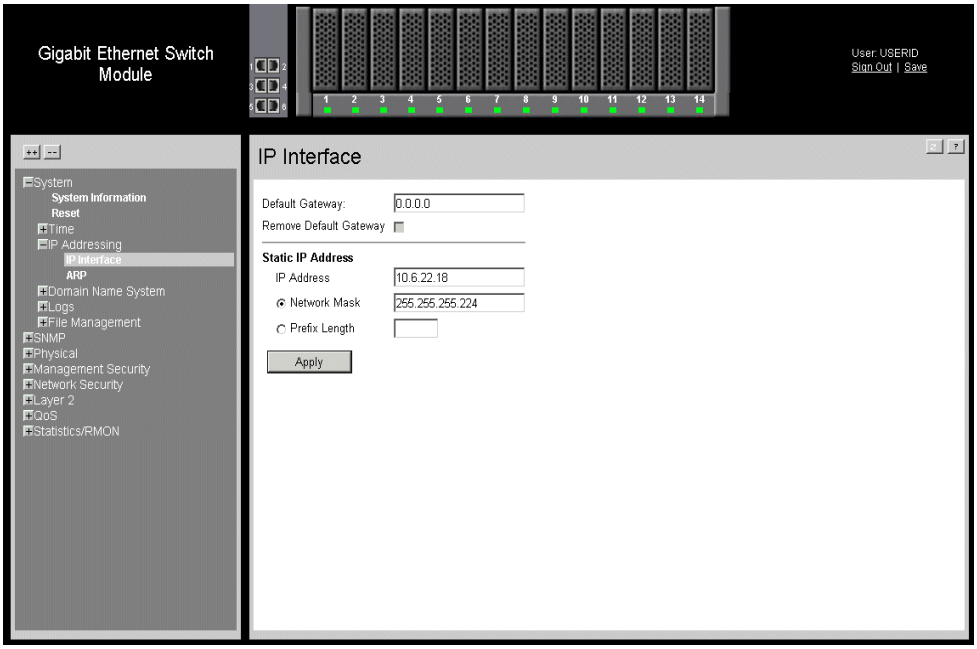



**Figure 82. IP Interface Page**

The *IP Interface Page* contains the following fields:

- **Default Gateway** — Defines the default gateway IP address.
- **Remove Default Gateway** — Removes the user defined IP address from the interface. The possible field values are:
  - *Checked* — Removes the user defined IP address from the interface.
  - *Unchecked* — Maintains the user defined IP address assigned to the Interface.
- **Static IP Address** — Indicates the currently configured IP address. The possible field values are:
  - *IP Address* — Displays the currently configured IP address.
  - *Network Mask* — Displays the currently configured IP address mask.
  - *Prefix Length* — Defines the number of bits that comprise the static IP address prefix.

2. Define the relevant fields.
3. Click Apply . The IP configuration fields are saved, and the device is updated.

# Defining ARP Settings

To define ARP settings:

1. Click **System > IP Addressing > ARP.** The *ARP Settings Page* opens:

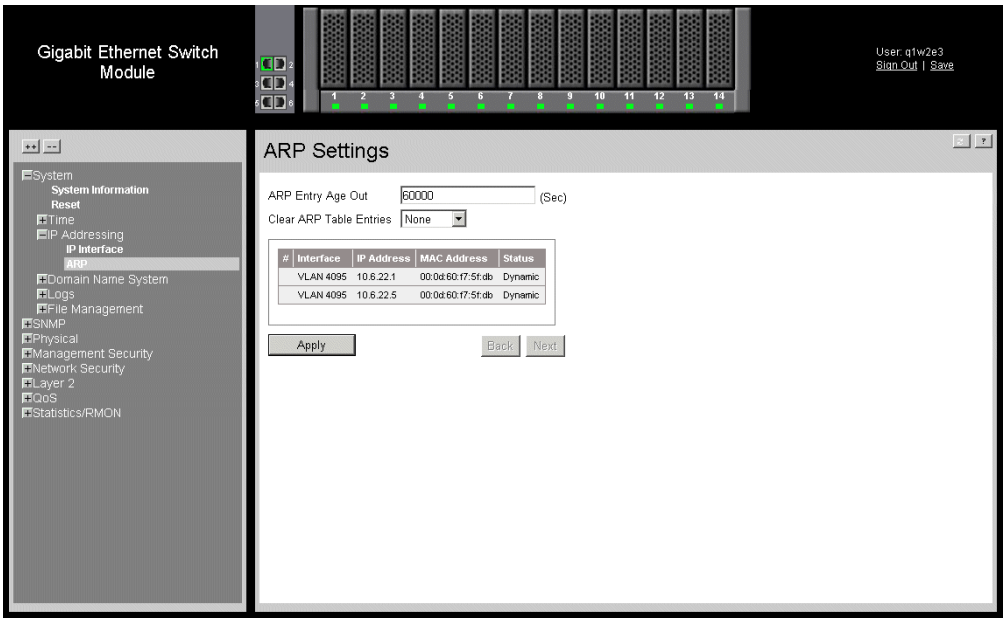



**Figure 83. ARP Settings Page**

The *Address Resolution Protocol* converts IP addresses into physical addresses. The ARP Settings page allows network managers to define ARP settings on the system.The *ARP Settings Page* contains the following fields:

- **ARP Entry Age Out** — Specifies the amount of time (in seconds) that passes between ARP Table entry requests. Following the ARP Entry Age period, the entry is deleted from the table. The range is 1 - 40000000. The default value is 60000 seconds.
- **Clear ARP Table Entries** — Specifies the types of ARP entries that are cleared. The possible values are:
  - *None* — Maintains the ARP entries.
  - *All* — Clears all ARP entries.
  - *Dynamic* — Clears only dynamic ARP entries.
  - *Static* — Clears only static ARP entries.
- **Unit No.** — Displays the unit number.

- **Interface** — Displays the interface used to manage the device. The possible selections are:
  - *Port* — Displays the port for which the IP address is defined.
  - *LAG* — Displays the LAG for which the IP address is defined.
  - *VLAN* — Displays the VLAN for which the IP address is defined.
- **IP Address** — Displays the IP address.
- **MAC Address** — Displays the MAC address.
- **Status** — Displays the status of the IP address. The possible selections are:
  - *Dynamic* — Displays the IP address dynamically retrieved from the DHCP Server.
  - *Static* — Displays the currently configured IP address.

2. Define the relevant fields.
3. Click Apply. The ARP settings are saved, and the device is updated.

# Configuring Domain Name Servers

*Domain Name System* (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated into 192.87.56.2. DNS servers maintain databases of domain names and their corresponding IP addresses.

This section contains the following topics:

- Defining DNS Servers
- Defining DNS Host Mapping

# Defining DNS Servers

The *DNS Server Page* contains fields for enabling and activating specific DNS servers.

To enable a DNS server:

1. Click **System > Domain Name System > DNS Server.** The *DNS Server Page* opens:

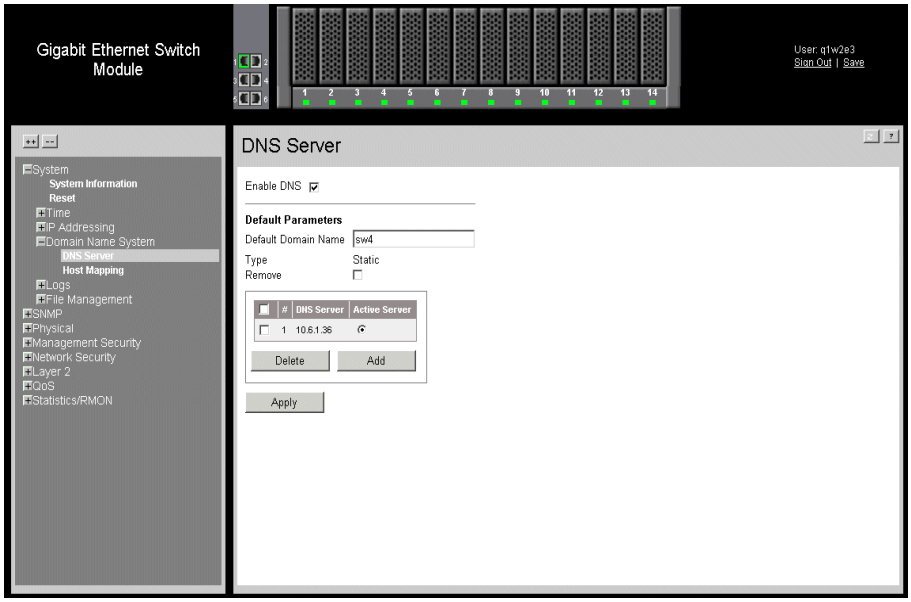



**Figure 84. DNS Server Page**

The *DNS Server Page* contains the following fields:

- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:
  - *Checked* — Translates the domains into IP addresses.
  - *Unchecked* — Disables translating domains into IP addresses.

**Default Parameters**

- **Default Domain Name** (1 -158 Characters) — Specifies the user-defined DNS server name.
- **Type** — Displays the IP address type. The possible field values are:
  - *DHCP* — The IP address is dynamically created.
  - *Static* — The IP address is a static IP address.
- **Remove** — Removes DNS servers. The possible field values are:
  - *Checked* — Removes the selected DNS server.
  - *Unchecked* — Maintains the current DNS server list.

The *DNS Server Page* also contains the following fields:

- **Remove**— The possible field values are:
  - — *Checked* — Removes the selected server.
  - — *Unchecked* — Maintains the current server list.
- **Unit No.** — Displays the unit number.
- **DNS Server** — Displays the DNS server IP address. DNS servers are added in the *Add DNS Server Page*.
- **Active Server**— Specifies the DNS server that is currently active.

2. Select *Enable DNS Status*.
3. Define the relevant fields.
4. Click Apply. The DNS server is enabled, and the device is updated.

To add a new DNS Server:

1. Click **System > Domain Name System > DNS Server.** The *DNS Server Page* opens.
2. Click Add. The *Add DNS Server Page* opens:

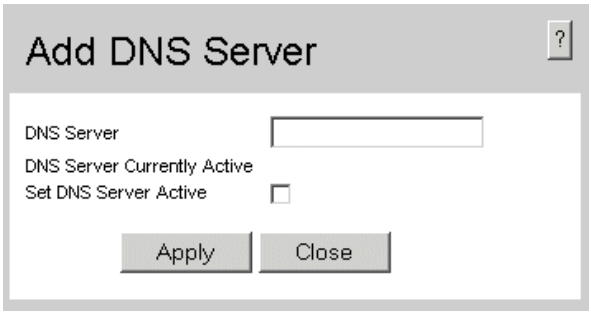



**Figure 85. Add DNS Server Page**

3. Define the relevant fields.
4. Click Apply. The DNS server is added, and the device is updated.

# Defining DNS Host Mapping

The *DNS Host Mapping Page* provides information for defining DNS Host Mapping.

To define DNS host mapping:

1. Click **System > Domain Name System > Host Mapping**. The *DNS Host Mapping Page* opens:

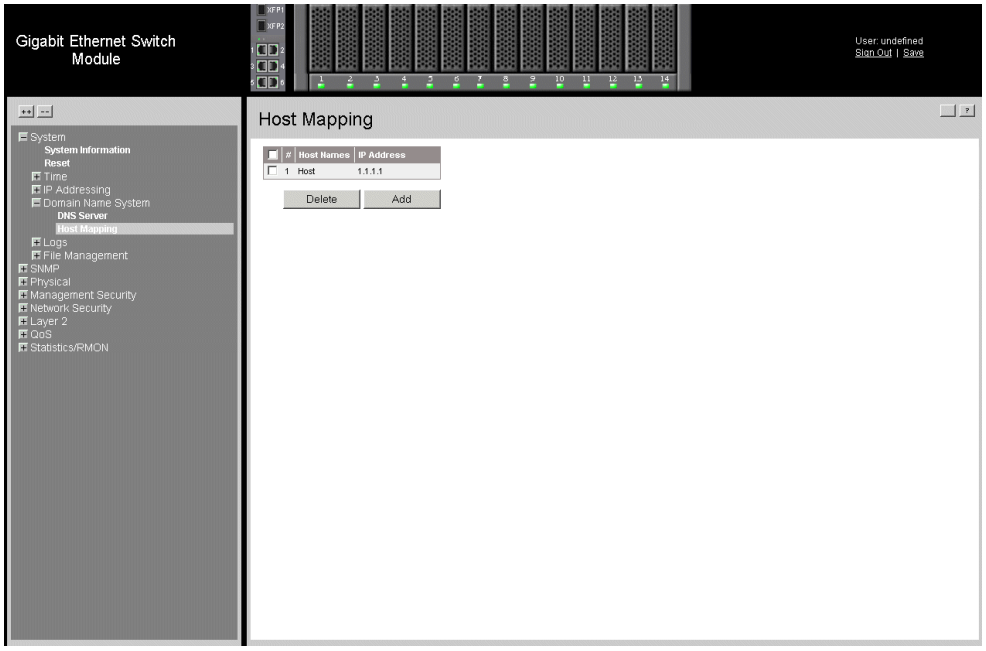



**Figure 86. DNS Host Mapping Page**

The *DNS Host Mapping Page* contains the following fields:

- **Remove** — Removes default domain names. The possible field values are:
  - — *Checked* — Removes the selected DNS host.
  - — *Unchecked* — Maintains the current DNS host mapping list.
- **Unit No.** — Displays the unit number.
- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.

2. Click Add . The *Add DNS Host Page* opens:

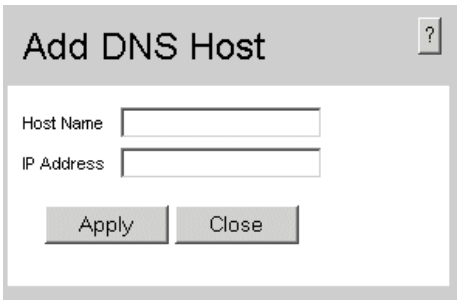



**Figure 87. Add DNS Host Page**

3. Define the relevant fields.
4. Click Apply . The DNS host is added, and the device is updated.

# 11 Defining the Forwarding Database and Static Routes

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 *Forwarding Database 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 Forwarding Database Static Addresses Page* opens.

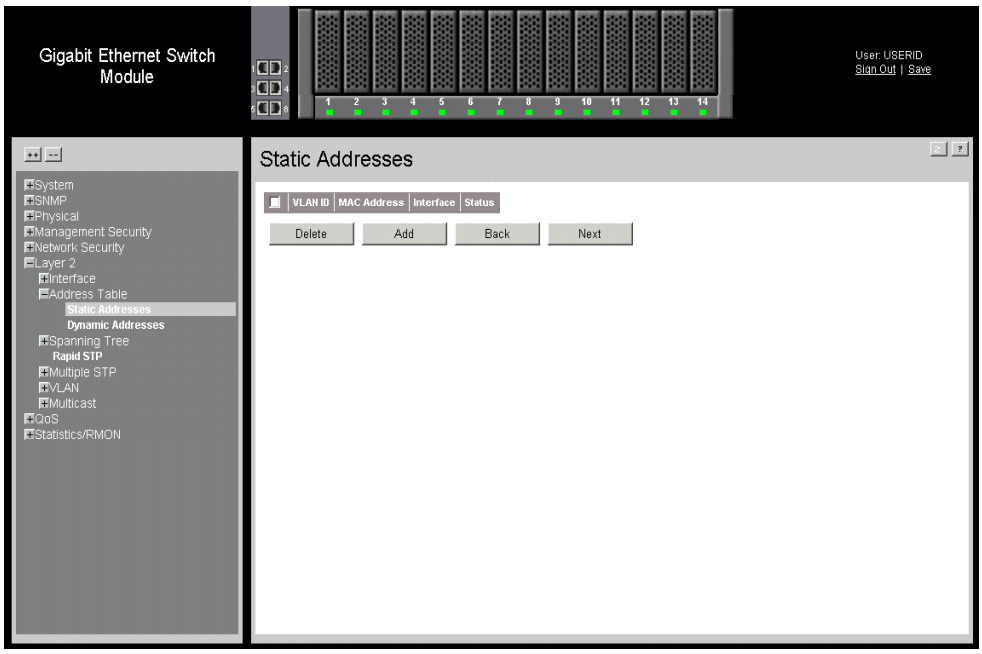



**Figure 88. Forwarding Database Static Addresses Page**

The *Forwarding Database Static Addresses Page* contains the following fields:

- **Remove** — Removes the entry. The possible field values are:
  - *Checked* — Removes 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:
  - *Secure* — The MAC Address is defined for locked ports.
  - *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.

***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.*

To add a new static forwarding database entry:

1. Click **Layer 2 > Address Table > Static Addresses**. *The Forwarding Database Static Addresses Page* opens.
2. Click Add . The Add Forwarding Database Page opens:

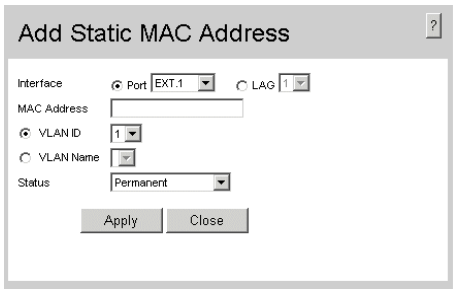



**Figure 89. Add Forwarding Database Page**

3. Define the relevant fields.
4. Click Apply . The forwarding database information is modified, and the device is updated.

# Defining Dynamic Forwarding Database Entries

The  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* opens.

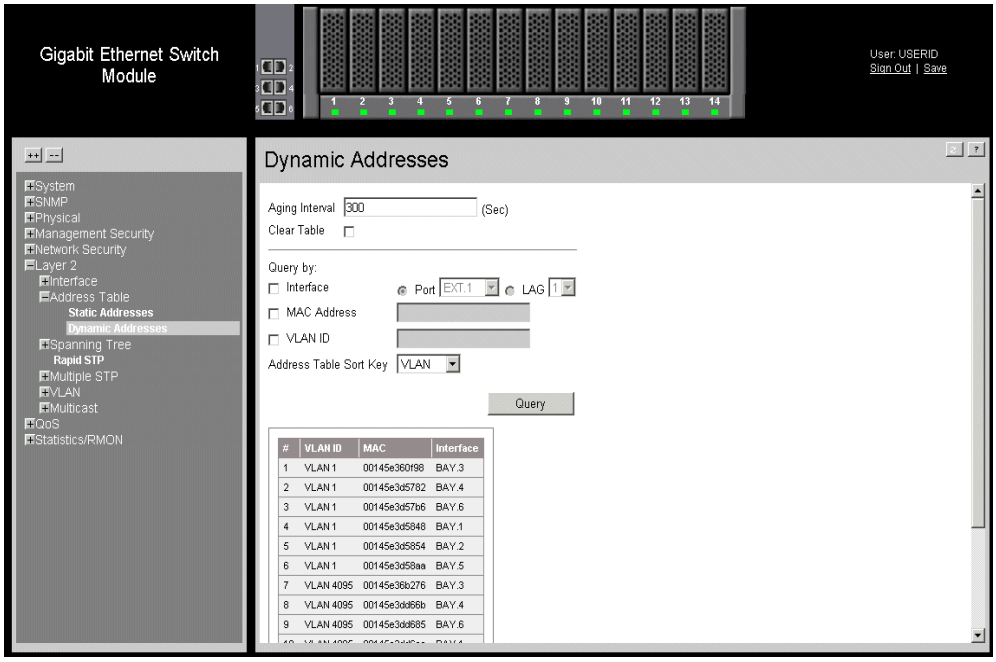



**Figure 90. Dynamic Addresses Page**

The contains the following fields:

- **Aging Interval (secs)** — 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 address, VLAN, or interface.

2. Define the fields.
3. Click Apply . 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* opens.
2. Select a *port*, *MAC Address*, and *VLAN ID*.
3. Select an *Address Table Sort Key*.
4. Click Query . The Dynamic MAC Address Table is queried, and the results are displayed.

# 12 Configuring Multicast Forwarding

This section contains information for configuring Multicast forwarding and Multicast TV, 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.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

***Note:*** *Ensure that Bridge Multicast Forwarding is enabled before enabling IGMP Snooping.*

To enable IGMP Snooping:

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

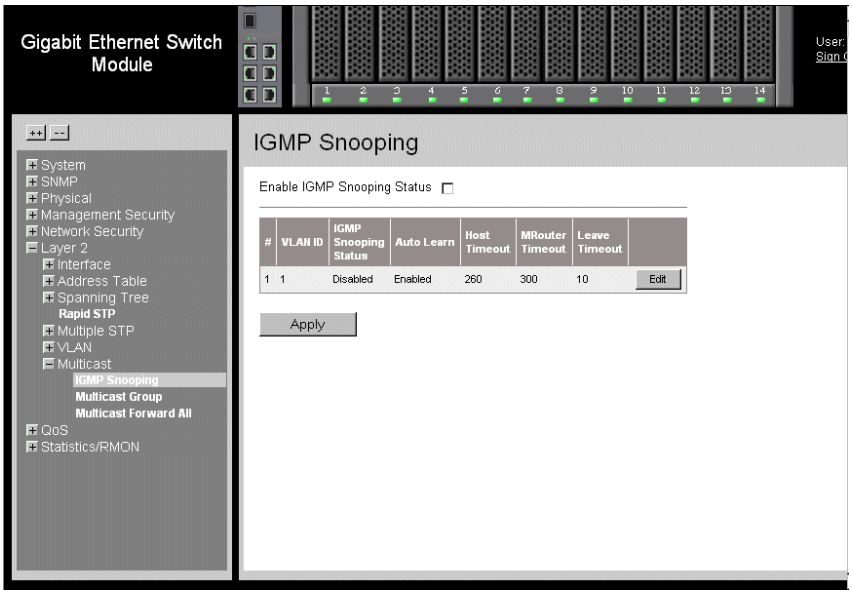



**Figure 91. IGMP Snooping Page**

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.
- **Unit No.** — Displays the unit number.
- **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 device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device.The possible field values are:
  - — *Enable* — Enables auto learn
  - — *Disable* — Disables auto learn.
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. 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. 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:

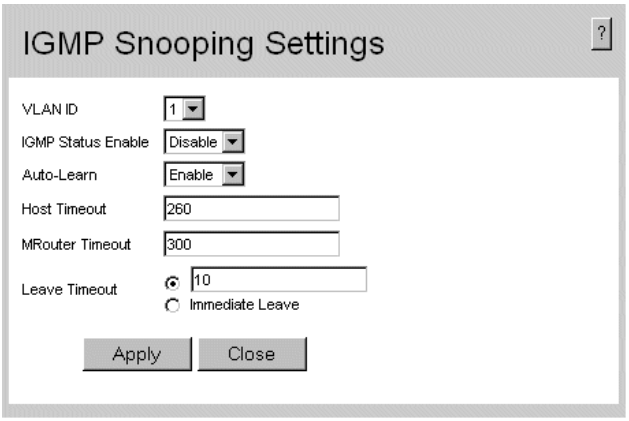



**Figure 92. IGMP Snooping Settings Page**

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 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.

To define multicast groups:

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

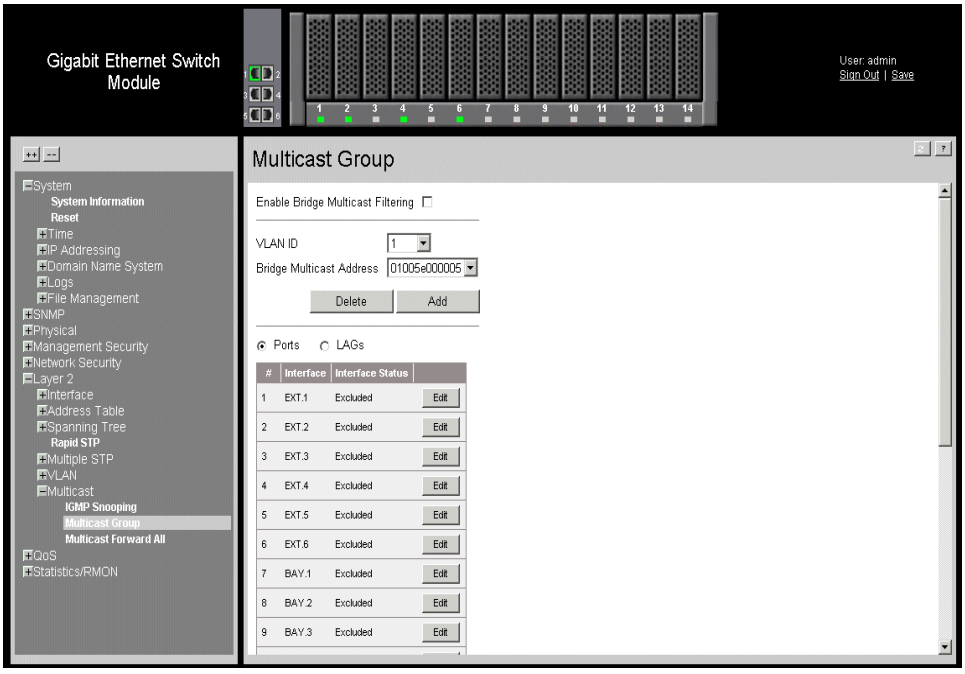



**Figure 93. Multicast Group Page**

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.
- **Unit No.** — Displays the unit number.
- **Interface** — Displays the port number.
- **Interface Status** — Indicates the port status. The possible field values are:
  - *Non* — Indicates the port is not part of a Multicast group.
  - *Static* — Attaches the port to the Multicast group as static member.

— *Forbidden* — Indicates the port is not included in the Multicast group, even if IGMP snooping designated the port to join a Multicast group.

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

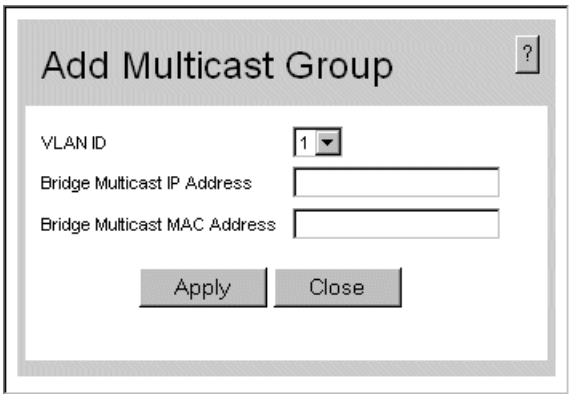



**Figure 94. Add Multicast Group Page**

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

To modify the multicast group:

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

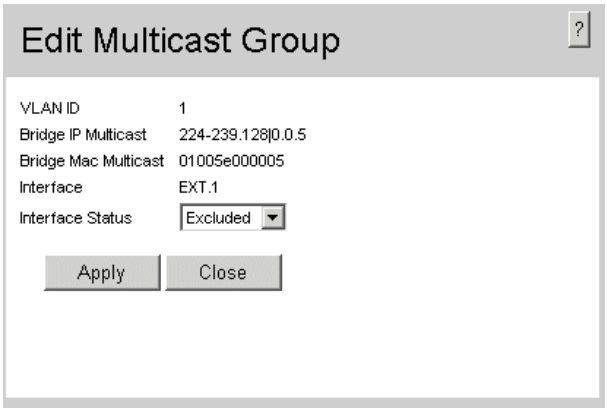



**Figure 95. Edit Multicast Group Page**

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* contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, multicast packets are forwarded to the appropriate port or VLAN. Unless LAGs are defined, only a *Multicast Forward All* table displays.

To define multicast forward all settings:

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

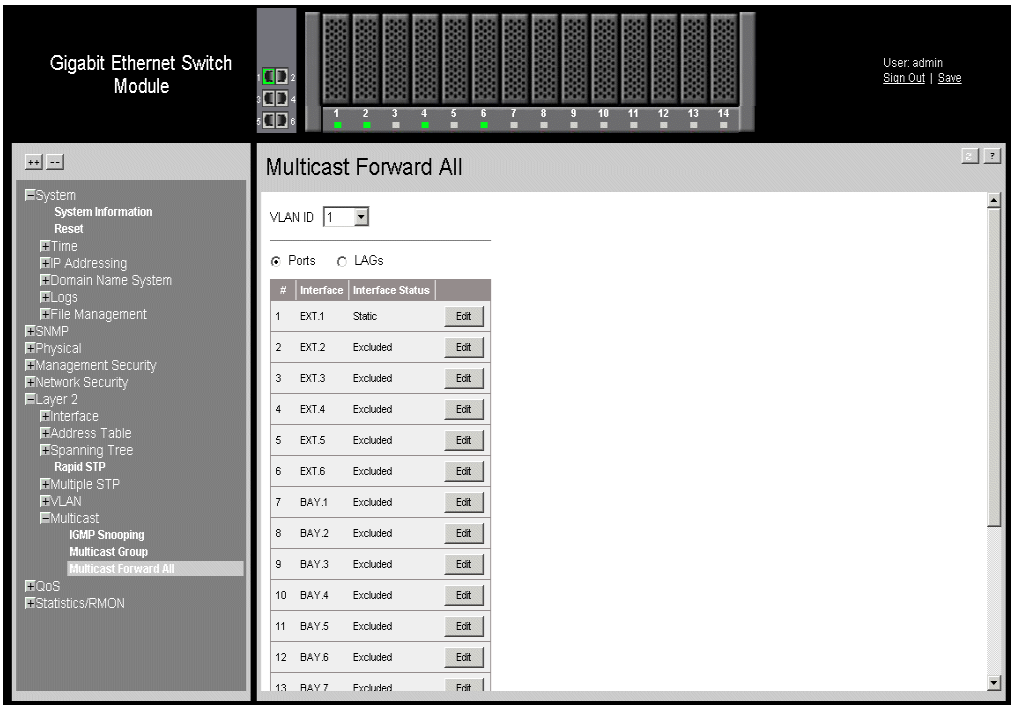



**Figure 96. Multicast Forward All Page**

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 status. The possible field values are:
  - *Static* — Attaches the port to the Multicast group as static member.
  - *Forbidden* — Indicates the port is not included in the Multicast group, even if IGMP snooping designated the port to join a Multicast group.

