GS900M Series

Gigabit Ethernet Switches

Management Software
Web Browser User's Guide

613-002051 Rev. A

This product includes software licensed under the Berkeley Software Distribution (BSD) License. As such, the following language applies for those portions of the software licensed under the BSD License:

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

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* 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.
* Neither the name of Allied Telesis, Inc. nor the names of the respective companies above 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 HOLDER 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.

Allied Telesis, Inc., hereby disclaims all copyright interest of the following products:

* Portmap: this product includes Portmap 5beta developed by the University of California, Berkeley and its contributors.
* OpenSSL: this product includes OpenSSL 0.9.8d developed by the OpenSSL Project for use in the OpenSSL Toolkit.
* Mathopd: this product includes Mathopd 1.6 copyright (c) 1996 - 2005 by Michiel Boland
* zlib: this product includes zlib version 1.2.3 copyright (c) 1995 - 2005 by Jean-loup Gailly and Mark Adler

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request

Allied Telesis, Inc.

3041 Orchard Parkway

San Jose, California 95134

Contents

Figures

Tables

Preface

This guide explains how to use the web browser management interface in the Allied Telesis GS900M Series of Gigabit Ethernet switches to configure the features and view statistics. The preface contains the following sections:

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support page on the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis technical experts.
- USA and EMEA phone support — Select the phone number that best fits your location and customer type.
- Hardware warranty information — Learn about Allied Telesis warranties and register your product online.
- Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.

Chapter 1
Introduction

This chapter contains introductory information about the web browser management interface on the switch and basic instructions on how to use the interface to configure the parameter settings of the features. The chapter contains the following sections:

Introduction

This manual describes the web browser management interface for the GS900M Series of Gigabit Ethernet Switches. The instructions explain how to use the web browser windows to configure the parameter settings and features of the devices, as well as view status information and statistics.

Switch Models

The manual applies to the following models of the GS900M Series of Gigabit Ethernet Switches:

- AT-GS908M
- AT-GS916M
- AT-GS924M

Management Interfaces

The switches have three management interfaces: The interfaces are described in Table 1.

Table 1. Management Interfaces

Management Interface	Description
Command line	This management interface consists of a series of commands. The interface is available locally through the Console port on the switch as well as remotely with a Telnet client on a management workstation. You may use the commands to manage and configure all of the features and parameters on the switch.
Web Browser	This management interface consists of web browser windows and is used remotely with web browsers from management workstations on your network. You may use this interface to manage nearly all of the features and parameters of the switch. The few exceptions are listed in “Differences Between the Management Interfaces” on page 27. This interface is not available through the Console port.

Table 1. Management Interfaces (Continued)

Management Interface	Description
SNMPv1 and v2c	This management interface consists of management information base (MIB) objects, which represent the parameters and settings of the features on the switch. This form of management requires a Simple Network Management Protocol (SNMP) application. The interface is available from remote management workstations that have SNMP applications. It is not available through the Console port. The switches support the following MIBs: SNMP MIB-II (RFC 1213) Ethernet MIB (RFC 3635) Extended Interface MIB (RFC 2863) Bridge MIB (RFC 1493) Dot1q MIB (RFC 2674) Allied Telesis managed switch MIBs

Main Software Features

Here are the main software features of the switches:

- Port mirroring
- Static port trunks
- Port-based and tagged VLANs
- Protected ports VLANs
- Class of Service
- Quality of Service Policies
- Rapid Spanning Tree Protocol (STP compatible)
- Multiple Spanning Tree Protocol (STP compatible)
- Loop Detection Frame
- IGMP v3 Snooping
- MLD v2 Snooping
- DHCP Snooping
- Broadcast, multicast, and unknown unicast packet filters
- Traffic rate thresholds with actions
- Ethernet Protected Switched Ring (transit node only)
- RADIUS client with accounting
- Port authentication with 802.1x, MAC address, or web browser
- MAC address-based port security
- Trigger actions for automated tasks
- Event log
- Syslog server
- SNTP client
- Statistics
- Telnet server
- HTTP server
- Management access filter
- Command line management interface
- Web browser management interface
- SNMPv1 and v2c
- BPDU/EAP forwarding

Differences Between the Management Interfaces

There are several differences between the command line and web browser interfaces. The differences are listed in Table 2.

Table 2. Differences in the Management Interfaces

Feature	Difference
DCHP client	The switch has a DHCP client. You may use it to assign the device an IP address configuration from a DHCP server on your network. You have to use the command line interface to enable or disable the client. You may use the web browser interface to assign a static IP address to the switch, but you cannot use it to control the DHCP client.
Ping utility	The switch has a PING utility. You may use it to test for active paths between the switch and other devices. The utility is only available from the command line interface. It is not supported from the web browser interface.
PURGE commands	The command line interface has a series of PURGE commands for returning the parameter settings of many of the individual features to their default settings. The web browser interface does not have a similar function.
Resetting Flash Memory	The command line interface has the CLEAR FLASH TOTAL command, which you may use to delete all of the files in flash memory. You may use the web browser interface to delete individual files in flash memory, but you cannot delete all of the files at one time.

Elements of the Web Browser Windows

Figure 1 is an example of a web browser window of the management interface. The interface displays this window first when you start a management session.

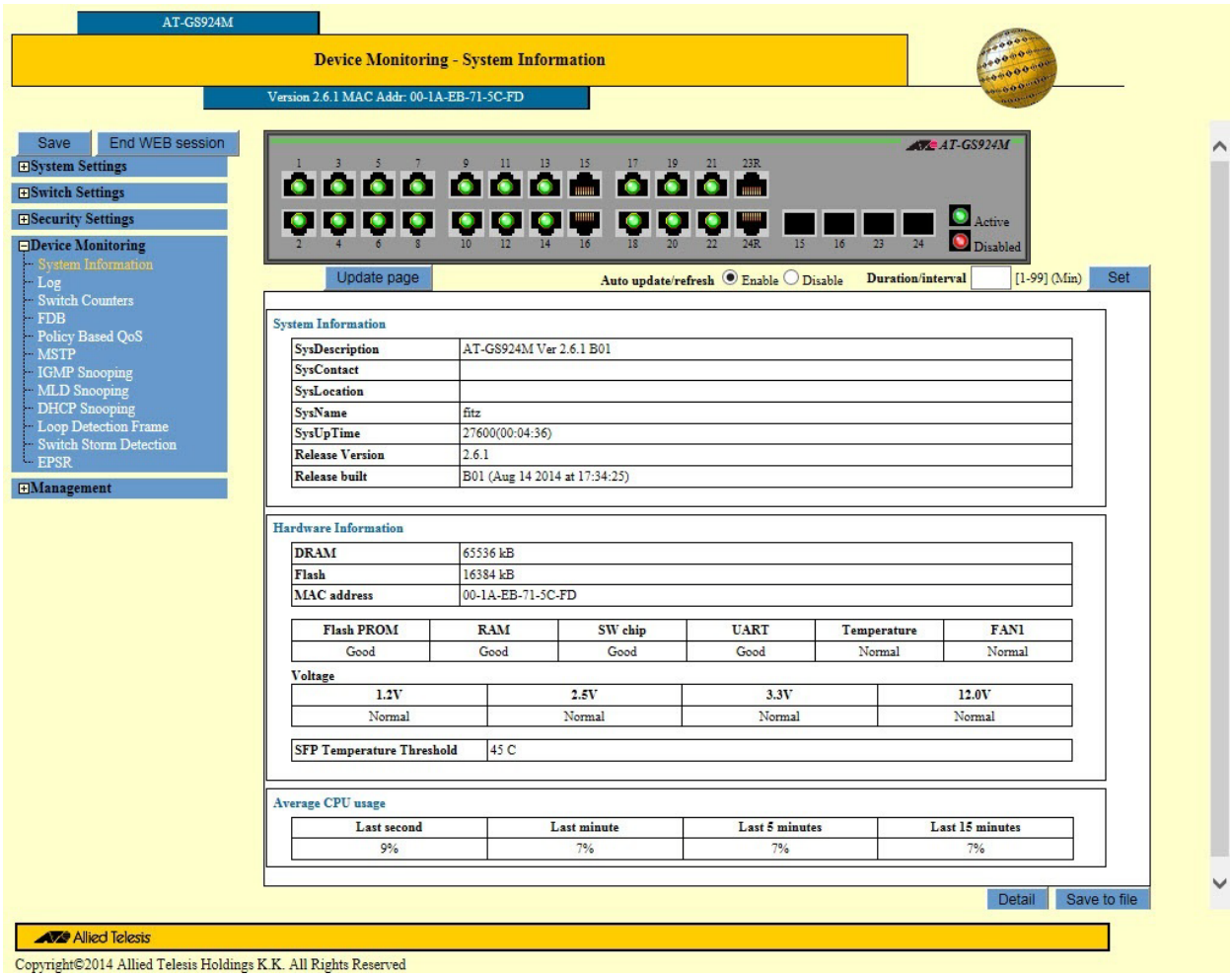

Figure 1. Example of a Web Browser Management Window

At the top of every window is a banner. The components of a banner are identified in Figure 2 on page 29.

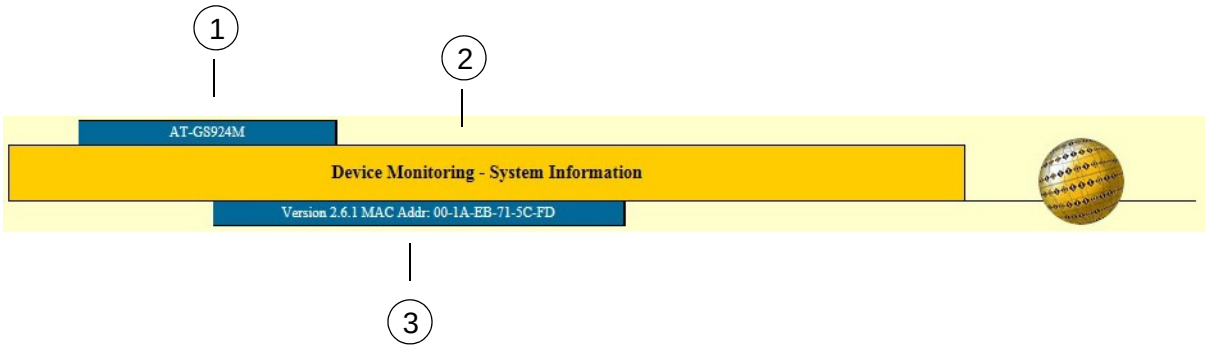

Figure 2. Window Banner

Table 3 defines the banner components.

Table 3. Window Banner

Section	Description
1	Displays the model name of the switch you are currently managing.
2	Displays the window name. The first part of the name is the name of the submenu from where the window is accessed.
3	Displays the version number of the management software and the MAC address of the switch.

The web browser interface has a main menu in the upper left corner of the browser windows. The elements of the main menu are shown in Figure 3 on page 30.

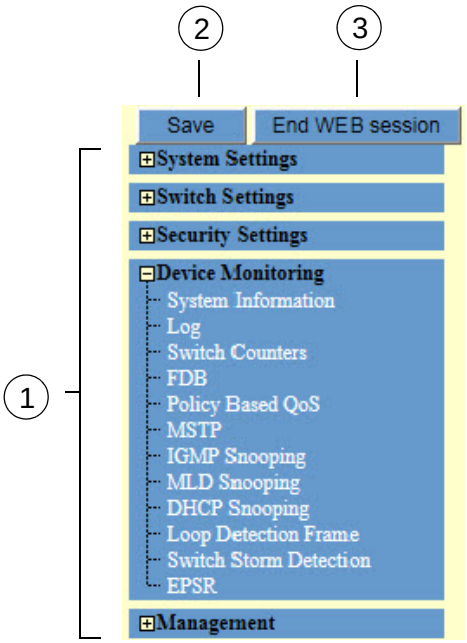

Figure 3. Main Menu

Table 4 defines the main menu components.

Table 4. Main Menu

Section	Description
1	Displays the main menu.
2	Saves your changes to the parameter settings of the switch to the active configuration file in the file system. For more information, refer to the “Save Button” on page 32.
3	Ends a web browser management session.

Working with the Web Browser Interface

This section has guidelines on how to use the web browser interface.

Operating Systems

The web browser interface has been tested on the following operating systems:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

Web Browsers

For general management functions and tasks, Allied Telesis recommends Microsoft Internet Explorer 6 (Windows version) or later. For transferring configuration files or operating system files to the switch, Allied Telesis recommends Microsoft Internet Explorer 7 (Windows version) or later.

> **Note**
> You may need to add the IP address of the switch to the Compatibility View Settings in the web browser if you have a newer version of the Microsoft Internet Explorer and the web browser interface on the switch displays some of the windows incorrectly or not at all.

Menus and Options

The main menu shown in Figure 3 on page 30 has the following five options:

- System Settings
- Switch Settings
- Security Settings
- Device Monitoring
- Management

The options have submenus. Clicking on an option in the main menu expands it to display the submenu. Clicking on a main menu option collapses the submenu again.

To select an option in a submenu, click on it. The switch displays the appropriate window. You may select only one submenu option at a time.

Apply and Set Buttons

Management windows with adjustable parameters have Apply or Set buttons. After changing a parameter setting of a feature, you have to click one of these buttons to activate your change on the switch. Your changes are not implemented on the switch until you click the button.

Save Button

The switch stores its parameter settings in a configuration file in its file system. The file enables the switch to retain its settings even when it is powered off or reset.

The switch does not automatically update the configuration file when you click the Apply or Set button to implement your changes to the parameter settings of a feature. Instead, you have to instruct the switch to update the file yourself with the Save button, located above the main menu. (Refer to Figure 3 on page 30.)

When you click the Save button, the switch displays the Save Configuration window, shown in Figure 4 on page 32.

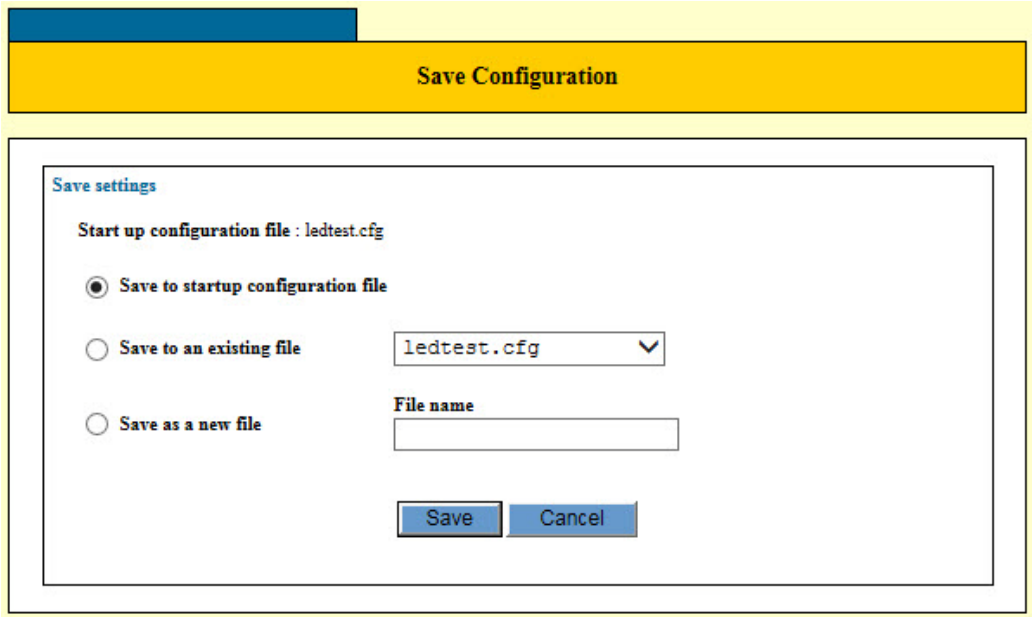

Figure 4. Save Configuration Window

The options in the window are described Table 5.

Table 5. Save Configuration Window

Option	Description
Save To Startup Configuration File	Use this option to save the parameter settings of the switch to the active configuration file. This is the option you are most likely to use.

Table 5. Save Configuration Window (Continued)

Option	Description
Save to an Existing File	Use this option to save the parameter settings of the switch to another configuration file in the file system. To use this option, select the desired configuration file from the pull-down menu.
Save as a New File	Use this option to store the parameter settings in a new configuration file in the file system. Enter the filename for the new configuration file in the File Name field to the right of the option. Here are the filename guidelines: The filename must have the ".cfg" extension. The main portion of the filename can be up to sixteen characters. Spaces and special characters are not allowed in a filename. Filename examples are Sales_switch.cfg and Bldg2_sw4.cfg.

For more information about configuration files, refer to Chapter 42, "Configuration Files" on page 521.

Reset Button

Windows that have an Apply button also have a Reset button. You may use this button to discard your changes to the parameter settings in a window. But this button only works if you have not clicked the Apply button to activate your changes. The Reset button has no affect after the Apply button is used. For example, let's assume that you changed the parameters in a feature window and then decided you preferred to discard your changes and return the parameters in the window to their previous values. If you had not clicked the Apply button to implement your new changes, you could click the Reset button to return the values to their previous settings. But if you click the Apply button and then the Reset button, the values remain at their new settings.

Starting or Ending a Web Browser Management Session

This section contains the procedures for starting or ending a web browser management session on the switch.

Starting a Management Session

To start a web browser management session with the switch, perform the following procedure:

Note
If you are using the default IP address of the switch, start with step 1. If you have already assigned the switch a new address, start with step 3.

1. Change the IP address of your computer to 192.168.1.*n*, where n is a number from 2 to 254.

2. Connect the Ethernet network port on your computer to any of the Ethernet ports on the switch.

   Note
   Do not use the Console port. The Console port does not support the web browser management interface.

3. Start the web browser on your computer and enter the IP address of the switch in the URL field.

   The default address is 192.168.1.1 with the subnet mask 255.255.255.0.

   The switch displays the logon window, shown in Figure 5 on page 35.

Figure 5. Logon Window

4. Enter the username and password for the switch. The default settings are “manager” and “friend”, respectively. The username and password are case sensitive. (The password appears in the Password field as a series of asterisks.)

   The switch displays the Device Monitoring - System Information window, shown in Figure 1 on page 28.

Ending a Management Session

To end a web browser management session, click the End Web Session button above the main menu. Refer to Figure 3 on page 30. You should always end your management session and close the web browser window when you are finished managing the switch. This may protect the switch from unauthorized changes to its configuration settings should you leave your computer unattended.

What to Configure During the First Management Session

Here are a few suggestions on what to configure during the first management session.

Creating a Configuration File

Your first step should be to create a configuration file in the file system of the switch. The device uses the file to store its parameter settings so that you do not have to reenter them when you power off or reset the unit. To create a configuration file, perform the following procedure:

1. Start a web browser management session on the switch. For instructions, refer to “Starting a Management Session” on page 34.
2. Click on the Management menu in the main menu to display the menu options.
3. Click on the Configuration File option in the Management menu.

   The switch displays the Management - Configuration File window. Refer to Figure 6.

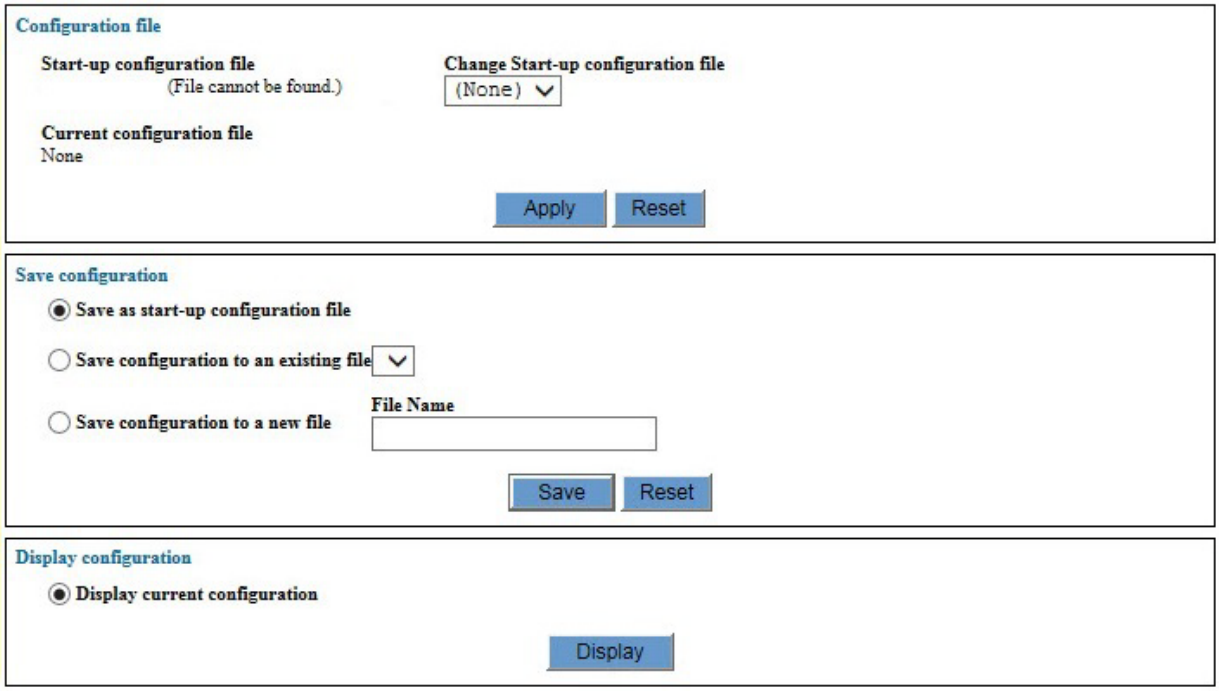

Figure 6. Management - Configuration File Window

4. Click the dialog circle for the Save Configuration to a New File option in the Save Configuration section of the window.
5. Click the File Name field and enter a name for the new configuration file.

Here are the filename guidelines:

- ❒ The filename must have the ".cfg" extension.
- ❒ The main portion of the filename can be up to sixteen characters.
- ❒ Spaces and special characters are not allowed in a filename.

Filename examples are Sales_switch.cfg and Bldg2_sw4.cfg.

6. After entering the filename, click the Save Button.

   The switch creates the new configuration file and stores it in its file system. It also updates the window by displaying the name of the new configuration file in the Change Start-up Configuration File pull-down menu in the Configuration File section of the window.

7. Click the Apply button in the Configuration File section of the window.

   This step designates the new file as the active configuration file. The switch now uses the file to store its parameter settings when you click the Save button. For more information, refer to Chapter 42, "Configuration Files" on page 521.

Changing the Manager Password

To change the password to the manager account, perform the following procedure:

1. Click on the System Settings menu in the main menu to display the menu options.

2. Click on the System option in the Management menu.

   The switch displays the System Settings - System window. Refer to Figure 7 on page 38.

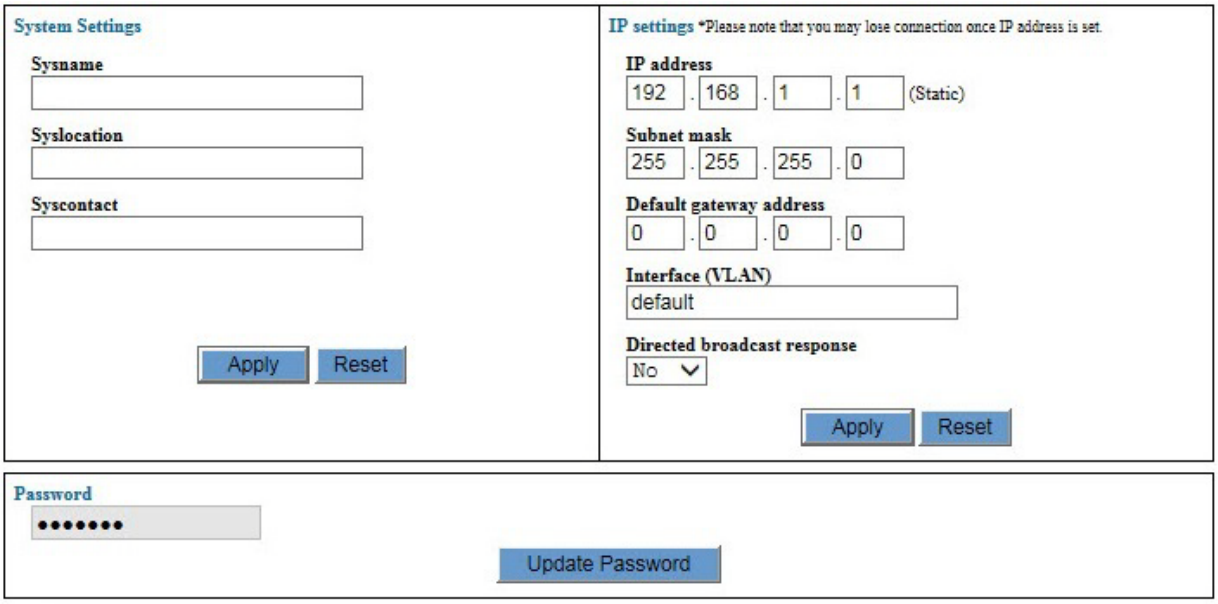

Figure 7. System Settings - System Window

3. Click the Update Password button in the Password section of the window.

   The Password window is shown in Figure 8.

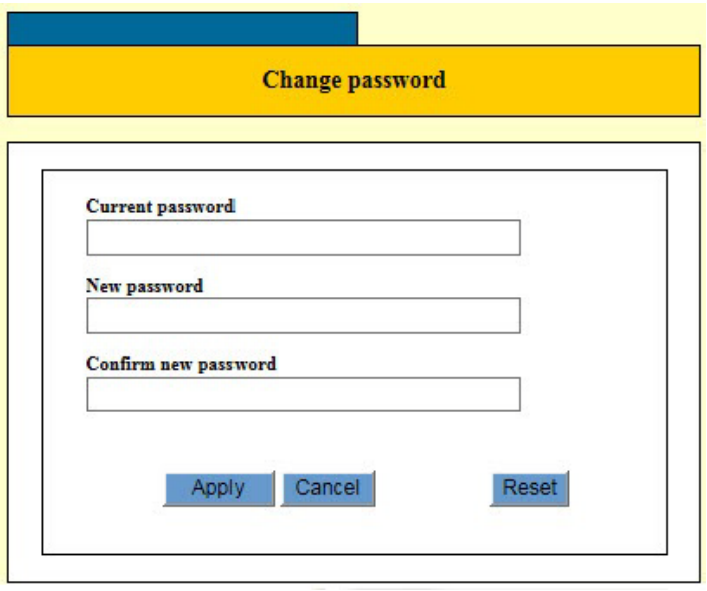

Figure 8. Change Password Window

4. Use the three fields in the Change Password window to change the manager password. The password is case sensitive. The fields are described in Table 6 on page 39.

Table 6. Password Window Parameters

Parameter	Description
Current Password	Use this field to enter the current manager password. The default password is “friend.”
New Password	Use this field to enter the new manager password. The password can be from 0 to 16 characters in length. The password is case sensitive.
Confirm New Password	Use this field to confirm the new password.

Caution
Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

5. Click the Apply button to activate your change on the switch.
6. To permanently save your changes in the configuration file, click the Save button option above the main menu.

   Changing the manager password requires that you log on again.
7. Log on using the new password. The username is “manager” and the password is the new password you assigned the switch in this procedure.

Setting the System Name, Location, and Contact Information

Changing the manager password is not the only management function of the System Settings - System window. It is used for several functions, including setting the system name, location, and contact information of the switch, which can be useful information if you are having to manage a large number of network devices. If you still have the window open from changing the manager password, you might as well set that information, as well. The corresponding fields in the window are described in Table 7 on page 40.

Table 7. Name, Location, and Contact Fields in the System Settings - System Window

Parameter	Description
Sysname	Use this parameter to specify a name for the switch (for example, Sales Ethernet switch). The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.
Syslocation	Use this parameter to specify the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.
Syscontact	Use this parameter to specify the name of a network administrator who is responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

Chapter 2

Basic Switch Parameters

This chapter contains the following sections:

Displaying the System Window

The system window is used to perform the following management tasks:

- Change the name, location, or administrator of the switch.
- Change the password of the manager account.
- Set the IP address of the management VLAN.
- Designate the management VLAN.
- Enable or disable broadcast responses.

To display the system window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9.

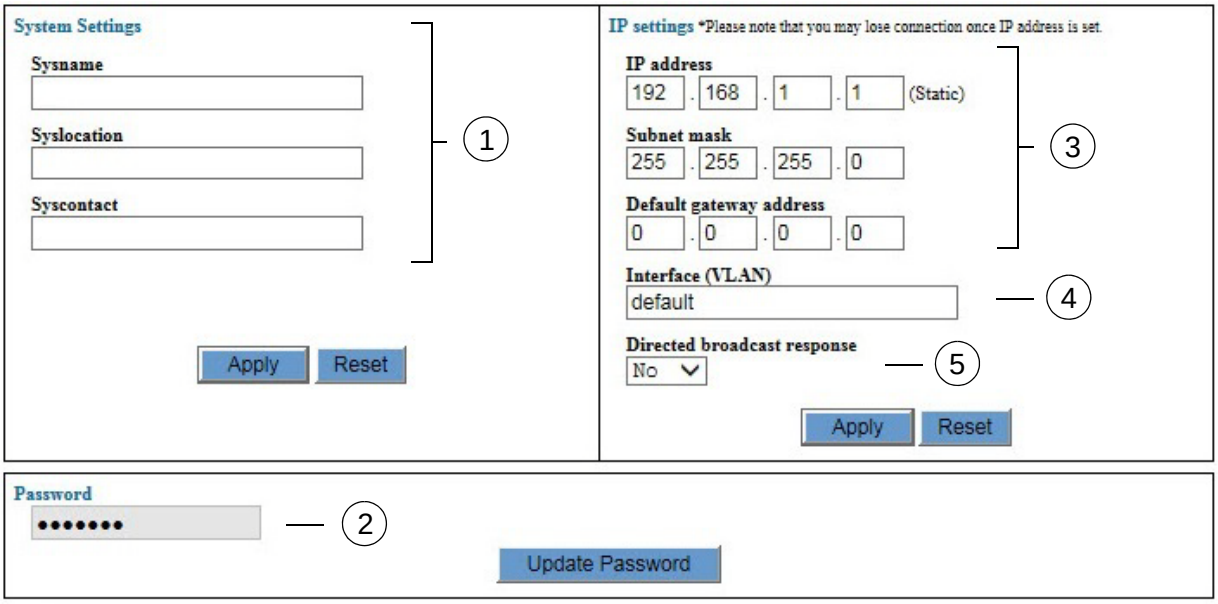

Figure 9. System Settings - System Window

The sections in the System Settings - System window are defined in Table 8 on page 43.

Table 8. Switch Settings - System Window

Section	Description
1	Use the fields in this section to set the name, location, and administrator of the switch. For instructions, refer to "Configuring the Switch Name, Location, and Contact" on page 44.
2	Use this field to change the password of the manager account on the switch. For instructions, refer to "Changing the Password to the Manager Account" on page 46,
3	Use the fields in this section to manually change the IP address, subnet mask, and default gateway of the switch. For instructions, refer to "Changing the IP Address Configuration" on page 48.
4	Use this field to specify the management VLAN on the switch. For instructions, refer to "Specifying the Management VLAN" on page 50.
5	Use this field to control whether the switch responds to broadcast IP PING queries from network devices. For instructions, refer to "Responding to Broadcast PING Queries" on page 51.

Configuring the Switch Name, Location, and Contact

To configure the name, location, and administrator of the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9 on page 42.
3. Configure the Sysname, Syslocation, and Syscontact parameters in the window in Figure 9 on page 42.

   The parameters are described in Table 9.

Table 9. Name, Location, and Contact Fields in the System Settings - System Window

Parameter	Description
Sysname	Use this parameter to specify a name for the switch (for example, Sales Ethernet switch). The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.
Syslocation	Use this parameter to specify the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.
Syscontact	Use this parameter to specify the name of a network administrator who is responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

4. Click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Changing the Password to the Manager Account

The switch has one manager account. The login name is “manager” and the default password is “friend.” You may not change the manager name, but you may change the password. To change the password, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9 on page 42.
3. Click the Update Password button in the Password section of the window.

   The Password window is shown in Figure 10.

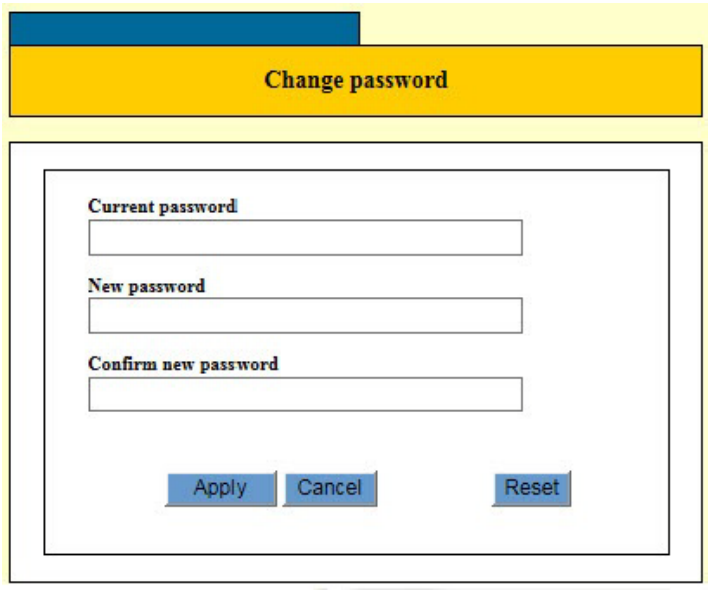

Figure 10. Change Password Window

4. Use the three fields in the Change Password window to change the manager password. The password is case sensitive. The fields are described in Table 10.

Table 10. Password Window Parameters

Parameter	Description
Current Password	Use this field to enter the current manager password.

Table 10. Password Window Parameters (Continued)

Parameter	Description
New Password	Use this field to enter the new manager password. The password can be from 0 to 16 characters in length. The password is case sensitive.
Confirm New Password	Use this field to confirm the new password.

Caution

Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

5. Click the Apply button to activate your change on the switch.
6. To permanently save your changes in the configuration file, click the Save button option above the main menu.

   Changing the manager password requires that you log on again.
7. Log on again using the new password. The username is “manager” and the password is the new password you assigned the switch in this procedure.

Changing the IP Address Configuration

The IP address configuration of the switch consists of the following components:

- IP address
- Subnet mask
- Gateway address

Note
Changing the IP address of the switch from a web browser management session will interrupt your session. To resume managing the switch, start a new session using the new IP address.

Note
The switch has a DHCP client and can obtain its IP configuration from a DHCP server on a network. However, you cannot enable or disable the client from the web browser interface. You have to use the command line interface. For instructions, refer to the AT-GS900M Command Line Interface User's Guides.

To change the IP address configuration of the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9 on page 42.
3. Configure the IP Address, Subnet Mask, and Default Gateway Address fields in the window, as needed.

   The parameters are described in Table 11 on page 49.

Table 11. IP Address Configuration Parameters in the System Settings - System Window

Parameter	Description
IP Address	Use this parameter to specify the IP address of the switch for remote management functions. The switch can have only one IP address. The address must be a unique member of the subset or network of the switch.
Subnet Mask	Use this parameter to specify the subnet mask of the IP address. Subnet masks can be of variable length, provided that the “1” bits are consecutive (e.g., 128, 192, 224, etc.
Default Gateway Address	Use this parameter to specify the default gateway of the switch. This is the IP address of an interface on a router or Layer 3 routing device that is acting as the first hop to reaching management devices, such as management workstations or a syslog server, on remote subnets or networks. The switch can have only one default gateway and the network portion of the address must be the same as the IP address of the switch.

4. Click the Apply button to activate your changes on the switch.

Note
At this point, the switch will probably stop responding to your management commands. To resume managing the device, try starting a new web browser management session using the new IP address or start a local session on the Console port,

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Specifying the Management VLAN

Please review the following information before changing the management VLAN on the switch.

- ❒ You can specify only one VLAN as the management VLAN.
- ❒ The VLAN must already exist on the switch. For information on VLANs, refer to Chapter 16, “Port-based and Tagged VLANs Overview” on page 177 and Chapter 17, “Port-based and Tagged VLANs” on page 191.
- ❒ Changing the management VLAN may interrupt your remote web browser management session of the switch.

To specify a different management VLAN on the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9 on page 42.
3. Select the Interface (VLAN) field and enter the name or VID of the new management VLAN. You may specify only one VLAN.
4. Click the Apply button to activate your changes on the switch.

   Note
   If the switch stops responding to your management session, it probably means that changing the management VLAN has interrupted the session. To resume managing the switch, try connecting your management workstation to a switch port that is a member of the new management VLAN or start a local management session on the Console port of the unit.
5. To permanently save your change in the configuration file, click the Save button above the main menu.

Responding to Broadcast PING Queries

The PING utility is a convenient tool for testing for active paths between network devices or for determining whether a network device is operating properly. However, the utility can also be used to breach the security of a network. By sending broadcast PING queries, network intruders can learn the IP addresses of the network devices or flood a network with PING queries and responses.

Once the switch has an IP address configuration, it does respond to PING queries. However, you may configure the device to respond to or ignore broadcast PING queries as opposed to unicast queries. The default setting is to ignore broadcast PINGS.

To permit or prevent responses by the switch to broadcast PING queries, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the System option from the System Settings menu.

   The System Settings - System window is shown in Figure 9 on page 42.
3. Set the Directed Broadcast Response to either Yes or No.

   When the parameter is set to Yes, the switch responds to broadcast PING queries. When the parameter is set to No, the default setting, the switch ignores broadcast PING queries.

   Note
   The switch responds to unicast PING requests that contain its IP address even when the Directed Broadcast Response parameter is set to No.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your change in the configuration file, click the Save button above the main menu.

Rebooting the Switch

To reboot the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the Reboot option from the Management menu.

   The switch displays a confirmation prompt.
3. Click OK to reboot the switch or Cancel to cancel the procedure.
4. Wait approximately thirty seconds for the switch to initialize its operating system.
5. Start a new management session, if desired.

Resetting Ports

This procedure is used to perform software resets on individual ports on the switch. Resetting a port clears the MAC address table of the addresses learned on the port and deletes the port statistics counters. To perform software resets on individual ports on the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the Port Reset option from the Management menu.

   The switch displays the Management - Port Reset window, shown in Figure 11.

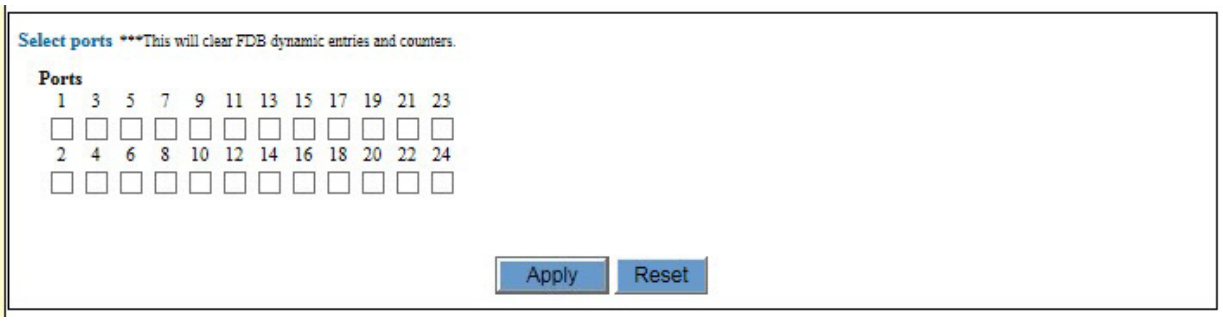

Figure 11. Management - Port Reset Window

3. Click the dialog boxes of the ports you want to reset.
4. Click the Apply button.

Chapter 3

System Date and Time

This chapter contains the following sections:

Displaying the System Date and Time Window

To display the window for setting the date and time on the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Time option from the System Settings menu.

   The System Settings - System Time window is shown in Figure 12.

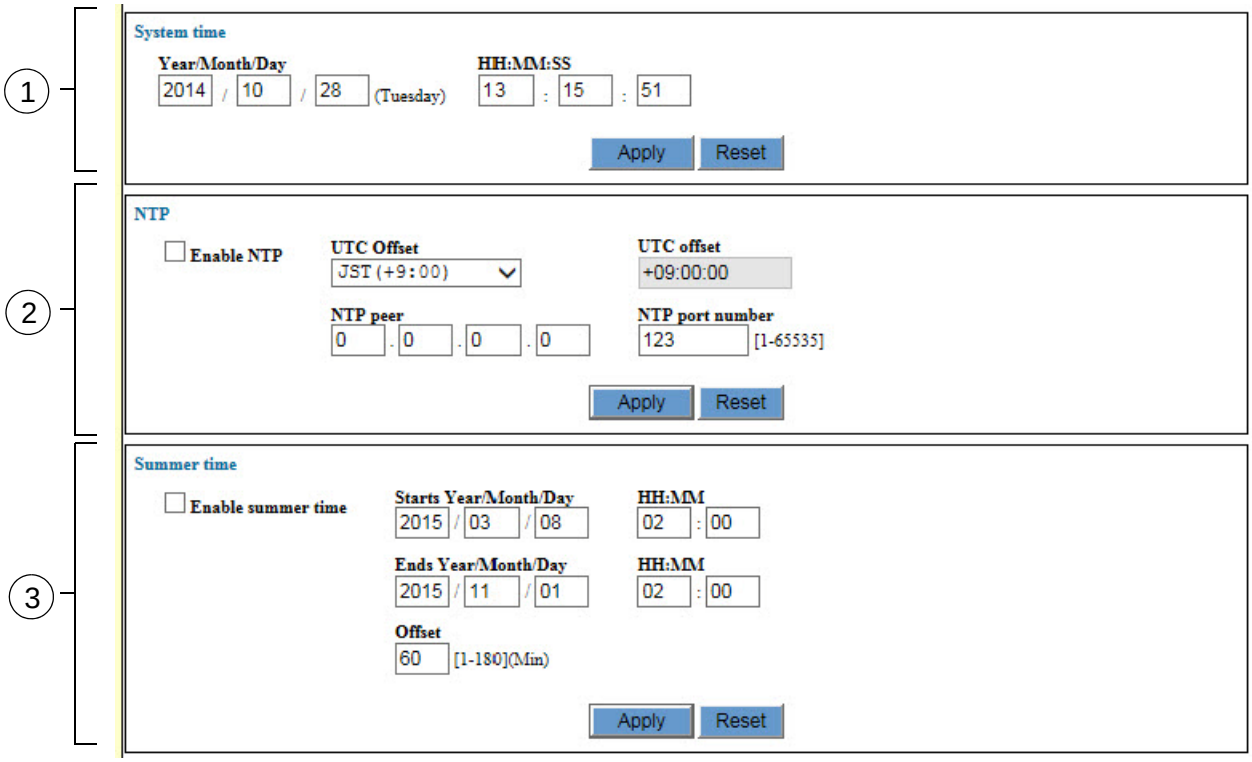

Figure 12. System Settings - System Time Window

The sections in the window are defined in Table 12.

Table 12. System Settings - System Window

Section	Description
1	Use the options in this section to manually set the date and time. For instructions, refer to “Manually Setting the System Date and Time” on page 58.

Table 12. System Settings - System Window (Continued)

Section	Description
2	Use the options in this section of the window to configure the NTP client so that the switch obtains its date and time from an NTP server on your network or the Internet. For instructions, refer to "Setting the System Date and Time with an NTP Server" on page 59.
3	Use the options in this section to configure the switch for Daylight Savings Time (DST). For instructions, refer to "Configuring Daylight Savings Time" on page 61

Manually Setting the System Date and Time

To manually set the date and time on the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Time option from the System Settings menu.

   The System Settings - System Time window is shown in Figure 12 on page 56.
3. Configure the parameters in the System Time section of the window. The fields are defined in Table 13.

Table 13. System Time Section of the System Settings - System Time Window

Parameter	Description
Year/Month/Day	Enter the current year, month, and day in the three fields. The year must be represented with four digits. The month and day can be represented by one or two digits. For example, August 2, 2014 can be entered as 2014/8/2 or 2014/08/02.
HH:MM:SS	Enter the current hours, minutes, and seconds. The hours are entered in 24-hour format. The numbers can have one or two digits. For example, the time of 9:02 am can be entered as 9:2:0 or 09:02:00.

4. After configuring the fields, click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Setting the System Date and Time with an NTP Server

The switch has a Network Time Protocol (NTP) client so that it can set the date and time from an SNTP or NTP server on your network or the Internet. Here are the guidelines to using the NTP client:

- The switch must have an IP address. For instructions, refer to "Changing the IP Address Configuration" on page 48.
- If the switch and NTP server are in different networks or subnetworks, the switch must also have the IP address of a default gateway. This is the IP address of a routing interface that represents the first hop to reaching the remote network of the SNTP or NTP server. For instructions, refer to "Changing the IP Address Configuration" on page 48.
- When you configure the client, you must specify the offset of the location of the switch from Coordinated Universal Time (UTC).
- The switch polls the NTP server for the date and time when you configure the client and whenever the unit is powered on or reset.

To configure the NTP client, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Time option from the System Settings menu.

   The System Settings - System Time window is shown in Figure 12 on page 56.
3. Configure the parameters in the NTP section of the window.

   The fields are defined in Table 14.

Table 14. NTP Client Parameters

Parameter	Description
Enable NTP	Use this parameter to enter or disable the NTP client. The NTP client is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
Time Zone	Use this parameter to select the correct time zone for the location of the switch from the pull-down menu.

Table 14. NTP Client Parameters (Continued)

Parameter	Description
UTC Offset	Use this pull-down menu to select the difference between the UTC and local time.
NTP Peer	Use this parameter to enter the IP address of the NTP server.
NTP Port	Use this parameter to enter the listening port number for the NTP client. The range is 1 to 65535. The default is 123.

4. After configuring the fields, click the Apply button to activate your changes on the switch.

   If you enabled the NTP client, the switch immediately polls the designated SNTP or NTP server for the current date and time. The switch automatically polls the server whenever a change is made to any of the parameters in this menu, as long as NTP is enabled.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring Daylight Savings Time

This procedure is for locations that observe Daylight Saving Time (DST). It explains how to add the start and end dates of DST and the number of minutes of the time change so that the switch adjusts its clock automatically. To configure the switch to observe Daylight Savings Time (DST), perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Time option from the System Settings menu.

   The System Settings - System Time window is shown in Figure 12 on page 56.
3. Configure the parameters in the Summer Time section of the window.

   The fields are defined in Table 15.

Table 15. Summer Time Parameters

Parameter	Description
Enable summer time	Use this option to enable or disable Daylight Savings Time on the switch. DST is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled.
Starts Year/Month/Day HH:MM	Enter the start date and time for DST. The years must have four digits.
Ends Year/Month/Day HH:MM	Enter the end date and time for DST. The years must have four digits.
Offset	Use this option to specify the number of minutes the clock is to move forward at the start of DST and move back at the return to Standard Time (ST). The range is 1 to 180 minutes (3 hours). The default is 60 minutes.

4. After configuring the fields, click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 4

Event Log

This chapter describes how to view switch activity by displaying or saving the contents of the event log. Sections in the chapter include:

Introduction

A managed switch is a complex piece of computer equipment that includes both hardware and software components. Multiple software features operate simultaneously, interoperating with each other and processing large amounts of network traffic. It is often difficult to determine exactly what is happening when a switch appears not to be operating normally, or what happened when a problem occurred.

The operation of the switch can be monitored by viewing the event messages generated by the device. These events and the vital information about system activity that they provide can help you identify and solve system problems.

The events are stored by the switch in an event log, in permanent memory. The events in the log are retained even when you reset or power cycle the switch.

The event messages include the following information:

- The time and date of the event
- The severity of the event
- An event description

The switch also has a syslog client. You may use the client to send the event messages from the switch to a syslog server on your network for storage. For more information, refer to Chapter 5, “Syslog Client” on page 75.

Displaying the Event Log Window

To display the event log window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Log option from the System Settings menu.

   The System Settings - Log window is shown in Figure 13.

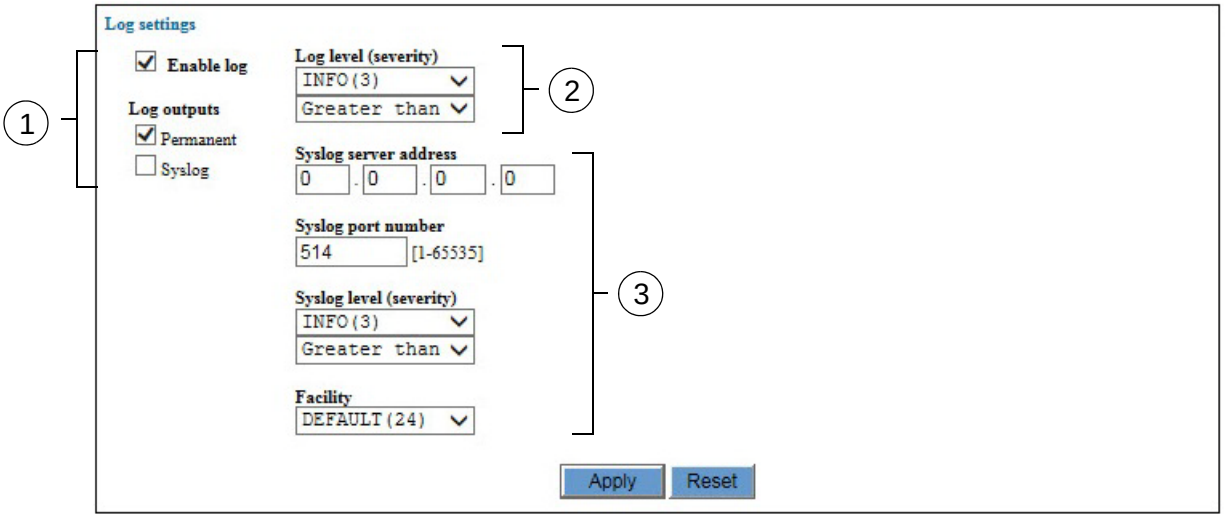

Figure 13. System Settings - Log Window

The sections in the System Settings - Log window are described in Table 16.

Table 16. System Settings - Log Window

Section	Description
1	Use the options in this section to enable or disable the event log or syslog client. When the event log is enabled, the switch stores event messages in its event log in permanent memory. When the syslog client is enabled, the switch transmits the event messages to a syslog server on your network. Refer to “Configuring the Event Log” on page 67.
2	Use the options in this section to specify the types of messages the switch is to store in the event log. Refer to “Configuring the Event Log” on page 67.

Table 16. System Settings - Log Window (Continued)

Section	Description
3	Use the options in this section to configure the syslog client so that the switch transmits the event messages to a syslog server on your network. Refer to Chapter 5, “Syslog Client” on page 75.

Configuring the Event Log

This procedure explains how to enable or disable the event log. It also describes how to specify the types of event messages the switch is to store in the log.

> **Note**
> Allied Telesis recommends setting the switch's date and time if you intend to use the event log or syslog client. Otherwise, the entries will not have the correct date and time. For instructions, refer to Chapter 3, "System Date and Time" on page 55.

To configure the event log, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Log option from the System Settings menu.

   The System Settings - Log window is shown in Figure 13 on page 65.
3. To enable the event log, do the following:
   a. Verify that the Enable Log option has a check mark in its dialog box. If it does not have a check mark, click it.
   b. Verify that the Permanent option under Log Outputs has a check mark in its dialog box. If it does not have a check mark, click it.
   c. Continue with step 5.
4. To disable the event log, do the following:
   a. Remove the check mark from either the Enable Log option or the Permanent option under Log Outputs. If you are using the syslog client to send the event messages to a syslog server, do not remove the check mark from the Enable Log option. Instead, remove the check mark only from the Permanent option. This will stop the switch from storing messages in the event log, but allow it to continue to send them to the syslog server.
   b. Go to step 7.
5. Click the Log Level (Severity) pull-down menu and select the severity of the messages the switch is to store in the event log. You may choose only one severity level. The severity levels are listed in Table 17 on page 68.

Table 17. Severity Levels

Severity Level	Description
7 Critical	Event messages of this level contain information about critical failures that have affected switch operations.
6 Urgent	Event messages of this level contain information about possible pending failures that require immediate attention.
5 Important	Event messages of this level contain information about possible pending failures.
4 Notice	Event messages of this level contain information about events that do not affect switch operations.
3 Info	Event messages of this level contain information about events that do not affect switch operations.
2 Detail	Event messages of this level contain information about events that do not affect switch operations.
1 Trivial	Event messages of this level contain information about events that do not affect switch operations.
0 Debug	Event messages of this level contain debug information.

6. Click the pull-down menu directly below the Severity parameter and select the option that represents the range of messages, by severity, to be stored in the event log. The options are described in Table 18 on page 69.

Table 18. Event Log Options

Option	Description
Less Than	Use this option to designate event messages with the same or less severity as the severity chosen in the previous step. For example, if you choose Info(3) in the previous step and this option, the switch stores messages with severity levels 0 to 3. As another example, if you choose Critical(7) in the previous step and this option, the switch stores all of the messages.
Greater Than	Use this option to designate event messages with the same or greater severity as the severity chosen in the previous step. For example, if you choose Info(3) in the previous step and this option, the switch stores messages with severity levels 3 to 7. As another example, if you choose Debug(0) in the previous step and this option, the switch stores all of the messages.
No Equal	Use this option to designate all severity levels of event messages except the level chosen in the previous step. For example, if you choose Info(3) in the previous step and this option, the switch stores messages with the levels 0 to 2 and 4 to 7.
Equal To	Use this option to designate only the event messages with the same severity level chosen in the previous step. For example, if you choose Info(3) in the previous step and this option, the switch stores only messages with the severity level 3.

7. After configuring the fields, click the Apply button to activate your changes on the switch.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying or Saving the Event Messages in the Event Log

To view or save the messages in the event log, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the Log option from the Monitoring menu.

   The Device Monitoring - Log window is shown in Figure 14.

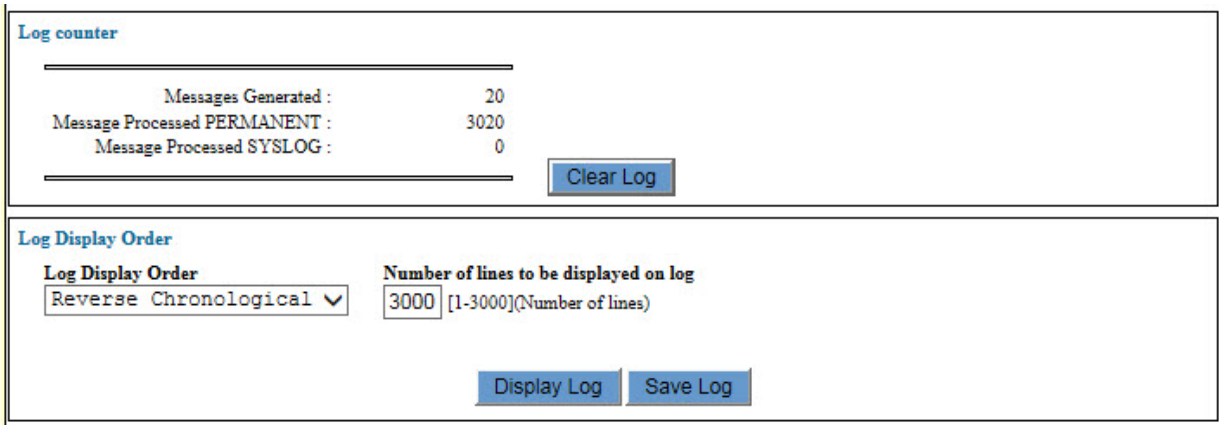

Figure 14. Device Monitoring - Log Window

The fields in the Log Counter portion of the window are described in Table 19.

Table 19. Log Counter Fields

Field	Description
Messages Generated field	Displays the total number of messages the switch has generated.
Messages Processed Permanent field	Displays the total number of messages the switch has stored in the event log. This number may be the same as or less than the number displayed in the Messages Generated field, depending on how you configure the log in “Configuring the Event Log” on page 67.
Messages Processed Syslog field	Displays the total number of messages the switch has sent to a syslog server on your network.
Clear Log button	Clears the above counters and deletes all of the messages from the event log.

3. Use the Display Order pull-down menu to specify the order in which the messages in the event log are to be displayed on your screen or saved in a file. Your options are listed in Table 20.

Table 20. Display Order Options

Field	Description
Reverse Chronological	Use this option to display or save the messages from newest to oldest.
Chronological	Use this option to display or save the messages from oldest to newest.
Latest	Use this option to display or save the messages newest to oldest. This selection is identical to the Reverse Chronological option.

4. In the Display Number field, enter the number of messages to be displayed on the screen or saved in a file. The range is 1 to 3000 messages. The default is 3000 messages.

5. To display the messages on the screen, click the Display Log button. An example of the event log is shown in Figure 15 on page 72.

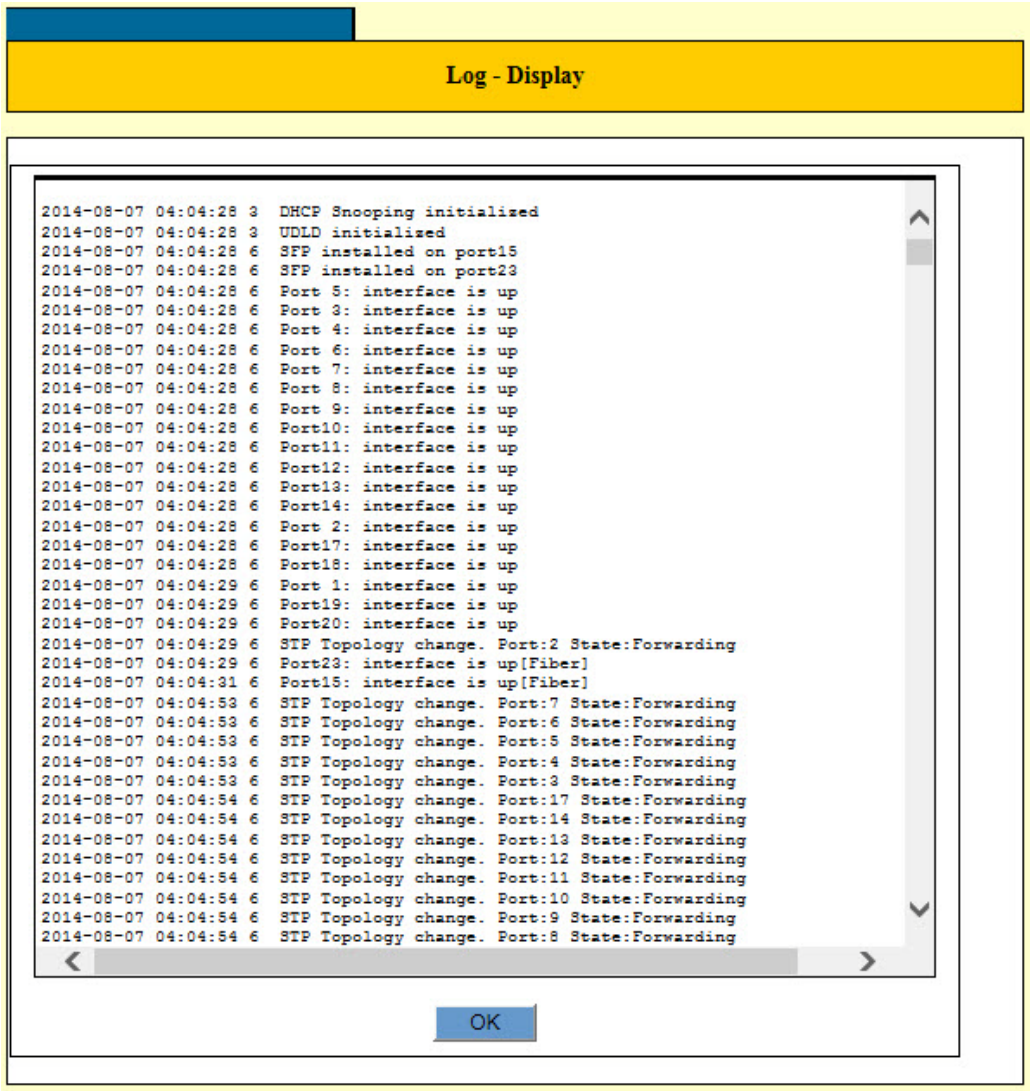

Figure 15. Log - Display Window

The columns in the window are described in Table 21.

Table 21. Columns in the Log - Display Window

Column	Description
Date	Displays the date the event message was generated, in year, month, day format.
Time	Displays the time of the event message, in hours, minutes, and seconds format.
Level	Displays the severity level of the event message. Refer to Table 17 on page 68.
Message	Displays the event message.

6. To save the messages in the log to a file on your management workstation, click the Save Log button.

7. At the prompt, enter a name for the file.

8. The switch saves the log as a text file on your management workstation.

Deleting Messages in the Event Log

To delete the messages in the event log, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the Log option from the Device Monitoring menu.

   The Device Monitoring - Log window is shown in Figure 14 on page 70.

3. Click the Clear Log button to delete all of the messages in the event log and return the log counters to zero.

   Note
   You may not delete individual messages from the event log.

Chapter 5

Syslog Client

This chapter explains how to use the syslog client on the switch to transmit the event messages to a syslog server on your network. Sections in the chapter include:

Introduction

The syslog client allows the switch to send its event messages to a syslog server on your network. Here are the guidelines to using the syslog client:

- You can specify only one syslog server.
- The switch must have a management IP address. For instructions, refer to “Changing the IP Address Configuration” on page 48.
- The syslog server must be a member of the management VLAN on the switch, or must be able to access the VLAN through routers or other Layer 3 devices.
- If the syslog server is not a member of the management VLAN, the switch must have a default gateway that specifies the first hop to reaching the server. For instructions on specifying the default gateway, refer to “Changing the IP Address Configuration” on page 48.
- The event messages are transmitted when they are generated. Any event messages that already exist in the event log are not transmitted when you configure the syslog client.

Configuring the Syslog Client

To configure the syslog client, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Log option from the System Settings menu.

   The System Settings - Log window is shown in Figure 13 on page 65.
3. To enable the syslog client, do the following:

   a. Verify that the Enable Log option has a check mark in its dialog box. If it does not have a check mark, click it.

   b. Verify that the Syslog option under Log Outputs has a check mark in its dialog box. If it does not have a check mark, click it.

   c. Continue with step 5.
4. To disable the syslog client, do the following:

   a. Remove the check mark from either the Enable Log option or the Syslog option under Log Outputs. If you are storing event messages in the event log, do not remove the check mark from the Enable Log option. Instead, remove the check mark only from the Syslog option This will stop the switch from sending messages to the syslog server but allows it to continue to save the event messages in the event log.

   b. Go to step 6.
5. Configure the syslog client parameters in the System Settings - Log window. The parameters are described in Table 22.

Table 22. Syslog Client Parameters

Parameter	Description
Syslog Server Address	Use this parameter to specify the IP address of the syslog server on your network. You may enter only one IP address.
Syslog Port Number	Use this parameter to specify the UDP port for the syslog client. The syslog server and client must use the same value. The range is 1 to 65535. The default value is 514.

Table 22. Syslog Client Parameters (Continued)

Parameter	Description
Syslog Severity (severity)	Use the top pull-down menu to specify the severity of messages the switch is to send to the syslog server. You may choose only one severity. The severities are listed in Table 17 on page 68. Use the bottom pull-down menu to select the option that represents the range of messages, by severity, to be sent to the syslog server. The symbols are described in Table 18 on page 69.
Facility	Use the pull-down menu to select a facility code for the event messages. The switch adds the code to the messages as it transmits them to the syslog server on your network. You may use the code to group the event messages on the syslog server by the switch that generated them. This can be useful when the syslog server collects events from multiple network devices. For example, the default setting adds the facility code 24 to the event messages. You may select only one facility code. The codes are described in Table 23.

The facility codes are listed in Table 23.

Table 23. Facility Codes for the Syslog Client

Facility Value	Description	Facility Code
DEFAULT	Default value.	24
LOCAL7	Local use 7 (local7)	23
LOCAL6	Local use 6 (local6)	22
LOCAL5	Local use 5 (local5)	21
LOCAL4	Local use 4 (local4)	20
LOCAL3	Local use 3 (local3)	19
LOCAL2	Local use 2 (local2)	18
LOCAL1	Local use 1 (local1)	17

Table 23. Facility Codes for the Syslog Client (Continued)

Facility Value	Description	Facility Code
LOCAL0	Local use 0 (local0)	16
CRON2	Clock daemon.	15
ALERT	Log alert.	14
AUDIT	Log audit.	13
NTP	NTP subsystem.	12
FTP	FTP daemon.	11
AUTHPRIV	Security/authorization messages	10
CRON	Clock daemon.	9
UUCP	UUCP subsystem.	8
NEWS	Network news subsystem.	7
LPR	Line printer subsystem	6
SYSLOG	Messages generated by the syslog client.	5
AUTH	Security/authorization messages	4
DAEMON	System Daemons	3
MAIL	Mail system	2
USER	User-level messages	1
KERNEL	Kernel messages	0

6. After configuring the syslog client parameters, click the Apply button to activate your changes on the switch.

   The switch begins to send new event messages to the designated syslog server. Any messages already in the event log are not sent.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 6

Management Tools and Alerts

This chapter contains instructions on how to configure the management tools and alerts. The chapter contains the following sections:

Introduction

This chapter explains how to configure the following management tools and functions:

- Console port
- Web browser server
- Telnet server
- FTP/TFTP server
- Temperature alerts for the SFP modules
- Fan alert

Configuring the Management Tools and Alerts

To configure the management tools and alerts, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Others option from the System Settings menu.

   The System Settings - Others window is shown in Figure 16.

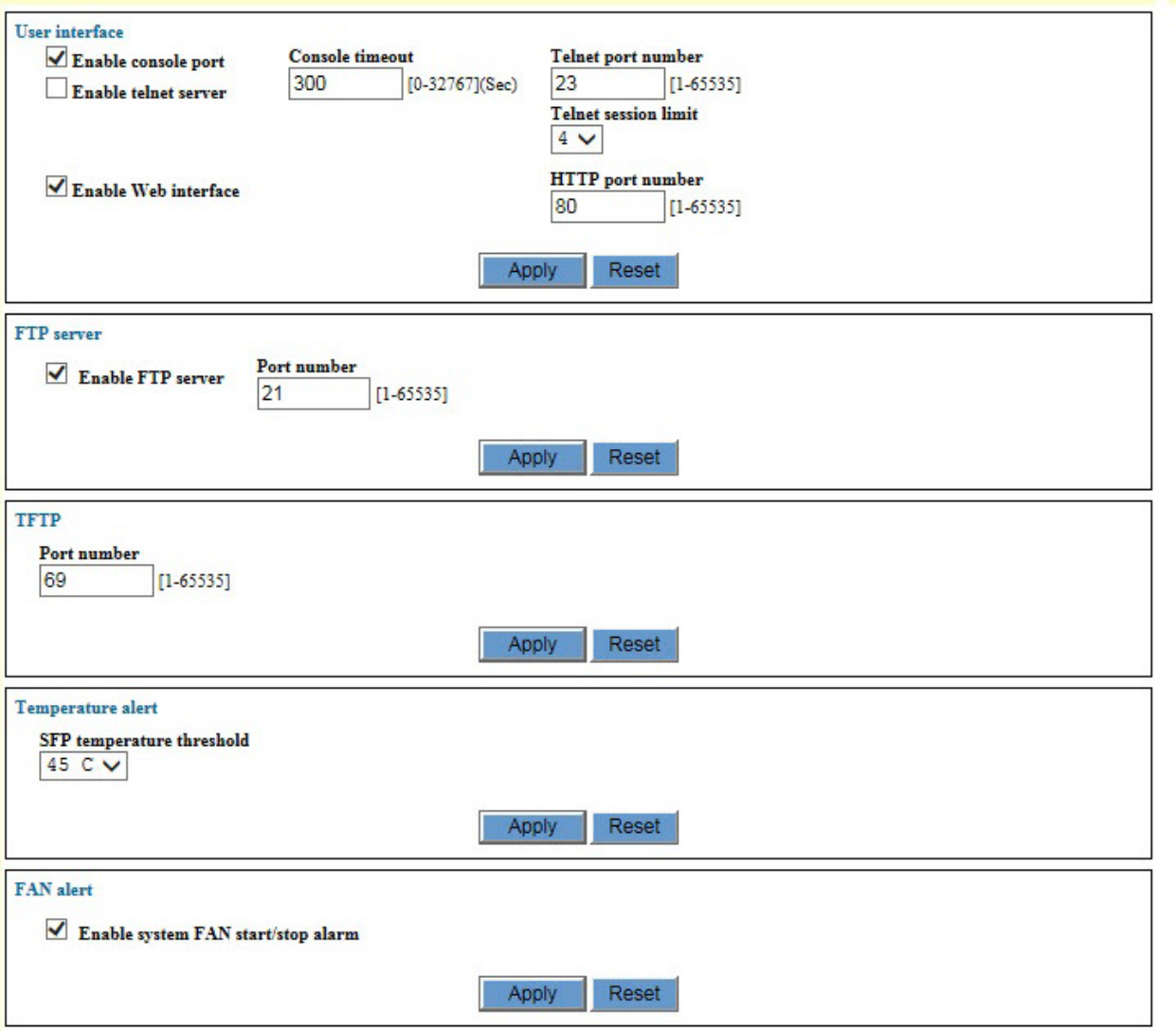

Figure 16. System Settings - Others Window

The parameters in the window are defined in Table 24 on page 84.

Table 24. System Settings - Others Window

Parameter	Description
User Interface	
Enable Console Port	Use this option to enable or disable the Console port on the switch. When the Console port is enabled, you may use the port to manage the switch. This is the default setting. When the Console port is disabled, you may not use the port to manage the switch. The Console port is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
Console Timeout	Use this option to specify the management session timeout value for the Console port. The timeout value controls the amount of time the switch waits before it ends inactive management sessions on the Console port. The range is 1 to 32767 seconds. The default is 300 seconds (five minutes).
Enable Telnet Server	Use this option to enable or disable the Telnet server on the switch. When the server is enabled, you may remotely manage the switch with a Telnet client on a network workstation. When the server is disabled, you may not manage the switch with a Telnet client. This is the default setting. The Telnet server is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
Telnet Port Number	Use this option to set the TCP port number for the Telnet server. The range is 1 to 65535. The default value is 23.
Telnet Session Limit	Use this option to specify the maximum number of remote Telnet sessions the switch will support at one time. The range is 1 to 4 sessions. The default value is 4 sessions.

Table 24. System Settings - Others Window (Continued)

Parameter	Description
Enable Web Browser	Use this option to enable or disable the web browser server on the switch. When the server is enabled, you may use a web browser on a network workstation to remotely manage the switch. This is the default setting. When the server is disabled, you may not use a web browser to remotely manage the switch. The server is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
HTTP Port Number	Use this option to set the TCP port number for the web browser server. The range is 1 to 65535. The default value is 80.
FTP Server	
Enable FTP Server	Use this option to enable or disable the FTP server on the switch. When the server is enabled, you may use FTP or TFTP to upload or download files to the file system in the switch. When the server is disabled, you may not use FTP or TFTP to upload or download files to the switch. The server is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is enabled.
Port Number	Use this option to set the TCP port number for the FTP server. The range is 1 to 65535. The default value is 21.
TFTP	
Port Number	Use this option to set the TCP port number for the TFTP server. The range is 1 to 65535. The default value is 69.
Temperature Alert	
SFP Temperature Threshold	Use this option to set the temperature threshold for the SFP modules. The switch sends a trap if the temperature is exceeded. The values are 40°, 45°, and 50° C. The default is 45° C.

Table 24. System Settings - Others Window (Continued)

Parameter	Description
Fan Alert	
Enable System Fan Start/ Stop Alarm	Use this option to enable or disable the fan alert. When the alert is enabled, the switch sends a trap when the fan starts or stops. This is the default setting. When the alert is disabled, the switch does not send a trap when the fan starts or stops. The alert is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting for the alert is enabled.

3. After configuring the parameters, click the Apply button to implement your changes on the switch.

4. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 7

System Information and Packet Statistics

This chapter contains instructions on how to display system and port information. The chapter contains the following sections:

Viewing Basic System and Port Information

To view basic system and port information, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the System Information option from the Device Monitoring menu.

   The Device Monitoring - System Information window is shown in Figure 17.