— *Exclude* — Indicates the port is not part of a Multicast group.

2. 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:

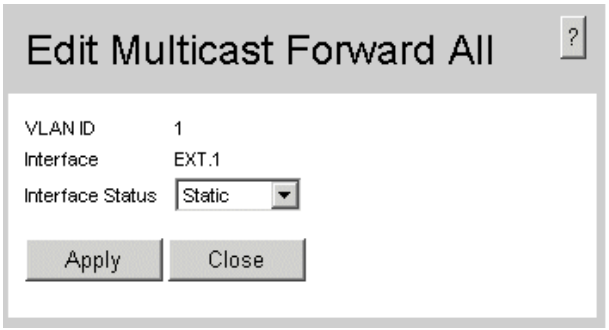



**Figure 97. Edit Multicast Forward All Page**

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

# 13 Configuring Spanning Tree

The *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. For more information on configuring Classic STP, see *Defining Classic 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*.

This section contains the following topics:

- Defining Classic Spanning Tree
- Defining Spanning Tree Interface Settings
- Defining Rapid STP
- Defining Multiple STP

# Defining Classic 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:

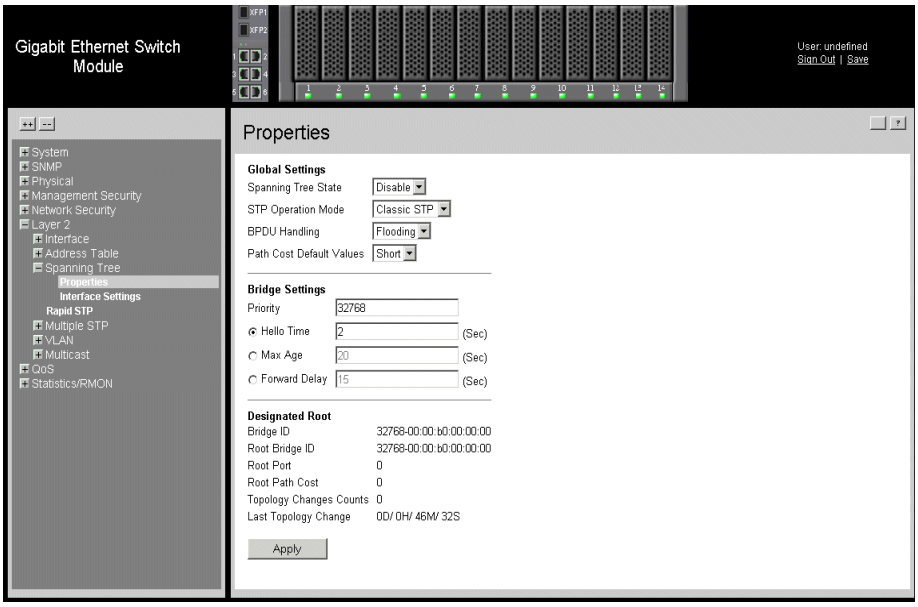



**Figure 98. Spanning Tree Properties Page**

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. This is the default value.
  - *Rapid STP* — Enables Rapid STP on the device.
  - *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 (0-65535)** — 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 default value is 32768. The port priority value is provided in increments of 4096.
- **Hello Time (1-10)** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root Bridge waits between configuration messages. The default is 2 seconds.
- **Max Age (6-40)** — 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 default Maximum Age Time is 20 seconds.
- **Forward Delay (4-30)** — 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 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** — 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.

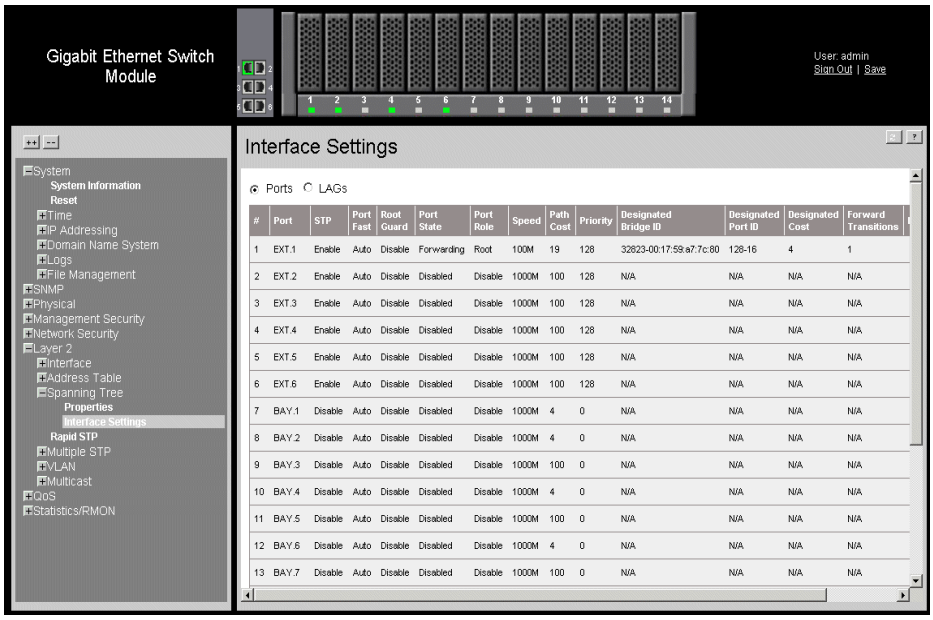
2. Define the relevant fields.
3. Click Apply. STP is enabled, and the device is updated.

# 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:




| # | Port | STP | Port Fast | Root Guard | Port State | Port Role | Speed | Path Cost | Priority | Designated Bridge ID | Designated Port ID | Designated Cost | Forward Transitions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | EXT.1 | Enable | Auto | Disable | Forwarding | Root | 100M | 19 | 128 | 32823-00:17:59:a7:7c:80 | 128-16 | 4 | 1 |
| 2 | EXT.2 | Enable | Auto | Disable | Disabled | Disable | 1000M | 100 | 128 | N/A | N/A | N/A | N/A |
| 3 | EXT.3 | Enable | Auto | Disable | Disabled | Disable | 1000M | 100 | 128 | N/A | N/A | N/A | N/A |
| 4 | EXT.4 | Enable | Auto | Disable | Disabled | Disable | 1000M | 100 | 128 | N/A | N/A | N/A | N/A |
| 5 | EXT.5 | Enable | Auto | Disable | Disabled | Disable | 1000M | 100 | 128 | N/A | N/A | N/A | N/A |
| 6 | EXT.6 | Enable | Auto | Disable | Disabled | Disable | 1000M | 100 | 128 | N/A | N/A | N/A | N/A |
| 7 | BAY.1 | Disable | Auto | Disable | Disabled | Disable | 1000M | 4 | 0 | N/A | N/A | N/A | N/A |
| 8 | BAY.2 | Disable | Auto | Disable | Disabled | Disable | 1000M | 4 | 0 | N/A | N/A | N/A | N/A |
| 9 | BAY.3 | Disable | Auto | Disable | Disabled | Disable | 1000M | 100 | 0 | N/A | N/A | N/A | N/A |
| 10 | BAY.4 | Disable | Auto | Disable | Disabled | Disable | 1000M | 4 | 0 | N/A | N/A | N/A | N/A |
| 11 | BAY.5 | Disable | Auto | Disable | Disabled | Disable | 1000M | 100 | 0 | N/A | N/A | N/A | N/A |
| 12 | BAY.6 | Disable | Auto | Disable | Disabled | Disable | 1000M | 4 | 0 | N/A | N/A | N/A | N/A |
| 13 | BAY.7 | Disable | Auto | Disable | Disabled | Disable | 1000M | 100 | 0 | N/A | N/A | N/A | N/A |

**Figure 99. 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* is selected, the following fields are displayed:

- **Unit No.** — Displays the unit number.
- **Port** — Displays the port on which STP is enabled.
- **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:

  - *Enable* — Port Fast is enabled.
  - *Disable* — Port Fast is disabled.
  - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.

- **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.
- **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 *Blocking* state to *Forwarding* state.
- **LAG** — Indicates the LAG to which the port belongs.

If *LAGs* is 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:
  - *Enable* — Port Fast is enabled.
  - *Disable* — Port Fast is disabled.
  - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
- **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.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
- **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 *Blocking* state to *Forwarding* state.

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

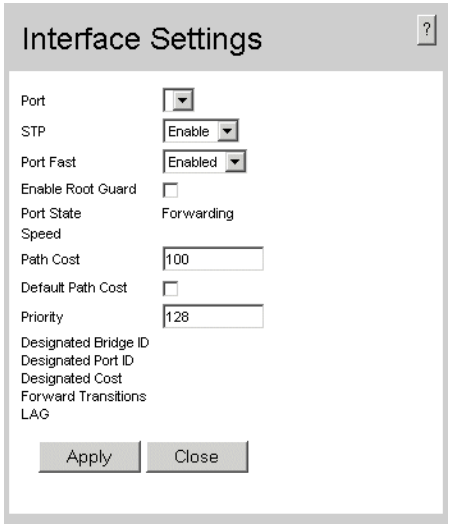



**Figure 100. Spanning Tree Interface Settings Page**

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 represent the LAG RSTP information.

To define Rapid STP on the device:

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

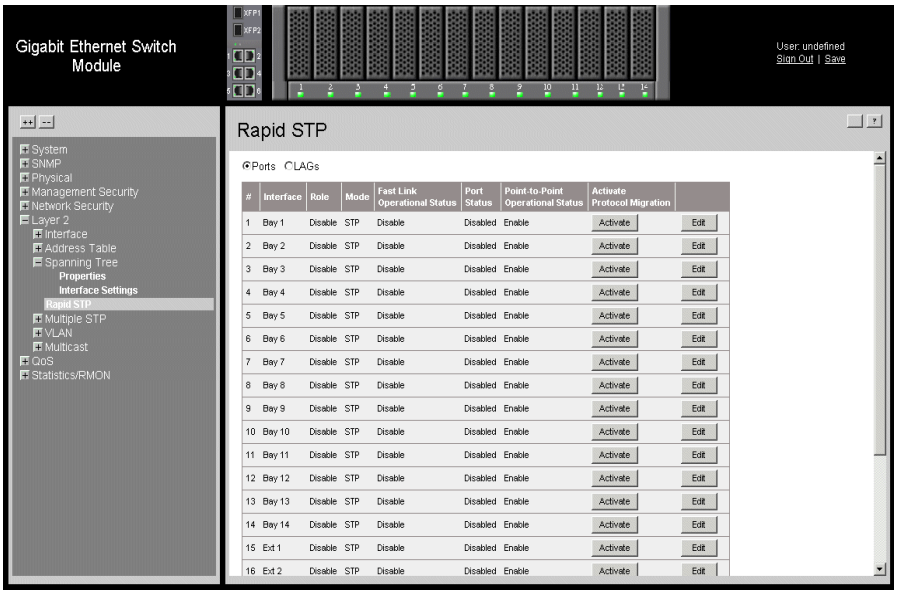



**Figure 101. Rapid STP Page**

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.
- **Unit No**. — Indicates the unit number.
- **Interface** — Displays the port or LAG on which Rapid STP is enabled.
- **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 status of a the port.
- **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:

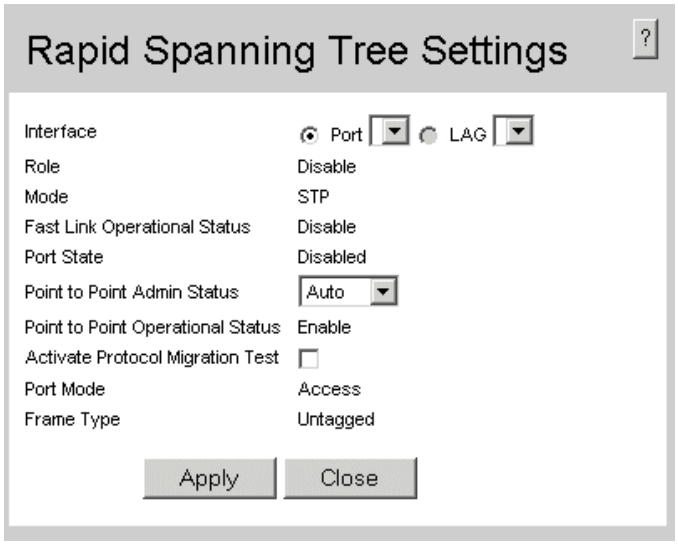



**Figure 102. Rapid Spanning Tree Settings Page**

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:

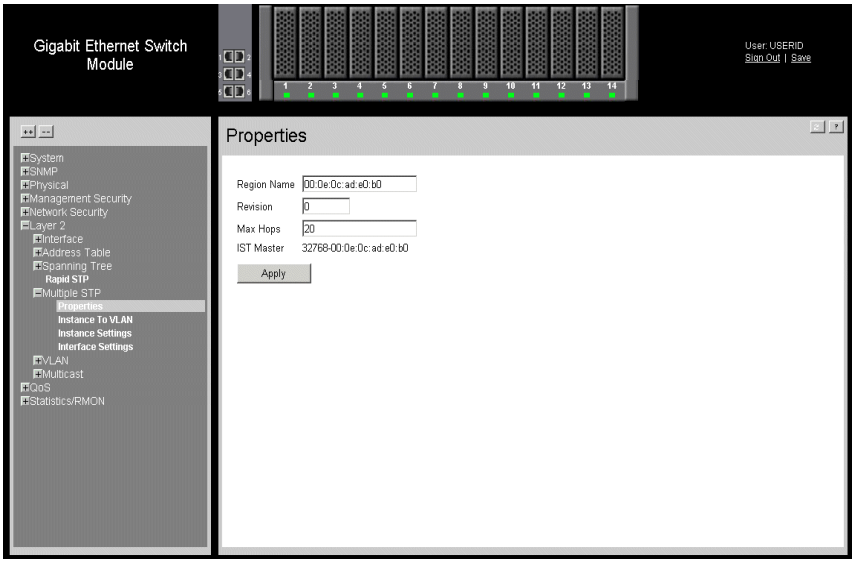



**Figure 103. Multiple STP Properties Page**

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.

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. When configuring VLANs to MSTP instances, note the following:

- VLAN 1 mapped to MSTP instance 1 by default.
- VLAN 2 mapped to MSTP instance 2 by default.

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:

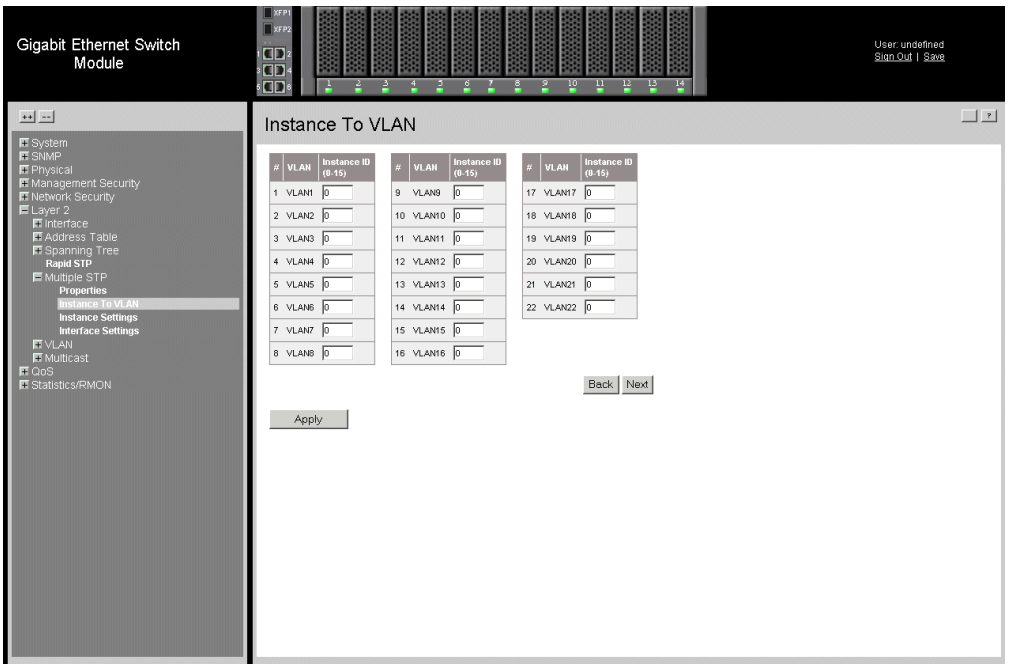



**Figure 104. Instance To VLAN Settings Page**

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

- **Unit No.** — Displays the unit number.
- **VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Instance ID (0-15)** — 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:

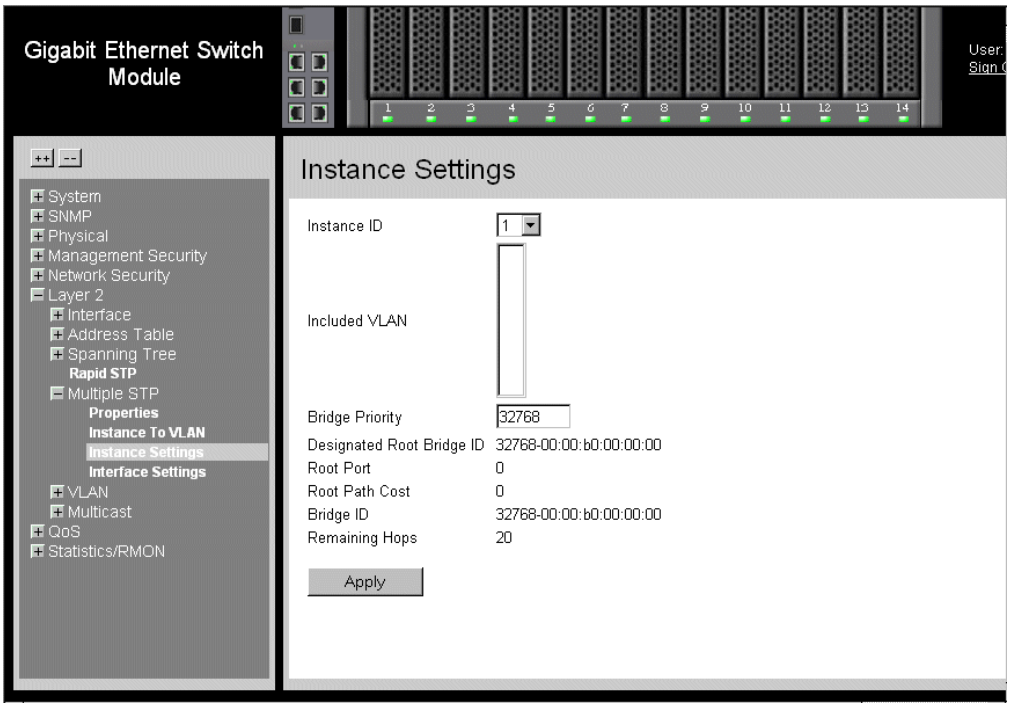



**Figure 105. Instance Settings Page**

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

- **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 Apply . 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:

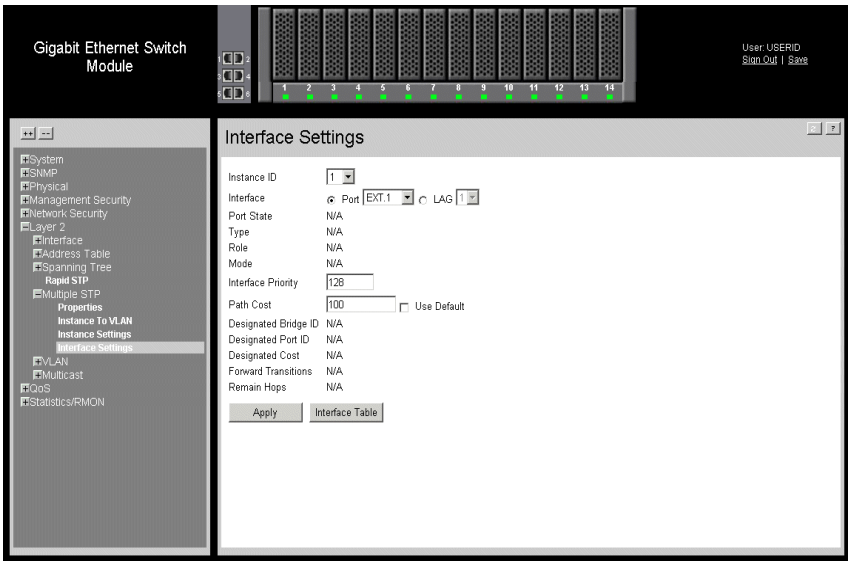



**Figure 106. Interface Settings Page**

The *Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-15.
- **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.

- **MSTP** — Specifies whether or not MSTP is enable on the interface. The possible field values are:
  - *Enabled* — Enables MSTP on the interface.
  - *Disabled* — Disables MSTP on the interface.
- **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 or Master 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.
- **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. This is the default value.
  - *Rapid STP* — Rapid STP is enabled on the device.
  - *Multiple STP* — Multiple STP is enabled on the device.
- **Interface Priority** — Defines the interface priority for the specified instance. The default value is 128.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **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 LAG State has changed from a *Forwarding* state to a *Blocking* state.
- **Remain Hops** — Indicates the hops remaining to the next destination.

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

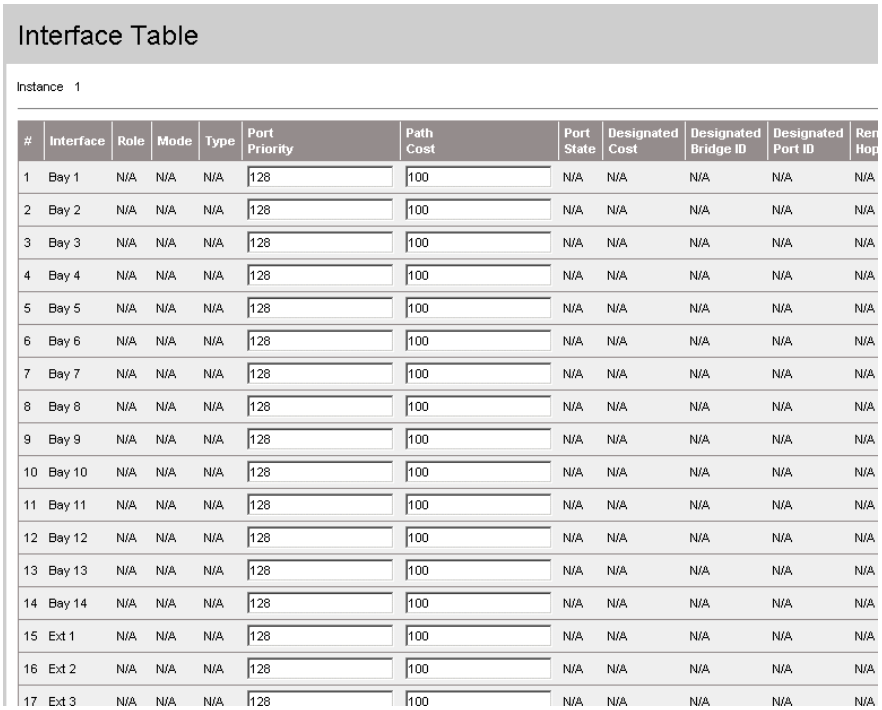



**Figure 107. Interface Table Page**

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

# 14 Configuring SNMP

*Simple Network Management Protocol* (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP v1 and v2c
- SNMP v3

## SNMP v1 and v2c

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

## SNMP v3

SNMP v3 applies access control and a new traps mechanism. In addition, User Security Model (USM) parameters are defined for SNMPv3, including:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against the disclosure of message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on a SNMP message, or both authentication and privacy are enabled on a SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OIDs). OIDs are used by the system to manage device features.

SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The device generates the Copy trap.

This section contains the following topics:

- Configuring SNMP Notifications
- Configuring SNMP Security

# Configuring SNMP Security

This section contains information for configuring SNMP security parameters, and contains the following topics:

- Defining SNMP Security
- Defining SNMP Views
- Defining SNMP Group Profiles
- Defining SNMP Group Members
- Defining SNMP Communities

## Defining SNMP Security

The *SNMP Security Global Parameters Page* permits the enabling of both SNMP and Authentication notifications.

To define the SNMP security parameters:

1. Click **SNMP > Security > Global Parameters**. The *SNMP Security Global Parameters Page* opens:

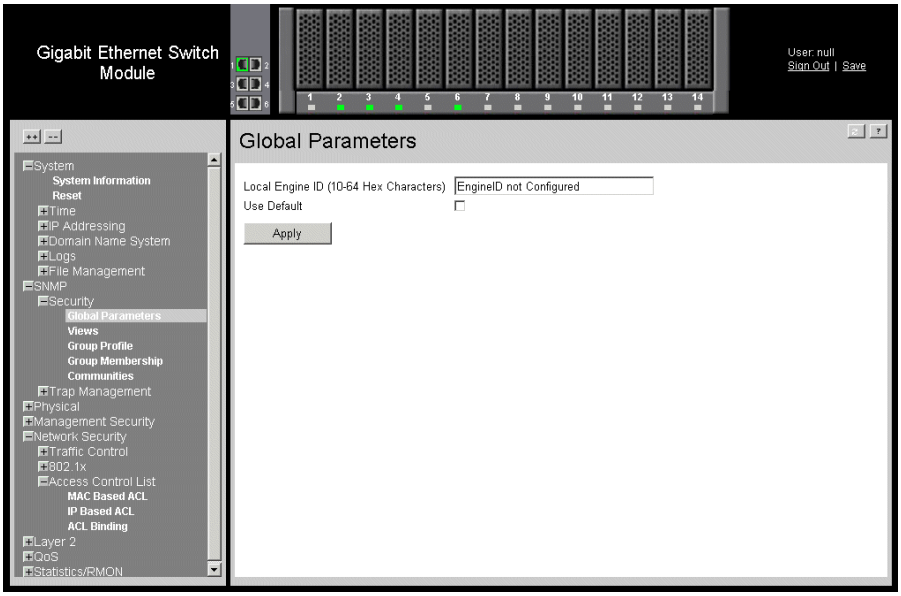



**Figure 108. SNMP Security Global Parameters Page**

The *SNMP Security Global Parameters Page* contains the following fields:

- **Local Engine ID (10-64 Characters)**— Displays the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of an Enterprise number and the default MAC address.
- **Use Default** — Uses the device-generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
  - — *First 4 octets* — first bit = 1, the rest is IANA Enterprise number.
  - — *Fifth octet* — Set to 3 to indicate the MAC address that follows.
  - — *Last 6 octets* — MAC address of the device.

2. Define the relevant fields.
3. Click Apply . The *SNMP Global Security Parameters* are set, and the device is updated.

# Defining SNMP Views

SNMP insert space views provide or block access to device features or portions of features. For example, a view can be defined, which provides that SNMP group A has *Read Only* (R/O) access to Multicast groups, while SNMP group B has *Read-Write* (R/W) access to Multicast groups. Feature access is granted via the MIB name or MIB Object ID.

To define SNMP views:

1. Click **SNMP > Security > Views**. The *SNMP Security Views Page* opens:

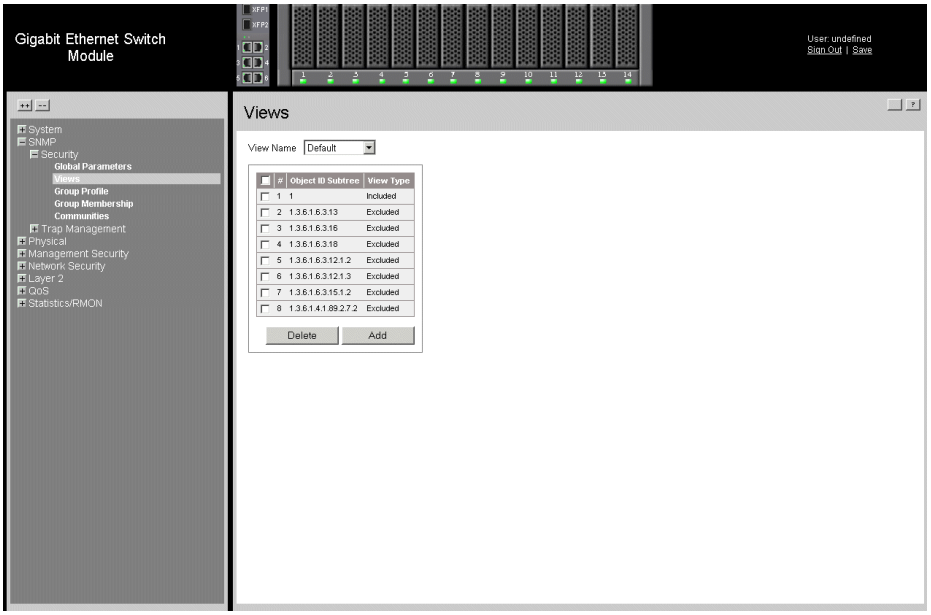



**Figure 109. SNMP Security Views Page**

The *SNMP Security Views Page* contains the following fields:

- **View Name** — Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.The possible field values are:
  - — *Default* — Enables read-only access for the default view.
  - — *Default Super* — Enables Super read-only, read-write, and management access to the default SNMP view.
- **Remove** — Deletes the currently selected view. The possible field values are:
  - — *Checked* — Removes the selected view.
  - — *Unchecked* — Maintains the list of views.
- **Unit No.** — Displays the unit number.
- **Object ID Subtree** — Displays the device feature OID included in or excluded from the selected SNMP view.

- **View Type** — Indicates whether the defined OID branch is included in or excluded from the selected SNMP view.