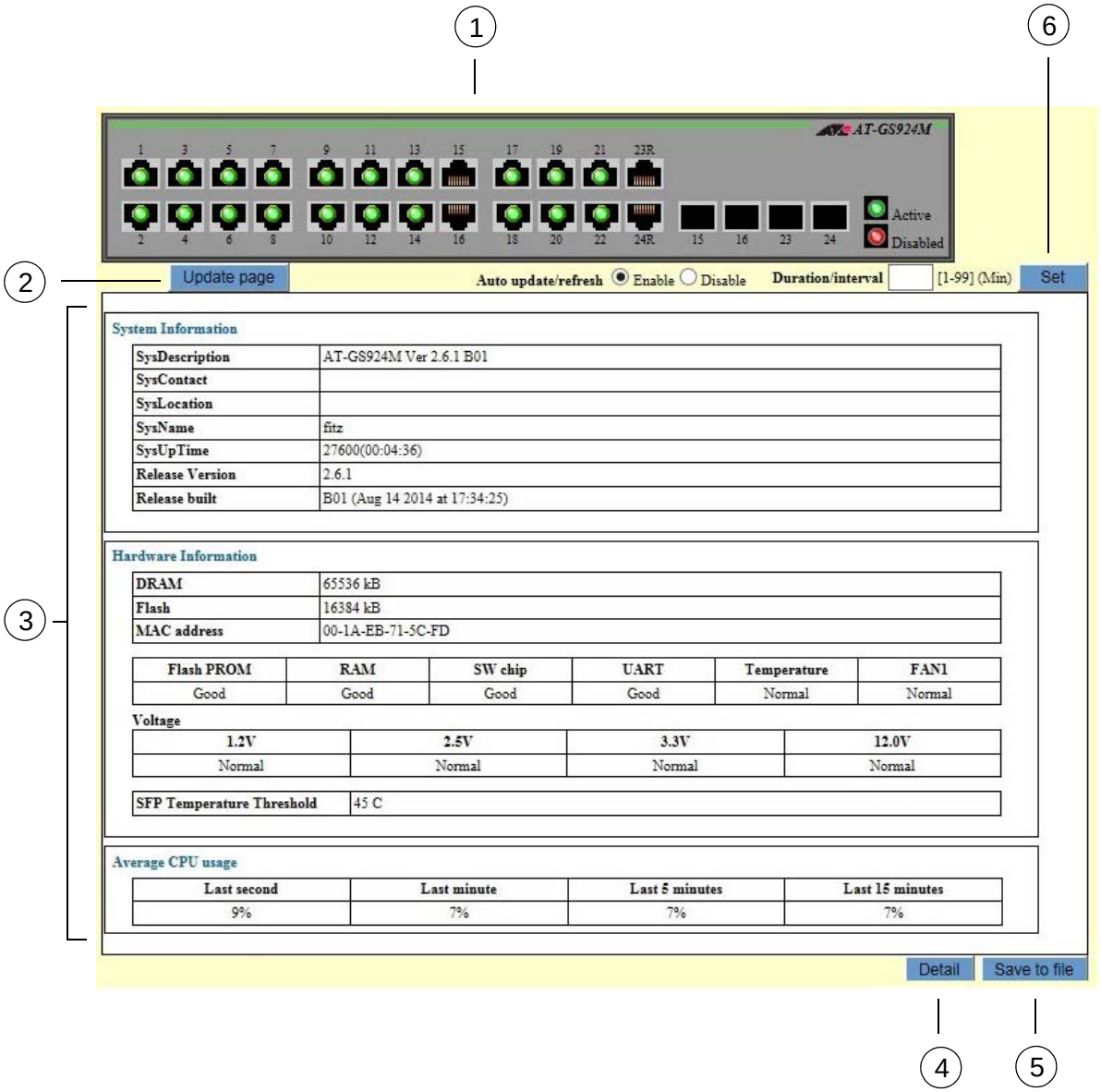

Figure 17. Device Monitoring - System Information Window

The sections in the window are defined in Table 25.

Table 25. Device Monitoring - System Information Window

Section	Description
1	Use the image of the front panel of the switch to view the status of the links on the ports and to display the port configuration settings. The possible states of the ports are listed here: Black - The port has not established a link to a network device. Green - The port has established a link to a network device. Red - The port is disabled. For more information, refer to “Displaying Port Configurations” on page 91.
2	Use the Update Page button to refresh the states of the ports in the switch image and the information in the table.
3	Use the table to view software and hardware information about the switch.
4	Use the Detail button to view configuration information about the switch. For more information, refer to “Detail Button” on page 89.
5	Use the Save to File button to save the information displayed by the Detail button to a file in the file system of the switch. For instructions, refer to “Save to File Button” on page 90.
6	Use the options of the Set button to control how frequently the switch updates the information in the switch image and table. For instructions, refer to “Refreshing the Window” on page 92.

Detail Button

You may use the Detail Button in the Device Monitoring - System Information window to display the entire configuration of the switch, with debug information. The configuration settings of the features are displayed with the corresponding command line commands. The window contains only those parameter settings that have been changed from their default values. An example of the window is shown in Figure 18 on page 90.

Note
It may take the switch several seconds to assemble and display the information on your workstation.

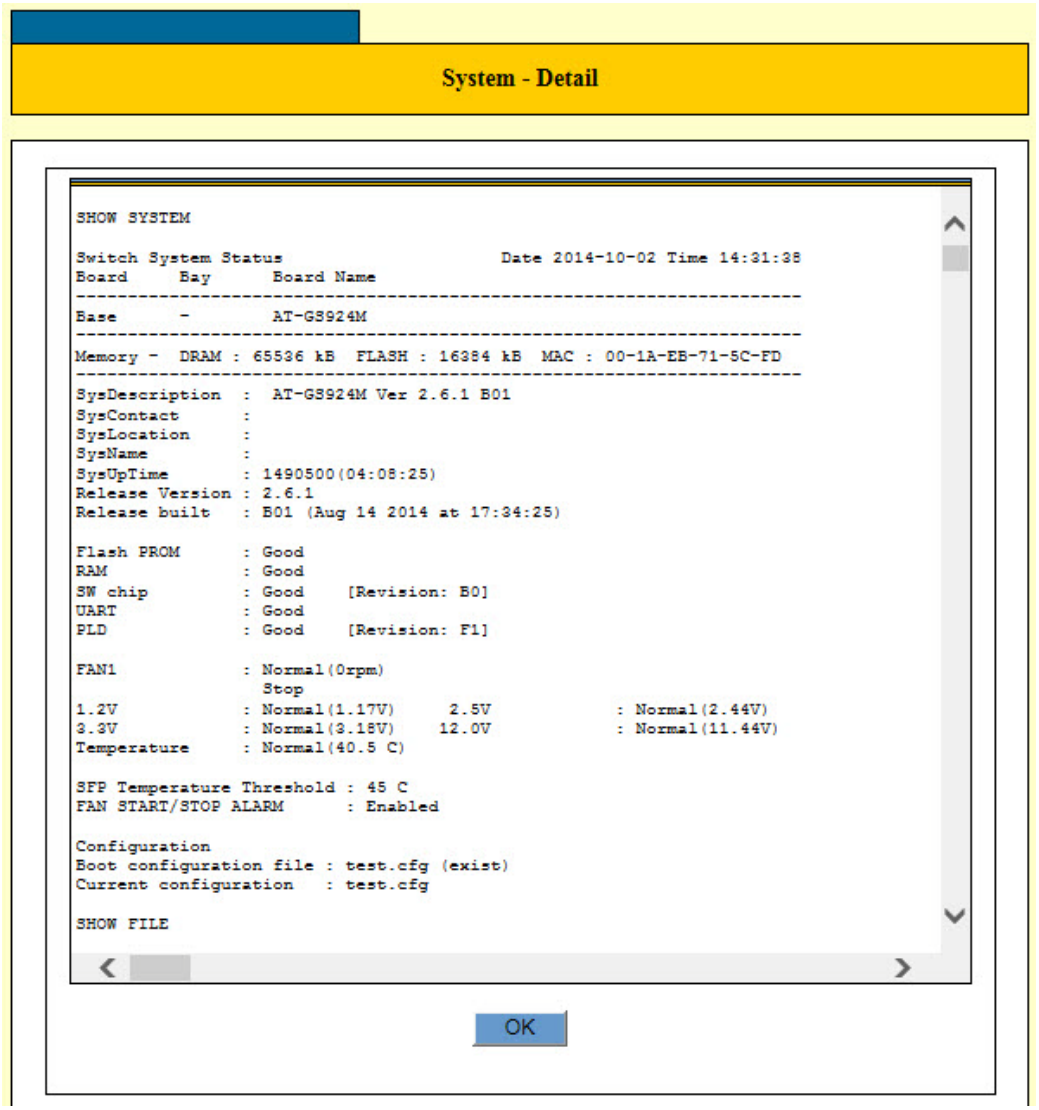

Figure 18. System - Detail Window

Save to File Button

You may use the Save to File button in the bottom right corner of the window to save the information from the Detail button to a file on your workstation or a network server. You might be asked to provide this file if your contact Allied Telesis for assistance in resolving a technical problem.

Note
It may take the switch several seconds to assemble the information before it displays the prompt for saving the file on your workstation.

Displaying Port Configurations

To display port parameter settings, click on a port in the image of the front panel. The switch displays the Display Port Status window. You may view the parameters of only one port at a time. An example of the window is shown in Figure 19. The parameters in the window are defined in Figure 35 on page 125.

Figure 19. Display Port Status Window

Refreshing the Window

There are two ways to update the information in the window, besides opening another window and then returning to it again. The first way is to click the Update Page button in the upper left corner of the window. The button immediately updates the information in the switch image and table.

The other way to update the window is have the switch do it for you, automatically. This approach is accomplished with the Auto Update/ Refresh and Duration/Interval options of the Set button. The options are defined in Table 26.

Table 26. Automatic Refresh Option in the Device Monitoring

Option	Description
Auto Update/Refresh	Use this option to enable or disable the automatic refresh option. The options are defined here: Enable - Select this option to enable automatic updates of the window. Disable - Select this option to disable automatic updates of the window.
Duration/Interval	Use this option to define how frequently the switch updates the window if you enable the update feature. The range is 1 to 99 minutes.

After setting the options, click the Set button. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Statistics Counters

The switch has statistics counters you might find useful when troubleshooting network problems. The first statistics window is displayed by selecting the Switch Counters option from the Device Monitoring window. The window is shown in Figure 20.

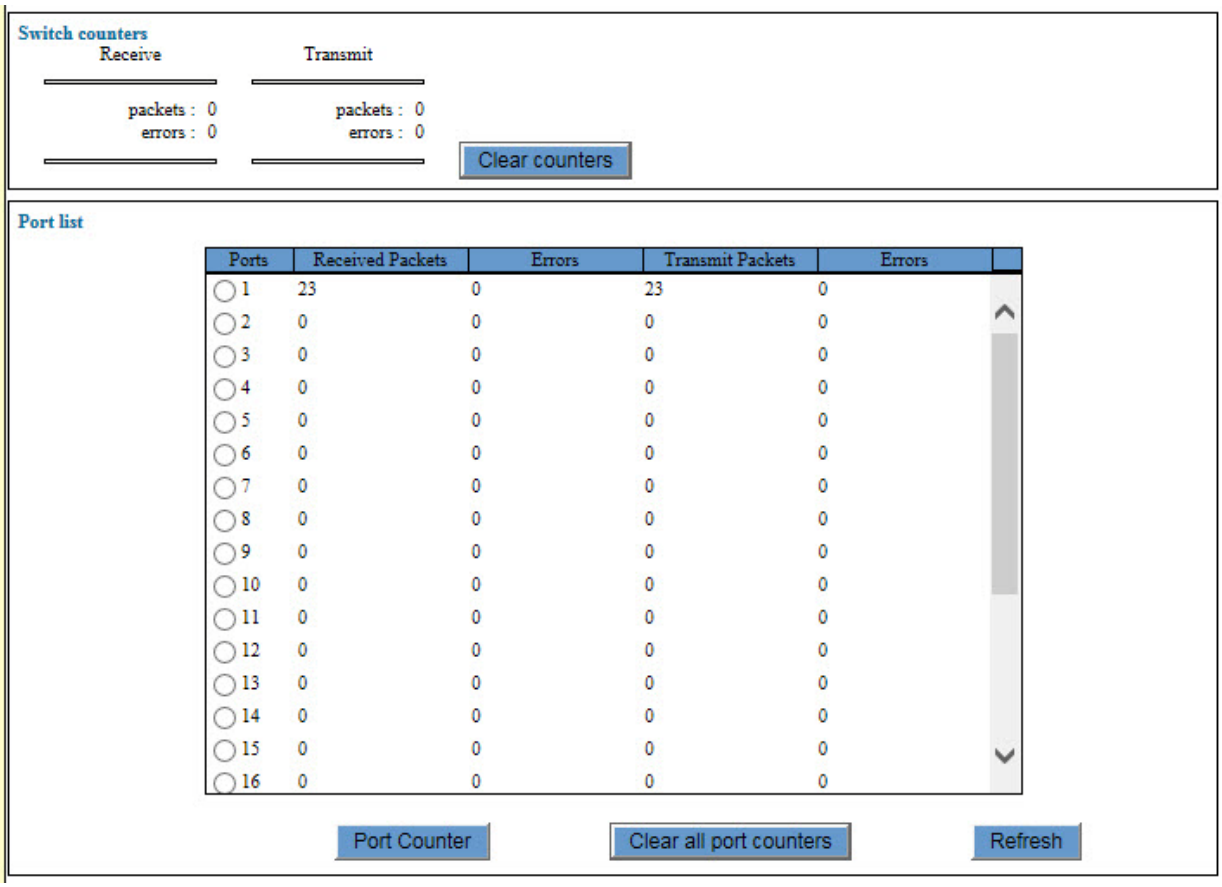

Figure 20. Device Monitoring - Switch Counter Window

To display additional port statistics, click the dialog circle of a port and click the Port Counter button. You may view the statistics of only one port at a time. An example of the port statistics window is shown in Figure 21 on page 94.

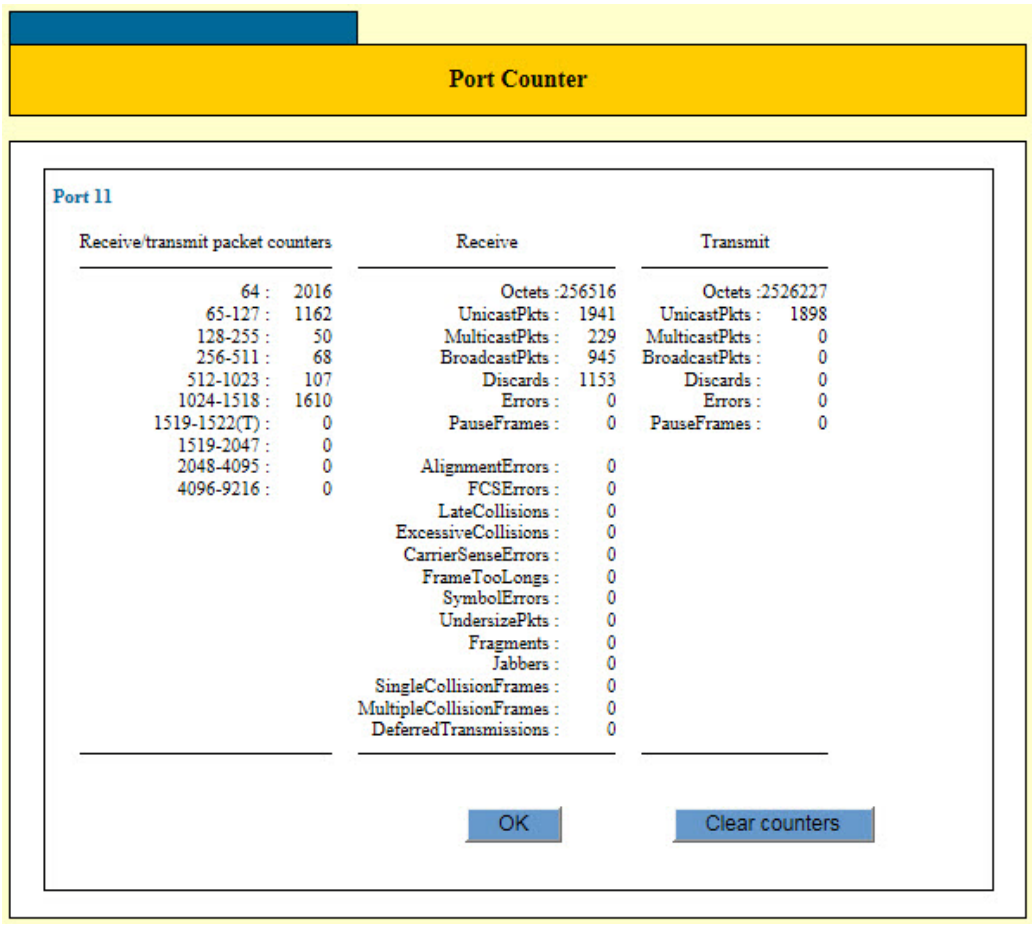

Figure 21. Port Counter Window

Chapter 8

Port LEDs

This chapter describes how to control the port LEDs from the web browser windows. Sections in the chapter include:

Displaying the Port LEDs Window

To display the port LED window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Port LED option from the System Settings menu.

   The System Settings - LED window is shown in Figure 22.

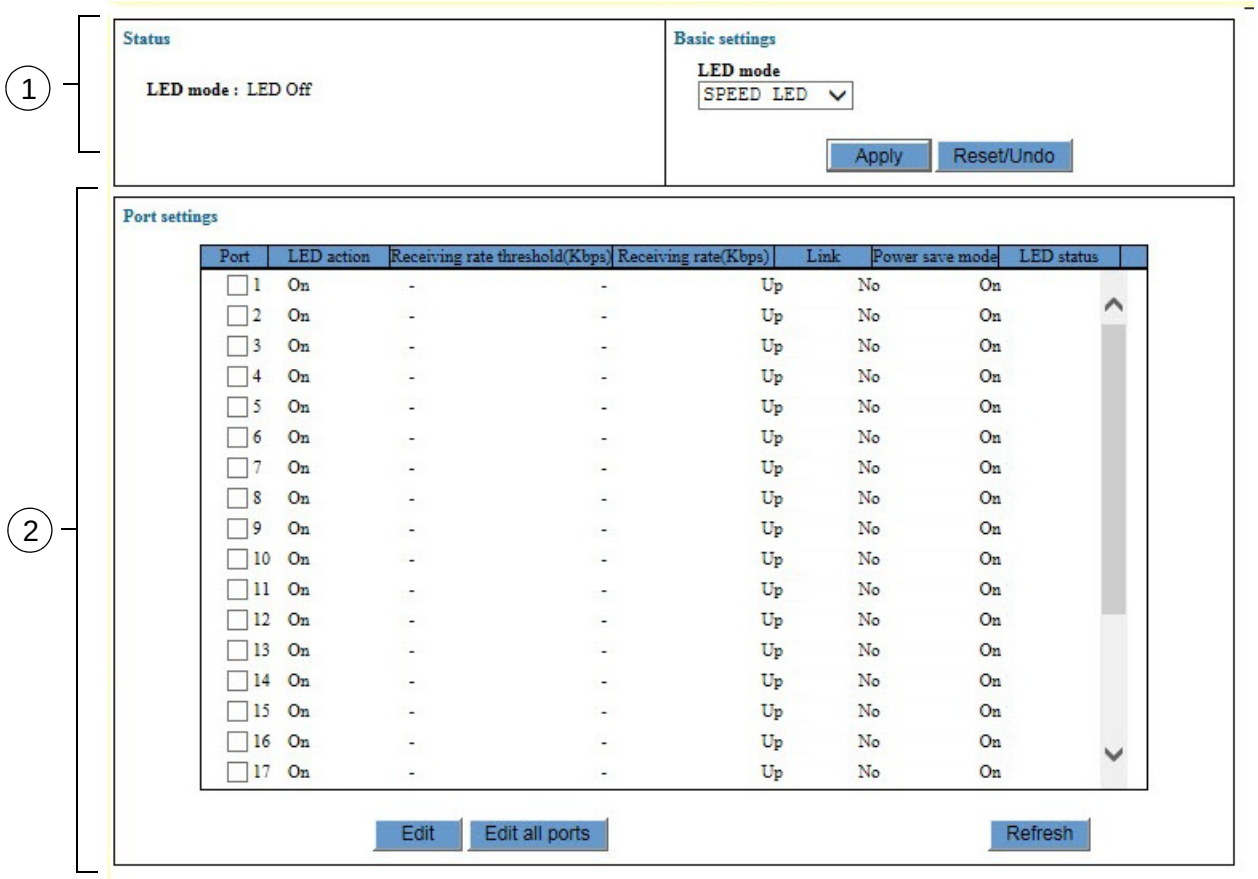

Figure 22. System Settings - LED Window

The sections in the System Settings - Log window are described in Table 27 on page 97.

Table 27. System Settings - Log Window

Section	Description
1	Use the pull-down menu in this section to control the mode of the Speed/Duplex Mode LEDs. The menu performs the same function as the LED Mode button on the front panel of the switch. Refer to “Setting the Mode of the Speed/Duplex Mode LEDs” on page 98.
2	Use the options in this table to set ingress threshold levels for the Link/Activity LEDs. Refer to “Setting the Traffic Thresholds for the Link/Activity LEDs” on page 99.

Setting the Mode of the Speed/Duplex Mode LEDs

The ports on the switch have two LEDs. The Link/Activity LEDs display the link and activity status of the ports and the Speed/Duplex Mode LEDs display the speed or duplex modes. The Speed/Duplex Mode LED can reflect either the speed or duplex mode of its port, but not both at the same time. To toggle the Speed/Duplex Mode LEDs between the modes, you may use the LED mode button on the front panel of the switch or the System Settings - LED window in the management software.

To toggle the modes of the Speed/Duplex Mode LEDs on the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Port LED option from the System Settings menu.

   The System Settings - Port LED window is shown in Figure 22 on page 96.

3. To configure the LED mode of the Speed/Duplex Mode LEDs, use the LED Mode pull-down menu in the Basic Settings section of the window.

   The LED Mode pull-down menu has the following options:

   - ❒ Speed LED - Sets the Speed/Duplex Mode LEDs to display port speeds. This is the default setting.
   - ❒ Duplex LED - Sets the Speed/Duplex Mode LEDs to display the duplex modes of the ports.
   - ❒ LED Off - Turns off the Link/Activity and Speed/Duplex Mode LEDs.

   Note
   Changing the mode of the LEDs does not affect the performance of the ports.

4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Setting the Traffic Thresholds for the Link/Activity LEDs

The Link/Activity LEDs are usually used to view the link and activity status of the ports on the switch. But you can also configure the Link/Activity LED of a port to turn off if the ingress traffic falls below a defined threshold level for about thirty seconds. The LED remains off even if the traffic exceeds the threshold again. You might find this feature useful in identifying ports that periodically experience low traffic.

There is, however, one pre-condition to using this feature. You have to turn off all of the Speed/Duplex Mode LEDs. The switch cannot automatically turn off the Link/Activity LEDs if the Speed/Duplex Mode LEDs are on.

To configure the ingress traffic thresholds for the Link/Activity LEDs, perform the following procedure:

1. Expand the System Settings menu in the main menu.

2. Select the Port LED option from the System Settings menu.

   The System Settings - Port LED window is shown in Figure 22 on page 96.

3. Select the LED Off setting for the LED Mode pull-down menu in the Basic Settings section of the window.

   This step turns off all of the port LEDs on the switch.

   In the Port Settings portion of the window, click the dialog box of the port you want to configure. You may configure more than one port at a time.

4. Click the Edit button. To configure all of the ports on the switch, click the Edit All Ports button.

   The switch displays the Port LED - Port Settings window shown in Figure 23 on page 100.

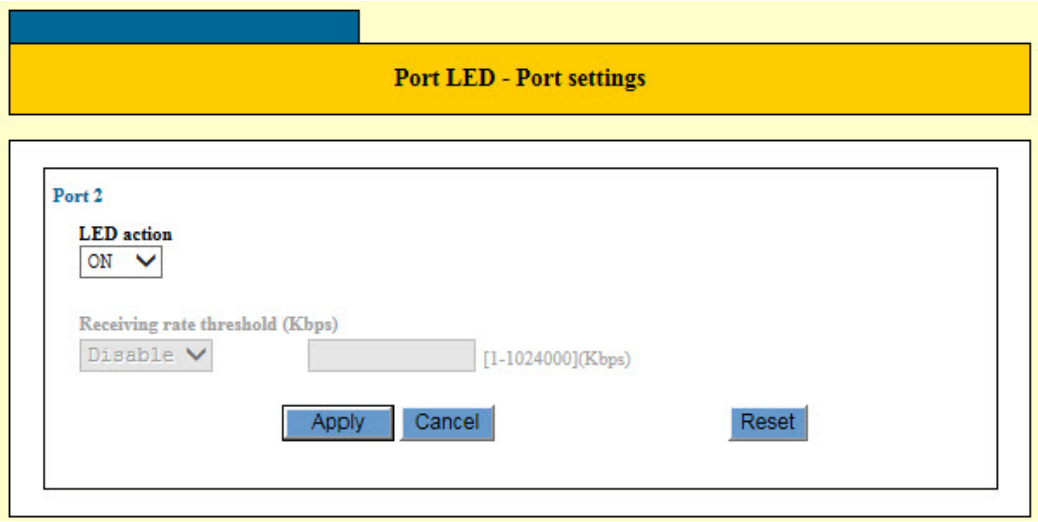

Figure 23. Port LED - Port Settings Window

5. Set the LED Action pull-down menu to Off.
6. Set the Receiving Rate Threshold (Kbps) pull-down menu to Enable.
7. Click the field and enter the ingress traffic threshold in Kbps. The range is 1 to 1024000 Kbps.

   The switch turns off the Link/Activity LED of the port if the ingress traffic drops below the specified threshold for about 30 seconds.

   To turn on the LEDs of ports that have been turned off by this feature, change to LED mode on the switch with the LED mode button on the front panel or with the instructions in “Setting the Mode of the Speed/ Duplex Mode LEDs” on page 98.
8. Click the Apply button to activate your changes on the switch.
9. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 9

SNMPv1 and SNMPv2c

This chapter explains how to activate SNMP management on the switch and create, modify, or delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

Introduction

The Simple Network Management Protocol (SNMP) is another way for you to monitor and configure the switch. This method lets you view and change the individual objects in the Management Information Base (MIB) in the management software on the switch, without having to use the command line commands or the web browser windows.

The switch supports SNMPv1 and SNMPv2c. Here are the main steps to using SNMP:

- Assign a management IP address to the switch. For instructions, refer to “Changing the IP Address Configuration” on page 48.
- Activate SNMP management on the switch. The default setting is disabled.
- Create one or more community strings.
- Load the Allied Telesis MIBs for the switch onto your SNMP management workstation. The MIBs are available from the Allied Telesis web site at www.alliedtelesis.com.

Displaying the SNMP Window

The SNMP window is used to enable or disable SNMP on the switch and to manage community strings. When SNMP is enabled, you can manage the unit remotely using SNMP clients on your manager workstations. The switch also sends SNMP traps to alert you of events.

To display the SNMP window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the SNMP option from the System Settings menu.

   The System Settings - SNMP window is shown in Figure 24.

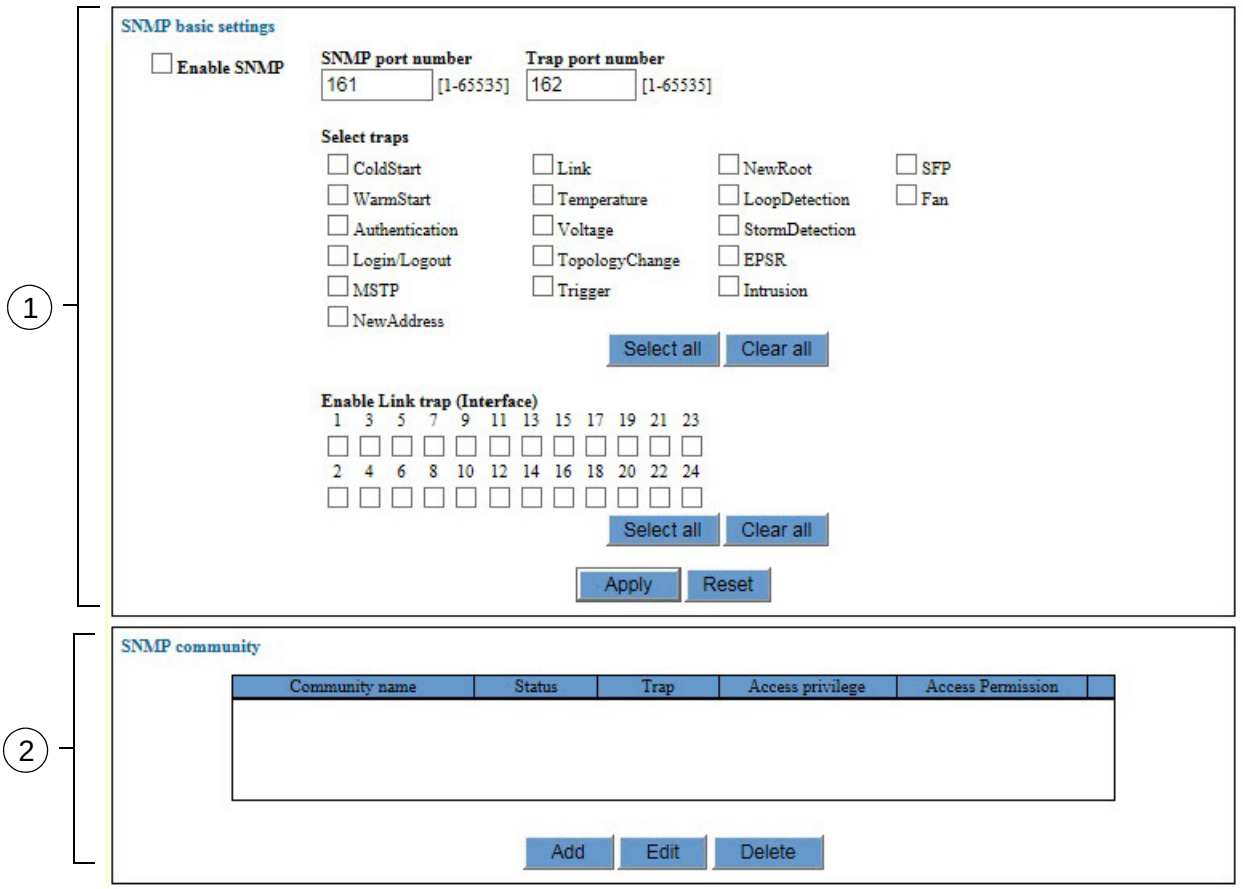

Figure 24. System Settings - SNMP Window

The sections in the window are described in Table 28 on page 104.

Table 28. SNMP Window

Section	Description
1	Use this section to perform the following SNMP configuration tasks: Enable or disable SNMP Set the listening ports for get and set actions, and for traps. Select the traps. Enable or disable link traps on the individual ports.
2	Use this section to view the current communities or to add or delete communities.

The SNMP Community table at the bottom of the window displays the current communities on the switch. The columns in the table are described in Table 29.

Table 29. SNMP Community Table

Column	Description
Community Name	Displays the community name.
Status	Displays the status of the community string. The possible states are listed here: Enabled - Network managers may use the community string to manage the switch. Disabled - Network managers may not use the community string.
Trap	Displays whether the status of the traps of the community string. The possible states are listed here: Enabled - The community string can send traps. Disabled - The community string cannot send traps.

Table 29. SNMP Community Table (Continued)

Column	Description
Access Privilege	Displays the access modes of the community. The access modes are listed here: Read-only - The community string may be used to view but not change the values of the MIBs on the switch. Read-write - The community string may be used to view and change the values of the MIBs on the switch.
Access Permissions	Displays the access status of the community string. The status are listed here: Yes - The community has an open status. Any management workstation can use it. No - The community string has a closed status. It can be used only by those workstations whose IP addresses are assigned to it.

Configuring Basic SNMP Parameters

To configure the basic parameters of SNMP on the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the SNMP option from the System Settings menu.

   The SNMP page is shown in Figure 24 on page 103.
3. Configure the parameters in the SNMP Basic Settings section of the window. The parameters are described in Table 30.

Table 30. SNMP Basic Settings

Parameter	Description
Enable SNMP	Use this parameter to enable or disable SNMP on the switch. SNMP is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
SNMP Port Number	Use this parameter to set the UDP port number for SNMP. The range is 1 to 65535 and the default is 161.
Trap Port Number	Use this parameter to set the UDP port number for SNMP traps. The range is 1 to 65535 and the default is 162.
Select Traps	Use this section to select the traps that the community strings are permitted to send. A trap is enabled when its dialog box has a check mark and disabled when the dialog box is empty. The default is no selected traps.
Enable Link Trap (Interface)	Use this section to select ports for link traps. The switch sends link traps when there are changes to the link states on the designated ports.

4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding New SNMP Community Strings

To add new SNMP community strings, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the SNMP option from the System Settings menu.

   The System Settings - SNMP page is shown in Figure 24 on page 103.
3. Click the Add button at the bottom of the window.

   The SNMP Community - Add window is shown in Figure 25.

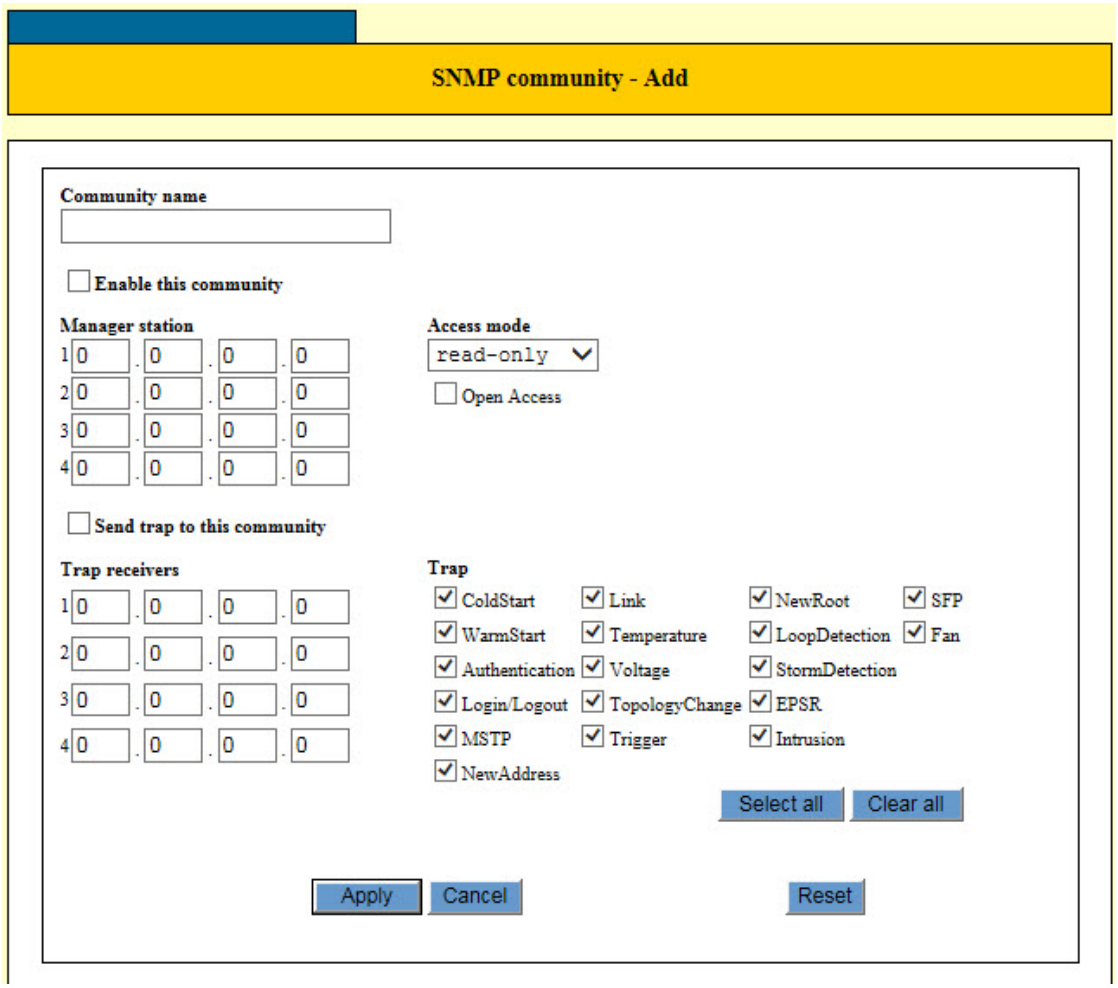

Figure 25. SNMP Community - Add Window

4. Configure the parameters in the window for the new community. The parameters are described in Table 31,

Table 31. SNMP Community - Add Window

Parameter	Description
Community Name	Use this field to enter a name for the new community string. The name can be up to 32 alphanumeric characters. No spaces or special characters (such as /, #, or &) are allowed.
Enable this Community	Use this dialog box to either enable or diable the community. The community is enabled when the box has a check mark and disabled when the box is empty.
Manager Stations	Use these fields to specify the IP addresses of up to four management workstations for a community with a closed access. (See Open Access parameter.) A community with a closed status can only be used by the management workstations listed here. Entering manager IP addresses for a community string with an open status has no affect on the string.
Access Mode	Use this pull-down-menu to specify the access mode of the SNMP community. The access modes are listed here: Read-only - The community string may be used to view but not change the values of the MIBs on the switch. Read-write - The community string may be used to view and change the values of the MIBs on the switch.
Open Access	Use this parameter to set the community string as opened or closed. If there is no check in the dialog box next to the option, the community string is closed; only those workstations whose IP addresses are assigned to the community string can use it. If there is a check in the box, the string is open, meaning any SNMP management workstation can use it to access the switch.

Table 31. SNMP Community - Add Window (Continued)

Parameter	Description
Send Trap to this Community	Use this dialog box to control whether the switch can use the community to send traps. Trap transmission is allowed when the dialog box has a check mark and not allowed with the box is empty.
Trap Receivers	Use these fields to enter the IP addresses of up to four trap receivers. These are nodes on your network, such as management workstations, to act as trap receivers for the switch.
Traps	Use these fields to specify the traps the switch is to send using the community. A trap is enabled when its dialog box has a check mark and disabled when its box is empty. The traps selected in this window must also be selected in the System Settings - SNMP window, shown in Figure 24 on page 103

5. After configuring the new community, click the Apply button to activate your changes on the switch.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying SNMP Communities

To modify an SNMPv1 and SNMPv2c community, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the SNMP option from the System Settings menu.

   The System Settings - SNMP page is shown in Figure 24 on page 103.
3. In the table of communities at the bottom of the window, click the dialog box next to the community you want to modify. You can modify only one community at a time.
4. Click the Edit button.

   The settings of the selected SNMP community string are displayed in the SNMP Community - Edit window.
5. Modify the parameters as needed. The parameter are defined in Table 31 on page 108. You cannot change the community name.
6. After modifying the community, click the Apply button to activate your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting SNMP Communities

To delete an SNMP community, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the SNMP option from the System Settings menu.

   The System Settings - SNMP window is shown in Figure 24 on page 103.
3. In the table of communities at the bottom of the window, click the dialog box next to the community you want to delete. You can delete only one community at a time.
4. Click the Delete button.

   A confirmation prompt is displayed.
5. Click the OK button.

   The community string is deleted from the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 10

Port Parameters

This chapter explains how to view or adjust the parameter settings of the individual ports on the switch. Examples of the parameters include port speeds and duplex modes.

This chapter contains the following procedures:

Displaying the Port Parameters Window

The operating parameters of the individual ports on the switch are viewed and configured from the Switch Settings - Port window. To display the window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Port option from the Switch Settings menu.

   The Switch Settings - Port window is shown in Figure 26.

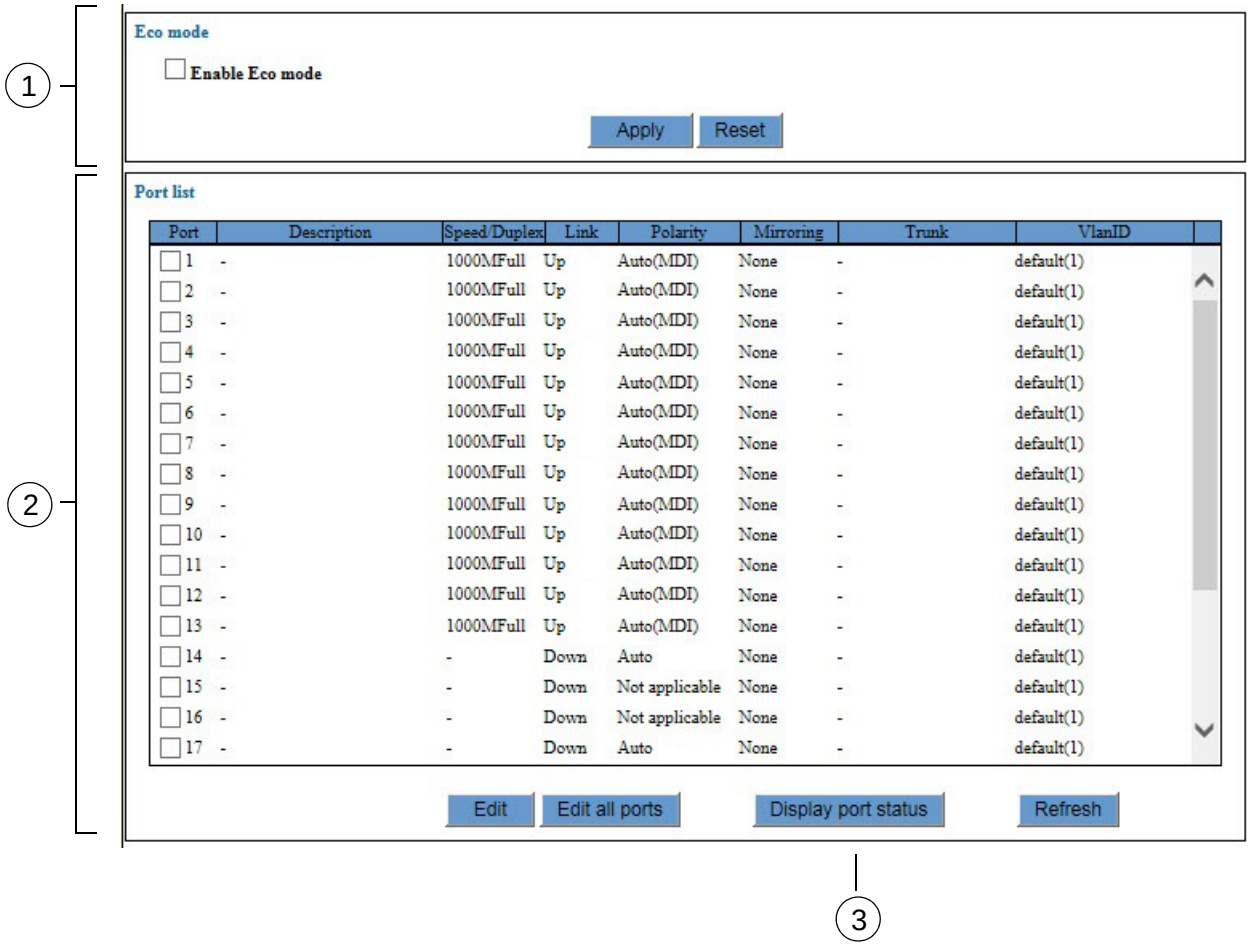

Figure 26. Switch Settings - Port Window

The sections in the window are described in Table 32 on page 115.

Table 32. Switch Settings - Port Window

Section	Description
1	Use the option in this section of the window to enable or disable the power saving mode on the switch. For instructions, refer to “Enabling or Disabling the Power Saving Mode” on page 117.
2	Use this section to view or configure the port parameters. Refer to “Configuring Port Parameters” on page 118.
3	Use this button to view the port configurations. Refer to “Displaying Port Configurations” on page 124.

The current operational settings of the ports are displayed in the Port List table in the window. The columns in the table are described in Table 33.

Table 33. Port List Table in the Switch Settings - Port Window

Column	Description
Port	Displays the port number.
Description	Displays the description of the port.
Speed/Duplex	Displays the current speed and duplex mode of the port.
Link	Displays the link status of a port. The possible states are listed here: Up - A port has established a link to a network device. Down - A port has not established a link to a network device or the port was disabled with the Disable (Down) link state. Here are a couple points to know about this status. - A port that is in the spanning tree discarding state will have an Up status. - A port that was disabled with the Enable (Up) link state will also have an Up status.
Polarity	Displays the current MDI state of a port.

Table 33. Port List Table in the Switch Settings - Port Window (Continued)

Column	Description
Mirroring	Displays whether a port is a member of a port mirror. For background information, refer to Chapter 13, “Port Mirroring” on page 147. The possible states are listed here: None - A port is not a member of a port mirror. Mirror - A port is the mirror port. The switch is copying the traffic from the source ports to this port. The switch can have only one mirror port. Rx - A port is a source port of the port mirror. The switch is copying its ingress traffic to the mirror port. Tx - A port is a source port of the port mirror. The switch is copying its egress traffic to the mirror port. Both - A port is a source port of the port mirror. Its ingress and egress traffic are being copied to the mirror port.
Trunk	Displays the name of a port trunk if a port is a trunk member. The column is empty if the port is not a member of a port trunk. For background information, refer to Chapter 14, “Static Port Trunks” on page 153.
VlanID	Displays the name and VID of the VLAN where a port is an untagged member.

Enabling or Disabling the Power Saving Mode

The power saving mode reduces the overall power usage of the unit by decreasing the amount of power the switch provides to ports that have not established links to network devices. Please review the following information before using this feature:

- This feature is activated at the switch level. You may not enable it on individual ports.
- The feature does not affect the network operations of the ports.
- When the feature is enabled on the switch, ports may take up to three seconds to initially establish links with network devices.

To enable or disable the power saving mode, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Port option from the Switch Settings menu.

   The Switch Settings- Port window is shown in Figure 26 on page 114.
3. Click the Enable Eco Mode dialog box at the top of the window to enable or disable the power saving mode on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
4. Click the Apply button to activate your change on the switch.
5. To permanently save your change in the configuration file, click the Save button above the main menu.

Configuring Port Parameters

To configure the parameter settings of the ports on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Port option from the Switch Settings menu.

   The Switch Settings - Port window is shown in Figure 26 on page 114.
3. To configure the settings of a port, click its dialog box to add a check mark. You may configure more than one port at a time.

   Note
   Do not configure twisted pair and fiber optic ports at the same time.

4. Click the Edit button. To configure all of the ports, click the Edit All Ports button.

   The switch displays the Port Settings window. Refer to Figure 27.

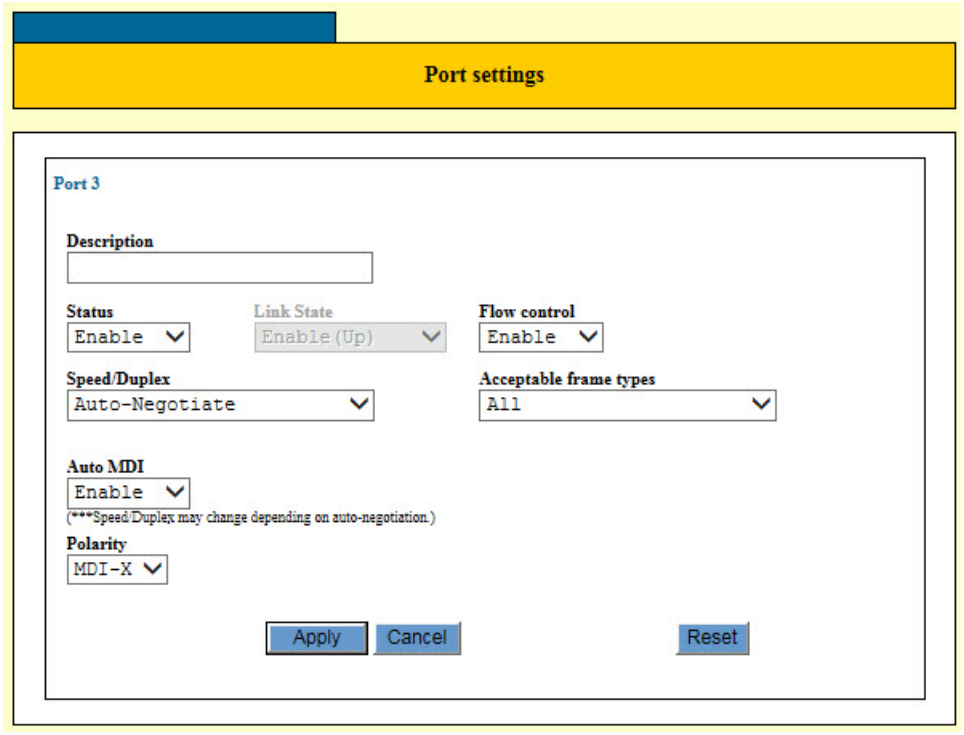

Figure 27. Port Settings Window

Note
The window displays the current settings of a port if you are configuring only one port. If you are configuring more than one port, the window displays the default port values.

Note
The Port Settings window in the figure is from a 10/100/1000 Mbps twisted pair port. The window for a fiber optic port will contain a subset of the parameters.

5. Configure the port parameters, as needed. Refer to Table 34.

Table 34. Port Settings Window

Parameter	Description
Description	Use this parameter to assign a name to a port. A name can be from 1 to 20 alphanumeric characters. Spaces are allowed in a name, but not special characters, such as asterisks or exclamation points.
Status	Use this selection to enable or disable a port. A disabled port does not accept or forward frames. You might disable a port to secure it from unauthorized use if it is unused, or if there is a problem with the cable or network device. The possible settings are listed here: Enabled - The port forwards ingress and egress packets. This is the default setting. Disabled - The port does not forward any ingress or egress packets.

Table 34. Port Settings Window (Continued)

Parameter	Description
Link State	Use this option to control the link status of a disabled port. This option is only available when a port is disabled with the Status option. The possible options are listed here: Enable (Up) - The port stops forwarding network packets but the link remains up. Disable (Down) - The port stops forwarding network packets and drops the link.
Speed/Duplex	Use this parameter to set the speed and duplex mode of a port. You may select Auto-Negotiation so that a port sets its speed and duplex mode automatically or you may manually select the appropriate speed and duplex mode from the list of settings. For further information, please refer to “Setting the Speed and Duplex Mode” on page 122.
Auto MDI	Use this parameter to enable or disable Auto MDI. When Auto MDI is enabled on a port, the MDI/MDIX wiring configuration is set automatically. When Auto MDI is disabled, you may use the Polarity parameter to manually set the wiring configuration. For more information, refer to “Setting the Wiring Configuration” on page 123. This parameter is not available on the combo twisted pair ports.
Polarity	Use this parameter to set the wiring configuration of a port when Auto MDI is disabled. The selections are MDI and MDIX. This parameter is not available on the combo twisted pair ports.

Table 34. Port Settings Window (Continued)

Parameter	Description
Flow Control	Use this parameter to set the flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses flow control to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames when a port's ingress buffers are full. The pause packet notifies the end node to stop transmitting for a specified period of time. The possible settings are listed here: Enabled - Enables flow control on a port. Disabled - Disables flow control on a port. This is the default.
Acceptable Frame Types	Use this parameter to control whether a port accepts untagged packets as well as tagged packets. For background information on untagged and tagged packets, refer to "Port-based and Tagged VLANs Overview" on page 177. The possible settings are listed here: All - The port forwards both ingress tagged and untagged packets. Tagged Packets Only - The port accepts ingress tagged packets and discards untagged packets.

Table 34. Port Settings Window (Continued)

Parameter	Description
Combo Port	Use this parameter to specify the priorities of the twisted pair port and SFP slot of the combo ports. This parameter is only available on the combo ports. The possible settings are listed here: Fiber-Auto - The SFP slot is the primary port and the twisted pair port is the secondary port if both ports of the combo pair are connected to active network devices. The twisted pair port transmits packets only when the SFP slot does not have a link to a network device. Copper-Auto - The twisted pair port is the primary port and the SFP slot is the secondary port if both ports of the combo pair are connected to active network devices. The SFP slot transmits packets only when the twisted pair port does not have a link to a network device. Fiber - Only the SFP slot is active. The twisted pair port is inactive. Copper - Only the twisted pair port is active. The SFP slot is inactive.

6. Click the Apply button to activate your changes on the switch.

7. To permanently save your change in the configuration file, click the Save button above the main menu.

Setting the Speed and Duplex Mode

The Speed/Duplex parameter is used to set the speed and duplex mode of a port. You may set the speed and duplex mode manually or activate the Auto-Negotiation feature so that the switch sets the parameters automatically. Here are a few guidelines to setting the speed and duplex mode of the ports:

- The default speed setting for the ports is Auto-Negotiation. This setting is appropriate for ports connected to network devices that also support Auto-Negotiation.
- The default speed setting of Auto-Negotiation is not appropriate for ports connected to 10/100Base-TX network devices that do not support Auto-Negotiation and have fixed speeds. For those switch

ports, you should disable Auto-Negotiation and set the port's speed manually to match the speeds of the network devices.

- The 10/100/1000Base-T ports must be set to Auto-Negotiation, the default setting, to operate at 1000Mbps.
- The default duplex mode setting for the ports is Auto-Negotiation. This setting is appropriate for ports connected to network devices that also support Auto-Negotiation for duplex modes.
- The default duplex mode setting of Auto-Negotiation is not appropriate for ports connected to network devices that do not support Auto-Negotiation and have fixed duplex modes. You should disable Auto-Negotiation on those ports and set their duplex modes manually to avoid the possibility of duplex mode mismatches. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation, which can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

Setting the Wiring Configuration

Please review the following guidelines for setting the Auto MDI parameters:

- The default setting for the wiring configurations of the ports is Auto MDI. The default setting is appropriate for switch ports that are connected to 10/100Base-TX network devices that also support auto-MDI/MDI-X.
- You should not use the default Auto MDI setting on switch ports that are connected to 10/100Base-TX network devices that do not support auto-MDI/MDI-X and have a fixed wiring configuration. You should disable Auto MDI on switch ports that are connected to network devices with fixed wiring configurations, and manually set the wiring configurations.
- The appropriate MDI/MDI-X setting for a switch port connected to a 10/100Base-TX network device with a fixed wiring configuration depends on the setting of the network device and whether the switch and network device are connected with straight-through or crossover cable. If you are using straight-through twisted pair cable, the wiring configurations of a port on the switch and a port on a network device must be opposite each other, such that one port uses MDI and the other MDI-X. For example, if a network device has a fixed wiring configuration of MDI, you must disable auto-MDI/MDI-X on the corresponding switch port and manually set it to MDI-X. If you are using crossover twisted pair cable, the wiring configurations of a port on the switch and a port on a network device must be the same.

Displaying Port Configurations

To display the configurations of the ports on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Port Settings option from the Switch Settings menu.The Switch Settings - Port window is shown in Figure 26 on page 114.
3. Click the dialog box of a port. You may view the parameters of only one port at a time.
4. Click the Display Port Status button.

   An example of the window is shown in Figure 28.

Figure 28. Display Port Status Window

The parameters in the window are described in Table 35.

Table 35. Display Port Status Window

Parameter	Description
Description	Displays the port description.
Status	Displays whether the port is enabled or disabled. The possible states are listed here: Enabled - The port can forward ingress and egress packets. Disabled - The port cannot forward ingress or egress packets.
Link State	Displays the current status of the port link.
Configured Speed/Duplex	Displays the configured speed and duplex mode of the port.
Port Speed	Displays the actual speed of the port.
Up Time	Displays the amount of time the link on the port has been up.
Port Media Type	Displays the media type, which for twisted pair ports is Ethernet CSMA/CD.
Port Type	Displays the port type.
Auto MDI	Displays whether Auto MDI is enabled or disabled.
Port Polarity	Displays the actual MDI/MDIX setting.
Broadcast, Unknown unicast, and Multicast Rate Limits	Displays the packet rate limits. For background information, refer to Chapter 12, “Packet Storm Protection” on page 141.

Table 35. Display Port Status Window (Continued)

Parameter	Description
Acceptable Frame Types	Displays whether a port is accepting both tagged and untagged packets or only tagged packets. The possible states are listed here: Acceptable All Frames - The port is accepting both tagged and untagged packets. Admit Only VLAN-tagged Frames - The port is accepting only tagged packets.
Acceptable Frame Types (Continued)	For background information on untagged and tagged packets, refer to “Port-based and Tagged VLANs Overview” on page 177.
Security Mode	Displays the security mode of the port. For background information, refer to Chapter 37, “MAC Address-based Port Security Overview” on page 447.
Mirroring	Displays whether the port is a source port of a port mirror. For background information, refer to Chapter 13, “Port Mirroring” on page 147.
Mirror Port	Displays whether the port is acting as a port mirror. For background information, refer to Chapter 13, “Port Mirroring” on page 147.
Enabled Flow Control	Displays whether flow control is enabled on a port. This option only applies to ports operating in full-duplex mode. The possible states are listed here: - - Flow control is not enabled or the port is not connected to an active network device. Pause - Flow control is enabled.

Table 35. Display Port Status Window (Continued)

Parameter	Description
Trunk Group	Displays the name of the trunk group to which the port belongs. This field will be empty if the port is not a member of a trunk group. For background information, refer to Chapter 14, "Static Port Trunks" on page 153.
Tagged VLANs	Displays the VIDs of the VLANs where the port is a tagged member. For background information, refer to Chapter 16, "Port-based and Tagged VLANs Overview" on page 177.
Port-based VLAN ID	Displays the name and VID where the port is an untagged member. For background information, refer to Chapter 16, "Port-based and Tagged VLANs Overview" on page 177.
Ingress Filtering	Displays whether ingress filtering is enabled or disabled. Ingress filtering controls whether tagged ports accept or reject tagged packets whose VIDs do not match the VLANs to which the ports are members. The possible states are listed here: Off: Ingress filtering is disabled. On: Ingress filtering is enabled. To set this parameter, refer to "Displaying the VLAN Window" on page 194.
Port Priority	Displays the priority value assigned to ingress untagged packets on the port. For instructions on how to set the parameter, refer to "Setting the Priority Values for Ingress Untagged Packets" on page 230.

Chapter 11

MAC Address Table

This chapter contains instructions on how to view the MAC addresses in the MAC address table and add or delete static addresses. This chapter contains the following procedures:

Displaying the MAC Address Window

To display the MAC Address window, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the FDB option from the Device Monitoring menu. (FDB is an acronym for “forwarding database,” which is another name for the MAC address table.)

   The Device Monitoring - FDB window is shown in Figure 29.

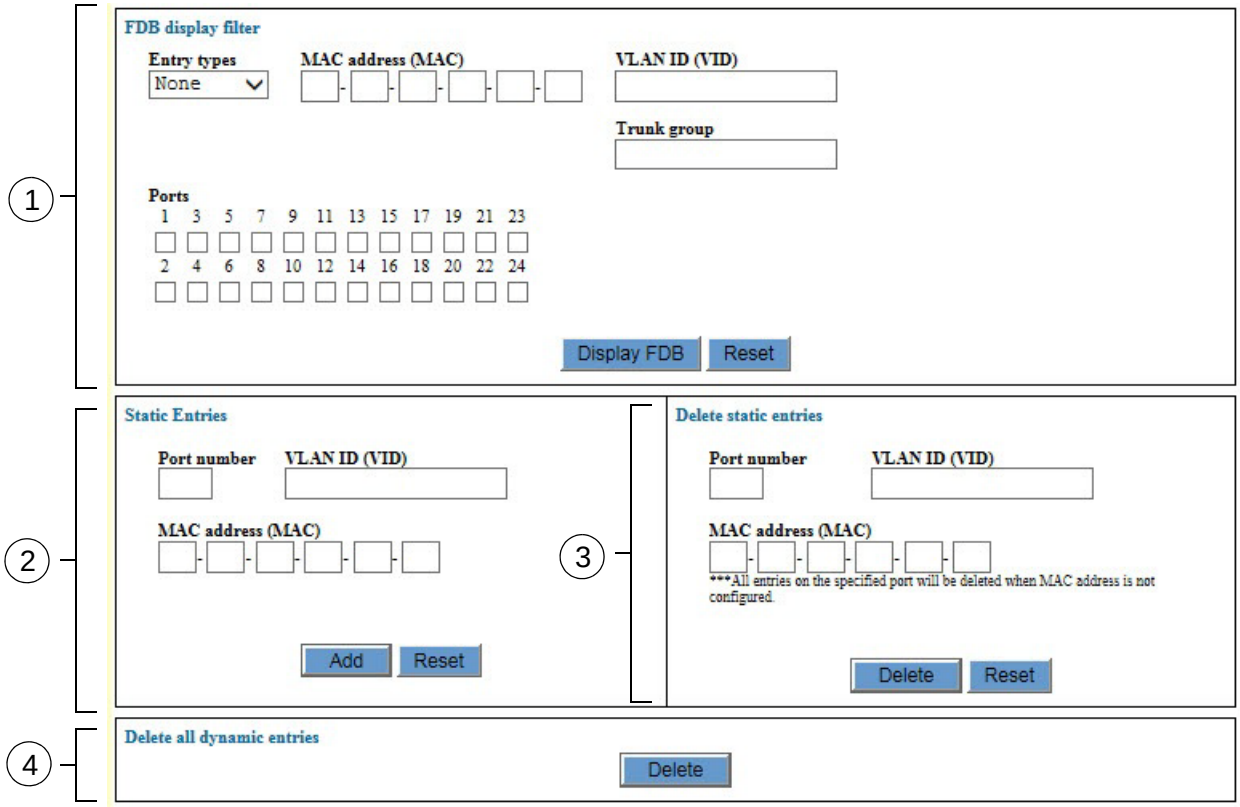

Figure 29. Device Monitoring - FDB Window

The sections in the window are described in Table 36.

Table 36. Device Monitoring - FDB Window

Section	Description
1	Use this section to display the MAC addresses in the MAC address table. For instructions, refer to “Displaying the MAC Address Table” on page 132.

Table 36. Device Monitoring - FDB Window (Continued)

Section	Description
2	Use this section to add static MAC addresses to the switch. For instructions, refer to “Adding Static Unicast MAC Addresses” on page 135.
3	Use this section to delete static MAC addresses from the switch. For instructions, refer to “Deleting Static Unicast Addresses” on page 136
4	Use the button in this section to delete all of the dynamic MAC addresses from the MAC address table. For instructions, refer to “Deleting All of the Dynamic MAC Addresses” on page 137.

Displaying the MAC Address Table

To view the addresses in the MAC address table, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the FDB option from the Device Monitoring menu.

   The Device Monitoring - FDB window is shown in Figure 29 on page 130. The options for viewing the MAC addresses in the table are located in the top section of the window, labelled FDB Display Filter.
3. Do one of the following:
   - ❒ To view all of the addresses in the table, leave the filter options at the default settings and click the Display FDB button in the top section of the window.
   - ❒ To filter the table for specific MAC addresses, configure the parameters in the top section of the window and then click the Display FDB button. The parameters are described in Table 37.

Table 37. FDB Display Filter

Parameter	Description
Entry Types	Use the options in this pull-down menu to display categories of MAC addresses. The options are listed here: None - Disables this filter. Static - Displays static addresses. Dynamic - Displays dynamic addresses. Discard - Displays the MAC addresses of nodes that were denied entry to the switch.
MAC Address MAC	Use this option to enter a specific MAC address. You might use this option to learn the port on which the switch has learned a particular address. You may enter only one MAC address at a time.

Table 37. FDB Display Filter (Continued)

Parameter	Description
VLAN Name (ID)	Use this option to view the MAC addresses the switch has learned on the ports of a particular VLAN. You may identify the VLAN by its name or VID. You can enter only one VLAN at a time. To view the VLANs on the switch, refer to "Displaying the VLAN Window" on page 194.
Trunk Group	Use this option to view the MAC addresses the switch has learned on the ports of a port trunk. You identify the trunk by its name. You may specify only one port trunk at a time. To view the trunks on the switch, refer to "Creating a Port Trunk" on page 156.
Ports	Use the options in this section to view the MAC addresses the switch has learned on specific ports. You may view the MAC addresses of more than one port at a time. A port is selected when its dialog box has a check mark and not selected when its dialog box is empty.

An example of the table is shown in Figure 30 on page 134.

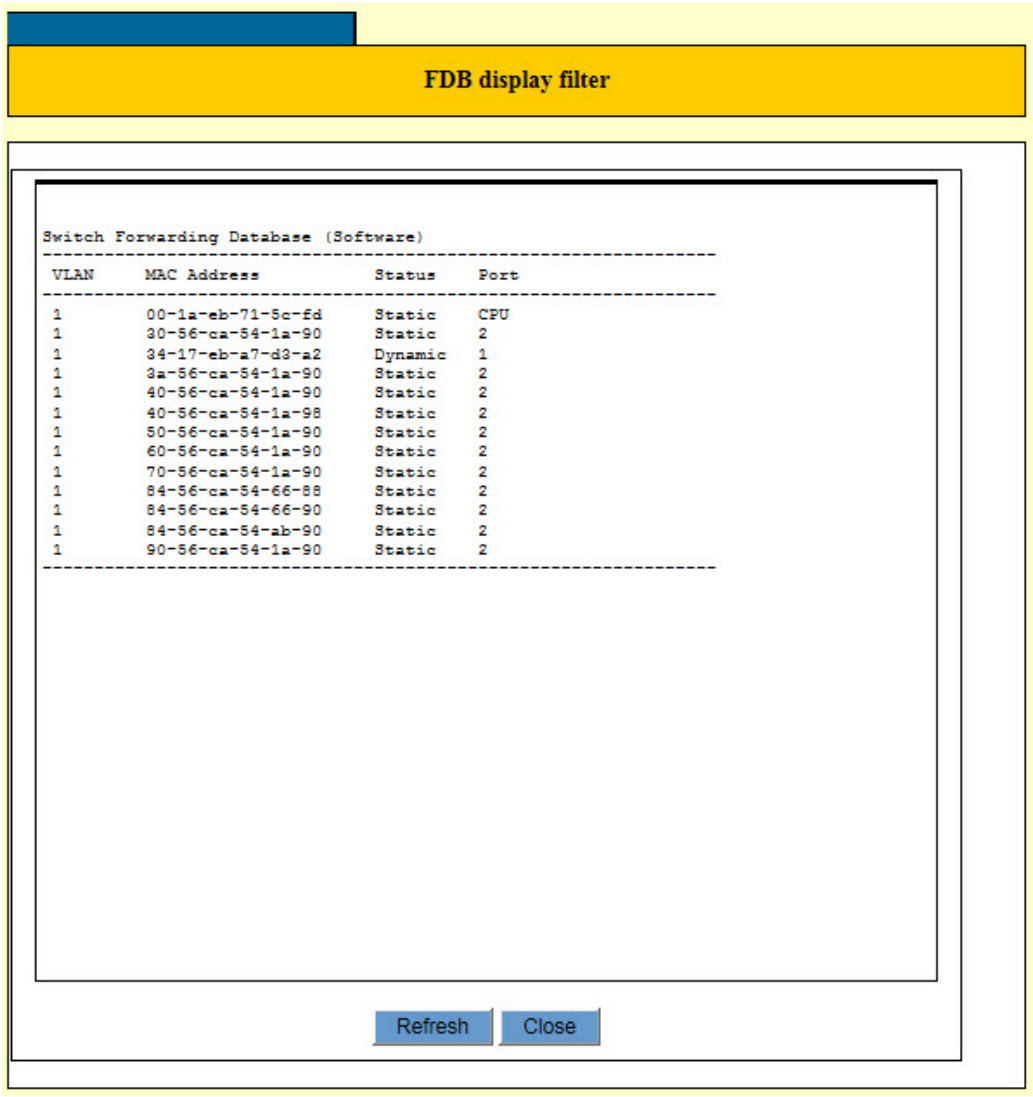

Figure 30. FDB Display Filter Window

Adding Static Unicast MAC Addresses

The section contains the procedure for adding static unicast MAC addresses to the address table.

Note
You may not add static multicast MAC addresses.

To add static unicast MAC addresses to the MAC address table in the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the FDB option from the Monitoring menu.

   The Device Monitoring - FDB window is shown in Figure 29 on page 130.

3. Configure the parameters in the Static Entries section of the window, as needed. The variables are described in Table 38. Please observe the following guidelines:

   - ❒ You must enter values for all of the parameters in the section.
   - ❒ You may add only one address at a time.

Table 38. Add Static Entry

Parameter	Description
Port Number	Use this option to specify the number of the port on the switch where you want to assign the static address. You can enter only one port number.
VLAN Name	Use this option to specify the VID or name of the VLAN where the port is a member.
MAC Address	Use this option to enter the new static MAC address. You may enter only one address at a time.

4. After configuring the parameters, click the Add button.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting Static Unicast Addresses

To delete static unicast MAC addresses from the address table in the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the FDB option from the Device Monitoring menu.

   The Device Monitoring - FDB window is shown in Figure 29 on page 130. MAC addresses are deleted with the options in the Delete Static Entries section of the window.

3. Do one of the following:

   - To delete all of the static addresses assigned to a port on the switch, enter the port number in the Port Number field and click the Delete button. You may specify only one port at a time.
   - To delete a specific MAC address, enter the port number of the address in the Port Number field and the address in the MAC Address (MAC) field. You do not have to enter the VLAN. Then click the Delete button. You may delete only one address at a time.

4. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting All of the Dynamic MAC Addresses

To delete all of the dynamic MAC addresses from the MAC address table, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the FDB option from the Device Monitoring menu.

   The Device Monitoring - FDB window is shown in Figure 29 on page 130.
3. Click the Delete button in the bottom section of the window.

   The switch does not display a confirmation prompt.

Changing the Aging Timer

This procedure changes the aging timer of the MAC address table. The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. The switch deletes an address from the table if no packets are sent to or received from the address for the duration of the timer. This prevents the table from becoming full of addresses of inactive nodes. The default setting for the aging time is 300 seconds (5 minutes).

To configure the aging time, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Others option from the Switch Settings menu.

   The Switch Settings - Others window is shown in Figure 31

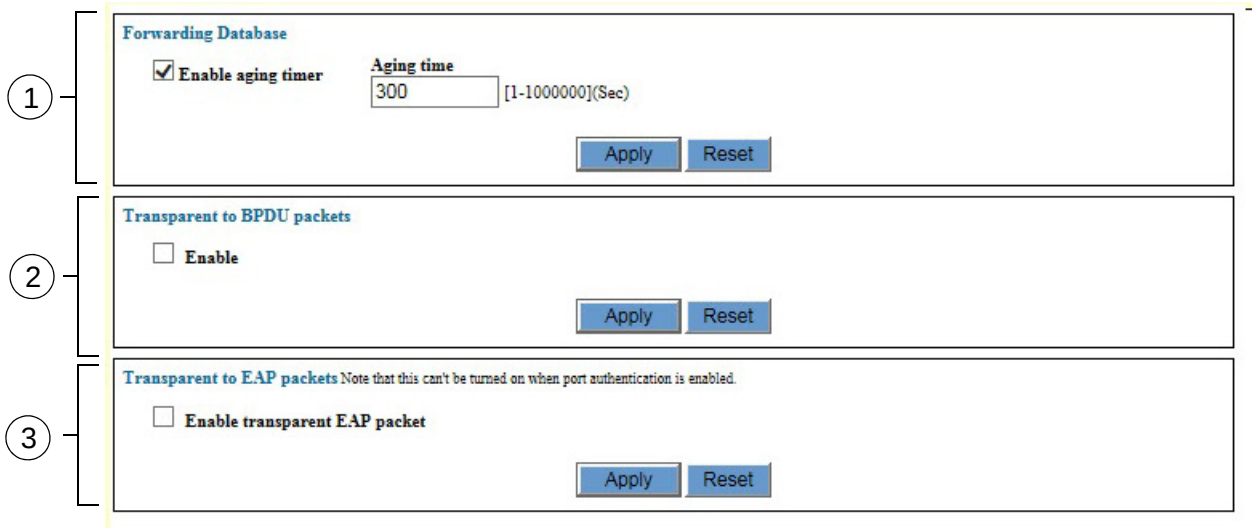

Figure 31. Switch Settings - Others Window

The sections in the window are described in Table 39.

Table 39. Switch Settings - Others Window

Section	Description
1	Use this section to enable or disable the MAC address aging timer or to adjust the timer. This section of the window is explained in this procedure.

Table 39. Switch Settings - Others Window (Continued)

Section	Description
2	Use this option to configure the switch to forward BPDU packets when it is not running RSTP or MSTP. For instructions, refer to "Enabling or Disabling BPDU Transparency for RSTP" on page 315 or "Enabling or Disabling BPDU Transparency for MSTP" on page 360.
3	Use this option to configure the switch to forward EAP packets when it is not running port authentication. For instructions, refer to "Enabling or Disabling EAP Transparency" on page 519.

3. To enable or disable the aging timer, click the dialog box for the Enable Aging Time option.

   The timer is enabled when the dialog box has a check mark and disabled when the dialog box is empty. Disabling the timer means that inactive addresses are never deleted from the table. The switch continues to learn new addresses until the table reaches its maximum capacity.

4. To adjust the aging timer, click the Aging Time field and enter the new value. The range is 1 to 1000000 seconds.

5. Click the Apply button to activate your changes on the switch.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 12

Packet Storm Protection

This chapter contains instructions on how to configure the packet storm protection feature on the switch. The chapter contains the following procedures:

Introduction

The packet storm protection feature allows you to set a threshold for the maximum number of ingress broadcast, multicast, or unknown unicast packets on the ports. Packets above the threshold are discarded by the switch. The switch supports only one threshold setting, which is set in bits per second (bps). However, you may activate packet filtering on the individual ports.

Displaying the Packet Storm Protection Window

To display the packet storm protection window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Protection option from the Switch Settings menu.

   The Switch Settings - Protection window is shown in Figure 32.

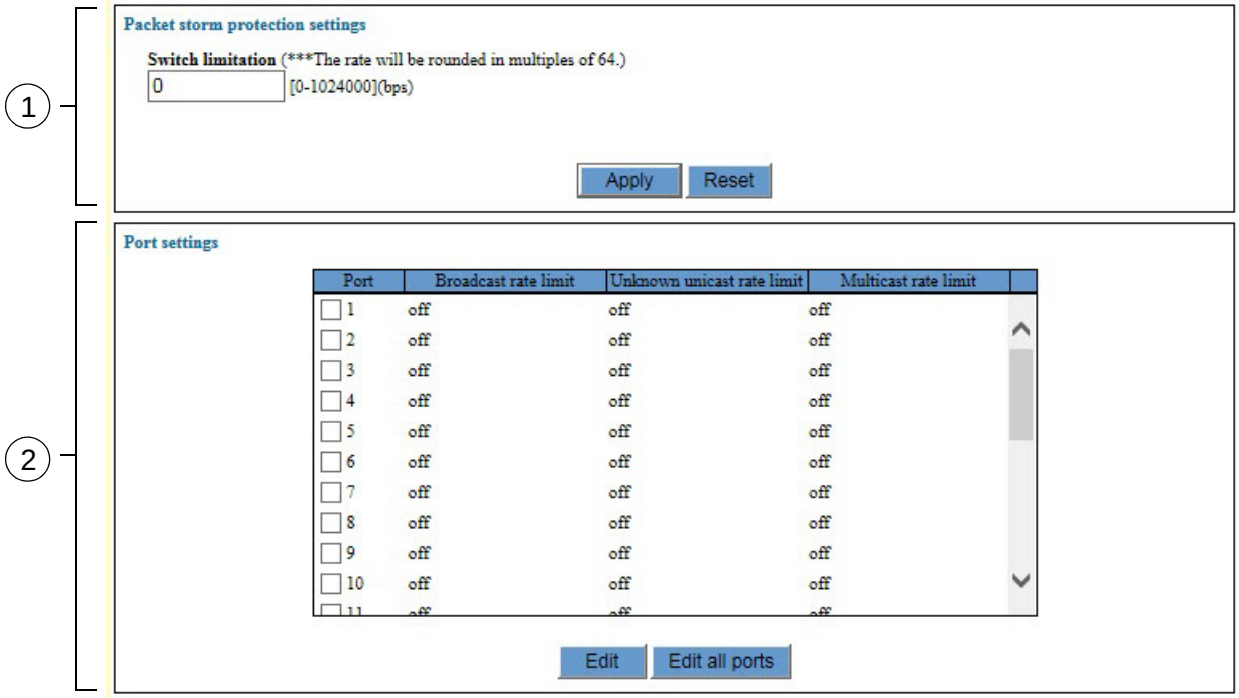

Figure 32. Switch Settings - Protection Window

The sections in the window are described in Table 40.

Table 40. Switch Settings - Protection Window

Section	Description
1	Use this option to set the threshold limit for packet filtering.
2	Use this table to view the current settings of the ports or to enable or disable the feature on the ports. Refer to “Configuring Packet Storm Protection” on page 145.

The columns in the table in the window are defined in Table 41.

Table 41. Port Settings Table in the Switch Settings - Protection Window

Column	Description
Port	Displays the port number.
Broadcast Rate Limit	Displays whether rate limiting for ingress broadcast packets is enabled (on) or disabled (off) on the port.
Unknown Unicast Rate Limit	Displays whether rate limiting for ingress unknown unicast packets is enabled (on) or disabled (off) on the port. An unknown unicast packet is a packet with a destination MAC address that is not listed in the MAC address table.
Multicast Rate Limit	Displays whether rate limiting for ingress multicast packets is enabled (on) or disabled (off) on the port.

Configuring Packet Storm Protection

To configure packet storm protection, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Protection option from the Switch Settings menu.

   The Switch Settings - Protection window is shown in Figure 32.
3. To adjust the threshold packet limit, click the Switch Limitation field and enter a new value. The range is 0 to 1024000 bps. The switch automatically rounds your value to a multiple of 64 bps.
4. To enable or disable packet storm protection on a port, click its dialog box in the Port Settings table. You may configure more than one port at a time.
5. Click the Edit button. To configure all of the ports, click the Edit All Ports button.

   The switch displays the Packet Storm Protection Settings Window for the selected port, shown in Figure 33.

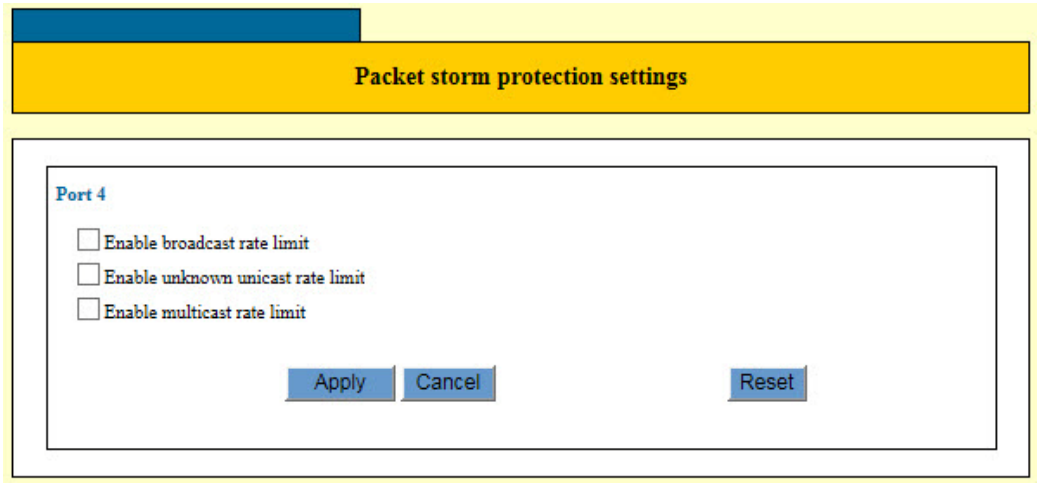

Figure 33. Packet Storm Protection Settings Window

6. Click the dialog boxes of the filters to enable or disable the feature on the port. A filter is enabled when its dialog box has a check mark and disabled when the dialog box is empty.
7. Click the Apply button to implement your changes on the switch.
8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 13

Port Mirroring

This chapter contains the procedures for managing the port mirroring feature. The sections in the chapter include:

Introduction

The port mirror is a management tool that allows you to monitor the traffic on one or more ports on the switch. It works by copying the traffic from designated ports to another port where the traffic can be monitored with a network analyzer. The port mirror can be used to troubleshoot network problems or to investigate possible unauthorized network access. The performance and speed of the switch is not affected by the port mirror.

To use the feature, you need to designate one or more source ports and the mirror port. The source ports are the ports whose packets are to be monitored. The mirror port is the port where the packets from the source ports are copied and where the network analyzer is connected.

Here are the guidelines to using the port mirror:

- The switch supports only one port mirror at a time.
- The port mirror can have only one mirror port.
- The mirror port must be a member of the default VLAN.
- The mirror port cannot be a member of a static port trunk.
- The port mirror can have more than one source port. This allows you to monitor the traffic on multiple ports at the same time. For example, you might monitor the traffic on all of the ports of a VLAN.
- You can mirror the ingress traffic, the egress traffic or both on the source ports.
- The source ports can be members of different VLANs.
- You may not use the mirroring feature with the Rapid Spanning Tree or Multiple Spanning Tree Protocol.

Enabling the Port Mirror

To enable the port mirror, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Mirroring option from the Switch Settings menu.

   The Switch Settings - Mirroring window is shown in Figure 34.

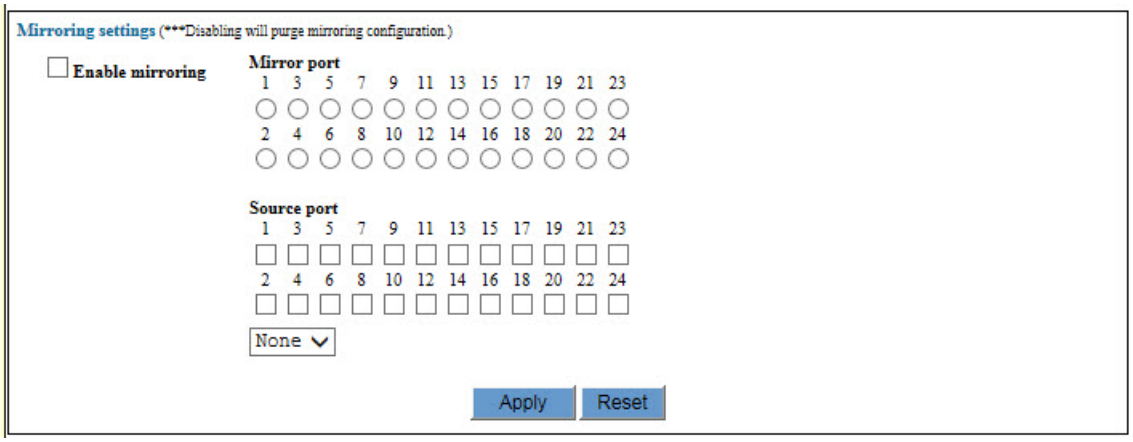

Figure 34. Switch Settings - Mirroring Window

3. Click the Enable Mirroring dialog box to add a check mark to it.
4. In the Mirror Port section of the window, click the dialog circle of the port to be the mirror port. The switch will copy the network traffic of the source ports to this port. You may designate only one mirror port.
5. In the Source Port section of the window, click the dialog box of the port to be the source port. This is the port whose traffic is to be copied to the mirror port. You may select more than one source port. You may mirror one port, a few ports, or all of the ports on the switch, with the exception of the mirror port.
6. Select the pull-down menu beneath the source ports and select the traffic to be monitored on the source ports. The options are described here:

   - Rx - The ingress traffic on the source ports are copied to the mirror port.
   - Tx - The egress traffic on the source ports are copied to the mirror port.
   - Both - Both the ingress and egress traffic on the source ports are copied to the mirror port.

- None - No traffic on the source ports are copied to the mirror port. The is the default setting. You may not select None.

7. Click the Apply button to implement your changes on the switch.

   The feature is now active on the switch. You may now connect a data analyzer to the mirror port to monitor the traffic on the source ports.

   If all of your settings disappear from the window when you click the Apply button, it probably means that you did not check the Enable Mirroring option in the top right corner of the window.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Disabling the Port Mirror

To disable the port mirror, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Mirroring option from the Switch Settings menu.

   The Switch Settings - Mirroring window is shown in Figure 34 on page 149.
3. Click the Enable Mirroring dialog box to remove the check mark from it.
4. Click the Apply button to implement your changes on the switch.

   The feature is now disabled. The switch stops copying traffic on the source ports to the mirror port.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 14

Static Port Trunks

This chapter contains the procedure for managing static port trunks. The sections in this chapter are listed here:

Introduction

Static port trunks are groups of two to eight ports that act as single virtual links between the switch and other network devices. Static port trunks are commonly used to improve network performance by increasing the bandwidth between the switch and other network devices and to enhance the reliability of the connections between network devices.

Figure 35 is an example of a static port trunk of four links between two switches.

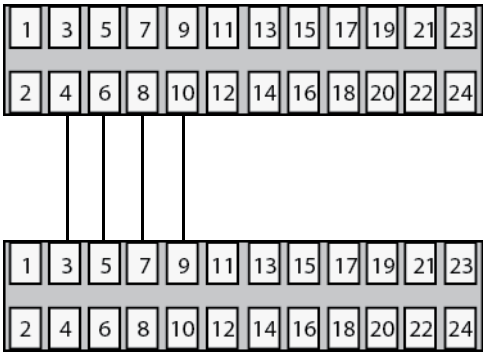

Figure 35. Static Port Trunk Example

Here are the guidelines for static port trunks:

- The switch can support up to eight static trunks at one time.
- A static trunk can have up to eight ports.
- A static port trunk cannot have both twisted pair and SFP fiber optic ports.
- A port can belong to only one static trunk at a time.
- The ports of a trunk can be either consecutive (for example ports 5-9) or nonconsecutive (for example, ports 4, 8, 11, 20).
- The ports of a static port trunk must be members of the same VLAN.
- Before creating a port trunk, you should set the speed, duplex mode, flow control, and back pressure settings the same on all the ports to be in the trunk.
- After creating a port trunk, do not change the parameter settings of any port in the trunk without also changing the same settings on the other ports.
- To create a trunk of combo ports, you have to set the ports to either the Fiber or Copper configuration setting. You may not use the Fiber-Auto or Copper-Auto setting. For instructions, refer to “Configuring Port Parameters” on page 118.

- The ports of a trunk cannot be authenticator or supplicant ports in port authentication. For further information, refer to Chapter 40, "Port Authentication Overview" on page 471 or Chapter 41, "Port Authentication" on page 487.
- You may use static port trunks with the spanning tree protocols because the switch considers the ports of a trunk as a single virtual link.
- Because network equipment vendors tend to employ different techniques for static trunks, a static trunk on one device might not be compatible with the same feature on a device from a different manufacturer. For this reason, Allied Telesis recommends using this feature only between Allied Telesis network devices.

Creating a Port Trunk

Please check the following items before creating a port trunk:

- Check that the parameter settings are the same on all of the ports that are to be in the trunk. For instructions, refer to “Configuring Port Parameters” on page 118.
- Check that the ports are members of the same VLAN. For instructions, refer to “Displaying the VLAN Window” on page 194.
- If you plan to use combo ports in the trunk, check that they are set to the Fiber or Copper configuration setting. You may not use the Fiber-Auto or Copper-Auto setting. For instructions, refer to “Configuring Port Parameters” on page 118.

Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the remote device. Connecting the cables prior to configuring the trunk can create a loop in your network topology. This can cause a broadcast storm and poor network performance.

To create a port trunk, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Trunking option from the Switch Settings menu.

   The Switch Settings - Trunking window is shown in Figure 36.

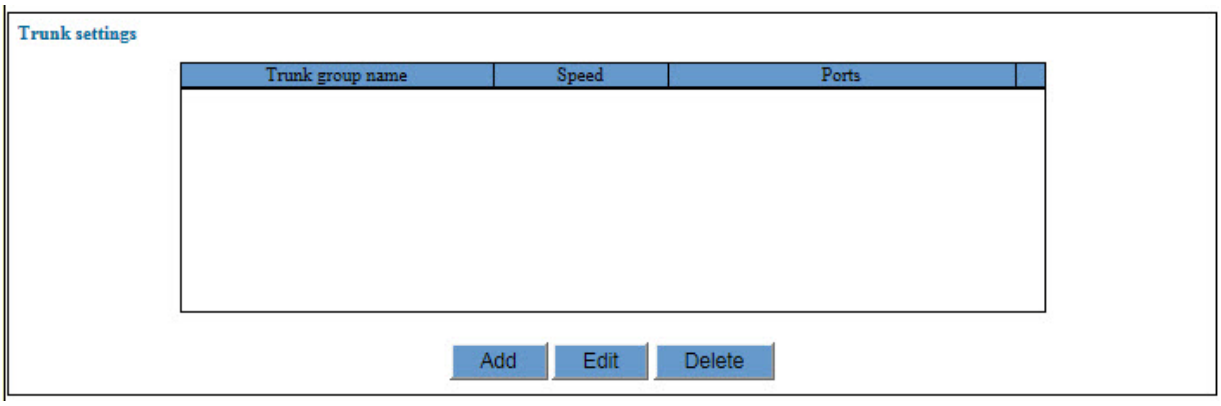

Figure 36. Switch Settings - Trunking Window

The table in the window displays the specifications of the existing trunks. The columns in the window are described in Table 42 on page 157.

Table 42. Switch Settings - Trunking Window

Column	Description
Trunk Group Name	Displays the name of a port trunk.
Speed	Displays the speed of the ports of a trunk.
Ports	Displays the ports of a trunk.

3. Click the Add button.

   The switch displays the Trunk Settings - Add window, shown in Figure 37.

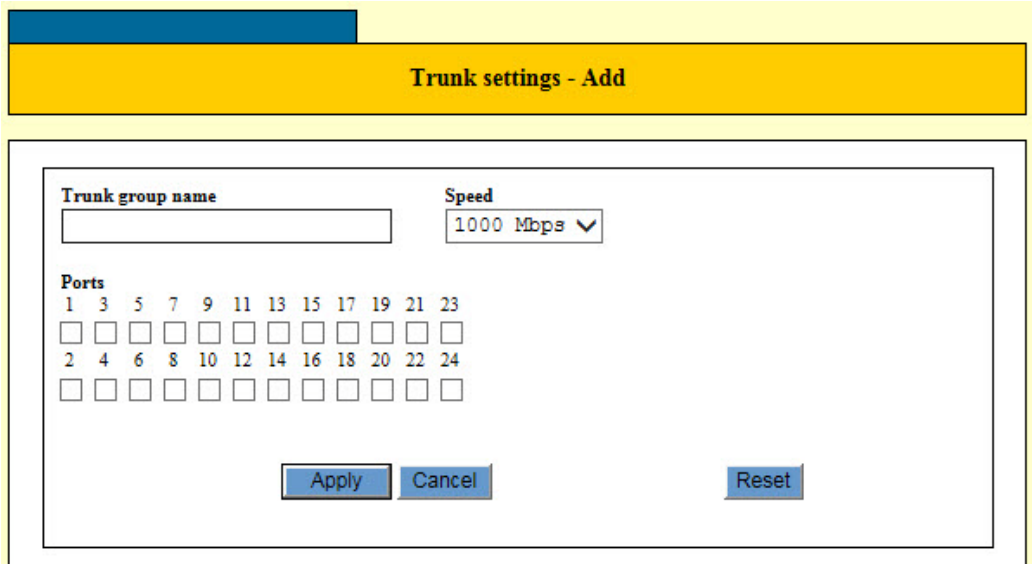

Figure 37. Trunk Settings - Add Window

4. Configure the parameters in the window to create the new port trunk. The parameters are described in Table 43.

Table 43. Trunk Settings - Add Window

Parameter	Description
Trunk Group Name	Use this field to specify a name for the new trunk. The name can be up to 20 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.
Speed	Use this pull-down menu to select the speed of the ports in the trunk.

Table 43. Trunk Settings - Add Window (Continued)

Parameter	Description
Ports	Use the Ports section to specify the members of the trunk by clicking on the dialog boxes of the ports. A port is a member of a trunk when its dialog box has a check mark and is not a member of the trunk when its dialog box is empty. A port trunk can have up to eight ports.

5. After configuring the parameters, click the Apply button to add the new trunk to the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.
7. Configure the ports on the remote device for port trunking.
8. Connect the cables to the ports of the trunk on the switch and the remote device.

   The port trunk is ready for network operations.

Modifying a Port Trunk

This section contains the procedure for modifying a static port trunk on the switch. Please review the following information before modifying a trunk:

- You may not change the name of a trunk.
- You may add or remove ports from a trunk as well as change the trunk speed.
- If you are adding ports to an existing trunk, check that the speed, duplex mode, flow control, and back pressure settings of the new ports are the same as the ports already in the trunk. For instructions, refer to "Configuring Port Parameters" on page 118.
- If you are adding ports, check that the new ports are members of the same VLAN as the ports already in the trunk. For instructions, refer to "Displaying the VLAN Window" on page 194.

Caution

If you are adding or removing ports from the trunk on the switch, disconnect all of the data cables from the ports of the trunk before performing this procedure. Leaving the cables connected can form a loop in your network topology, which can result in a broadcast storm and poor network performance.

To modify a static port trunk, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Trunking option from the Switch Settings menu.

   The Switch Settings - Trunking window is shown in Figure 36 on page 156.
3. In the Trunk Settings table, click the dialog box of the trunk you want to modify. You may modify only one trunk at a time.

   The switch displays the Trunk Settings - Edit window. An example of the window is shown in Figure 38 on page 160.

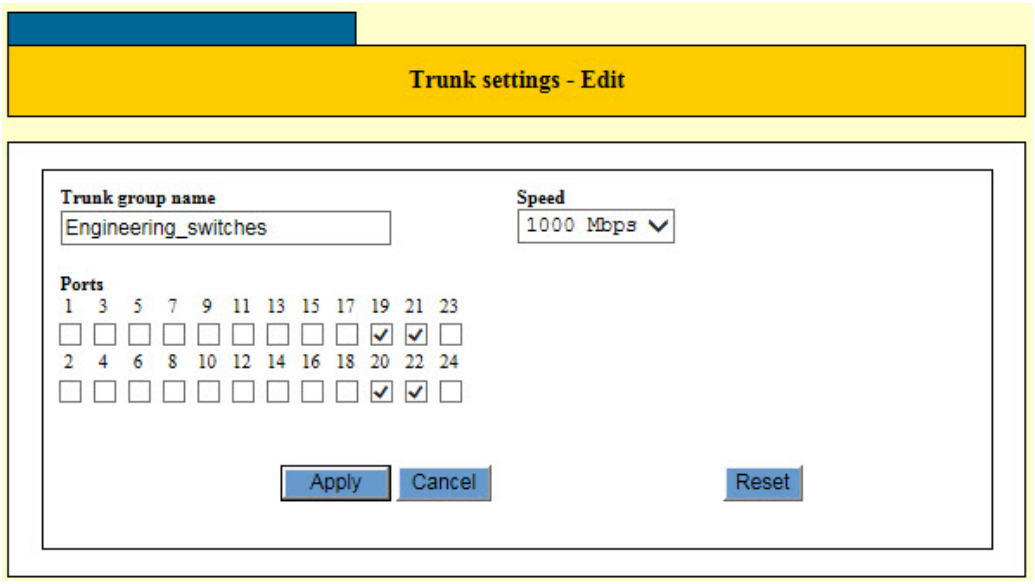

Figure 38. Trunk Settings - Edit Window

4. Modify the parameters in the window, as needed. The parameters are described in Table 43 on page 157.
5. After modifying the parameters, click the Apply button to activate your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.
7. Modify the trunk ports on the remote device, if necessary.
8. Reconnect the cables to the ports of the trunk on the switch.

Deleting a Port Trunk

This sections contains the procedure for deleting static port trunks.

Caution
Disconnect the cables from the ports of the static port trunk on the switch before performing this procedure. Deleting the trunk without first disconnecting the cables can result in the formation of a loop in your network topology, which can cause a broadcast storm and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Trunking option from the Switch Settings menu.

   The Switch Settings - Trunking window is shown in Figure 36 on page 156.
3. Click the dialog box of the trunk you want to delete. You may delete only one trunk at a time.
4. Click the Delete button to delete the trunk from the switch.

   The switch displays a confirmation prompt.
5. Click OK to delete the trunk or Cancel to retain the trunk.

   The trunk is deleted from the switch.
6. To permanently save your change in the configuration file, click the Save button above the main menu.

Chapter 15

Triggers

This chapter describes triggers. Sections in the chapter include:

Introduction

Triggers perform specific actions on the switch at scheduled times, automatically. There are three available actions. The actions are defined in Table 44.

Table 44. Trigger Actions

Action	Description
Sleep	Places the switch in a sleep mode. The switch stops forwarding all network traffic. It automatically reboots at the end time of the trigger.
LEDs off	Turns off the Link/Activity LEDs.
Disable ports	Disables individual ports to stop them from forwarding network traffic.

Triggers have four main variables. The variables are defined in Table 45.

Table 45. Trigger Variables

Variable	Description
Action	Defines what a trigger is to do on the switch. The functions are listed in Table 44.
Start and end times	Defines the start and end times of a trigger. The hours are entered in 24-hour format. For example, to designate 8:00 pm to 6:30 am, you enter 20:00 and 6:30 as the start and end times, respectively. To designate all 24 hours in a day, you could enter the start time as 00:00 and the end time as 23:59.
Start and end days or dates	Defines the days of the trigger. You may specify the days as days of the week or as dates.
Ports	Defines the switch ports of a trigger. A trigger may be assigned to a single port, several ports, or all of the ports on the switch. (This variable does not apply to the sleep action, which applies to the entire switch.)

Here are several examples of triggers. The first example creates a trigger that disables ports 12 and 13 on November 2 and 3, 2014. Here are the trigger variables:

- Action: Disable ports
- Start and end times: 00:00 to 23:59
- Start and end dates: 2014/11/2 to 2014/11/3
- Ports: 12, 13

This example creates a trigger that turns off all of the Link/Activity LEDs every evening at 6:00 pm and turns them on again at 6:00 am, to conserve electricity. The trigger has these variables:

- Action: LEDs off
- Start and end times: 18:00 to 6:00
- Start and end dates: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
- Ports: All ports

This example places the switch in the sleep mode from 2:00 am to 10:00 am on November 15, 2014: The trigger has these variables:

- Action: Sleep
- Start and end times: 2:00 to 10:00
- Start and end dates: 2014/11/15
- Ports: Not applicable

Guidelines

Here are general trigger guidelines:

- The switch can have up to ten triggers.
- The start and end times are entered in 24-hour format.
- Triggers with the LED off or disable ports action can be assigned to individual ports.
- Triggers with the sleep mode action shut down all of the ports.

Here are the guidelines for the sleep action:

- You cannot manage a switch that is in the sleep mode.
- You have to power off the switch and power it on again if you need to manually override the sleep mode and restart a unit.
- A switch should not be placed in the sleep mode for more than 28 days because it might not restart automatically.

The LED off action, which turns off the Link/Activity LEDs on the ports, has very specific requirements. Triggers with this action will not work if the

requirements are not followed. Here are the steps you have to perform before creating triggers with the LED off action:

1. You first have to turn off all of the port LEDs on the switch from the System Settings - LED window, shown in Figure 22 on page 96.

   The top part of the window has a section called Basic Setting, which has a pull-down menu. The options in the menu perform the same functions as the mode button on the front of the switch. They set the mode of the Speed/Duplex LEDs or turn off the LEDs. You have to select the LED Off option from the pull-down menu and click the Apply button. This turns off all of the port LEDs.

2. You have to override the off status of the Link/Activity LEDs on the switch by setting the LED action to On in the Port LED - Port Settings window, shown in Figure 23 on page 100.

   From the same System Settings - LED window in which you performed step 1, you now have to override the off status of the Link/Activity LEDs of the ports that are to have triggers with the LED off action. To do this, click the dialog boxes of the ports to have the triggers and click the Edit button. From the Port LED - Port Settings window, select On from the LED Action pull-down menu and click the Apply button. This activates the Link/Activity LEDs again.

3. Create the triggers with the LED off action.

Note
All of the Speed/Duplex Mode LEDs on the switch have to remain off if you want to use triggers that turn off the Link/Activity LEDs.

Displaying the Trigger Window

To display the trigger window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Trigger option from the System Settings menu.

   The System Settings - Trigger window is shown in Figure 39.

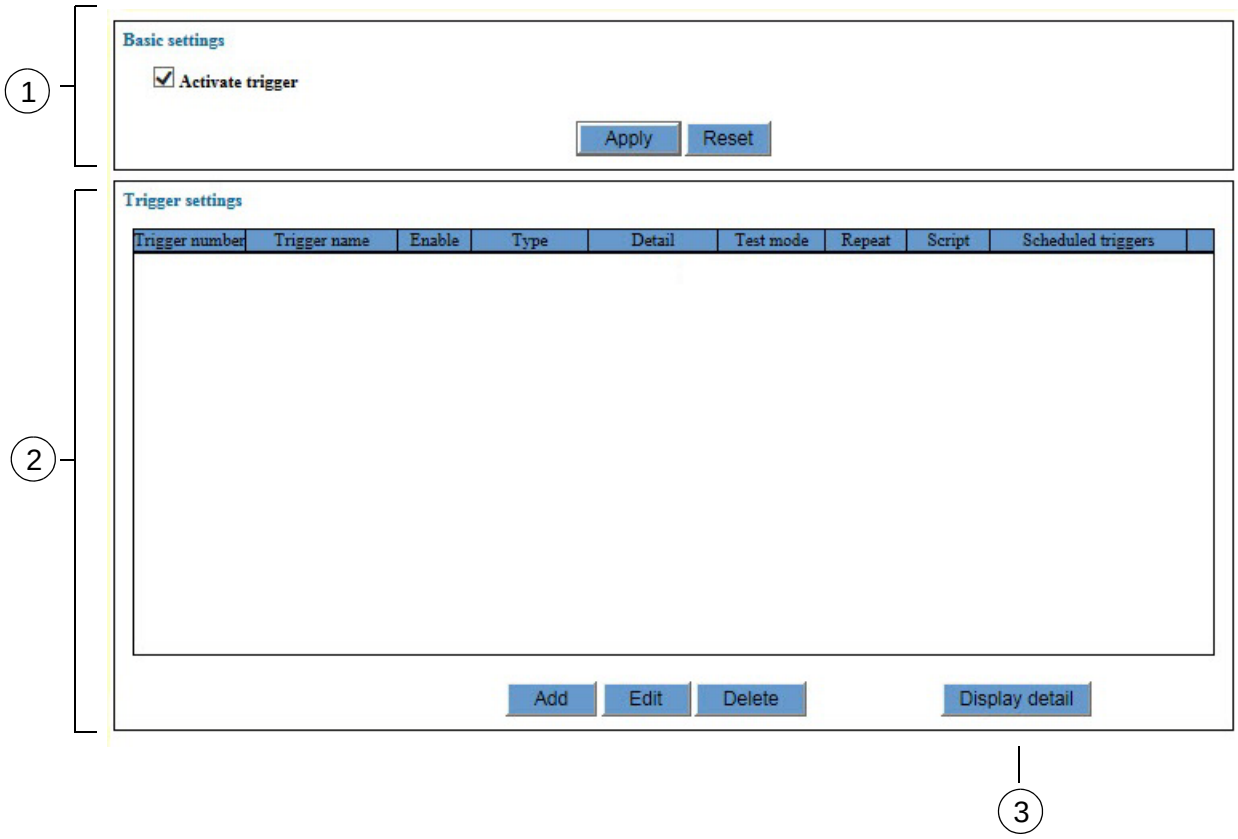

Figure 39. System Settings - Trigger Window

The sections in the System Settings - Trigger window are described in Table 46 on page 168.

Table 46. System Settings - Trigger Window

Section	Description
1	Use the option in this section to enable or disable the trigger feature. The triggers are enabled when the dialog box has a check mark and disabled when the dialog box is empty. For instructions, refer to “Enabling or Disabling the Trigger Feature” on page 169.
2	Use the table in this section to view details about the existing triggers or to add, edit, or delete triggers. The columns in the table are defined in Table 47. For more information, refer to “Adding Triggers” on page 170, “Modifying Triggers” on page 173, or “Deleting Triggers” on page 174.
3	Use this button to view additional information about the triggers. For information, refer to “Displaying Triggers” on page 175.

The columns in the Trigger Settings table are defined in Table 47.

Table 47. Trigger Settings Table in System Settings - Trigger Window

Column	Description
Trigger Number	Displays the ID number to the trigger.
Trigger Name	Displays the name of the trigger.
Enable	Displays whether the trigger is enabled or disabled.
Type	Displays the action.
Detail	Displays the schedule of the trigger.
Test mode	Not used. The status is always No.
Repeat	Not used. The status is always Yes.
Script	Not used. The status is always 0.
Scheduled Triggers	Displays the start and end days or dates of the trigger.

Enabling or Disabling the Trigger Feature

To enable or disable the trigger feature, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Triggers option from the System Settings menu.

   The System Settings - Triggers window is shown in Figure 39 on page 167.
3. Click the dialog box of the Activate Trigger option in the Basic Settings section of the window.

   The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is enabled.
4. Click the Apply button.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding Triggers

To add a trigger to the switch, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Triggers option from the System Settings menu.

   The System Settings - Triggers window is shown in Figure 39 on page 167.
3. Click the Add button.

   The switch displays the Trigger Settings - Add window, shown in Figure 40.

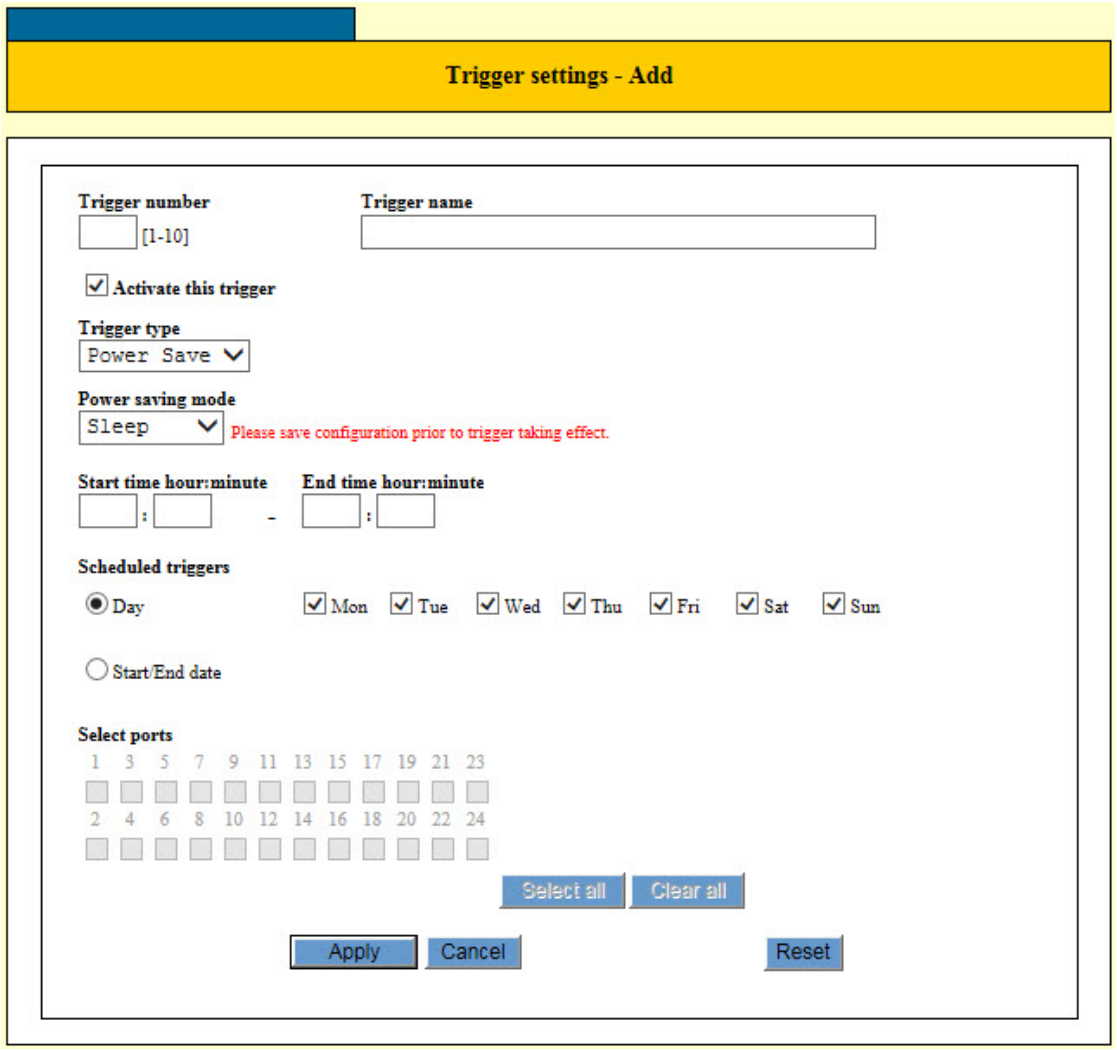

Figure 40. Trigger Settings - Add Window

4. Configure the parameters in the window, as needed.

   The parameters are defined in Table 48.

   Note
   You may specify the start and end times of a trigger by days of the week or dates.

Table 48. Trigger Settings - Add Window

Parameter	Description
Trigger Number	Use this parameter to assign an ID number to the trigger. The range is 1 to 10.
Trigger Name	Use this parameter to assign a name to the trigger. A name can have up to forty characters. A name may contain spaces.
Activate This Trigger	Use this option to enable or disable the trigger. The trigger is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is enabled.
Trigger Type	Use this parameter to specify the trigger type. The only selection is “Power Save.”
Power Saving Mode	Use this parameter to specify the action of the trigger. The available actions are listed here: Sleep - Shuts down the switch. LEDs Off - Turns off the Link/Activity LEDs. (Be sure to review “Guidelines” on page 165 before using this action.) Disable Ports - Disables ports.
Start Time	Use this parameter to specify the start time of the function. You enter the hours and minutes in 24-hour format.
Enter Time	Use this parameter to specify the end time of the function. The hours are entered in 24-hour format.

Table 48. Trigger Settings - Add Window (Continued)

Parameter	Description
Scheduled Triggers - Day	Use this parameter to specify the days of the week when the function is to be performed. A day is selected when its dialog box has a check mark and not selected when the dialog box is empty.
Scheduled Triggers - Start/ end Date	Use this parameter to specify the start and end dates of the trigger. The date format is shown here: yyyy:mm:dd The year must have four digits. For example, to specify the start and end dates November 9 to 11, 2014, you enter: 2014/11/9 - 2014/11/11
Select Ports	Use this section to designate the ports of the trigger. You may assign a trigger to more than one port. A port is selected when its dialog box has a check mark and not selected when its dialog box is empty. This option is not available with the sleep action because that action applies to the entire switch.

5. After configuring the parameters, click the Apply button to create the new trigger.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying Triggers

To modify a trigger, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Triggers option from the System Settings menu.

   The System Settings - Triggers window is shown in Figure 39 on page 167.
3. Click the dialog box of the trigger you want to modify. You may edit only one trigger at a time.
4. Click the Edit button.

   The switch displays the Trigger Settings - Edit window.
5. Edit the parameter, as needed.

   The parameters are described in Table 48 on page 171. You may not change the ID number of a trigger.
6. After configuring the parameters, click the Apply button to implement your changes to the trigger.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting Triggers

To delete triggers, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Triggers option from the System Settings menu.

   The System Settings - Triggers window is shown in Figure 39 on page 167.
3. Click the dialog box of the trigger you want to delete. You may delete only one trigger at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Edit OK to delete the trigger or Cancel to keep it.

   Note
   Deleting a trigger cancels its action. For example, a port automatically becomes enabled again if you delete a trigger that disabled it.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Triggers

To display information about triggers, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Triggers option from the System Settings menu.

   The System Settings - Triggers window is shown in Figure 39 on page 167.
3. Click the dialog box of the trigger you want to view. You may view only one trigger at a time.
4. Click the Display Detail button.

   An example of the window is shown in Figure 41.

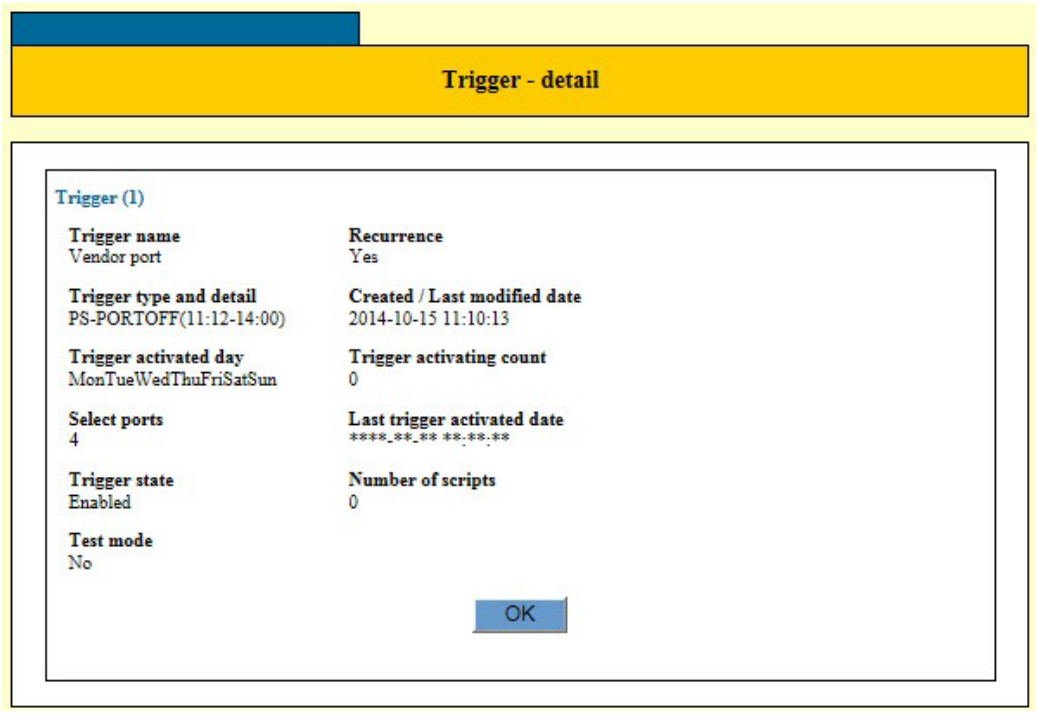

Figure 41. Trigger - Detail Window

The fields in the window are defined in Table 49.

Table 49. Trigger - Detail Window

Field	Description
Trigger	Displays the ID number of the trigger.

Table 49. Trigger - Detail Window (Continued)

Field	Description
Trigger Name	Displays the name of the trigger.
Trigger Type and Detail	Displays the action and the start and end times of the trigger.
Trigger Activated Day	Displays either the days of the week, or start and end dates of the trigger.
Select Ports	Displays the ports to which the trigger is assigned. (This field does not apply to the sleep action.)
Trigger State	Displays whether the trigger is enabled or disabled.
Test mode	Not used. The status is always No.
Recurrence	Not used. The status is always Yes.
Created/Last Modified Date	Displays the date and time when the trigger was created or last modified.
Trigger Activating Count	Displays the number of times the switch has activated the trigger.
Last Trigger Activated Date	Displays the date and time when the trigger was last activated. The field will contain asterisks if the trigger has not been activated.
Number of Scripts	Not used. The status is always 0.

5. To close the window, click the OK button.

Chapter 16

Port-based and Tagged VLANs Overview

This chapter covers the following topics:

Overview

A VLAN is a group of ports that form a logical Ethernet segment on an Ethernet switch. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remain within the VLAN.

VLANs are used to segment a network through the switch's management software so that nodes with related functions are grouped into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

Advantages of VLANs

VLANs offer several benefits:

- Improved network performance

  Network performance often suffers as networks grow in size and as traffic increases. The more nodes on each LAN segment vying for bandwidth, the greater the likelihood overall network performance will decrease.

  VLANs improve network performance because VLAN traffic stays within the VLANs. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them and frees up bandwidth within all the logical workgroups.

  In addition, broadcast traffic remains within a VLAN because each VLAN constitutes a separate broadcast domain. This, too, can improve overall network performance.

- Increased security

  Because network traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, you can use VLANs to control the flow of packets in your network and prevent packets from flowing to unauthorized end nodes.

- Simplified network management

  VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to be made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment often required a change to the wiring at the switch.

  With VLANS, you can use the switch's management software to change the LAN segment assignments of end nodes, without having to physically move workstations or move cables from one switch port to another port.

- Virtual LANs can also span more than one switch. This makes it possible to create VLANs of end nodes that are connected to switches located in different physical locations.

Types of VLANs

The switch supports the following types of VLANs:

- Port-based VLANs
- Tagged VLANs
- Protected ports VLANs

Port-based and tagged VLANs are described in this chapter. Protected ports VLANs are described in Chapter 18, "Protected Ports VLANs Overview" on page 205.

Port-based VLAN Overview

A VLAN consists of a group of ports that form an independent traffic domain on one or more Ethernet switches. Traffic generated by the end nodes remain within their respective VLANs and do not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Gigabit Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note
The switch is pre-configured with one port-based VLAN, called the default VLAN. All of the ports on the switch are members of this VLAN.

The parts of a port-based VLAN are:

- VLAN name
- VLAN Identifier
- Untagged ports
- Port VLAN Identifier

VLAN Name

A port-based VLAN must have a name. A name should reflect the function of the network devices that are to be members of the VLAN. Examples include Sales, Production, and Engineering.

VLAN Identifier

Every VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and network.

If a VLAN consists only of ports located on one physical switch in your network, you have to assign it a VID that is different from all of the other VIDs of the VLANs in your network.

If a VLAN spans multiple switches, you have to assign the same VID to each part of the VLAN on the different switches. That way, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN named Marketing that spanned three switches, you would assign the Marketing VLAN on each switch the same VID.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to a port on which a frame is received, and forwards a frame only to those ports that have the same PVID. Consequently, all of the ports of a port-based VLAN must have the same PVID. In addition, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, if you want to create a port-based VLAN on the switch and assign it a VID of 5, you would need to assign each port in the VLAN the PVID 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the management software on this switch performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is a member, when you assign the port as an untagged member to a VLAN.

Untagged Ports

You need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as untagged ports and the frames received on the ports as untagged frames. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's PVID. (There is another type of VLAN where VLAN membership is determined by information within the frames themselves, rather than by a port's PVID. This type of VLAN is explained in "Tagged VLAN Overview" on page 710.)

A port on the switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be a member of two or more port-based VLANs at the same time.

Guidelines to Creating a Port-based VLAN

Here are the guidelines to creating a port-based VLAN.

- A port-based VLAN must be assigned a unique VID. A VLAN that spans multiples switches must be assigned the same VID on each switch.
- A port can be an untagged member of only one port-based VLAN at a time.
- The PVID of a port must be identical to the VID of the VLAN where the port is an untagged member. The PVID value is automatically assigned by the switch.
- A port-based VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an

interconnection between the switches where the various parts of the VLAN reside. This is illustrated in “Port-based Example 2” on page 184.

- The switch can support up to a total of 4094 port-based, tagged, and protected ports VLANs.
- A port set to the 802.1x authenticator or supplicant role must be changed to the 802.1x none role before you can change its untagged VLAN assignment. After the VLAN assignment is made, you may return the port’s role to authenticator or supplicant, if desired.
- You cannot delete the default VLAN from the switch.
- Deleting an untagged port from the default VLAN without assigning it to another VLAN or while it is a tagged member of a VLAN results in the port being an untagged member of no VLAN.

Drawbacks of Port-based VLANs

Here are several drawbacks to port-based VLANs:

- It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to interconnect the port-based VLANs. The introduction of a router into your network could create security issues from unauthorized access to your network.
- A VLAN that spans several switches requires a port on each switch to interconnect the various parts of the VLAN. For example, a VLAN that spans three switches would require one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports could end up being used ineffectively just to connect the various VLANs. This is illustrated in “Port-based Example 2” on page 184.

Port-based Example 1

Figure 42 on page 183 illustrates an example of one switch with three port-based VLANs. (The default VLAN is not shown in the following examples.)

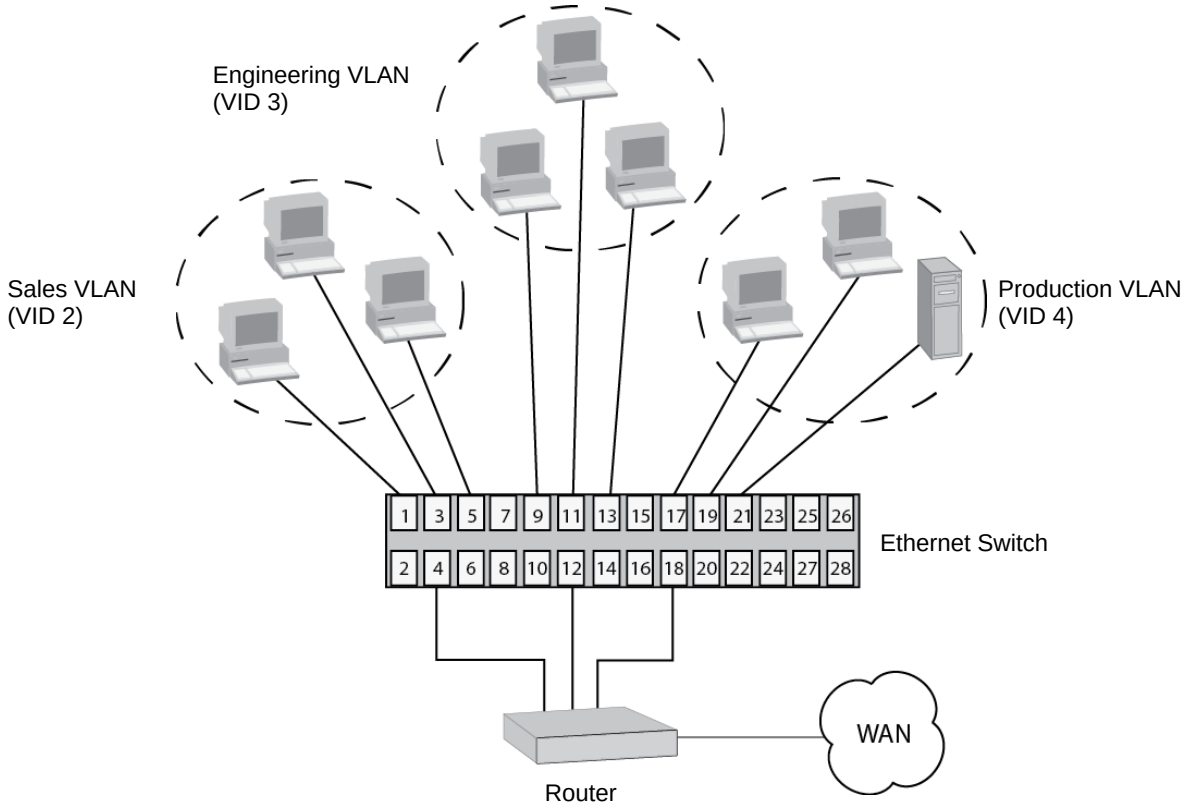

Figure 42. Port-based VLAN - Example 1

Table 50 lists the port assignments of the Sales, Engineering, and Production VLANs on the switch.

Table 50. Example 1 of Port-based VLANs

	Sales VLAN (VID 2)	**Engineering VLAN (VID 3)**	**Production VLAN (VID 4)**
Ethernet Switch	Ports 1, 3 - 5 (PVID 2)	Ports 9, 11 - 13 (PVID 3)	Ports 17 - 19, 21 (PVID 4)

The VLANs have unique VIDs, which are assigned when the VLANs are added to the switch.

The ports are automatically assigned PVIDs by the switch. The PVIDs match the VIDs of the VLANs in which the ports are untagged members.

In the example, each VLAN has one port connected to the router. The router interconnects the various VLANs and functions as a gateway to the WAN.

Port-based Example 2

Figure 43 is another example of port-based VLANs. In this example, two VLANs, Sales and Engineering, span two switches.

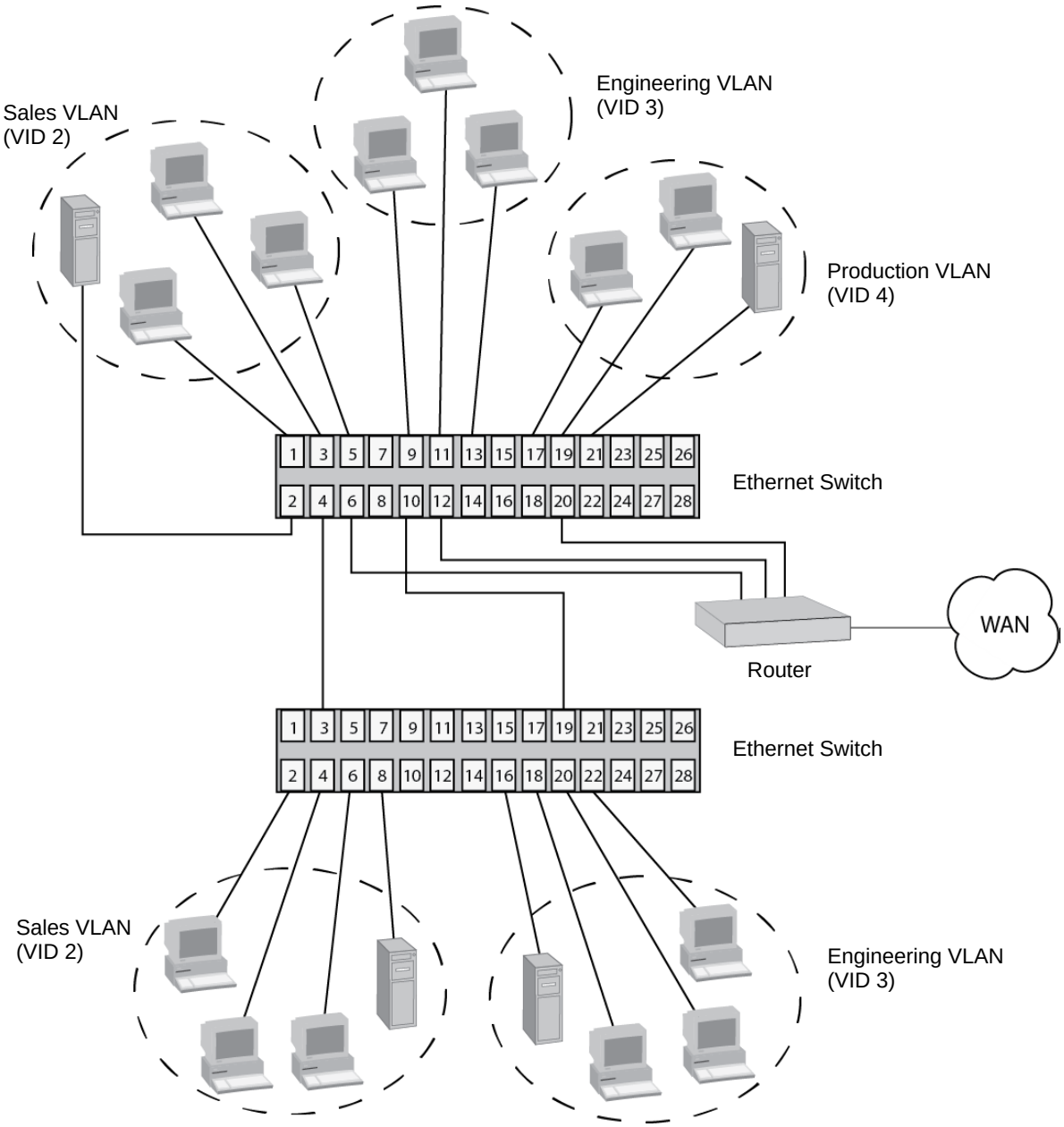

Figure 43. Port-based VLAN - Example 2

Table 51 on page 185 lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

Table 51. Example 2 of Port-based VLANs

	Sales VLAN (VID 2)	**Engineering VLAN (VID 3)**	**Production VLAN (VID 4)**
Top Ethernet Switch	Ports 1 - 6 (PVID 2)	Ports 9 - 13 (PVID 3)	Ports 17, 19 - 21 (PVID 4)
Bottom Ethernet Switch	Ports 2 - 4, 6, 8 (PVID 2)	Ports 16, 18-20, 22 (PVID 3)	none

The VLANs are described here:

- Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of six untagged ports on the top switch and five untagged ports on the bottom switch.

  The two parts of the VLAN are connected by a direct link from port 4 on the top switch to port 3 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.

  Port 6 on the top switch connects to the router. This port allows the Sales VLAN to exchange Ethernet frames with the other VLANs and to access the WAN.

- Engineering VLAN - The workstations of this VLAN are connected to ports 9 to 13 on the top switch and ports 16, 18 to 20, and 22 on the bottom switch.

  Because this VLAN spans multiple switches, it needs a direct connection between its various parts to provide a communications path. This is provided in the example with a direct connection from port 10 on the top switch to port 19 on the bottom switch.

  This VLAN uses port 12 on the top switch as a connection to the router and the WAN.

- Production VLAN - This is the final VLAN in the example. It has the VLAN of 4, and its ports have been assigned the PVID also of 4.

  The nodes of this VLAN are connected only to the top switch. So this VLAN does not require a direct connection to the bottom switch. However, it uses port 20 as a connection to the router.

Tagged VLAN Overview

The second type of VLAN is the tagged VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a tag or tagged header. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in “VLAN Identifier” on page 180, this number uniquely identifies the VLANs in a network.

When the switch receives a frame with a VLAN tag, referred to as a tagged frame, the switch forwards the frame only to those ports that share the same VID.

A port to receive or transmit tagged frames is referred to as a tagged port. Any network device connected to a tagged port must be IEEE 802.1q compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that tagged ports can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch to connect all of the VLANs on the switch to another switch.

The IEEE 802.1q standard describes how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame’s VID tag matches one of the VIDs of a VLAN of which the port is a tagged member, the frame is accepted and forwarded to the appropriate ports. If the frame’s VID does not match any of the VLANs in which the port is a member, the frame is discarded.

The parts of a tagged VLAN are similar to those for a port-based VLAN. They are listed here:

- VLAN Name
- VLAN Identifier
- Tagged and Untagged Ports

- Port VLAN Identifier

For explanations of VLAN name and VLAN identifier, refer back to "VLAN Name" on page 180 and "VLAN Identifier" on page 180.

Tagged and Untagged Ports

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which are untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the PVID of a port determines the VLAN where the port is an untagged member.

Because a tagged port determines VLAN membership by examining the tagged header within the frames that it receives and not the PVID, you might conclude that there is no need for a PVID. However, the PVID is used if a tagged port receives an untagged frame — a frame without any tagged information. The port forwards the frame based on the port's PVID. This is only in cases where an untagged frame arrives on a tagged port. Otherwise, the PVID on a tagged port is ignored.

Guidelines to Creating a Tagged VLAN

Below are the guidelines to creating a tagged VLAN.

- Each tagged VLAN must have a unique VID. If a VLAN spans multiple switches, you have to assign the same VID to each part of the VLAN on the different switches.
- A tagged port can be a member of multiple VLANs.
- An untagged port can be an untagged member of only one VLAN at a time.
- The switch can support up to a total of 4094 port-based, tagged, and protected ports VLANs.

Tagged VLAN Example

Figure 44 on page 188 illustrates how tagged ports can be used to interconnect IEEE 802.1q-based products.

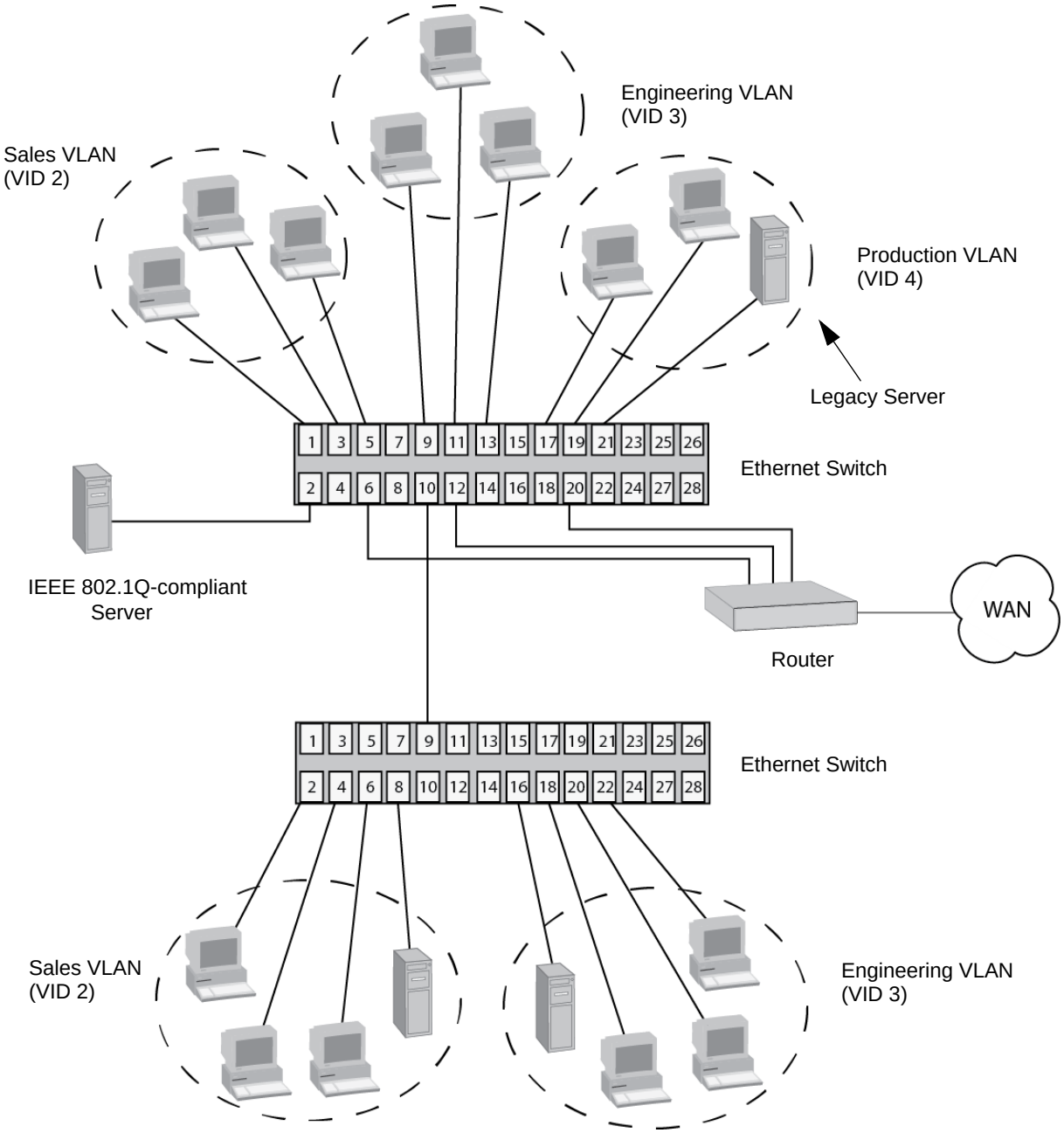

Figure 44. Example of a Tagged VLAN

The port assignments of the VLANs are described in Table 52 on page 189.

Table 52. Example of Tagged VLANs

	Sales VLAN (VID 2)		**Engineering VLAN (VID 3)**		**Production VLAN (VID 4)**	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
Top Ethernet Switch	1, 3 to 5 (PVID 2)	2, 10	9, 11 to 13 (PVID 3)	2, 10	17, 19 to 21 (PVID 4)	2
Bottom Ethernet Switch	2, 4, 6, 8 (PVID 2)	9	16, 18, 20, 22 (PVID 3)	9	none	none

This example is nearly identical to the "Port-based Example 2" on page 184. Tagged ports have been added to simplify network implementation and management.

One of the tagged ports is port 2 on the top switch. This port has been made a tagged member of the three VLANs. It is connected to an IEEE 802.1q-compliant server, meaning the server can handle frames from multiple VLANs. Now all of the three VLANs can access the server without going through a router or other interconnection device.

It is important to note that even though the server is accepting frames from and transmitting frames to more than one VLAN, data separation and security remain.

Two other tagged ports are used to simplify network design in the example. They are port 10 on the top switch and port 9 on the lower switch. These ports have been made tagged members of the Sales and Engineering VLANs so that they can carry traffic from both VLANs, simultaneously. These ports provide a common connection that enables different parts of the same VLAN to communicate with each other while maintaining data separation between the VLANs.

In comparison, the Sales and Engineering VLANs in the "Port-based Example 2" on page 184 had to have their own individual network links between the switches to connect the different parts of the VLANs. But with tagged ports, you can use one data link to carry data traffic from several VLANs, while still maintaining data separation and security. The tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the tagged frame originated.

Chapter 17

Port-based and Tagged VLANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs. This chapter contains the following sections:

Guidelines to Adding or Removing Ports from VLANs

Creating a new VLAN or modifying an existing one typically involves changing the VLAN assignments of ports on the switch. This section contains guidelines that may assist you as you move ports among the VLANs. Here are several general guidelines:

- A port can be an untagged member of only one VLAN at a time.
- A port can be a tagged member of more than one VLAN at a time.

Here are a few guidelines for adding ports to a VLAN:

- A port usually has to be an untagged member of the default VLAN before you can assign it as an untagged member of another VLAN. If a port is an untagged member of a VLAN other than the default VLAN, and you want to move it to a different VLAN, you first have to remove it from its current assignment, which automatically returns it to the default VLAN as an untagged port.

  Here is an example. Let's assume you want to move untagged port 5 from its current assignment in the Sales VLAN to the Accounting VLAN. In this situation, you would first have to remove the port from the Sales VLAN before adding it to the Accounting VLAN.

- There is an exception to the rule, and that is if a port is not an untagged member of any VLAN on the switch. Ports that are not untagged members of any VLAN can be assigned to a different VLAN without first being returned to the default VLAN. A port becomes an untagged member of no VLAN if it is removed from its VLAN and it is a tagged member of at least one other VLAN.
- Adding a tagged port to a VLAN does not change any of its other tagged or untagged VLAN assignments, because a tagged port can be a member of more than one VLAN at a time.

Here are a few guidelines for removing ports from VLANs:

- If you remove an untagged port from a VLAN and the port is not a tagged member of any other VLAN, it is automatically returned to the default VLAN.
- If you remove an untagged port from a VLAN and the port is a tagged member of one or more VLANs, it becomes an untagged port of no VLAN.
- You may not remove a tagged port from a VLAN if it is not an untagged or a tagged member of another VLAN on the switch. In this situation, you must first assign the port to another VLAN before removing it from its current VLAN assignment.
- Removing a tagged port from a VLAN does not change any of its

other tagged and untagged VLAN assignments, because a tagged port can be a member of more than one VLAN at a time.

Displaying the VLAN Window

To display the VLAN window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 45.

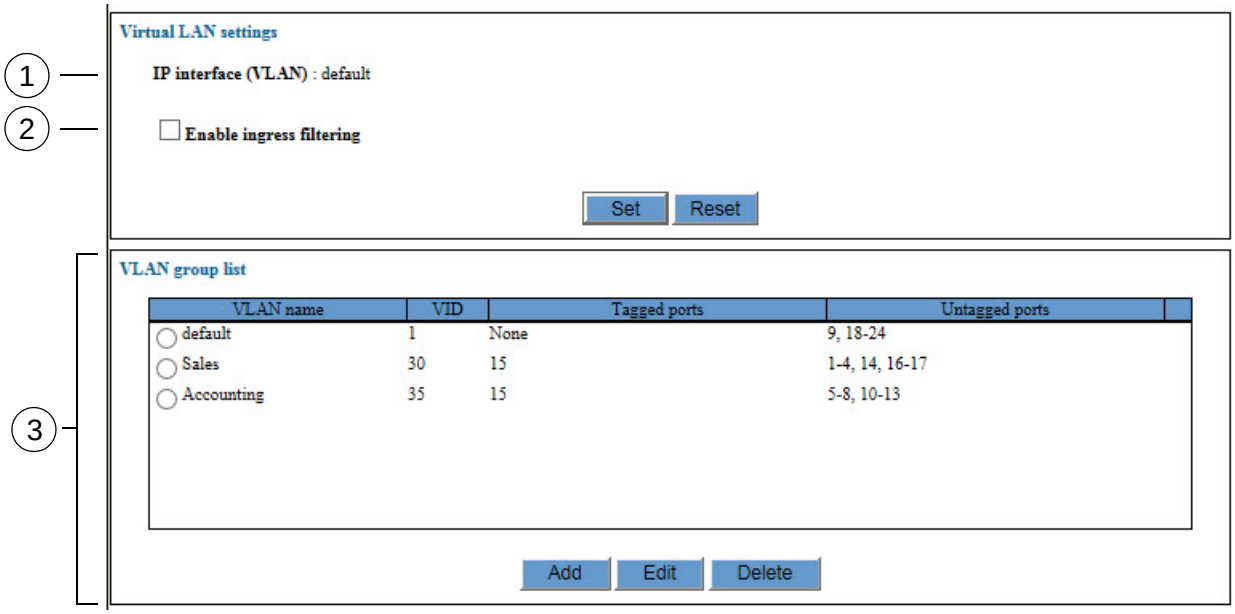

Figure 45. Switch Settings - Virtual LAN Window

The items in the window are described in Table 53.

Table 53. Switch Settings - Virtual LAN Window

Item	Description
1	Use this field to view the name of the management VLAN. The switch uses the management VLAN for remote management functions, such as Telnet, web browser, and SNMP management sessions. A switch can have only one management VLAN. Refer to “Specifying the Management VLAN” on page 50,
2	Use this option to enable or disable ingress filtering. Ingress filtering controls whether tagged ports accept or reject tagged packets whose VIDs do not match the VLANs to which the ports are members.

Table 53. Switch Settings - Virtual LAN Window (Continued)

Item	Description
3	Use this section to view the details of the existing VLANs on the switch and to create, edit, or delete VLANs. Refer to “Creating a Port-based or IEEE 802.1Q Tagged VLAN” on page 196, “Modifying a Port-based or Tagged VLAN” on page 201, and “Deleting a VLAN” on page 203.

The current VLANs on the switch are listed in the VLAN Group List table in the bottom section of the VLAN window. The columns in the table are described in Table 54.

Table 54. VLAN Group List Table

Columns	Description
VLAN Name	Displays the name of a VLAN.
VID	Displays the identifier of a VLAN. A VLAN can have only one VID.
Tagged Ports	Displays the tagged ports of a VLAN.
Untagged Ports	Displays the untagged ports of a VLAN.

Creating a Port-based or IEEE 802.1Q Tagged VLAN

This procedure explains how to create a new port-based or tagged VLAN. For guidelines on changing the VLAN assignments of ports, refer to “Guidelines to Adding or Removing Ports from VLANs” on page 192.

To create a new port-based or tagged VLAN, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 45 on page 194.
3. If the new VLAN is to contain untagged ports, examine the VLAN table to determine the current assignments of the ports, and do one of the following:

   - If the ports are untagged members of the default VLAN or no VLAN, you may continue with step 4.
   - If the ports are currently untagged members of a VLAN other than the default VLAN, do not continue. Instead, remove the ports from their current untagged VLAN assignments to return them to the default VLAN. For instructions, refer to “Modifying a Port-based or Tagged VLAN” on page 201.
4. Click the Add button at the bottom of the window.

   The VLAN Settings - Add window is shown in Figure 46 on page 197.

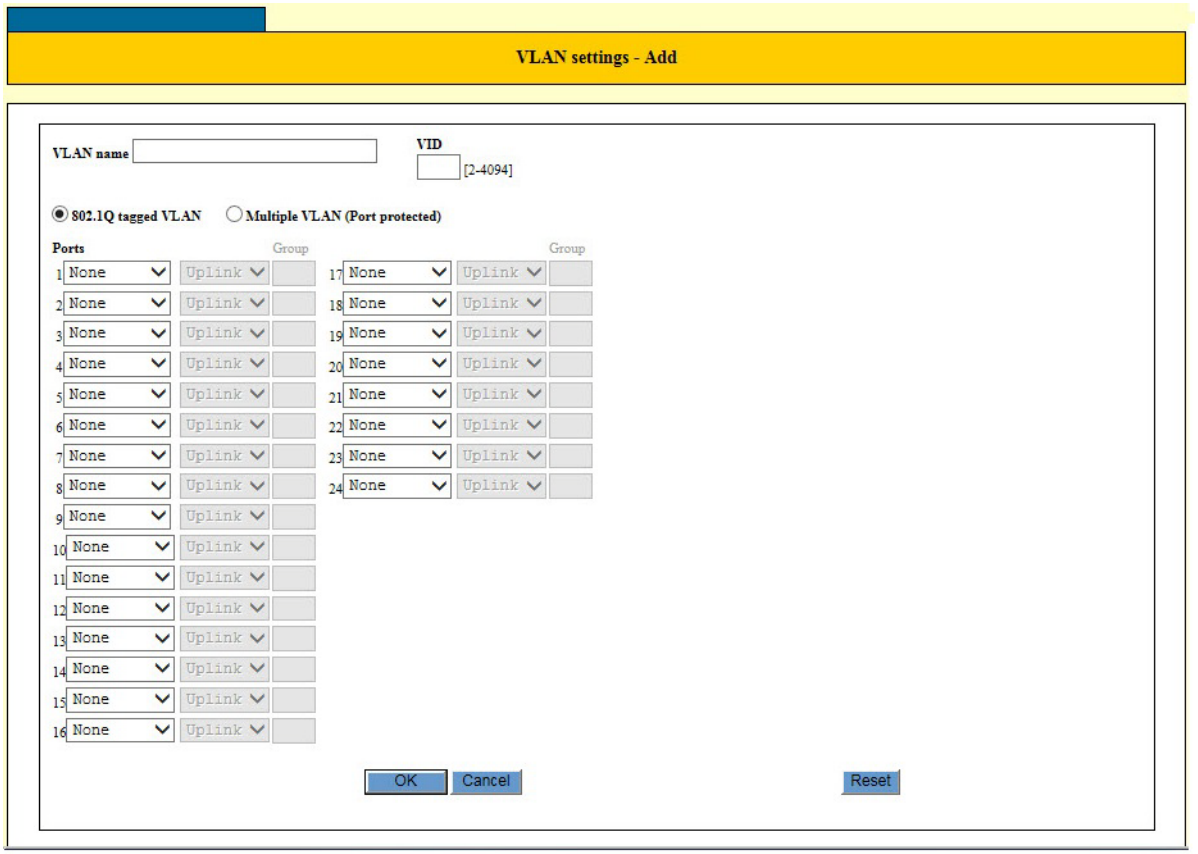

Figure 46. VLAN Settings - Add Window

5. Configure the parameters in the window to create the new VLAN. The parameters are described in Table 55.

Table 55. VLAN Settings - Add Window for Port-based or Tagged VLANs

Parameter	Description
VLAN Name	Use this parameter to enter a name for a new VLAN. A VLAN must have a name. The name can be up to twenty alphanumeric characters. The name of a VLAN will be easier to remember if it reflects the function of the nodes that are part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

Table 55. VLAN Settings - Add Window for Port-based or Tagged VLANs

Parameter	Description
VLAN Name (Continued)	If the VLAN is unique in your network, then the name should be unique as well. If the VLAN is part of a larger VLAN that spans multiple switches, then the name of the VLAN should be the same on each switch where nodes of the VLAN are connected.
VID	Use this parameter to assign a VID to a new VLAN. A VLAN must have a VID. The range is 2 to 4096. The default is the next available VID number on the switch. If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you should assign the Sales VLAN on each switch the same VID value. The switch is only aware of the VIDs of the VLANs on the device and not those already being used in the network. Consequently, the switch cannot notify you if the VID you are using for a new VLAN has already been assigned to another VLAN in your network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.
802.1Q tagged VLAN	Use this parameter to create port-based or tagged VLANs. Its dialog circle should be selected. If the dialog circle is empty, click it to select it.
Multiple VLAN (Port Protected)	This parameter is not used with port-based or tagged VLANs. If its dialog circle is selected, click the 802.1Q tagged VLAN parameter to deselect it.