2. Click Add . The *Add SNMP View Page* opens:

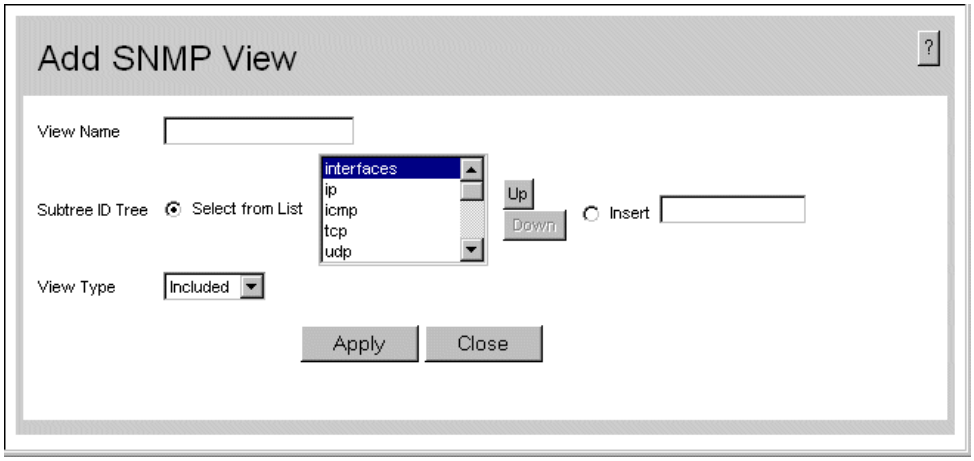



**Figure 110. Add SNMP View Page**

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

# Defining SNMP Group Profiles

The *SNMP Group Profile Page* provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or feature aspects.

To define an SNMP group:

1. Click **SNMP > Security > Group Profile**. The *SNMP Group Profile Page* opens:

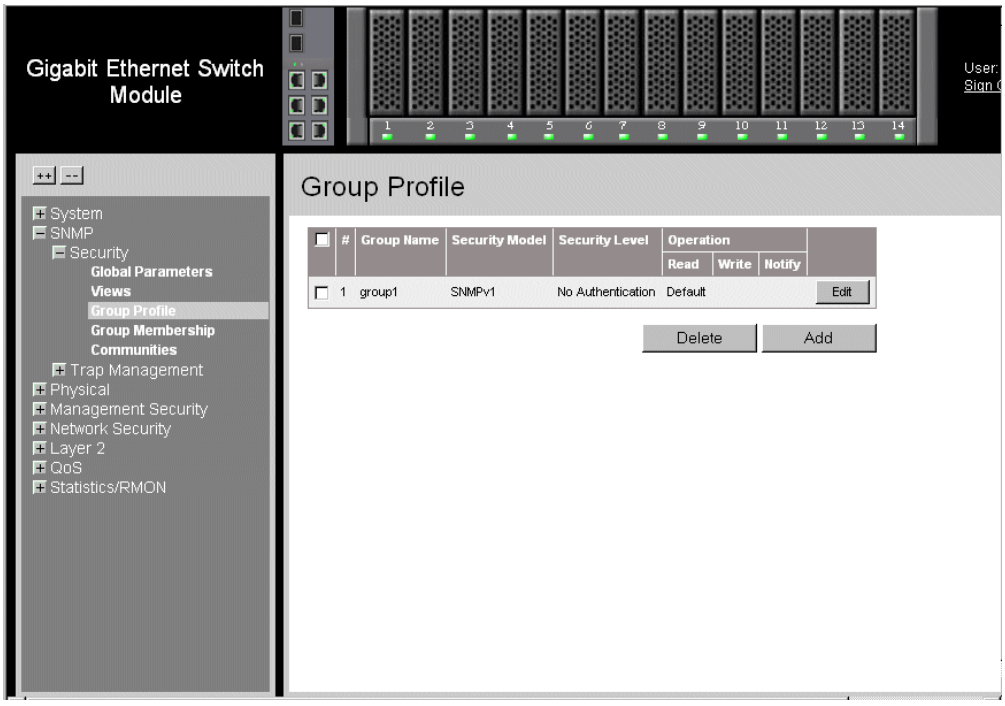



**Figure 111. SNMP Group Profile Page**

The *SNMP Group Profile Page* contains the following fields:

- **Remove** — Removes SNMP groups. The possible field values are:
  - *Checked* — Removes the selected SNMP group.
  - *Unchecked* — Maintains the SNMP groups.
- **Unit No.** — Displays the unit number.
- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2c* — SNMPv2c is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
  - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.

— *Authentication* — Authenticates SNMP messages, and ensures that the SNMP message's origin is authenticated.

— *Privacy* — Encrypts SNMP messages.

- **Operation** — Defines the group access rights. The possible field values are:

— *Read* — Management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.

— *Write* — Management access is read-write and changes can be made to the assigned SNMP view.

— *Notify* — Sends traps for the assigned SNMP view.

2. Click Add . The *Add SNMP Group Profile Page* opens:

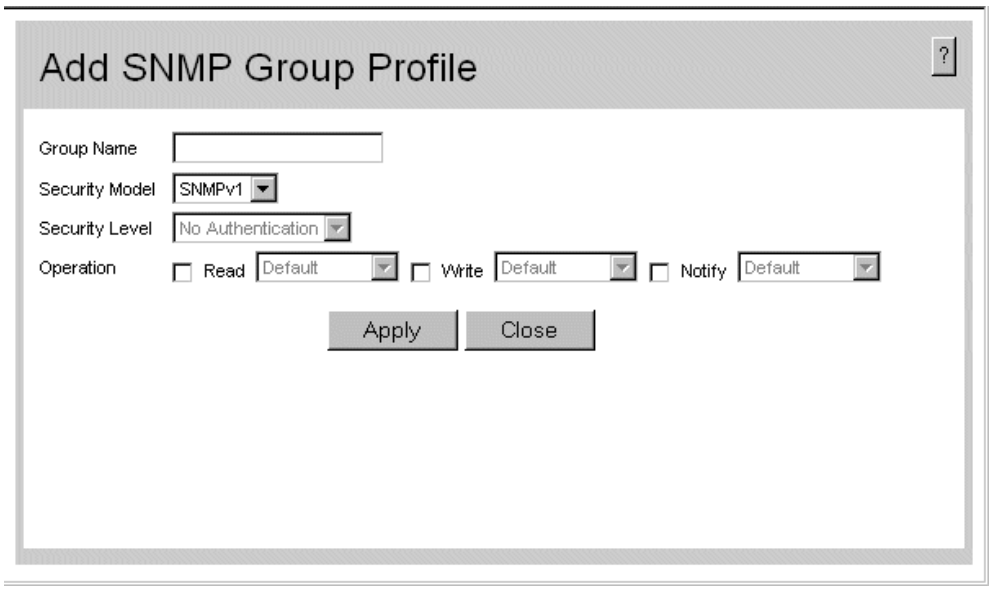



**Figure 112. Add SNMP Group Profile Page**

3. Define the relevant fields.
4. Click Apply . The *SNMP Group Profile* is added, and the device is updated.

To modify SNMP Group Settings:

1. Click **SNMP > Security > Group Profile**. The *SNMP Group Profile Page* opens.
2. Click Edit . The *SNMP Group Profile Settings Page* opens:

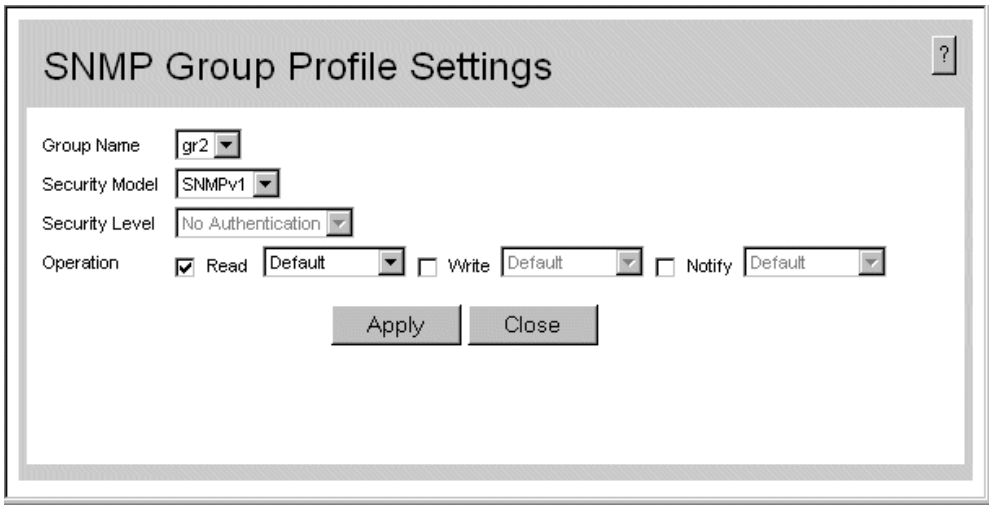



**Figure 113. SNMP Group Profile Settings Page**

3. Modify the relevant fields.
4. Click Apply . The *SNMP Group Profile* is modified, and the device is updated.

# Defining SNMP Group Members

The *SNMP Group Membership Page* enables assigning system users to SNMP groups and defines the user authentication method.

1. Click **SNMP > Security > Group Membership**. The *SNMP Group Membership Page* opens:

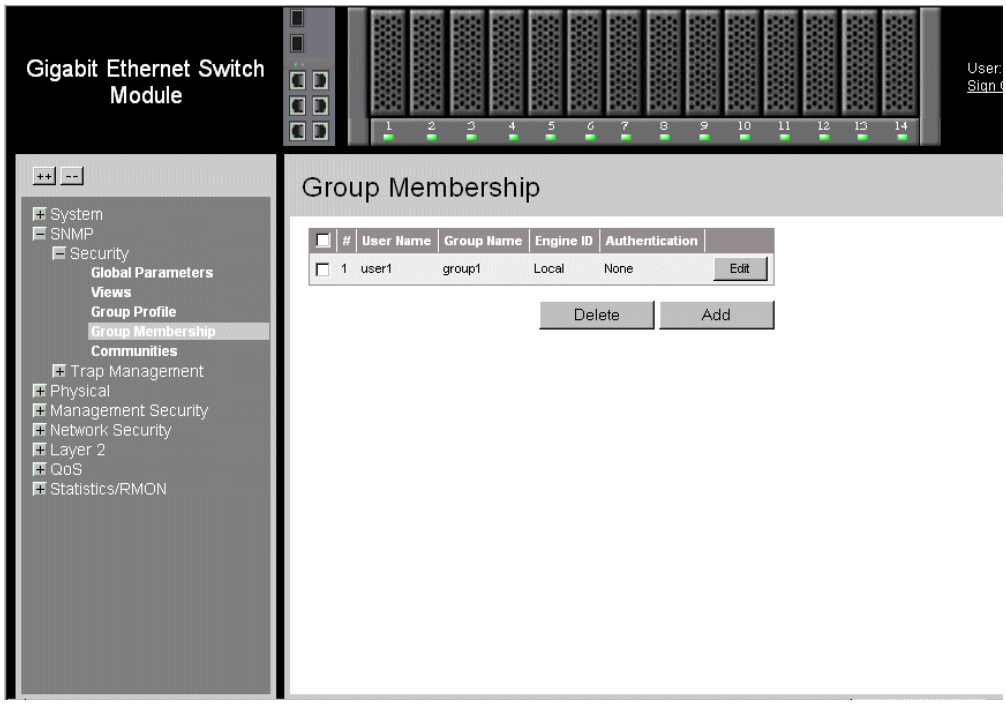



**Figure 114. SNMP Group Membership Page**

The *SNMP Group Membership Page* contains the following fields:

- **Remove** — Removes users from a specified group. The possible field values are:
  - *Checked* — Removes the selected user.
  - *Unchecked* — Maintains the list of users.
- **Unit No.** — Displays the unit number.
- **User Name** — Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Engine ID** — Displays either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 user database. The possible field values are:
- **Authentication** — Displays the method used to authenticate users. The possible field values are:
  - *None* — No user authentication is used.
  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.

— *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.

— *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.

2. Click Add . The *Add SNMP Group Membership Page* opens:

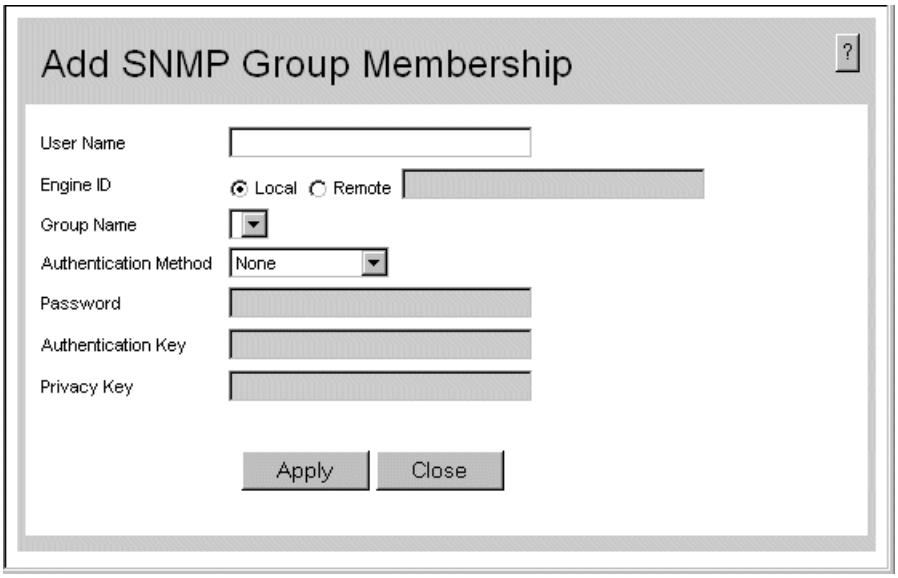



**Figure 115. Add SNMP Group Membership Page**

In addition to the fields in the *SNMP Group Membership Page*, the *Add SNMP Group Membership Page* contains the following fields:

- **Authentication Method** — Defines the SNMP Authentication Method.
- **Password** — Defines the password for the group member
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.
- **Privacy Key** — Defines the privacy key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

3. Define the relevant fields.
4. Click Apply . The *SNMP Group Membership* is modified, and the device is updated.

To modify SNMP Group Membership Settings:

1. Click **SNMP > Security > Group Membership**. The *SNMP Group Membership Page* opens.
2. Click Edit . The *SNMP Group Membership Settings Page* opens:

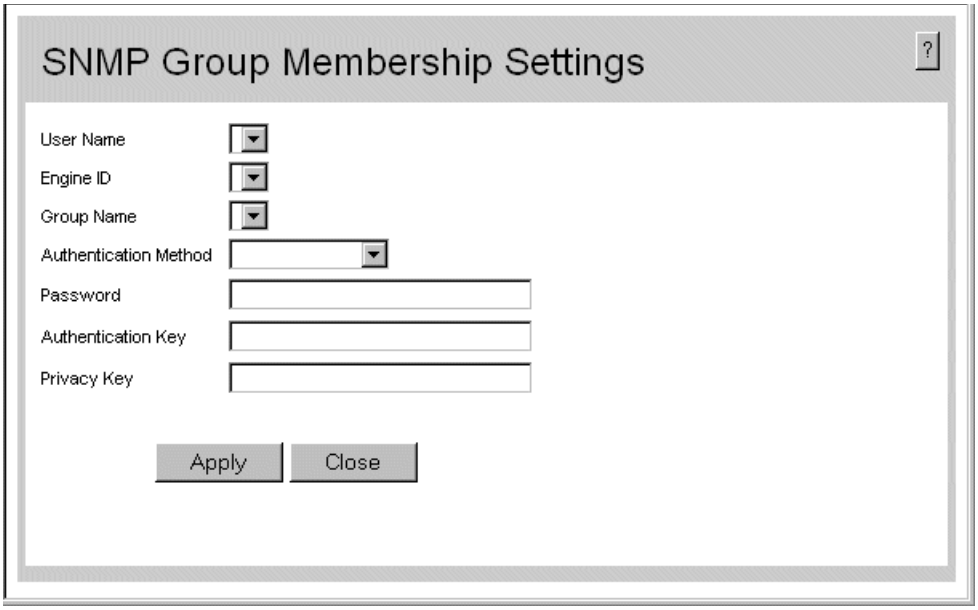



**Figure 116. SNMP Group Membership Settings Page**

3. Modify the relevant fields.
4. Click Apply . The *SNMP Group Membership* is modified, and the device is updated.

# Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

To define SNMP communities:

1. Click **SNMP > Security > Communities**. The *SNMP Communities Page* opens:


**Figure 117. SNMP Communities Page**

The *SNMP Communities Page* is divided into the following tables:

- SNMP Communities Basic Table
- SNMP Communities Advanced Tables

## SNMP Communities Basic Table

The *SNMP Communities Basic Table* contains the following fields:

- **Remove** — Removes a community. The possible field values are:
  - *Checked* — Removes the selected SNMP community.
  - *Unchecked* — Maintains the SNMP communities.
- **Unit No.** — Displays the unit number.
- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Access Mode** — Defines the access rights of the community. The possible field values are:

- — *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
- — *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
- — *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.

- **View Name** — Contains a list of user-defined SNMP views

## SNMP Communities Advanced Tables

The *SNMP Communities Advanced Table* contains the following fields:

- **Remove** — Removes a community. The possible field values are:
  - — *Checked* — Removes the selected SNMP communities.
  - — *Unchecked* — Maintains the SNMP communities.
- **Unit No.** — Displays the unit number.
- **Management Station** — Displays the management station IP address for which the advanced SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Group Name** — Defines advanced SNMP community group names.

1. Click Add . The *Add SNMP Community Page* opens:

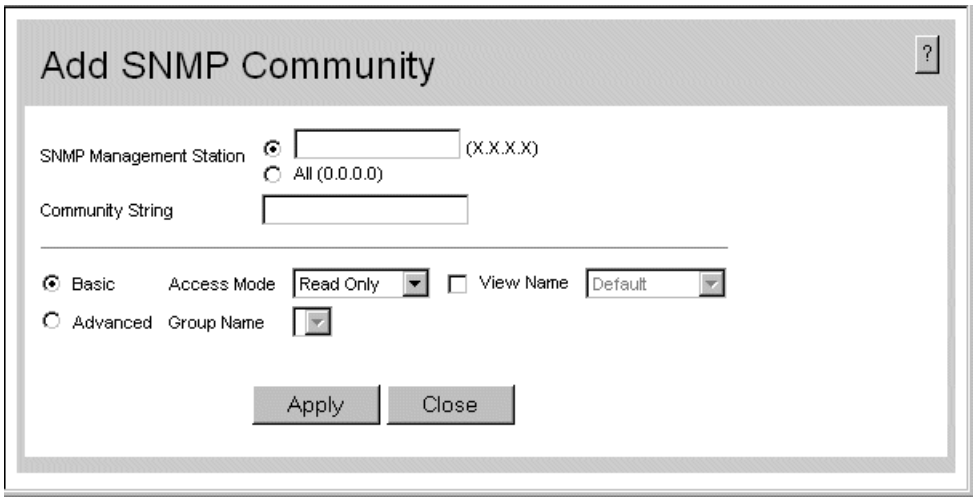



**Figure 118. Add SNMP Community Page**

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

To modify SNMP Group Membership Settings:

1. Click **SNMP > Security > Communities**. The *SNMP Communities Page* opens.
2. Click Edit . The *SNMP Community Settings Page* opens:

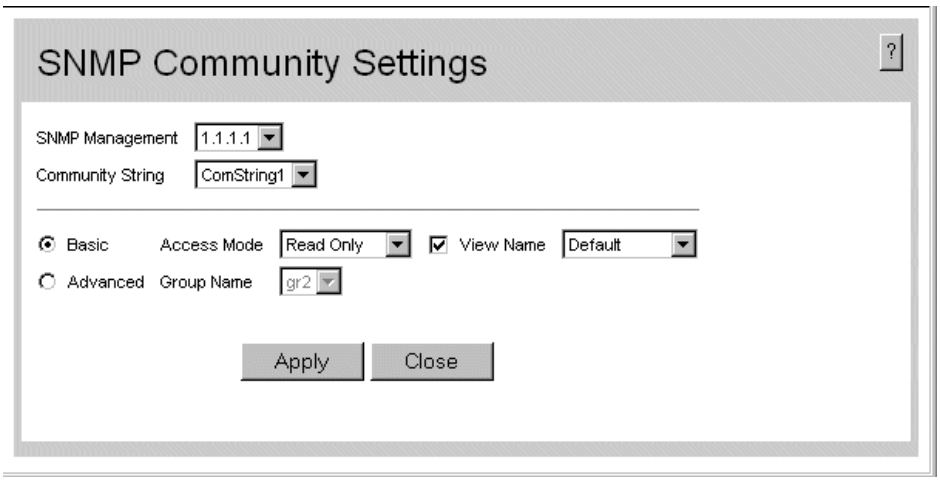



**Figure 119. SNMP Community Settings Page**

3. Modify the relevant fields.
4. Click Apply . The *SNMP Community* is modified, and the device is updated.

# Configuring SNMP Notifications

This section contains information for configuring SNMP Notifications, and contains the following topics:

- Defining SNMP Notification Global Parameters
- Defining SNMP Notification Recipients
- Defining SNMP Notification Recipients

# Defining SNMP Notification Global Parameters

The *SNMP Trap Management Properties Page* contains parameters for defining SNMP notification parameters.

To define SNMP notification global parameters:

1. Click **SNMP > Trap Management > Properties**. The *SNMP Trap Management Properties Page* opens:

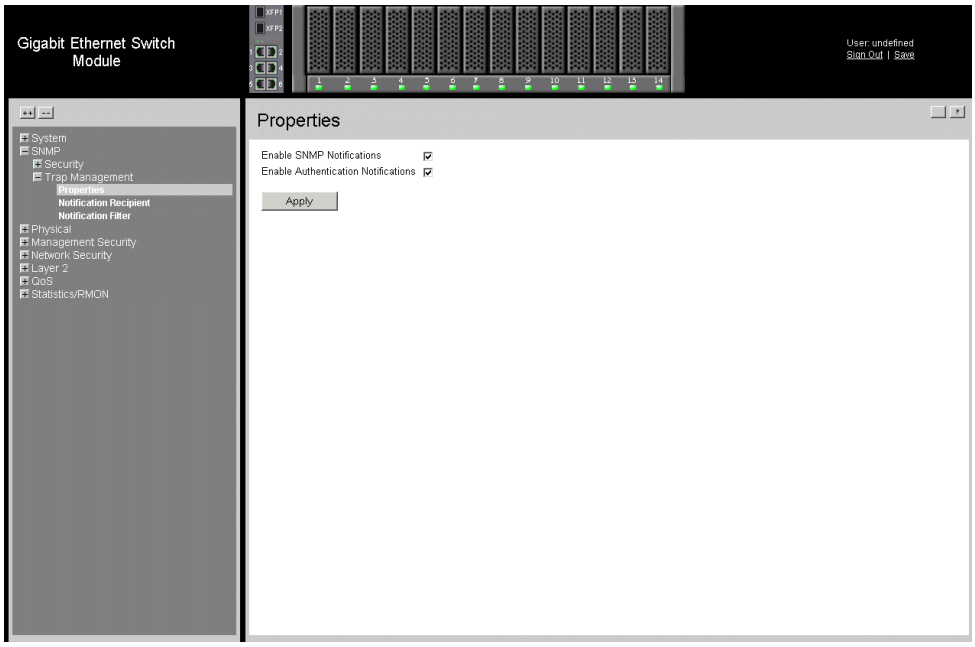



**Figure 120. SNMP Trap Management Properties Page**

The *SNMP Trap Management Properties Page* contains the following fields:

- **Enable SNMP Notifications** — Specifies whether the device can send SNMP notifications. The possible field values are:
  - — *Enable* — Enables SNMP notifications.
  - — *Disable* — Disables SNMP notifications.
- **Enable Authentication Notifications** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
  - — *Enable* — Enables the device to send authentication failure notifications.
  - — *Disable* — Disables the device from sending authentication failure notifications.

2. Define the relevant fields.
3. Click Apply. The *SNMP Trap Management* properties are defined, and the device is updated.

# Defining SNMP Notification Recipients

The *SNMP Trap Management Notification Recipient Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To define SNMP notification filters:

1. Click **SNMP > Trap Management > Notification Recipient**. The *SNMP Trap Management Notification Recipient Page* opens:

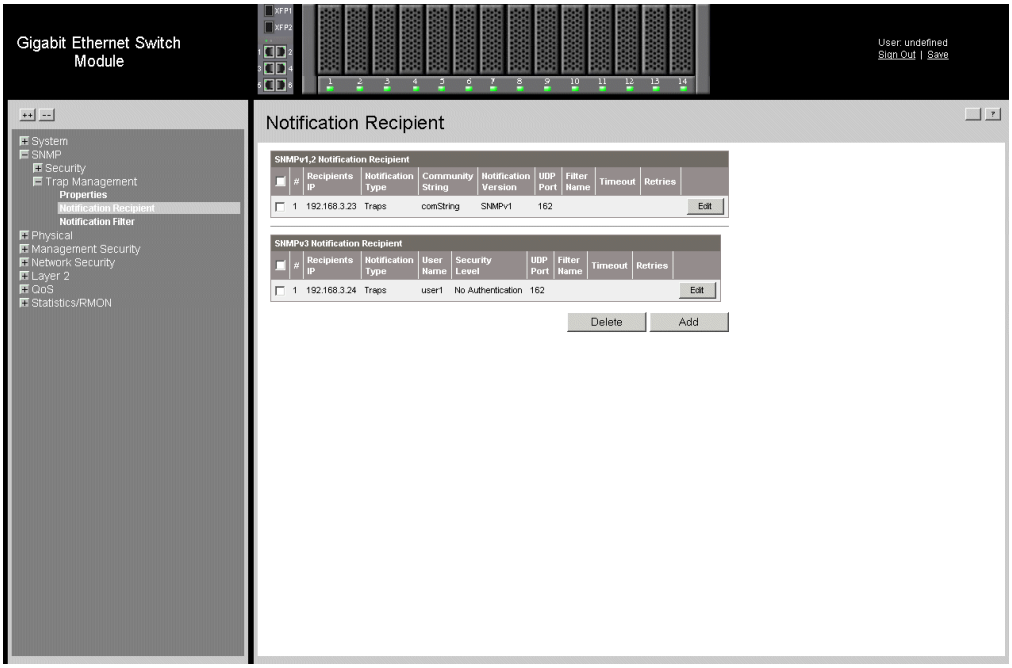



**Figure 121. SNMP Trap Management Notification Recipient Page**

The *SNMP Trap Management Notification Recipient Page* is divided into the following tables:

- SNMPv1,2c Notification Recipient
- SNMPv3 Notification Recipient

## SNMPv1,2c Notification Recipient

The *SNMP v1, v2c Recipient* table contains the following fields:

- **Remove** — Deletes the currently selected recipient. The possible field values are:
  - *Checked* — Removes the selected recipient from the list of recipients.
  - *Unchecked* — Maintains the list of recipients.
- **Recipients IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.
- **Community String** — Displays the community string of the trap manager.
- **Notification Version** — Displays the trap type. The possible field values are:
  - *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
  - *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

## SNMPv3 Notification Recipient

The *SNMPv3 Notification Recipient* table contains the following fields:

- **Remove** — Deletes the currently selected recipient. The possible field values are:
  - *Checked* — Removes the selected recipient from the list of recipients.
  - *Unchecked* — Maintains the list of recipients.
- **Recipients IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  - *Trap* — Indicates that traps are sent.
  - *Inform* — Indicates that informs are sent.
- **User Name** — Displays the user to which SNMP notifications are sent.
- **Security Level** — Displays the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates that the packet is neither authenticated nor encrypted.

— *Authentication* — Indicates that the packet is authenticated.

- **UDP Port** — The UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Includes or excludes SNMP filters.
- **Timeout** — The amount of time (seconds) the device waits before resending informs. The field range is 1-300. The default is 10 seconds.
- **Retries** — The amount of times the device resends an inform request. The field range is 1-255. The default is 3.

2. Click Add . The *Add SNMP Notification Recipient Page* opens:

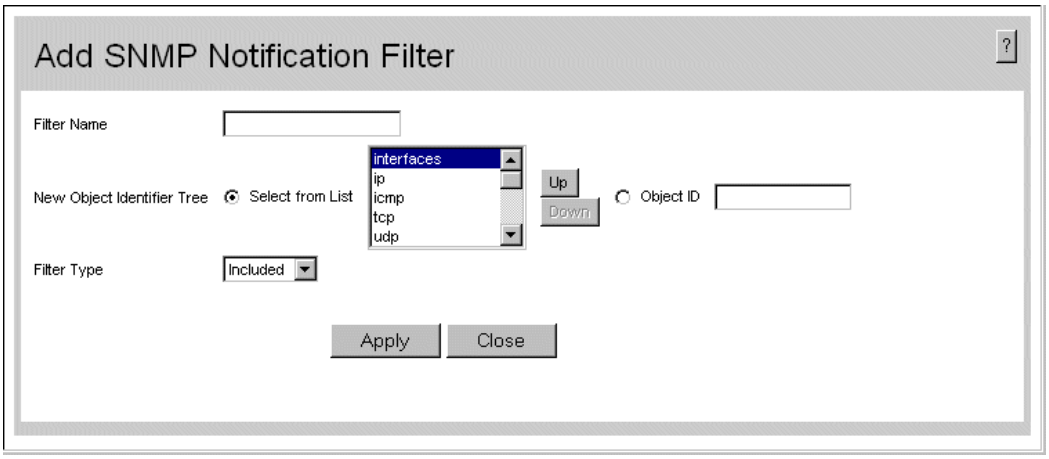



**Figure 122. Add SNMP Notification Recipient Page**

3. Define the relevant fields.
4. Click Apply . The *SNMP Notification Recipient* is defined, and the device is updated.

# Defining SNMP Notification Filters

The*SNMP Trap Management Notification Filter Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a portion of a feature. The *SNMP Trap Management Notification Filter Page* also allows network managers to filter notifications.