Table 55. VLAN Settings - Add Window for Port-based or Tagged VLANs

Parameter	Description
Ports	Use the pull-down menus to designate the tagged and untagged ports of the VLAN. A VLAN can contain from one port to all the ports on the switch. The default setting for a new VLAN is no ports. The options are described here: None - Use this option to designate a port as not a member of the new VLAN. This is the default setting. Untagged - Use this option to add a port as an untagged port of the new VLAN. Tagged - Use this option to add a port as a tagged port of the new VLAN.
Uplink	This parameter is not used with port-based or tagged VLANs.
Group	This parameter is not used with port-based or tagged VLANs.

6. After configuring the parameters, click the OK button to add the new VLAN to the switch.

   Here are a couple points to consider:

   - If you see the error message "Contains port(s) of other VLANs, the switch could not add the new VLAN because one or more of its untagged ports belong to another VLAN other than the default VLAN. Untagged ports have to belong to the default VLAN before you can add them to a new VLAN. In some situations, this may require removing untagged ports from their current VLAN assignments to return them to the default VLAN before adding them to a new VLAN.

     For example, let's assume that you want to create a new VLAN called Sales with untagged ports 1 to 5 that already belong as untagged ports in a VLAN called Accounting. In this situation you have to remove the ports from the Accounting VLAN before adding them to the new VLAN. For instructions on how to remove untagged ports from VLANs, refer to "Modifying a Port-based or Tagged VLAN" on page 201.

   - If your remote web browser management session stops responding after you create the new VLAN, it might be because you moved the port through which your remote session is

managing the switch to another VLAN that is not the management VLAN. To continue managing the unit, start a local management session on the console port.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying a Port-based or Tagged VLAN

This procedure explains how to add or remove ports from a port-based or IEEE 802.1Q tagged VLAN on the switch. For guidelines on changing the VLAN assignments of ports, refer to "Guidelines to Adding or Removing Ports from VLANs" on page 192.

Note
You cannot change the name or VID of a VLAN.

To modify a port-based or tagged VLAN, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 45 on page 194.
3. Click the dialog circle of the VLAN you want to modify from the list of VLANs in the table in the window. You may modify only one VLAN at a time.
4. Click the Edit button.

   The switch displays the VLAN Settings - Edit window. An example of the window is shown in Figure 47 on page 202.

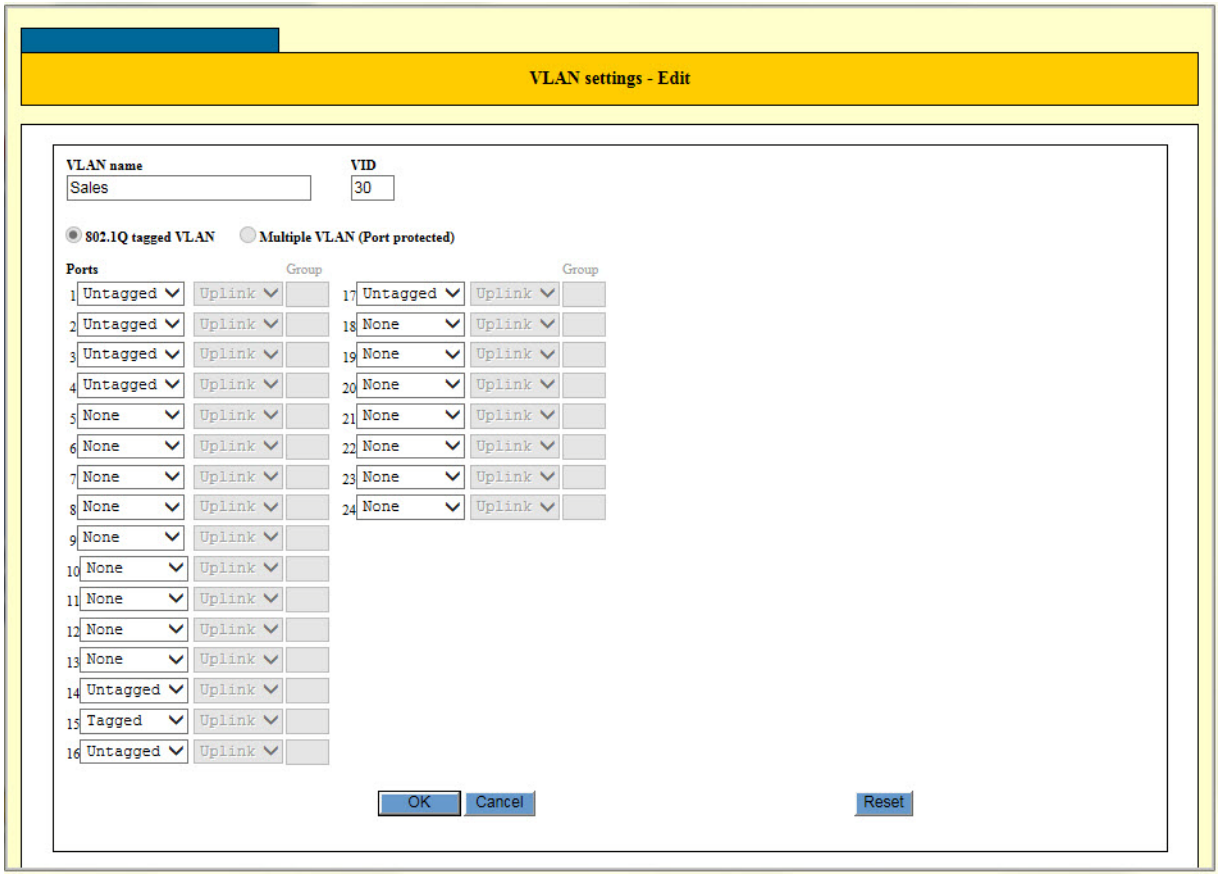

Figure 47. VLAN Settings - Edit Window

5. Modify the parameters in the window, as needed. The parameters are described in Table 55 on page 197.

6. After configuring the parameters, click the OK button to implement your changes to the VLAN.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting a VLAN

This procedure explains how to delete port-based or tagged VLANs from the switch. Please review the following information before deleting VLANs:

- You cannot delete the default VLAN.
- You cannot delete the management VLAN. The management VLAN is specified in the System Settings - System window, shown in Figure 9 on page 42.
- The untagged ports of a deleted VLAN are automatically returned to the default VLAN as untagged ports, except if they are tagged ports of other VLANs. In the latter case, they become untagged members of no VLAN.
- You may not delete a VLAN that has tagged ports that are not tagged or untagged members of another VLAN. For example, let's assume port 5 is a tagged member of the Sales VLAN and is not a tagged or untagged member of any other VLAN. To delete the Sales VLAN, you would first have to assign port 5 as a tagged or an untagged member to another VLAN on the switch.
- Static addresses assigned to the ports of a deleted VLAN are deleted from the MAC address table.

To delete port-based or tagged VLANs from the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 45.
3. Click the dialog circle of the VLAN you want to delete from the list of VLANS in the window. You may delete only one VLAN at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click the OK button to delete the VLAN or Cancel to cancel the procedure.

   Here are a couple items to consider:

   - If you see the message "Cannot delete VLAN when contains IP Interface," you tried to delete the management VLAN, which is not permitted. Designate another VLAN as the management VLAN. For instructions, refer to "Specifying the Management VLAN" on page 50.

- If you see the message “Cannot delete a tagged port when it is only associated with the specified VLAN,” you tried to delete a VLAN that has one or more tagged ports that are not assigned to any other VLANs on the switch. Assign the ports as tagged or untagged ports to other VLANs and then delete the VLAN.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 18

Protected Ports VLANs Overview

This chapter explains protected ports VLANs. It contains the following sections:

Overview

A protected ports VLAN consists of two or more port groups. Each group functions as a separate LAN within a protected ports VLAN. The member ports of a group are able to share traffic with ports in the same group, but not with ports in other groups. However, all of the port groups of a protected ports VLAN share a common uplink port.

Protected ports VLANs are typically used in network environments that require a great degree of network segmentation. An example application would be reading booths in a library. You could place the Ethernet connections in the booths into different port groups of a protected ports VLAN and connect the shared uplink port to the network. This approach would allow the library customers to use their computers in the reading booths to access the Internet or a library server via the single uplink connection, but would prevent them from communicating directly with each other.

Port groups are an essential component of protected ports VLANs. A group consists of one or more ports that function as a LAN segment within a protected ports VLAN. The ports of a group are independent of the ports in the other groups of the same VLAN. The ports of a group can share traffic only amongst themselves and with the uplink port, but not with ports in other groups in the same VLAN or different VLANs.

A protected ports VLAN can consist of two or more groups and a group can consist of one or more ports. The ports of a group can be either tagged or untagged.

This type of VLAN shares some common features with tagged VLANs, where one or more ports are shared by different LAN segments. But there are significant differences. First, all of the ports in a tagged VLAN are considered a LAN segment, while the ports in a protected ports VLAN, though residing in a single VLAN, are subdivided into the smaller unit of groups, which represent the LAN segments.

Second, a tagged VLAN, by its nature, contains one or more tagged ports. These are the ports that are shared among one or more tagged VLANs. The device connected to a tagged port must be 802.1Q compliant and it must be able to handle tagged packets.

In contrast, the uplink port in a protected ports VLAN, which is shared by the ports in the different groups, can be either tagged or untagged. The device connected to it does not necessarily have to be 802.1Q compliant.

Note
For explanations of VIDs and tagged and untagged ports, refer to Chapter 16, “Port-based and Tagged VLANs Overview” on page 177.

The procedure of creating a protected ports VLAN has some of the same steps as creating a new port-based or tagged VLAN. You have to give it a name and a unique VID, and indicate which of the ports will be tagged and untagged. What makes this type of VLAN different is that you must assign the ports of the VLAN to their respective groups and designate the uplink port.

Following is an example of a protected ports VLAN. Table 56 lists the name of the VLAN, the VID, and the tagged and untagged ports. It also indicates which port will function as the uplink port, in this case port 15.

Table 56. Example of a Protected Ports VLAN - Part I

Name	Reading_room_4
VID	8
Client Untagged Ports in VLAN	1-10
Client Tagged Ports in VLAN	none
Uplink Port(s)	15

Table 57 lists the different groups in the VLAN and the ports of the groups.

Table 57. Example of a Protected Ports VLAN - Part II

Client Port(s)	Group Number
1-2	1
3	2
4	3
5-7	4
8	5
9-10	6

Allied Telesis recommends that you create tables similar to these before creating your own protected ports VLANs. Having the tables will make your job easier when you create the VLANs.

Guidelines

Here are the guidelines for protected ports VLANS:

- A protected ports VLAN should contain a minimum of two groups. A protected ports VLAN of only one group can be replaced with a port-based or tagged VLAN instead.
- A protected ports VLAN can contain any number of groups.
- A group can contain any number of ports.
- The ports of a group can be tagged or untagged.
- Each group must be assigned a unique group number on the switch. The number can be from 1 to 256.
- Uplink ports can be either tagged or untagged.
- Uplink ports can be shared among more than one protected ports VLAN, but only if they are tagged.
- A switch can contain a combination of port-based and tagged VLANs and protected ports VLANs.
- A port that is a member of a group in a protected ports VLAN cannot be a member of a port-based or tagged VLAN.
- A group can be a member of only one protected ports VLAN at a time.

Chapter 19

Protected Ports VLANs

This chapter explains how to manage protected ports VLANs. This chapter contains the following sections:

Creating a New Protected Ports VLAN

This procedure explains how to create a new protected ports VLAN. Please review the following information before creating a new VLAN:

- The task of creating a new protected ports VLAN will be easier if you complete tables with the VLAN information, including the client ports, uplink port, group numbers, and VID. Examples are provided in Table 56 on page 207 and Table 57 on page 207.
- For guidelines on changing the VLAN assignments of ports, refer to “Guidelines to Adding or Removing Ports from VLANs” on page 192.

To create a new protected ports VLAN, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the VLAN option from the Switch Settings menu.

   The switch displays the Switch Settings - VLAN window. The window is described in “Displaying the VLAN Window” on page 194.
3. Examine the VLAN table in the window to determine the current assignments of the untagged ports you want to add to the new VLAN, and do one of the following:

   - If the ports are untagged members of the default VLAN or no VLAN, you may continue with step 4.
   - If the ports are currently untagged members of a VLAN other than the default VLAN, do not continue. Instead, remove the ports from their current untagged VLAN assignments to return them to the default VLAN. For instructions, refer to “Modifying a Port-based or Tagged VLAN” on page 201 or “Modifying a Protected Ports VLAN” on page 214.
4. Click the Add button.

   The VLAN Settings - Add window is shown in Figure 46 on page 197.
5. Configure the parameters in the window to create the new protected ports VLAN. You may create only one VLAN at a time. The parameters are described in Table 58 on page 211.

Note
The columns for designating the client and uplink ports and for entering the group numbers of a protected ports VLAN are initially greyed out in the window. They become active when you select the Multiple VLAN (port protected) option.

Table 58. VLAN Settings - Add Window for Protected Ports VLAN

Parameter	Description
VLAN Name	Use this parameter to enter a name for the new VLAN. A VLAN must have a name. The name of a VLAN can be from one to fifteen alphanumeric characters. An example of a name for a protected ports VLAN is Reading_room_4. The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).
VID	Use this parameter to assign a VID to the new VLAN. A VLAN must have a VID. The range is 2 to 4096. The switch is only aware of the VIDs of the VLANs on the device and not those already being used in the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.
802.1Q VLAN	Use this parameter to create port-based or tagged VLANs. This option is not used with protected ports VLANs. Its dialog circle should not be selected. If the dialog circle is selected, click the Protected Port option to deselect it.
Multiple VLAN (Port Protected)	Use this parameter to designate the new VLAN as a protected ports VLAN. Click the option to select it. Selecting the option activates the client and uplink columns in the window.

Table 58. VLAN Settings - Add Window for Protected Ports VLAN

Parameter	Description
Ports	Use the pull-down menus to add ports as tagged or untagged members of the new protected ports VLAN. The default setting for a new VLAN is no ports. The options are described here: None - Use this option to designate a port as not a member of the new VLAN. This is the default setting. Untagged - Use this option to add a port as an untagged port of the VLAN. Tagged - Use this option to add a port as a tagged port of the VLAN.
Uplink	Use the pull-down menus to designate the uplink port of the new protected ports VLAN. A protected ports VLAN can have only one uplink port.
Group	Use this parameter to assign group numbers to the ports of the new VLAN. The range is 1 to 65535.

Figure 48 on page 213 is an example of how the VLAN Settings - Add window would look for the protected ports VLAN detailed in Table 56 on page 207 and Table 57 on page 207.

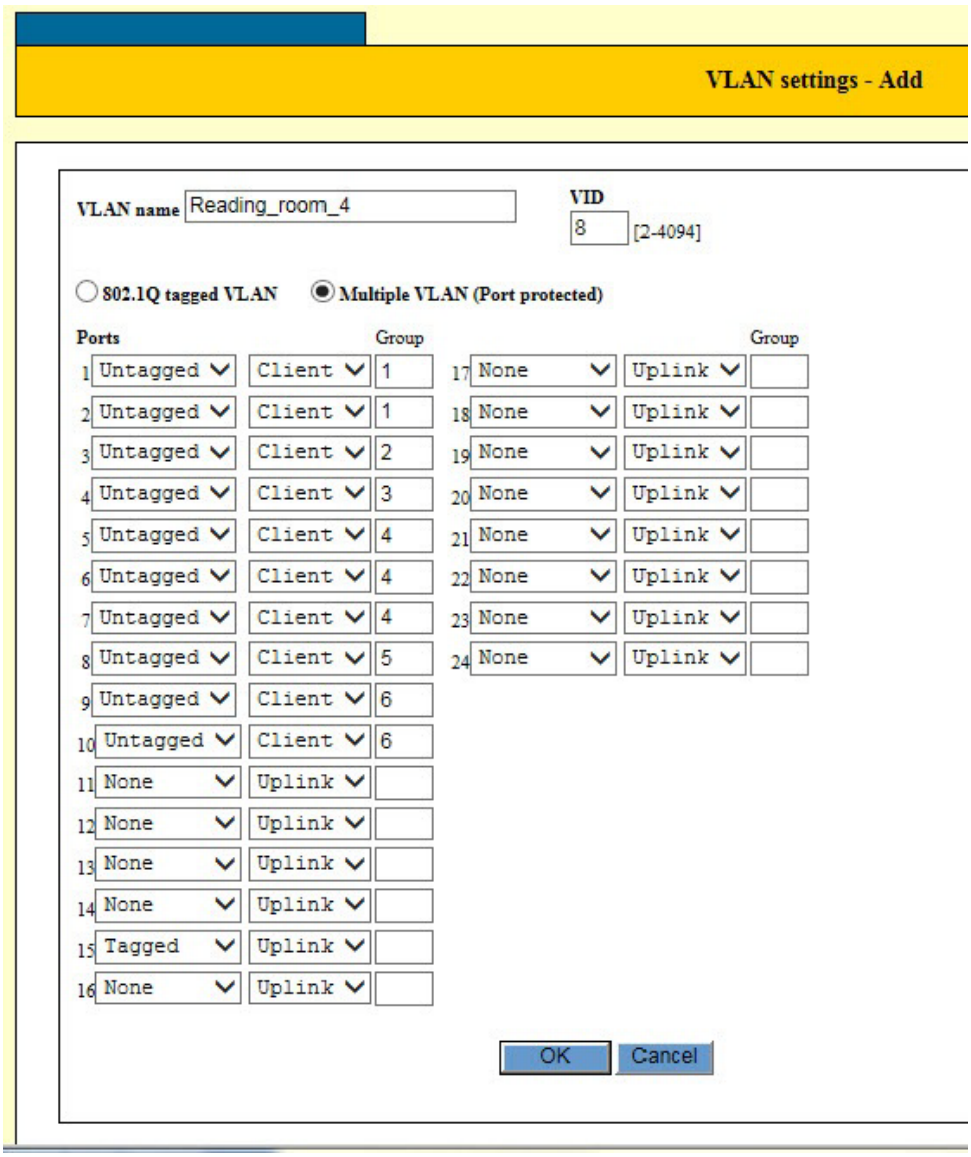

Figure 48. Example of the VLAN Settings - Add Window for a Protected Ports VLAN

6. After configuring the parameters, click the Apply button to add the new protected ports VLAN to the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying a Protected Ports VLAN

This procedure explains how to modify a protected ports VLAN. For guidelines on changing the VLAN assignments of ports, refer to “Guidelines to Adding or Removing Ports from VLANs” on page 192.

To modify a protected ports VLAN, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the VLAN option from the Switch Settings menu.

   The switch displays the Switch Settings - VLAN window. The window is described in “Displaying the VLAN Window” on page 194.
3. Click the dialog circle of the VLAN you want to modify from the list of VLANs in the window. You may modify only one VLAN at a time.
4. Click the Edit button.

   The switch displays the VLAN Settings - Edit window.
5. Modify the parameters in the window, as needed. The parameters are described in Table 58 on page 211.
6. After configuring the parameters, click the Apply button to implement your changes on the switch.
7. To permanently save your changes in the configuration file, select the Save button above the main menu.

Deleting a Protected Ports VLAN

This procedure deletes protected ports VLANs from the switch. Please review the following information before deleting VLANs:

- You cannot delete the default VLAN.
- You cannot delete the management VLAN. The management VLAN is specified in the System Settings - System window, shown in Figure 9 on page 42.
- The untagged ports of a deleted VLAN are automatically returned to the default VLAN as untagged ports, except if they are tagged ports of other VLANs. In the latter case, they become untagged members of no VLAN.
- You may not delete a VLAN that has tagged ports that are not tagged or untagged members of another VLAN. For example, let's assume port 5 is a tagged member of the Sales VLAN and is not a tagged or untagged member of any other VLAN. To delete the Sales VLAN, you would first have to assign port 5 as a tagged or an untagged member of another VLAN on the switch.
- Static addresses assigned to the ports of a deleted VLAN are deleted from the MAC address table.

To delete a protected ports VLAN, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the VLAN option from the Switch Settings menu.

   The switch displays the Switch Settings - VLAN window. The window is described in "Displaying the VLAN Window" on page 194.
3. Click the dialog circle of the VLAN you want to delete from the list of VLANs in the window. You may delete only one VLAN at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click the OK button to delete the VLAN or Cancel to cancel the procedure.

   Here are some items to consider:

   - If you see the message "Cannot delete VLAN when contains IP Interface," you tried to delete the management VLAN, which is not permitted. Designate another VLAN as the management VLAN. For instructions, refer to "Specifying the Management VLAN" on page 50.

- If you see the message “Cannot delete a tagged port when it is only associated with the specified VLAN,” you tried to delete a VLAN that has one or more tagged ports that are not assigned to any other VLAN on the switch. Assign the ports to another VLAN, such as the default VLAN, and then delete the VLAN.

6. Click the Apply button to implement your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 20

Quality of Service Overview

This chapter describes the Class of Service (CoS) feature of Quality of Service. Sections in the chapter include:

IEEE 802.1p Priority Levels and Egress Priority Queues

Quality of Service is a broadly used term that encompasses a range of methods for prioritizing traffic and/or limiting the bandwidth available to it. This chapter and the next chapter are concerned with the Class of Service (CoS) portion of QoS.

An Ethernet switch becomes oversubscribed when its egress queues contain more packets than it can handle in a timely manner. In this situation, it may be forced to delay transmitting some packets or even discard packets. Although minor delays are often of no consequence to a network or its performance, there are applications, referred to as delay or time-sensitive applications, that can be impacted by packet delays. Voice transmission and video conferencing are two examples. A delay in the transmission of packets carrying their data could reduce the quality of the audio or video.

This is where CoS can be of value. It permits the switch to give higher priority to some packets over others.

There are two principal types of traffic found on the ports of a Fast or Gigabit Ethernet switch, one being untagged packets and the other tagged packets. As explained in “Tagged VLAN Overview” on page 186, one of the principal differences between them is that tagged packets contain VLAN information.

CoS applies mainly to tagged packets because, in addition to carrying VLAN information, these packets can also contain a priority level that indicates how important (delay sensitive) a packet is in comparison to other packets. The switch refers to this number when determining a packet’s priority level.

CoS, as defined in the IEEE 802.1p standard, has eight levels of priority. The priorities are 0 to 7, with 0 the lowest priority and 7 the highest.

Each switch port has four egress queues, labeled Q0, Q1, Q2, and Q3. Q0 is the lowest priority queue and Q3 is the highest. A packet in a high priority egress queue is typically transmitted out a port sooner than a packet in a low priority queue.

When a tagged packet arrives on a port, the switch examines its priority value to determine which egress priority queue the packet should be directed to on the egress port. Table 59 on page 219 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 59. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0 (lowest)
2	Q0
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3 (highest)

For example, when a tagged packet with a priority level of 3 enters a port on the switch, the packet is stored in Q1 queue on the egress port.

Note that priority 0 is mapped to CoS queue 1 instead of CoS queue 0 because tagged traffic that has never been prioritized has a VLAN tag User Priority of 0. If priority 0 was mapped to CoS queue 0, this default traffic would go to the lowest queue, which would probably be undesirable. This mapping also makes it possible to give some traffic a lower priority than the default traffic.

You can change these mappings. For example, you might decide that packets with a priority of 2 should be handled by egress queue Q1 and packets with a priority of 5 should be handled in Q3. The result is shown in Table 60.

Table 60. Example of New Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0 (lowest)
2	Q1
3	Q1
4	Q2
5	Q3

Table 60. Example of New Mappings of IEEE 802.1p Priority Levels to Priority Queues (Continued)

IEEE 802.1p Priority Level	Port Priority Queue
6	Q3
7	Q3 (highest)

Note that these mappings are applied at the switch level. They cannot be set on a per-port basis.

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain priority levels. By default, all untagged packets are assigned a priority of 0 and are placed in a port's Q1 egress queue. But you can override this and instruct a port's untagged frames to be stored in a different priority queue.

Additionally, CoS does not change the priority levels in tagged packets. The packets leave the switch with the same priority levels they had when they entered. This is true even if you change the default priority-to-egress queue mappings.

Scheduling

A switch port needs to have a mechanism that specifies the order of transmittal of the packets from its four egress queues. For example, should a port that has packets in all of its queues transmit all of the packets from Q3, the highest priority queue, before moving on to the other queues, or should it transmit a few packets from each queue and, if so, how many?

This control mechanism is called *scheduling*. The switch has two types of scheduling:

- Strict priority
- Weighted round robin priority

Note
Scheduling is set at the switch level. You cannot set this on a per-port basis.

Strict Priority Scheduling

A port set to this scheduling method transmits all of the packets out of the higher priority queues before transmitting the packets in the lower priority queues. For instance, as long as there are packets in Q3 a port does not handle any of the packets in Q2.

The value to this type of scheduling is that high priority packets are always handled before low priority packets.

The problem is that some low priority packets might never be transmitted out the port because a port might never get to the low priority queues. A port handling a large volume of high priority traffic may be so busy transmitting traffic that it never has an opportunity to get to any of the packets stored in its low priority queues.

Weighted Round Robin Priority Scheduling

The weighted round robin scheduling method functions as its name implies. A port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. This method guarantees that every queue receives some attention from a port for transmitting packets.

To use this scheduling method, you have to specify the maximum number of packets a port should transmit from a queue before moving to the next queue. This is referred to as specifying the “weight” of a queue. In most cases, you will want to give greater weight to the higher priority queues over the lower priority queues.

Table 61 on page 222 shows the default values for the queues.

Table 61. Default Values for Weighted Round Robin

Port Egress Queue	Maximum Number of Packets
Q0 (lowest)	1
Q1	4
Q2	10
Q3	15

At the default settings, a port transmits a maximum number of 15 packets from Q3 before moving to Q2, from where it transmits up to 10 packets, and so forth.

Chapter 21

Quality of Service

This chapter explains how to configure the Class of Service portion of Quality of Service (QoS). This chapter contains the following procedures:

Displaying the Quality of Service Window

To display the Quality of Service window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the QoS option from the Switch Settings menu.

   The Switch Settings - QoS window is shown in Figure 49.

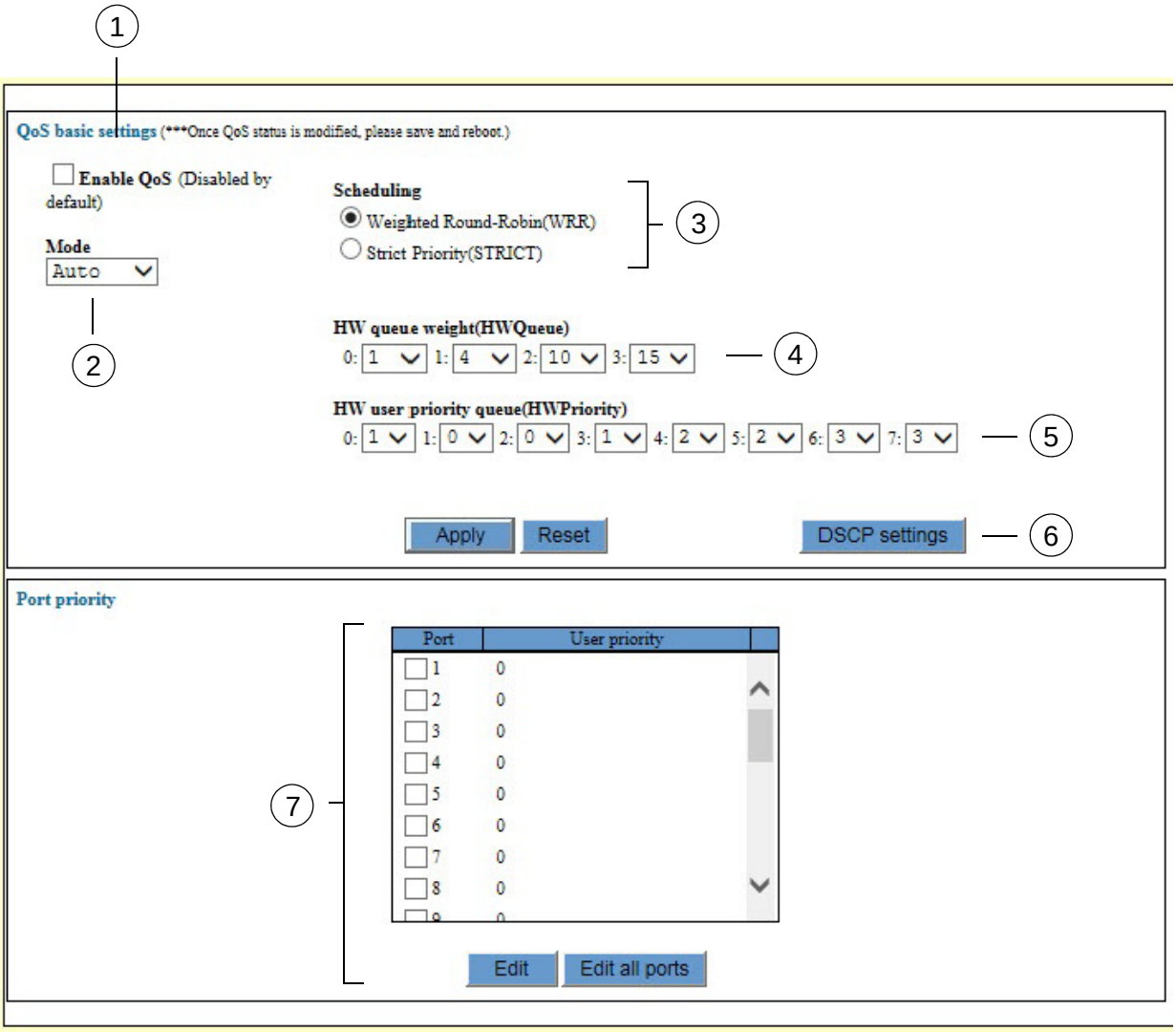

Figure 49. Switch Settings - QoS Window

The sections in the window are described in Table 62 on page 225.

Table 62. Switch Settings - QoS Window

Section	Description
1	Use this option to enable or disable QoS on the switch.
2	Use this option to specify the manner in which packets are prioritized. The options are listed here: Auto - Packet priority is based on the DSCP value, IEEE802.1p priority tag, and port priority, in that order. 802.1p - Packet priority is based only on the IEEE802.1p priority tag.
3	Use these options to specify egress packet scheduling. This controls the order in which ports transmit packets from their egress packet queues. For background information, refer to “Scheduling” on page 221. For instructions on how to set the feature, refer to “Configuring Egress Packet Scheduling” on page 226.
4	Use this option with weighted round robin scheduling to specify the number of packets the switch is to transmit from the egress queues on a port. For background information, refer to “Weighted Round Robin Priority Scheduling” on page 221. For instructions on how to set the feature, refer to “Configuring Egress Packet Scheduling” on page 226.
5	Use this line to adjust the mappings of CoS priority values to egress packet queues. For background information, refer to “IEEE 802.1p Priority Levels and Egress Priority Queues” on page 218. For instructions on how to set the feature, refer to “Mapping CoS Priorities to Egress Queues” on page 227.
6	Use this button to map DSCP values to CoS priority values. For instructions, refer to “Setting the Priority Values for DSCP Packets” on page 228.
7	Use this section to set the Class of Service priority values for the ports. The priority values determine which hardware queues store ingress untagged packets. For background information, refer to “IEEE 802.1p Priority Levels and Egress Priority Queues” on page 218. For instructions, refer to “Setting the Priority Values for Ingress Untagged Packets” on page 230.

Configuring Egress Packet Scheduling

To configure egress packet scheduling, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the QoS option from the Switch Settings menu.

   The Switch Settings - QoS window is shown in Figure 49 on page 224.
3. Do one of the following:

   - If you want the switch to use weighted round-robin scheduling to transmit packets from the egress queues of the ports, click the dialog circle for Weighted Round-Robin (WRR). This is the default setting.
   - If you want the switch to use strict priority scheduling to transmit packets from the egress queues of the ports, click the dialog circle for Strict Priority (STRICT).

   For background information, refer to “Scheduling” on page 221.
4. If you selected weighted round-robin scheduling, use the fields in the HW Queue Weight option to specify the maximum number of packets a port can transmit from an egress queue before going to the next queue.

   The queues are numbered 0 to 3. Queue 0 is the lowest priority and queue 3 the highest. The range is 1 to 15 packets.
5. Click the Apply button to implement your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues. Mappings are set at the switch level. Changes to the mappings apply to all of the ports in the switch. For background information, refer to "IEEE 802.1p Priority Levels and Egress Priority Queues" on page 218. To change the mappings, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.

2. Select the QoS option from the Switch Settings menu.

   The Switch Settings - QoS window is shown in Figure 49 on page 224. The mappings of priorities to egress priority queues are controlled with the HW User Priority line. The numbers in front of the pull-down menus represent the CoS priorities 0 to 7. The pull-down menus represent the hardware port queues. Each port has four queues, numbered 0 to 3.

   The default mappings are shown in Table 59 on page 219.

3. Use the pull-down menus in the HW User Priority line to adjust the mappings.

   For example, if you want to store ingress packets with the CoS priority 5 in hardware queue 3 on the ports, you use the pull-down menu for CoS priority 5 and select queue 3.

4. Click the Apply button to implement your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Setting the Priority Values for DSCP Packets

To change the mappings of DSCP values to CoS priority levels, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the QoS option from the Switch Settings menu.

   The Switch Settings - QoS window is shown in Figure 49 on page 224.
3. Click the DSCP Settings button.

   The switch displays the DSCP Settings - QoS window, shown in Figure 50.

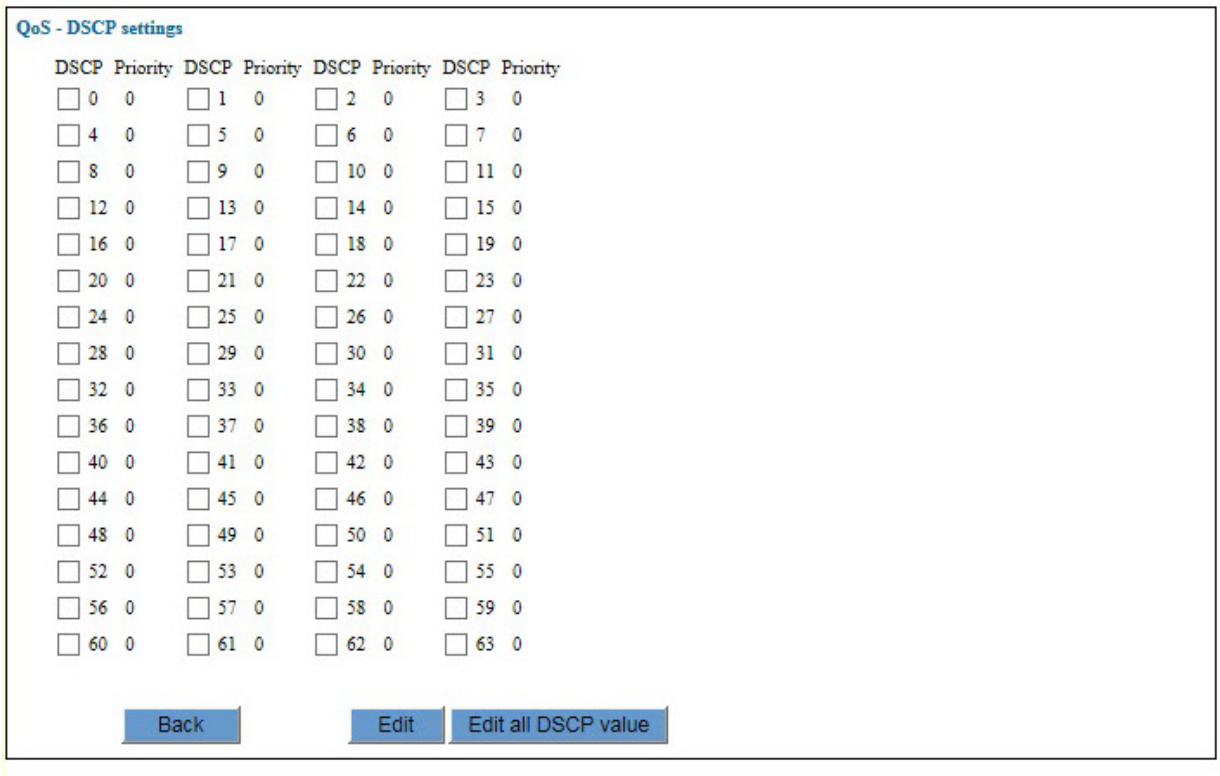

Figure 50. QoS - DSCP Settings Window

4. Click the dialog box of the DSCP value whose priority level you want to change. You may change more than one DSCP value at a time.
5. Click the Edit button. To change the values for all of the DSCP values, click the Edit All DSCP Values button.

   The switch displays the QoS DSCP Settings window, shown in Figure 51 on page 229.

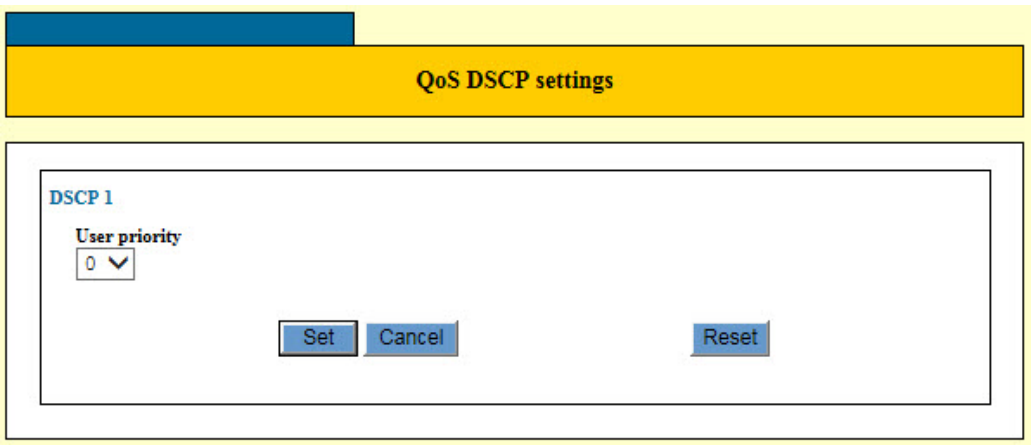

Figure 51. QoS DSCP Settings Window

6. Use the pull-down menu in the window to select the new CoS priority level for the selected DSCP values. The default is level 0.

7. Click the Set button to implement your changes on the switch.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Setting the Priority Values for Ingress Untagged Packets

This procedure configures the Class of Service priority levels for ingress untagged packets on the ports. The priority level dictates which priority queues the packets are stored in on the egress ports. A port can have only one priority value for untagged packets, but because this is set at the port level, the ports can have different values.

In the default settings, ingress untagged packets on a port are assigned a priority level of 0 and are stored in egress queue Q1 on an egress port. To adjust the mappings of priority levels to egress queues, refer to “Mapping CoS Priorities to Egress Queues” on page 227.

To change the CoS priority level on a port, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the QoS option from the Switch Settings menu.

   The Switch Settings - QoS window is shown in Figure 49 on page 224.
3. In the Port Priority section of the window, click the dialog box of the port whose Class of Service priority value you want to change. You may configure more than one port at a time.
4. Click the Edit button. To change the values for all the ports, click the Edit All Ports button.

   The switch displays the QoS - Port Priority window, shown in Figure 52.

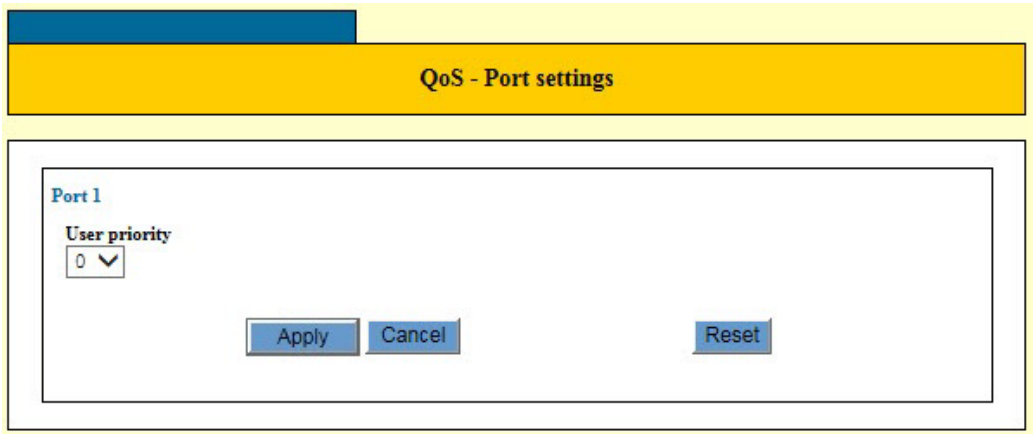

Figure 52. QoS - Port Settings Window

5. Use the pull-down menu in the window to select the new CoS priority level for the selected ports. The default is level 0. The new priority level will apply to all ingress untagged packets.

6. Click the Apply button to implement your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 22

Classifier Overview

This chapter explains classifiers for Quality of Service policies. The sections in this chapter include:

Overview

A classifier defines a *traffic flow*. A traffic flow consists of packets that share one or more characteristics. A traffic flow can range from being very broad to very specific. An example of the former might be all IP traffic, while an example of the latter could be packets with specific source and destination MAC addresses.

A classifier contains a set of criteria for defining a traffic flow. Examples of the variables include source and destination MAC addresses, source and destination IP addresses, IP protocols, source and destination TCP and UDP ports numbers, and so on. You can also specify more than one criteria within a classifier to make the definition of the traffic flow more specific. Some of the variables you can mix-and-match, but there are restrictions, as explained later in this section in the descriptions of the individual variables.

Classifiers are not used by themselves. Rather, they are used with Quality of Service (QoS) policies to regulate the various traffic flows that pass through the switch. For instance, you might raise or lower the user priority values of traffic packets or increase or decrease their allotted bandwidths.

You specify the traffic flow of interest by creating one or more classifiers and applying them to a QoS policy. The action to be taken by a port when it receives a packet that corresponds to the prescribed flow is dictated by the QoS policy, as explained in Chapter 24, “Quality of Service Policies Overview” on page 251.

In summary, a classifier is a list of variables that define a traffic flow. You apply a classifier to a QoS policy to define the traffic flow you want the QoS policy to affect or control.

Classifier Criteria

The components of a classifier are defined in the following subsections.

Destination or Source MAC Address (Layer 2)

You can identify a traffic flow by specifying a source and/or destination MAC address. For instance, you might create a classifier for a traffic flow destined to a particular destination node, or from a specific source node to a specific destination node, all identified by their MAC addresses. Classifiers may contain specific MAC addresses or ranges of addresses.

Ethernet 802.2 and Ethernet II Frame Types (Layer 2)

You can create a classifier that filters packets based on Ethernet frame type and whether a packet is tagged or untagged within a frame type. (A tagged Ethernet frame contains within it a field that specifies the ID number of the VLAN to which the frame belongs. Untagged packets lack this field.) Options are:

- Ethernet II tagged packets
- Ethernet II untagged packets
- Ethernet 802.2 tagged packets
- Ethernet 802.2 untagged packets

802.1p Priority Level (Layer 2)

Tagged Ethernet frames contain fields that specify their VLAN memberships, as explained in “Tagged VLAN Overview” on page 186. Such frames also contain user priority levels that the switch uses to determine the Quality of Service to apply to the frame and which egress queues on the egress ports the packets should be stored in. The priority level is a three bit binary number that represents the eight priority levels, 0 to 7, with 0 the lowest priority and 7 the highest. Figure 53 illustrates the location of the user priority field within an Ethernet frame.

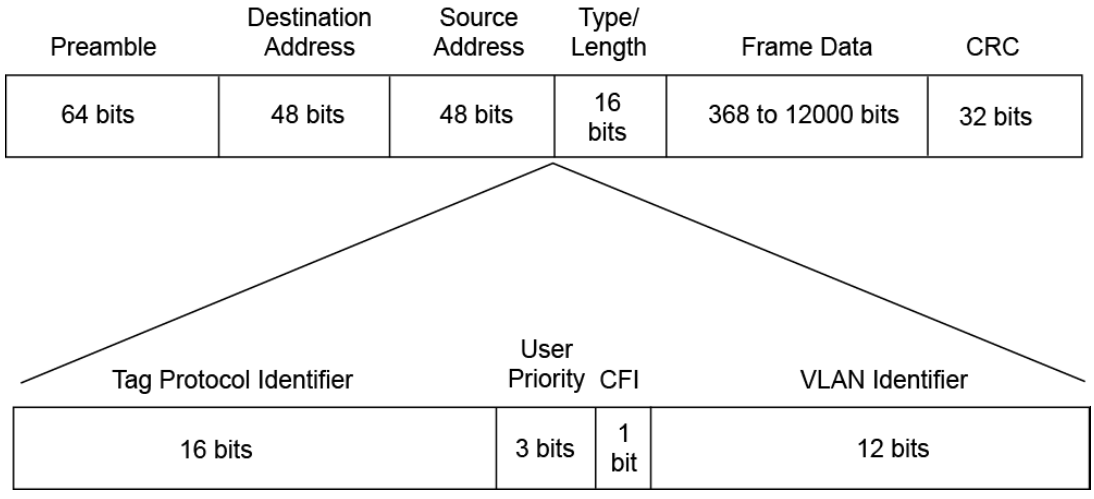

Figure 53. User Priority and VLAN Fields within an Ethernet Frame

You can identify a traffic flow of tagged packets using the user priority value. A classifier for such a traffic flow instructs a port to watch for tagged packets containing the specified user priority level.

The priority level criteria can contain only one value, and the value must be from 0 (zero) to 7. Multiple classifiers are required if a port is to watch for several different traffic flows of different priority levels.

Protocol (Layer 2)

Traffic flows can be identified by the protocol specified in the Ethertype field of the MAC header in an Ethernet II frame. Possible values are:

- IP
- ARP
- RARP
- Protocol number

Observe the following guidelines when using this variable:

- When selecting a Layer 3 or Layer 4 variable, this variable must be left blank or set to IP.
- If you choose to specify a protocol by its number, you may enter the number in decimal or hexadecimal format. The decimal range is 1536 to 65535. The hexadecimal range is 0x600 to 0xFFFF.

VLAN ID (Layer 2)

A tagged Ethernet frame also contains within it a field of 12 bits that specifies the ID number of the VLAN to which the frame belongs. The field, illustrated in Figure 53, can be used to identify a traffic flow.

A classifier can contain only one VLAN ID. Multiple classifiers are required for QoS policies that apply to different VLAN IDs.

IP ToS (Type of Service) (Layer 3)

Type of Service (ToS) is a standard field in IP packets. It is used by applications to indicate the priority and Quality of Service for a frame. The range of the value is 0 to 7. The location of the field is shown in Figure 54 on page 237.

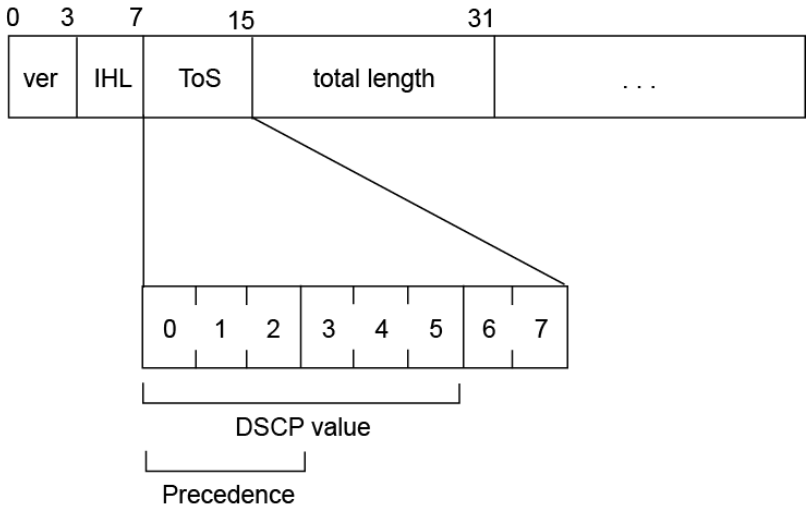

Figure 54. ToS field in an IP Header

Observe these guidelines when using this criterion:

- The Protocol variable must be left blank or set to IP.
- You cannot specify both IP ToS and IP DSCP values in the same classifier.

IP DSCP (DiffServ Code Point) (Layer 3)

The Differentiated Services Code Point (DSCP) tag indicates the class of service to which packets belong. The DSCP value is written into the TOS field of the IP header, as shown in Figure 54. Routers within the network use this DSCP value to classify packets, and assign QoS appropriately. When a packet leaves the DiffServ domain, the DSCP value can be replaced with a value appropriate for the next DiffServ domain.The range of the value is 0 to 63.

Observe these guidelines when using this criterion:

- The Protocol variable must be left blank or set to IP.
- You cannot specify both IP ToS and IP DSCP values in the same classifier.

IP Protocol (Layer 3)

You can define a traffic flow by the following Layer 3 protocols:

- TCP
- UDP
- ICMP
- IGMP
- IP protocol number

To specify a protocol number, you may enter the number in decimal or hexadecimal format. The decimal range is 0 to 255. The hexadecimal range is 0x0 to 0xFF.

Source IP Address and Mask (Layer 3)

You may use the source IP address to define a traffic flow for IP packets. The address can be a subnet or specific end node.

You do not need to enter a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, for a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask “255.255.255.0.”

This variable requires that the Protocol variable be blank or set to IP.

Destination IP Address and Mask (Layer 3)

You can also define a traffic flow based on the destination IP address of a subnet or a specific end node.

You do not need to enter a destination IP mask for an IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address while a “0” indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask “255.255.255.0.”

This variable requires that the Protocol variable be blank or set to IP.

TCP Source or Destination Ports (Layer 4)

A traffic flow can be identified by a source and/or destination TCP port number in the header of an IP frame. Observe the following guidelines when using these criteria:

- ❒ The Protocol variable must be left blank or set to IP.
- ❒ The IP Protocol variable must be left blank or set to TCP.
- ❒ A classifier cannot contain criteria for both TCP and UDP ports.

UDP Source or Destination Ports (Layer 4)

A traffic flow can be identified by a source and/or destination UDP port number contained within the header of an IP frame. Observe the following guidelines when using these criteria:

- ❒ The Protocol variable must be left blank or set to IP.
- ❒ The IP Protocol variable must be left blank or set to UDP.
- ❒ A classifier cannot contain criteria for both TCP and UDP ports. You may specify only one in a classifier.

TCP Flags

A traffic flow can be based on the following TCP flags:

- ❒ URG - Urgent
- ❒ ACK - Acknowledgement

- PSH - Push
- RST - Reset
- SYN - Synchronization
- FIN - Finish

Observe the following guidelines when using this criterion:

- The Protocol variable must be left blank or set to IP.
- The IP Protocol variable must be left blank or set to TCP.
- A classifier cannot contain both a TCP flag and a UDP source and/or destination port.

Guidelines

Here are the guidelines for classifiers:

- Each classifier represents a separate traffic flow.
- The variables within a classifier are linked by AND. The more variables you define within a classifier, the more specific it becomes in terms of the flow it defines. For instance, specifying both a source IP address and a TCP destination port within the same classifier defines a traffic flow that relates to IP packets containing both the designated source IP address and the TCP destination port. There are, however, some restrictions on combining variables in the same classifier. For the restrictions, refer to “Classifier Criteria” on page 235.
- You can apply the same classifier to more than one QoS policy.
- A classifier without any defined variables applies to all packets.
- You cannot create two classifiers that have the same settings. There can be only one classifier for any given type of traffic flow.
- A classifier can have a maximum of eight defined criteria, not including the classifier ID number and description.
- The switch can store up to 256 classifiers. However, the maximum number of classifiers you can assign to active QoS policies at any one time will be from 14 to 127. The number depends on several factors, such as the number of ports to which the classifiers are assigned and the types of criteria defined in the classifiers.
- You cannot modify a classifier if it belongs to a QoS policy that is assigned to a port. You must remove the port assignments from the policy and reassign them after modifying the classifier.
- You cannot delete a classifier that is assigned to a QoS policy. You have to remove a classifier from all of its QoS policy assignments before you can delete it.

Chapter 23

Classifiers

Classifiers define traffic flows for Quality of Service policies. This chapter contains the following sections:

Note
For background information on classifiers, refer to Chapter 22, “Classifier Overview” on page 233.

Displaying the Classifier Window

To display the Classifier window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Classifier option from the Switch Settings menu.

   The Switch Settings - Classifier window is shown in Figure 55.

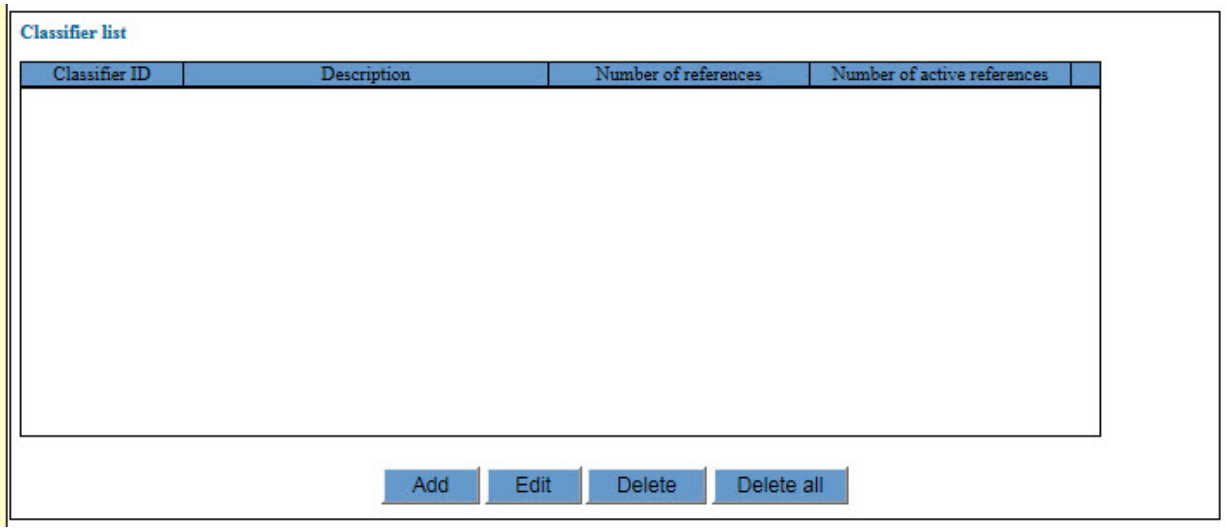

Figure 55. Switch Settings - Classifier Window

The Classifier List table has four columns. The columns are defined in Table 63.

Table 63. Switch Settings - Classifier Window

Column	Description
Classifier ID	Displays the ID number of a classifier.
Description	Displays the description of a classifier.
Number of References	Displays the number of QoS policies to which the classifier is currently assigned. If this column is 0 (zero), the classifier is not assigned to any policies.
Number of Active Associations	Displays the number of active QoS policies to which the classifier is currently assigned. A QoS policy is active if it is assigned to at least one port, and inactive if it is not assigned to any ports.

Creating a Classifier

To create a new classifier, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Classifier option from the Switch Settings menu.

   The Switch Settings - Classifier window is shown in Figure 55 on page 242.

3. Click the Add button.

   The Classifier - Add window is shown in Figure 56.

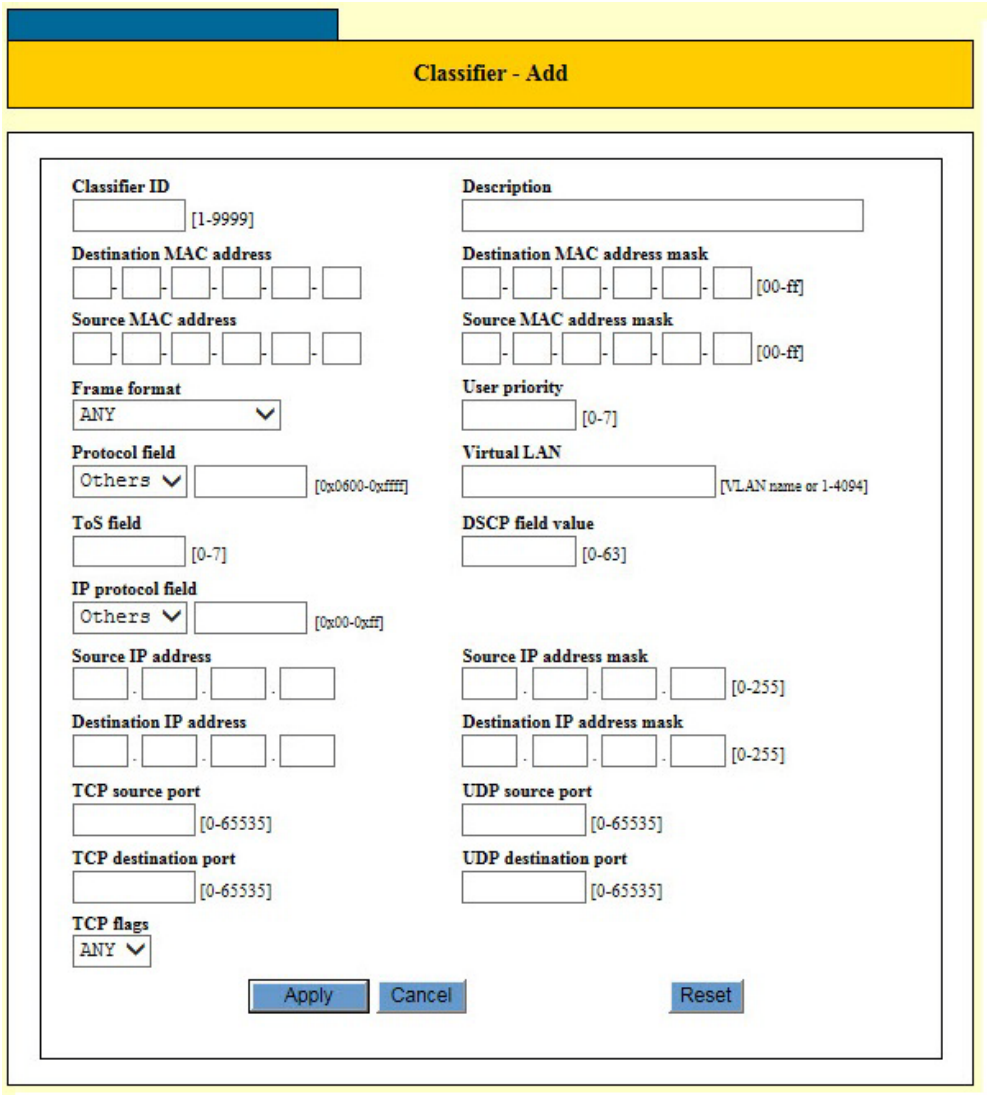

Figure 56. Classifier - Add Window

4. Configure the parameters, as needed. The parameters are described in Table 64.

Table 64. Classifier - Add Window

Parameter	Description
Classifier ID	Use this parameter to specify an ID number for a new classifier. Each classifier on the switch must have a unique ID number. The range is 1 to 9999. This parameter is required.
Description	Use this parameter to specify a description for a new classifier. A description can be up to thirty one alphanumeric characters. Spaces are allowed.
Destination MAC Address	Use this parameter to define a traffic flow by its destination MAC address.
Destination MAC Address Mask	Use this parameter to specify a mask for the destination MAC address. The mask is used to define the destination MAC address as referring to a single node or a range of nodes with consecutive MAC addresses. The values in the mask can be either of the following: F - Use this value to indicate the parts of the destination MAC address the switch should filter on. 0 (zero) - Use this value to indicate the parts of the destination MAC address the switch should ignore.
Source MAC Address	Use this parameter to define a traffic flow by its source MAC address.

Table 64. Classifier - Add Window (Continued)

Parameter	Description
Source MAC Address Mask	Use this parameter to specify a mask for the source MAC address. The mask is used to define the source MAC address as referring to a single node or a range of nodes with consecutive MAC addresses. The values in the mask can be either of the following: F - Use this value to indicate the parts of the source MAC address the switch should filter on. 0 (zero) - Use this value to indicate the parts of the source MAC address the switch should ignore.
Frame Format	Use this parameter to define a traffic flow by its Ethernet format. The selections are listed here: Any - Use this value to specify all Ethernet format types. This is the default value. ETHII-Untagged - Use this value to specify Ethernet II untagged packets. ETHII-Tagged - Use this value to specify Ethernet II tagged packets. 802.2-Untagged - Use this value to specify Ethernet 802.2 untagged packets. 802.2-Tagged - Use this value to specify Ethernet 802.2 tagged packets.
User Priority	Use this parameter to define a traffic flow by the user priority level in tagged Ethernet frames. The range is 0 to 7.

Table 64. Classifier - Add Window (Continued)

Parameter	Description
Protocol Field	Use this parameter to define a traffic flow by the protocol specified in the Ethertype field of the MAC header in an Ethernet II frame. Possible values in the pull-down menu are listed here: Others IP ARP RARP You may select only one protocol. If you select Others, you may enter the protocol number in the Ethertype field of the MAC header in Ethernet II frames. You may enter the number in decimal or hexadecimal format. The decimal range is 1536 to 65535. The hexadecimal range is 0x600 to 0xFFFF.
Virtual LAN	Use this parameter to define a traffic flow of tagged packets by the VLAN ID number. You may specify the VLAN by its name or VID. The VID range is 1 to 4094. You may specify only one VLAN.
TOS Field	Use this parameter to define a traffic flow by the Type of Service value. The range is 0 to 7.
DSCP Field Value	Use this parameter to define a traffic flow by the DSCP (DiffServ Code Point) value. The range is 0 to 63.

Table 64. Classifier - Add Window (Continued)

Parameter	Description
IP Protocol Field	Use this parameter to define a traffic flow by the IP Layer 3 protocol. Possible values in the pull-down menu are listed here: Others TCP UDP ICMP IGMP If you select Others, enter an IP Layer 3 protocol number in the field next to the pull-down menu. The number must be entered in hexadecimal format. The number must be preceded by “0x”. The range is 0x00 to 0xFF.
Source IP Address	Use this parameter to define a traffic flow by a source IP address. The address can be for a specific node or subnet.
Source IP Address Mask	Use this parameter to define a mask for the source IP address. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask “255.255.255.0”.
Destination IP Address	Use this parameter to define a traffic flow by a destination IP address. The address can be for a specific node or subnet.
Destination IP Address Mask	Use this parameter to define a mask for the destination IP address. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask “255.255.255.0”.

Table 64. Classifier - Add Window (Continued)

Parameter	Description
TCP Source Port	Use this parameter to define a traffic flow by a source TCP port. This field requires that the IP Protocol Field be set to TCP
TCP Destination Port	Use this parameter to define a traffic flow by a destination TCP port. This field requires that the IP Protocol Field be set to TCP.
UDP Source Port	Use this parameter to define a traffic flow by a source UDP port. This field requires that the IP Protocol Field be set to UDP
UDP Destination Port	Use this parameter to define a traffic flow by a destination UDP port. This field requires that the IP Protocol Field be set to UDP.
TCP Flags	Use this parameter to define a traffic flow by a TCP flag. This field requires that the IP Protocol Field be set to TCP. The options are listed here: URG - Urgent ACK - Acknowledgement PSH - Push RST - Reset SYN - Synchronization FIN - Finish

5. After defining the variables of the classifier, click the Apply button to create the classifier.

6. To permanently save your changes in the configuration file, select the Save button above the main menu.

Modifying a Classifier

This procedure explains how to modify a classifier.

To modify a classifier, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Classifier option from the Switch Settings menu.

   The Switch Settings - Classifier window is shown in Figure 55 on page 242.
3. In the Classifier List table, check the value in the Number of Active References column for the classifier you want to modify.

   If the value is 0, you may continue with the next step to modify the classifier. If the value is 1 or more, do not continue. The classifier is assigned to a QoS policy that is assigned to one or more switch ports. You have to remove the ports from the policy before you can modify the classifier. For instructions, refer to “Modifying a QoS Policy” on page 290.
4. In the Classifier List table, click the dialog circle of the classifier you want to modify. You may modify only one classifier at a time.
5. Click the Edit button.

   The switch displays the Classifier - Edit window. The window contains the settings of the selected classifier.
6. Modify the parameters as necessary. The parameters are described in Table 64 on page 244.
7. After modifying the parameters of the classifier, click the Apply button to implement your changes.
8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting a Classifier

To delete a classifier, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Classifier option from the Switch Settings menu.

   The Switch Settings - Classifier window is shown in Figure 55 on page 242.
3. In the Classifier List table, check the value in the Number of References column for the classifier you want to delete.

   If the value is 0, you may continue with the next step to delete the classifier. If the value is 1 or more, do not continue. The classifier is assigned to one or more QoS policies. You have to remove the classifier from the policies before you can delete it. For instructions, refer to “Modifying a Flow Group” on page 277.
4. In the Classifier List table, click the dialog circle of the classifier you want to delete. You may delete only one classifier at a time.
5. Click the Delete button. To delete all of the classifiers, click the Delete All button.

   The switch displays a confirmation prompt.
6. Click the OK button to delete the classifier or Cancel to retain the classifier.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 24

Quality of Service Policies Overview

This chapter describes Quality of Service (QoS). Sections in the chapter include:

Overview

Quality of Service allows you to prioritize traffic and/or limit the bandwidth available to it. The concept of QoS is a departure from the original networking protocols, which treated all traffic on the Internet or within a LAN in the same manner. Without QoS, every traffic type is equally likely to be dropped if a link becomes oversubscribed. This approach is now inadequate in many networks, because traffic levels have increased and networks transport time-critical applications such as streams of video and data. QoS also enables service providers to easily supply different customers with different amounts of bandwidth.

Configuring Quality of Service involves two separate stages:

- Classifying traffic into flows, according to a wide range of criteria. Classification is performed by the switch's packet classifiers, described in Chapter 22, "Classifier Overview" on page 233.
- Acting on these traffic flows.

Quality of Service is a broadly used term that encompasses as a minimum both Layer 2 and Layer 3 in the OSI model. QoS is typically demonstrated by how the switch accomplishes the following:

- Assigns priority to incoming frames, if they do not carry priority information
- Maps prioritized frames to traffic classes, or maps frames to traffic classes based upon other criteria
- Maps traffic classes to egress queues, or maps prioritized frames to egress queues
- Provides maximum bandwidth limiting for traffic classes, egress queues and/or ports
- Schedules frames in egress queues for transmission (for example, empty queues in strict priority or samples each queue)
- Relabels the priority of frames
- Determines which frames to drop if the network becomes congested
- Reserves memory for switching/routing or QoS operation (e.g. reserving buffers for egress queues, or buffers to store packets with particular characteristics)

Note
QoS is only performed on packets that are switched at wire speed. This includes IP, IP multicast, IPX, and Layer 2 traffic within VLANs.

The QoS functionality described in this chapter sorts packets into various flows, according to the QoS policy that applies to the port the traffic is received on. The switch then allocates resources to direct this traffic according to bandwidth or priority settings in the policy. A policy contains traffic classes, flow groups, and classifiers. Therefore, to configure QoS policies, you have to perform the following tasks:

- Create *classifiers* to sort packets into traffic flows.
- Create *flow groups* and add classifiers to them. Flow groups are groups of classifiers which group together similar traffic flows. You can apply QoS prioritization to flow groups.
- Create *traffic classes* and add flow groups to them. Traffic classes are groups of flow groups and are central to QoS. You can apply bandwidth limits and QoS prioritization to traffic classes.
- Create *policies* and add traffic classes to them. Policies are groups of traffic classes. A policy defines a complete QoS solution for a port or group of ports.
- Associate policies with ports.

Note
The steps listed above are in a conceptually logical order, but the switch cannot check a policy for errors until the policy is attached to a port. To simplify error diagnosis, define your QoS configuration on paper first, and then enter it into the management software starting with classifiers.

Policies, traffic classes, and flow groups are created as individual entities. When a traffic class is added to a policy, a logical link is created between the two entities. Destroying the policy unlinks the traffic class, leaving the traffic class in an unassigned state. Destroying a policy does not destroy any of the underlying entities. Similarly, destroying a traffic class unlinks flow groups, and destroying flow groups unlinks classifiers.

Classifiers

Classifiers identify particular traffic flows, and range from general to specific. (See Chapter 22, “Classifier Overview” on page 233 for more information.) Note that a single classifier should not be used in different flows that will end up, through traffic classes, assigned to the same policy. A classifier should only be used once per policy. Traffic is matched in the order of classifiers. For example, if a flow group has classifiers 1, 3, 2 and 5, that is the order in which the packets are matched.

Flow Groups

Flow groups group similar traffic flows together, and allow more specific QoS controls to be used, in preference to those specified by the traffic class. Flow groups consist of a small set of QoS parameters and a group of classifiers. After a flow group has been added to a traffic class it cannot be added to another traffic class. A traffic class may have many flow groups. Traffic is matched in the order of the flow groups. For example, if a traffic class has flow groups 1, 3, 2 and 5, this is the order in which the packets are matched.

QoS controls at the flow group level provide a QoS hierarchy. Non-default flow group settings are always used, but if no setting is specified for a flow group, the flow group uses the settings for the traffic class to which it belongs. For example, you can use a traffic class to limit the bandwidth available to web and FTP traffic combined. Within that traffic class, you can create two different flow groups with different priorities, to give web traffic a higher priority than FTP. Web traffic would then be given preferential access to bandwidth, but would be limited to the bandwidth limit of the traffic class.

Traffic Classes

Traffic classes are the central component of the QoS solution. They provide most of the QoS controls that allow a QoS solution to be deployed. A traffic class can be assigned to only one policy. Traffic classes consist of a set of QoS parameters and a group of QoS *flow groups*. Traffic can be prioritized, marked (IP TOS or DSCP field set), and bandwidth limited. Traffic is matched in the order of traffic class. For example, if a policy has traffic classes 1, 3, 2 and 5, this is the order in which the packets are matched.

Policies

QoS policies consist of a collection of user defined traffic classes. A policy can be assigned to more than one port, but a port may only have one policy.

Note that the switch can only perform error checking of parameters and parameter values for the policy and its traffic classes and flow groups when the policy is set on a port.

QoS controls are applied to ingress traffic on ports. Therefore, to control a particular type of traffic, an appropriate QoS policy must be attached to each port that type of traffic ingresses.

Although a policy can be applied to an egress port, the classifiers and the QoS controls are actually applied by the switch on the ingress ports of the traffic. This means the parameters used to classify the traffic and the actions specified by the policy are checked and applied on the ingress traffic of every port, before the traffic reaches an egress queue. As a consequence, a policy is never applied to the whole aggregated traffic of a designated egress port, but rather to the individual ingress flows destined to the port.

The effects of this behavior become evident when using the maximum bandwidth feature of QoS. Here is an example. Suppose you have a policy that assigns 5 Mbps of maximum bandwidth to an egress port. Now assume there are 10 ports on the switch where ingress traffic matches the criteria specified in the classifier assigned to the policy of the egress port. Since the policy considers each ingress flow separately, the result would be a maximum bandwidth of 50 Mbps (10 x 5 Mbps) on the egress port, because there are 10 flows, one from each ingress port, directed to the egress port.

An additional factor to consider when specifying an egress port in a policy is that if the destination MAC address of the traffic flow has not been learned by the egress port or, alternatively, added as a static address to the port, the policy remains inactive. This is because the ingress ports consider the traffic as unknown traffic and flood the traffic to all the ports. This applies equally to unknown unicast and unknown multicast traffic, as well as broadcast traffic.

QoS Policy Guidelines

The following is a list of QoS policy guidelines:

- A classifier may be assigned to many flow groups. However, assigning a classifier more than once within the same policy may lead to undesirable results. A classifier may be used successfully in many different policies.
- A flow group must be assigned at least one classifier but may have many classifiers.
- A flow group may be assigned to only one traffic class.
- A traffic class may have many flow groups.
- A traffic class may only be assigned to one policy.
- A policy may have many traffic classes.
- A policy may be assigned to many ports.
- A port may only have one policy.
- A policy that is not assigned to any port on the switch is inactive.
- A policy must have at least one action defined in the flow group, traffic class, or the policy itself. A policy without an action is invalid.
- The switch can store up to 64 flow groups.
- The switch can store up to 64 traffic classes.
- The switch can store up to 64 policies.

Packet Processing

You can use the switch's QoS tools to perform any combination of the following functions on a packet flow:

- Limiting bandwidth
- Prioritizing packets to determine the level of precedence the switch will give to the packet for processing
- Replacing the VLAN tag User Priority to enable the next switch in the network to process the packet correctly
- Replacing the TOS precedence or DSCP value to enable the next switch in the network to process the packet correctly.

Bandwidth Allocation

Bandwidth limiting is configured at the level of traffic classes, and encompasses the flow groups contained in the traffic class. Traffic classes can be assigned maximum bandwidths, specified in kbps, Mbps, or Gbps.

Packet Prioritization

The switch has four Class of Service (CoS) egress queues, numbered from 0 to 3. Queue 3 has the highest priority. When the switch becomes congested, it gives high priority queues precedence over lower-priority queues. When the switch has information about a packet's priority, it sends the packet to the appropriate queue. You can specify the queue where the switch sends traffic, how much precedence each queue has, and whether priority remapping is written into the packet's header for the next hop to use.

Prioritizing packets cannot improve your network's performance when bandwidth is over-subscribed to the point that egress queues are always full. If one type of traffic is causing the congestion, you can limit its bandwidth. Other solutions are to increase bandwidth or decrease traffic.

You can set a packet's priority by configuring a priority in the flow group or traffic class to which the packet belongs. The packet is put in the appropriate CoS queue for that priority. If the flow group and traffic class do not include a priority, the switch can determine the priority from the VLAN tag User Priority field of incoming tagged packets. The packet is put in the appropriate CoS queue for its VLAN tag User Priority field. If neither the traffic class / flow group priority nor the VLAN tag User Priority is set, the packet is sent to the default queue, queue 1.

Both the VLAN tag User Priority and the traffic class / flow group priority setting allow eight different priority values (0-7). These eight priorities are mapped to a port's four CoS queues. The default mappings are shown in Table 59 on page 219. Note that priority 0 is mapped to CoS queue 1 instead of CoS queue 0 because tagged traffic that has never been prioritized has a VLAN tag User Priority of 0. If priority 0 was mapped to CoS queue 0, this default traffic goes to the lowest queue, which is probably undesirable. This mapping also makes it possible to give some traffic a lower priority than the default traffic.

Replacing Priorities

The traffic class or flow group priority (if set) determines the egress queue a packet is sent to when it egresses the switch, but by default has no effect on how the rest of the network processes the packet. To permanently change the packet's priority, you need to replace one of two priority fields in the packet header:

- The User Priority field of the VLAN tag header. Replacing this field relabels VLAN-tagged traffic, so that downstream switches can process it appropriately.
- The DSCP value of the IP header's TOS byte (Figure 54 on page 237). Replacing this field may be required as part of the configuration of a DiffServ domain. See "DiffServ Domains" on page 262 for information on using the QoS policy model and the DSCP value to configure a DiffServ domain.

VLAN Tag User Priorities

Within a flow group or traffic class, the VLAN tag User Priority value of incoming packets can be replaced with the priority specified in the flow group or traffic class. Replacement occurs before the packet is queued, so this priority also sets the queue priority.

DSCP Values

There are three methods for replacing the DSCP byte of an incoming packet. You can use these methods together or separately. They are described in the order in which the switch performs them.

- The DSCP value can be overwritten at ingress, for all traffic in a policy.
- The DSCP value in the packet can be replaced at the traffic class or flow group level.
- You can use these two replacements together at the edge of a DiffServ domain, to initialize incoming traffic.
- The DSCP value in a flow of packets can replaced if the bandwidth allocated to that traffic class is exceeded. This option allows the next switch in the network to identify traffic that exceeded the bandwidth allocation.

DiffServ Domains

Differentiated Services (DiffServ) is a method of dividing IP traffic into classes of service, without requiring that every router in a network remember detailed information about traffic flows. DiffServ operates within a *DiffServ domain*, a network or subnet that is managed as a single QoS unit. Packets are classified according to user-specified criteria at the edge of the network, divided into classes, and assigned the required class of service. Then packets are marked with a Differentiated Services Code Point (DSCP) tag to indicate the class of service to which they belong. The DSCP value is written into the TOS field of the IP header. Routers within the network then use this DSCP value to classify packets and assign QoS appropriately. When a packet leaves the DiffServ domain, the DSCP value can be replaced with a value appropriate for the next DiffServ domain.

A simple example of this process is shown in Figure 57, for limiting the amount of bandwidth used by traffic from a particular IP address. In the domain shown, this bandwidth limit is supplied by the class of service represented by a DSCP value of 40. In the next DiffServ domain, this traffic is assigned to the class of service represented by a DSCP value of 3.

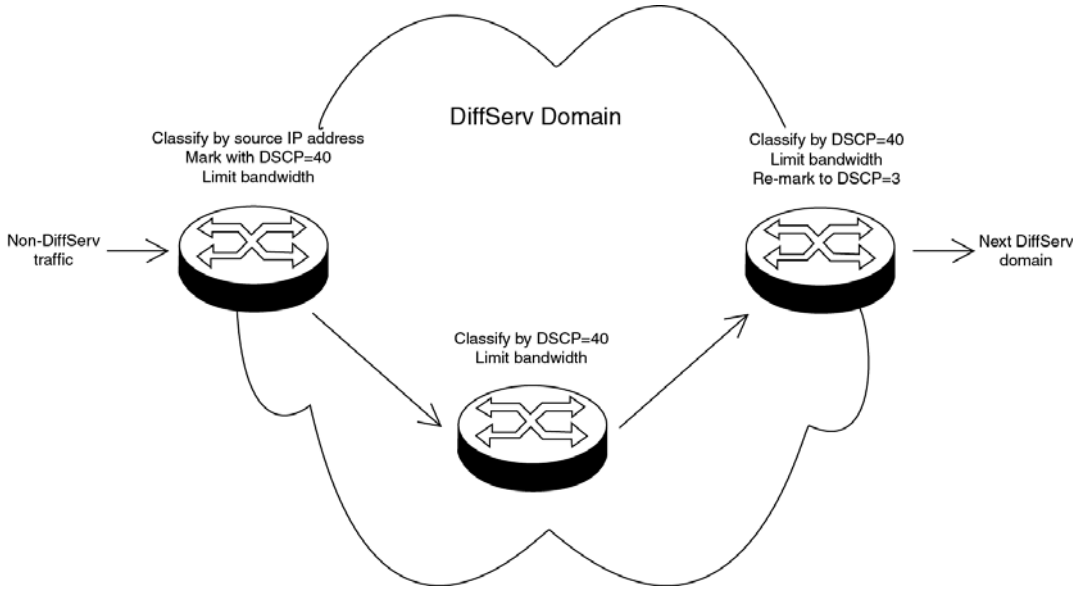

Figure 57. DiffServ Domain Example

To use the QoS tool set to configure a DiffServ domain:

1. As packets come into the domain at edge switches, replace their DSCP value, if required.

    - Classify the packets according to the required characteristics. For

available options, see Chapter 22, "Classifier Overview" on page 233.

- ❒ Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.
- ❒ Give each traffic class the priority and/or bandwidth limiting controls that are required for that type of packet within this part of the domain.
- ❒ Assign a DSCP value to each traffic class, to be written into the TOS field of the packet header.

2. On switches and routers within the DiffServ domain, classify packets according to the DSCP values that were assigned to traffic classes on the edge switches.

   - ❒ Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.
   - ❒ Give each traffic class the priority and/or bandwidth limiting controls that are required for that type of packet within this part of the domain. These QoS controls need not be the same for each switch.

3. As packets leave the DiffServ domain, classify them according to the DSCP values.

   - ❒ Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.
   - ❒ Give each traffic class the priority and/or bandwidth limiting controls required for transmission of that type of packet to its next destination, in accordance with any Service Level Agreement (SLA) with the providers of that destination.
   - ❒ If necessary, assign a different DSCP value to each traffic class, to be written into the TOS field of the packet header, to match the DSCP or TOS priority values of the destination network.

Examples

The following examples demonstrate how to implement QoS in three situations:

- “Voice Applications”
- “Video Applications” on page 266
- “Critical Database” on page 268

Voice Applications

Voice applications typically require a small but consistent bandwidth. They are sensitive to *latency* (interpacket delay) and *jitter* (delivery delay). Voice applications can be set up to have the highest priority.

This example creates two policies that ensure low latency for all traffic sent by and destined to a voice application located on a node with the IP address 149.44.44.44. The policies raise the priority level of the packets to 7, the highest level. Policy 6 is for traffic from the application that enters the switch on port 1. Policy 11 is for traffic arriving on port 8 going to the application. The components of the policies are shown in Figure 58 on page 265.

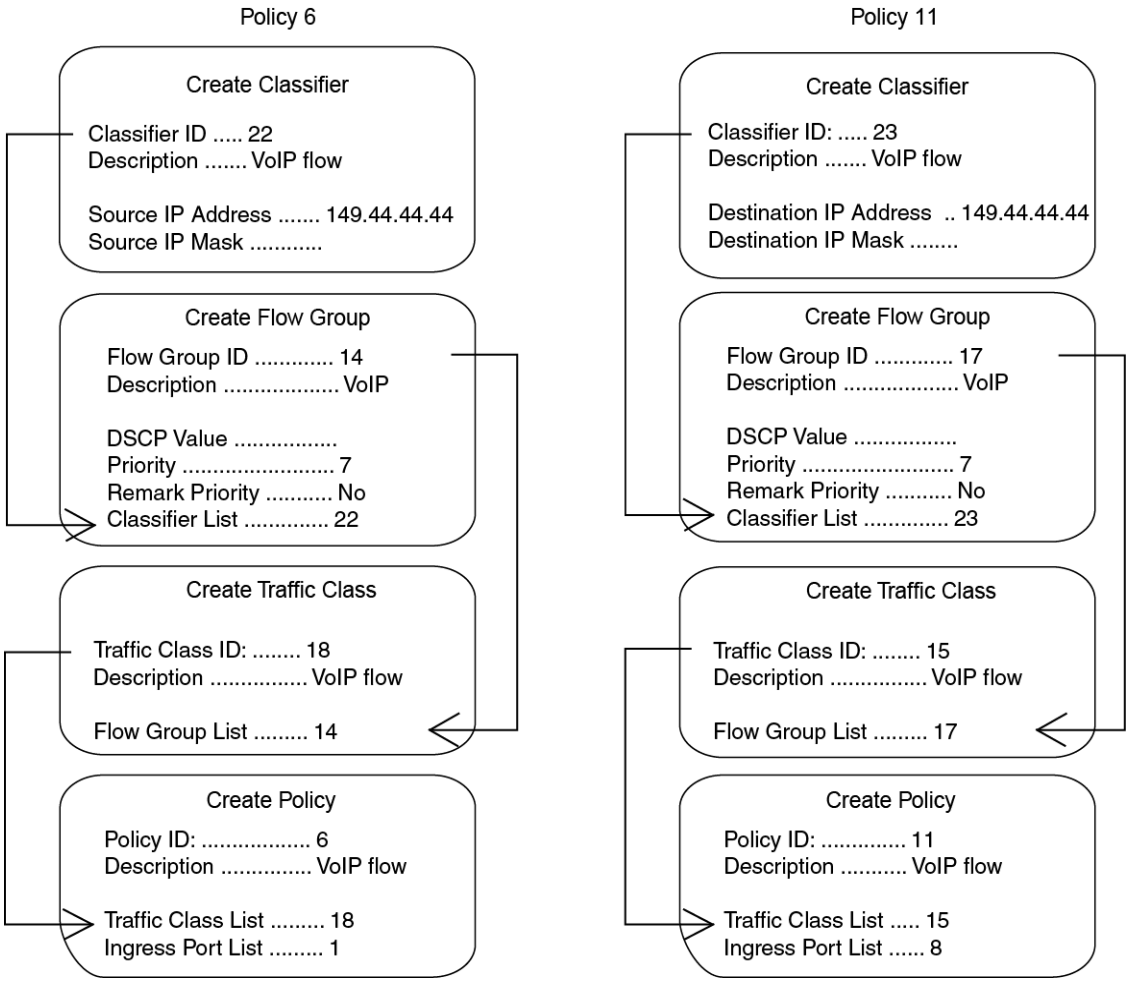

Figure 58. QoS Voice Application Example

The parts of the policies are described here:

- Classifier - Defines the traffic flow by specifying the IP address of the node with the voice application. The classifier for Policy 6 specifies the address as a source address because this classifier is part of a policy for packets coming from the application. The classifier for Policy 11 specifies the address as a destination address because this classifier is part of a policy for packets going to the application.
- Flow Group - Specifies the new priority level of 7 for the packets. In this example the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only as the packets traverse the switch. To change the packets' priority level so that they leave with the new level, you would change option 5, Remark Priority, to Yes.
- Traffic Class - No action is taken by the traffic class, other than to specify the flow group. Traffic class has a priority setting you can

use to override the priority level of packets, just as in a flow group. If you enter a priority value in both places, the setting in the flow group overrides the setting in the traffic class.

- Policy - Specifies the traffic class and the port to which the policy is to be assigned. Policy 6 is applied to port 1 because this is where the application is located. Policy 11 is applied to port 8 because this is where traffic going to the application will be received.

Video Applications

Video applications typically require a larger bandwidth than voice applications. Video applications can be set up to have a high priority and buffering, depending on the application.

This example creates policies with low latency and jitter for video streams (for example, net conference calls). The policies in Figure 59 on page 267 assign the packets a priority level of 4. The policies also limit the bandwidth for the video streams to 5 Mbps to illustrate how you can combine a change to the priority level with bandwidth restriction to further define traffic control. The node containing the application has the IP address 149.44.44.44. Policy 17 is assigned to port 1, where the application is located, and Policy 32 is assigned to port 8 where packets destined to the application enter the switch.

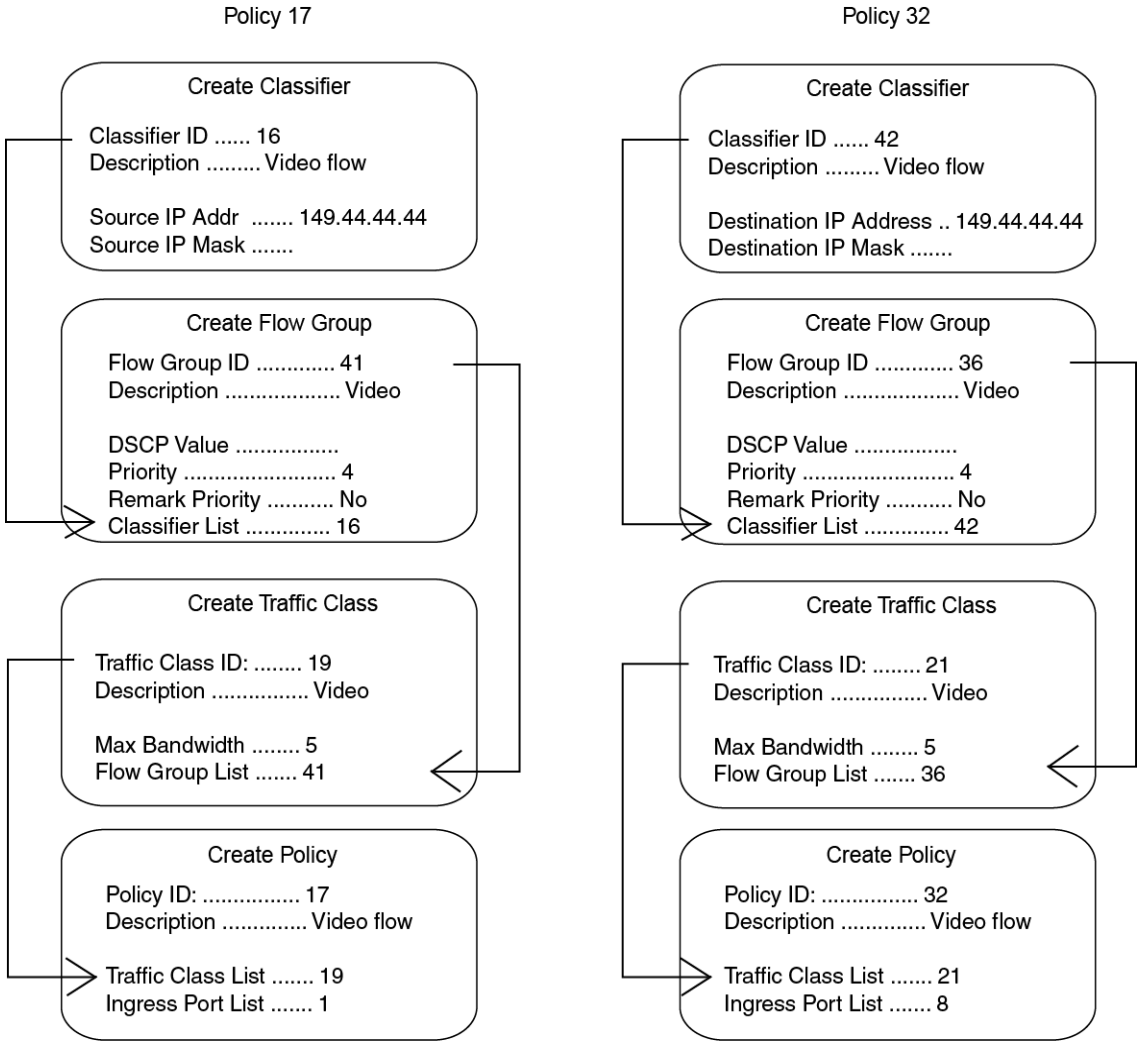

Figure 59. QoS Video Application Example

The parts of the policies are:

- Classifier - Specifies the IP address of the node with a video application. The classifier for Policy 17 specifies the address as a source address since this classifier is part of a policy concerning packets coming from the application. The classifier for Policy 32 specifies the address as a destination address because this classifier is part of a policy concerning packets going to the application.
- Flow Group - Specifies the new priority level of 4 for the packets. As with the previous example, the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only while the packets traverse the switch. To alter the packets so they leave containing the new level, you would change option 5, Remark Priority, to Yes.

- Traffic Class - The packet stream is assigned a maximum bandwidth of 5 Mbps. Bandwidth assignment can only be made at the traffic class level.
- Policy - Specifies the traffic class and the port where the policy is to be assigned.

Critical Database

Critical databases typically require a high bandwidth. They also typically require less priority than either voice or video.

The policies in Figure 60 assign 50 Mbps bandwidth, with no change to priority, to traffic going to and from a database. The database is located on a node with the IP address 149.44.44.44 on port 1 of the switch.

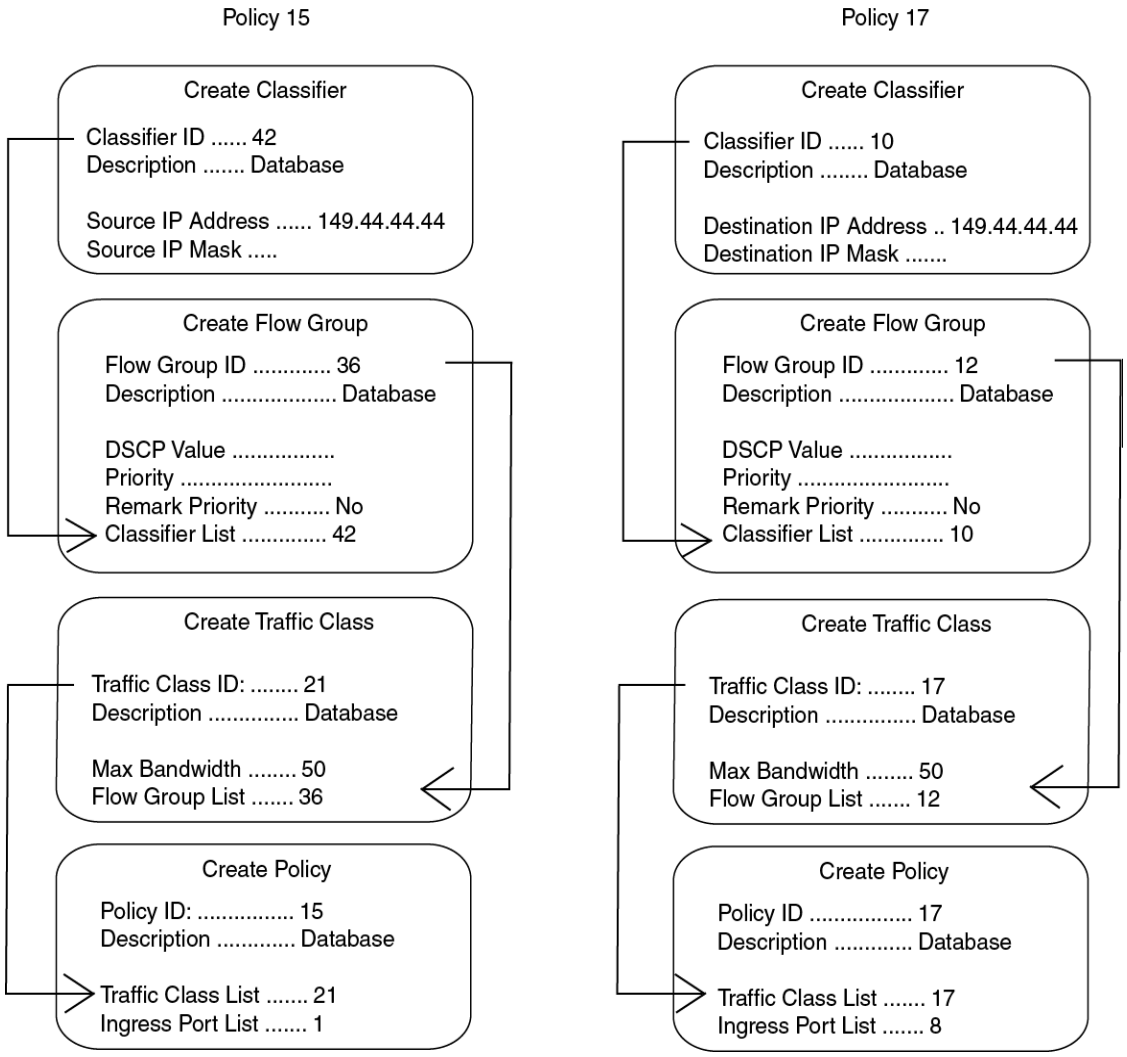

Figure 60. QoS Critical Database Example

Policy Component Hierarchy

The purpose of this example is to illustrate the hierarchy of the components of a QoS policy and how that hierarchy needs to be taken into account when assigning new priority and DSCP values. A new priority can be set at the flow group and traffic class levels, while a new DSCP value can be set at all three levels—flow group, traffic class and policy. The basic rules are:

- A new setting in a flow group takes precedence over a corresponding setting in a traffic class or policy.
- A new setting in a traffic class takes precedence over a corresponding setting in a policy.
- A new setting in a policy is used only if there is no corresponding setting in a flow group or traffic class.

This concept is illustrated in Figure 61 on page 270. It shows a policy for a series of traffic flows consisting of subnets defined by their destination IP addresses. New DSCP values for the traffic flows are established at different levels within the policy.

Traffic flows 149.11.11.0 and 149.22.22.0, defined by classifiers 1 and 2, are attached to a flow group, traffic class, and policy that contain new DSCP values. Because a setting in a flow group takes precedence over that of a traffic class or policy, the value in the flow group is used. The result is that the DSCP value in the two traffic flows is changed to 10.

The flow group for traffic flows 149.33.33.0 and 149.44.44.0, defined in classifiers 3 and 4, does not contain a new DSCP value. Therefore, the new value in the traffic class is used, in this case 30. The policy also has a DSCP setting, but it is not used for these traffic flows because a new DSCP setting in a traffic class takes precedence over that of a policy.

Finally, the new DSCP value for traffic flows 149.55.55.0 and 149.66.66.0, defined in classifiers 5 and 6, is set at the policy level to a value of 55 because the flow group and traffic class do not specify a new value.

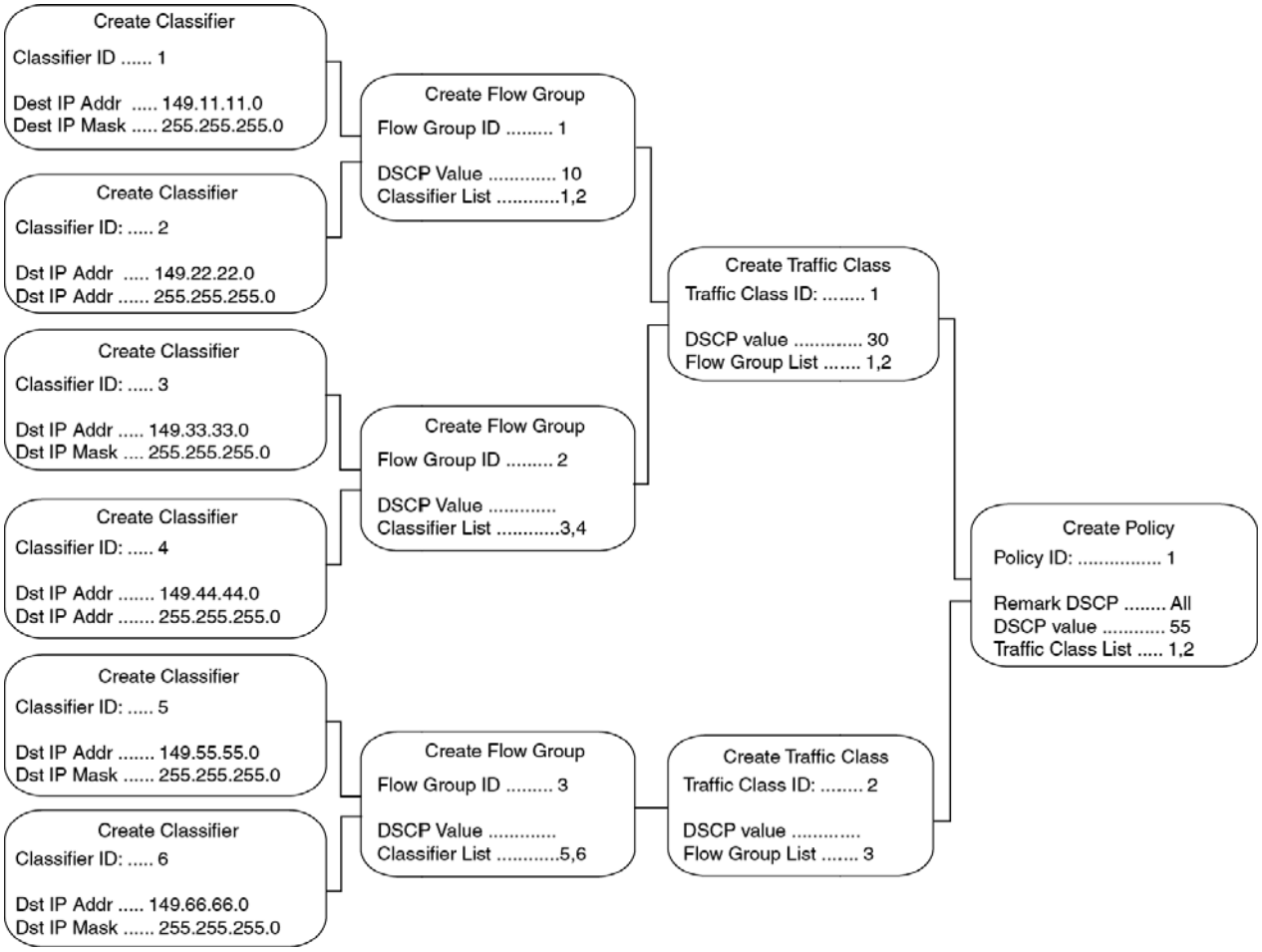

Figure 61. Policy Component Hierarchy Example

Chapter 25

Quality of Service Policies

This chapter contains instructions on how to configure Quality of Service (QoS) policies. This chapter contains the following procedures:

Note
For background information, refer to Chapter 24, “Quality of Service Policies Overview” on page 251.

Displaying the QoS Policies Window

To display the QoS policies window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62.

Figure 62. Switch Settings - Policy Based QoS Window

The three sections in the window are defined in Table 65.

Table 65. Switch Settings - Policy Based QoS Window

Section	Description
1	Use this section to manage QoS policies. The columns in the table are described in Table 66. For instructions, refer to “Managing Policies” on page 286.
2	Use this section to manage QoS traffic classes. The columns in the table are described in Table 67 on page 273. For instructions, refer to “Managing Traffic Classes” on page 279.
3	Use this section to manage flow groups. The columns in the table are described in Table 68 on page 274. For instructions, refer to “Managing Flow Groups” on page 275.

The QoS Policy List table in the window displays the current policies on the switch. The columns in the table are described in Table 66.

Table 66. QoS Policy List Table

Column	Description
QoS Policy ID	Displays the ID number of a policy.
Description	Displays the description of a policy.
Active	Displays the status of a policy. The status of a policy can be active or inactive. A policy has an active status when it is assigned to at least one switch port and an inactive state when it is not assigned to any switch ports.
Traffic Class List	Displays the traffic classes of the policy.
Ingress Port	Displays the ingress ports of a policy.

The Traffic Class List table in the Switch Settings - Policy Based QoS window displays the current traffic classes on the switch. The columns in the table are described in Table 67.

Table 67. Traffic Class List Table

Column	Description
Traffic Class ID	Displays the ID number of a traffic class.

Table 67. Traffic Class List Table (Continued)

Column	Description
Description	Displays the description of a traffic class.
Active	Displays the state of a traffic class. The state of a traffic class can be active or inactive. A traffic class has an active status if it belongs to a policy that is assigned to at least one switch port. A traffic class has an inactive status if it is not assigned to any policies or to policies that have not been assigned to switch ports.
QoS Policy ID	Displays the QoS policy of a traffic class.
Flow Group ID	Displays the flow groups of a traffic class.

The Flow Group List table in the Switch Settings - Policy Based QoS window displays the current flow groups on the switch. The columns in the table are described in Table 68.

Table 68. Flow Group List Table

Column	Description
Flow Group ID	Displays the ID number of a flow group.
Descriptions	Displays the description of a flow group.
Active	Displays the status of a flow group. The status can be active or inactive. A flow group is active if it is part of a policy that is assigned to a switch port. A flow group is inactive if it is not part of any policies or if the policies are not assigned to any ports.
Traffic Class ID	Displays the ID numbers of the traffic classes of the flow groups.
Classifier ID	Displays the classifiers of a flow group.

Managing Flow Groups

This section contains the following procedures:

- "Adding a Flow Group"
- "Modifying a Flow Group" on page 277
- "Deleting a Flow Group" on page 278

Adding a Flow Group

To add a new flow group to the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.
3. Click the Add button in the Flow Group section of the window.

   The switch displays the Flow Group - Add window, shown in Figure 63.

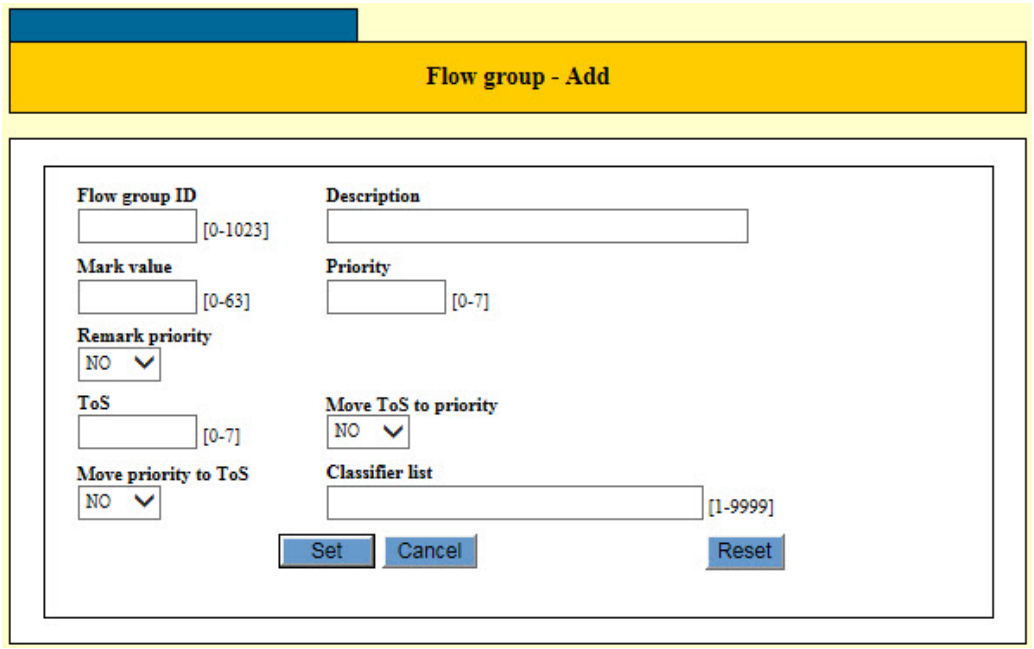

Figure 63. Flow Group - Add Window

4. Configure the parameters in the Flow Group - Add window, as needed. The parameters are described in Table 69 on page 276.

Table 69. Flow Group - Add Window

Parameter	Description
ID	Use this parameter to assign an ID number to a flow group. Each flow group on the switch must have a unique ID number. The range is 0 to 1023.
Description	Use this parameter to assign a description to the flow group. A description can have up to 31 alphanumeric characters. Spaces are allowed.
Mark Value	Use this parameter to specify a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.
Priority	Use this parameter to specify a new user 802.1p priority value for the packets. The range is 0 to 7. You can specify a new priority value at both the flow group and traffic class levels. If you specify a new user priority value at both levels, the value in the flow group here overrides the value in Traffic Class. If you want the packets to retain the new value when they exit the switch, change Remark Priority to Yes.
Remark Priority	If set to Yes, replaces the user priority value in the packets with the new value specified in the Priority parameter when the packets leave the switch.
ToS	Use this parameter to specify a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. New ToS values can be set in flow groups, traffic classes, and policies. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

Table 69. Flow Group - Add Window (Continued)

Parameter	Description
Move ToS to Priority	Use this parameter to replace the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. The available options are listed here: Yes: Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. No: Does not replace the preexisting 802.1p priority level. This is the default.
Move Priority to ToS	Use this parameter to replace the value in the ToS priority field with the 802.1p priority field in IPv4 packets. The available options are listed here: Yes: Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. No: Does not replace the ToS priority field. This is the default.
Classifier List	Use this parameter to add the classifier to the flow group. The classifier must already exist on the switch. A flow group can have more than one classifier. Separate multiple classifiers with commas or spaces.

5. Click the Set button to add the new flow group to the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying a Flow Group

This procedure explains how to modify a flow group. If the flow group is already part of a QoS policy assigned to one or more switch ports, you have to modify the policy by removing the port assignments before you can modify the flow group. You can reassign the ports to the policy after modifying the flow group.

To modify a flow group, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.

3. In the Flow Group List section of the window, click the dialog box of the flow group you want to modify. You may modify only one flow group at a time.
4. Click the Edit button in the Flow Group List section of the window.

   The switch displays the parameter settings of the selected flow group in the Flow Group - Edit window.
5. Configure the parameters in the window, as needed. The parameters are described in Table 69 on page 276.
6. Click the Set button to activate your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting a Flow Group

This procedure explains how to delete a flow group from the switch. If the flow group to be deleted is already part of a QoS policy assigned to one or more switch ports, you have to modify the policy by removing the port assignments before you can delete the flow group. You can assign the ports back to the policy after you have deleted the flow group.

To delete a flow group, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.
3. In the Flow Group List table, click the dialog box of the flow group you want to delete.
4. Click the Delete button. To delete all of the flow groups, click the Delete All button.

   The switch displays a confirmation prompt.
5. Click the OK button to delete the flow group or Cancel to retain it.

   The flow group is deleted from the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Managing Traffic Classes

This section contains the following procedures:

- "Adding a Traffic Class"
- "Modifying a Traffic Class" on page 284
- "Deleting a Traffic Class" on page 285

Adding a Traffic Class

To add a new traffic class to the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.
3. Click the Add button in the Traffic Class List section of the window.

   The switch displays the Traffic Class - Add window, shown in Figure 64.

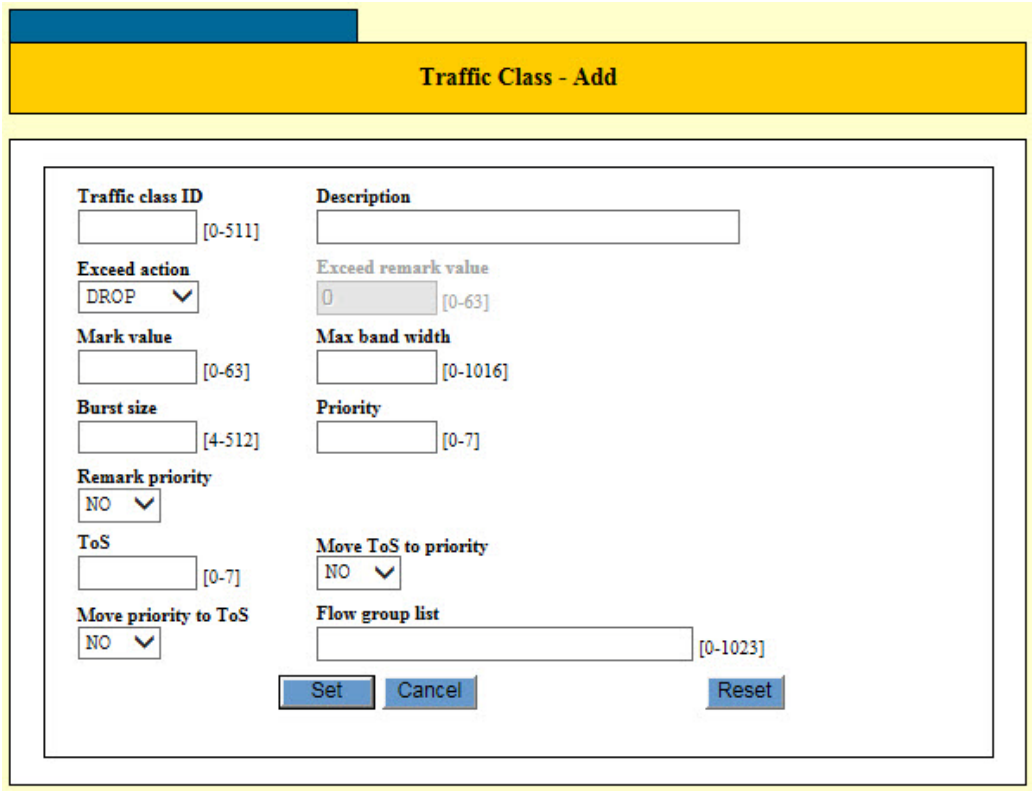

Figure 64. Traffic Class - Add Window

4. Configure the parameters in the Traffic Class - Add window, as needed. The parameters are described in Table 70.

Table 70. Traffic Class - Add Window

Parameter	Description
ID	Use this parameter to assign an ID number to the traffic class. Each traffic class on the switch must have a unique number. The range is 0 to 511. The default is 0. This parameter is required.
Description	Use this parameter to assign a description to the traffic class. A description can be up to 15 alphanumeric characters. Spaces are allowed.
Exceed Action	Use this parameter to specify the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth. The available options are listed here: Drop: Traffic exceeding the bandwidth is discarded. Remark: Packets are forwarded after replacing the DSCP value with the new value specified in Exceed Remark Value. The default is drop.
Exceed Remark Value	Use this parameter to specify the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The range is 0 to 63. The default is 0.
Mark Value	Use this parameter to specify a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.

Table 70. Traffic Class - Add Window (Continued)

Parameter	Description
Max Bandwidth	Use this parameter to specify the maximum available bandwidth for the traffic class. The range is 0 to 1016 Mbps. This parameter determines the maximum rate at which the ingress port accepts packets belonging to the traffic class before either dropping or remarking occurs, depending on the Exceed Action parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified. The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16). If this option is set to 0 (zero), all traffic that matches the traffic class is dropped. However, an access control list can be created to match the traffic that is marked for dropping, or a subset of it, and given an action of permit, to override this. This functionality can be used to discard all but a certain type of traffic.

Table 70. Traffic Class - Add Window (Continued)

Parameter	Description
Burst Size	Use this parameter to specify the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. The default is 512 Kbps. The token bucket is used in situations where you set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded. Tokens are added to the bucket at the same rate as the traffic class' maximum bandwidth, set with option 6, Max Bandwidth. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at the same rate. If the amount of traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic is discarded since no tokens are available for handling the increase. If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded. Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added.

Table 70. Traffic Class - Add Window (Continued)

Parameter	Description
Burst Size (Continued)	To use this parameter you must specify a maximum bandwidth with the Max Bandwidth parameter. Specifying a token bucket size without also entering a maximum bandwidth serves no function.
Priority	Use this parameter to specify the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of four Class of Service (CoS) queues based on the priority value. If you want the packets to retain the new value when they exit the switch, change the Remark Priority parameter to Yes. If you specify a new user priority value here and in Flow Group, the value in Flow Group overwrites the value here.
Remark Priority	Use this parameter to replace the user priority value in the packets with the new value specified in the Priority parameter, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.
ToS	Use this parameter to specify a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A ToS value can be set at all three levels: flow group, traffic class, and policy. The ToS value in a flow group overrides the value specified at the traffic class or policy level, while the ToS value in a traffic class overrides the value in a policy.

Table 70. Traffic Class - Add Window (Continued)

Parameter	Description
Move ToS to Priority	Use this parameter to replace the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. The available options are listed here: Yes: Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. No: Does not replace the preexisting 802.1p priority level. This is the default.
Move Priority to ToS	Use this parameter to replace the value in the ToS priority field with the 802.1p priority field on IPv4 packets. The available options are listed here: Yes: Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. No: Does not replace the ToS priority field. This is the default.
Flow Group List	Use this parameter to specify the flow group for the traffic class. A traffic class can have more than one flow group. Separate multiple flow groups with commas or spaces.

5. Click the Set button to add the new traffic class to the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying a Traffic Class

This procedure explains how to modify an existing traffic class. If the traffic class to be modified is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can modify the traffic class. You can reassign the ports back to the policy after you have finished modifying the traffic class.

To modify a traffic class, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.

3. In the Traffic Class List section of the window, click the dialog box of the traffic class you want to modify. You may modify only one traffic class at a time.

4. Click the Edit button in the Traffic Class section of the QoS window.

   The switch displays the parameter settings of the selected traffic class in the Traffic Class - Edit window.

5. Modify the parameters in the window, as needed. The parameters are described in Table 70 on page 280.

6. Click the Set button to activate your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting a Traffic Class

This procedure explains how to delete a traffic class. If the traffic class to be deleted is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can delete the traffic class. You can reassign the ports back to the policy after you have deleted the traffic class.

To delete a traffic class, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.

2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.

3. In the Traffic Class table, click the dialog box of the traffic class you want to delete.

4. Click the Delete button. To delete all of the traffic classes, click the Delete All button.

   The switch displays a confirmation prompt.

5. Click the OK button to delete the traffic class or Cancel to retain it.

   The traffic class is deleted from the switch.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Managing Policies

This section contains the following procedures:

- “Adding a Policy”
- “Modifying a QoS Policy” on page 290
- “Deleting a QoS Policy” on page 290

Adding a Policy

To add a new QoS policy, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.
3. Click the Add button in the QoS Policy List section of the window.

   The switch displays the QoS Policy - Add window, shown in Figure 65.

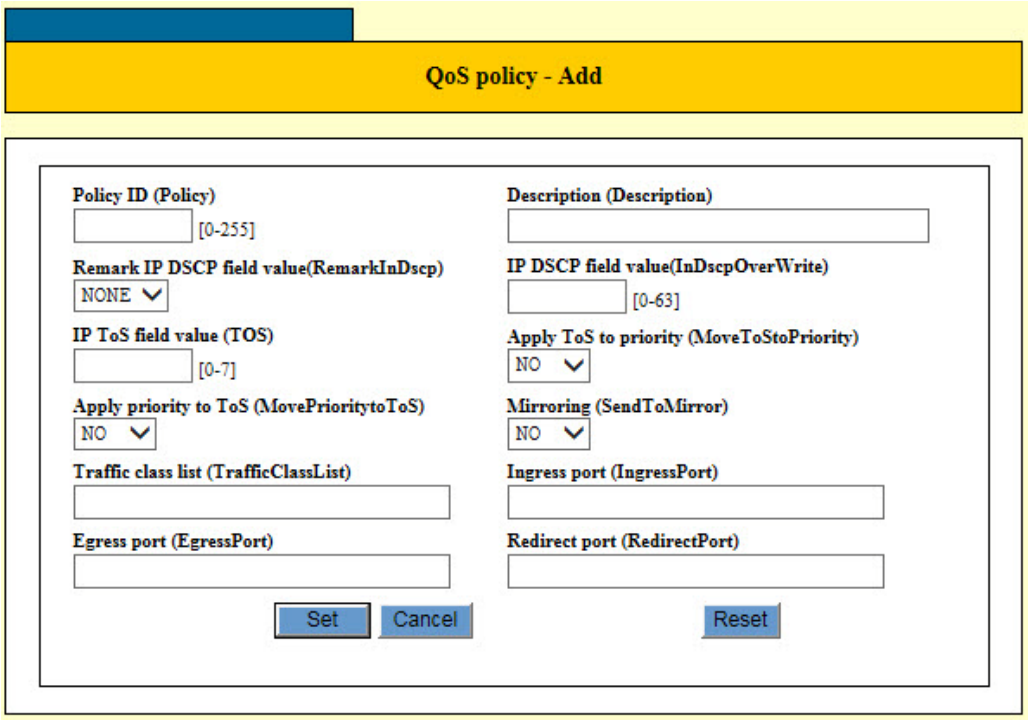

Figure 65. QoS Policy - Add Window

4. Configure the parameters in the QoS Policy - Add window, as needed. The parameters are described in Table 71 on page 287.

Table 71. QoS Policy - Add Window

Parameter	Description
Policy ID (Policy)	Use this parameter to assign an ID number to the policy. Every policy on the switch must have a unique number. The range is 0 to 255. The default is 0. This parameter is required.
Description	Use this parameter to add a description to the new policy. A description can have up to 31 alphanumeric characters. Spaces are allowed. A description is optional.
Remark IP DSCP Field Value (RemarkInDSCP)	Use this parameter to specify whether the DSCP values in the ingress packets are overwritten. The available options are listed here: None - The DSCP values in the packets are not overwritten. All - The DSCP values in the packets are overwritten.
IP DSCP Field Value (InDscpOverWrite)	Use this parameter to specify a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. None value is accepted. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value is specified at the flow group or traffic class level.

Table 71. QoS Policy - Add Window (Continued)

Parameter	Description
IP ToS Field Value (TOS)	Use this parameter to specify a replacement value for the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. None value is accepted. A ToS value can be set at all three levels: flow group, traffic class, and policy. The ToS value in a flow group overrides the value specified at the traffic class or policy level, while the ToS value in a traffic class overrides the value in a policy.
Apply ToS to Priority (MoveToStoPriority)	Use this parameter to replace the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. The available options are listed here: Yes: Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. No: Does not replace the preexisting 802.1p priority level. This is the default.
Apply Priority to ToS (MovePrioritytoToS)	Use this parameter to replace the value in the ToS priority field with the 802.1p priority field in IPv4 packets. The available options are listed here: Yes: Replaces the value in the ToS priority field with the 802.1p priority field in IPv4 packets. No: Does not replace the ToS priority field. This is the default.

Table 71. QoS Policy - Add Window (Continued)

Parameter	Description
Mirroring (SendtoMirror)	Use this parameter to copy the traffic that meets the criteria of the policy's classifiers to a destination mirror port. The available options are listed here: Yes: Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror. For instructions, refer to Chapter 13, "Port Mirroring" on page 147. No: Does not copy the traffic to a destination mirror port. This is the default.
Traffic Class List (TrafficClassList)	Use this parameter to specify the traffic class for the policy. The traffic class, which is specified by its ID number, must already exist. A policy can have more than one traffic class. Separate multiple ID numbers with commas or spaces.
Ingress Port (IngressPort)	Use this parameter to specify the ingress port of the policy. A policy can be assigned to more than one ingress port. Separate multiple port numbers with commas or spaces. A port can be an ingress port of only one policy at a time.
Egress Port (EgressPort)	Use this parameter to specify the egress port of the policy. You can enter only one egress port. A port can be an egress port of only one policy at a time. A port that is already an egress port of a policy must be removed from its current policy assignment before it can be added to another policy.
Redirect Port (RedirectPort)	Use this parameter to specify a port to where the traffic is to be redirected. Traffic that matches the defined traffic flow is redirected to the specified port. You can specify only one port.

5. Click the Set button to add the new QoS policy to the switch.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Modifying a QoS Policy

To modify a QoS policy, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings- Policy Based QoS window is shown in Figure 62 on page 272.
3. In the QoS Policy List table, click the dialog box of the policy you want to modify. You can modify only one policy at a time.
4. Click the Edit button in the QoS Policy List table.

   The switch displays the QoS Policy - Edit window with the parameters of the selected policy.
5. Modify the parameters in the window, as needed. The parameters are described in Table 71 on page 287.
6. Click the Set button to activate your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting a QoS Policy

To delete a QoS policy, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Policy Based QoS option from the Switch Settings menu.

   The Switch Settings - Policy Based QoS window is shown in Figure 62 on page 272.
3. In the QoS Policy List table, click the dialog box of the policy you want to delete.
4. Click the Delete button. To delete all of the policies, click the Delete All button.

   The switch displays a confirmation prompt.
5. Click the OK button to delete the QoS policy or Cancel to retain it.

   The policy is deleted from the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying QoS Policy Statistics

To display statistics on the number of packets that have been processed by the QoS policies on the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the Policy Based QoS option from the Device Monitoring menu.

   An example of the Device Monitoring - Policy Based QoS window is shown in Figure 66.

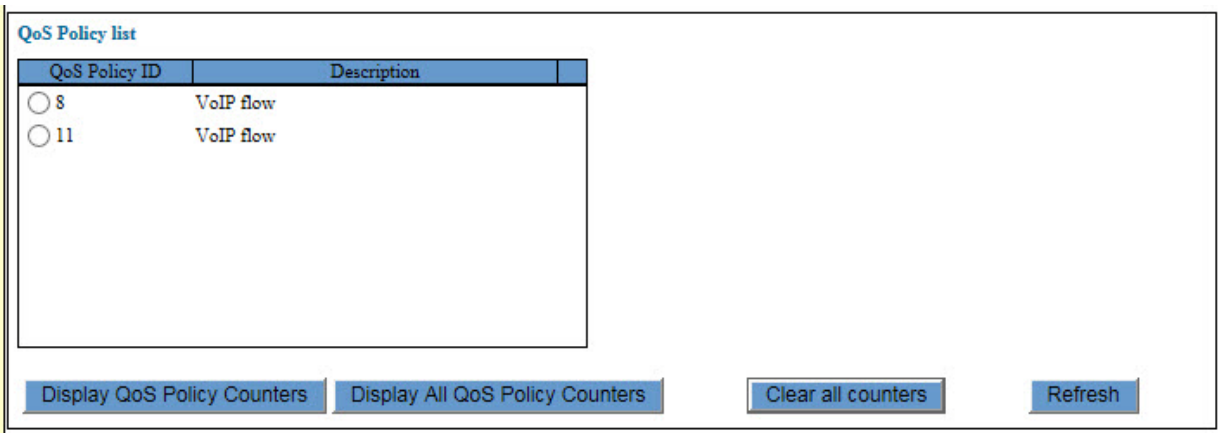

Figure 66. Device Monitoring - Policy Based QoS window

   The window lists the QoS policies on the switch.

3. If you want to view the statistics of only one policy, click its dialog circle to select it and then click the Display QoS Policy Counters button. To view the statistics for all of the policies, click the Display All QoS Policy Counters button.

   An example of the QoS Policy Counters window is shown in Figure 67 on page 292.

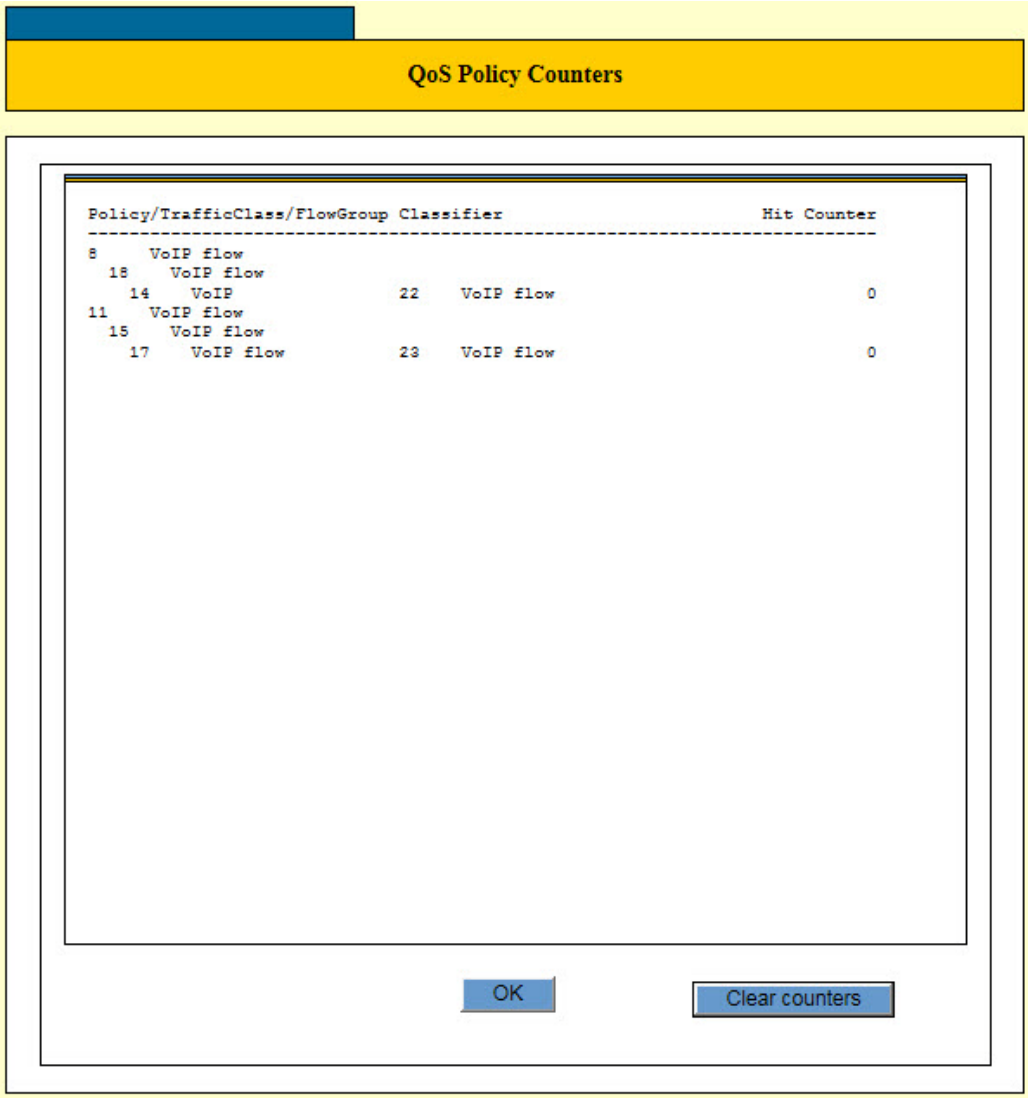

Figure 67. QoS Policy Counters Window

The Hit Counter displays the number of packets a QoS policy has processed.

4. To clear the counters, do one of the following:

   - ❒ To clear the counters for all of the policies, click the Clear All Counters button in the Device Monitoring - Policy Based QoS window.
   - ❒ To clear the counters for a particular policy, click the Clear Counters button in the QoS Policy Counters window.

Chapter 26

Rapid Spanning Tree Protocol Overview

This chapter provides background information on the Rapid Spanning Tree Protocol (RSTP). The sections in the chapter are listed here:

Overview

Spanning tree protocols are designed to detect and block loops in the wiring topology of a network. A data loop exists when two or more nodes can transmit data to each other over more than one data path in a network. Data loops can cause broadcast storms that can significantly reduce network performance. Where multiple paths exist, a spanning tree protocol places the extra paths in a standby or blocking mode by disabling ports, so that there is only one active path.

Spanning tree protocols can also activate redundant paths if active main paths go down. This enables the protocols to maintain network connectivity between different parts of a network in the event of a failure of a primary path.

There are three versions of the protocol. This switch comes with two of them. They are listed here:

- Rapid Spanning Tree Protocol (RSTP) - This version of the protocol is described in this chapter. The instructions for configuring RSTP parameters are found in Chapter 27, “Rapid Spanning Tree Protocol” on page 303.
- Multiple Spanning Tree Protocol - This version of the spanning tree protocol is intended for large networks. It allows you to group bridges into multiple spanning tree domains, which can increase the speed of the protocol in identifying and resolving loops in a network. Introductory information on the protocol can be found in Chapter 28, “Multiple Spanning Tree Protocol Overview” on page 317. The instructions on how to configure the settings are found in Chapter 29, “Multiple Spanning Tree Protocol” on page 333.

The third version of the protocol, which is also the original version, is called Spanning Tree Protocol (STP). The switch does not come with this version. However, the RSTP and MSTP protocols have STP-compatible modes that makes them compatible with STP on legacy devices.

Note
For detailed information on the Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

Bridge Priority and the Root Bridge

The Rapid Spanning Tree Protocol designates one of the bridges as the root bridge. The root bridge distributes network topology information to the other network bridges and is used by the other bridges to search for redundant paths in the network topology.

A root bridge is selected by the *bridge priority* number, also referred to as the bridge identifier. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number of the switch. You can designate a switch as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge offline, and assign that bridge the second lowest bridge identifier number. The bridge priority has a range 0 to 61440 in increments of 4096.

Path Costs and Port Costs

After the root bridge is selected, the bridges determine if the network contains redundant paths and, if one is found, select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the root port.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by a determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed in the blocking state.

Path cost is determined by evaluating *port costs*. Every port on a bridge participating in the spanning tree protocol has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

The port cost of a port on the switch is adjustable. The range for RSTP is 0 to 20,000,000.

Port cost also has an Auto-Detect feature. This feature allows spanning tree to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting. Table 72 lists the RSTP port costs with Auto-Detect.

Table 72. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 73 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 73. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

You can override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter. This parameter is used as a tie breaker when two paths have the same cost.

The range for port priority is 0 to 240 in increments of 16. The default value is 128.

Forwarding Delay and Topology Changes

The failure, removal, or addition of an active component in a network topology might cause a change to the active topology. This may trigger a change in the state of some blocked ports.

A change in a port state is not activated immediately. It might take time for the root bridge to notify all of the bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all of the bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states—listening and learning—before it begins to forward frames. The amount of time a port spends in these states is set by the forwarding delay value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the switch. The appropriate value for this parameter depends on a number of variables; the size of your network is a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Note
The forwarding delay parameter applies only to ports on the switch that are operating in the STP-compatible mode.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought online, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the hello time. This is a value that you can set on the switch. The interval is measured in seconds and the default is two

seconds. Consequently, if the switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With the port types defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- Point-to-point port
- Edge port

A bridge port that is operating in full-duplex mode functions as a point-to-point port. Figure 68 illustrates two switches that are connected with one data link of point-to-point ports operating in full-duplex mode.

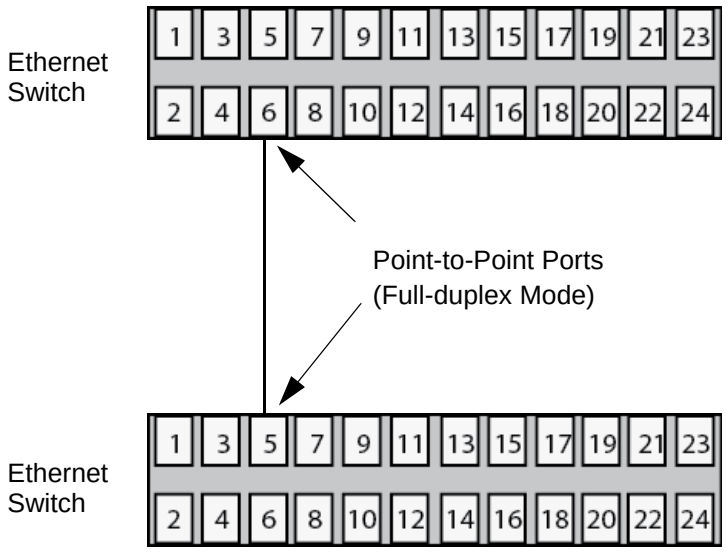

Figure 68. Point-to-Point Ports

A port is an edge port if it is operating in half-duplex mode and is not connected to a spanning tree protocol bridge. Figure 69 on page 299 illustrates an edge port on a switch. The port is connected to an Ethernet hub operating in half-duplex mode, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is operating at half-duplex mode and there are no spanning tree devices connected to it.

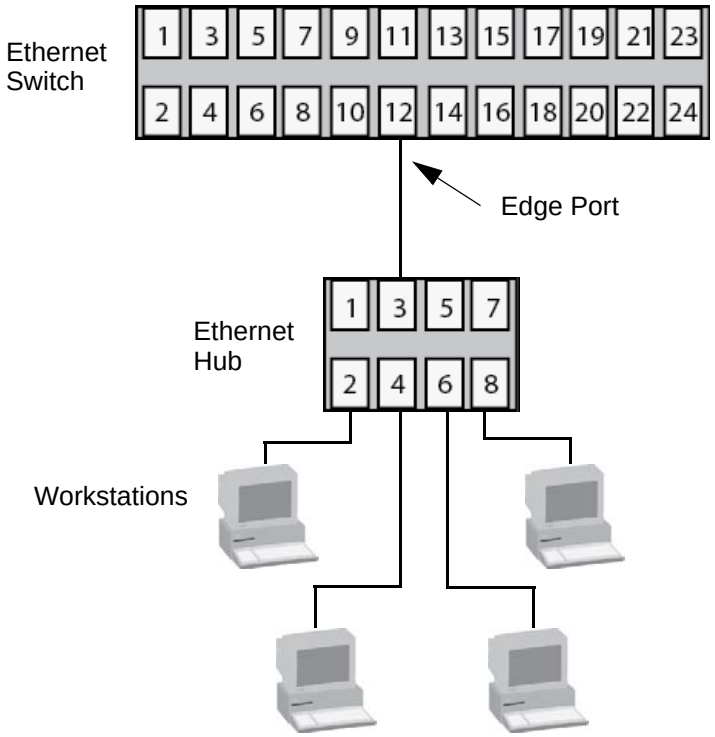

Figure 69. Edge Port

A port can be both a point-to-point and an edge port at the same time. It operates in full-duplex and is not connected to a spanning tree device. Figure 70 illustrates a port functioning as both a point-to-point and edge port.

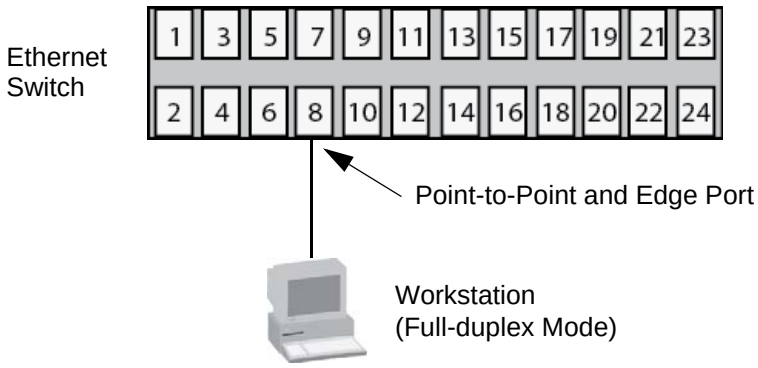

Figure 70. Point-to-Point and Edge Port

Determining whether a bridge port is point-to-point, edge, or both, can be confusing. For that reason, do not change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values work well.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. A network can have both protocols active at the same time. If both RSTP and STP are present in a network, they operate together to create a single spanning tree domain. The switch combines its RSTP with the STP on the other switches by monitoring the traffic on the ports for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP mode while ports receiving STP BPDU packets operate in STP mode.

VLANs

The protocol supports a single-instance spanning tree that encompasses all of the ports on the switch. If the ports are grouped into VLANs, the spanning tree protocol crosses the VLAN boundaries. This point can be a problem in networks that contain multiple VLANs that span different switches and that are connected with untagged ports. In this situation, the spanning tree protocol might block a data link if it detects a data loop, causing fragmentation of the VLANs.

This issue is illustrated in Figure 71. Two VLANs, Sales and Production, span two switches. Two links consisting of untagged ports connect the separate parts of each VLAN. If the protocol is activated on the switches, one of the links is disabled because the links form a loop. In the example, the port on the top switch that links the two parts of the Production VLAN is changed to the blocking state. This leaves the two parts of the Production VLAN unable to communicate with each other.

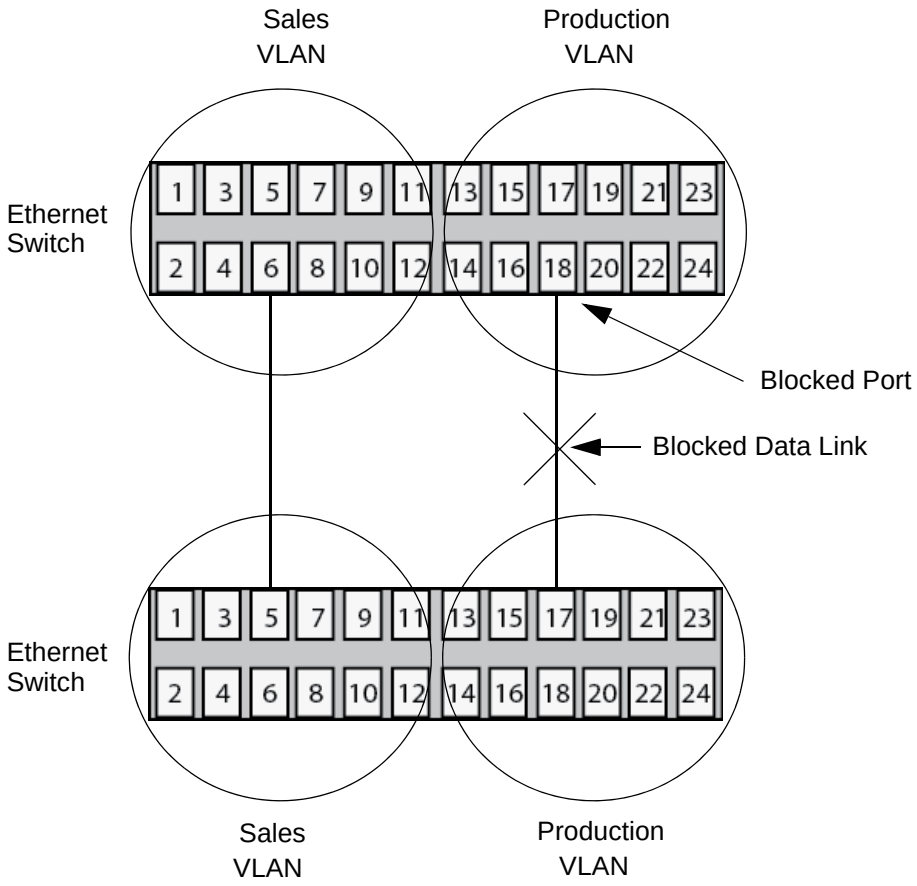

Figure 71. VLAN Fragmentation

You can avoid this problem by not activating spanning tree or by connecting VLANs using tagged instead of untagged ports. (For information on tagged and untagged ports, refer to Chapter 16, “Port-based and Tagged VLANs Overview” on page 177.)

Chapter 27

Rapid Spanning Tree Protocol

This chapter explains how to configure the RSTP parameters on the switch. The sections in the chapter are listed here:

Caution

The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience or an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

Displaying the RSTP Window

To display the RSTP window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the RSTP option from the Switch Settings menu.

   The Switch Settings - RSTP window is shown in Figure 72.

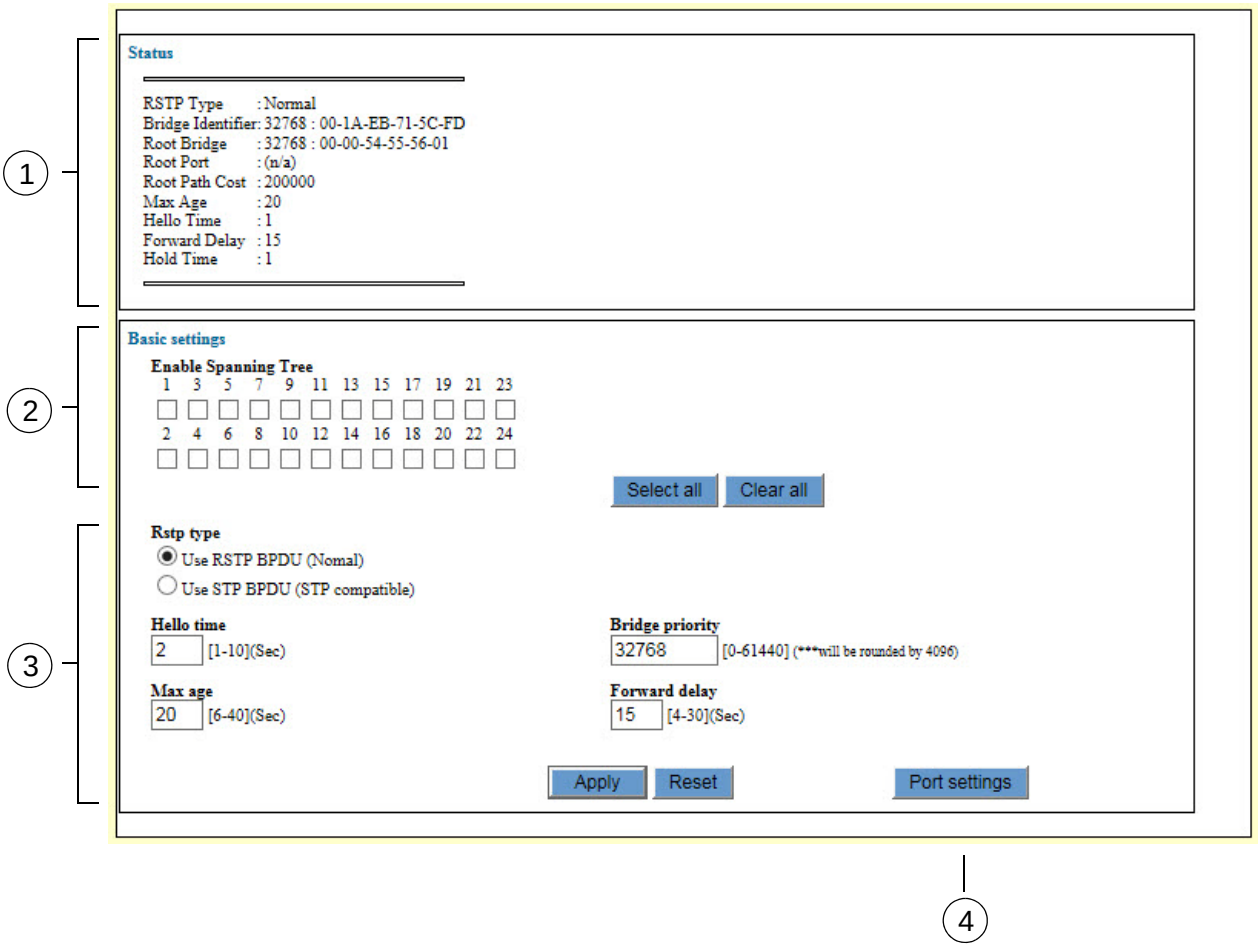

Figure 72. Switch Settings - RSTP Window

The sections in the Switch Settings - RSTP window are defined in Table 74 on page 305.