To define SNMP notification filters:

1. Click **SNMP > Trap Management > Notification Filter**. The *SNMP Trap Management Notification Filter Page* opens:

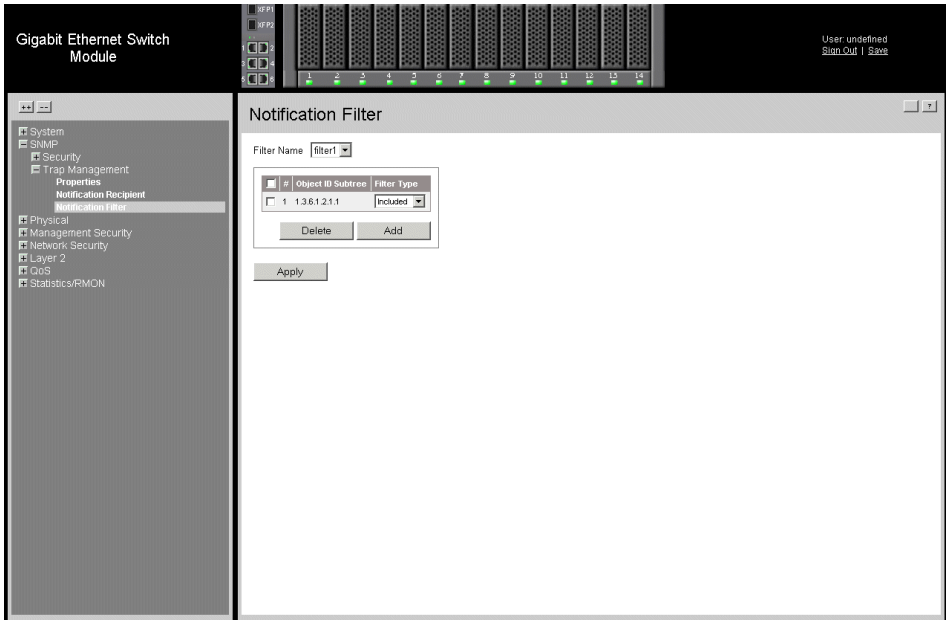



**Figure 123. SNMP Trap Management Notification Filter Page**

The *SNMP Trap Management Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Remove** — Deletes filters.
  - Checked — Deletes the selected filter.
  - Unchecked — Maintains the list of filters.
- **Object Identifier Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. OIDs are selected from either the *Select from* field or the *Object ID* field.
- **Filter Type** — Indicates whether to send traps or informs relating to the selected OID.
  - *Included* — Sends traps or informs.
  - *Excluded* — Does not send traps or informs.

2. Click Add . The *Add SNMP Notification Filter Page* opens:

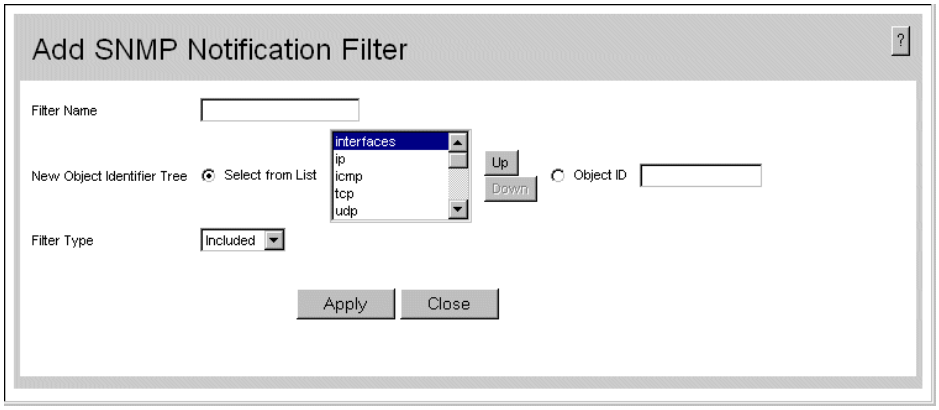



**Figure 124. Add SNMP Notification Filter Page**

3. Define the relevant fields.
4. Click Apply . The *SNMP Notification Filter* is defined, and the device is updated.

# 15 Configuring Quality of Service (QoS)

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. All queues can participate in WRR, expect SP queues. 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:

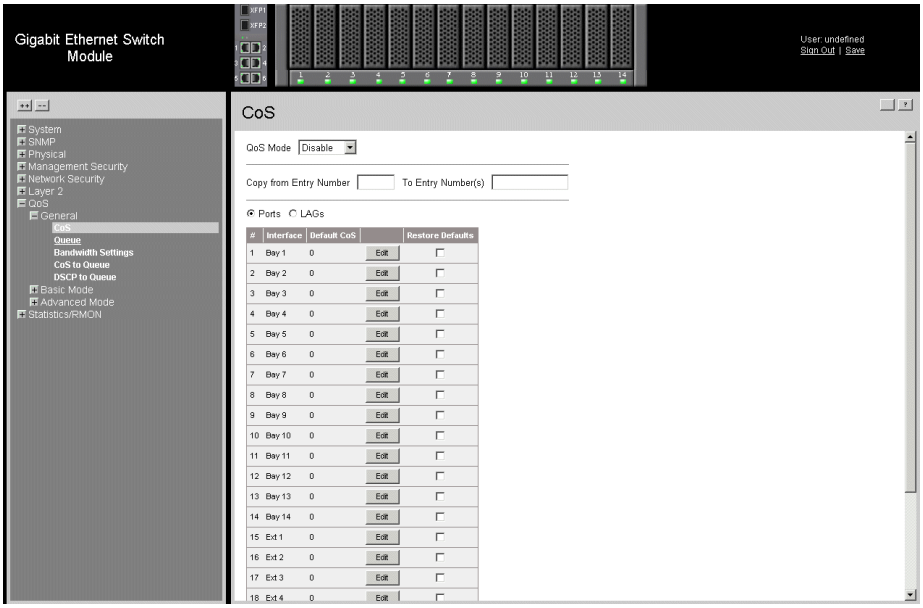



**Figure 125. CoS Global Settings Page**

The *CoS Global Settings Page* contains the following:

- **QoS Mode** — Determines whether QoS is enabled on the interface. The possible values are:
  - *Disable* — Disables QoS on the interface.
  - *Basic* — Enables CoS Basic mode on the device.
  - *Advanced* — Enables Advanced CoS mode on the device.
- **Copy from Entry Number** — Indicates the row number from which CoS parameters are copied.
- **To Entry Number(s)** — Indicates the row number to which CoS parameters are copied.
- **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 tag 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:

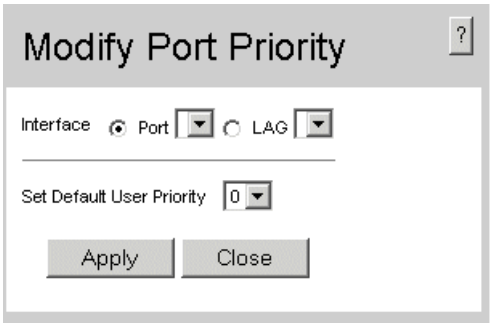



**Figure 126. Modify Port Priority Page**

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 bandwidth to specific QoS service queues.

To set the queue settings:

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

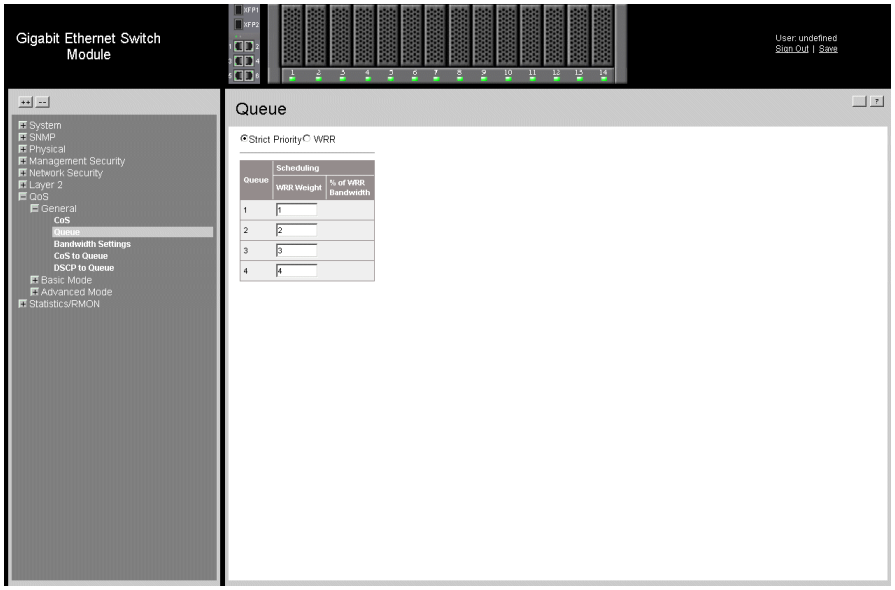



**Figure 127. Queue Page**

The *Queue Page* contains the following fields:

- **Strict Priority** — Specifies whether traffic scheduling is based strictly on the queue priority.
- **WRR —** 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 and is effectively closed. Each queue has a weight range, queues 1-3 have the range 0-255, and queue 4 has the range 1-255.
- **Queue** — Displays the CoS queue for which the bandwidth settings are defined.
- **Schedule** — Displays WWR weight assigned to a specific queue. The possible field values are:
  - *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 and is effectively closed. Each queue has a weight range.
  - *% of WRR Bandwidth* — Indicates the amount of bandwidth assigned to the QoS queue.

2. Define the relevant fields.

3. Click Apply. 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 egress interface. Modifying queue scheduling affects the queue settings globally.

Queue shaping can be based per queue and/or per interface. Shaping is determined by the lower specified value. 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:

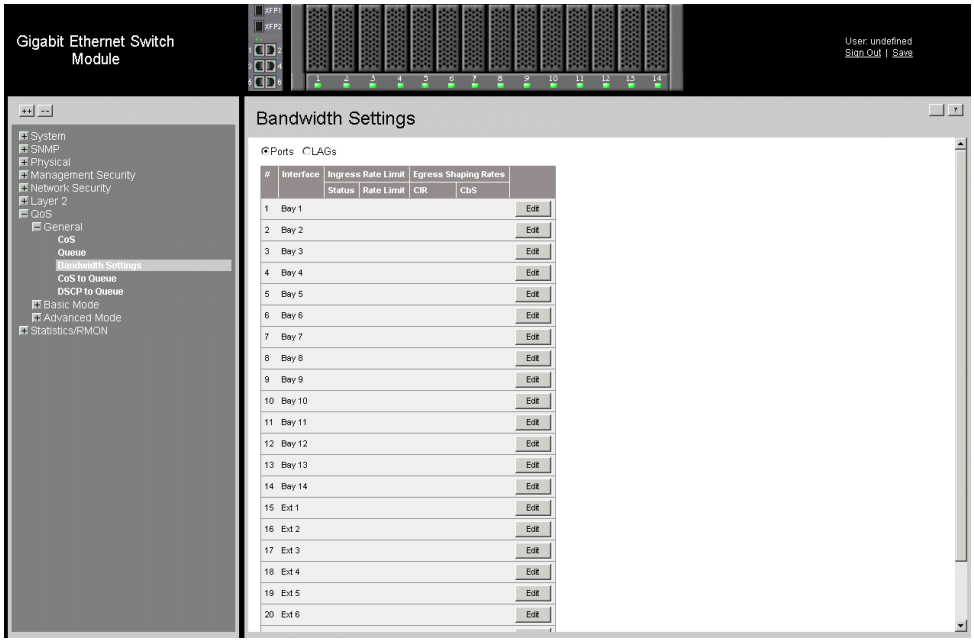



**Figure 128. Bandwidth Settings Page**

The *Bandwidth Settings Page* contains the following fields:

- **Ports** — Indicates the specific port for which the bandwidth settings are defined.
- **LAGs** — Indicates the specific LAG 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 rate at which network traffic is forwarded.
- **Egress Shaping Rates** — Configures the traffic shaping type for selected interfaces. The possible field values are:

— *CIR* — Defines CIR as the queue shaping type. The possible field value is 4096 - *1,000,000,000 bits per second.*

— *CbS* — Defines CbS as the queue shaping type. The possible field value is *4096-16,000,000 bytes.*

2. Select an interface.
3. Click Edit . The *Modify Bandwidth Settings Page* opens.

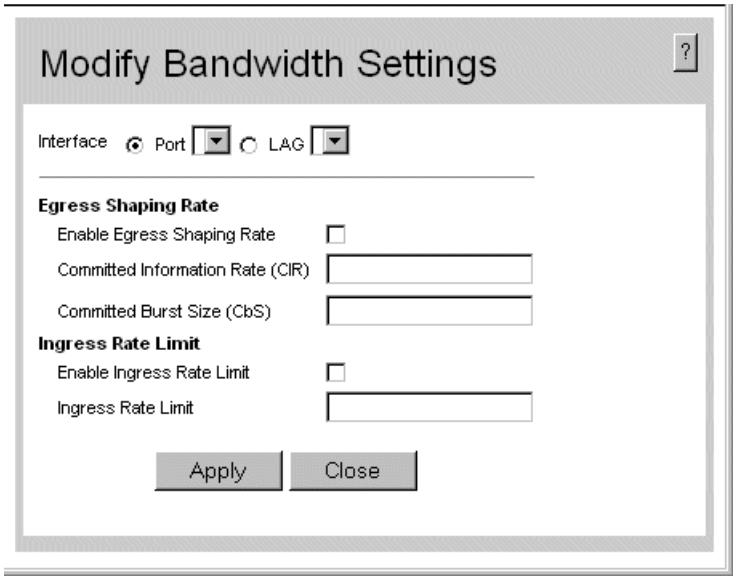



**Figure 129. Modify Bandwidth Settings Page**

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 and DSCP 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.

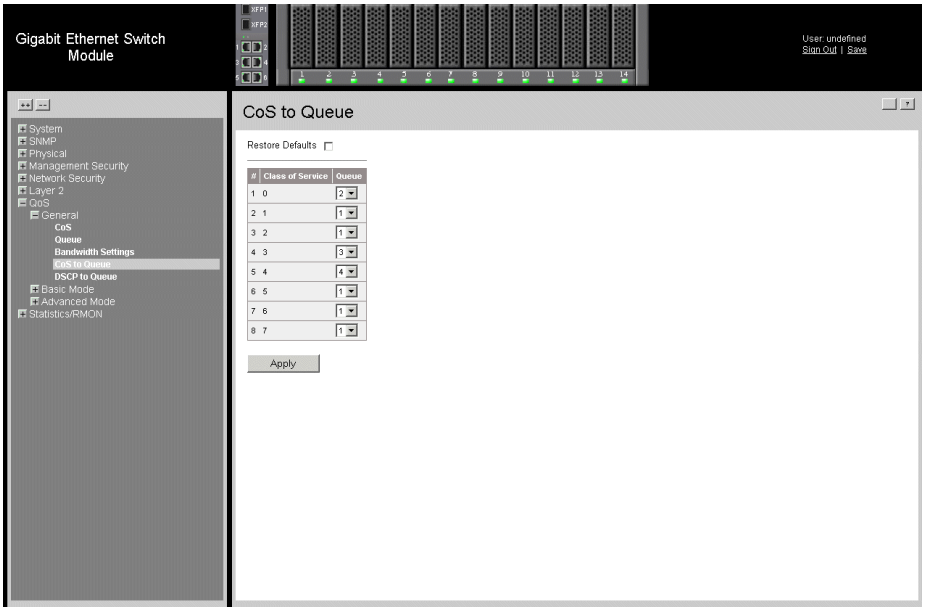



**Figure 130. CoS to Queue Page**

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

- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.
- **Unit No.** — Displays the unit number.
- **Class of Service** — Specifies the CoS priority tag 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.

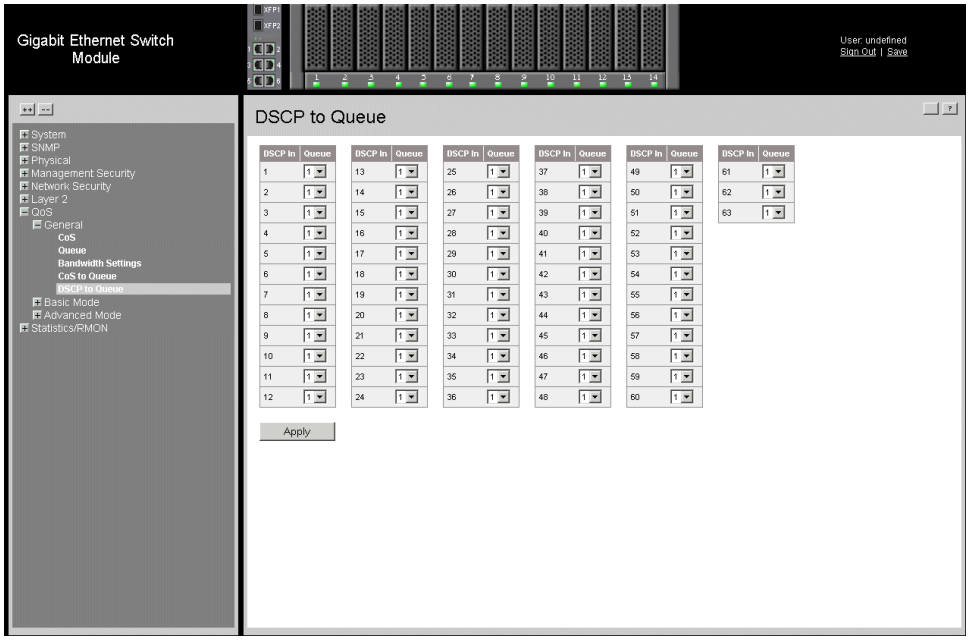



**Figure 131. DSCP to Queue Page**

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

- **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:

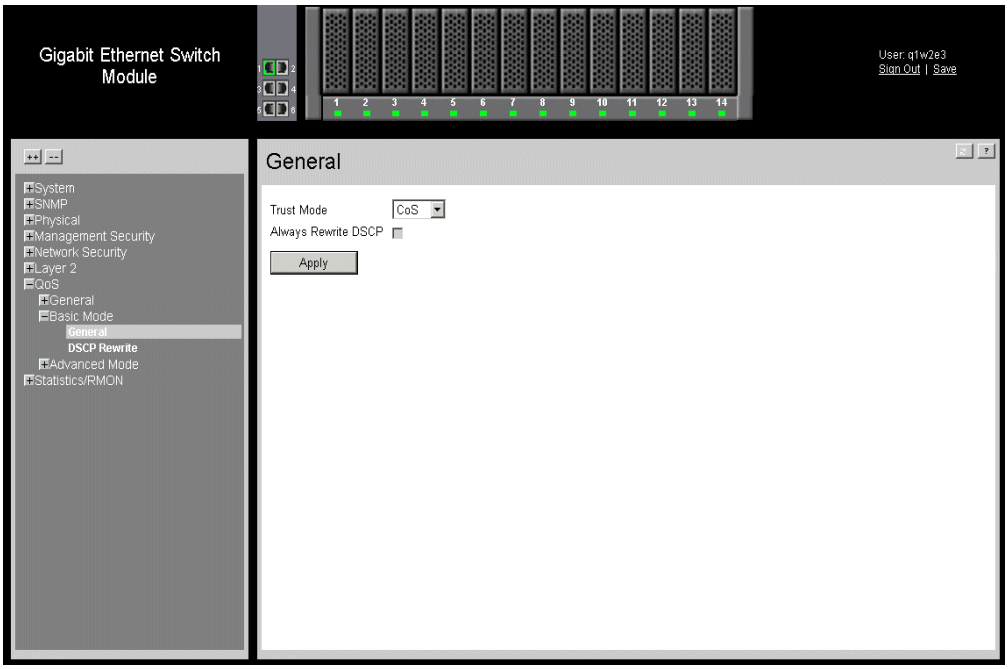



**Figure 132. Basic Mode General Settings Page**

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

- **Trust Mode** — Defines which packet fields to use for classifying packets entering the device. When no rules are defined, the traffic containing the predefined packet CoS field is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust Mode field values are:
  - *CoS* — Classifies traffic based on the CoS tag value.
  - *DSCP* — Classifies traffic based on the DSCP tag values.
- **Always Rewrite DSCP** — Indicates if the DSCP value is always reassigned. The possible field values are:
  - *Checked* — Enables reassigning the DSCP value.
  - *Unchecked* — Disables reassigning the DSCP value. This is the default value..

2. Define the relevant fields.
3. Click Apply . The *QoS General Settings* are configure, and the device is updated.

## Configuring DSCP Rewrite

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

To configure the DSCP rewrite:

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

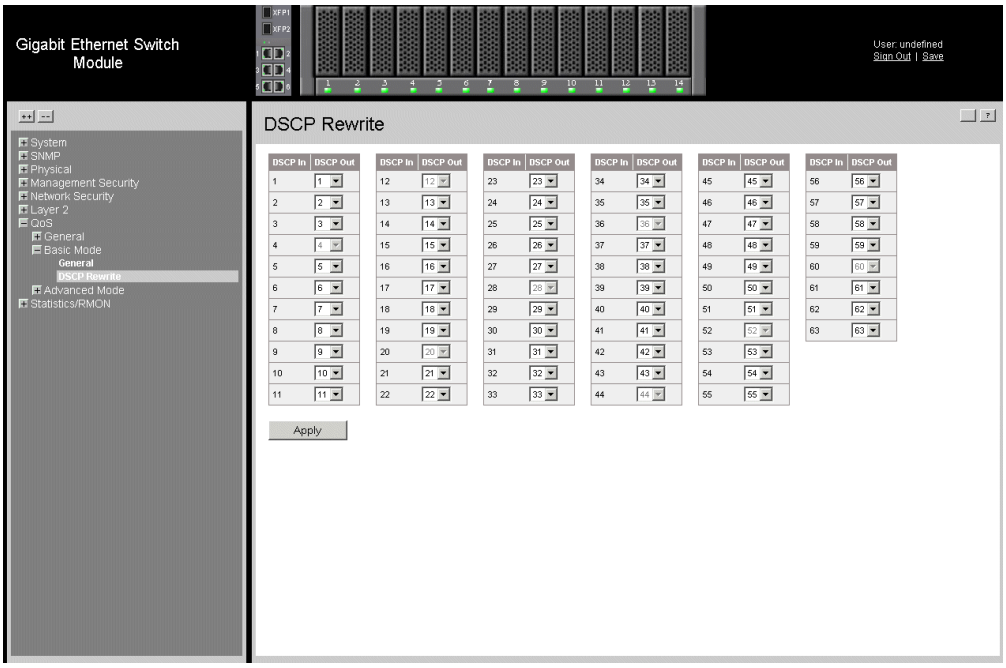



**Figure 133. QoS DSCP Rewrite Page**

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 Policiers

## Mapping DSCP Values

When traffic exceeds user-defined limits, use the *Policied 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 > Policied DSCP**. The *Policied DSCP Page* opens.

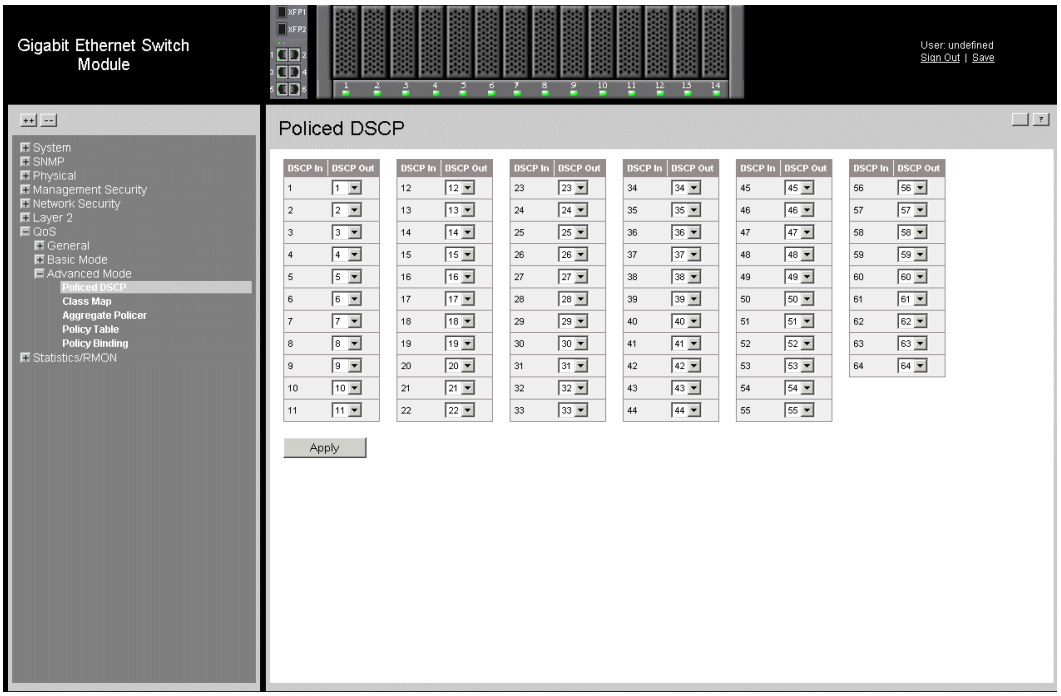



**Figure 134. Policied DSCP Page**

The *Policied 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:

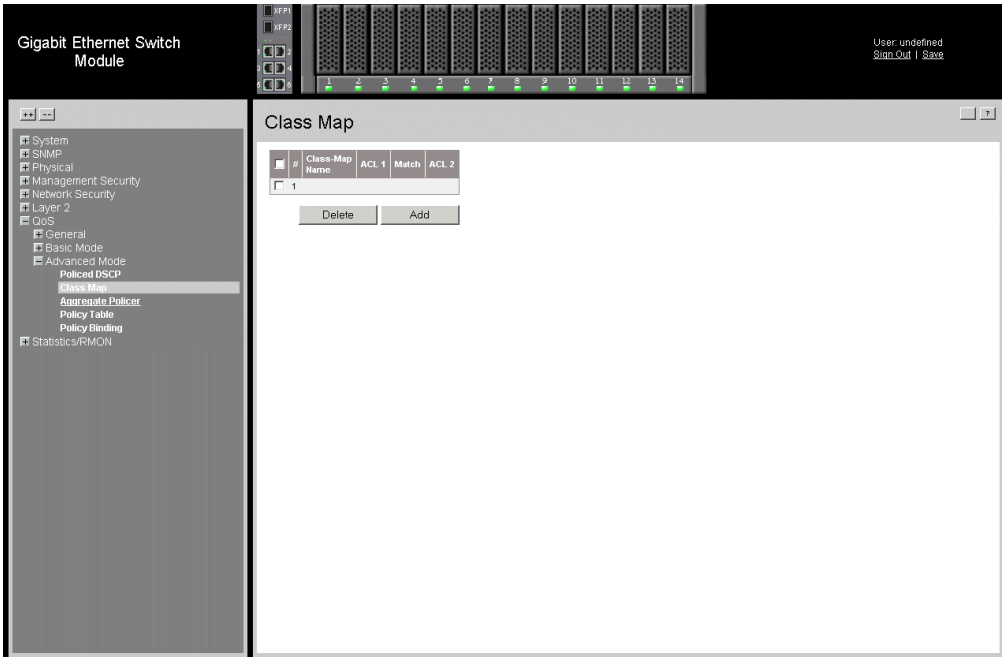



**Figure 135. Class Map Page**

The *Class Map Page* contains the following fields:

- **Remove** — Removes Class Maps. The possible field values are:
  - — *Checked* — Removes 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 class maps with an ACL's address. 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 Rule . The *Add Class Map Page* opens.

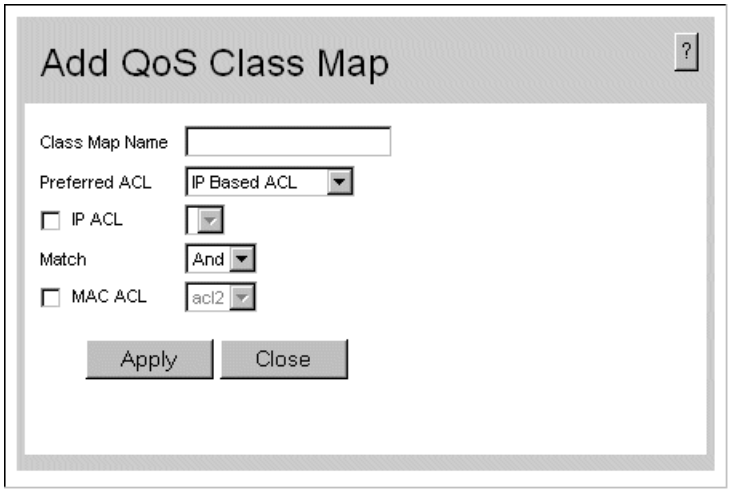



**Figure 136. Add Class Map Page**

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 policiers enforce limits on a group of flows. An aggregate policier 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:

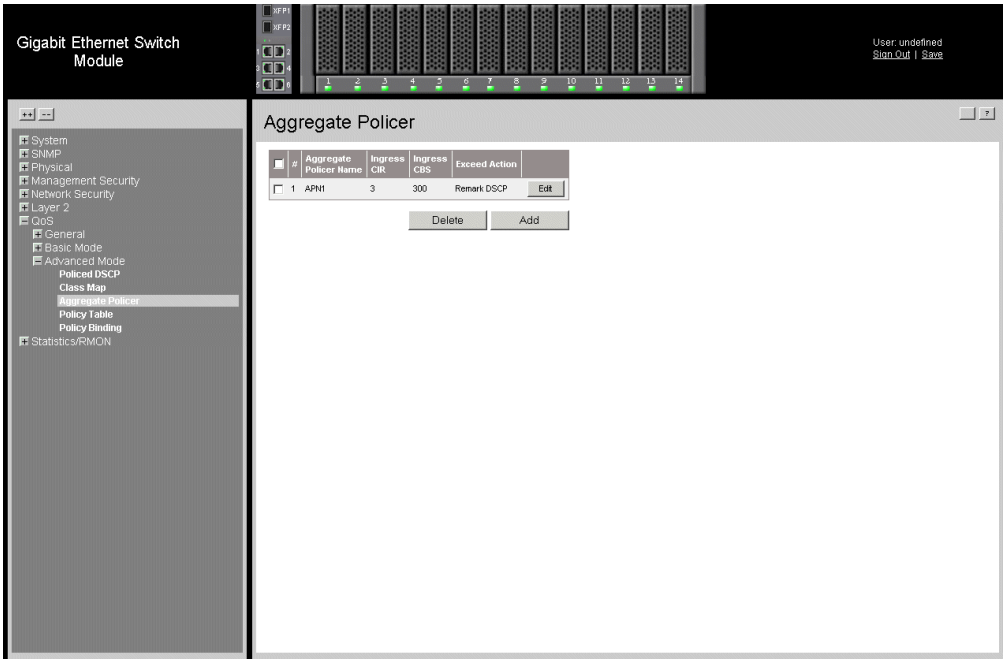



**Figure 137. Aggregated Policier Page**

The *Aggregated Policier Page* contains the following fields:

- **Remove** — Removes Aggregated Policy. The possible field values are:
  - *Checked* — Removes the selected Aggregated Policy.
  - *Unchecked* — Maintains the current Aggregated Policy.
- **Aggregate Policer Name** — Specifies the aggregate policer name.
- **Ingress CIR**— Defines the CIR in bits 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.

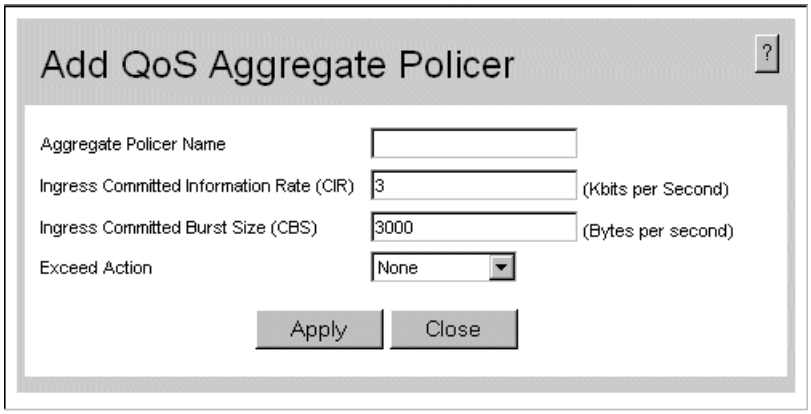



**Figure 138. Add Aggregated Policier Page**

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:

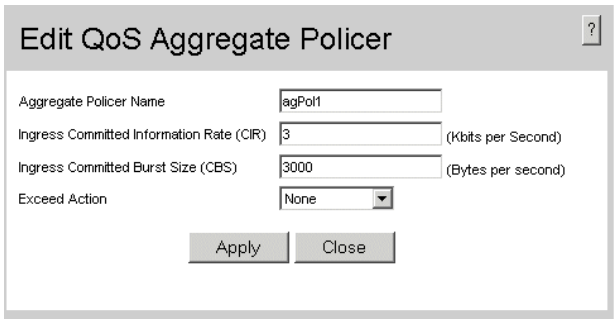



**Figure 139. Edit QoS Aggregate Policier Page**

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
- Attaching Policies to Interfaces

## 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. Policiers 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:

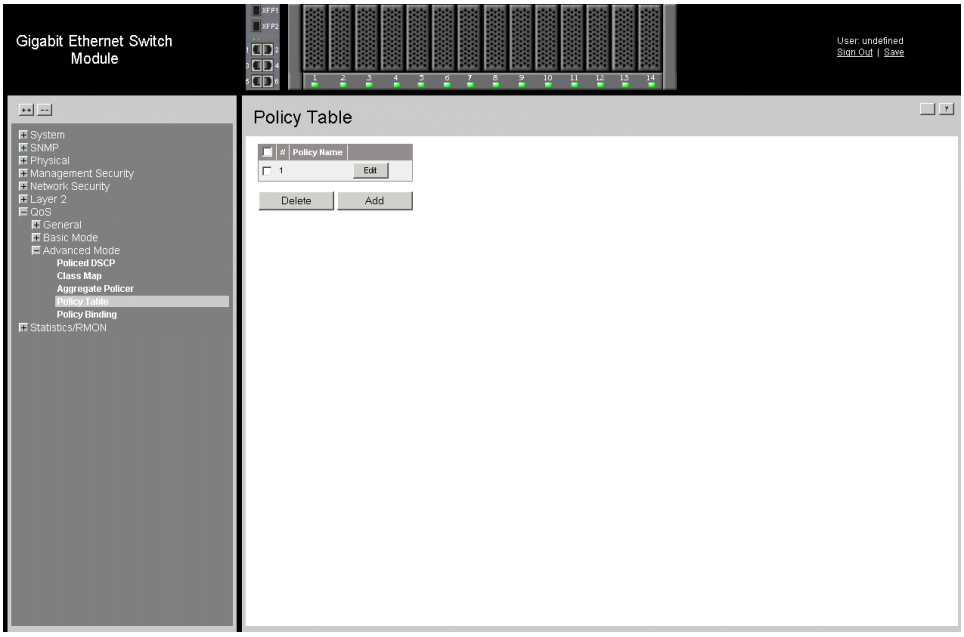



**Figure 140. Policy Table Page**

The *Policy Table Page* contains the following fields:

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

2. Click Add . The *Add QoS Policy Profile Page* opens:

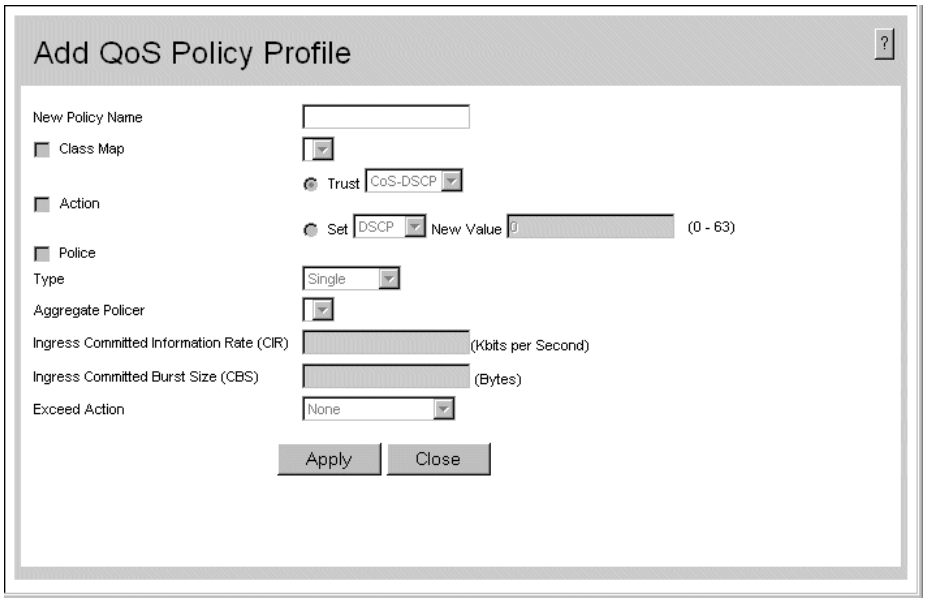



**Figure 141. Add QoS Policy Profile Page**

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

- **Class Map** — Selects a class map for the class.
- **Action** — Indicates the action performed on incoming packets matching the policy profile. The possible field values are:
  - *Trust* - Applies the selected Trust settings.
  - *Set* - Redefines the DSCP settings.
- **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 bits 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.

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:

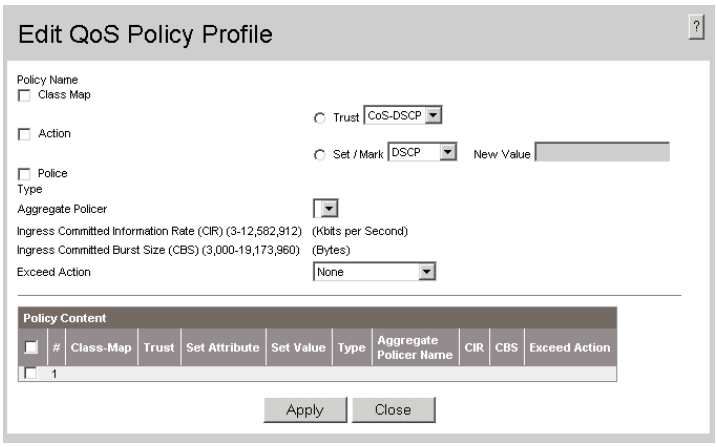



**Figure 142. Edit QoS Policy Profile Page**

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.

To attach a policy to an interface:

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

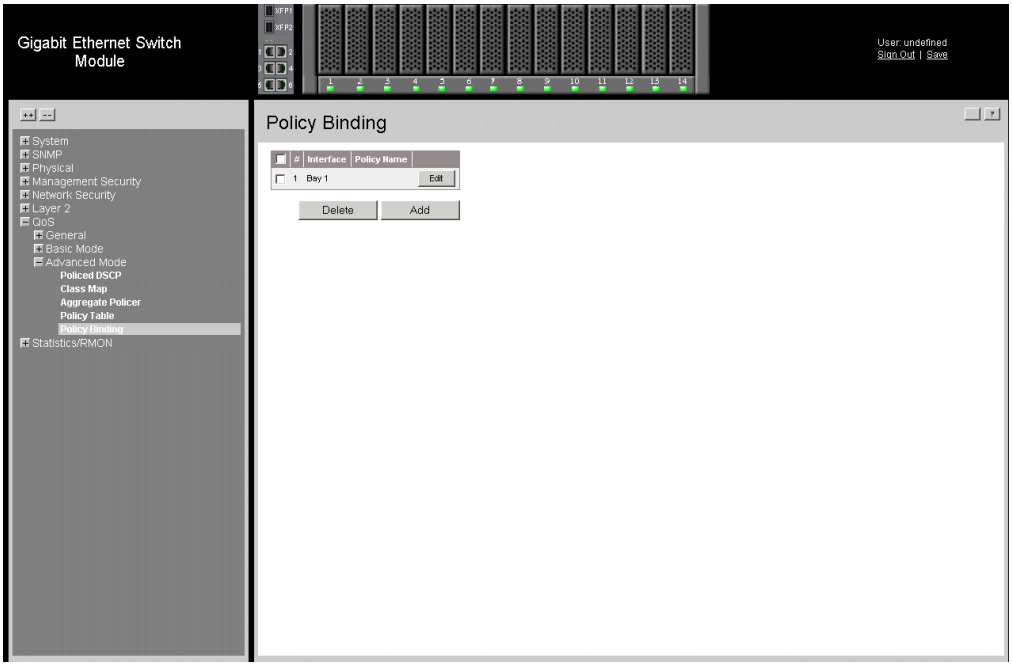



**Figure 143. Policy Binding Page**

The *Policy Binding Page* contains the following fields:

- **Remove** — Removes policies.
  - — *Checked* — Removes 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.

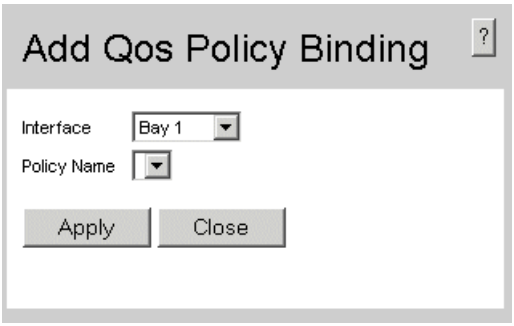



**Figure 144. Add Qos Policy Binding Page**

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:

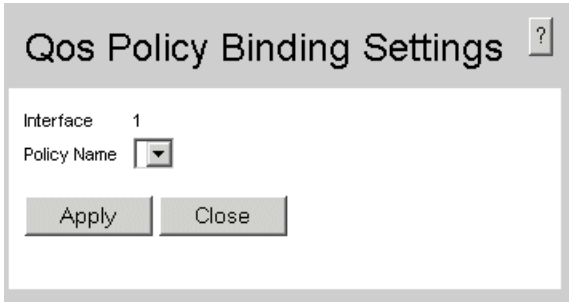



**Figure 145. Qos Policy Binding Settings Page**

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

# 16 Managing System Files

File maintenance includes both configuration file management and device access. This section contains the following topics:

- File Management Overview
- Downloading System Files
- Uploading System Files
- Activating Image Files

## File Management Overview

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Image files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

# Downloading System Files

There are two types of files, firmware files and configuration files. The firmware files manage the device, and the configuration files configure the device for transmissions. Only one type of download can be performed at any one time.

The *File Download* page contains parameters for downloading system files.

To download system files via TFTP or HTTP:

1. Click **System > File Management > File Download**. The *File Download Page* opens.


**Figure 146. File Download Page**

The *File Download Page* contains the following download types:

- **Download via TFTP** — Enables downloading through the Trivial File Transfer Protocol.
- **Download via HTTP** — Enables downloading through the HyperText Transfer Protocol.

The *File Download Page* is divided into the following sections:

- Firmware Download
- Configuration Download

## Firmware Download

The *Firmware Download* section contains the following fields:

- **Firmware Download** — Indicates that the download is for firmware. If *Firmware Download* is selected, the Configuration Download fields are grayed out.
- **Server IP Address** — Specifies the Server IP Address from which files are downloaded.
- **Source File Name** — Specifies the file to be downloaded.
- **Destination File** — Specifies the destination file type to which to the file is downloaded. The possible field values are:
  - *Software Image* — Downloads the Image file.
  - *Boot Code* — Downloads the Boot file.

## Configuration Download

The *Configuration Download* section contains the following fields:

- **Configuration Download** — Indicates that the download is for configuration files. If *Configuration Download* is selected, the Firmware Download fields are grayed out.
- **Server IP Address** — Specifies the Server IP Address from which the configuration files are downloaded.
- **Source File Name** — Specifies the configuration files to be downloaded.
- **Destination File** — Specifies the destination file to which to the configuration file is downloaded. The possible field values are:
  - *Running Configuration* — Downloads commands into the Running Configuration file.
  - *Startup Configuration* — Downloads the Startup Configuration file, and overwrites the old Startup Configuration file.
  - *Backup Configuration* — Downloads the Backup Configuration file. One only Backup Configuration file can be saved

To download files via TFTP or HTTP:

1. Open the File Download Page.
2. Select the file type.
3. Define the relevant fields.
4. Click Apply. The files are downloaded.

# Uploading System Files

The *File Upload Page* contains fields for uploading the software from the device to the TFTP server.

To upload system files:

1. Click **System > File Management > File Upload**. The *File Upload Page* opens:

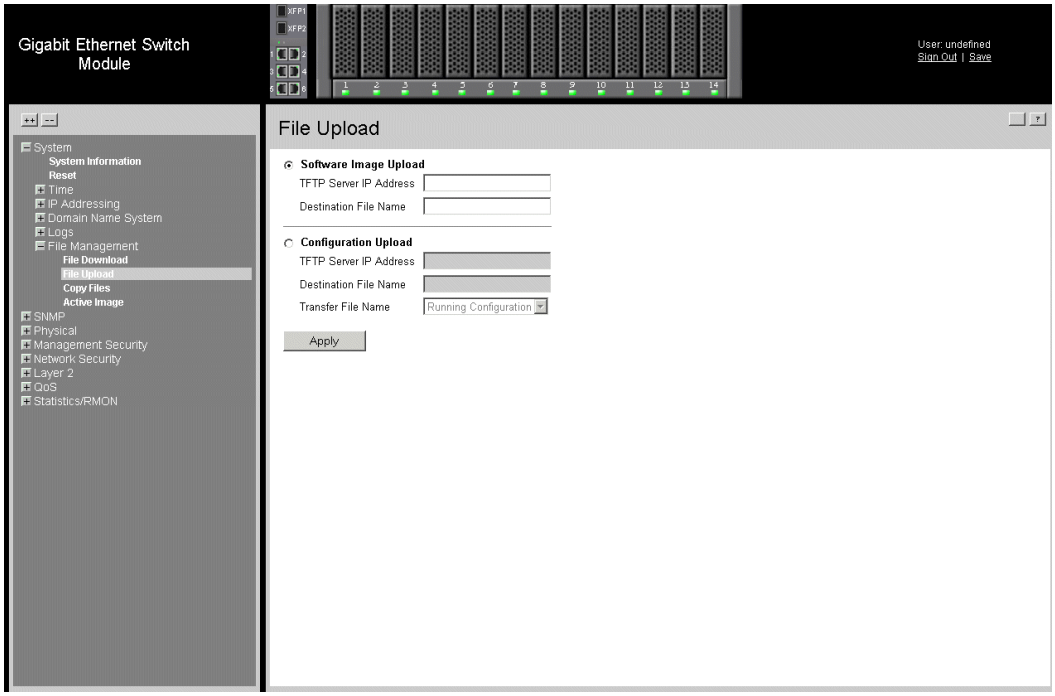



**Figure 147. File Upload Page**

The *File Upload Page* is divided into the following sections:

- Software Image Upload
- Configuration Upload

# Software Image Upload

The *Software Image Upload* section contains the following fields:

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Software Image is uploaded.
- **Destination File Name** — Specifies the software image file path to which the file is uploaded.

# Configuration Upload

The *Configuration Upload* section contains the following fields:

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Configuration file is uploaded.
- **Destination File Name**— Specifies the file name to which the Startup Configuration file is uploaded.
- **Transfer file name** — Specifies the Configuration file name that is uploaded. The possible field values are:
  - *Running Configuration* — Uploads the Running Configuration file.
  - *Startup Configuration* — Uploads the Startup Configuration file.
  - *Backup Configuration* — Uploads the Backup Configuration file. One only Backup Configuration file can be saved

To upload files:

1. Open the *File Upload Page*.
2. Define the relevant fields.
3. Click Apply . The software is uploaded to the device.

# Copying Files

Files can be copied and deleted from the *Copy Files Page*.

To copy files:

1. Click **System > File Management > Copy Files.** The *Copy Files Page* opens.

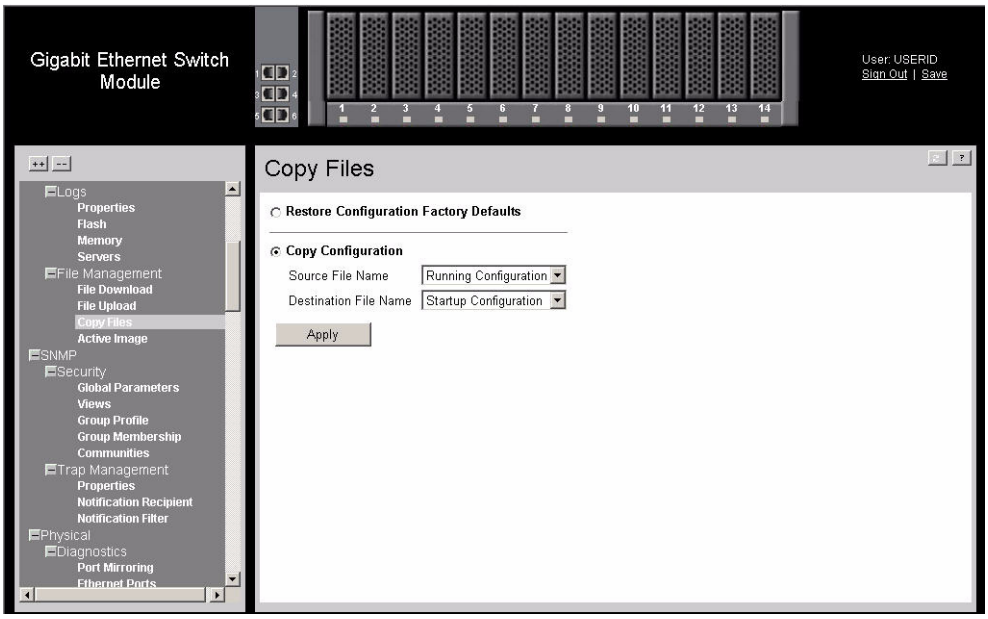



**Figure 148. Copy Files Page**

The *Copy Files Page* contains the following fields:

- **Restore Configuration Factory Defaults** — Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When unselected, the device maintains the current Configuration file.
- **Source** — Indicates the system file to be copied. The possible field values are:
  - *Software Image* — Copies the software Image file.
  - *Boot Code* — Copies the boot code.
- **Destination Unit** — Indicates the Startup Configuration file is selected.
- **Copy Configuration** — Copies the Running Configuration file to the Startup Configuration file.
- **Source** — Indicates the Running Configuration file is selected. The possible field values are:
  - *Running Configuration* — Copies the Running Configuration file.
  - *Startup Configuration* — Copies the Startup Configuration file.

— *Backup Configuration* — Copies the Backup Configuration file.

- **Destination** — Indicates the Startup Configuration file is selected. The possible field values are:
  - — *Running Configuration* — Specifies the destination of the Running Configuration file.
  - — *Startup Configuration* — Specifies the destination of the Startup Configuration file.
  - — *Backup Configuration* — Specifies the destination of the Backup Configuration file. One only Backup Configuration file can be saved.

2. Select the relevant fields.
3. Click Apply. The file is copied.

## Restoring the Default Configuration File

1. Click **System > File Management > Copy Files**. The *Copy Files Page* opens.
2. Select *Restore Configuration Factory Defaults*.
3. Click Apply. The factory defaults are restored, and the device is updated.

# Activating Image Files

The *Active Image Page* allows network managers to select and reset the Image files. The Active Image file for each unit can be individually selected.

To select an active image:

1. Click **System > File Management > Active Image**. The *Active Image Page* opens:

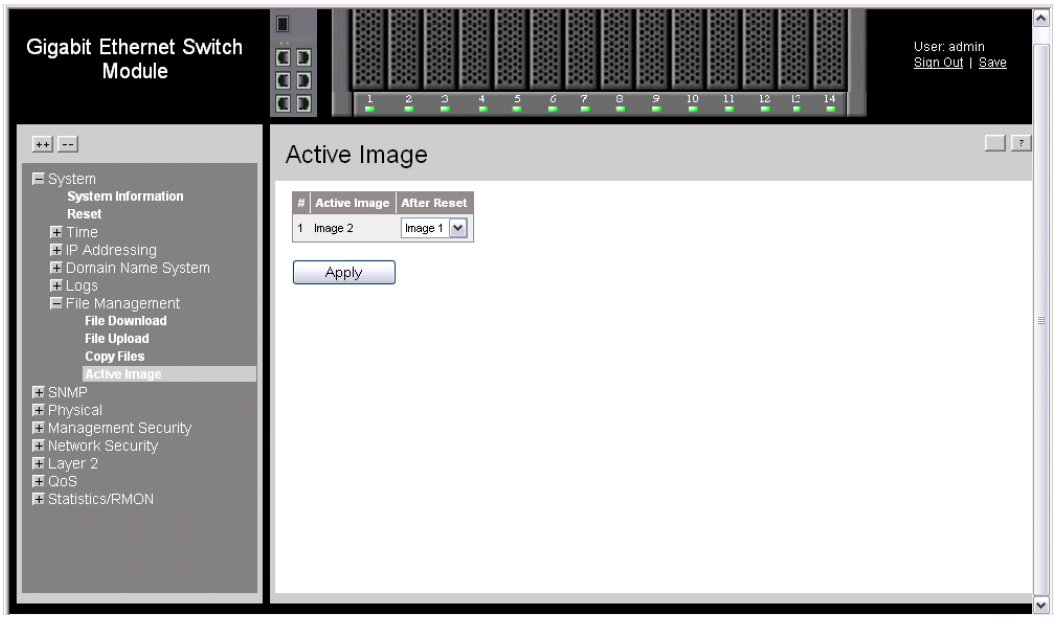



**Figure 149. Active Image Page**

The *Active Image Page* contains the following fields:

- **Active Image** — The Image file which is currently active on the unit.
- **After Reset** — The Image file which is active on the unit after the device is reset. The possible field values are:
  - — *Image 1* — Activates Image file 1 after the device is reset.
  - — *Image 2* — Activates Image file 2 after the device is reset.

2. Define the Active Image field.
3. Click Apply. The select image file is activated after the device is reset.

# 17 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:

**Table 3. 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
- Defining Servers Log Parameters

# Enabling System Logs

The *Syslog 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.

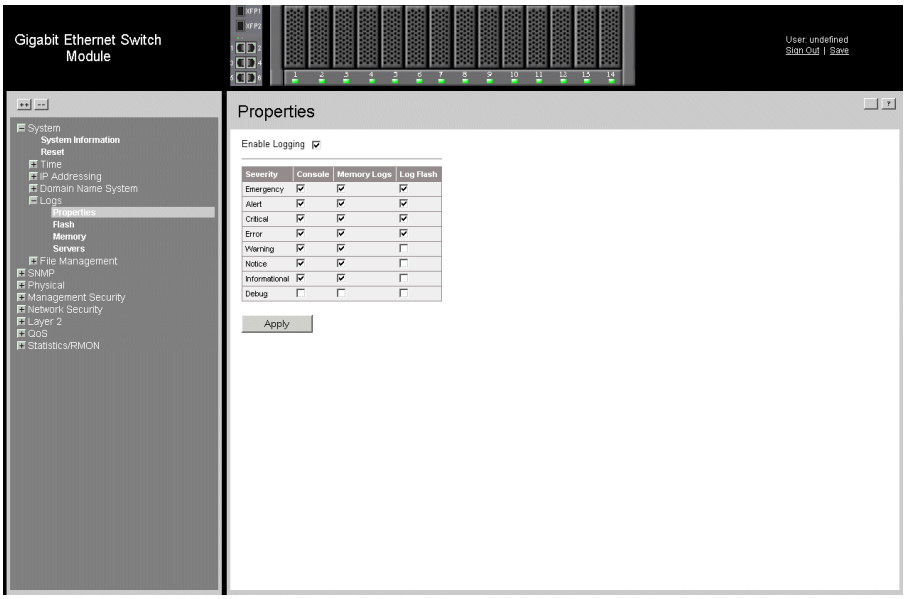



**Figure 150. System Logs Properties Page**

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

- **Enable Logging** — Indicates if device global logs for Cache, File, and Server 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, for example, if a single port is offline.

— *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 Logs Flash 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 Logs Flash Page* opens:

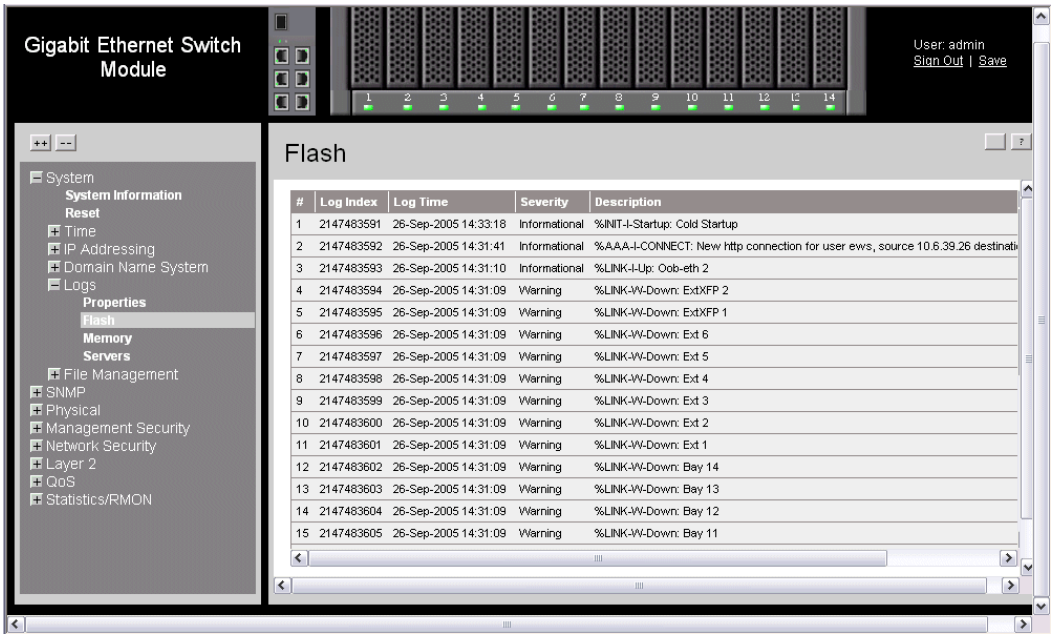



**Figure 151. System Logs Flash Page**

The *System Logs Flash 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 Log Flash Page*.

To clear message logs:

1. Click **System** > **Logs** > **Flash**. The *System Log Flash 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.

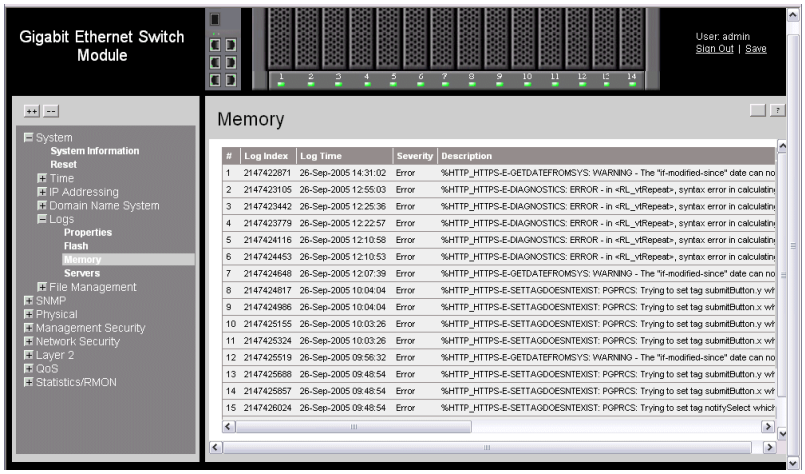



**Figure 152. Device Memory Log Page**

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 Clear Logs . The message logs are cleared.

# Defining Servers Log Parameters

The *System Log Servers Settings Page* contains information for viewing and configuring the remote log servers. New log servers can be defined, and the log severity sent to each server.