Table 74. Switch Settings - RSTP Window

Section	Description
1	Use this section to view the RSTP bridge settings on the current and root bridges of the spanning tree domain. The parameters are described in Table 75 on page 305.
2	Use this section to enable or disable RSTP on the individual ports on the switch. Refer to "Enabling or Disabling RSTP on the Ports" on page 314.
3	Use the options in this section to configure the RSTP bridge settings. Refer to "Configuring RSTP Bridge Settings" on page 308.
4	Use this button to configure the RSTP port settings. Refer to "Configuring RSTP Port Settings" on page 311.

The top section of the RSTP window displays the bridge RSTP settings. Please review the following information about this part of the window:

- The Max Age to Hold Time parameters are from the root bridge of the spanning tree domain.
- Most of the values will be 0 if the switch is not connected to another switch running a spanning tree protocol or if RSTP is not enabled on any of the ports.

The parameters in the Status section of the RSTP window are defined in Table 75.

Table 75. Switch Settings - RSTP Window

Parameter	Description
Protocol Version	Displays whether the bridge is operating with RSTP or in an STP-compatible mode. The possible options are listed here: Normal - The switch is transmitting RSTP BPDUs from the ports, except on ports that are receiving STP BPDUs. STPCompatible - The switch is using the RSTP parameter settings but is transmitting only STP BPDUs.

Table 75. Switch Settings - RSTP Window (Continued)

Parameter	Description
Bridge Identifier	Displays the current switch's bridge priority value and MAC address, separated by a colon (:).
Root Bridge	Displays the identification of the root bridge of the spanning tree domain. The identification consists of the bridge priority value and MAC address, separated with a colon (:), of the root bridge. Please note the following about this parameter: - This parameter will be zero if the spanning tree protocol is not enabled on any of the ports on the switch. - This parameter will be same as the Bridge Identifier parameter if the switch you are currently managing is the root bridge of the spanning tree domain.
Root Port	Displays the port on the switch that leads to the root bridge of the spanning tree domain. This parameter will be "n/a" if the current switch is the root bridge of the spanning tree domain or if RSTP is not activated on any of the ports.
Root Path Cost	Displays the path cost from the switch to the root bridge of the spanning tree domain. This parameter will be 0 if the current switch is the root bridge of the spanning tree domain or if RSTP is not activated on any of the ports.
Max Age	Displays the length of time after which stored bridge protocol data units (BPDUs) are deleted by all bridges in the spanning tree domain. This value is from the root bridge of the spanning tree domain.
Hello Time	Displays the time interval between generating and sending configuration messages by all bridges in the spanning tree domain.

Table 75. Switch Settings - RSTP Window (Continued)

Parameter	Description
Forward Delay	Displays the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after a change to the network topology. This value is from the root bridge of the spanning tree domain.
Hold Time	Displays the minimal interval between the transmission of BPDUs by the switch. The default value is 1 second. This value cannot be changed. This value is from the root bridge of the spanning tree domain.

Configuring RSTP Bridge Settings

To configure the RSTP bridge parameters for the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the RSTP option from the Switch Settings menu.

   The Switch Settings - RSTP window is shown in Figure 72 on page 304.
3. Configure the parameters in the Bridge Settings section of the window, as needed.

   The Bridge Settings section of the window is identified in section 3 in Figure 72 on page 304 and the parameters are described in Table 76.

Table 76. RSTP Bridge Parameters

Parameter	Description
RSTP Type	Use this parameter to control whether the bridge operates with RSTP or in an STP-compatible mode. The possible options are listed here: Use RSTP BPDU (Normal) - The switch operates all ports in RSTP, except for those ports that receive STP BPDU packets. Use STP BPDU (STP Compatible) - The switch operates in RSTP, using the RSTP parameter settings, but sends only STP BPDU packets from the ports.
Hello Time	Use this parameter to set the time interval between generating and sending configuration messages by the bridge. The range of the parameter is 1 to 10 seconds. The default is 2 seconds.

Table 76. RSTP Bridge Parameters (Continued)

Parameter	Description
Max Age	Use this parameter to set the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds. The parameter has the following guidelines: MaxAge must be greater than (2 x (HelloTime + 1)). MaxAge must be less than (2 x (ForwardingDelay - 1))
Bridge Priority	Use this parameter to set the priority number for the bridge. The number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority.

Table 76. RSTP Bridge Parameters (Continued)

Parameter	Description
Forward Delay	Use this parameter to set the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

4. After configuring the parameters, click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button option above the main menu.

Configuring RSTP Port Settings

To configure RSTP port parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the RSTP option from the Switch Settings menu.

   The Switch Settings - RSTP window is shown in Figure 72 on page 304.

3. Click the Port Settings button at the bottom of the window.

   The switch displays the RSTP Port Parameters window. Refer to Figure 73.

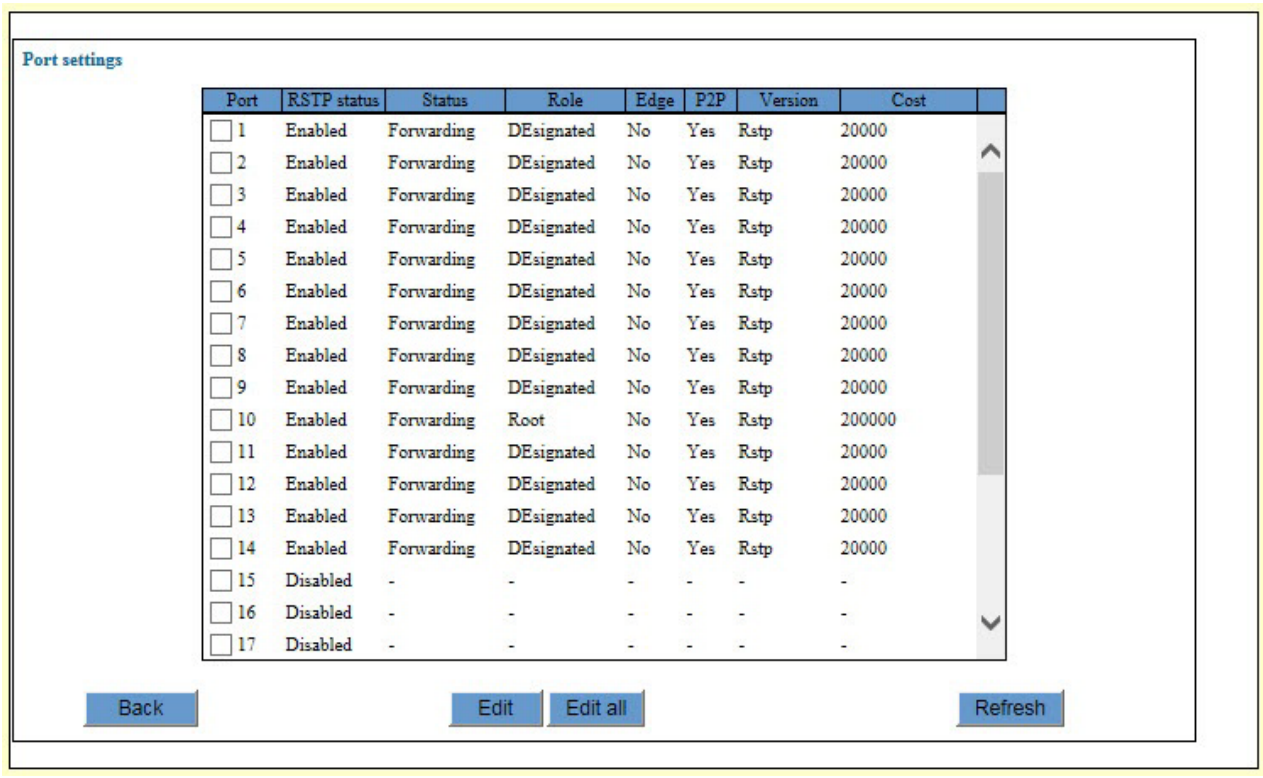

Figure 73. RSTP Port Settings Window

4. Click the dialog box of the port to be configured. You may configure more than one port at a time.
5. Click the Edit button. To configure all of the ports, click the Edit All button.

   The switch displays the Spanning Tree - Port Settings window. Refer to Figure 74 on page 312.

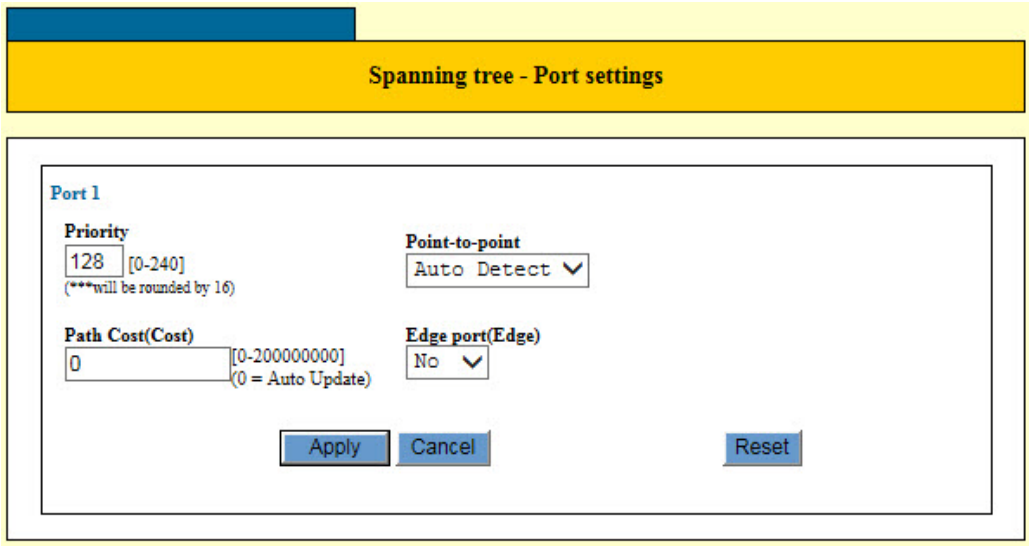

Figure 74. Spanning Tree - Port Settings Window

6. Configure the parameters, as needed. The parameters are described in Table 77.

Table 77. Spanning Tree - Port Settings Window

Parameter	Description
Priority	Use this parameter to set the tie breaker when two or more ports have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 128.
Path Cost	Use this parameter to set the cost of the port. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.
Point-to-Point	Use this parameter to define the port as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

Table 77. Spanning Tree - Port Settings Window (Continued)

Parameter	Description
Edge Port (Edge)	Use this parameter to define whether the port is functioning as an edge port. The possible settings are Yes and No.

7. Click the Apply button to activate your changes on the switch.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Enabling or Disabling RSTP on the Ports

To enable or disable RSTP on the ports, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the RSTP option from the Switch Settings menu.

   The Switch Settings - RSTP window is shown in Figure 72 on page 304.
3. In the middle section of the window, click the dialog boxes of the ports on which you want to enable or disable RSTP. A check mark in a dialog box enables RSTP and an empty dialog box disables the feature.

   Note
   Disabling RSTP on all of the ports disables the feature on the switch.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Enabling or Disabling BPDU Transparency for RSTP

You may configure the switch to either forward or discard BPDU packets when RSTP is disabled. As explained in "Hello Time and Bridge Protocol Data Units (BPDU)" on page 297, network devices that are running a spanning tree protocol use BPDUs to transmit spanning tree domain information to each other. At its default settings, the switch discards all BPDU packets it receives when RSTP is disabled. In some circumstances, you may want the switch to forward the packets even if it is not running the spanning tree protocol. You can do this by activating BPDU transparency. When the feature is enabled and RSTP is disabled, the switch forwards all of the BPDU packets it receives.

Note
You may not use RSTP and BPDU transparency on the switch at the same time. You should check to be sure that RSTP is disabled on all of the ports before activating BPDU transparency. For instructions, refer to "Enabling or Disabling RSTP on the Ports" on page 314.

To configure BPDU transparency on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Others option from the Switch Settings menu.

   The Switch Settings - Others window is shown in Figure 31 on page 138.
3. Click the dialog box in the Transparent to BPDU Packets section of the window to enable or disable the BPDU transparency feature.

   The feature is enabled when the dialog box has a check mark. The switch forwards BPDUs when the feature is enabled. The feature is disabled when the dialog box is empty. The switch does not forward the packets when the feature is disabled. The default setting is disabled.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 28

Multiple Spanning Tree Protocol Overview

This chapter provides background information on the Multiple Spanning Tree Protocol (MSTP). The sections in the chapter are listed here:

Overview

MSTP has the same function as RSTP, which is explained in Chapter 26, “Rapid Spanning Tree Protocol Overview” on page 293. It searches for loops in the wiring topology of a network and, where loops exist, blocks bridge ports to prevent broadcast storms. MSTP differs from RSTP in that it lets you group the bridges of a network into multiple spanning tree domains. This can be useful in networks with large number of bridges because it enables the spanning tree protocol to react to and resolve loops more quickly than if all of the bridges are one domain.

The following sections describe some of the terms and concepts related to MSTP.

Note
Do not activate MSTP on the switch without first familiarizing yourself with the following concepts and guidelines. Unlike RSTP, you cannot activate this spanning tree protocol on the switch without configuring the protocol parameters.

Note
The MSTP implementation on the switch complies with the new IEEE 802.1s standard and is compatible with other vendors’ compliant 802.1s implementations.

Multiple Spanning Tree Instance (MSTI)

The individual spanning trees domains in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). An MSTI can span any number of switches.

To create an MSTI, you assign it a number, referred to as the MSTI ID. The range is 1 to 15. (The switch is shipped with a default MSTI with an ID of 0. This default spanning tree instance is discussed later in "Common and Internal Spanning Tree (CIST)" on page 324.)

After selecting an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Here are the MSTI guidelines:

- The switch supports up to 16 spanning tree instances, including the CIST.
- An MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- A switch port can belong to more than one spanning tree instance at a time by being an untagged and tagged member of VLANs belonging to different MSTIs. This is possible because a port can be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to "Ports in Multiple MSTIs" on page 319.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called associations. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTIs. In this circumstance, a port might have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port's MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set only once on a port and apply to all the MSTIs where the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to

multiple MSTIs, can have only one external path cost. Another generic parameter designates a port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI in which a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

Multiple Spanning Tree Regions

Another important concept of MSTP is regions. An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. The characteristics are listed here:

- Configuration name
- Revision number
- VLANs
- VLAN to MSTI ID associations

A configuration name is a name that identifies a region. You must assign each bridge in a region exactly the same name; even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The revision number is an arbitrary number assigned to a region. You might use this number to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that all of the bridges in a region have the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all of the bridges in a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP considers the bridges as residing in different regions.

Figure 75 on page 322 illustrates the concept of regions. It shows one MSTP region with two switches. The switches have the same configuration names and revision levels. They also have the same five VLANs and the VLANs are associated with the same MSTIs.

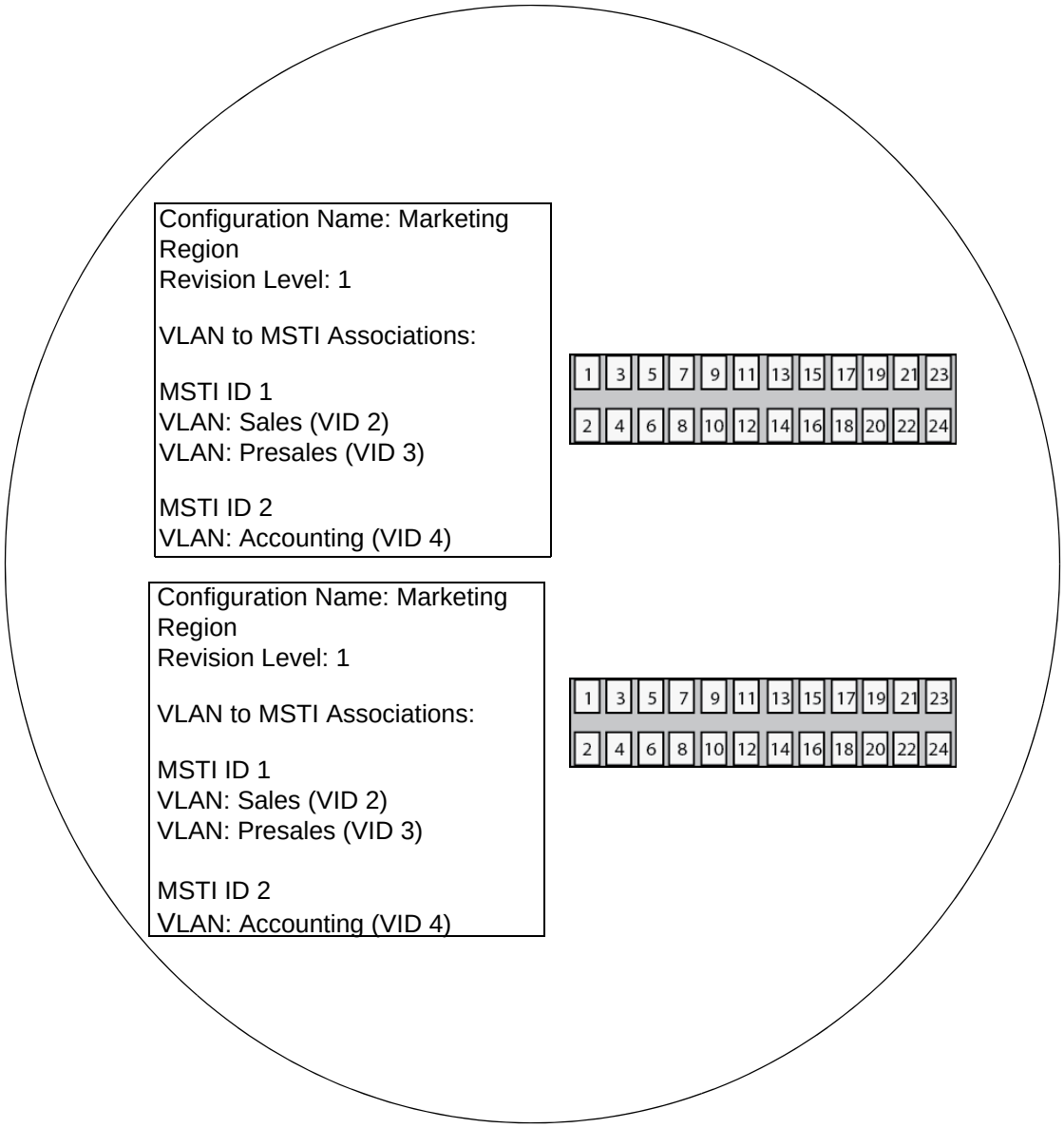

Figure 75. Multiple Spanning Tree Region

The switch determines regional boundaries by examining the MSTP BPDUs it receives on the ports. A port that receives an MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for ports connected to bridges running STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops

within the spanning tree instance. An MSTI's root bridge is called a regional root. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root of an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the MSTI priority value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used to determine the regional root of a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority; from 0 to 61,440 in sixteen increments of 4,096.

Region Guidelines

Here are the guidelines for regions.

- A network can contain any number of regions and a region can contain any number of switches.
- A switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.
- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- The regional root of an MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs you create yourself. First, you cannot delete this instance or change its MSTI ID. Second, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The default VLAN is also associated by default with CIST.

Another important difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP bridges in a network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and STP and RSTP bridges, to form one spanning tree for the entire bridged network.

MSTP uses CIST to form the spanning tree of an entire bridged network because CIST can cross regional boundaries, while an MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and STP and RSTP bridges in the bridged network.

The CIST regional root is set with the CIST Priority parameter. This parameter, which functions similar to the RSTP bridge priority value, selects the root bridge for the entire bridged network. If the switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP bridges in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on the switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of an MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all of the rules and guidelines mentioned in earlier sections, and provides a few new ones:

- The switch can support up to 16 spanning tree instances, including the CIST.
- An MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- An MSTI ID can be from 1 to 15.
- The CIST ID is 0. You cannot change this value.
- A switch port can belong to more than one spanning tree instance at a time. This allows you to assign a port as an untagged and tagged member of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.
- A router or Layer 3 network device is required to forward traffic between VLANs.
- A network can contain any number of regions and a region can contain any number of switches.
- The switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.
- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- The regional root of an MSTI must be in the same region as the MSTI.
- The CIST must have a regional root for communicating with other regions and single-instance spanning trees.
- MSTP is compatible with STP and RSTP.
- A port transmits CIST information even when it is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in "Associating VLANs to MSTIs" on page 328.

Note
The MSTP implementation on the switch complies with the IEEE 802.1s standard and is compatible with similar products from other vendors, provided that their products are also compliant with the standard.

Associating VLANs to MSTIs

Allied Telesis recommends that you assign all of the VLANs on the switch, including the default VLAN, to an MSTI. You should not leave VLANs assigned to only the CIST. This is to prevent the switch from blocking ports that should be in the forwarding state. The reason for this guideline is explained here.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all of the ports belong to the CIST instance. So CIST is included in the BPDU. If a port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is illustrated in Figure 76. Port 8 in switch A is a member of a VLAN assigned to MSTI ID 7 while port 1 is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 8 to switch B indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from port 1 indicates the port is a member of the CIST and MSTI 10.

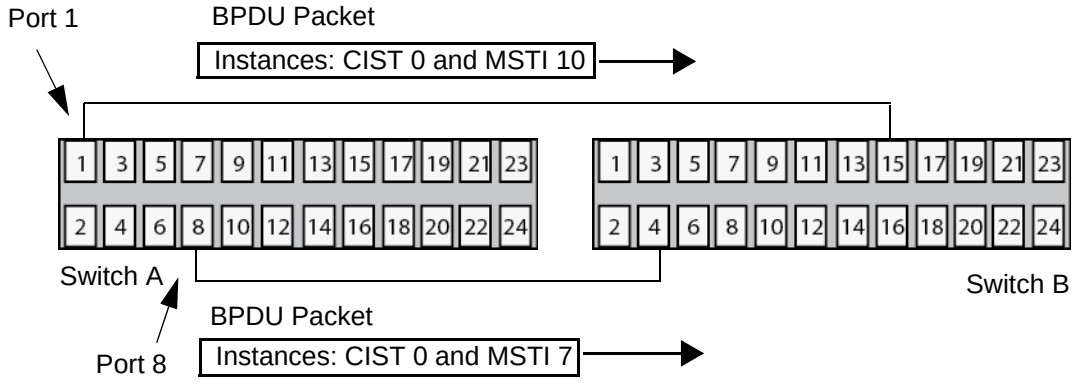

Figure 76. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When switch B receives a packet from switch A, it uses MSTI, not CIST, to determine whether a loop exists. And because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise if you assign some VLANs to MSTIs while leaving others only in CIST. The problem is illustrated in Figure 77 on page 329. The network is the same as the previous example. The difference is that the VLAN containing port 8 on Switch A has not been assigned to an MSTI, and belongs only to CIST with its MSTI ID 0.

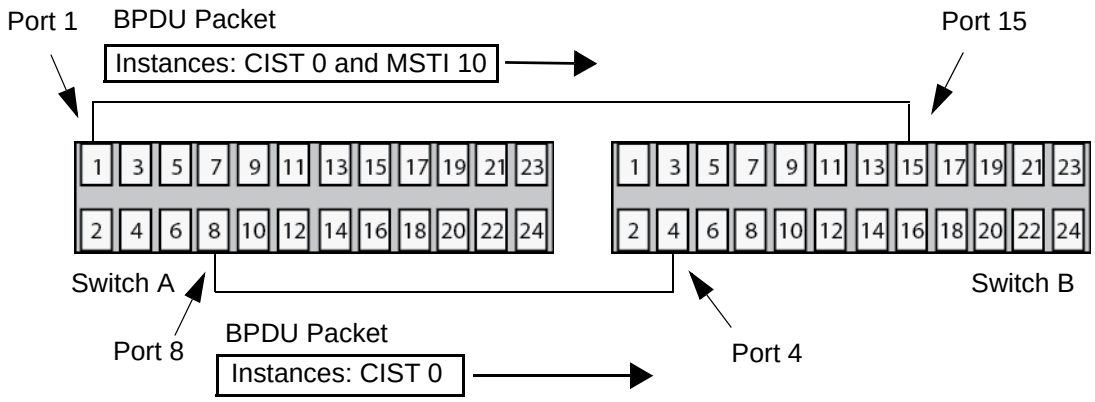

Figure 77. CIST and VLAN Guideline - Example 2

When port 4 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST. Therefore, switch B uses CIST to determine whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block a port to block the loop.

To avoid this issue, always assign all of the VLANs on the switch, including the Default VLAN, to MSTIs. This guarantees that all of the ports on the switch have an MSTI ID and ensures that loop detection is based on the MSTIs and not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when you connect different MSTP regions or an MSTP region and an STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANS of your network.

As mentioned previously, only the CIST can span regions. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 78. The example shows two switches that reside in different regions. Port 1 in switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 16 is a tagged and untagged member of three different VLANs, all associated to MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop exists between the regions, and Switch B would block a port.

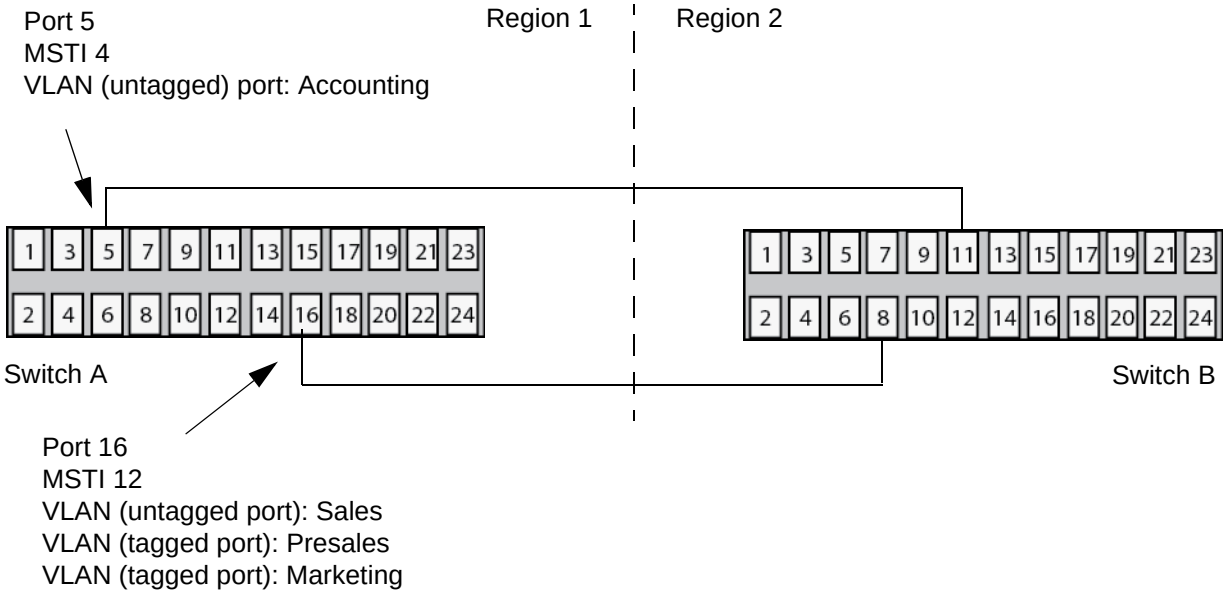

Figure 78. Spanning Regions - Example 1

There are several ways to address this issue. One way is to have only one MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. Those VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Assume that you have two regions that contain the following VLANS:

Region 1 VLANs
Sales
Presales
Marketing
Advertising
Technical Support
Product Management
Project Management
Accounting

Region 2 VLANs
Hardware Engineering
Software Engineering
Technical Support
Product Management
CAD Development
Accounting

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You could group those VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. After they are grouped, you can connect the VLANs across the regions using a link of tagged ports.

Chapter 29

Multiple Spanning Tree Protocol

This chapter contains instructions on how configure the Multiple Spanning Tree Protocol (MSTP) on the switch. It contains the following procedures:

Displaying the MSTP Window

To display the MSTP window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79.

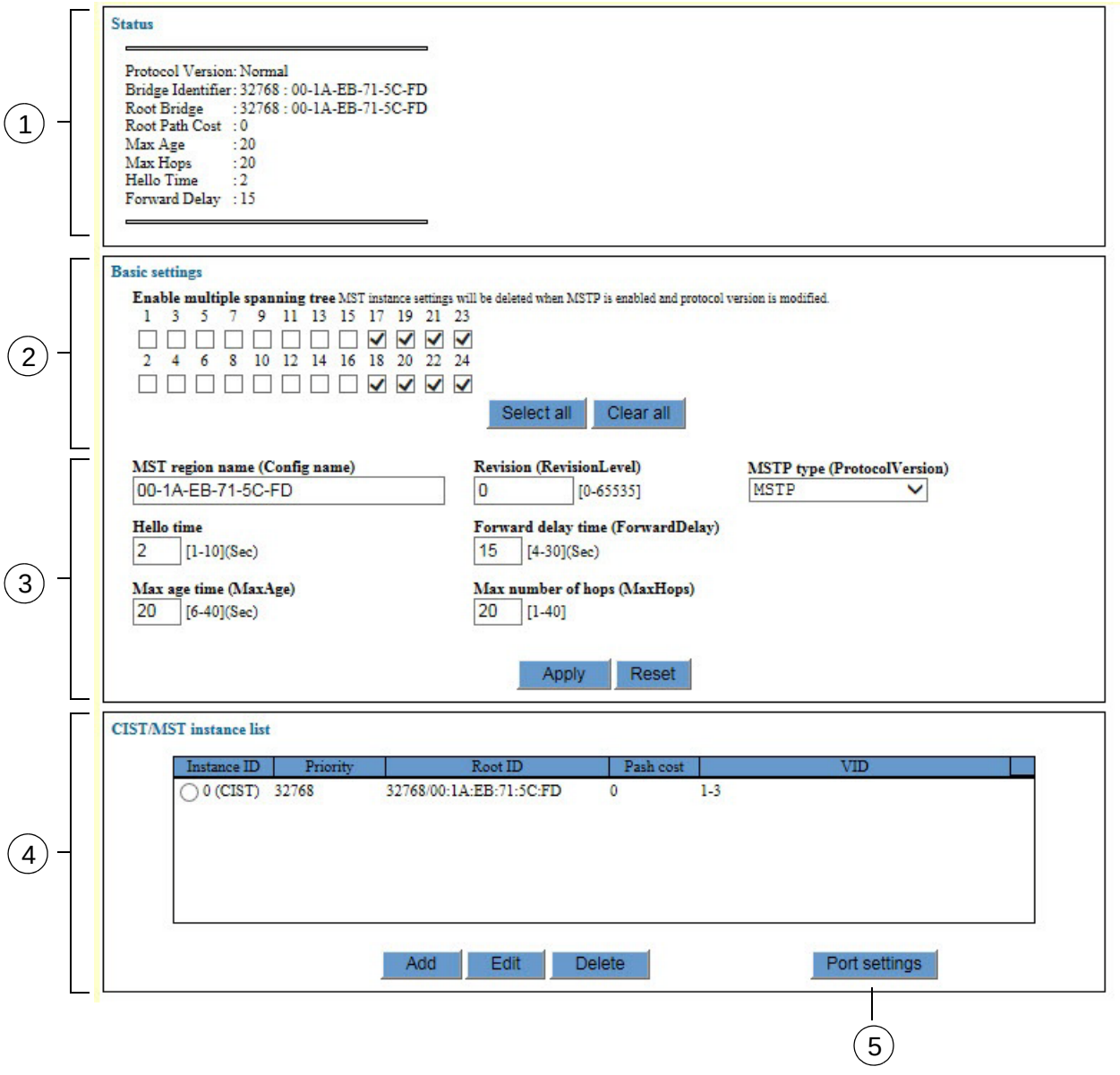

Figure 79. Switch Settings - MSTP Window

The sections in the window are defined in Table 78.

Table 78. Switch Settings - MSTP Window

Section	Description
1	Use this section in the MSTP window to view the bridge settings on the root bridge of the spanning tree region. The parameters are described in Table 79 on page 336.
2	Use this section to enable or disable MSTP on the individual ports on the switch. Refer to “Enabling or Disabling MSTP on the Ports” on page 338.
3	Use the options in this section to configure the MSTP bridge settings on the switch. Refer to “Configuring the MSTP Bridge Parameters” on page 339.
4	Use the table in this section to manage the CIST and MSTIs. Refer to “Configuring the CIST Priority” on page 342 and “Managing MSTIs” on page 344.
5	Use this button to configure the MSTP port settings. Refer to “Configuring MSTP Port Parameters” on page 349.

The top section of the window displays the MSTP settings on the root bridge in the spanning tree region of the switch. All of the spanning tree devices in the region are using these settings. Please review the following information about this part of the window:

- MSTP is disabled on the switch if the Root Bridge parameter is zero.
- The values in this section will be the same values as on the switch if the switch is operating as the root bridge of the spanning tree region.

The parameters in the Status section of the MSTP window are defined in Table 79 on page 336.

Table 79. Status Parameters in the MSTP Window

Parameter	Description
Protocol Version	Displays the MSTP protocol version. The possible values are listed here: Normal - The ports on the switch are using MSTP, except those ports that are receiving STP or RSTP BPDU packets. This is the default setting. Force STP Compatible - The bridge is using the MSTP parameters, but the ports are sending only STP BPDU packets.
Bridge Identifier	Displays the identifier of the switch. The identifier consists of the switch's bridge priority value and MAC address, separated by a slash (/).
Root Bridge	Displays the identifier of the root bridge of the spanning tree region. The identifier consists of the bridge priority value and MAC address, separated with a slash (/) of the root bridge. This parameter will be zero if RSTP is disabled on the switch. This parameter will be same as the Bridge Identifier parameter if the switch is acting as the root bridge of the spanning tree region.
Root Path Cost	Displays the path cost from the switch to the root bridge of the spanning tree region. The path cost is 0 if the current switch is the root bridge.
Max Age	Displays the maximum length of time the bridges in the spanning tree region retain bridge protocol data units (BPDUs).
Max Hops	Displays the maximum number of hops before BPDUs are deleted. The Max Hop counter in a BPDU is decremented every time a BPDU crosses an MSTP region boundary. After the counter reaches zero, a BPDU is deleted.

Table 79. Status Parameters in the MSTP Window (Continued)

Parameter	Description
Hello Time	Displays the time interval between generating and sending configuration messages by the bridges in the spanning tree domain.
Forward Delay	Displays the amount of time the bridge waits before changing to a new state, such as becoming the new root bridge after a change to the network topology.

Enabling or Disabling MSTP on the Ports

To enable or disable MSTP on the individual ports on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79 on page 334.
3. Click the dialog boxes of the port numbers in the Basic Settings section in the middle of the MSTP window to enable and disable MSTP on the ports.

   A check mark in a dialog box activates MSTP on the corresponding port. An empty check box disables MSTP.

   Disabling MSTP on all of the ports disables the protocol on the switch.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring the MSTP Bridge Parameters

To configure the MSTP bridge parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79 on page 334.
3. Configure the bridge MSTP parameters in the window, as needed.

   The parameters are located in section 3 in Figure 79 on page 334 and are defined in Table 80.

Table 80. Bridge MSTP Settings

Parameter	Description
MST Region Name (Config Name)	Use this option to enter a name for the MSTP region. The name can be from 0 (zero) to 32 alphanumeric characters in length. The name, which is case sensitive, must be the same on all of the bridges in a region. Examples of a configuration name include Sales Region and Production Region. The default region name is the MAC address of the switch.
Hello Time	Use this option to set the time interval for the bridge between generating and sending configuration messages. The range is 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of a region.

Table 80. Bridge MSTP Settings (Continued)

Parameter	Description
Max Age Time (MaxAge)	Use this option to set the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs. All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds. Be sure to follow these rules when selecting a value for the maximum age: MaxAge must be greater than (2 x (HelloTime + 1)) MaxAge must be less than (2 x (ForwardingDelay - 1))
Revision (RevisionLevel)	Use this option to set the revision level of an MSTP region. This is an arbitrary number you assign to a region. The revision level must be the same on all of the bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 65535.

Table 80. Bridge MSTP Settings (Continued)

Parameter	Description
Forward Delay Time (ForwardDelay)	Use this option to set the waiting period for a bridge when it changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.
Max Number of Hops (MaxHops)	Use this option to set the maximum number of hops before BPDUs are deleted. The Max Hop counter in a BPDU is decremented every time a BPDU crosses an MSTP region boundary. After the counter reaches zero, a BPDU is deleted.
MSTP Type (ProtocolVersion)	Use this option to set the bridge to the MSTP or STP-compatible mode. The options are listed here: MSTP - The bridge operates all of the ports in MSTP, except those ports that receive STP or RSTP BPDU packets. This is the default setting. STP Compatible mode - The bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. Selecting this option deletes all of the spanning tree instances on the switch.

4. After configuring the parameters, click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring the CIST Priority

This section explains how to change the CIST priority parameter for the switch. The number is used to determine the root bridge of the bridged network and is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

To configure the CIST priority, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79 on page 334.
3. In the CIST/MST Instance List table at the bottom of the window, click the dialog circle for the CIST entry.
4. Click the Edit button.

   The switch displays the Modify CIST window, shown in Figure 80.

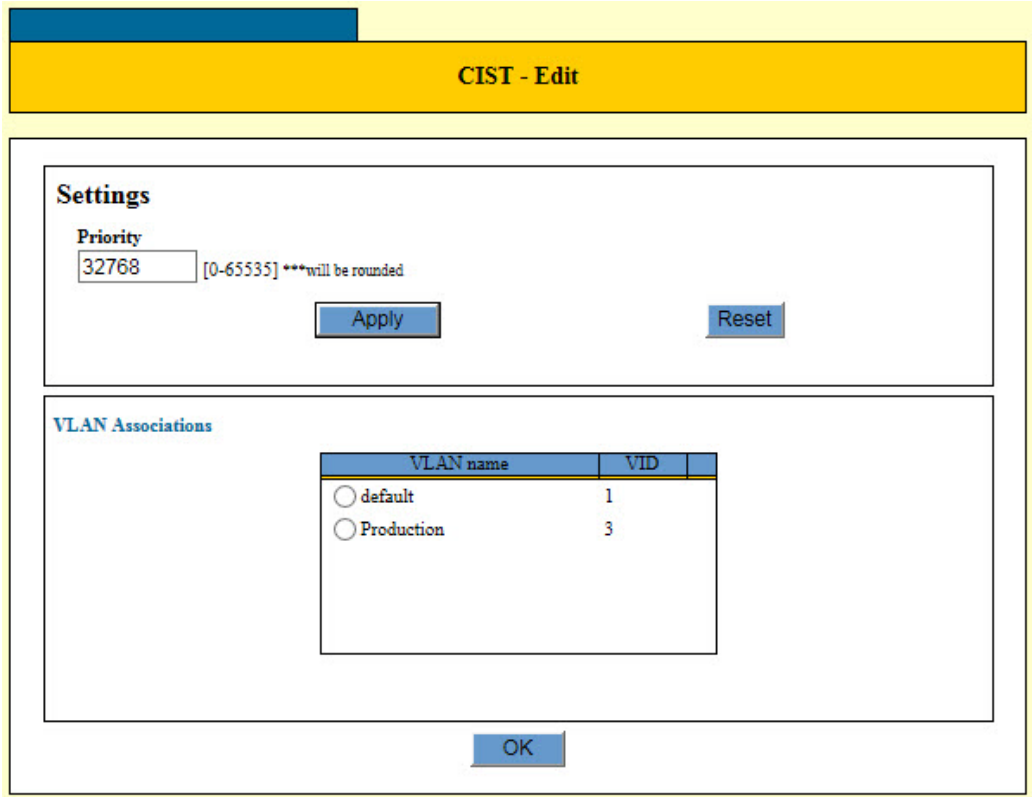

Figure 80. CIST - Edit Window

Note
The VLAN Associations table in the window lists the VLANs that are associated with the CIST. You may not use this window to change the VLANs of the CIST. VLANs are removed from the CIST when you associate them with MSTIs and are returned to the CIST when you remove them from MSTIs.

5. Select the Priority field and enter the new CIST value for the switch. The range is 0 to 65535 in increments of 4096. The default value is 32768. A value that is not an increment of 4096 is automatically rounded down.

6. After configuring the parameters, click the Apply button to activate your changes on the switch.

7. To permanently save your change in the configuration file, click the Save button above the main menu.

Managing MSTIs

This section contains the following procedures:

Creating an MSTI

During the procedure you have to specify the VIDs or names of the VLANs you want to associate with the new MSTI. To learn the VIDs and names of the VLANs on the switch, refer to “Displaying the VLAN Window” on page 194.

To create an MSTI, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The MSTP window is shown in Figure 79 on page 334.
3. Examine the CIST/MST Instance List at the bottom of the window for the VLANs you intend to associate with the new MSTI. The VLANs are identified by their VIDs. VLANs have to be associated with the CIST before you can add them to a new MSTI. They cannot belong to other MSTIs. Do one of the following:

   - ❒ If the VLANs for the new MSTI belong to CIST, continue with the next step.
   - ❒ If the VLANs belong to other MSTIs, remove them from their current MSTI associations by performing “Modifying an MSTI” on page 346 before performing this procedure.
4. Click the Add button in the MSTI section at the bottom of the window.

   The MST Instance - Add window is shown in Figure 81 on page 345.

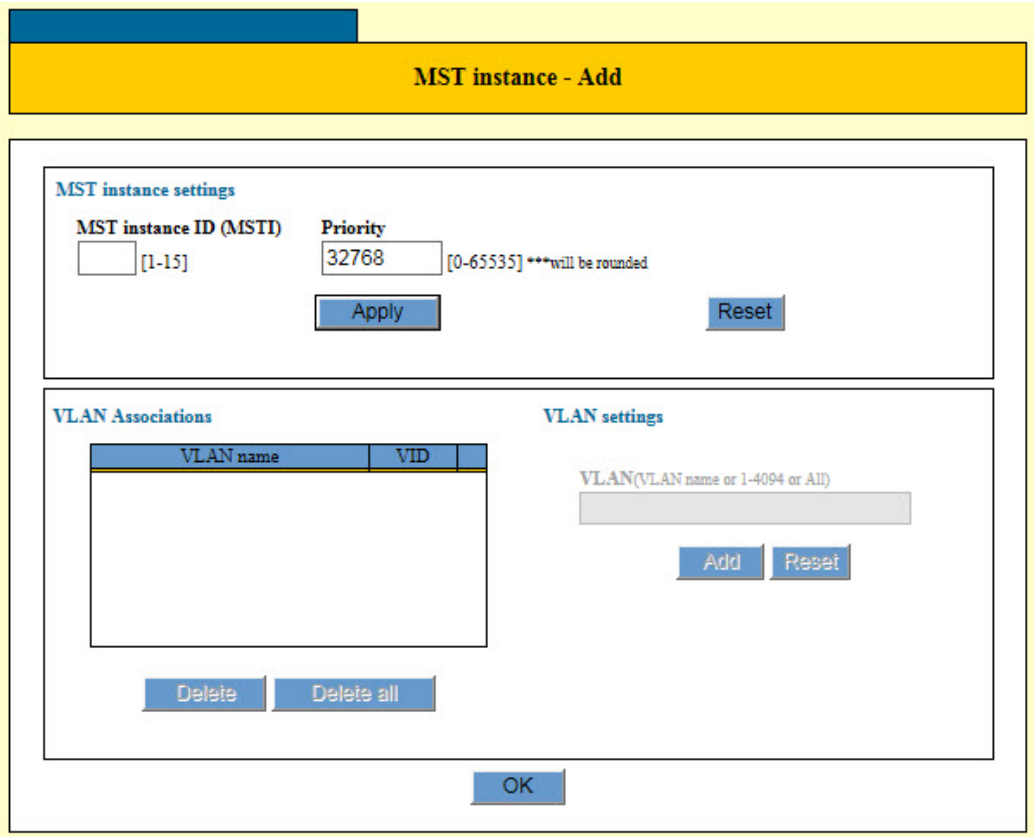

Figure 81. MST Instance - Add Window

5. Configure the parameters in the window, as needed. The parameters are defined in Table 81.

Note
You have to specify the MSTI ID number and priority value, and click the Apply button, before adding the VLAN associations.

Table 81. MST Instance - Add Window

Parameter	Description
MST Instance ID (MSTI)	Use this parameter to enter an ID number for the MSTI. The range is 1 to 15.

Table 81. MST Instance - Add Window (Continued)

Parameter	Description
Priority	Use this parameter to enter an MSTI priority value for the new MSTI. The parameter is used to select a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. A value that is not an increment of 4,096 is automatically rounded down. The default is 0.
VLAN Associations	Use this table to view the names of the VLANs associated with the MSTI. The table will be empty for a new MSTI.
VLAN Settings	Use this field to enter the name or VID of a VLAN for the new MSTI. You may specify only one VLAN at a time. After specifying a VLAN, click the Add button.

6. After configuring the parameters, click the OK button to activate your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.
8. Repeat this procedure starting with step 3 to create additional MSTIs.

Modifying an MSTI

To modify an MSTI, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The MSTP window is shown in Figure 79 on page 334.
3. In the CIST/MST Instance List at the bottom of the window, click the dialog circle of the MSTI you want to modify. You may modify only one MSTI at a time.
4. Click the Edit button beneath the CIST/MSTI table.

   The switch displays the MST Instance - Edit window. The window contains the parameter settings of the selected MSTI. An example of the window is shown in Figure 82 on page 347.

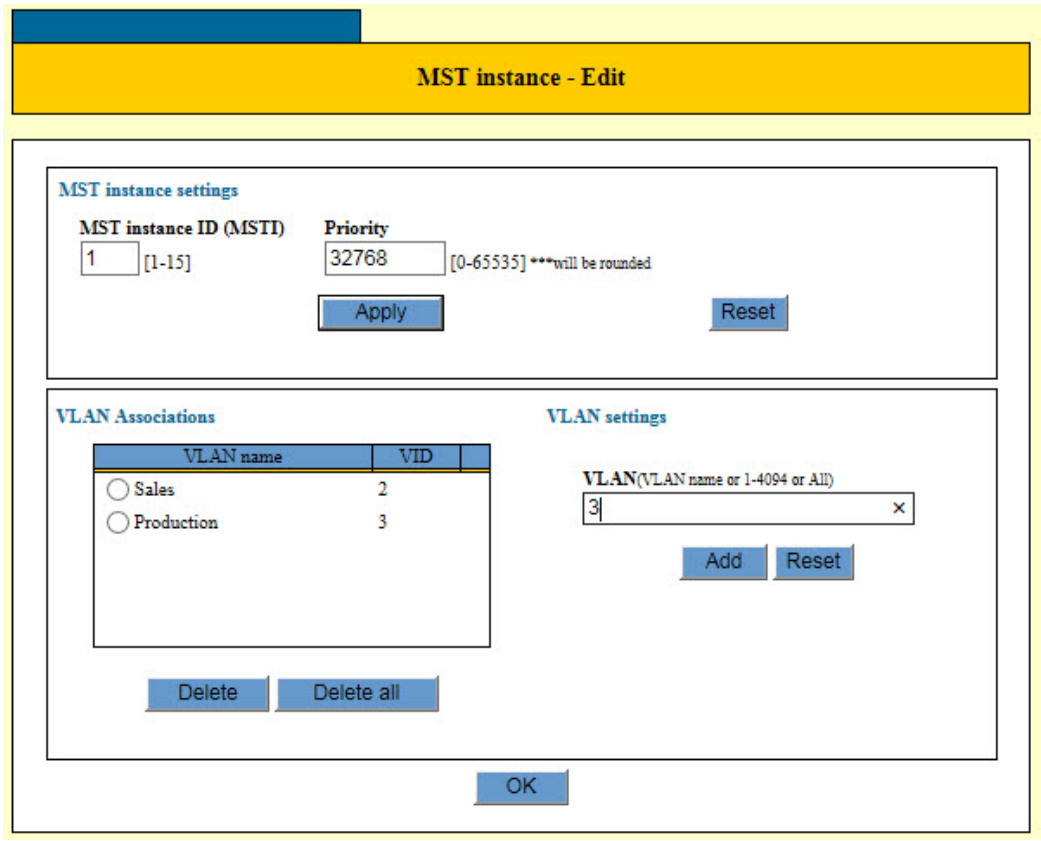

Figure 82. MST Instance - Edit Window

5. Modify the parameters are needed.

   The parameters in the window are defined in Table 81 on page 345. Please review the following information before modifying the parameters of the MSTI.

   - ❒ You may not change the MSTI ID.
   - ❒ To delete a VLAN from an MSTI, click its dialog circle in the VLAN Associations list and click the Delete button. To delete all of the VLANs, click the Delete All button. The VLANs are automatically returned to the CIST.
   - ❒ To add a VLAN to an MSTI, enter its name or VID in the VLAN Settings field in the window and click the Add button. You may add only one VLAN at a time. VLANs that are added to an MSTI are automatically removed from the CIST.

6. If you changed the Priority value, click the Apply button. If you changed the VLAN associations, click the OK button.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting an MSTI

To delete an MSTI from the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79 on page 334.
3. In the CIST/MST Instance List at the bottom of the window, click the dialog circle of the MSTI you want to delete. You may delete only one MSTI at a time.
4. Click the Delete button beneath the CIST/MSTI table

   The switch displays a confirmation prompt.
5. Click OK to delete the MSTI or Cancel to retain it.

   All of the VLANs associated with the deleted MSTI are returned to the CIST.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring MSTP Port Parameters

The port parameters are divided into two groups: generic parameters and MSTI-specific parameters. Generic port parameters are set once on a port and apply to all of a port's MSTIs assignments. The generic parameters are listed here:

- External path cost
- Point-to-point port
- Edge port

The MSTI-specific parameters are set on a per MSTI basis. This means a port that is a member of more than one MSTI can have different parameter values in each instance. The parameters are listed here:

- Internal path cost
- Port priority

To configure MSTP port parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MSTP option from the Switch Settings menu.

   The Switch Settings - MSTP window is shown in Figure 79 on page 334.
3. In the CIST/MST Instance List at the bottom of the window, do one of the following:

   - To configure the port parameters in CIST, which include the generic port parameters, click the CIST entry in the table.
   - To configure MSTI-specific parameters for ports, click the dialog circle of the MSTI that contains the VLAN with ports you want to configure. You may select only one MSTI.
4. Click the Port Settings button at the bottom of the window.

   The switch displays the Port Settings / Instance ID window. The window displays a table of the ports. An example of the window is shown in Figure 83 on page 350.

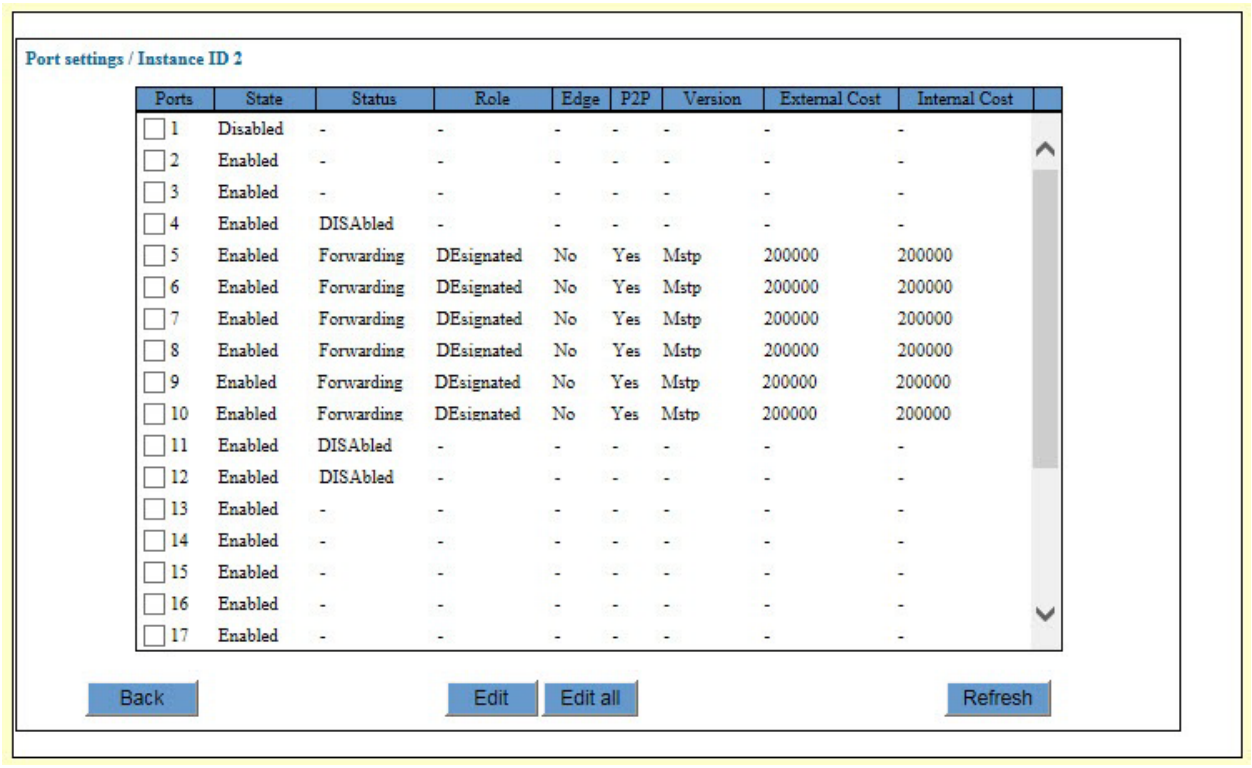

Figure 83. Port Settings / Instance ID Window

If you are configuring MSTI port parameters, you can use the Status column to identify the member ports of the VLANs of the selected MSTI. A port is a member of an MSTI if its status is Disabled or another state, such as Forwarding or Listening. A port is not a member of the MSTI if its status is empty (-). For example, referring to Figure 83, the VLANs of the selected MSTI consist of ports 4 to 12. The other ports on the switch are members of other VLANs associated with other MSTIs, or are not associated with any MSTIs.

The columns in the window are described in Table 82.

Table 82. Port Settings / Instance ID Window

Column	Description
Ports	Displays the port number.

Table 82. Port Settings / Instance ID Window (Continued)

Column	Description
State	Displays the MSTP state of the port. The possible states are listed here: Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission. Learning - The port is enabled for receiving, but not forwarding packets. Forwarding - Normal operation. Disabled - The port has not established a link with an end node.
Role	Displays the MSTP role of the port. The possible roles are listed here: Root - The port that is connected to the root switch, directly or through other switches, with the least path cost. Alternate - The port offers an alternate path in the direction of the root switch. Backup - The port on a designated switch that provides a backup for the path provided by the designated port. Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch. Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called “master” when the CIST role is “root.”
Edge	Displays whether or not the port is an edge port.
P2P	Displays whether or not the port is a point-to-point port.

Table 82. Port Settings / Instance ID Window (Continued)

Column	Description
Version	Displays whether the port is operating in MSTP mode or STP-compatible mode.
External Cost	Displays the external cost of the port.
Internal Cost	Displays the internal cost of the port.

5. Click the dialog box of the port you want to modify. You may configure more than one port at a time.

6. Click the Edit button. To change the settings of all of the ports, click the Edit All button.

   The next window that the switch displays depends on whether you selected the CIST or an MSTI in step 3. Figure 84 is an example of the CIST - Port Settings window. The switch displays this window when you configure a port from the CIST.

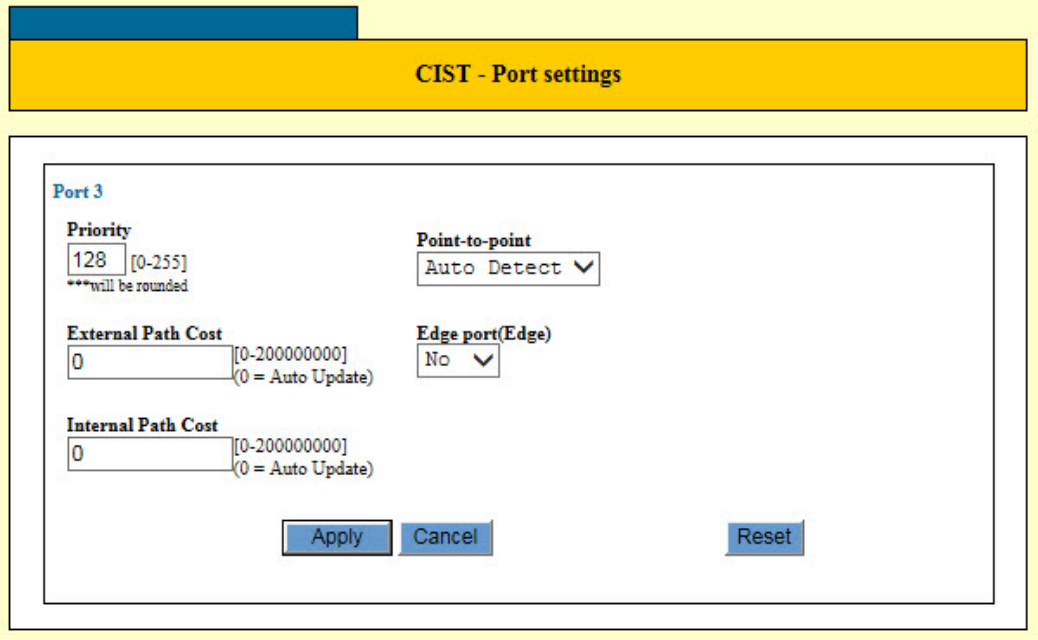

Figure 84. CIST- Port Settings Window

Figure 85 on page 353 is an example of the MSTI Instance - Port Settings window. The switch displays this window when you configure ports from an MSTI. There are only two parameters in the window. These are the MSTI-specific port parameters. A port can have different values for these parameters in different MSTis.

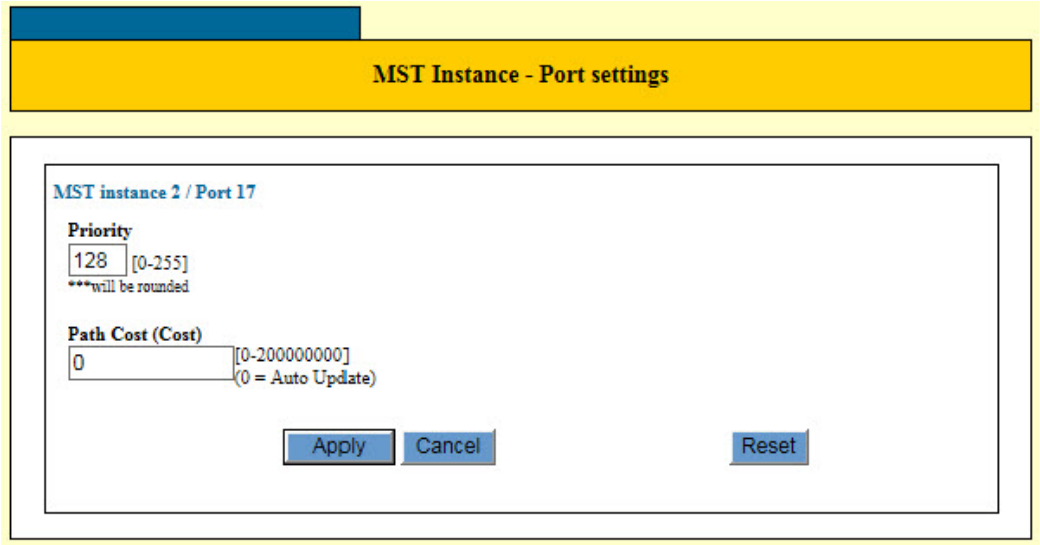

Figure 85. MST Instance - Port Settings Window

7. Configure the parameters in the window, as needed.

   The parameters are described in Table 83.

Table 83. MST Instance - Port Settings

Parameter	Description
Priority	Use this parameter to set the priority parameter for a port. The priority is used as a tie breaker when two or more ports have equal costs to the regional root bridge. The range is 0 to 255 in increments of 16. The default value is 128.

Table 83. MST Instance - Port Settings (Continued)

Parameter	Description
External Path Cost	Use this parameter to set the cost of a port that is connected to a bridge that is a member of another MSTP region or an STP or RSTP domain. The range is 0 to 200,000,000. The value 0 activates the Auto setting, which sets the value according to port speed. Here are the MSTP port costs with the Auto setting when a port is not a member of a trunk. 10 Mbps - 2,000,000 100 Mbps - 200,000 1000 Mbps - 20,000 Here are the MSTP port costs with the Auto setting when a port is a member of a trunk. 10 Mbps - 20,000 100 Mbps - 20,000 1000 Mbps - 2,000
Internal Path Cost	Use this parameter to set the cost of a port that is connected to a bridge that is a member of the same MSTP region. The range is 0 to 200,000,000. The value 0 activates the Auto setting, which sets the value according to port speed. Here are the MSTP port costs with the Auto setting for a port that is not a member of a trunk. 10 Mbps - 2,000,000 100 Mbps - 200,000 1000 Mbps - 20,000 Here are the MSTP port costs with the Auto setting for a port that is a member of a trunk. 10 Mbps - 20,000 100 Mbps - 20,000 1000 Mbps - 2,000

Table 83. MST Instance - Port Settings (Continued)

Parameter	Description
Point-to-Point	Use this parameter to define whether a port is a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 22, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Features Guide*.
Edge	Use this parameter to define whether a port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 22, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Features Guide*.

Note
The Path Cost variable in the MSTI Instance - Port Settings window is the internal path cost of a port.

8. After modifying the parameters, click the Apply button to activate your changes on the switch.

9. To permanently save your changes in the configuration file, click the Save button above the main menu.

10. Repeat this procedure to configure the MSTP parameters of other switch ports.

Displaying MSTP Statistics

To display MSTP statistics, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the MSTP option from the Monitoring menu.

   The switch displays the Device Monitoring - MSTP window shown in Figure 86.

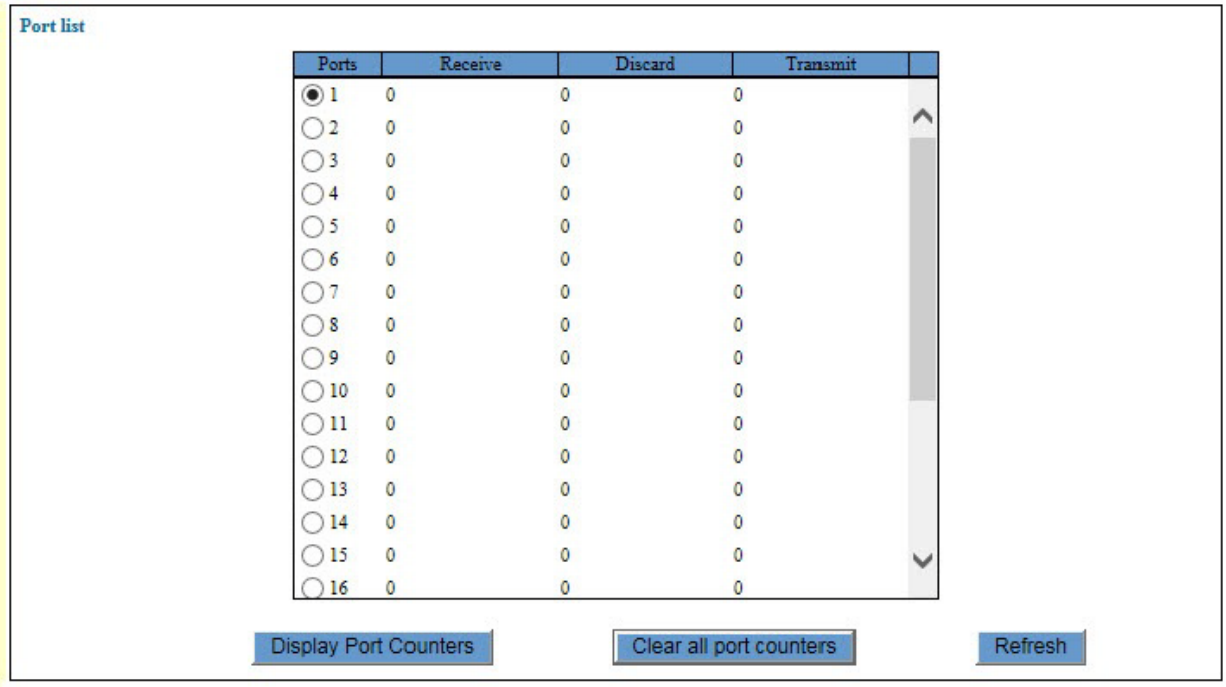

Figure 86. Device Monitoring - MSTP Window

The columns in the table are defined in Table 84.

Table 84. MSTI Statistics Window

Column	Description
Port	Displays the port numbers.
Receive	Displays the total number of STP, RSTP, and MSTP BPDUs the ports have received from other network devices.
Discard	Displays the total number of BPDUs the ports have discarded because they had the wrong Type value.

Table 84. MSTI Statistics Window (Continued)

Column	Description
Transmit	Displays the total number of STP, RSTP, and MSTP BPDUs the ports have transmitted to other network devices.

3. To view more port statistics, click the dialog circle of a port and click the Display Port Counters button. You can view the statistics of only one port at a time.

   The switch displays the MSTP Port Counters window, shown in Figure 87.

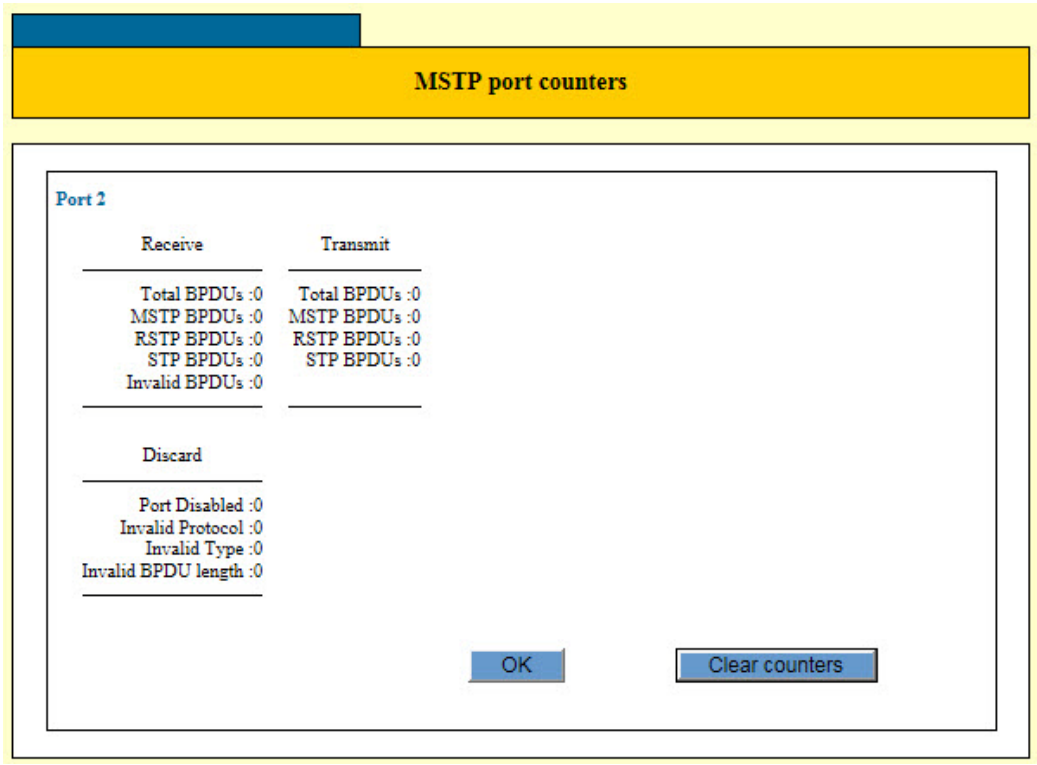

Figure 87. MSTP Port Counters Window

The counters in the table are defined in Table 85 on page 358.

Table 85. MSTI Statistics Window

Statistic	Description
Receive	
Total BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has received from other network devices.
MSTP BPDUs	Displays the total number of MSTP BPDUs the port has received from other network devices.
RSTP BPDUs	Displays the total number of RSTP BPDUs the port has received from other network devices.
STP BPDUs	Displays the total number of STP BPDUs the port has received from other network devices.
Invalid BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has deleted because they had the wrong type value.
Transmit	
Total BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has transmitted to other network devices.
MSTP BPDUs	Displays the total number of MSTP BPDUs the port has transmitted to other network devices.
RSTP BPDUs	Displays the total number of RSTP BPDUs the port has transmitted to other network devices.
STP BPDUs	Displays the total number of STP BPDUs the port has transmitted to other network devices.
Discard	
Port Disabled	This statistics is not supported. The value is always 0.
Invalid Protocol	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because the values in their protocol ID or protocol version ID fields were incorrect.

Table 85. MSTI Statistics Window (Continued)

Statistic	Description
Invalid Type	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because they contained the wrong type value.
Invalid BPDU length	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because they were the wrong length.

Enabling or Disabling BPDU Transparency for MSTP

The unit, at its default settings, discards BPDU packets from other network devices if it is not running RSTP or MSTP. As explained in “Hello Time and Bridge Protocol Data Units (BPDU)” on page 297, network devices that are running a spanning tree protocol use BPDUs to transmit spanning tree domain information to each other. In some circumstances, you may want the switch to forward these packets even if it is not running a spanning tree protocol. You can do this by activating BPDU transparency on the switch.

Note
The switch cannot be running RSTP or MSTP on any of its ports if it is to be transparent to BPDUs.

To configure BPDU transparency on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Others option from the Switch Settings menu.

   The Switch Settings - Others window is shown in Figure 31 on page 138.
3. Click the dialog box in the Transparent to BPDU Packets section of the window to enable or disable the BPDU transparency feature.

   The feature is enabled when the dialog box has a check mark. The switch forwards BPDUs when the feature is enabled. The feature is disabled when the dialog box is empty. The switch does not forward the packets when the feature is disabled. The default setting is disabled.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 30

Loop Detection Frame

This chapter describes how to configure the Loop Detection Frame feature on the ports on the switch. The sections in the chapter include:

Introduction

This feature enables the switch to detect loops in the wiring topology of a network and to perform specific actions if loops are detected. A loop exists when a network node can communicate with another node over more than one data path. The problem with wiring loops in Ethernet networks is that they can cause broadcast storms that consume network bandwidth and reduce network performance.

The feature can perform several actions if it detects a loop in the wiring topology of a network. The actions are defined in Table 86.

Table 86. Actions for Loop Detection Frame

Action	Description
PortDisable	Disables the port, but not the link. The port stops forwarding traffic, but the link to the remote network device remains up. The feature also enters a message in the event log. This is the default action.
LinkDown	Disables the port and link to block all traffic. It also enters a message in the event log.
BC Discard	Discards all broadcast packets and forwards all other traffic. It enters a message in the event log.
None	Takes no action, but enters a message in the event log.

This feature operates by transmitting a series of Loop Detection Frames (LDFs) from the designated switch ports. If no loops exist, then none of the frames should return to the switch. If a frame returns to the switch, the detection mechanism assumes that there is a loop somewhere in the network and performs the designated action.

Each LDF is a Layer 2 LLC frame with the following information:

- The source MAC address of the originating switch.
- The destination MAC address of the non-existent end station 00-00-F4-27-71-01.
- A randomly generated LDF ID number.

The loop packets can cross VLAN boundaries. The feature assumes a loop exists and performs the designated action even if the egress and ingress ports of the frames are in different VLANs.

Displaying the Loop Detection Frame Window

To display the Loop Detection Frame window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Loop Detection Frame option from the Switch Settings menu.

   The Switch Settings - Loop Detection Frame window is shown in Figure 88.