To open the *System Log Servers Settings Page*:

1. Click **System > Syslog > Servers**. The *System Log Servers Settings Page* opens.

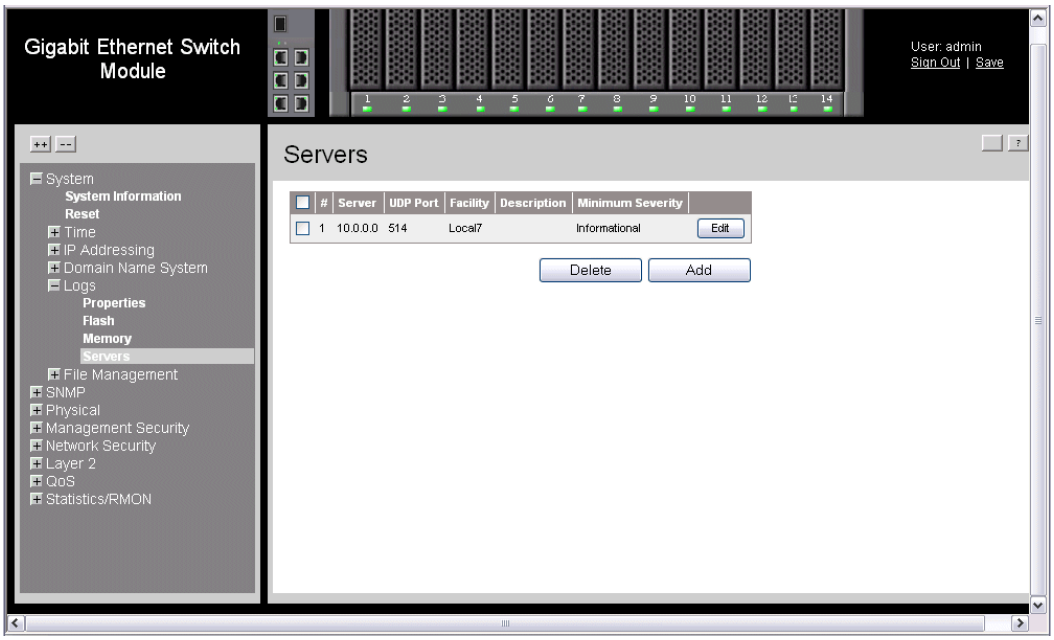



**Figure 153. System Log Servers Settings Page**

The *System Log Servers Settings Page* contains the following fields:

- **Remove** — Deletes the currently selected server from the Servers list. The possible field values are:
  - — *Checked* — Removes the selected server from the *Servers Log Parameters Page*. Once removed, logs are no longer sent to the removed server.

— *Unchecked* — Maintains the remote servers.

- **Server** — Specifies the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.
- **Facility** — Defines an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are *Local 0* - *Local 7*.
- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity from which logs are sent to the server. For example, if *Notice* is selected, all logs with a severity level of *Notice* and higher are sent to the remote server.

2. Click Add . The *Add Syslog Server Settings Page* opens:

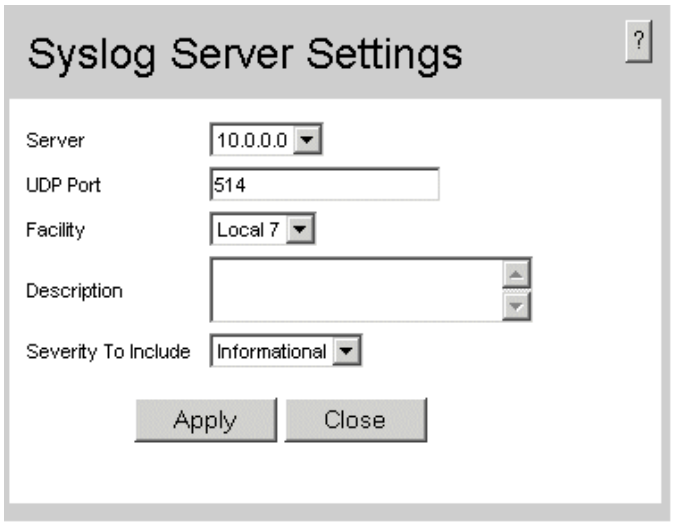



**Figure 154. Add Syslog Server Settings Page**

3. Define the relevant fields.
4. Click Apply . The *System Log Server* is defined, and the device is updated.

To modify the :

1. Click **System > Logs > Servers.** The  opens.
2. Click Edit . The  opens:

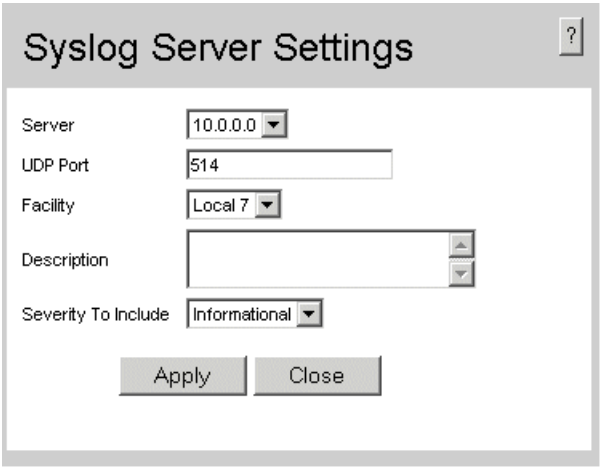



**Figure 155. Syslog Server Settings Page**

3. Modify the relevant fields.
4. Click Apply . The *System Log Server* is modified, and the device is updated.

# 18 Managing Device Diagnostics

This section contains the following topics:

- Configuring Port Mirroring
- Ethernet Ports Diagnostics

## 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 **Physical > Diagnostics > Port Mirroring**. The *Ethernet Ports Page* opens:

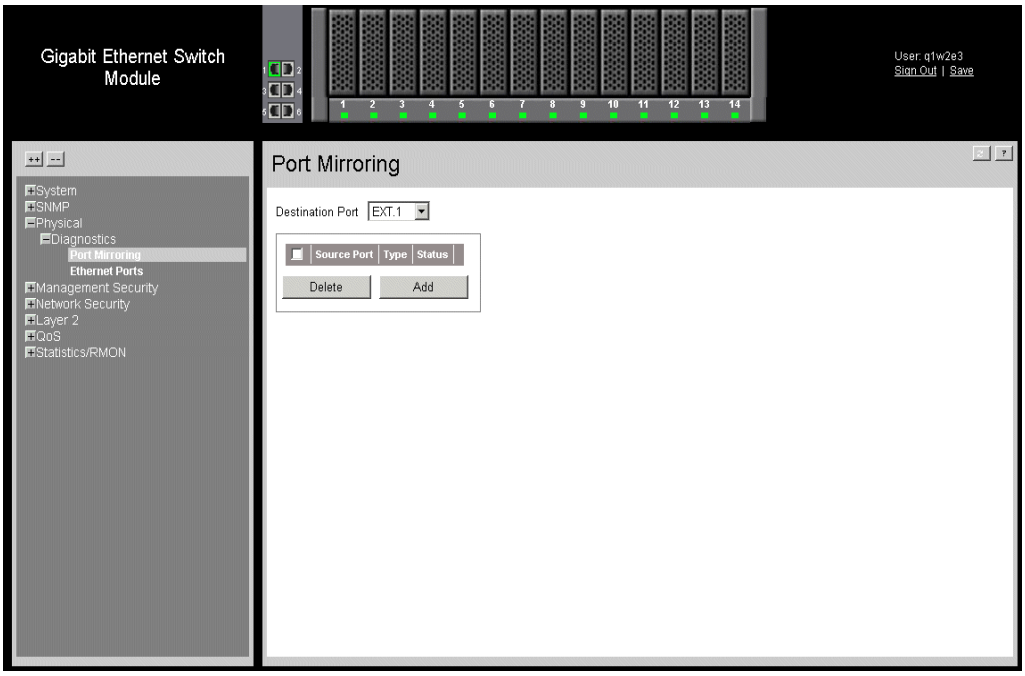



**Figure 156. Port Mirroring Page**

The *Ethernet Ports Page* contains the following fields:

- **Destination Port** — Defines the port number to which port traffic is copied.
- **Remove** — Removes the port mirroring session. The possible field values are:
  - *Checked* — Removes 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* — Defines the port mirroring on receiving ports.
  - *TX* — Defines the port mirroring on transmitting ports.
  - *Both* — 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.

2. Click Add . The *Add Port Mirroring Page* opens:

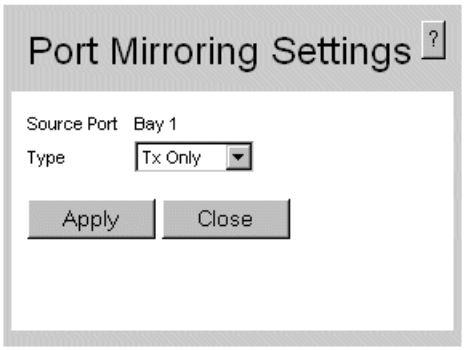



**Figure 157. Add Port Mirroring Page**

3. Define the relevant fields.
4. Click Apply . The port mirroring session is defined, and the device is updated.

To modify the port mirroring settings:

1. Click **Physical > Diagnostics > Port Mirroring**. The *Ethernet Ports Page* opens.
2. Click Edit . The *Port Mirroring Settings Page* opens:

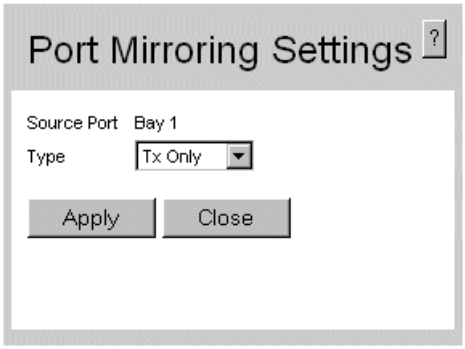



**Figure 158. Port Mirroring Settings Page**

3. Modify the relevant fields.
4. Click Apply . The port mirroring settings are modified, and the device is updated.

# Ethernet Ports Diagnostics

To test ethernet ports:

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

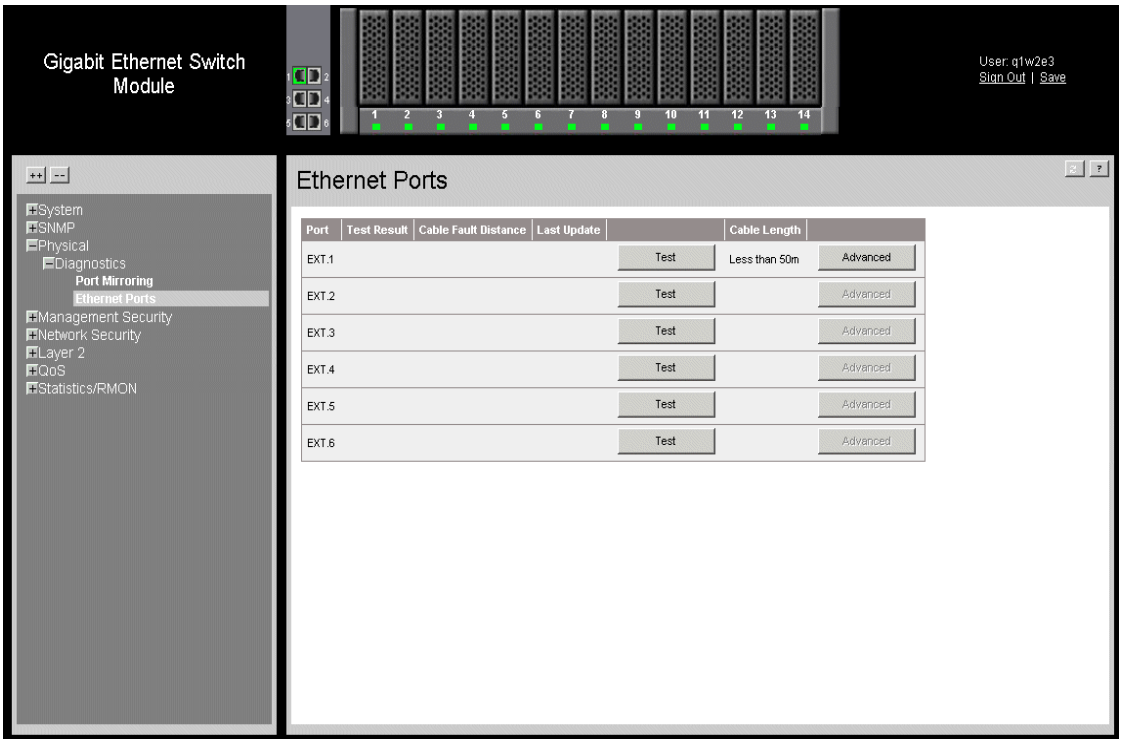



**Figure 159. Ethernet Ports Page**

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 Test . The ethernet port is tested.

To perform an advance test on the ethernet port:

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

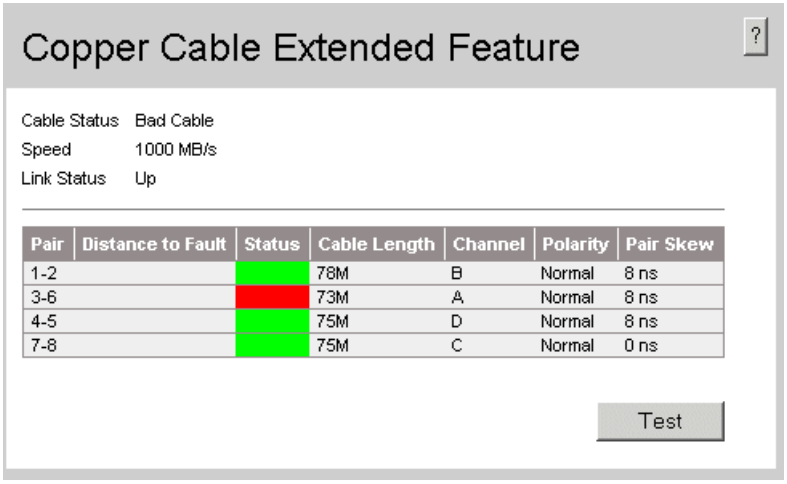



**Figure 160. Copper Cable Extended Feature Page**

3. Click Test . The ethernet port is tested.

# 19 Configuring System Time

This section provides information for configuring system time parameters, including:

- Configuring Daylight Savings Time
- Configuring SNTP
- Defining SNTP Global Settings
- Defining SNTP Authentication

## Configuring Daylight Savings Time

The *System Time Page* contains fields for defining system time parameters for both the local hardware clock and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

The following is a list of Daylight Savings Time start and end times in specific countries:

- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania —** From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with Daylight Savings Time in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — In Easter Island, from March 9 until October 12. In the rest of the country, from the first Sunday in March or after 9th March.
- **China** — China does not use Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — From the last weekend of March until the last weekend of October.

- **Denmark** — From the last weekend of March until the last weekend of October.
- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use Daylight Saving Time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use Daylight Saving Time.
- **Jordan** — From the last weekend of March until the last weekend of October.
- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.
- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.

- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use Daylight Saving Time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use Daylight Saving Time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the last weekend of March until the last weekend of October.
- **United States of America** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.

To configure the system time:

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

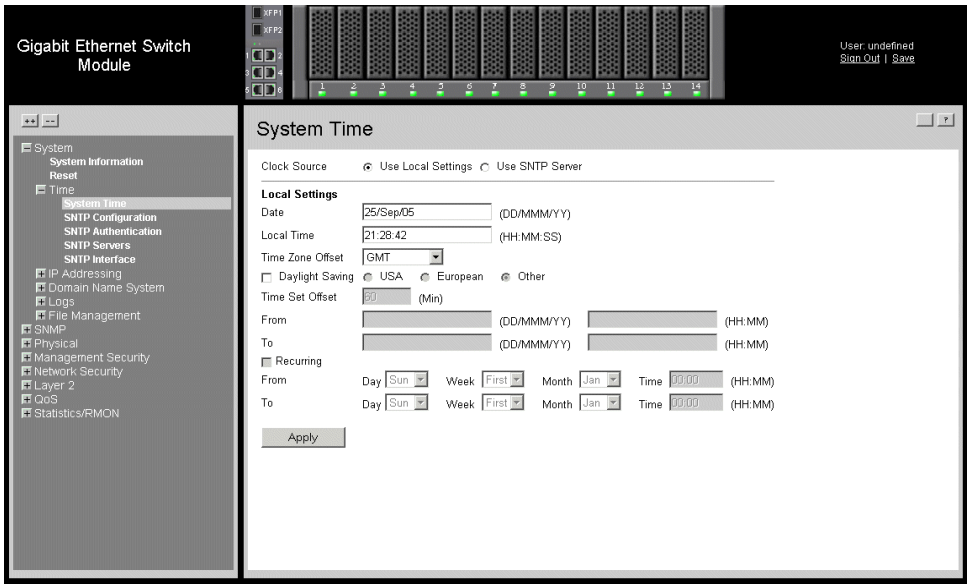



**Figure 161. System Time Page**

The *System Time Page* contains the following sections:

- **Clock Source** — Displays the source used to set the system clock. The possible field values are:
  - — *Use Local Settings* — Indicates that a clock source is not used. The clock is set locally.
  - — *Use SNTP Server*— Indicates that the system time is set via an SNTP server.

- **Date** — Displays the system date. The field format is Day/Month/Year. For example: 04/May/50 (May 4, 2050).
- **Local Time** — Displays the system time. The field format is HH:MM:SS. For example: 21:15:03.
- **Time Zone Offset** — Displays the difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.
  - *Daylight Savings* — Enables automatic Daylight Savings Time (DST) on the device based on the device's location. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area. The possible field values are:
  - *USA* — Indicates the device switches to DST at 2:00 a.m. on the first Sunday of April, and reverts to standard time at 2:00 a.m. on the last Sunday of October.
  - *European* — Indicates the device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.
  - *Other* — Indicates the DST definitions are user-defined based on the device locality. If Other is selected, the *From* and *To* fields must be defined.
- **Time Set Offset (1-1440)** — Indicates the time offset for non-USA and European countries to set the amount of time for DST (in minutes). The default time is 60 minutes.
  - ***From*** — Indicates the time that DST begins in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST begins on October 25, 2007 at 5:00 am, the two fields are set to 25/Oct/07 and 05:00. The possible field values are:
  - *Date* — Indicates the date on which DST begins. The possible field range is 1-31.
  - *Month* — Indicates the month of the year in which DST begins. The possible field range is Jan-Dec.
  - *Year* — Indicates the year in which the configured DST begins.
  - *Time* — Indicates the time at which DST begins. The field format is HH:MM. For example: 05:30.
  - ***To*** — Indicates the time that DST ends in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST ends on March 23, 2008 at midnight, the two fields are 23/Mar/08 and 00:00. The possible field values are:
  - *Date* — Indicates the date on which DST ends. The possible field range is 1-31.
  - *Month* — Indicates the month of the year in which DST ends. The possible field range is Jan-Dec.
  - *Year*— Indicates the year in which the configured DST ends.

- ***Time*** — Indicates the time at which DST starts. The field format is HH:MM. For example: 05:30.
- **Recurring** — Enables user-defined DST for countries in which DST is constant from year to year, other than the USA and Europe.
  - ***From*** — Indicates the time that DST begins each year. In the example, DST begins locally every first Sunday in April at midnight. The possible field values are:
  - *Day* — Indicates the day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
  - *Week* — Indicates the week within the month from which DST begins every year. The possible field range is 1-5.
  - *Month* — Indicates the month of the year in which DST begins every year. The possible field range is Jan-Dec.
  - *Time* — Indicates the time at which DST begins every year. The field format is Hour:Minute. For example: 02:10.
  - ***To*** — Indicates the time that DST ends each year. In the example, DST ends locally every first Sunday in October at midnight. The possible field values are:
  - *Day* — Indicates the day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
  - *Week* — Indicates the week within the month at which DST ends every year. The possible field range is 1-5.
  - *Month* — Indicates the month of the year in which DST ends every year. The possible field range is Jan-Dec.
  - *Time* — Indicates the time at which DST ends every year. The field format is HH:MM. For example: 05:30.

2. Define the relevant fields.
3. To configure the device to automatic, switch to DST, select *Daylight Savings* and select either *USA*, *European*, or *Other*. If you select *Other*, you must define its *From* and *To* fields. To configure DST parameters that will recur every year, select *Recurring* and define its *From* and *To* fields.
4. Click Apply . The DST settings are saved, and the device is updated.

# Configuring SNTP

The device supports the *Simple Network Time Protocol* (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above.

The following is an example of stratums:

- **Stratum 0** — A real time clock (such as a GPS system) is used as the time source.
- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2** — The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the Time level and server type. SNTP time definitions are assessed and determined by the following time levels:

- **T1** — The time at which the original request was sent by the client.
- **T2** — The time at which the original request was received by the server.
- **T3** — The time at which the server sent the client a reply.
- **T4** — The time at which the client received the server's reply.

## Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing device time.

## Polling for Anycast Time Information

Polling for Anycast information is used when the SNTP server IP address is unknown. The first Anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information.

## Broadcast Time Information

Broadcast information is used when the server IP address is unknown. When a broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

*Message Digest 5* (MD5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

This section contains the following topics:

- Defining SNTP Global Settings
- Defining SNTP Authentication

# Defining SNTP Global Settings

To configure SNTP:

1. Click **System** > **Time** > **SNTP Configuration**. The *SNTP Configuration Page* opens:

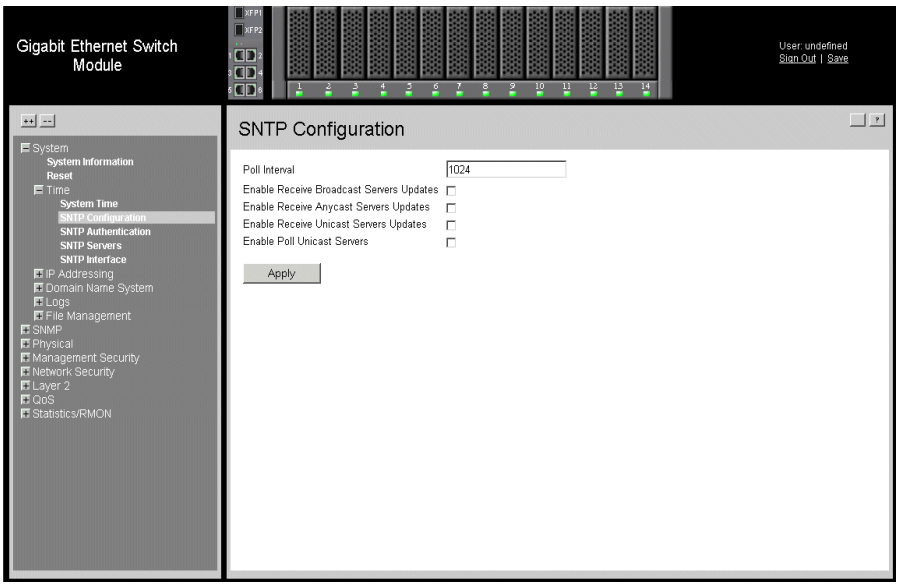



**Figure 162. SNTP Configuration Page**

The *SNTP Configuration Page* contains the following fields:

- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 1024 seconds.
- **Enable Receive Broadcast Servers Updates** — Enables updates for receiving broadcasts.
- **Enable Receive Anycast Servers Updates** — Enables updates for receiving anycast.
- **Enable Receive Unicast Servers Updates** — Enables updates for unicast broadcasts.

2. **Enable Poll Unicast Servers** — Enables poll unicast servers.Define the relevant fields.
3. Click Apply. The SNTP is configured, and the device is updated.

•

The *SNTP Servers Page* provides information for defining SNTP parameters globally.

To define SNTP global parameters:

1. Click **System** > **Time** > **SNTP Servers**. The *SNTP Servers Page* opens:

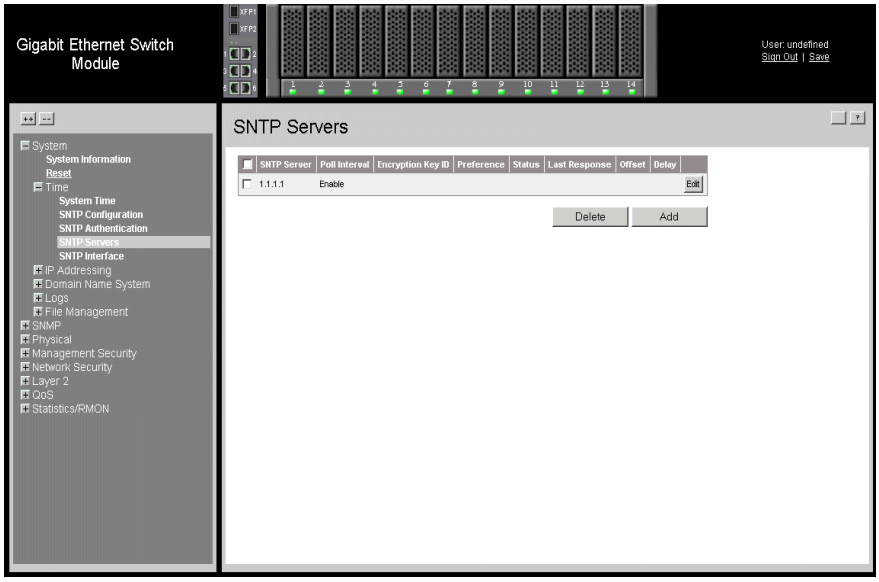



**Figure 163. SNTP Servers Page**

The *SNTP Servers Page* contains the following fields:

- **SNTP Server —** Displays user-defined SNTP server IP addresses. Up to eight SNTP servers can be defined.
- **Poll Interval —** Indicates whether or not the device polls the selected SNTP server for system time information.
- **Encryption Key ID —** Displays the encryption key identification used to communicate between the SNTP server and device. The field range is 1-4294967295.
- **Preference** — Indicates which SNTP server provides the SNTP system time. The possible field values are:
  - *Primary* — Indicates the primary server provides SNTP information.
  - *Secondary* — Indicates the backup server provides SNTP information.
  - Status — The operating SNTP server status. The possible field values are:
  - *Up* — Indicates the SNTP server is currently operating normally.
  - *Down* — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
  - *In progress* — Indicates the SNTP server is currently sending or receiving SNTP information.
  - *Unknown* — Indicates the progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.
- **Status** — Indicates the SNTP server status.
- **Last Response** — Displays the last time a response was received from the SNTP server.
- **Offset** — Indicates the time difference between the device local clock and the acquired time from the SNTP server.
- **Delay** — Indicates the amount of time it takes for a device request to reach the SNTP server.

2. Click Add . The *Add SNTP Servers Page* opens:

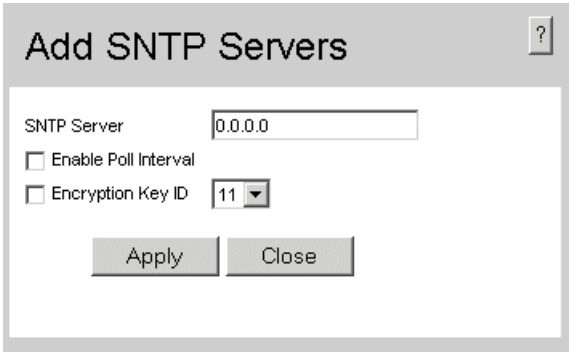



**Figure 164. Add SNTP Servers Page**

3. Define the relevant fields.
4. Click Apply . The SNTP Server is added, and the device is updated.

To edit the SNTP global parameters:

1. Click Edit . The *SNTP Server Settings Page* opens:

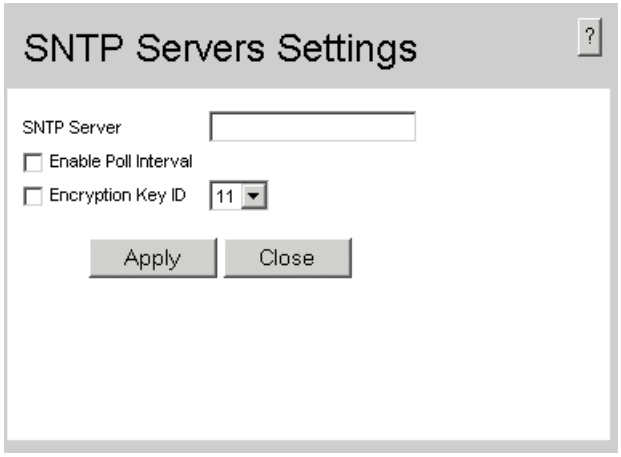



**Figure 165. SNTP Server Settings Page**

2. Define the relevant fields.
3. Click Apply . The SNTP Server is modified, and the device is updated.

# Defining SNTP Authentication

The *SNTP Authentication Page* provides parameters for defining the means by which the SNTP server is authenticated.

To define SNTP authentication:

1. Click **System > Time > SNTP Authentication**. The *SNTP Authentication Page* opens:

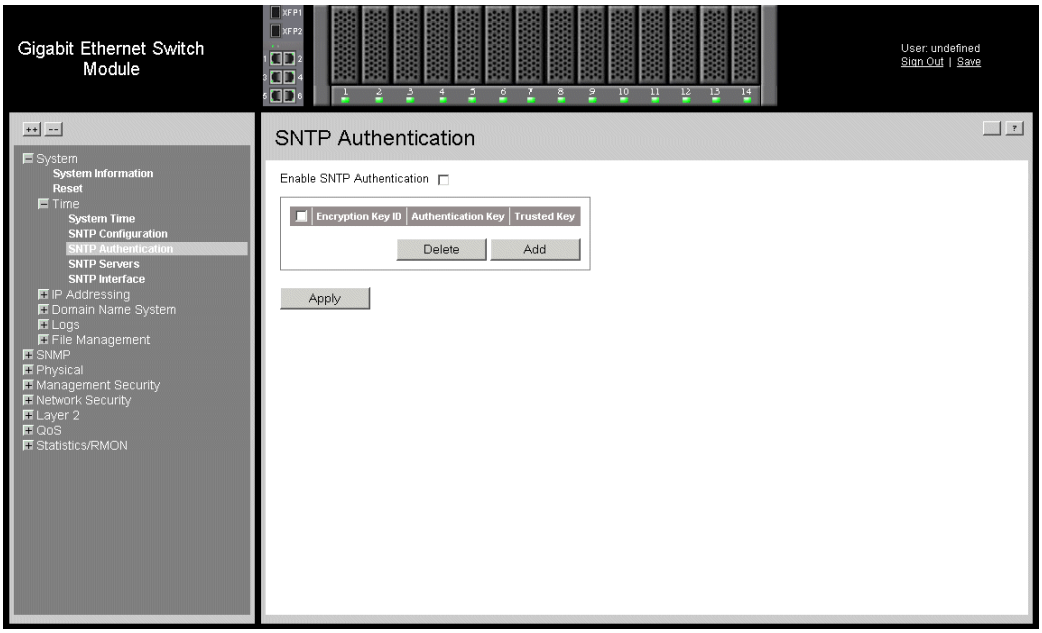



**Figure 166. SNTP Authentication Page**

The *SNTP Authentication Page* contains the following fields:

- **Enable SNTP Authentication** — Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:
  - — *Checked* — Authenticates SNTP sessions between the device and SNTP server.
  - — *Unchecked* — Disables authenticating SNTP sessions between the device and SNTP server.
- **Remove** — Removes Encryption Key IDs. The possible field values are:
  - — *Checked* — Removes the selected Encryption Key ID.
  - — *Unchecked* — Maintains the Encryption Key IDs. This is the default value.
- **Encryption Key ID** — Indicates if the encryption key identification is used to authenticate the SNTP server and device. The field value is up to 4294967295.
- **Authentication Key** — Indicates the key used for authentication.