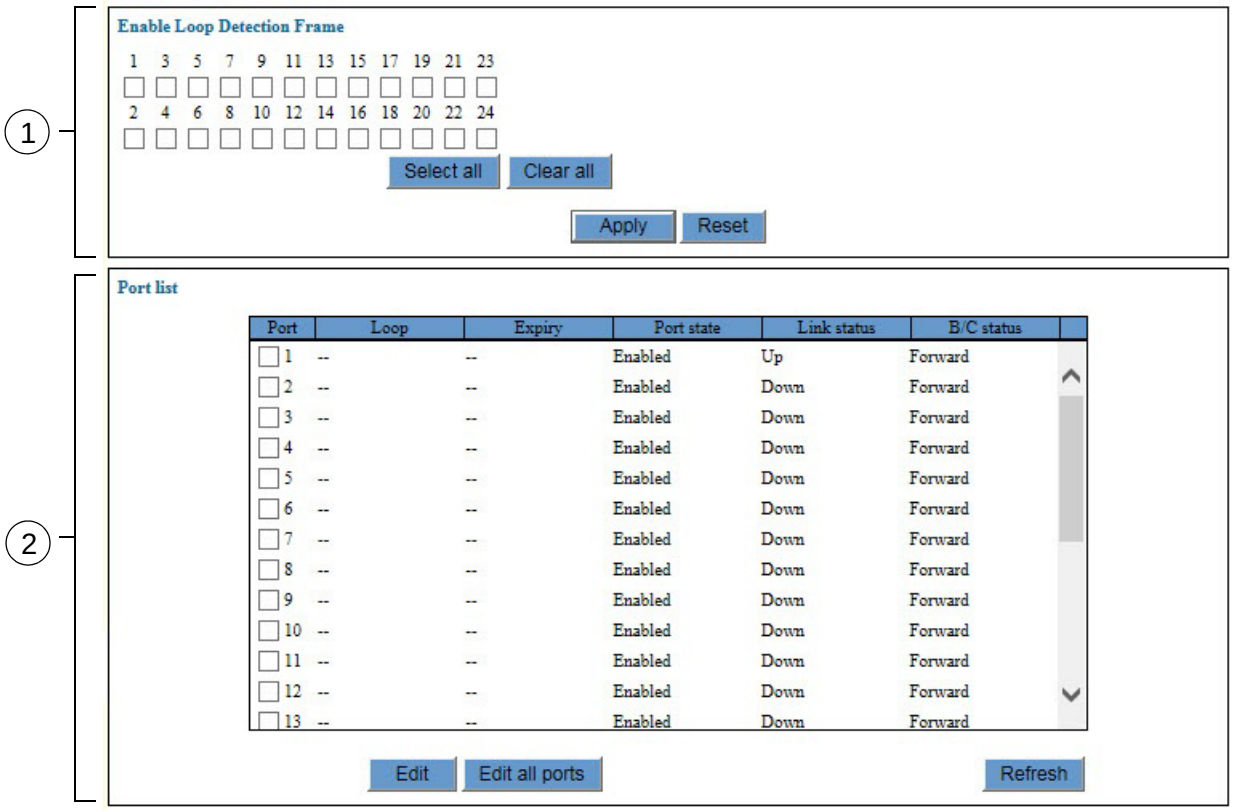

Figure 88. Switch Settings - Loop Detection Frame Window

The sections in the window are described in Table 87 on page 364.

Table 87. Switch Settings - Loop Detection Frame Window

Section	Description
1	Use this section to enable or disable Loop Detection Frame on the individual ports on the switch. Refer to “Enabling or Disabling Loop Detection Frame” on page 367.
2	Use this section to configure the port settings for Loop Detection Frame or to view port status. Refer to “Configuring Loop Detection Frame” on page 368. The columns in the table are described in Table 88.

The Port List table displays the current state of the Loop Detection Frame feature on the ports. The columns are described in Table 88.

Table 88. Port Settings Table in the Switch Settings - Loop Detection Frame Window

Column	Description
Port	Displays the port number.
Loop	Displays whether a loop has been detected on the port. The possible states are listed here: -- - The feature is not enabled on the port. Normal - The feature is enabled on the port. Blocking - The feature has detected a loop on the port and is blocking either all of the traffic or only the broadcast frames, depending on the action setting. Detected - The switch has detected a loop on the port, but because the action on the port is None, it is taking no action other than entering a message in the event log.

Table 88. Port Settings Table in the Switch Settings - Loop Detection Frame Window (Continued)

Column	Description
Expiry	Displays the amount of time remaining before the action expires. If the loop persists after the action expires, the switch reapplies the action to the port. Please note the following information: If the threshold action is PortDisable or LinkDown, the Expiry states the remaining time before the port begins forwarding traffic again. If the action is BC Discard, the Expiry states the remaining time before the port begins forwarding broadcast traffic again. If the port action is None, the Expiry value is not applicable and can be ignored. If the Loop status of the port is Blocking but there is no expiration time, the port is configured to remain in the action state until it is manually overridden. To override the action of a port in this state, display Port Settings window for the port, as explained in "Configuring Port Parameters" on page 118, and click the Apply button.
Port State	Displays the current state of the port. The possible states are listed here: Enabled - The port is enabled. (A port will have a Port State of Enabled even if it performs the PortDisable, BC Discard, or None action.) Disabled(Act) - The switch disabled the port because it detected a loop and the action is set to LinkDown. Disabled(User) - The port was manually disabled. For instructions on how to manually enable ports, refer to "Configuring Port Parameters" on page 118.

Table 88. Port Settings Table in the Switch Settings - Loop Detection Frame Window (Continued)

Column	Description
Link Status	Displays the link state. The possible states are listed here: Up - The port has established a link to a network device. Down - The port has not established a link to a network device. Down(Act) - The switch has disabled the link on the port because it detected a loop and LinkDown is the defined action.
B/C Status	Displays the status of the forwarding of broadcast packets. The possible states are listed here: Forward - The port may forward broadcast frames. Discard - The port is discarding broadcast packets because there is a loop and the action is set to BC Discard.

Enabling or Disabling Loop Detection Frame

This section explains how to enable or disable Loop Detection Frame on the individual ports on the switch.

> **Note**
> Allied Telesis recommends configuring the port settings before enabling the feature. For instructions, refer to "Configuring Loop Detection Frame" on page 368.

To enable or disable Loop Detection Frame on the ports, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Loop Detection Frame option from the Switch Settings menu.

   The Switch Settings - Loop Detection Frame window is shown in Figure 88 on page 363.
3. In the top section of the window, click the dialog boxes of the ports where you want to enable or disable the feature. The feature is enabled on a port when a dialog box has a check mark and disabled when a dialog box is empty.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button in the main menu.

Configuring Loop Detection Frame

To configure the parameter settings of the Loop Detection Frame on the ports, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Loop Detection Feature option from the Switch Settings menu.

   The Switch Settings - Loop Detection Feature window is shown in Figure 88 on page 363.
3. In the bottom section of the window, click the dialog box of the port you want to configure. You may configure more than one port at a time.
4. Click the Edit button. To configure all of the ports on the switch, click the Edit All Ports button.

   The switch displays the LDF - Port Settings window, shown in Figure 89.

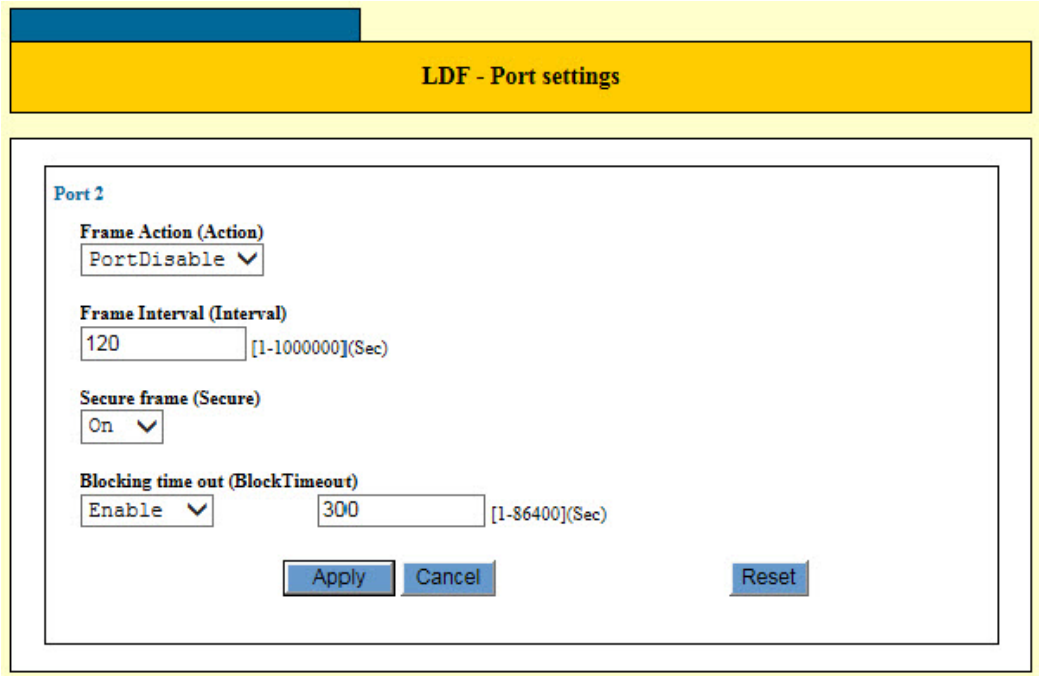

Figure 89. LDF - Port Settings Window

5. Configure the parameters, as needed. The parameters are described in Table 89 on page 369.

Table 89. LDF - Port Settings Window

Parameter	Description
Frame Action (Action)	Specifies the action of the switch if it detects a loop on a port. The options are listed here: PortDisable: Disables the port, but not the link. The port stops forwarding traffic, but the link to the remote network device remains up. This is the default setting. LinkDown: Disables the port and link. The port stops forwarding traffic and drops the link to the remote network device. BC Discard: Discards broadcast frames. None: Performs no action except to log a message in the event log.
Frame Interval (Interval)	Specifies the time interval in seconds between the transmission of Loop Detection Frames on the ports. The range is 1 to 1,000,000 seconds. The default is 120 seconds. At the default setting, the switch will not detect a loop for up to two minutes.
Secure Frame (Secure)	Specifies whether to discard LDFs that are received out of sequence. The options are listed here: On: Discards LDFs that are received out of sequence. This is the default setting. Off: Does not discard LDFs that are received out of sequence.

Table 89. LDF - Port Settings Window (Continued)

Parameter	Description
Blocking Time Out (BlockTimeout)	Specifies the status of the port after the switch detects a loop and activates the designated action. The possible options are listed here: Enable - Allows the port to return to its prior state (e.g., forwarding traffic) after the specified period of time of the action, provided that the loop is no longer present in the network. (If the loop persists, the switch reapplies the action to the port.) If you select this option, use the field next to the pull-down menu to specify how long the port is to remain disabled. The range is 1 to 86400 seconds. The default is 300 seconds (5 minutes). Disable - Maintains the action of the port until it is manually overridden. The action remains active (e.g., the port remains disabled) until you manually override it by displaying the Port Settings window of the port, as explained in “Configuring Port Parameters” on page 118, and clicking the Apply button.

Here are several factors to consider as you configure the feature:

- ❒ You should use the LinkDown action for the ports of a static port trunk.
- ❒ You may use the Loop Detection Feature and packet storm protection on the same ports. However, you may not specify BC Discard as the action on the ports.
- ❒ You should set the Blocking Time Out parameter to 60 seconds or more on ports with the LinkDown action.
- ❒ Breaking the link on a port, such as disconnecting the network cable, cancels the PortDisable, BC Discard, and None actions. Breaking the link on a port set to the LinkDown action does not cancel the action.

6. Click the Apply button to implement your changes on the switch.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Statistics for Loop Detection Frame

To view Loop Detection Frame statistics, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the Loop Detection Frame option from the Device Monitoring menu.

   The Device Monitoring - Loop Detection Feature window is shown in Figure 90.

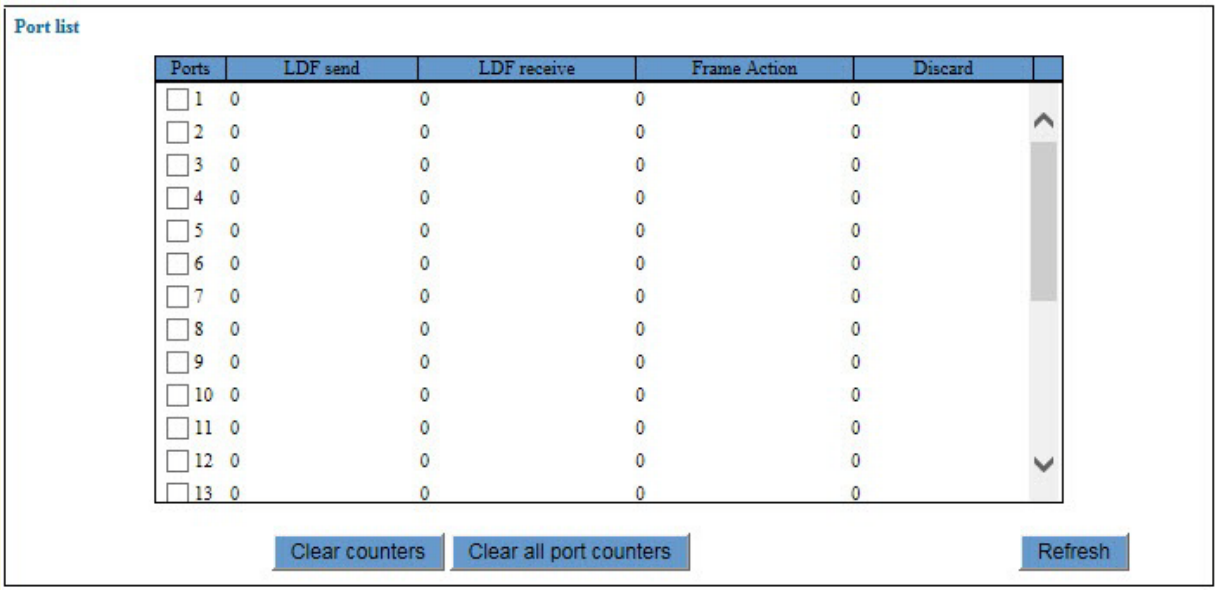

Figure 90. Device Monitoring - Loop Detection Frame Window

The columns in the table are described in Table 90.

Table 90. Device Monitoring - Loop Detection Frame Window

Column	Description
Port	Displays the port number.
Frame Send	Displays the number of Loop Detection Frames the port has transmitted.
Frame Receive	Displays the number of Loop Detection Frames the port has received.
Frame Action	Displays the number of times the switch has detected a loop on the port and performed the configured action.

Table 90. Device Monitoring - Loop Detection Frame Window (Continued)

Column	Description
Discard	Displays the number of ingress Loop Detection Frames the port has discarded.

3. To clear port statistics, do one of the following:
   - ❒ To clear the statistics for individual ports, click the dialog boxes of the ports and click Clear Counters button.
   - ❒ To clear the port statistics for all of the ports, click the Clear All Port Counters button.
4. To update the statistics, click the Refresh button.

Chapter 31

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. The sections in the chapter are listed here:

Introduction

Internet Group Management Protocol (IGMP) is used by IPv4 routers to build and maintain lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) A router builds a multicast membership list by periodically sending out queries to the local area networks connected to its ports and waiting for responses from the network nodes.

A node wanting to become a member of a multicast group responds to a query by sending a *report*. A report indicates an end node's intent to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. After becoming a member of a multicast group, a host node must continue to periodically issue reports to remain a member.

After the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are three versions of IGMP — versions 1, 2, and 3. One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1 it stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames, and removes it from the membership list of the multicast group.

In version 2 a host node exits from a multicast group by sending a *leave request*. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

Version 3 adds the ability of host nodes to join or leave specific sources in a multicast group.

The IGMP snooping feature allows the switch to monitor the flow of queries from routers and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports

connected to host nodes.

Without IGMP snooping a switch would have to flood multicast packets out all of its ports, except the port on which it received the packets. Such flooding of packets can negatively impact network performance.

The switch maintains its list of multicast groups through an adjustable timeout value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

The switch supports all three versions of IGMP.

Note
The default setting for IGMP snooping on the switch is disabled.

Displaying the IGMP Snooping Window

To display the IGMP snooping window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the IGMP Snooping option from the Switch Settings menu.

   The Switch Settings - IGMP Snooping window is shown in Figure 91.

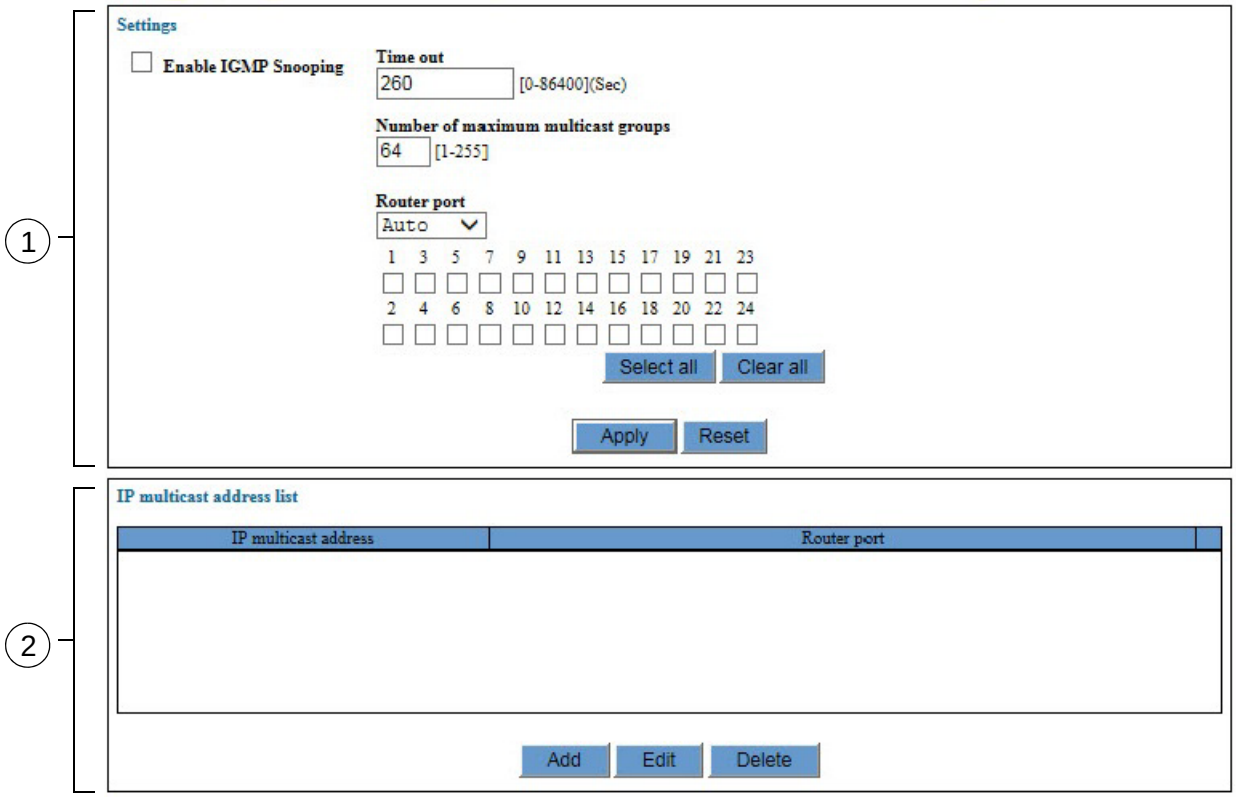

Figure 91. Switch Settings - IGMP Snooping Window

The sections in the window are briefly described in Table 91.

Table 91. Switch Settings - IGMP Snooping Window

Section	Description
1	Use this section to enable or disable IGMP snooping and to configure the feature parameters. Refer to “Configuring IGMP Snooping” on page 378.

Table 91. Switch Settings - IGMP Snooping Window (Continued)

Section	Description
2	Use this section to view the multicast addresses of the switch or to manually add or delete addresses. Refer to “Adding Static Multicast Addresses” on page 380 and “Deleting Static Multicast Addresses” on page 383.

The table in the bottom section of the window displays the multicast addresses that the switch has learned or that were entered manually into the switch. The two columns in the table are described in Table 92.

Table 92. IP Multicast Address List Table

Columns	Description
Multicast Address	Displays the multicast addresses the switch has learned or that were entered manually.
Router Ports	Displays the ports on which the multicast addresses were learned or added and where the multicast routers are located.

Configuring IGMP Snooping

To enable or disable IGMP snooping or to configure its parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the IGMP Snooping option from the Switch Settings menu.

   The Switch Settings - IGMP Snooping window is shown in Figure 91 on page 376.
3. Configure the parameters in the top part of the window.

   The parameters are defined in Table 93.

Table 93. Switch Settings - IGMP Snooping Window

Parameter	Description
Enable IGMP Snooping	Use this parameter to enable or disable IGMP snooping on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled.
Timeout	Use this option to specify the maximum amount of time the switch is to wait for responses from inactive host nodes. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds. If you set the timeout to zero (0), the timer never times out, and the timeout interval is essentially disabled. This parameter also controls the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

Table 93. Switch Settings - IGMP Snooping Window (Continued)

Parameter	Description
Number of Maximum Multicast Groups	Use this option to specify the maximum number of IGMP multicast groups the switch can learn. This parameter is useful with networks that contain a large number of multicast groups. The range is 1 to 255 groups. The default is 64 multicast groups.
Router Port	Use this pull-down menu to specify the manner by which the switch is to learn the ports where the multicast routers are located. The choices are listed here: Auto: This option enables the switch to automatically identify the router ports. None: This option sets the mode to manual without any router ports specified. Select: This option allows you to manually designate the router ports. If you choose Select, use the list of ports below the Router Port pull-down menu to designate the router ports. A check mark in a dialog box indicates that the corresponding port is a router port while an empty check mark indicates that the corresponding port is not a router port.

4. Click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Note
The combined number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

Adding Static Multicast Addresses

To manually add multicast addresses to the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the IGMP Snooping option from the Switch Settings menu.

   The Switch Settings - IGMP Snooping window is shown in Figure 91 on page 376.

   Note
   Steps 3 and 4 explain how to set the Router Port parameter to Select and manually designate the router port for the static address This is required for static multicast addresses.

3. In the Switch Settings - IGMP Snooping window, choose Select for the Router Port setting.

   Note
   Changing the Select parameter from Auto or None to Select deletes all of the multicast addresses the switch has already learned.

4. Beneath the Router Port parameter, click the port(s) where all of the multicast routers are located.

   When designating the router ports, be sure to designate the router ports for all of the static multicast addresses, and not only the port for the new static address you are adding.

5. Click the Apply button.
6. Click the Add button at the bottom of the window.

   The IP Multicast Address - Add window is shown in Figure 92 on page 381.

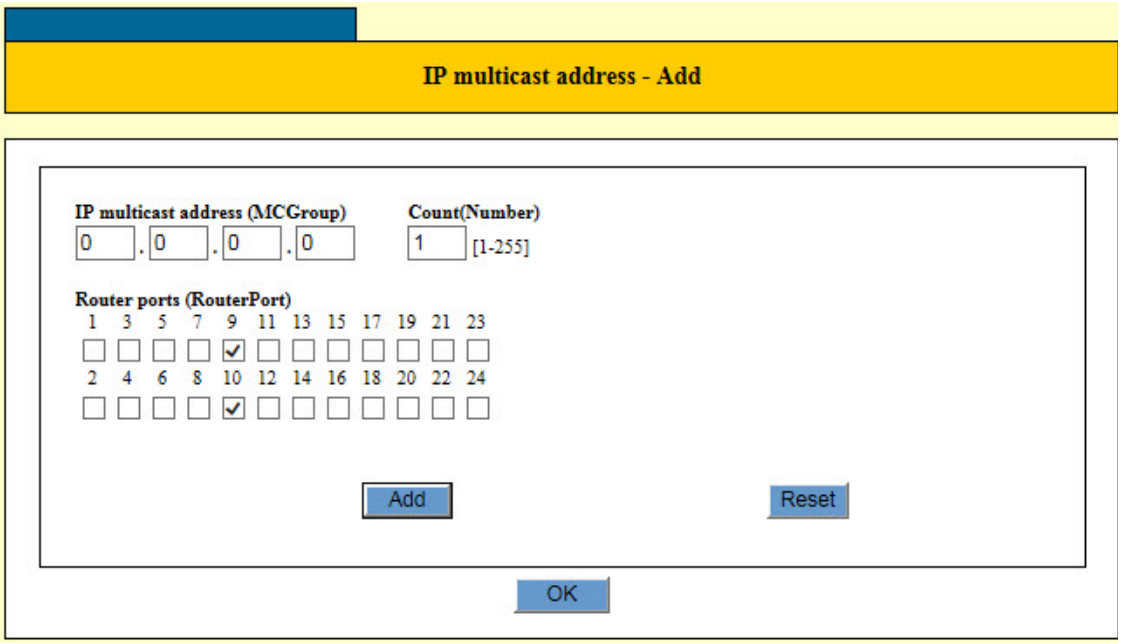

Figure 92. IP Multicast Address - Add Window

The list of ports in the window should have check marks in all of the router ports on the switch. The example window in Figure 92 indicates that ports 9 and 10 are router ports. If the window is not showing any router ports, click OK to close the window and repeat this procedure starting with step 3.

7. Configure the parameters in the window, as needed. The parameters are defined in Table 94.

Table 94. IP Multicast Address - Add Window

Parameter	Description
IP Multicast Address (MCGroup)	Use this parameter to specify an IP multicast address you want to add to the switch. If you want to enter a range of addresses, enter the lowest address of the range.
Count (Number)	Use this parameter to automatically enter consecutive multicast addresses. The range is 1 to 255 addresses.

Table 94. IP Multicast Address - Add Window (Continued)

Parameter	Description
Router Ports (RouterPorts)	Use the list of ports to designate the router port of the new static multicast address. This section should be identifying all of the router ports on the switch with check marks. If necessary, deselect those router ports that do not apply to the new address so as to leave a check mark in only the router port(s) for the new address. For example, let's assume that you are adding a multicast address to port 9 and both ports 9 and 10 have been designated as router ports, as shown in Figure 92 on page 381. Given that the new address applies only to router port 9, you would deselect port 10, leaving only port 9 with a check mark.

8. Click the Apply button to activate your changes on the switch.

9. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting Static Multicast Addresses

To delete static multicast addresses from the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the IGMP Snooping option from the Switch Settings menu.

   The Switch Settings - IGMP Snooping window is shown in Figure 91 on page 376.
3. In the IP Multicast Address List table in the bottom section of the window, click the dialog circle of the multicast address you want to delete. You may delete only one address at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click the Apply button to activate your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Multicast Groups

To display the multicast groups on the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the IGMP Snooping option from the Device Monitoring menu.

   The switch displays the Device Monitoring - IGMP Snooping window. An example of the window is shown in Figure 93.

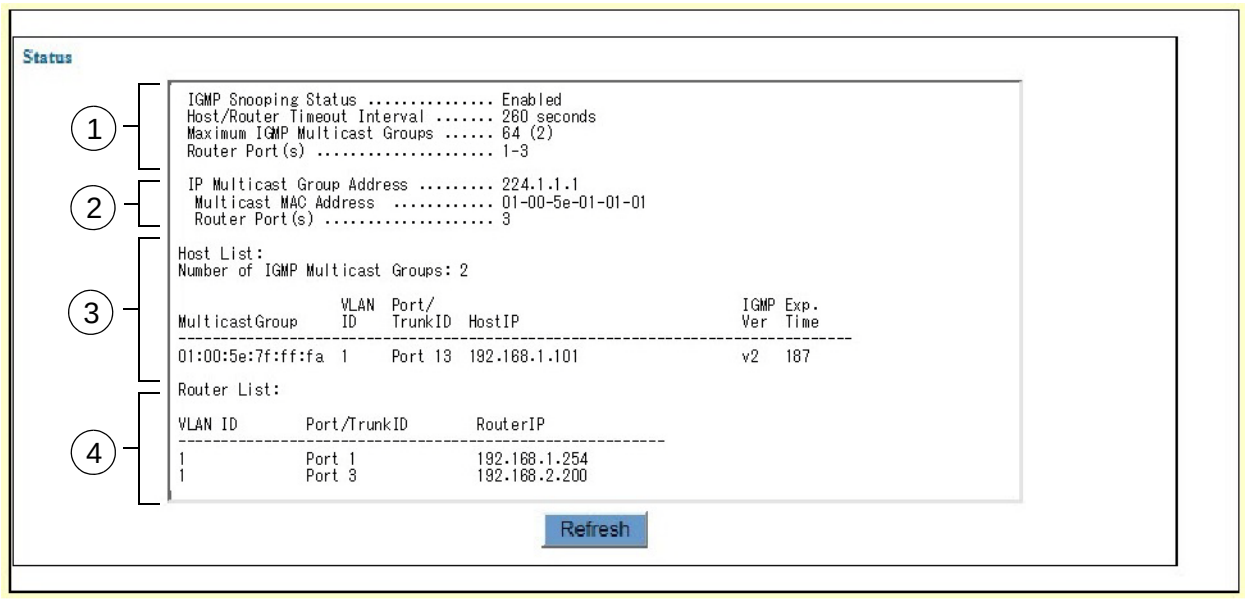

Figure 93. Device Monitoring - IGMP Snooping Window

The fields in section 1 contain the current settings for IGMP snooping and are defined in Table 93 on page 378.

Section 2 is displayed only for static multicast addresses that were entered manually. This section is not displayed if there are no static multicast addresses or if the switch has not detected the routers of the addresses.

The table in section 3 lists the multicast hosts. The columns in the table are defined in Table 95.

Table 95. Host List

Parameter	Description
Multicast Group	Displays the multicast address of the group.

Table 95. Host List (Continued)

Parameter	Description
VLAN ID	Displays the VID of the VLAN where the host port is an untagged member.
Port/Trunk ID	Displays the port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.
Host IP	Displays the IP address of the host node connected to the port.
IGMP Ver	Displays the version of IGMP used by the host.
Exp. Time	Displays the number of seconds remaining before the host is timed out if no further IGMP reports are received from it.

The table in section 4 lists the multicast routers. The columns in the table are defined in Table 96.

Table 96. Multicast Router List

Parameter	Description
VLAN ID	Displays the VID of the VLAN where the router port is an untagged member.
Port/Trunk ID	Displays the port on the switch where the router is connected. If the router is connected to the switch through a trunk, the trunk ID number, and not the port number, is displayed.
Router IP	Displays the IP address of the routing interface on the router.

Chapter 32

MLD Snooping

This chapter describes how to configure the MLD snooping feature on the switch. The sections in the chapter are listed here:

Introduction

MLD snooping is similar to IGMP snooping. Like IGMP snooping, it enables the switch to learn the addresses of multicast traffic so that it can direct the packets to only those ports that have multicast host nodes. This improves network performance by limiting multicast traffic to only those ports that have host nodes. The difference between the two snooping protocols relates to the versions of IP multicast traffic they support. IGMP snooping is for IPv4 multicast traffic while MLD snooping is for IPv6 multicast traffic.

Displaying the MLD Snooping Window

To display the MLD snooping window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MLD Snooping option from the Switch Settings menu.

   The Switch Settings - MLD Snooping window is shown in Figure 94.

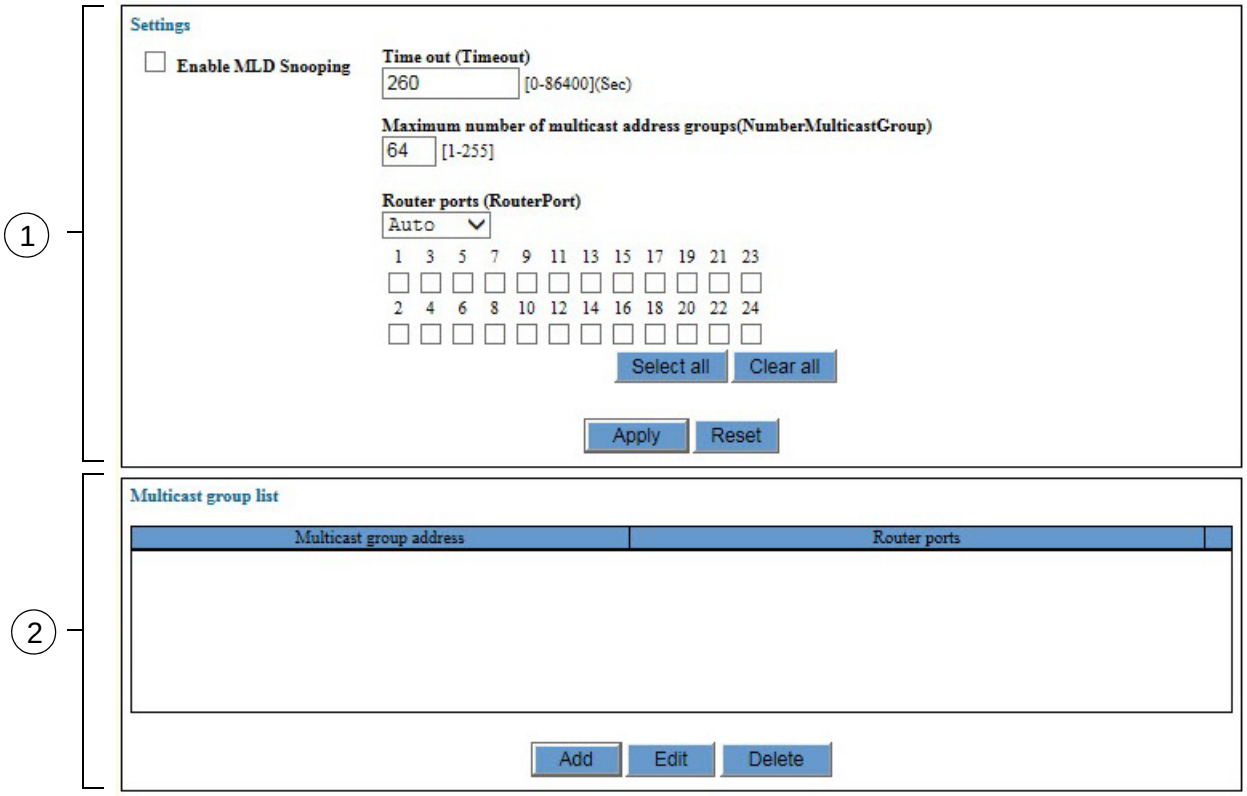

Figure 94. Switch Settings - MLD Snooping Window

The sections in the window are described in Table 97.

Table 97. Switch Settings - MLD Snooping Window

Section	Description
1	Use this section of the window to enable or disable MLD snooping or to configure the parameters. Refer to “Configuring MLD Snooping” on page 391.

Table 97. Switch Settings - MLD Snooping Window (Continued)

Section	Description
2	Use this section to view the multicast addresses of the switch or to manually add or delete addresses. Refer to “Adding Static Multicast Addresses” on page 393 or “Deleting Static Multicast Addresses” on page 396.

The Multicast Group List table in the bottom portion of the Switch Settings - MLD Snooping window displays the multicast addresses that the switch has learned or that were manually assigned to the switch. The table has two columns. The columns are described in Table 98.

Table 98. Multicast Group List Table

Column	Description
Multicast Address	Displays the multicast addresses the switch has learned or that were entered manually.
Router Ports	Displays the ports on which the multicast addresses were learned or added and where the multicast routers are located.

Configuring MLD Snooping

To enable or disable MLD snooping or to configure the parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MLD Snooping option from the Switch Settings menu.

   The Switch Settings - MLD Snooping window is shown in Figure 94 on page 389.
3. Configure the parameters in the top part of the window.

   The parameters are defined in Table 99.

Table 99. Switch Settings - MLD Snooping Window

Parameter	Description
Enable MLD Snooping	Use this parameter to enable or disable MLD snooping on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled.
Timeout (Timeout)	Use this parameter to specify the time period, in seconds, the switch uses to determine inactive host nodes. An inactive host node is a node that has not sent an MLD report during the specified time interval. The range is 1 to 86,400 seconds (24 hours). The default value is 260 seconds. This parameter also controls the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

Table 99. Switch Settings - MLD Snooping Window (Continued)

Parameter	Description
Maximum Number of Multicast Address Groups (NumberMulticast Group)	Use this parameter to specify the maximum number of multicast addresses the switch can learn. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 to 255 addresses. The default value is 64 addresses.
Router Ports (RouterPort)	Use this pull-down menu to specify the manner by which the switch is to learn the ports where the multicast routers are located. The choices are listed here: Auto: Use this option if you want the switch to identify the router ports automatically. None: Use this option to set the mode to manual without any router ports specified. Select: Use this option to manually designate the router ports. If you choose Select, use the list of ports below the Router Port pull-down menu to designate the router ports. A check mark in a dialog box indicates that the corresponding port is a router port while an empty check mark indicates that the corresponding port is not a router port.

4. Click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding Static Multicast Addresses

To manually add static IPv6 multicast addresses to the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MLD Snooping option from the Switch Settings menu.

   The Switch Settings - MLD Snooping window is shown in Figure 94 on page 389.

   Note
   Steps 3 and 4 explain how to set the Router Port parameter to Select and manually designate the router port for the static address This is required for static multicast addresses.

3. In the Switch Settings - MLD Snooping window, choose Select for the Router Port setting.

   Note
   Changing the Select parameter from Auto or None to Select deletes all of the multicast addresses the switch may have already learned.

4. Beneath the Router Port parameter, click the port(s) where all of the multicast routers are located.

   When designating the router ports, be sure to designate the router ports for all of the static multicast addresses, and not only the port for the new static address you are adding.

5. Click the Apply button.
6. Click the Add button at the bottom of the window.

   The Multicast Group - Add window is shown in Figure 95 on page 394.

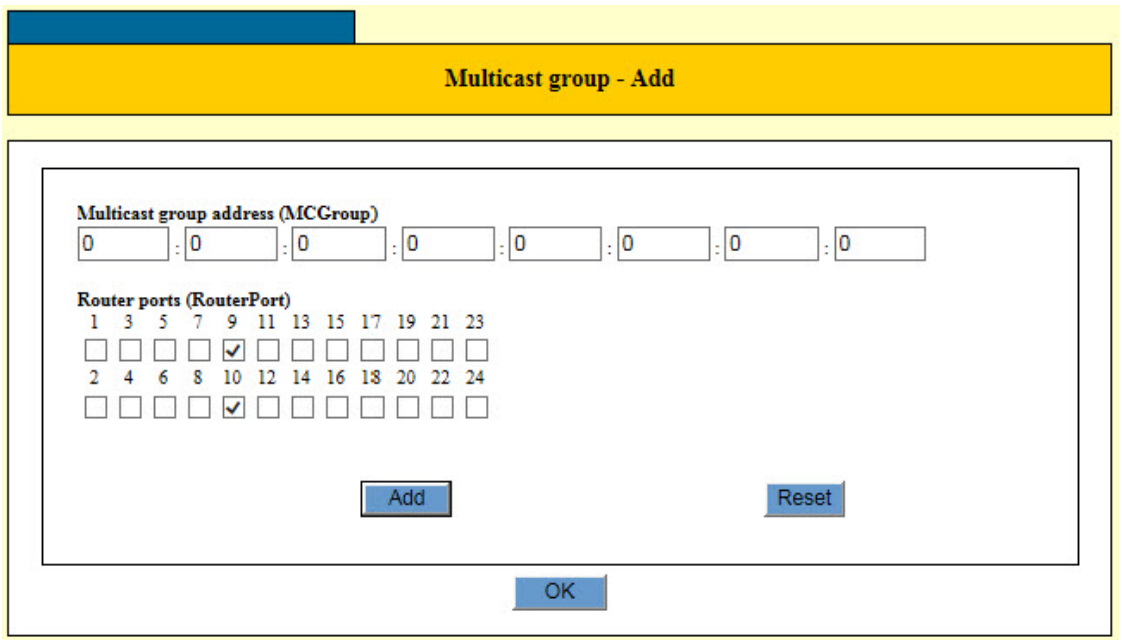

Figure 95. Multicast Group - Add Window

The list of ports in the window should have check marks in all of the router ports on the switch. The example window in Figure 95 indicates that ports 9 and 10 are router ports. If the window is not showing any router ports, click OK to close the window and repeat this procedure starting with step 3.

7. Configure the parameters in the window, as needed.

   The parameters are defined in Table 100.

Table 100. Multicast Group - Add Window

Parameter	Description
Multicast Group Address (MCGroup)	Use this parameter to specify the new IPv6 multicast address. You may enter only one address at a time. You may not enter a range of addresses.

Table 100. Multicast Group - Add Window (Continued)

Parameter	Description
Router Ports	Use the list of ports to designate the router port of the new static multicast address. This section should be identifying all of the router ports on the switch with check marks. If necessary, deselect those router ports that do not apply to the new address so as to leave a check mark in only the router port(s) for the new address. For example, let's assume that you are adding a multicast address to port 9 and both ports 9 and 10 have been designated as router ports, as shown in Figure 95 on page 394. Given that the new address applies only to router port 9, you would deselect port 10, leaving only port 9 with a check mark.

8. Click the Apply button to activate your changes on the switch.

9. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting Static Multicast Addresses

To delete static multicast addresses from the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the MLD Snooping option from the Switch Settings menu.

   The Switch Settings - MLD Snooping window is shown in Figure 94 on page 389.
3. In the Multicast Group List table in the bottom section of the window, click the dialog circle of the multicast address you want to delete. You may delete only one address at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click the Apply button to activate your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Multicast Groups

To display the IPv6 multicast groups that were learned by or assigned to the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the MLD Snooping option from the Device Monitoring menu.

   The switch displays the Device Monitoring - MLD Snooping page. An example of the window is shown in Figure 96.

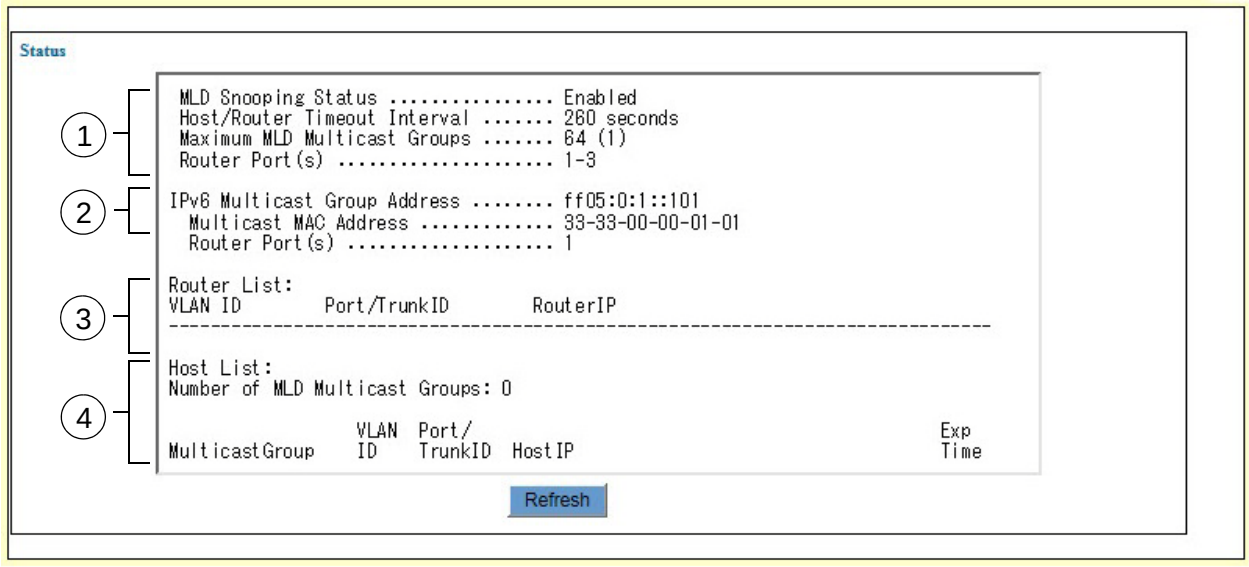

Figure 96. Device Monitoring - MLD Snooping

The fields in section 1 contain the current settings for MLD snooping and are defined in Table 99 on page 391.

Section 2 is displayed only for static multicast addresses that were entered manually. This section is not displayed if there are no static multicast addresses or if the switch has not detected the routers of the addresses.

The table in section 3 lists the multicast routers. The columns in the table are defined in Table 101.

Table 101. Multicast Router List

Column	Description
VLAN ID	Displays the VID of the VLAN where the router port is an untagged member.

Table 101. Multicast Router List (Continued)

Column	Description
Port/Trunk ID	Displays the port on the switch where the router is connected. If the router is connected to the switch through the ports of a trunk, the trunk ID number instead of the port numbers is displayed.
Router IP	Displays the IP address of the routing interface on the router.

The table in section 4 lists the multicast hosts the switch has learned. The columns in the table are defined in Table 102.

Table 102. Host List

Column	Description
Multicast Group	Displays the multicast address of the group.
VLAN ID	Displays the VID of the VLAN where the host port is an untagged member.
Port/Trunk ID	Displays the port on the switch where the host node is connected. If the host node is connected to the switch through the ports of a trunk, the trunk ID number instead of the port numbers is displayed.
Host IP	Displays the IP address of the host node on the port.
Exp. Time	Displays the number of seconds remaining before the host is timed out if no further MLD reports are received from it.

Chapter 33

DHCP Snooping

This chapter describes how to configure the DHCP snooping feature on the switch. The sections in the chapter include:

Displaying the DHCP Snooping Window

To display the DHCP snooping window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the DHCP Snooping option from the Switch Settings menu.

   The Switch Settings - DHCP Snooping window is shown in Figure 97.

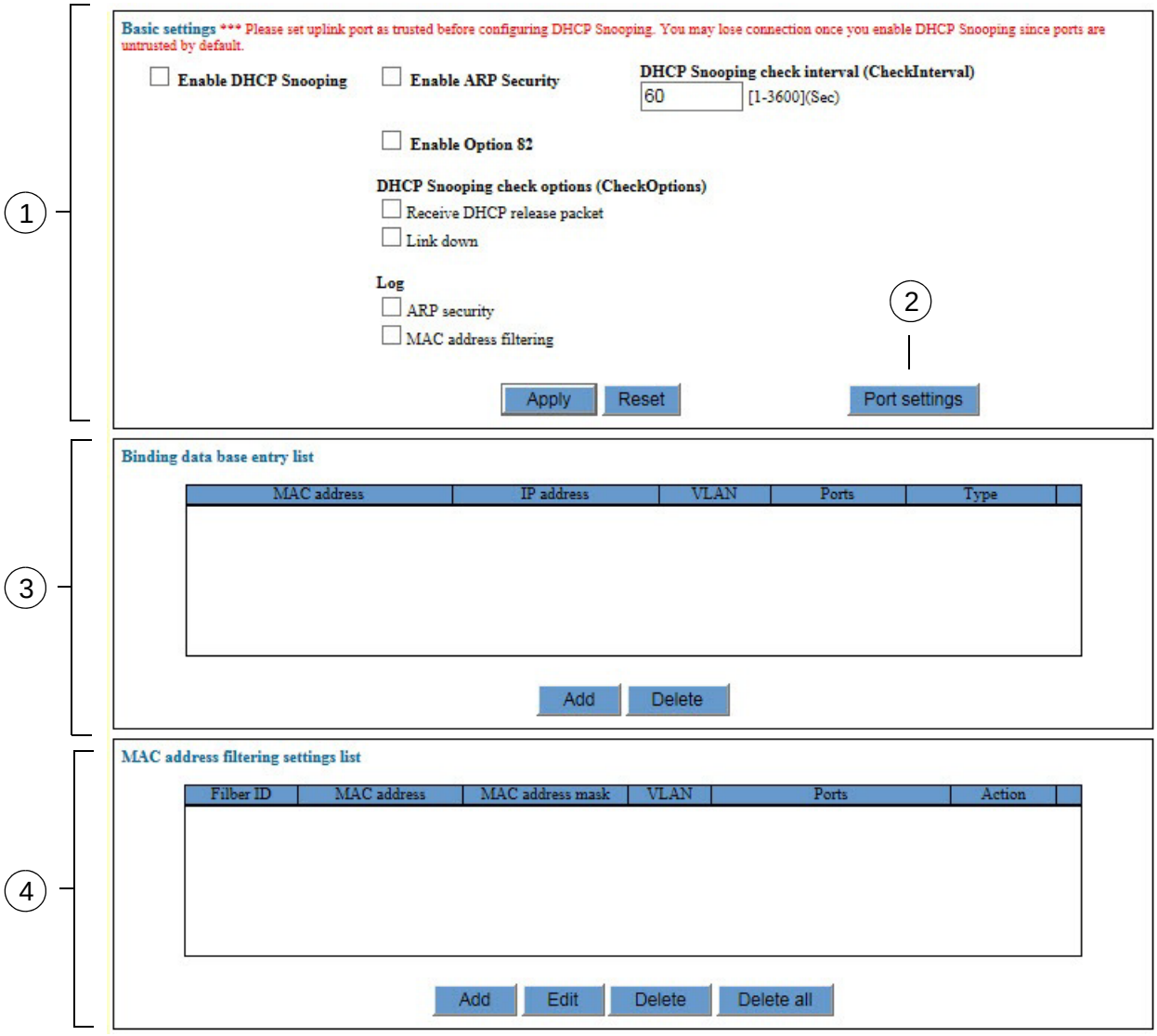

Figure 97. Switch Settings - DHCP Snooping Window

The sections in the window are briefly described in Table 103 on page 401.

Table 103. DHCP Snooping Window

Section	Description
1	Use this section to enable or disable DHCP snooping or to configure the basic parameters. Refer to "Configuring Basic DHCP Snooping Parameters" on page 402.
2	Use this Port Settings button to configure the ports. Refer to "Configuring the Ports" on page 404.
3	Use this section to manually add dynamic-like entries to the DHCP snooping database. Refer to "Adding Entries to the Binding Database" on page 407
4	Use this section to add MAC address filtering entries. Refer to "Adding MAC Address Filtering Entries" on page 409.

Configuring Basic DHCP Snooping Parameters

To enable or disable DHCP snooping or to configure its basic parameters, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the DHCP Snooping option from the Switch Settings menu.

   The DHCP Snooping window is shown in Figure 97 on page 400.
3. Configure the parameters in Basic Settings section of the window. The parameters are defined in Table 104.

Table 104. Basic Settings for DHCP Snooping

Parameter	Description
Enable DHCP Snooping	Use this parameter to enable or disable DHCP snooping on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled.
Enable ARP Security	Use this parameter to enable or disable ARP snooping on the untrusted ports on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled. When the option is enabled, the switch only responds to/forwards ARP packets if they have recognized IP and MAC source addresses.
DHCP Snooping Check Interval (CheckInterval)	Use this option to specify the time interval for verifying the binding database. The range is 1 to 3600 seconds. The default is 60 seconds.

Table 104. Basic Settings for DHCP Snooping (Continued)

Parameter	Description
Enable Option 82	Use this parameter to enable or disable DHCP Relay Agent Option 82 information insertion on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled. When this function is enabled, the switch does the following: - Inserts DHCP Relay Agent Option 82 information into DHCP packets it receives on untrusted ports. - Removes DHCP Relay Agent Option 82 information from DHCP packets it sends to untrusted ports.
Client Deletion Options	Use this option to specify the conditions that cause the switch to remove client data from the database.
Log - ARP Security	Use this option to enable or disable the entry of event messages in the event log when the switch detects an ARP security violation on an untrusted port in a VLAN where ARP security is enabled. The option is enabled when the dialog box has a check mark and disabled when the dialog box is empty. To view the messages, refer to “Displaying or Saving the Event Messages in the Event Log” on page 70.
Log - MAC Address Filtering	Use this option to enable or disable the entry of event messages in the event log when the switch detects MAC address security violation on an untrusted port.

4. Click the Apply button to activate your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring the Ports

To configure the ports for DHCP snooping, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the DHCP Snooping option from the Switch Settings menu.

   The DHCP Snooping window is shown in Figure 97 on page 400.
3. Click the Port Settings button in the top section of the window.

   The switch displays the Port Settings window in Figure 98.

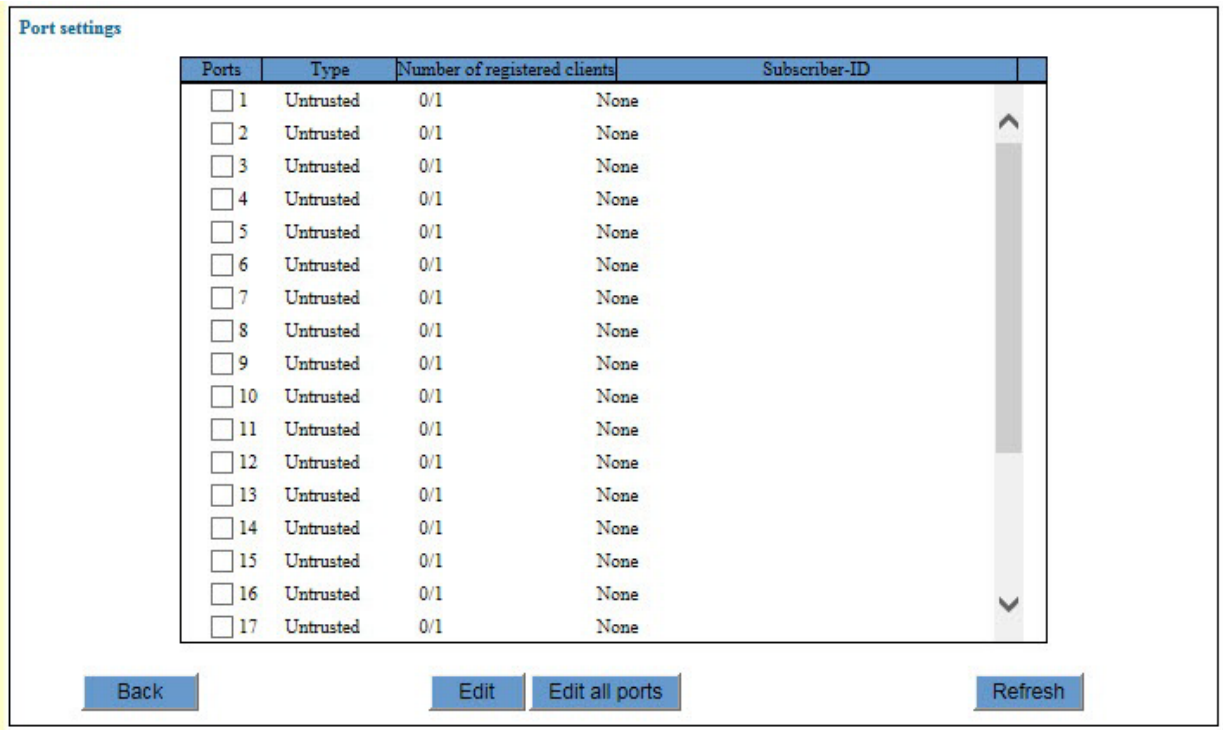

Figure 98. Port Settings Window for DHCP Snooping

4. Click the dialog box of the port you want to configure.

   You may configure more than one port at a time. A port is selected when its dialog box has a check mark and not selected when the dialog box is empty.
5. Click the Edit button. To configure all of the ports on the switch, click the Edit All Ports button.

The switch displays the DHCP Snooping - Port Settings window in Figure 99.

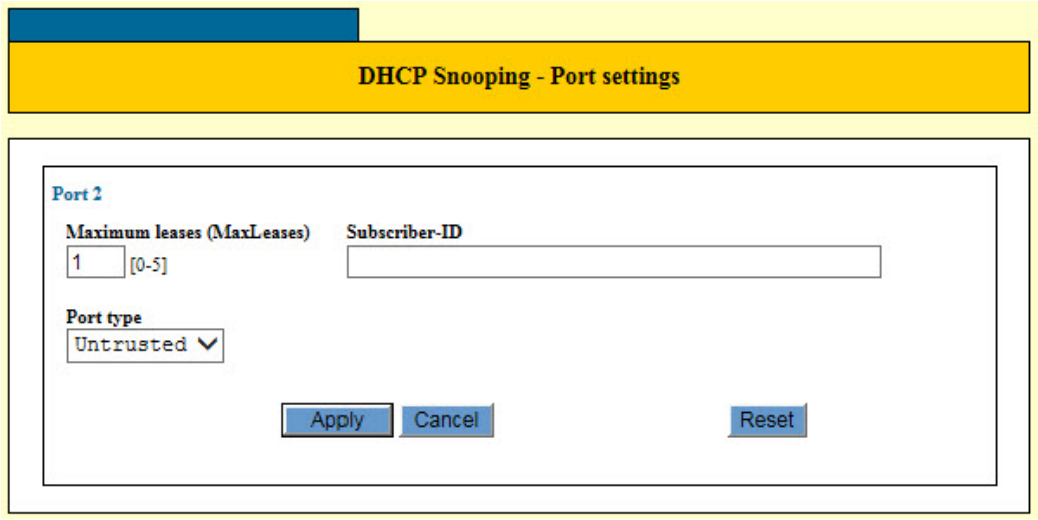

Figure 99. DHCP Snooping - Port Settings Window

6. Configure the parameters, as needed.

   The parameters are described in Table 105.

Table 105. DHCP Snooping - Port Settings Window

Parameter	Description
Maximum Leases (MaxLeases)	Use this option to specify the maximum number of DHCP lease entries that can be stored in the DHCP snooping database for a port. Once the limit is reached, no further DHCP lease allocations made to devices on a port are stored in the database.

Table 105. DHCP Snooping - Port Settings Window (Continued)

Parameter	Description
Subscriber-ID	Use this option to specify a Subscriber ID for a port. The Subscriber ID can be from 1 to 50 alphanumeric characters. The Subscriber ID is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port when all of the following are true: - A Subscribed ID is specified for the port using this option. - DHCP snooping Option 82 information insertion is enabled. - DHCP snooping is enabled on the switch. - DHCP snooping is enabled on the VLAN to which the port belongs.
Port Type	Use this option to set a port as a DHCP snooping trusted or untrusted port.

7. Click the Apply button to activate your changes on the switch.
8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding Entries to the Binding Database

To manually add an entry to the binding database, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the DHCP Snooping option from the Switch Settings menu.

   The DHCP Snooping window is shown in Figure 97 on page 400.
3. Click the Add button in the Binding Data Base Entry List section of the window.

   The Binding Data Base Client Information - Add window is shown in Figure 100.

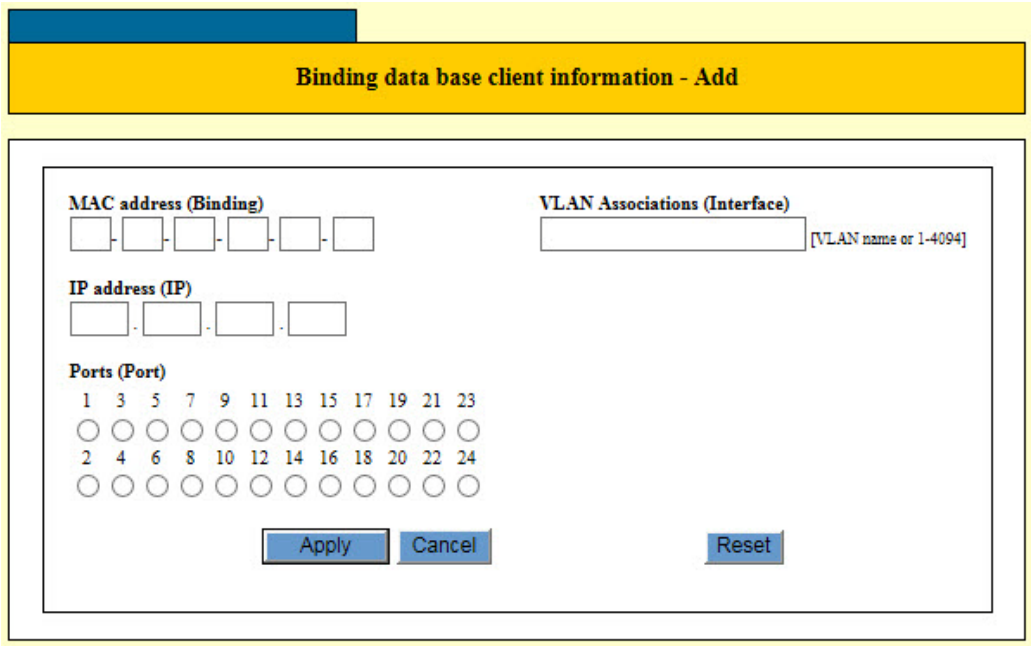

Figure 100. Binding Data Base Client Information - Add Window

4. Configure the parameters in the window, as needed. The parameters are defined in Table 106.

Table 106. Binding Data Base Client Information - Add Window

Parameter	Description
MAC Address (Binding)	Use this parameter to specify the client's MAC address.

Table 106. Binding Data Base Client Information - Add Window

Parameter	Description
VLAN Associations (Interface)	Use this option to enter the VLAN associated with the entry. You may identify the VLAN by its name or VID.
IP Address (IP)	Use this option to specify the IP address of the client.
Ports (Port)	Use this option to specify the port of the client.

5. Click the Apply button to activate your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding MAC Address Filtering Entries

To add MAC address filtering entries, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the DHCP Snooping option from the Switch Settings menu.

   The DHCP Snooping window is shown in Figure 97 on page 400.
3. Click the Add button in the MAC Address Filtering Settings List section of the window.

   The MAC Address Filtering Entry - Add window is shown in Figure 101.

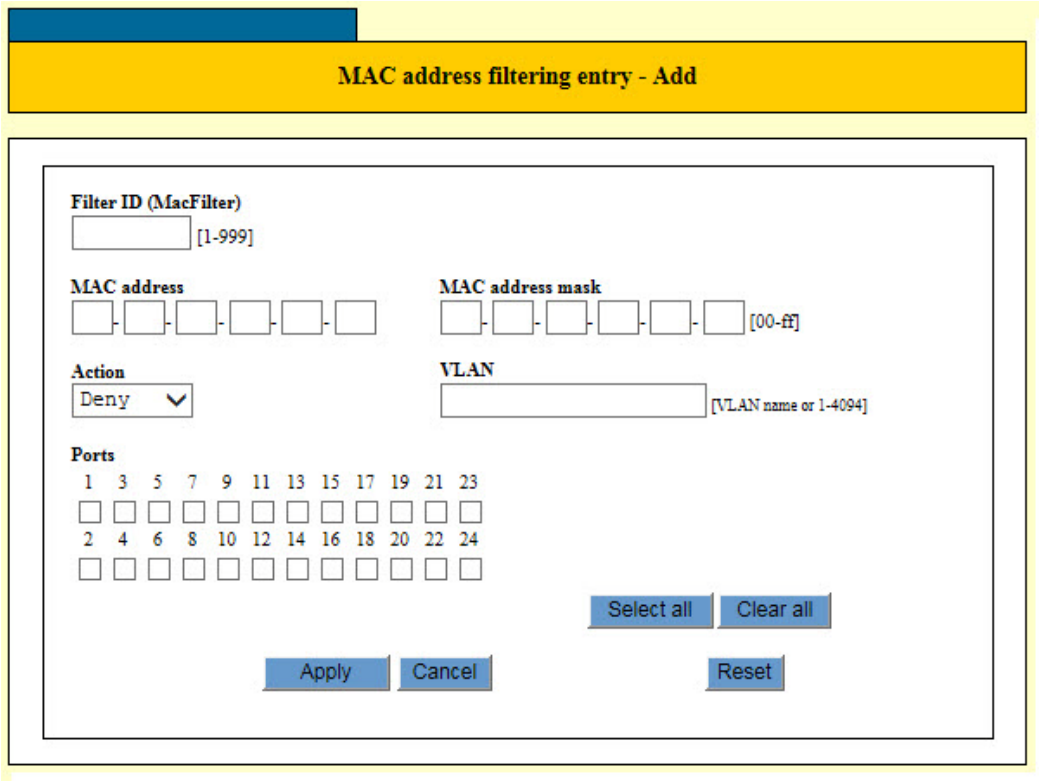

Figure 101. MAC Address Filtering Entry - Add Window

4. Configure the parameters in the window, as needed. The parameters are defined in Table 107 on page 410.

Table 107. MAC Address Filtering Entry - Add Window

Parameter	Description
Filter ID (Macfilter)	Use this option to enter an ID number for the entry. The range is 1 to 999.
MAC Address	Use this parameter to specify the MAC address of the filtered network device.
MAC Address Mask	Use this option to enter a mask for the MAC address. The mask for a specific address is FF:FF:FF:FF:FF:FF. \
Action	Use this option to specify the action of Permit or Deny for the filter.
VLAN	Use this option to specify the name or ID of the VLAN of the network device.
Ports	Use this section to specify the port on the switch to which the network device is connected.

5. Click the Apply button to activate your changes on the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying DHCP Snooping

To view DHCP snooping information, select the DHCP Snooping option from the Device Monitoring menu. An example of the window is shown in Figure 102.

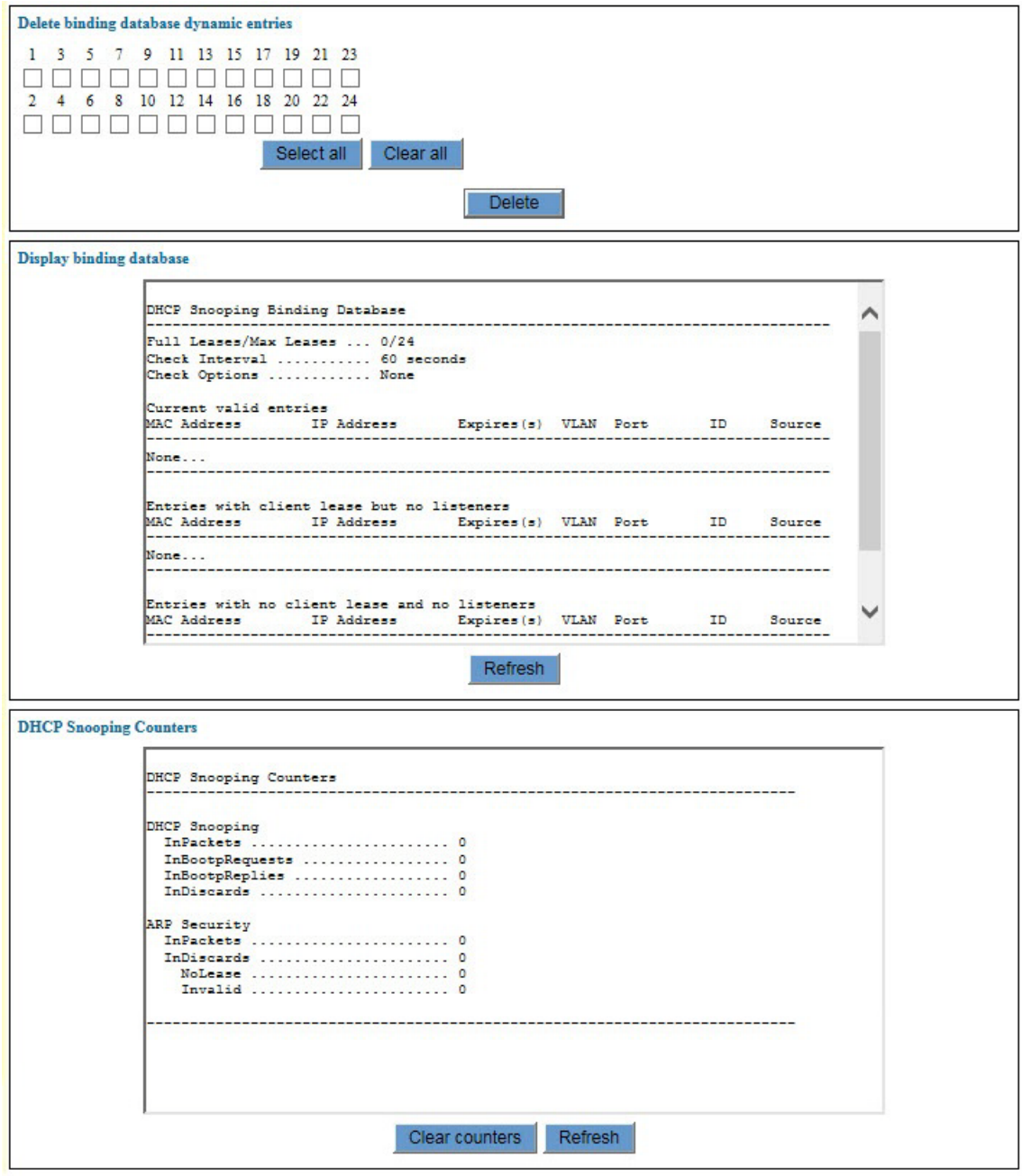

Figure 102. Device Monitoring - DHCP Snooping Window

Chapter 34
Switch Storm Detection

This chapter explains how to configure the storm detection feature of the switch. The sections in the chapter are listed here:

Introduction

You may use this feature to set high or low rate thresholds for the ingress packets on the individual ports on the switch, and actions for the ports to perform if the thresholds are crossed. Threshold violations can take the following forms:

- A violation on a low rate threshold occurs on a port when the actual ingress packet rate is above the defined threshold rate and falls below it. A violation does not occur if the packet rate is below the low rate threshold and rises above it.
- A violation on a high rate threshold occurs on a port when the actual ingress packet rate is below the defined threshold rate and rises above it. A violation does not occur if the packet rate is above the threshold and falls below it.

There are four actions a port can perform in response to a threshold violation. The actions are defined in Table 108.

Table 108. Actions for Switch Storm Detection

Action	Description
PortDisable	Disables the port, but not the link, when a packet rate threshold is crossed. The port stops forwarding all traffic, but the link to the remote network device remains up. The feature also enters a message in the event log. This is the default action.
LinkDown	Disables the port and link to block all traffic. It also enters a message in the event log.
BC Discard	Discards all broadcast packets, but forwards all other traffic. It enters a message in the event log.
None	Takes no action, but enters a message in the event log.

Here are the feature guidelines:

- The thresholds apply to the ingress traffic of a port, but not the egress traffic.
- The ports can have different thresholds and actions.
- You may specify different actions for the high and low thresholds of a port.

- You specify the thresholds in kilobits per second (Kbps).
- You may specify the time duration of an action on a port when a high or low threshold is crossed. A port returns to its previous state when the time duration of an action expires.
- You may disable the time duration so that an action remains in force on a port until it is manually overridden. For example, if the action of a threshold on a port is PortDisable and the threshold is crossed, the port remains disabled until the action is manually overridden.

Note
You may manually override an action by enabling a port. To accomplish this from the web browser windows, display the Port Settings window for the port and click the Apply button. For instructions, refer to "Configuring Port Parameters" on page 118. To enable a port from the command line interface, use the ENABLE SWITCH PORT command.

- You may apply packet rate thresholds to the ports of a static port trunk, but the action should be either LinkDown or None.
- The time duration for the LinkDown action should not be less than 60 seconds.The action may not work correctly if the time duration is less than 60 seconds.

Displaying the Switch Storm Detection Window

To display the switch storm detection window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Switch Storm Detection option from the Switch Settings menu.

   The Switch Settings - Switch Storm Detection window is shown in Figure 103.

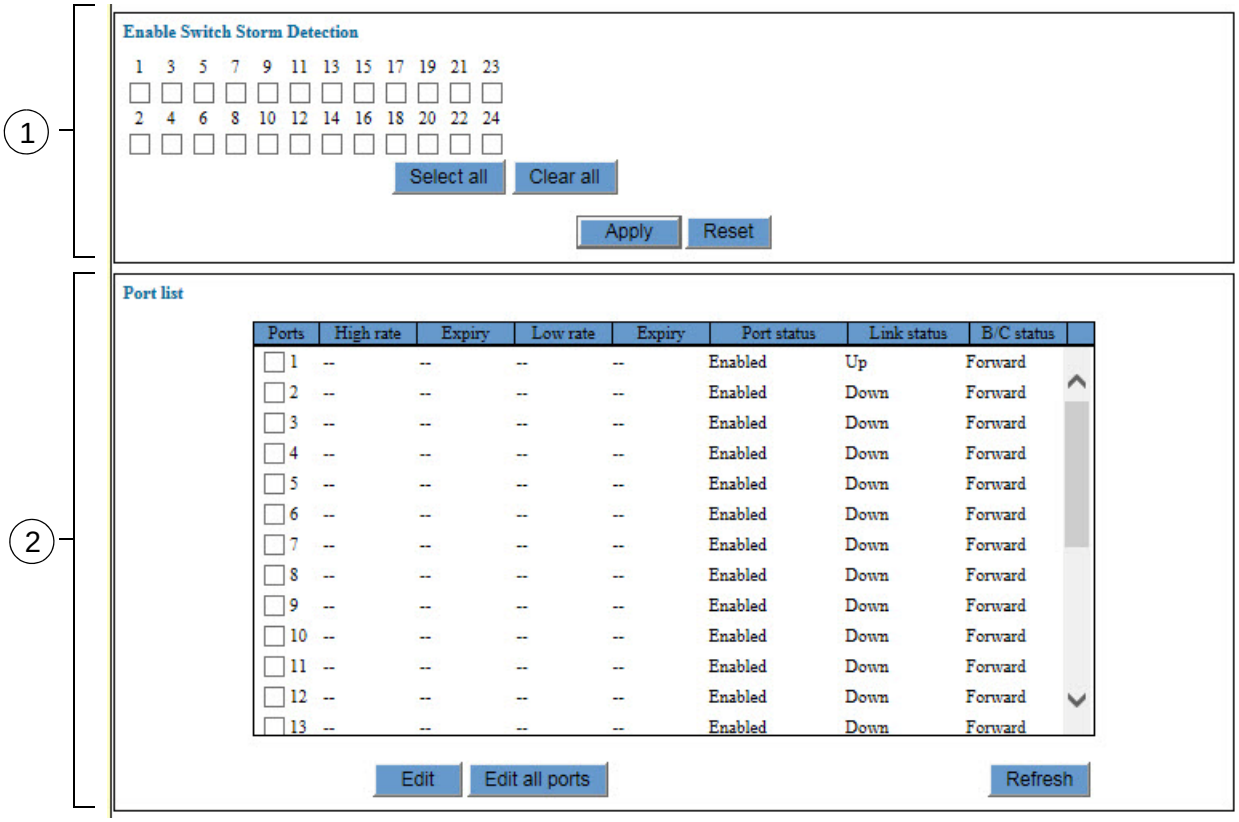

Figure 103. Switch Settings - Switch Storm Detection Window

The sections in the window are described in Table 109 on page 417.