- **Trusted Key —** Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.

2. To enable SNTP Authentication, select *Enable SNTP Authentication*
3. Click Apply. SNTP Authentication is defined, and the device is updated.

To define SNTP authentication parameters:

1. Click Add. The *Add SNTP Authentication* page opens:

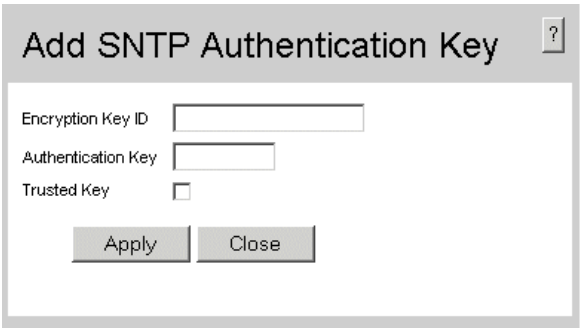



**Figure 167. Add SNTP Authentication**

2. Define the relevant fields.
3. Click Apply. The SNTP Authentication Key is added, and the device is updated.

# Adding an SNTP Interface

To add an SNTP interface:

1. Click **System > Time > SNTP Interface**. The *SNTP Authentication Page* opens:

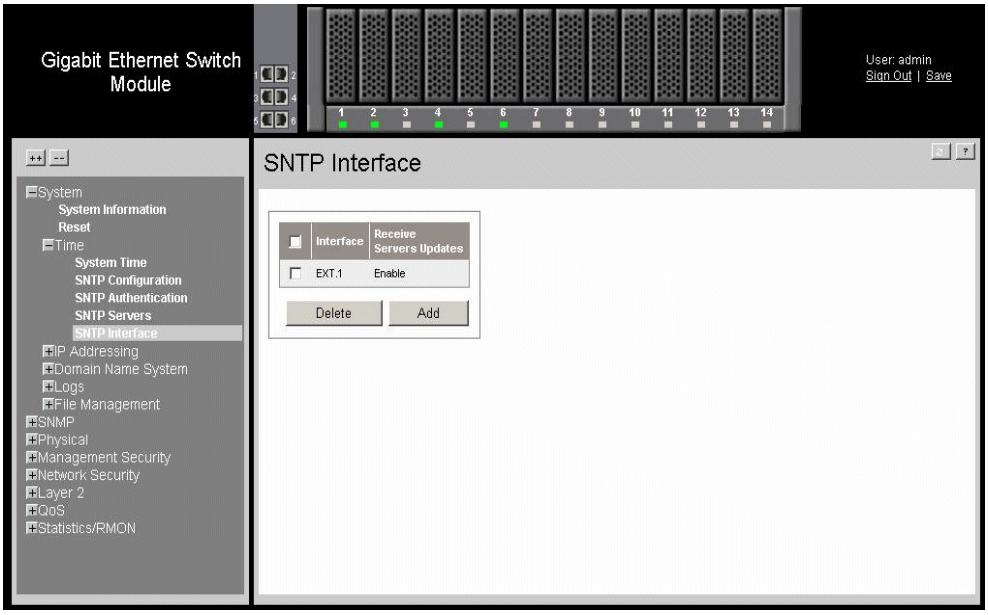



**Figure 168. SNTP Interface Page**

The *SNTP Interface Page* contains the following fields:

- **Interface** — Indicates the device for the SNTP interface.
- **Receive Server Updates** — Indicates receiving server updates for the device.

2. Click Add . The *Add SNTP Authentication* page opens:

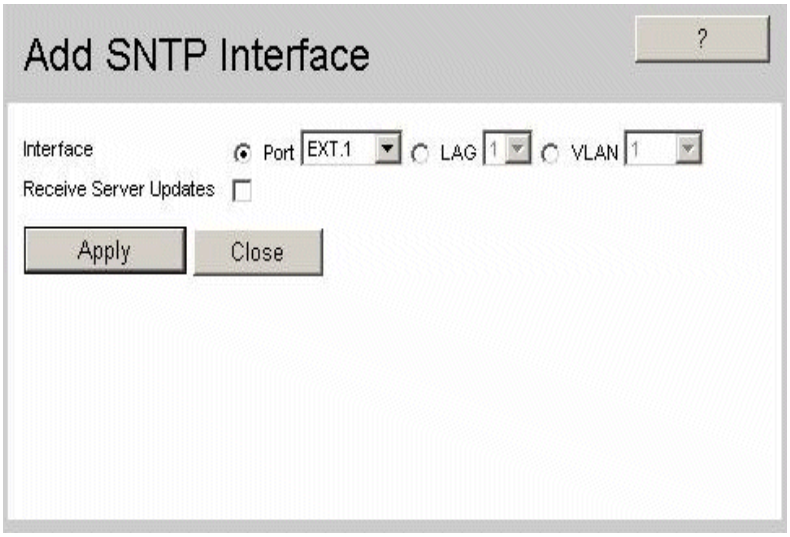



**Figure 169. Add SNTP Interface**

3. Define the relevant fields.
4. Click Apply. The SNTP interface is added, and the device is updated.

# 20 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 EAP 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.

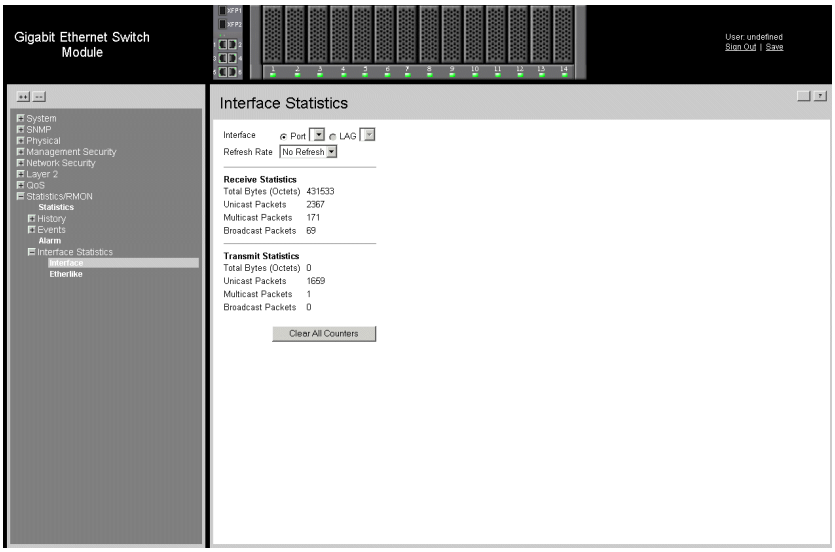



**Figure 170. Interface Statistics Page**

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.

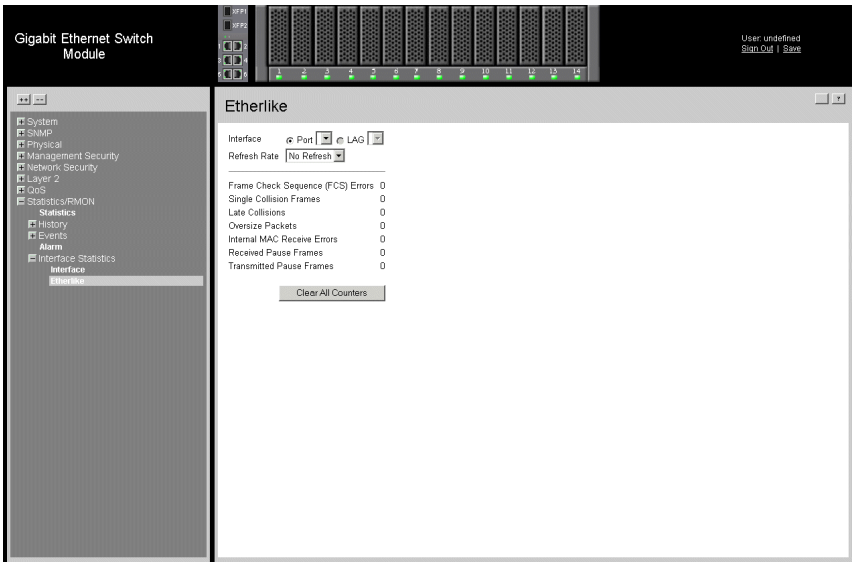



**Figure 171. Etherlike Statistics Page**

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 Paused 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 Clear All Counters . The Etherlike statistics counters are cleared.

# Viewing GVRP Statistics

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

To view GVRP statistics:

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

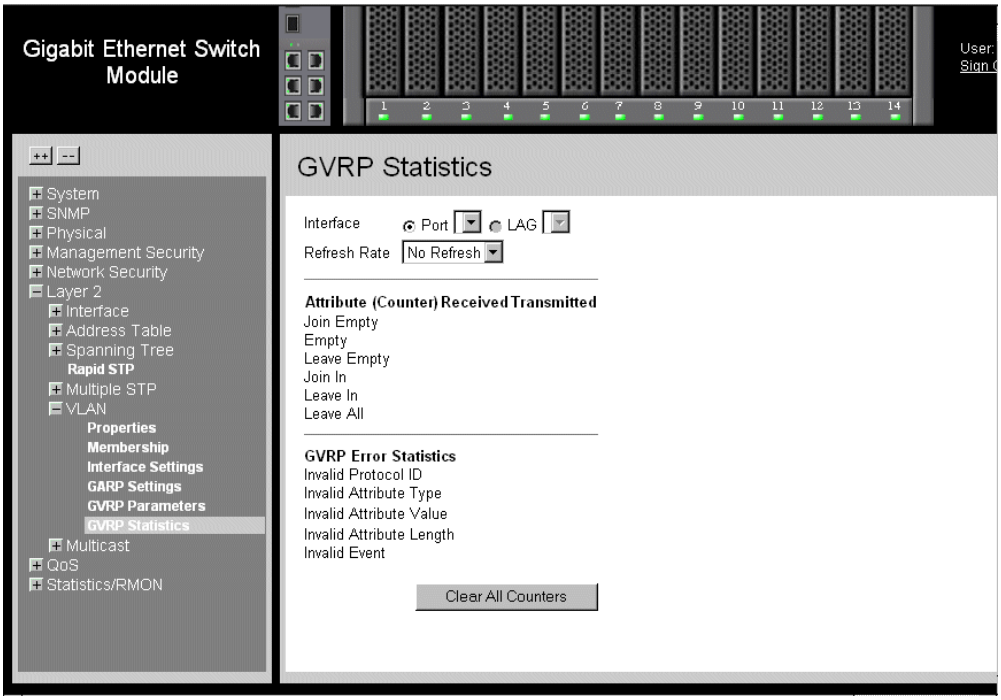



**Figure 172. GVRP Statistics Page**

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.

# Viewing EAP Statistics

The *EAP Statistics Page* contains information about EAP packets received on a specific port.

To view the EAP statistics:

1. Click **Network Security > 802.1x > EAP Statistics**. The *EAP Statistics Page* opens.

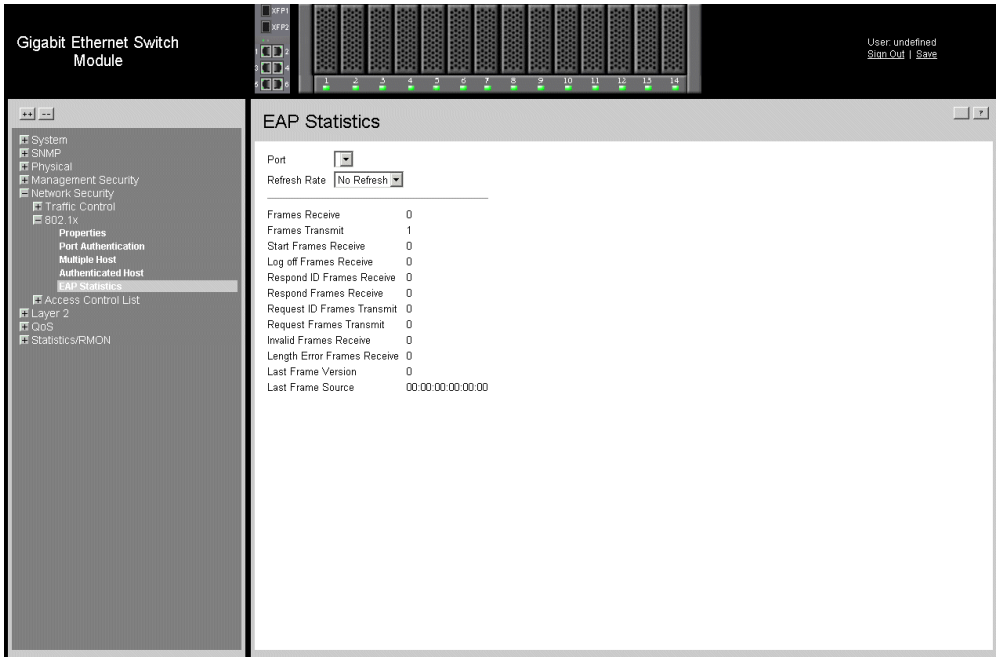



**Figure 173. EAP Statistics Page**

The *EAP Statistics Page* contains the following fields:

- **Port**—Indicates the port, which is polled for statistics.
- **Refresh Rate**—Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
  - *No Refresh* — Indicates that the EAP statistics are not refreshed.
  - *15 Sec*—Indicates that the EAP statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
- **Frames Receive** — Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** — Indicates the number of EAPOL frames transmitted via the port.

- **Start Frames Receive** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** — Indicates the number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Receive** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — Indicates the source MAC address attached to the most recently received EAPOL frame.

# 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.

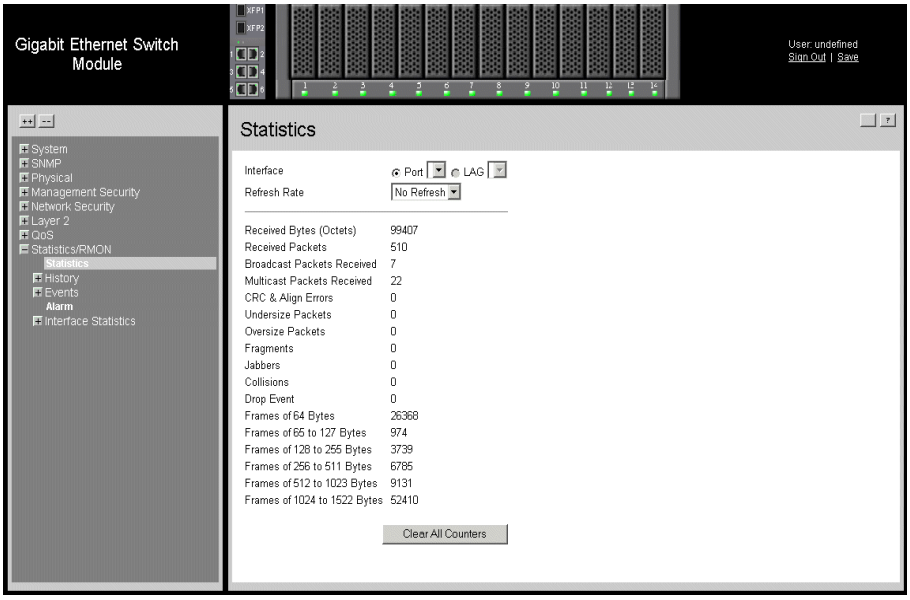



**Figure 174. RMON Statistics Page**

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 *xx* Bytes** — Number of *xx*-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 Clear All Counters . 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 samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

To view RMON history information:

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

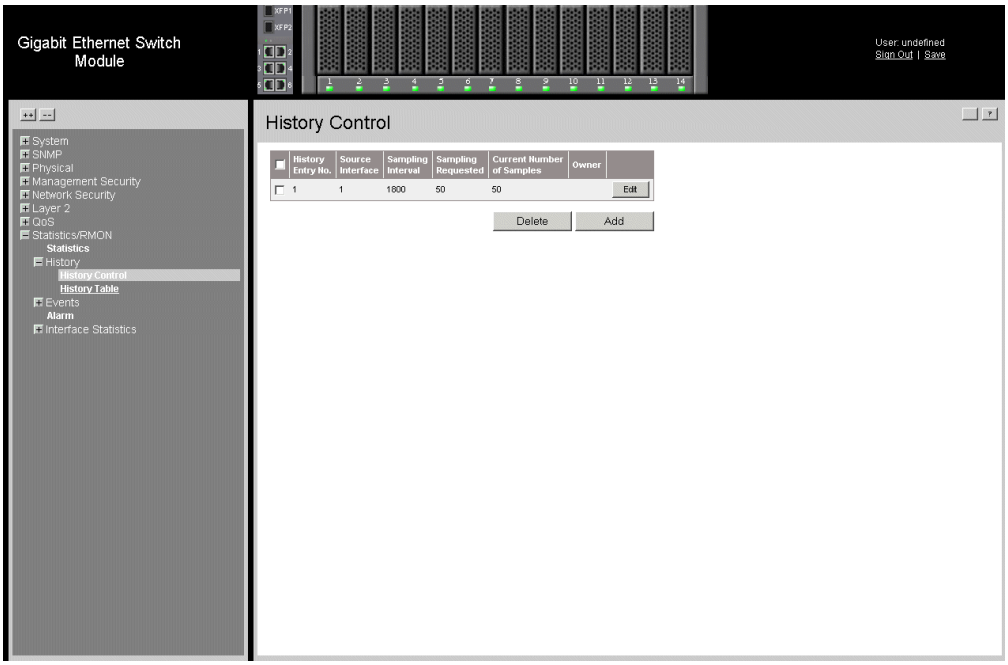



**Figure 175. RMON History Control Page**

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

- **Remove** — Removes History Control entries. The possible field values are:
  - *Checked* — Removes the selected History Control entry.
  - *Unchecked* — Maintains the current History Control entries.
- **History Entry No.** — Displays the entry number for the History Control Table page.
- **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).
- **Samples 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:

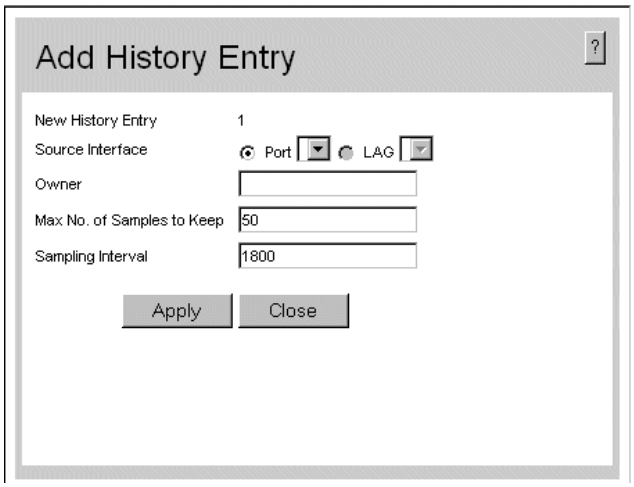



**Figure 176. Add History Entry Settings Page**

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:

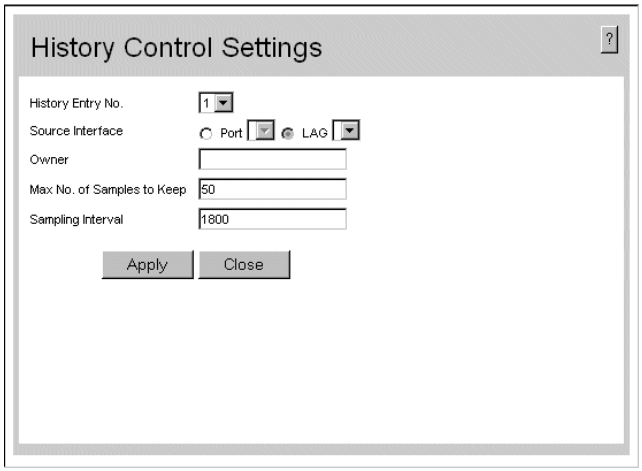



**Figure 177. RMON History Control Settings Page**

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.

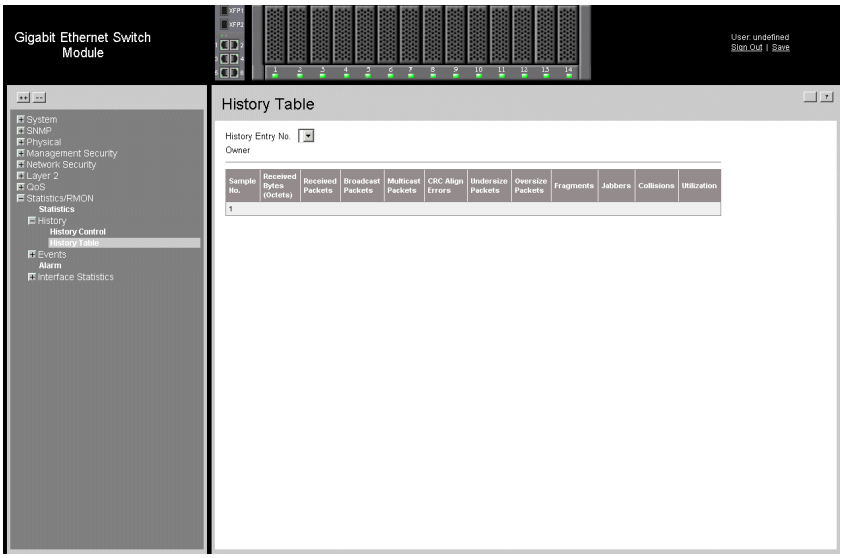



**Figure 178. RMON History Table Page**

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

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **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.

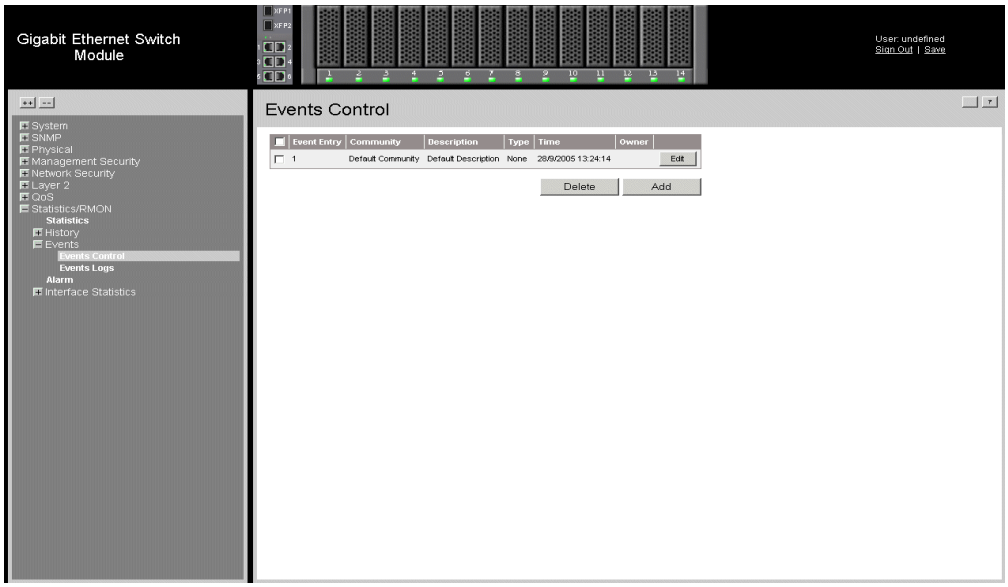



**Figure 179. RMON Events Control Page**

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

- **Remove** — Removes a RMON event. The possible field values are:
  - *Checked* — Removes 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.

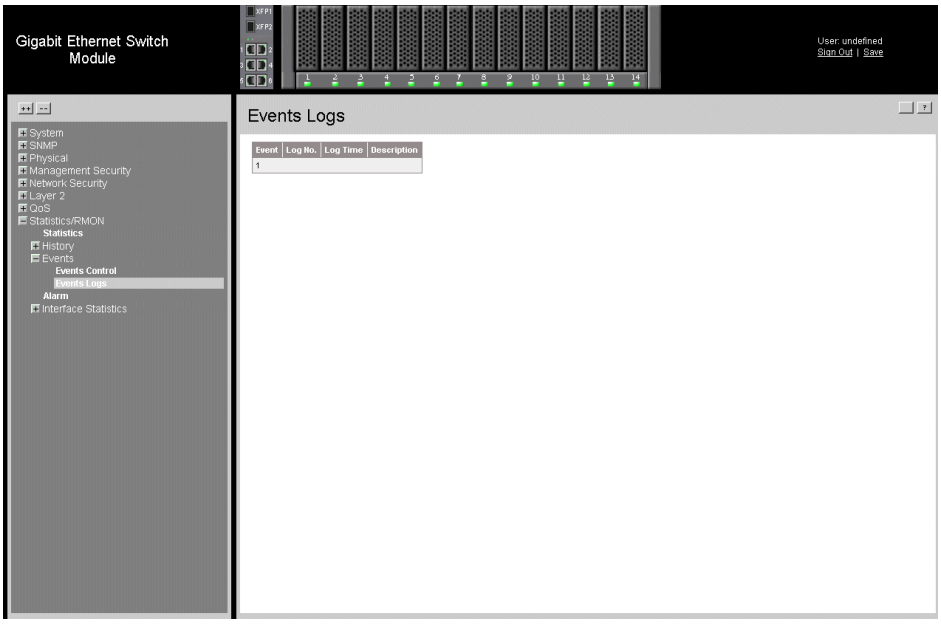



**Figure 180. RMON Events Logs Page**

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.

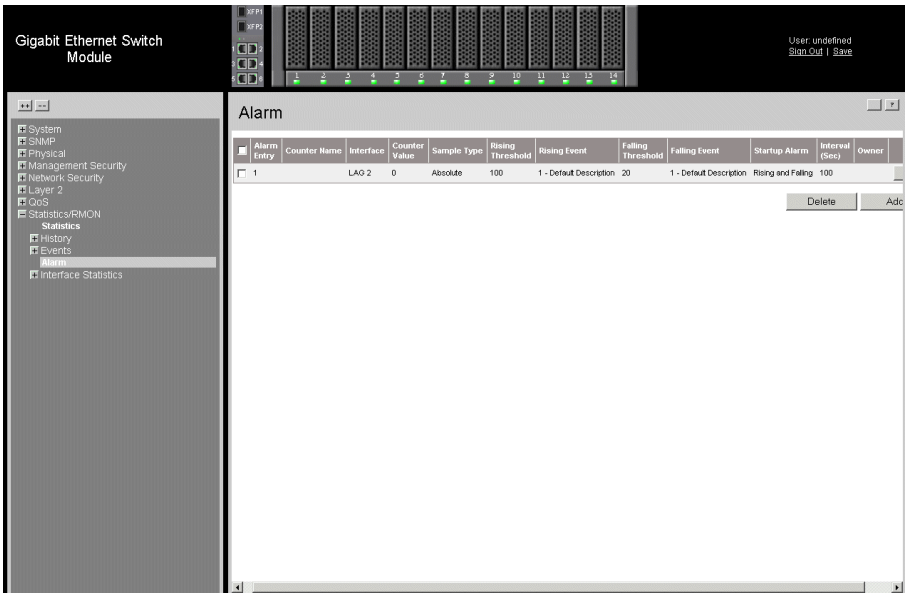



**Figure 181. RMON Alarm Page**

The *RMON Alarm Page* contains the following fields:

- **Remove** — Removes the RMON Alarms Table entry. The possible field values are:
  - *Checked* — Removes 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 mechanism in which the alarms are reported. The possible field values are:
  - — *LOG* — Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
  - — *TRAP* — Indicates that an SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
  - — *Both*— Indicates that both the Log and Trap mechanism are used to report alarms.
- **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 mechanism in which the alarms are reported.
- **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:

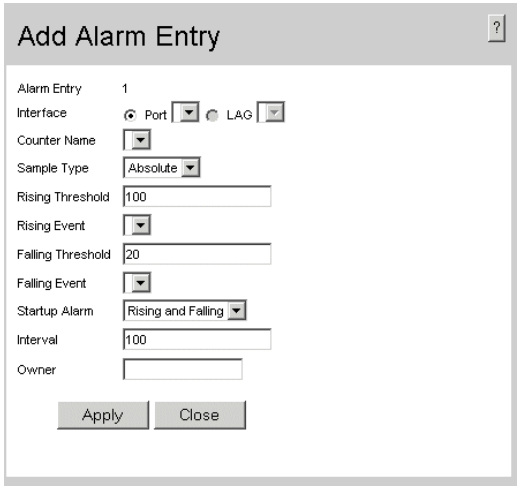



**Figure 182. Add Alarm Entry Page**

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:

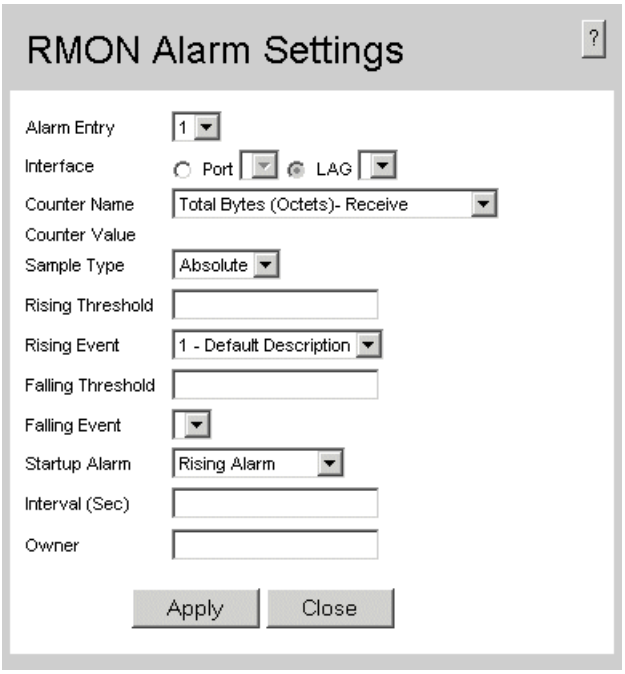



**Figure 183. RMON Alarms Definition Page**

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

# Appendix A: Getting Help

## World Wide Web

http://support.intel.com/support/motherboards/server/blade.htm.

## Telephone

All calls are billed US $25.00 per incident, levied in local currency at the applicable credit card exchange rate plus applicable taxes. (Intel reserves the right to change the pricing for telephone support at any time without notice).

Before calling, fill out an "Intel® Server Issue Report Form". A sample form is provided on the following pages. However, for the fastest service, please submit your form via the Internet.

For an updated support contact list, see http://www.intel.com/support/9089.htm/

### U.S. and Canada

1-800-404-2284

### Europe

**Belgium** ..... 02 714 3182

**Denmark** ... 38 487077

**Finland** ..... 9 693 79297

**France**..... 01 41 918529

**Germany** ... 069 9509 6099

**Holland**..... 020 487 4562

**Italy**..... 02 696 33276

**Norway** ..... 23 1620 50

**Spain**..... 91 377 8166

**Sweden**..... 08 445 1251

**UK**..... 870 6072439

## In Asia-Pacific Region

**Australia**.... 1800 649931

**Cambodia**.. 63 2 636 9797 (via Philippines)

**China** ..... 800 820 1100 (toll-free)

..... 8 621 33104691 (not toll-free)

**Hong Kong** 852 2 844 4456

**India**..... 0006517 2 68303634 (manual toll-free. You need an IDD-equipped telephone)

**Indonesia**... 803 65 7249

**Korea** ..... 822 767 2595

**Malaysia** .... 1 800 80 1390

**Myanmar**... 63 2 636 9796 (via Philippines)

**New Zealand** 0800 444 365

**Pakistan**..... 632 63684 15 (IDD via Philippines)

**Philippines** 1 800 1 651 0117

**Singapore** .. 65 6213-1311

**Taiwan** ..... 2 2545-1640

**Thailand**.... 1 800 631 0003

**Vietnam** ..... 632 6368416 (IDD via Philippines)

## Japan

**Domestic**.... 0120 868686

**Outside country** 81 298 47 0800

## Latin America

**Argentina** .. Contact AT&T USA at 0-800 222 1288. Once connected, dial 800 843 4481

**Brazil** ..... 001-916 377 0180

**Chile**

**Easter Island**. ..... Contact AT&T USA at 800 800 311. Once connected, dial 800 843 4481
**Mainland and Juan** .. Contact AT&T USA at 800 225 288. Once connected, dial 800 843 4481

**Colombia** ... Contact AT&T USA at 01 800 911 0010. Once connected, dial 800 843 4481

**Costa Rica** . Contact AT&T USA at 0 800 0 114 114. Once connected, dial 800 843 4481

**Ecuador**

**(Andimate)** .... Contact AT&T USA at 1 999 119. Once connected, dial 800 843 4481

**(Pacifictel)** ..... Contact AT&T USA at 1 800 225 528. Once connected, dial 800 843 4481

**Guatemala** . Contact AT&T USA at 99 99 190. Once connected, dial 800 843 4481

**Mexico** ..... Contact AT&T USA at 001 800 462 628 4240. Once connected, dial 800 843 4481

**Miami** ..... 1 800 621 8423

**Panama**..... Contact AT&T USA at 00 800 001 0109. Once connected, dial 800 843 4481

**Paraguay** ... 001 916 377 0114

**Peru** ..... 001 916 377 0114

**Uruguay**..... 001 916 377 0114

**Venezuela**... Contact AT&T USA at 0 800 2255 288. Once connected, dial 800 843 4481

# Appendix B: Troubleshooting

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

## Problems following Initial System Installation

Problems that occur at initial system startup are usually caused by an incorrect installation or configuration. Hardware failure is a less frequent cause.

### First Steps Checklist

- Is AC power available at the wall outlet?
- Are the power supplies plugged in? Check the AC cable(s) on the back of the chassis and at the AC source.
- Are all cables correctly connected and secured?
- Are the configuration settings made in Setup correct?
- Is the operating system properly loaded? See the operating system documentation.
- Is the system power cord properly connected to the system and plugged into a NEMA 5 15R outlet for 100-120V or a NEMA 6-15R outlet for 200-240V?

## Hardware Diagnostic Testing

This section provides a more detailed approach to identifying a hardware problem and locating its source.

***Caution:*** *Turn off devices before disconnecting cables: Before disconnecting any peripheral cables from the system, turn off the system and any external peripheral devices. Failure to do so can cause permanent damage to the system and/or the peripheral devices.*

1. Turn off the system and all external peripheral devices. Disconnect each device from the system, except for the keyboard and the video monitor.
2. Make sure the system power cord is plugged into a properly grounded AC outlet.
3. If the power LED does light.....

## Verifying Proper Operation of Key System Lights

As POST determines the system configuration, it tests for the presence of each mass storage device installed in the system. As each device is checked, its activity light should turn on briefly. Check for the following:

•

## Confirming Loading of the Operating System

Once the system boots up, the operating system prompt appears on the screen.

# Specific Problems and Corrective Actions

This section provides possible solutions for these specific problems:

- Power light does not light.
- No characters appear on screen.
- Characters on the screen appear distorted or incorrect.
- System cooling fans do not rotate.

Try the solutions below in the order given. If you cannot correct the problem, contact your service representative or authorized dealer for help.

## Power Light Does Not Light

Check the following:

- Did you press the power-on button?
- Is the system operating normally? If so, the power LED might be defective or the cable from the control panel to the server board might be loose.
- Have you securely plugged the server AC power cord into the power supply?

## No Characters Appear on Screen

Check the following:

- Is the keyboard functioning? Test it by turning the "Num Lock" function on and off to make sure the Num Lock light is functioning.
- Is the video monitor plugged in and turned on? If you are using a switch box, is it switched to the correct system?
- Are the brightness and contrast controls on the video monitor properly adjusted?
- Is the video monitor signal cable properly installed?

- Does this video monitor work correctly if plugged into a different system?

## Characters Are Distorted or Incorrect

Check the following:

- Are the brightness and contrast controls properly adjusted on the video monitor? See the manufacturer's documentation.
- Are the video monitor's signal and power cables properly installed?
- Does this video monitor work correctly if plugged into a different system?

## System Cooling Fans Do Not Rotate Properly

If the system cooling fans are not operating properly, it is an indication of possible system component failure.

Check the following:

- Is the power-on light lit?
- If your system has LED lights for the fans, is one or more of these LEDs lit?
- Are any other control panel LEDs lit?
- Have any of the fan motors stopped? Use the server management subsystem to check the fan status.
- Have your fans speeded up in response to an overheating situation?
- Have your fans speeded up in response to a fan that has failed?
- Are the power supply cables properly connected to the server board?
- Are there any shorted wires caused by pinched-cables or have power connector plugs been forced into power connector sockets the wrong way?

## Cannot Connect to a Server

- Make sure the network cable is securely attached to the correct connector at the system back panel.
- Try a different network cable.
- Make sure the hub port is configured for the same duplex mode as the network controller.
- Make sure the correct networking software is installed.
- If you are directly connecting two servers (without a hub), you will need a crossover cable.
- Check the network controller LEDs next to the NIC connectors.

# Problems with Network

## Diagnostics pass but the connection fails

- Make sure the network cable is securely attached.
- Make sure the cable is connected to the port from the onboard network controller.

# Problems with Application Software that Ran Correctly Earlier

Problems that occur after the system hardware and software have been running correctly sometimes indicate equipment failure. However, they can also be caused by file corruption or changes to the software configuration.

Check the following:

- If the problems are intermittent, there may be a loose cable, dirt in the keyboard (if keyboard input is incorrect), a marginal power supply, or other random component failures.
- If you suspect that a transient voltage spike, power outage, or brownout might have occurred, reload the software and try running it again. Symptoms of voltage spikes include a flickering video display, unexpected system reboots, and the system not responding to user commands.

***Note:*** *Random errors in data files: If you are getting random errors in your data files, they may be getting corrupted by voltage spikes on your power line. If you are experiencing any of the above symptoms that might indicate voltage spikes on the power line, you may want to install a surge suppressor between the power outlet and the system power cord.*

# Appendix C: Regulatory and Compliance Information

## Product Regulatory Compliance

### Product Safety Compliance

This product complies with the following safety requirements:

- UL60950-1 / CSA 60950-1 (USA / Canada)
- EN60950-1 (Europe)
- CB Certificate & Report, IEC60950-1 (report to include all country national deviations)
- CE - Low Voltage Directive 73/23/EEE (Europe)
- GOST Approval (Russia)

### Product EMC Compliance - Class A Compliance

***Note:*** *Legally this product is required to comply with Class A emission requirements because it is intended for a commercial type market place. Intel targets 10db margin to Class A Limits.*

This product has been tested and verified to comply with the following electromagnetic compatibility (EMC) regulations when installed in a compatible Intel® host system. For information on compatible host system(s), see Intel's Server Builder Web site or contact your local Intel representative.

- FCC /ICES-003 - Emissions (USA/Canada) Verification
- CISPR 22 - Emissions (International)
- EN55022 - Emissions (Europe)
- EN55024 - Immunity (Europe)
- CE - EMC Directive 89/336/EEC (Europe)
- VCCI Emissions (Japan)
- AS/NZS Emissions (Australia / New Zealand)
- GOST Approval (Russia)
- RRL MIC Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)

# Certifications / Registrations / Declarations

- UL/cUL Listed Accessory (US/Canada)
- CE Declaration of Conformity (CENELEC Europe)
- C-Tick Declaration of Conformity (Australia/New Zealand)
- VCCI Registration (Japan)
- GOST Certification (Russia)
- RRL Certification (Korea)

# Product Regulatory Compliance Markings

This product is marked with the following Product Certification Markings:

**Table 4. Product Certification Markings**

| Regulatory Compliance | Region | Marking |
|---|---|---|
| cULus Listings Marks | USA/Canada |  |
| CE Mark | Europe |  |
| FCC Marking (Class A) | USA | This device complies with Part 15 of the FCC Rules.<br>Operation of this device is subject ot the following two conditions:<br>(1) This device may not cause harmful interference, and ;<br>(2) This device must accept any interference received, including interference that may cause undesired operation. |
| EMC Marking (Class A) | Canada | CANADA ICES-003 CLASS A<br>CANADA NMB-003 CLASSE A |
| VCCI Marking (Class A) | Japan | この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。<br>取扱説明書に従って正しい取り扱いをして下さい。 |
| C-Tick Marking | Australia / New Zealand |  |

**Table 4. Product Certification Markings**

| Regulatory Compliance | Region | Marking |
|---|---|---|
| RRL MIC Mark | Korea |  |

# Electromagnetic Compatibility Notices

## FCC (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions related to the EMC performance of this product, contact:

```
Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, OR 97124-6497
1-800-628-8686
```

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Only peripherals (computer input/output devices, terminals, printers, etc.) that comply with FCC Class A or B limits may be attached to this computer product. Operation with noncompliant peripherals is likely to result in interference to radio and TV reception.

All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals, that are not shielded and grounded may result in interference to radio and TV reception.

## ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Apparelis Numériques", NMB-003 édictee par le Ministre Canadian des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

## Europe (CE Declaration of Conformity)

This product has been tested in accordance too, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

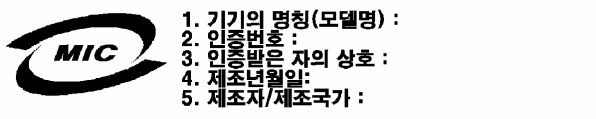
## VCCI (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

English translation of the notice above:

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) from Information Technology Equipment. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

## RRL (Korea)




English translation of the notice above:

1. Type of Equipment (Model Name): On License and Product
2. Certification No.: On RRL certificate. Obtain certificate from local Intel representative
3. Name of Certification Recipient: Intel Corporation
4. Date of Manufacturer: Refer to date code on product
5. Manufacturer/Nation: Intel Corporation/Refer to country of origin marked on product

# Restriction of Hazardous Substances (RoHS) Compliance

Intel has a system in place to restrict the use of banned substances in accordance with the European Directive 2002/95/EC. Compliance is based on declaration that materials banned in the RoHS Directive are either (1) below all applicable threshold limits or (2) an approved / pending RoHS exemption applies.

RoHS implementing details are not fully defined and may change.

Threshold limits and banned substances are noted below:

- Quantity limit of 0.1% by mass (1000 PPM) for:
  - Lead
  - Mercury
  - Hexavalent Chromium
  - Polybrominated Biphenyls Diphenyl Ethers (PBDE)
- Quantity limit of 0.01% by mass (100 PPM) for:
  - Cadmium

# End-of-Life / Product Recycling

Product recycling and end-of-life take-back systems and requirements vary by country. Contact the retailer or distributor of this product for information about product recycling and / or take-back.

# Appendix D: Intel® Server Issue Report Form

***Note:*** *An on-line / automatic submission version of this form is available at http:// support.intel.com/support/. For the fastest service, please submit your form via the Internet.*

Date Submitted: _____

Company Name: _____

Contact Name: _____

Email Address: _____

Intel Server Product: _____

Priority (Critical, Hot, High, Low): _____

Brief Problem Description. Provide a brief description below. See the last page for space to include a detailed problem description.

_____

_____

_____

_____

_____

## Board / Chassis Information

Baseboard Revision - PBA#: _____

Baseboard Serial Number: _____

Chassis Model: _____

CPU1 Speed/Stepping/Spec: _____

CPU2 Speed/Stepping/Spec: _____

System BIOS Version: _____

HSC Firmware Version: _____

## DIMM Configuration

DIMM1A MB and Vendor / part number: _____

DIMM1B MB and Vendor / part number: _____

DIMM2A MB and Vendor / part number: _____

DIMM2B MB and Vendor / part number: _____

DIMM3A MB and Vendor / part number: _____

DIMM3B MB and Vendor / part number: _____

DIMM4A MB and Vendor / part number: _____

DIMM4B MB and Vendor / part number: _____

## Operating System Information

Operating System:_____

Version: _____

Service Pack:_____

## Add-in Card, Peripheral, Video, NIC

Check each box below as applicable, and provide the requested information.

Peripheral Card or Peripheral Description Driver Revision IRQ # I/O Base Address NIC

| Peripheral | Description | Driver Revision | IRQ | I/O Base Address | FW Revision |
|---|---|---|---|---|---|
| **Low-profile Riser** | | | | | |
| PCI Slot 1 | | | | | |
| PCI Slot 2 | | | | | |
| PCI Slot 3 | | | | | |
| **Full-height Riser** | | | | | |
| PCI Slot 1 | | | | | |
| PCI Slot 2 | | | | | |
| PCI Slot 3 | | | | | |
| **Video** | | | | | |
| On-board Video | | | | | |

| Peripheral | Description | Driver Revision | IRQ | I/O Base Address | FW Revision |
|---|---|---|---|---|---|
| Add-in Video | | | | | |
| **NIC** | | | | | |
| On-Board NIC1 | | | | | |
| On-Board NIC2 | | | | | |

## Hard Drive Information

| Drive Type (SCSI, SATA, etc) | Make/Model | Hot-swap or Fixed | IRQ | FW Revision |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Management Information

On-Board Platform Instrumentation only _____

Intel® Server Management - Professional Edition_____

Intel® Server Management - Advanced Edition _____

## Control Panel Information

Standard Control Panel _____

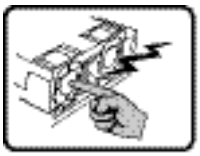
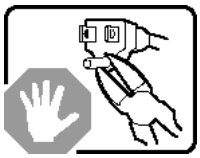
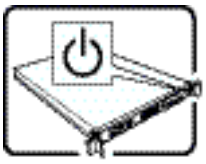
Intel® Local Control Panel_____

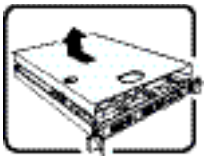
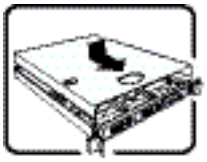
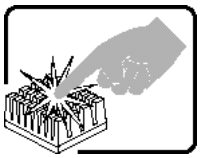
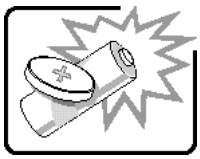
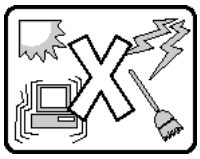
## Complete Problem Description

In the space below, provide a complete description of the steps used to reproduce the problem or a complete description of where the problem can be found. Please also include any details on troubleshooting already done.

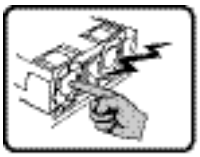
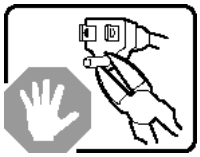
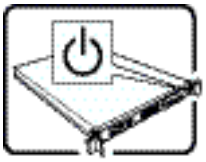
# Appendix E: Installation/Assembly Safety Instructions

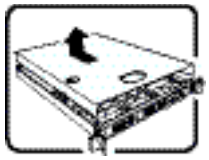
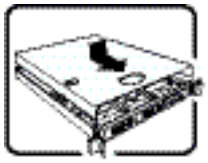
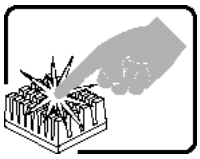
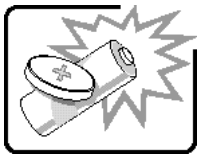
## English

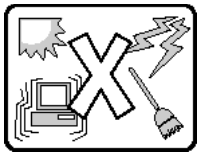
| | |
|---|---|
|  | The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified personnel. |
|  | Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate 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.<br>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:<br>1. Turn off all peripheral devices connected to the system.<br>2. Turn off the system by pressing the power button.<br>3. Unplug all AC power cords from the system or from wall outlets.<br>4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.<br>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.<br>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:<br>1. Unlock and remove the padlock from the back of the system if a padlock has been installed.<br>2. Remove and save all screws from the covers.<br>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:<br>1. Check first to make sure you have not left loose tools or parts inside the system.<br>2. Check that cables, add-in boards, and other components are properly installed.<br>3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly.<br>4. Insert and lock the padlock to the system to prevent unauthorized access inside the system.<br>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:<br>• Clean and free of airborne particles (other than normal room dust).<br>• Well ventilated and away from sources of heat including direct sunlight.<br>• Away from sources of vibration or physical shock.<br>• Isolated from strong electromagnetic fields produced by electrical devices.<br>• 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.<br>• Provided with a properly grounded wall outlet.<br>• Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect. |

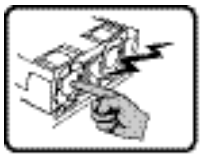
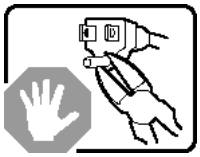
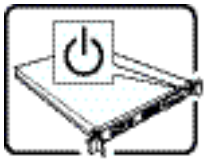
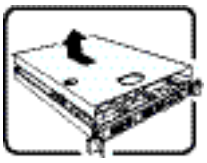
# Deutsch

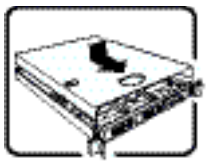
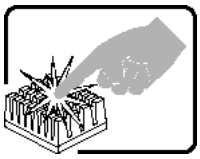
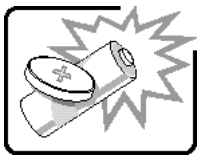
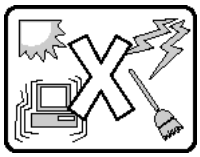
| | |
|---|---|
|  | Benutzer können am Netzgerät dieses Produkts keine Reparaturen vornehmen. Das Produkt enthält möglicherweise mehrere Netzgeräte. Wartungsarbeiten müssen von qualifizierten Technikern ausgeführt werden. |
|  | Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, 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. |
|  | SICHERHEISMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten:<br>1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.<br>2. Schalten Sie das System mit dem Hauptschalter aus.<br>3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.<br>4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab.<br>5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden.<br>6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein. |

| | |
|---|---|
|  | SICHERHEISMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten:<br>1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.<br>2. Schalten Sie das System mit dem Hauptschalter aus.<br>3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.<br>4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab.<br>5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden.<br>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:<br>1. Vergewissern Sie sich, daß Sie keine Werkzeuge oder Teile im Innern des Systems zurückgelassen haben.<br>2. Überprüfen Sie alle Kabel, Zusatzkarten und andere Komponenten auf ordnungsgemäßen Sitz und Installation.<br>3. Bringen Sie die Abdeckungen wieder am Gehäuse an, indem Sie die zuvor gelösten Schrauben wieder anbringen. Ziehen Sie diese gut an.<br>4. Bringen Sie die Verschlußeinrichtung (Padlock) wieder an und schließen Sie diese, um ein unerlaubtes Öffnen des Systems zu verhindern.<br>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. |

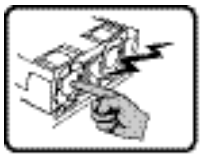
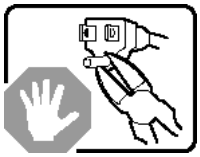
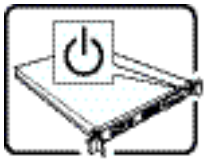
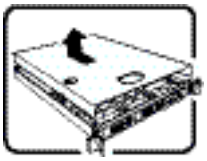
| | |
|---|---|
|  | Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der Standort sollte:<br>• "sauber und staubfrei sein (Hausstaub ausgenommen);<br>• "gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);<br>• "keinen Erschütterungen ausgesetzt sein;<br>• "keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;<br>• "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;<br>• "mit einer geerdeten Wechselstromsteckdose ausgerüstet sein;<br>• "über ausreichend Platz verfügen, um Zugang zu den Netzkabeln zu gewährleisten, da der Stromanschluß des Produkts hauptsächlich über die Kabel unterbrochen wird |

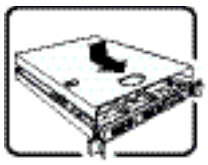
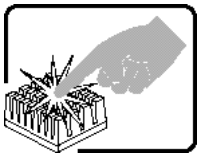
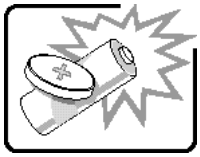
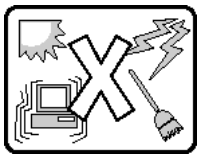
# Français

| | |
|---|---|
|  | 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:<br>1. Mettez hors tension tous les périphériques connectés au système.<br>2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).<br>3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.<br>4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système.<br>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).<br>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:<br>1. Si un cadenas a été installé sur à l'arrière du système, déverrouillez-le et retirez-le.<br>2. Retirez toutes les vis des panneaux et mettez-les dans un endroit sûr.<br>3. Retirez les panneaux. |

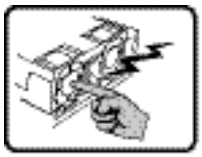
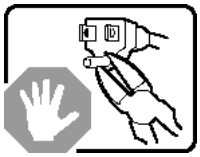
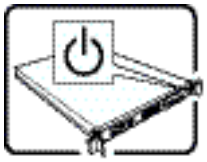
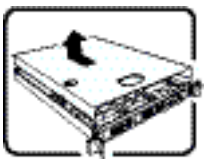
| | |
|---|---|
|  | Afin de permettre le refroidissement et l'aération du système, réinstallez toujours les panneaux du boîtier avant de mettre le système sous tension. Le fonctionnement du système en l'absence des panneaux risque d'endommager ses pièces. Pour installer les panneaux, procédez comme suit:<br>1. Assurez-vous de ne pas avoir oublié d'outils ou de pièces démontées dans le système.<br>2. Assurez-vous que les câbles, les cartes d'extension et les autres composants sont bien installés.<br>3. Revissez solidement les panneaux du boîtier avec les vis retirées plus tôt.<br>4. Remettez le cadenas en place et verrouillez-le afin de prévenir tout accès non autorisé à l'intérieur du système.<br>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:<br>• "Propre et dépourvu de poussière en suspension (sauf la poussière normale).<br>• "Bien aéré et loin des sources de chaleur, y compris du soleil direct.<br>• "A l'abri des chocs et des sources de vibrations.<br>• "Isolé de forts champs électromagnétiques géenérés par des appareils électriques.<br>• "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.<br>• "Muni d'une prise murale correctement mise à la terre.<br>• "Suffisamment spacieux pour vous permettre d'accéder aux câbles d'alimentation (ceux-ci étant le seul moyen de mettre le système hors tension). |

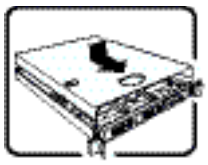
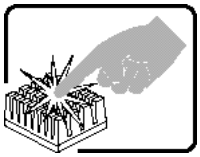
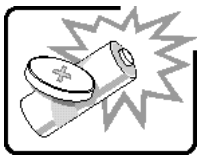
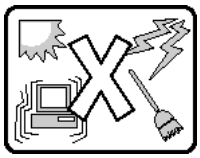
# Español

| | |
|---|---|
|  | 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.<br>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:<br>1. Apague todos los dispositivos periféricos conectados al sistema.<br>2. Apague el sistema presionando el interruptor encendido/ apagado.<br>3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna.<br>4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema.<br>5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujetada a la toma de tierra del chasis - o a cualquier tipo de superficie de metal sin pintar.<br>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:<br>1. Desbloquee y extraiga el bloqueo de seguridad de la parte posterior del sistema, si se ha instalado uno.<br>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:<br>1. Asegúrese primero de no haber dejado herramientas o componentes sueltos dentro del sistema.<br>2. Compruebe que los cables, las placas adicionales y otros componentes se hayan instalado correctamente.<br>3. Incorpore las tapas al chasis mediante los tornillos extraídos anteriormente, tensándolos firmemente.<br>4. Inserte el bloqueo de seguridad en el sistema y bloquéelo para impedir que pueda accederse al mismo sin autorización.<br>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:<br>• "Limpio y libre de partículas en suspensión (salvo el polvo normal).<br>• "Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.<br>• "Alejado de fuentes de vibración.<br>• "Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.<br>• "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.<br>• "Provisto de una toma de tierra correctamente instalada.<br>• "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:<br>1. Spegnere tutti i dispositivi periferici collegati al sistema.<br>2. Spegnere il sistema, usando il pulsante spento/acceso dell'interruttore del sistema.<br>3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche.<br>4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema.<br>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 - .<br>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 seque:<br>1. Aprire e rimuovere il lucchetto dal retro del sistema qualora ve ne fosse uno installato.<br>2. Togliere e mettere in un posto sicuro tutte le viti delle coperture.<br>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:<br>1. Controllare prima che non si siano lasciati degli attrezzi o dei componenti dentro il sistema.<br>2. Controllare che i cavi, dei supporti aggiuntivi ed altri componenti siano stati installati appropriatamente.<br>3. Attaccare le coperture al telaio con le viti tolte in precedenza e avvitarle strettamente.<br>4. Inserire e chiudere a chiave il lucchetto sul retro del sistema per impedire l'accesso non autorizzato al sistema.<br>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:<br>• "Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).<br>• "Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.<br>• "Al riparo da urti e lontana da fonti di vibrazione.<br>• "Isolata dai forti campi magnetici prodotti da dispositivi elettrici.<br>• "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.<br>• "Dotata di una presa a muro correttamente installata.<br>• "Dotata di spazio sufficiente ad accedere ai cavi di alimentazione, i quali rappresentano il mezzo principale di scollegamento del sistema. |

# Appendix F: Safety Information

## English

### Server Safety Information

This document applies to Intel® server boards, Intel® server chassis (pedestal and rack-mount) 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 leichteren Verletzungen bzw. Sachbeschädigungen führen kann. |
| WARNUNG | Weist auf eine Gefahrenquelle hin, die bei Nichtbeachtung der WARNUNG zu ernsten 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 eine 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 Sei 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 leitfahige Schaumstoffunterlage, aber niche 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'eléctrocution.*

*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 tapi de mousse conducteru, 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 todos 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 están desenchufados. Asegúrese de que los cables de alimentación de CA estén desenchufado antes de abrir le 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.*

# 体中文

# 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
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。

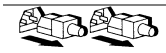
如果本文档中的信息与特定产品的随附信息或 Web
站点信息之间存在不一致，请以产品文档为准。

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
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
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。

# 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 |
| **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 |

# 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 IT
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
性尚有待进一步的评估。

# 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
  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。

# 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。

# 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
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
不止使用一根交流电线。请确保所有的交流电线都已拔下。打开机箱或增加或去
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
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
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
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、信系统、网络和调制解调器。

## 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。

# 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，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。
- 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，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
下风机防护装置运行系统。

## 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
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，
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
。

## 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
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
主板组件侧面朝上放置在无静电的接地表面上。请使用导电泡沫垫（若有），不
使用主板包装。请勿将主板在任何表面上滑动。

# 他危险

## 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。

## 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。

## 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