Table 109. Switch Settings - Switch Storm Detection Window

Section	Description
1	Use this section to enable or disable the feature on the individual ports. The feature is enabled on a port when a dialog box has a check mark and disabled when it is empty. For instructions, refer to “Enabling or Disabling Switch Storm Detection” on page 421.
2	Use the table in this section to view the status of the feature on the ports or to configure the port settings. The columns in the table are defined in Table 110. For instructions on how to configure the port parameters, refer to “Configuring Switch Storm Detection” on page 422.

The Port List table in the Switch Settings - Switch Storm Detection window displays the current states of the feature on the ports. The columns are described in Table 110.

Table 110. Switch Settings - Switch Storm Detection Window

Column	Description
Port	Displays the port number.
High Rate	Displays whether the high rate threshold has been crossed on the port. The possible states are listed here: -- - The feature is not enabled on the port. Normal - The feature is enabled on the port. Blocking - The high rate threshold has been crossed and the port is blocking either all of the traffic or only the broadcast frames, depending on the action setting. Detected - The high rate threshold has been crossed, but because the action on the port is None, the switch is taking no action other than entering a message in the event log.

Table 110. Switch Settings - Switch Storm Detection Window (Continued)

Column	Description
Expiry	Displays the amount of time remaining before the action for the high rate threshold expires. Please note the following information: If the threshold action is PortDisable or LinkDown, the Expiry states the remaining time before the port begins forwarding traffic again. If the action is BC Discard, the Expiry states the remaining time before the port begins forwarding broadcast traffic again. If the port action is None, the Expiry value is not applicable and can be ignored. If there is no expiration time and the High Rate column is Blocking, the port is configured to remain in the action state until it is manually overridden. To manually override the action of a port in this state, you have to enable the port by displaying the Port Settings window for the port, as explained in “Configuring Port Parameters” on page 118, and clicking the Apply button.
Low Rate	Displays whether the low rate threshold has been crossed on the port. The possible states are listed here: -- - The feature is not enabled on the port. Normal - The feature is enabled on the port. Blocking - The low rate threshold has been crossed and the port is blocking either all of the traffic or only the broadcast frames, depending on the action setting.

Table 110. Switch Settings - Switch Storm Detection Window (Continued)

Column	Description
Low Rate (Continued)	Detected - The low rate threshold has been crossed, but because the action on the port is None, the switch is taking no action other than entering a message in the event log.
Expiry	Displays the amount of time remaining before the action for the low rate threshold expires. The meaning of the timer with the possible threshold actions is the same as for the Expiry timer for the high rate threshold. Refer to the Expiry timer for the high rate threshold earlier in this table for further information.
Port Status	Displays the current state of the port. The possible states are listed here: Enabled - The port is enabled. (A port with a threshold action of PortDisable, BC Discard, or None will still have a Port State of Enabled even if a threshold is crossed and the corresponding action is activated.) Disabled(Act) - The switch disabled the port because the low or high threshold was crossed and the threshold action is LinkDown. Disabled(User) - The port was manually disabled. For instructions on how to manually enable ports, refer to “Configuring Port Parameters” on page 118.
Link Status	Displays the link state. The possible states are listed here: Up - The port has established a link to a network device. Down - The port has not established a link to a network device or was manually disabled.

Table 110. Switch Settings - Switch Storm Detection Window (Continued)

Column	Description
Link Status (Continued)	Down(Act) - The switch disabled the link on the port because the low or high threshold was crossed and LinkDown is the defined action.
B/C Status	Displays the status of the forwarding of broadcast packets on the port. The possible states are listed here: Forward - The port may forward broadcast frames. Discard - The port is discarding broadcast packets because a packet rate threshold was crossed and the threshold action is BC Discard.

Enabling or Disabling Switch Storm Detection

This section explains how to enable or disable switch storm detection on the individual ports on the switch.

> **Note**
> Allied Telesis recommends configuring the port settings before enabling the feature. For instructions, refer to "Configuring Switch Storm Detection" on page 422.

To enable or disable switch storm detection on the ports, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Switch Storm Detection option from the Switch Settings menu.

   The Switch Settings - Switch Storm Detection window is shown in Figure 103 on page 416.
3. In the top section of the window, click the dialog boxes of the ports where you want to enable or disable the feature. The feature is enabled on a port when a dialog box has a check mark and disabled when a dialog box is empty.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring Switch Storm Detection

To configure the parameter settings of switch storm detection on the ports, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Switch Storm Detection option from the Switch Settings menu.

   The Switch Settings - Switch Storm Detection window is shown in Figure 103 on page 416.
3. In the bottom section of the window, click the dialog box of the port you want to configure. You may configure more than one port at a time.
4. Click the Edit button. To configure all of the ports on the switch, click the Edit All Ports button.

   The switch displays the Switch Storm Detection - Port Settings window, shown in Figure 104.

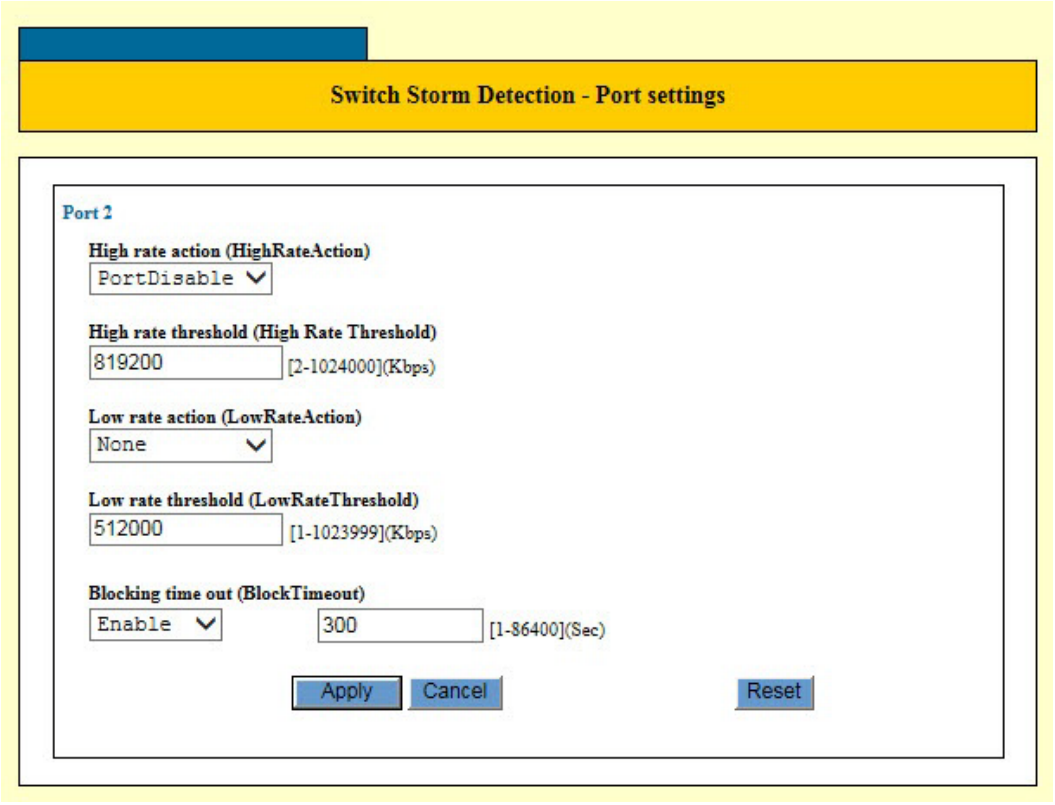

Figure 104. Switch Storm Detection - Port Settings Window

5. Configure the parameters, as needed. The parameters are described in Table 111.

Table 111. Switch Storm Detection - Port Settings Window

Parameter	Description
High Rate Action (HighRateAction)	Specifies the action of a port if the high packet rate threshold is crossed. The options are listed here: PortDisable: Disables the port, but not the link. The port stops forwarding traffic, but the link to the remote network device remains up. This is the default setting. LinkDown: Disables the port and link. The port stops forwarding traffic and drops the link to the remote network device. BC Discard: Discards broadcast frames. None: Performs no action, but enters a message in the event log.
High Rate Threshold (HighRateThreshold)	Specifies the high packet rate threshold, in kilobits per second. The range is 2 to 1024000 Kbps. The default is 819200 Kbps.
Low Rate Action (LowRateAction)	Specifies the action of a port if the low packet rate threshold is crossed. The actions are the same as for the high rate action.
Low Rate Threshold (LowRateThreshold)	Specifies the low packet rate threshold, in kilobits per second. The range is 1 to 1023999 Kbps. The default is 512000 Kbps.

Table 111. Switch Storm Detection - Port Settings Window (Continued)

Parameter	Description
Blocking Time Out (BlockTimeout)	Specifies the status of the port after the switch detects threshold violation and activates the designated action. The possible options are listed here: Enable - Allows the port to return to its prior state (e.g., forwarding traffic) after the specified period of time of the threshold action. If you select this option, use the field next to the pull-down menu to specify the time duration of the action (e.g., how long the port is disabled). The range is 1 to 86400 seconds. The default is 300 seconds (5 minutes). Disable - Maintains the action of the port until it is manually overridden. The action remains active (e.g., the port remains disabled) until you manually override it by displaying the Port Settings window of the port, as explained in “Configuring Port Parameters” on page 118, and clicking the Apply button.

6. After configuring the settings in the window, click the Apply button to activate your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Displaying Statistics for Switch Storm Detection

To display statistics for switch storm detection, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the Switch Storm Database option from the Device Monitoring menu.

   An example of the Device Monitoring - Switch Storm Database window is shown in Figure 105.

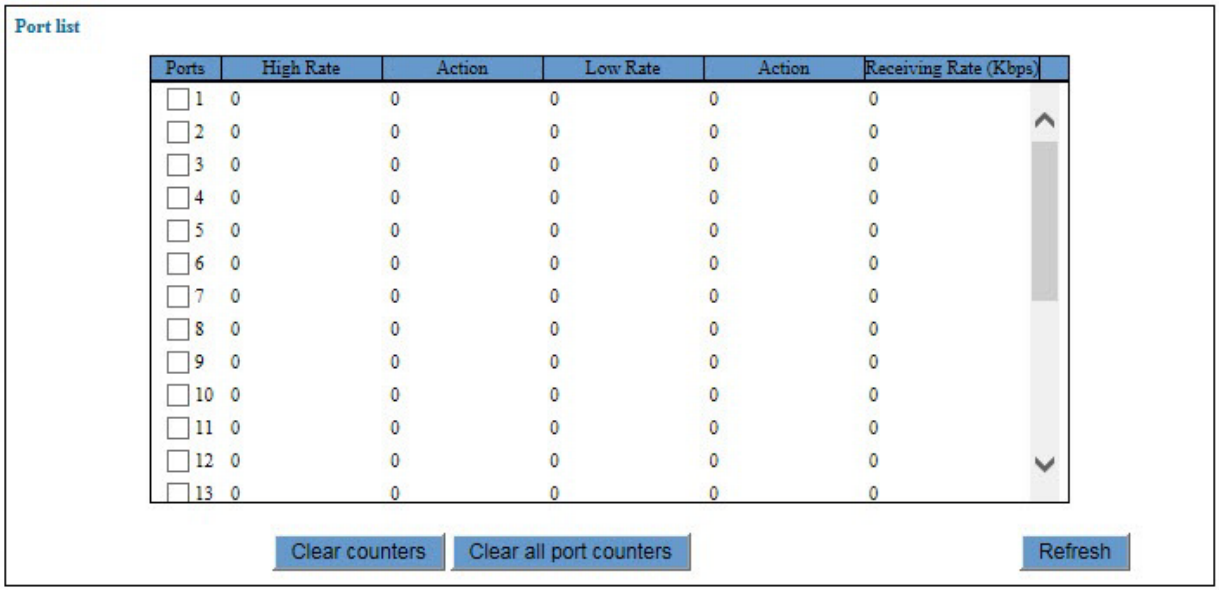

Figure 105. Device Monitoring - Switch Storm Database Window

The columns in the table are defined in Table 112.

Table 112. Device Monitoring - Switch Storm Database Window

Column	Description
Ports	Displays a port number.
High Rate	Displays the number of times the port has detected a high rate threshold violation.
Action	Displays the number of times a port performed the PortDisable, LinkDown, or BC Discard action after the high threshold was crossed. This counter does not count the None action.

Table 112. Device Monitoring - Switch Storm Database Window

Column	Description
Low Rate	Displays the number of times the port has detected a low packet rate threshold violation.
Action	Displays the number of times a port performed the PortDisable, LinkDown, or BC Discard action after the low rate threshold was crossed. This counter does not count the None action.
Receiving Rate (Kbps)	Displays the actual ingress packet rate on a port.

3. To clear port statistics, do one of the following:
   - ❒ To clear the statistics for individual ports, click the dialog boxes of the ports and click Clear Counters button.
   - ❒ To clear the port statistics for all of the ports, click the Clear All Port Counters button.
4. To update the statistics, click the Refresh button.

Chapter 35

Ethernet Protection Switching Ring

This chapter contains instructions on how to configure the Ethernet Protection Switching Ring (EPSR) feature. This chapter contains the following procedures:

Displaying the EPSR Window

To display the EPSR window, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the EPSR option from the Switch Settings menu.

   The Switch Settings - EPSR window is shown in Figure 106.

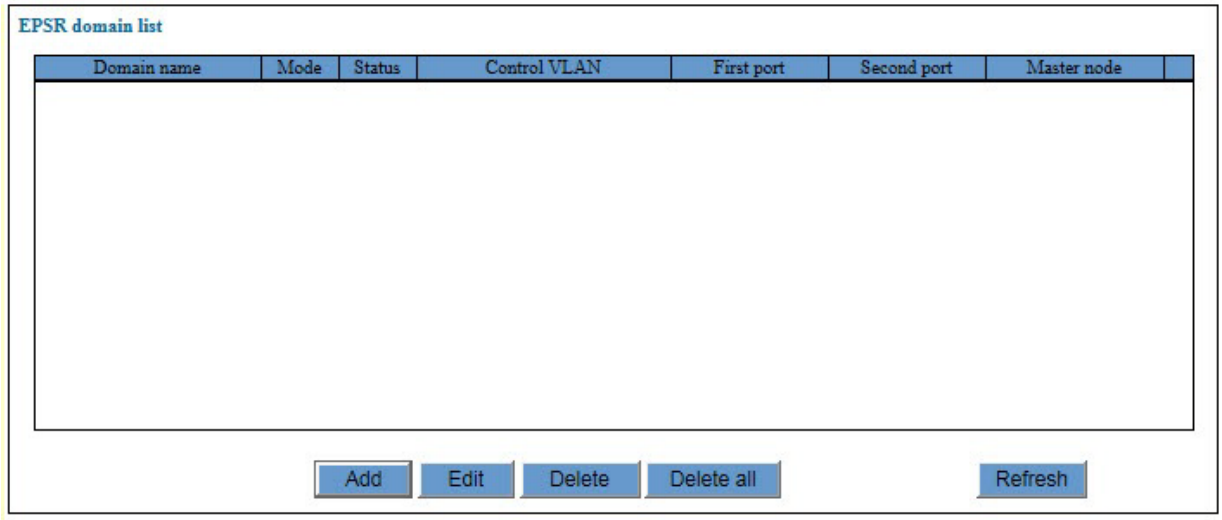

Figure 106. Switch Settings - EPSR Window

The columns in the window are described in Table 113.

Table 113. Switch Settings - EPSR Window

Column	Description
Domain Name	Displays the name of the domain.
Mode	Displays the mode of the domain. The mode can be Aware or Transit.
Status	Displays the domain status. The status can be Enabled or Disabled.
Control VLAN	Displays the name of the control VLAN.
First Port	Displays the first port of the ring. The column displays a port trunk name if the first port is a port trunk.

Table 113. Switch Settings - EPSR Window (Continued)

Column	Description
Second Port	Displays the second port of the ring. The column displays a port trunk name if the second port is a port trunk.
Master Node	Displays the MAC address of the master node of the ring.

Adding an EPSR Domain

To add an EPSR domain, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the EPSR option from the Switch Settings menu.

   The EPSR window is shown in Figure 106 on page 428.
3. Click the Add button.

   The EPSR Domain - Add window is shown in Figure 107.

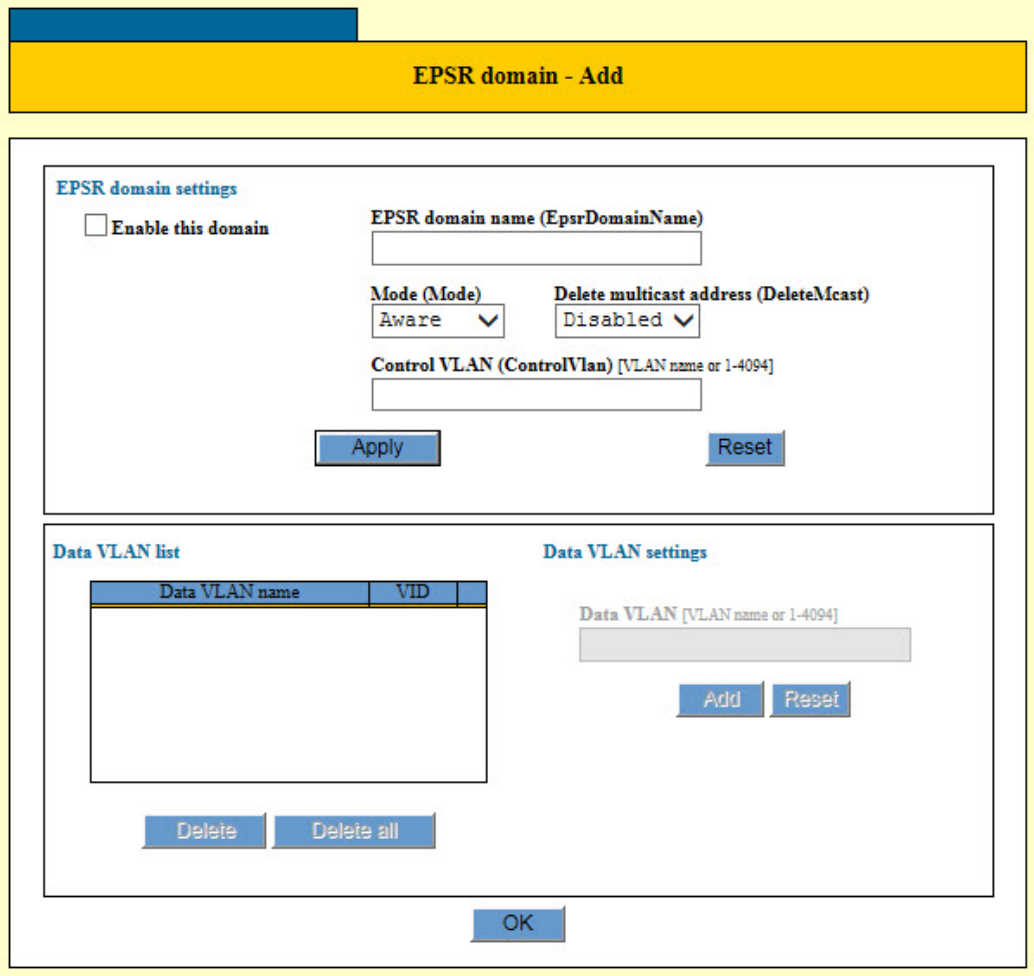

Figure 107. EPSR Domain - Add Window

4. Configure the parameters in the window, as needed. The parameters are defined in Table 114 on page 431.

Table 114. EPSR Domain Settings in the EPSR Domain - Add Window

Parameter	Description
Enable This Domain	Use this parameter to enable or disable the domain. The domain is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
EPSR Domain Name (EpsrDomainName)	Use this parameter to specify the EPSR domain name. The name can be up to fifteen characters. Spaces are not allowed.
Mode	Use this parameter to specify the EPSR mode of the domain. The selections are Aware, the default setting, and Transit.
Delete Multicast Address (DeleteMcast)	Use this parameter to control the deletion of multicast addresses from the MAC address table. The options are listed here: Enabled - The switch deletes dynamic IPv4 and IPv6 multicast addresses learned by IGMP and MLD snooping from the MAC address table. The switch does not delete static multicast addresses. Disabled - The switch does not delete IPv4 or IPv6 multicast addresses.
Control VLAN (ControlVlan)	Use this parameter to specify the name or VID of the control VLAN. You may specify only one VLAN.

5. Click the Apply button.

6. Click the Data VLAN field and enter the name or VID of the data VLAN of the EPSR instance.

   You may enter only one VLAN at a time. If the Data VLAN field is greyed-out, it means you have not completed adding the EPSR domain to the switch. Refer to Table 114 to complete the domain.

7. Click the Add button.

   The VLAN is added to the Data VLAN List table.

8. Repeat steps 4 and 5 to add more data VLANs to the domain, if desired.

9. Click the OK button to implement your changes on the switch.
10. To permanently save your changes in the configuration, click the Save button above the main menu.

Modifying an EPSR Domain

To modify an EPSR domain, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the EPSR option from the Switch Settings menu.

   The EPSR window is shown in Figure 106 on page 428.
3. Click the dialog box of the domain you want to modify and click the Edit button.

   The EPSR Domain - Edit window is displayed.
4. Configure the parameters in the window, as needed. The parameters are defined in Table 114 on page 431.
5. Click the Apply button.
6. To add data VLANs to the domain, perform the following steps:
   a. Click the Data VLAN field and enter the name or VID of the data VLAN of the EPSR instance.

      You may enter only one VLAN at a time. If the Data VLAN field is greyed-out, it means you have not completed adding the EPSR domain to the switch. Refer to Table 114 to complete the domain.
   b. Click the Add button.

      The VLAN is added to the Data VLAN List table.
   c. Repeat steps a and b to add more data VLANs, if desired.
7. To delete data VLANs from the domain, perform the following steps:
   a. In the Data VLAN List section of the window, click the dialog circle of the data VLAN you want to delete.
   b. Click the Delete button. To delete all of the data VLANs of the domain, click the Delete All button.
8. Click the OK button to implement your changes on the switch.
9. To permanently save your changes in the configuration, click the Save button above the main menu.

Deleting an EPSR Domain

To delete an EPSR domain, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the EPSR option from the Switch Settings menu.

   The EPSR window is shown in Figure 106 on page 428.
3. Click the dialog circle of the EPSR domain to be deleted. You may select only one domain.
4. Click the Delete button. To delete all of the EPSR domains on the switch, Click the Delete All button.

   The switch displays a confirmation prompt.
5. click OK to delete the domain or Cancel to retain the domains.

Displaying EPSR Status Information

To display the EPSR status information, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.
2. Select the EPSR option from the Device Monitoring menu.

   The Device Monitoring - EPSR window is shown in Figure 108.

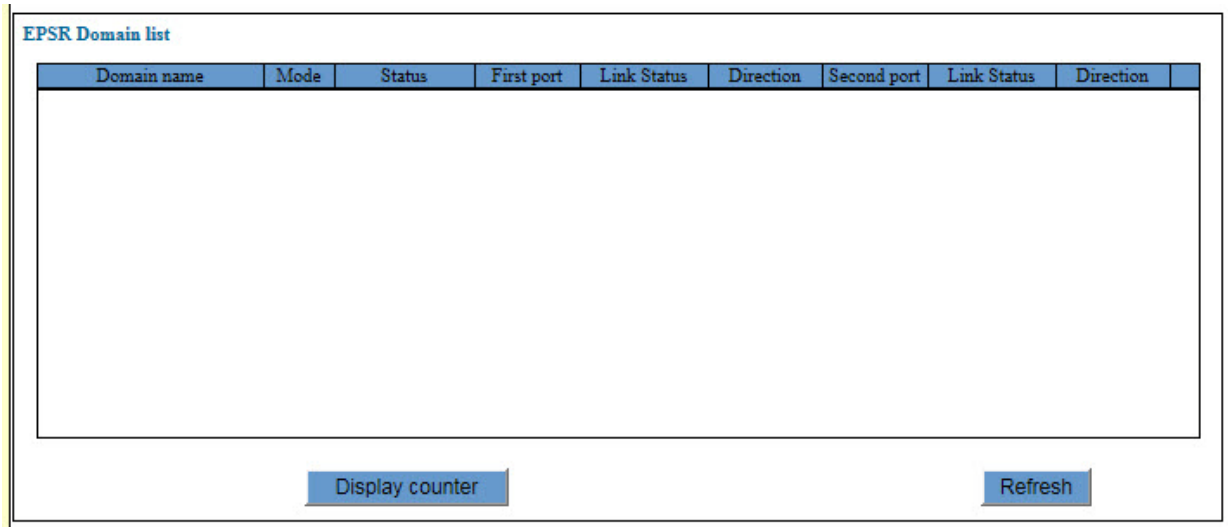

Figure 108. Device Monitoring - EPSR Window

The columns in the window are described in Table 115.

Table 115. Device Monitoring - EPSR Window

Column	Description
Domain Name	Displays the name of the domain.
Mode	Displays the mode of the domain. The mode can be Aware or Transit.
Status	Displays the domain status. The status can be Enabled or Disabled.
First Port	Displays the first port of the ring. The column displays a port trunk name if the first port is a port trunk.

Table 115. Device Monitoring - EPSR Window (Continued)

Column	Description
Link Status	Displays the status of the first port of the ring. The port status in the Aware mode can be Up, Down, and Unknown. The port status in the Transmit mode can be Forwarding, Down, Unknown, and Blocking. An Unknown status can also indicate that the domain is disabled.
Direction	Displays whether the first port is upstream or downstream of the master node of the ring.
Second Port	Displays the second port of the ring. The column displays a port trunk name if the second port is a port trunk.
Link Status	Displays the status of second first port of the ring. The port status in the Aware mode can be Up, Down, and Unknown. The port status in the Transmit mode can be Forwarding, Down, Unknown, and Blocking. An Unknown status can also indicate that the domain is disabled.
Direction	Displays whether the second port is upstream or downstream of the master node of the ring.

3. To display EPSR packet counters, click the Display Counter button.

Chapter 36

Access Filters

This chapter contains instructions on how to use access filters to increase the management security of the switch. This chapter contains the following procedures:

Introduction

If you are concerned about unauthorized individuals learning the username and password of the manager account on the switch, you might consider using access filters to add another level of protection to the unit. The filters allow you to define the workstations that you or other network managers can use to remotely manage the switch. Anyone who tries to access a management interface on the unit from an unapproved workstations is denied access. The workstations are identified by their IP addresses. For instance, if you are the only network manager who will be managing the switch, you might configure the access filters so that only your workstation can be used to remotely manage the device.

Each management interface has its own filter. The different filters are listed in Table 116.

Table 116. Access Filters

Management Interface Filter	Description
SNMP	Use this filter to specify the approved workstations for remote SNMP management of the switch.
FTP	Use this filter to specify the approved workstations for uploading or downloading files to the file system in the switch with FTP or TFTP.
Telnet	Use this filter to specify the approved workstations for remote Telnet management of the switch.
HTTP	Use this filter to specify the approved workstations for remote web browser management of the switch.
ICMP	Use this filter to specify the approved workstations from which you can use the PING utility to identify the switch.

There are two approaches you can take with the filters of a management tool. One approach is to create filters that identify the approved workstations. This is the approach you are most likely to take. The other approach is to create filters that identify unapproved workstations. You are not likely to use this approach because it requires knowing the IP addresses of all of the possible unauthorized workstations, which you are not likely to know.

Each management interface has a main filter and individual filter entries. The main filter dictates whether the switch permits or denies access to the switch using the interface. For example, if the Telnet main filter is set to deny, than the switch does not allow any workstation to access the unit using the Telnet protocol. Each management interface also has filter entries, which act as the exceptions to the main filter. If the Telnet main filter is set to deny to prevent anyone from using Telnet, you could add filter entries that would override the main filter and permit specific workstations to use Telnet to manage the switch.

Displaying the Access Filter Window

To display the access filter window, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Access Filter option from the System Settings menu.

   The System Settings - Access Filter window is shown in Figure 109.

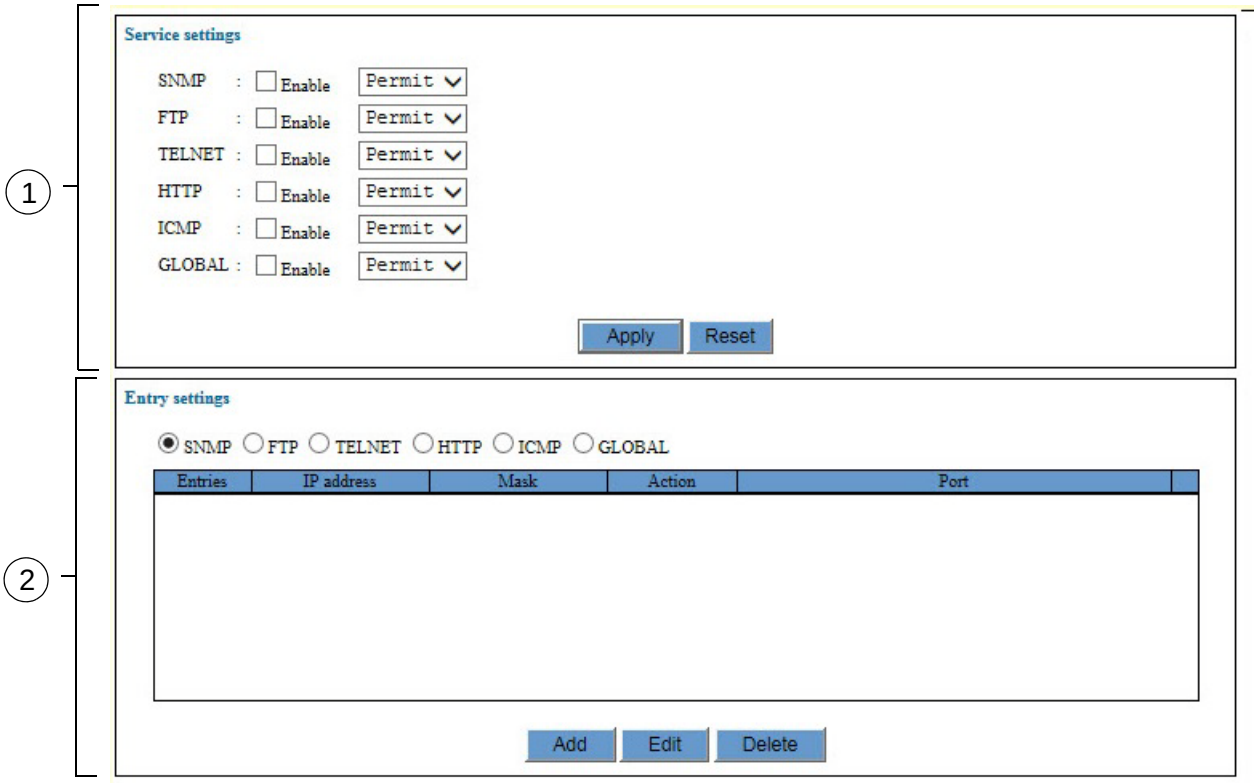

Figure 109. System Settings - Access Filter Window

The sections in the window are defined in Table 117.

Table 117. System Settings - Access Filter Window

Section	Description
1	Use this section of the window to enable or disable the main filters and to specify whether the filters are to permit or deny management access to the switch. For instructions, refer to “Enabling or Disabling Access Filters” on page 442.

Table 117. System Settings - Access Filter Window (Continued)

Section	Description
2	Use this section to add or delete filter entries. For instructions, refer to “Adding Filter Entries” on page 443 or “Deleting Filter Entries” on page 446

Enabling or Disabling Access Filters

This procedure explains how to enable or disable the access filters for the management interfaces. Before enabling a filter, you should add the filter entries first, as explained in “Adding Filter Entries” on page 443.

To enable or disable the main filters for the management interfaces, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Access Filter option from the System Settings menu.

   The System Settings - Access Filter window is shown in Figure 109 on page 440.
3. In the Service Settings section of the window, click the dialog boxes of the main filters to enable or disable them. A main filter is enabled when its dialog box has a check mark and disabled when the dialog box is empty. The default setting for a filter is disabled.
4. If you enabled a filter, use its pull-down menu to specify whether workstations are permitted or denied use of the management interface. The two options are listed here:
   - Permit - All workstations are allowed to use the management interface except for those workstations that are expressly denied use of it. If you select this option, the filter entries need to specify the workstations that are to be denied use of the management access method.
   - Deny - All workstations are denied use of the management interface except for those workstations that are expressly permitted to use it. If you select this option, the filter entries need to specify the workstations that are to be permitted to use the management interface. This is the selection you are most likely to use.
5. Click the Apply button to implement your changes on the switch.

   Note
   If you enabled the HTTP filter and the switch stops responding to your web browser management session, it probably means that you did not configure the HTTP filter to permit your management workstation to access the switch.
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Adding Filter Entries

To add a new filter entry, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Access Filter option from the System Settings menu.

   The System Settings - Access Filter window is shown in Figure 109 on page 440.
3. In the Entry Setting section of the window, click the dialog circle of the filter for the new entry. You may select only one filter. The Global filter applies to all of the management functions.
4. Click the Add button.

   The Add Access Filter window is shown in Figure 110.

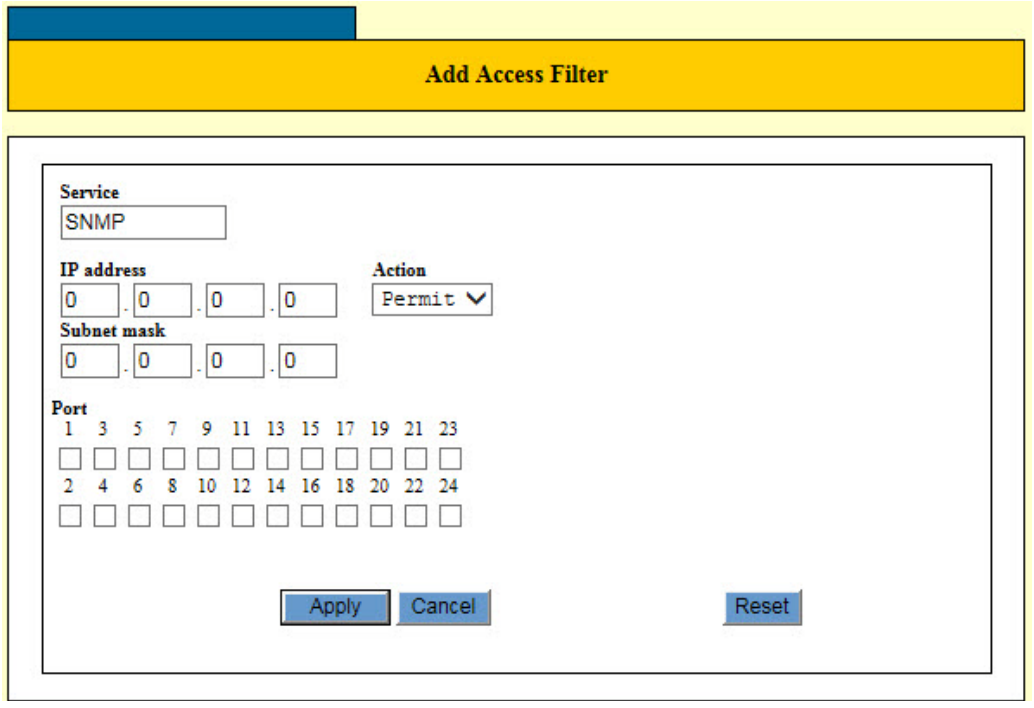

Figure 110. Add Access Filter Window

5. Configure the parameters, as needed.

   The filters are defined in Table 118 on page 444.

Table 118. Add Access Filter Window

Parameter	Description
Service	Use this parameter to view the filter you are currently managing. This parameter cannot be changed. To manage a different filter, close this window and repeat step 3.
IP Address	Use this parameter to specify the IP address of a computer to be allowed or denied access to the corresponding management interface on the switch. Here are the IP address guidelines: You may enter only one address. You may enter the address of a specific computer (e.g., 149.132.45.76) or a subnet (e.g., 149.132.45.0).
Mask	Use this parameter to specify the parts of the IP address for filtering. The mask is a decimal number that represents the number of bits, from left to right, that represent the filtering part of the IP address. Here are the mask guidelines: You may specify only one mask. As an example, the mask for the IP address of a specific workstation, such as 149.132.45.76, would be 255.255.255.255. As another example, the mask for a subnet such as 149.132.45.0 would be 255.255.255.0

Table 118. Add Access Filter Window (Continued)

Parameter	Description
Action	Use this parameter to set the action of the filter entry. This setting has to be opposite to the action of the main filter, which is set in the Service Settings portion of the System Settings - Access Filter window. Here is an example. Let's assume that you are configuring the Telnet filter and you set the main Telnet action to Deny. At that setting, the filter denies Telnet access to all workstations, but permits access to those workstations specified with filter entries. Consequently, you would create filter entries with the Permit action for those workstations to be allowed to use Telnet to manage the switch. Here is another example. Let's assume that you are configuring the SNMP filter and you set the main SNMP action to Permit. At that setting, the filter permits SNMP access to all workstations, but denies access to those workstations specified with filter entries. Consequently, you would create filter entries with an action of Deny for those workstations to be denied use of SNMP to manage the switch.
Port	Use this section to designate the port of the workstation for the filter entry. You may assign a filter entry to more than one port. A port is selected when its dialog box has a check mark and not selected when its dialog box is empty.

6. Click the Apply button to implement your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting Filter Entries

To delete filter entries, perform the following procedure:

1. Expand the System Settings menu in the main menu.
2. Select the Access Filter option from the System Settings menu.

   The System Settings - Access Filter window is shown in Figure 109 on page 440.
3. In the Entry Setting section of the window, click the dialog circle of the filter with the entries you want to delete. You may select only one filter.

   The switch displays the entries of the selected filter.
4. Click the dialog circle of the entry you want to delete. You may delete only one entry at a time.
5. Click the Delete button.

   The switch displays a confirmation prompt.
6. Click OK to delete the filter entry or Cancel to retain it.
7. Click the Apply button to implement your changes on the switch.
8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 37

MAC Address-based Port Security Overview

The sections in this chapter include:

Overview

You may use this port security feature to specify the network devices that are authorized to forward traffic through the switch and gain access to your network. This feature is similar to the MAC address authentication method of the port authentication feature, described in Chapter 40, “Port Authentication Overview” on page 471. Both features use the MAC addresses of the network devices to determine which network devices are authorized to access your network through the switch. The difference is that this feature does not require a RADIUS server. Rather, the switch uses its MAC address table to determine which packets to forward or discard.

There are four levels of MAC address-based port security:

- Automatic
- Secured
- Dynamic Limited
- Limited

You may set port security on a per port basis. A port may have only one security level at a time.

Automatic

The Automatic security mode disables port security on a port. This is the default security level for the ports.

Note
The static and dynamic addresses on a port are deleted from the MAC address table when the security level is changed to Automatic from one of the other security levels

Secured

Ports set to this security level immediately stop learning and storing new source MAC addresses in the MAC address table. They forward packets from only those network devices whose addresses they have already learned.

Here are the main points to this security level:

- Ports immediately stop learning and storing new source MAC addresses of network devices in the MAC address table.
- The switch converts the dynamic addresses already learned on the ports into static MAC addresses.
- The ports forward only those packets with source MAC addresses that are static addresses in the MAC address table and discard packets with unknown source addresses.

- Static addresses that are added to the ports before the feature is activated are retained after the feature is enabled.
- You may add or delete static addresses to ports in this security level.
- Because the dynamic addresses are converted into static addresses, they are not timed out of the table even when the corresponding network devices are inactive.

Here is an example, Let's assume you activate this security level on a port that has learned only one dynamic source address and has no static MAC addresses. After you activate the security level, the switch converts the one dynamic address learned by the port into a static entry in the table. The port then forwards the packets from only that one network device and discards all other packets.

Now assume you activate the feature on a port that has learned three dynamic address and already has two static addresses. The switch converts the three dynamic addresses into static addresses, and the port forwards the packets of the five MAC addresses.

Limited

You may use the Limited security level to specify the maximum number of dynamic source MAC addresses the ports can learn. Once ports have learned their maximum number of dynamic MAC addresses, they stop learning new addresses and forward the packets of only those devices they have already learned, Packets from devices with unknown addresses are discarded.

Here are the main points to this security level:

- When you activate the Limited security mode on a port, the switch deletes all of the dynamic MAC addresses already learned by the port from the MAC address table. The switch then allows the port to begin to learn new addresses, up to the defined maximum.
- After a port has learned its maximum number of addresses, it discards packets with unknown source MAC addresses.
- Static addresses that are added to the ports before the feature is activated are retained after the feature is enabled and are not counted against the maximum number of dynamic addresses.
- The dynamic addresses the ports learn are added as static address in the MAC address table.
- Because the dynamic addresses are added as static addresses in the table, they are not timed out even when the corresponding network devices are inactive.
- You may add or delete static addresses to ports in this security level. Static addresses that you manually add are not counted against the maximum number of addresses the ports can learn.

Here is an example. Let's assume you activate the security level on a port and specify ten addresses as the maximum number of addresses the port may learn. After you activate the feature, the switch deletes all of the dynamic addresses from the MAC address table the port has already learned. As the port begins to learn new addresses, they are added as static entries in the table. After learning ten addresses, the port forwards packets from only those network devices and discards packets with unknown addresses.

Dynamic Limited

The Dynamic Limited security level is very similar to Limited security mode. Just like a port set to the Limited security level, a port set to the Dynamic Limited security level can learn up to a defined number of MAC addresses. After learning its maximum number of MAC addresses, a port forwards packets from only those network devices and discards packets with unknown addresses.

The difference between the Limited and Dynamic Limit modes has to do with how they handle the dynamic MAC addresses. With the Limited security level, dynamic addresses are entered as static addresses in the table and thus are never deleted from the table even when network devices are inactive. In contrast, the source MAC addresses learned by a port in this security level are entered as dynamic addresses in the table and, consequently, are deleted when devices are inactive.

As an example, let's assume you activate this security level on a port and specify a maximum of fifteen dynamic MAC addresses. When you activate the feature, the switch deletes all of the dynamic MAC addresses the port has already learned and stored in the table. The new addresses the port learns are entered as dynamic entries in the table. After learning fifteen dynamic addresses, the port forwards only packets with source MAC addresses it has already learned and discards packets with unknown addresses. If a network device becomes inactive and its MAC address is deleted from the MAC address table, the port may learn a new dynamic address.

As with the Limited security level, any static addresses that might have been added to a port are retained after you activate this feature. Also, static addresses are not countered against the maximum number of dynamic addresses a port may learn, and you may continue to add or delete static addresses to a port after activating the security level on the ports.

Invalid Frames and Intrusion Actions

When a port receives an invalid frame, it performs an intrusion action, which defines the port's response to the packet. But before defining the intrusion actions, it helps to understand what constitutes an invalid frame. This differs for each security level, as explained here:

- Limited and Dynamic Limited security levels - An invalid frame for this security level is an ingress frame with a source MAC address not already learned by a port after reaching its maximum number of dynamic MAC addresses, or that was not assigned to the port as a static address.
- Secured security level - An invalid frame for this security level is an ingress frame with a source MAC address that the port has not already learned or that was not assigned as a static address.

An intrusion action defines what a port does when it receives invalid frames. The intrusion actions are defined in Table 119, "Intrusion Actions for MAC Address-based Port Security" on page 451.

Table 119. Intrusion Actions for MAC Address-based Port Security

Intrusion Action	Description
Discard	Discard invalid frames.
Disable	Disables the port. The link on the port remains up but the port stops forwarding traffic.
Trap	Discard invalid frames and send SNMP traps. (SNMP must be enabled on the switch.)
Log	Discard invalid frames and enter messages in the event log.

Guidelines

Here are the guidelines to MAC address-based port security:

- Packets are filtered on the ingress ports.
- You cannot use MAC address-based port security and port authentication on the same port. To configure a port as an Authenticator or Supplicant for port authentication, you have to set its MAC address security level to Automatic, which is the default setting.
- This port security is not supported on the combo ports.
- A port can have only one security level at a time.
- The static and dynamic addresses on a port are deleted from the MAC address table when the security level is changed to Automatic from one of the other security levels

Chapter 38

MAC Address-based Port Security

This chapter explains how to configure the MAC address-based security feature on the ports on the switch. For background information, refer to Chapter 37, “MAC Address-based Port Security Overview” on page 447. The sections in the chapter are listed here:

Displaying the MAC Address-based Port Security Window

To display the MAC Address-based Port Security window, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Security option from the Security Settings menu.

   The Security Settings - Port Security window is shown in Figure 111.

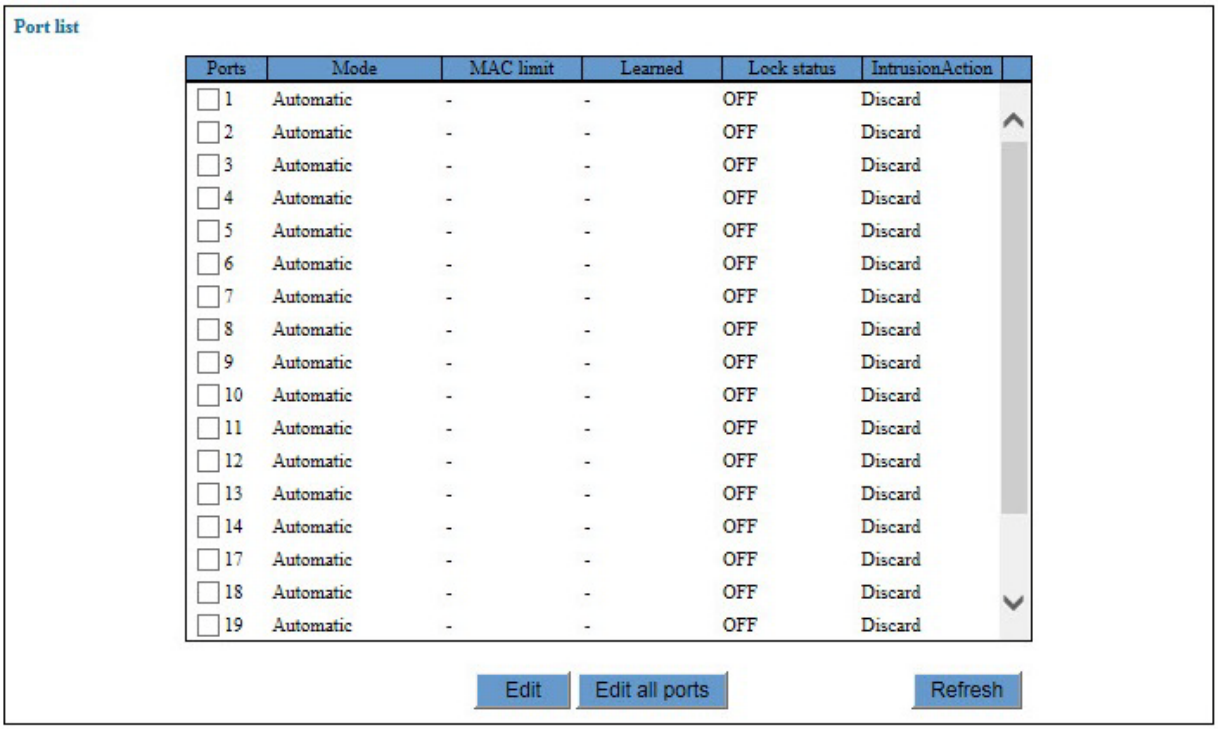

Figure 111. Security Settings - Port Security Window

The table in the window displays the current security settings of the ports. The columns are described in Table 120.

Table 120. Security Settings - Port Security Window

Column	Description
Port	Displays the port number.
Mode	Displays the security mode. The mode can be Automatic, Limited, Dynamic Limited, or Secured. The modes are described in “Overview” on page 448.

Table 120. Security Settings - Port Security Window (Continued)

Column	Description
MAC Limit	Displays the maximum number of dynamic MAC addresses the port is allowed to learn. This column applies to the Limited and Dynamic Limited security modes. The column does not apply to the Secured mode.
Learned	Displays the number of dynamic MAC addresses the port has already learned. This column applies to the Limited and Dynamic Limited security modes. The column does not apply to the Secured mode.
Lock Status	Displays whether the port can learn new dynamic MAC addresses. The possible states of lock status for a port in the Limited or Dynamic Limited security mode are listed here: Off: The port can learn more dynamic MAC addresses because it has not learned its maximum number of addresses. On: The port cannot learn any more MAC addresses because it has learned its maximum number of addresses. The lock status for ports in the Secured mode is always On because ports in that security mode are not allow to learn new dynamic MAC addresses.
Intrusion Action	Displays the intrusion action of the port. Intrusion actions are described in “Invalid Frames and Intrusion Actions” on page 451.

Changing the Port Security Settings

To configure the security settings of the ports, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Security option from the Security Settings menu.

   The Security Settings - Port Security window is shown in Figure 111 on page 454.
3. Click the dialog box of the port you want to configure. You may configure more than one port at a time.

   Note
   MAC address-based port security is not supported on the combo ports.
4. Click the Edit button. To configure all of the ports on the switch, click the Edit All Ports button.

   The switch displays the Port Security Settings window, shown in Figure 112.

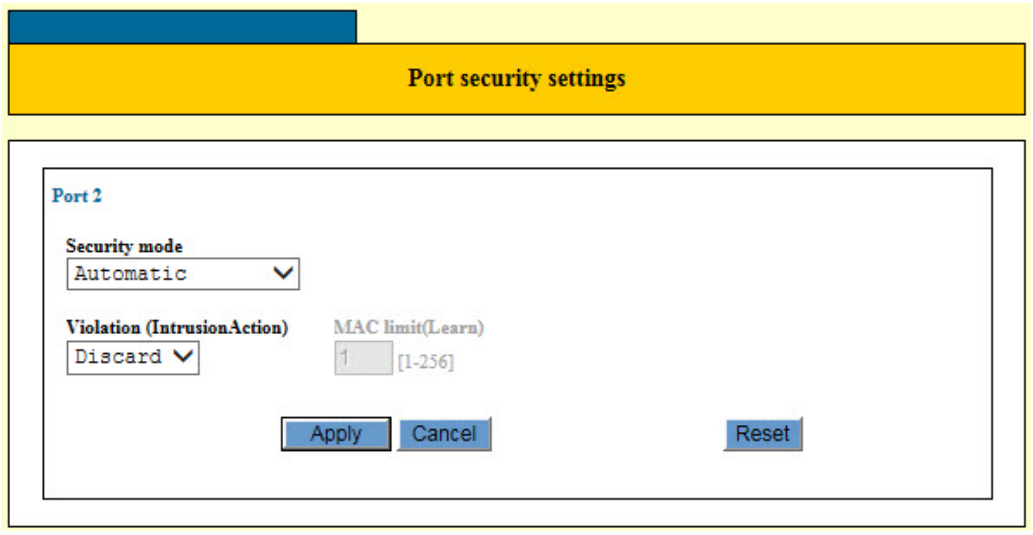

Figure 112. Port Security Settings Window

5. Configure the parameters, as needed. Refer to Table 121 on page 457.

Table 121. Port Security Settings Window

Parameter	Description
Security Mode	Use this parameter to set the security mode of a port. The options are listed here: Automatic (This option disables the security feature on a port.) Secured Dynamic Limited Limited The modes are described in “Overview” on page 448.
Violation (IntrusionAction)	Use this parameter to specify the action of a port if it receives invalid frames. This parameter only applies to ports set to the limit or dynamic limited security mode. The options are listed here: Discard - Discards invalid frames. Disable - Disables the port and sends an SNMP trap. Trap - Discards invalid frames and sends an SNMP trap. Log - Discards invalid frames and enters a message in the event log. The intrusion action for ports set to the secured mode is always discard invalid frames.
MAC Limit (Learn)	Use this parameter to specify the maximum number of dynamic MAC addresses a port can learn. This parameter applies to the Dynamic and Dynamic Limited security modes. The range is 1 to 256 addresses. The default is 1 address.

6. After configuring the parameters in the window, click the Apply button to implement your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 39

RADIUS Client

This chapter contains instructions on how to configure the RADIUS client on the switch. This chapter contains the following procedures:

Introduction

The port authentication feature described in Chapter 41, “Port Authentication” on page 487 uses Remote Authentication Dial In User Services (RADIUS) to authenticate the network users as they log on with their login credentials, such as usernames and passwords, on the authenticator ports on the switch. The RADIUS protocol maintains and validates the logon information the network users provide to access your network, and notifies the switch whether the network users have provided valid or invalid logon information.

The RADIUS protocol has server and client components. The server component stores and validates the log on information the network users provide to access the network. The information can consist of usernames and passwords, along with other information.

The RADIUS client acts as an intermediary between the network users and server. It automatically passes the usernames and passwords to the server on your network for validation when network users log on.

The GS900M Series switches have the client portion of the RADIUS protocol. They do not have a RADIUS server. Consequently, the switches do not validation the logon information the network users provide when they log on. Rather, they act as intermediaries by forwarding the logon credentials from the network users to RADIUS servers on your network for validation.

Guidelines

Here are the guidelines to using the RADIUS client with port authentication:

- You must obtain and install a RADIUS server on a device on your network. Allied Telesis does not provide RADIUS server software.
- The switch must have an IP address. For instructions, refer to “Changing the IP Address Configuration” on page 48.
- The RADIUS server and client need to communicate over the management VLAN of the switch. Consequently, the server must be a member of the management VLAN or have access to it through routers or other Layer 3 devices.
- The RADIUS protocol is used with all three port authentication methods: 802.,1x, MAC address-based, and web browser.
- The maximum length of a username for 802.1x or web browser authentication is 38 alphanumeric characters and spaces. The maximum length of a password is 16 alphanumeric characters.
- There are other authentication protocols, such as TACACS+. However, the switch supports the RADIUS protocol only.
- You may define two RADIUS servers in the client on the switch, for

redundancy. If a server fails or stops responding, the client automatically changes to the second server so that network users can continue to log on the network.

- The client includes RADIUS accounting so that you may monitor user activity on network devices. For background information, refer to "RADIUS Accounting" on page 483.
- This manual does not explain how to configure a RADIUS server. For instructions, refer to the documentation included with the server software.

Note
For more information on RADIUS, refer to the RFC 2865 standard.

Displaying the RADIUS Client Window

To display the RADIUS window, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the RADIUS Server option from the Security Settings menu.

Note
Although the menu option and window contain the word “Server,” the switch does not have a RADIUS server. It has the RADIUS client only.

The Security Settings - RADIUS Server window is shown in Figure 113.

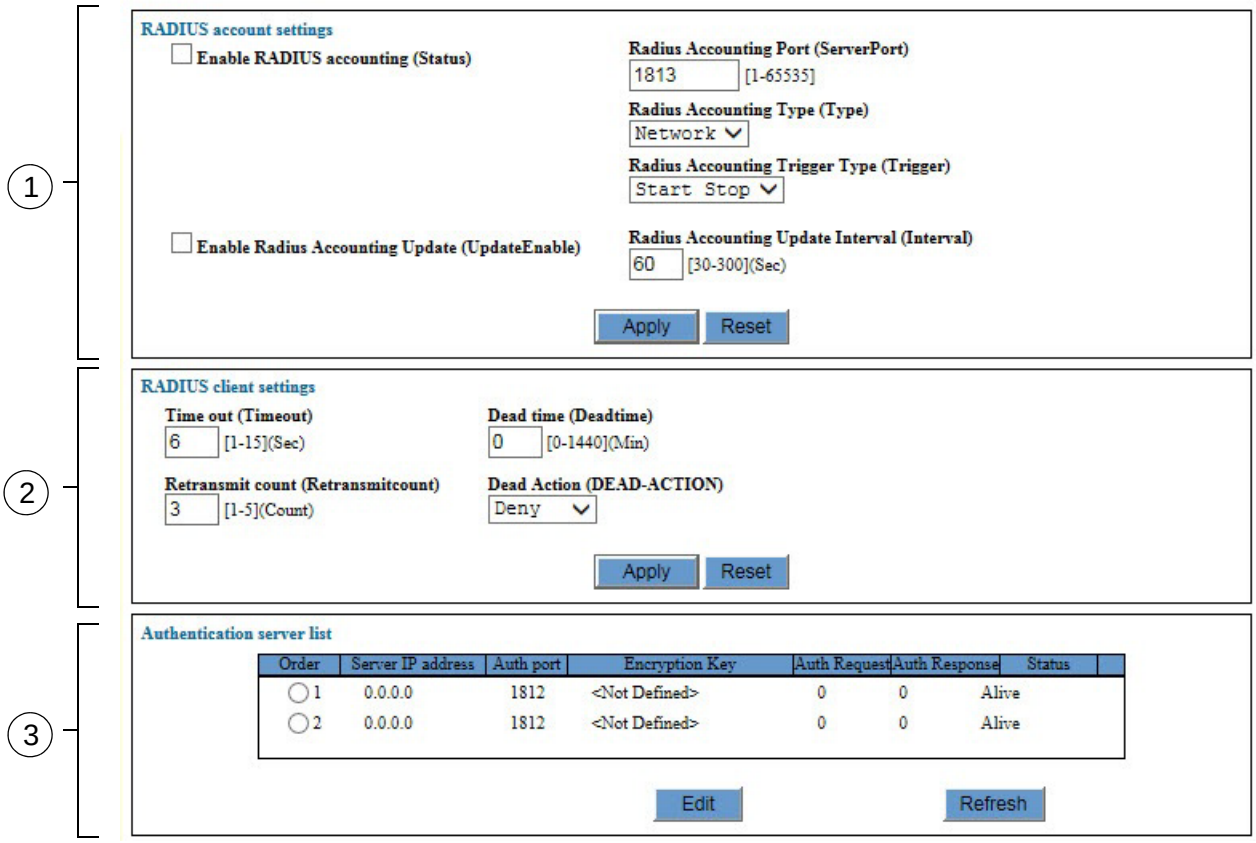

Figure 113. Security Settings - RADIUS Server Window

The sections in the Security Settings - RADIUS Server window are described in Table 122 on page 463.

Table 122. Security Settings - RADIUS Server Window

Section	Description
1	Use the parameters in this section to configure the RADIUS accounting settings. Refer to “Configuring RADIUS Accounting” on page 464.
2	Use the parameters in this section to configure the RADIUS client. Refer to “Configuring the RADIUS Client” on page 466.
3	Use the table in this section to view or modify the settings of the RADIUS server definitions. For instructions, refer to “Configuring RADIUS Server Definitions” on page 468.

Configuring RADIUS Accounting

The switch supports RADIUS accounting for ports operating in the authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. This feature is disabled by default on the switch. For more information, refer to “RADIUS Accounting” on page 483.

To configure RADIUS accounting, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the RADIUS Server option from the Security Settings menu.

   The Security Settings - RADIUS Server window is shown in Figure 113 on page 462.
3. Configure the parameters in the RADIUS Account Settings section of the window. The parameters are described in Table 123.

Table 123. RADIUS Account Settings in the Security Settings - RADIUS Server Window

Parameter	Description
Enable RADIUS account (Status)	Use this parameter to enable or disable RADIUS accounting on the switch. The feature is active when there is a check mark in the dialog box and disabled when the dialog box is empty.
Radius Accounting Port (ServerPort)	Use this parameter to specify the UDP port for RADIUS accounting. The range is 1 to 65535. The default is port 1813.
Radius Accounting Type (Type)	Use this parameter to specify the type of RADIUS accounting. The default is Network. You cannot change this value.
Radius Accounting Trigger Type (Trigger)	Use this parameter to specify the action that causes the switch to send accounting information to the RADIUS server. The possible settings are listed here: Start Stop - Use this option if you want the switch to send accounting information whenever clients log on or off the network. This is the default setting.

Table 123. RADIUS Account Settings in the Security Settings - RADIUS Server Window (Continued)

Parameter	Description
Radius Accounting Trigger Type (Trigger) (Continued)	Stop Only - Use this option if you want the switch to send accounting information only when clients log off.
Enable Radius Accounting Update (UpdateEnable)	Use this parameter to control the transmission of interim accounting updates to the RADIUS server. The feature is active when there is a check mark in the dialog box and disabled when the dialog box is empty.
Radius Accounting Update Interval (Interval)	Use this parameter to specify the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

4. Click the Apply button to implement your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring the RADIUS Client

The parameters in the RADIUS Client Settings portion of the Security Settings - RADIUS Server window are used to control the behavior of the client as it communicates with RADIUS servers. For example, you can use the parameters to change the number of times the client retransmits authentication requests to nonresponsive servers or how long it should ignore a nonresponsive server before attempting to reestablish communications.

To configure the RADIUS client parameters, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the RADIUS Server option from the Security Settings menu.

   The Security Settings - RADIUS Server window is shown in Figure 113 on page 462.
3. Configure the parameters in the RADIUS Client Settings section of the window. The parameters are described in Table 124.

Table 124. RADIUS Client Settings in the Security Settings - RADIUS Server Window

Parameter	Description
Time Out (Timeout)	Use this parameter to specify the maximum amount of time the RADIUS client is to wait for a reply from a RADIUS server to an authentication request. The range is 1 to 15 seconds. The default is 6 seconds.
Dead Time (Deadtime)	Use this parameter to specify the maximum amount of time that the RADIUS client skips over RADIUS servers that are not responding to authentication requests. The range is 0 to 1440 minutes. The default value is 0, which instructs the client not to skip over servers that are not responding.

Table 124. RADIUS Client Settings in the Security Settings - RADIUS Server Window (Continued)

Parameter	Description
Retransmit Count (Retransmitcount)	Use this parameter to specify the maximum number of times the RADIUS client is to retransmit an authentication request to an authentication server that is not responding, before trying the next server in the list. The range is 1 to 5. The default is 3.
Dead-action (DEAD-ACTION)	Use this parameter to specify the action of the RADIUS client to an authentication server that is not responding to authentication requests. The possible settings are listed here: Deny: Use this option to prevent the RADIUS client from attempting any further communications with nonresponsive servers. Permit: Use this option to allow the RADIUS client to resume communicates with RADIUS servers that were previously nonresponsive.

4. After configuring the parameters in the RADIUS Client Settings section of the window, click the Apply button to implement your changes on the switch.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring RADIUS Server Definitions

The instructions in this section explain how to configure the RADIUS server definitions in the RADIUS client on the switch. The client can have two server definitions. To configure a definition, you have to enter information about a RADIUS server on your network, such as its IP address and encryption key. The RADIUS client on the switch uses the information to identify and communicate with the servers.

The definitions are controlled in the bottom section of the Security Settings - RADIUS window, which contains a table with the current settings of the definitions. To define or modify the server definitions, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the RADIUS Server option from the Security Settings menu.

   The Security Settings - RADIUS Settings window is shown in Figure 113 on page 462.
3. Click the dialog circle of one of the two definitions in the table at the bottom section of the window. The switch supports only two definitions. You may configure only one definition at a time.
4. Click the Edit button.

   The switch displays the RADIUS Server Setting window. Refer to Figure 114.

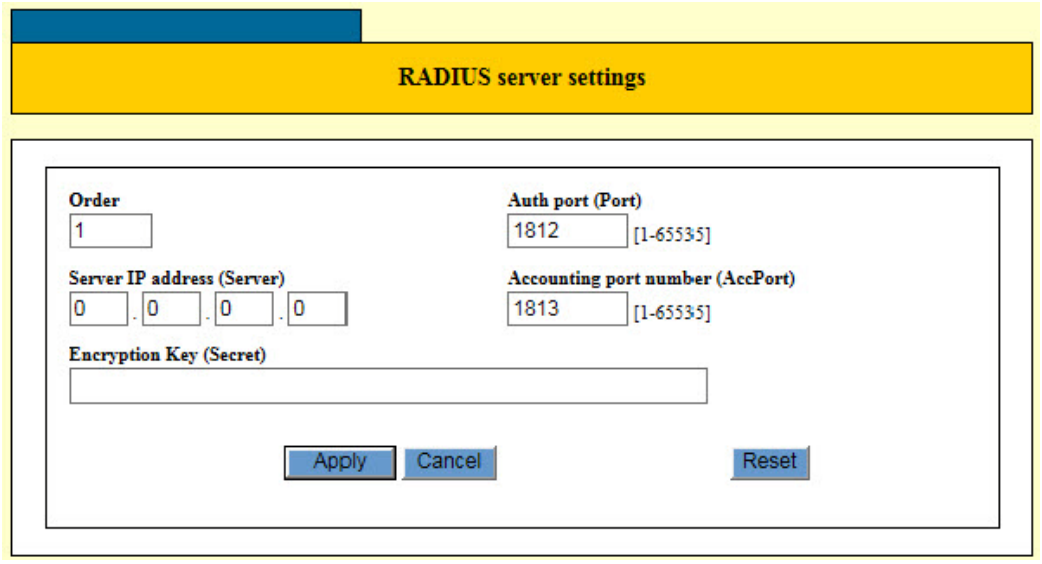

Figure 114. RADIUS Server Settings Window

5. Configure the parameters. The parameters are described in Table 125.

Table 125. RADIUS Server Settings Window

Parameter	Description
Order	Use this parameter to specify the order in which the switch uses the definitions to communicate with the RADIUS servers. The value can be 1 or 2. The parameter cannot be changed.
Auth Port (Port)	Use this parameter to specify the UDP port of the RADIUS server. The range is 1 top 65535. The default is 1812.
Server IP address (Server)	Use this parameter to specify the IP address of the RADIUS server. If you want to disable the definition such that the client stops using it to communicate with a RADIUS server, delete the IP address from the definition.
Accounting Port Number (AccPort)	Use this parameter to specify the UDP port of the accounting server.
Encryption Key (Secret)	Use this parameter to specify the shared secret authentication or encryption key for RADIUS communication between the client and server.

6. Click the Apply button to implement your changes on the switch.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 40

Port Authentication Overview

This chapter contains background information on the port authentication feature of the switch. The chapter contains the following sections:

Overview

Port authentication is a network security feature on the switch. It requires that network users log on a network by providing logon credentials before the switch will begin to forward their traffic. Depending on the authentication method, network users may be required to manually provide usernames and passwords when they log on or their workstations may automatically transmit their MAC addresses as their logon usernames and passwords. Network users without logon credentials are not allowed to forward traffic through the switch and are thus denied access to your network.

Port authentication uses the RADIUS authentication protocol. The protocol has server and client components. The switch has a RADIUS client. To use port authentication, you have to install a RADIUS server on your network. The client on the switch acts as an intermediary between the network users and the RADIUS server on your network. When network users provide their credentials to log on your network, the client on the switch forwards the information to the RADIUS server, which validates the credentials and notifies the switch as to whether the credentials are valid or invalid. For further information, refer to Chapter 39, “RADIUS Client” on page 459.

Note
RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication protocol for port authentication. This feature is not supported with the TACACS+ authentication protocol.

Here are several feature terms:

- Supplicant - A supplicant is an end user or node that wants to access the network through a switch port. A supplicant is also referred to as a client.
- Authenticator - The authenticator is a port that prohibits network access until a supplicant has logged on and been validated by the RADIUS server.
- Authentication server - The authentication server is the network device that has the RADIUS server software. This is the device that does the actual authenticating of the supplicants.

Authentication Methods

The switch supports three authentication methods:

- 802.1x port-based network access control
- MAC address-based authentication
- Web browser authentication

802.1x Port-based Network Access Control

Supplicants of this type of port authentication use usernames and passwords as their logon credentials. They have to provide their unique credentials when they initially begin to forward traffic through the ports on the switch. Supplicants may provide their usernames and passwords manually when prompted by their workstations or their network devices can provide the information automatically. The RADIUS client on the switch forwards the credentials to the RADIUS server on the network for verification.

Supplicants that manually enter their logon credentials are not tied to any specific computer or node. They can log on from any system and still be verified by the RADIUS server as valid users of the switch and network.

The supplicants must have 802.1x client software to support this port authentication method.

MAC address-based authentication

The logon credentials for supplicants of this type of port authentication consist of the MAC addresses of the network nodes. The MAC addresses of the devices are used as the usernames and passwords of the supplicants. Supplicants are not prompted for this information. Rather, the switch extracts the source MAC address from the initial frames received from a node and automatically sends it as both the username and password of the node to the RADIUS server for authentication.

The advantage to this approach is that supplicants need not have 802.1x client software. The disadvantage is that because clients are not prompted for usernames and passwords, it does not prevent an unauthorized individual from accessing a network through an unattended network node or by counterfeiting a valid network MAC address.

Web Browser Authentication

This authentication method is similar to 802.1x port-based network access control in that the logon credentials for supplicants are usernames and passwords. The switch passes the username and password combinations to a RADIUS server for confirmation before forwarding user traffic.

The difference between this authentication method and 802.1x port-based network access control authentication is that supplicant nodes do not need 802.1x client software.

Authenticator Port Operational Settings

An authenticator port on the switch can have one of three possible operational settings:

- Auto - Activates port authentication on a port. Supplicants must provide logon credentials for verification before a port begins to forward their network traffic. This is the default setting for an authenticator port.
- Force-authorized - Disables port authentication and automatically places the port in the authorized state without any authentication exchange required. The port transmits and receives normal traffic without authenticating the client.

Note
A supplicant connected to an authenticator port set to force-authorized must have 802.1x client software if the port's authenticator mode is 802.1x. Though the force-authorized setting prevents an authentication exchange, the supplicant must still have the client software to forward traffic through the port.

- Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. This setting is analogous to disabling a port.

As mentioned earlier, the switch itself does not authenticate the user names and passwords from the clients. That function is performed by the authentication server and the RADIUS server software on your network. The switch acts as an intermediary for the authentication server by denying access to the network by clients until the server has validated their logon credentials.

Authenticator Port Operating Modes

Authenticator ports support three modes:

- Single host mode
- Single host mode with Piggy-backing
- Multiple Host mode

Single Host Mode

An authenticator port set to the single host mode permits only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant that might try to log on.

In Figure 115, port 10 is an authenticator port set to the single host mode. It permits only one supplicant to log on and forwards the traffic of only that supplicant.

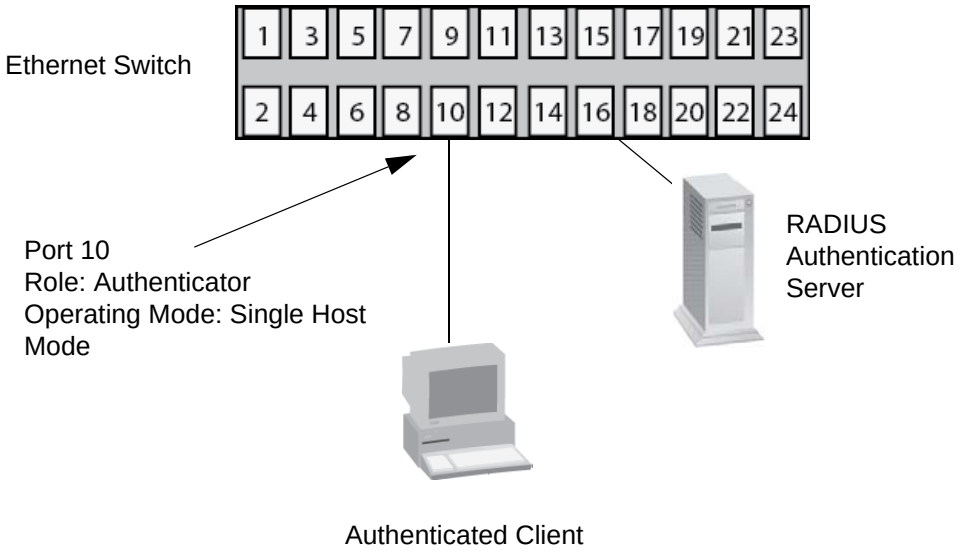

Figure 115. Single Host Mode

Single Host Mode with Piggy Backing

This mode permits multiple clients on an authenticator port, but only one of the clients is authenticated. An authenticator mode forwards packets from all of the clients after one client has successfully logged on. This mode is typically used in situations where you want to add authentication to a switch port that is supporting multiple clients, but do not want to create individual accounts for all the clients on the RADIUS server.

This is referred to as “piggy-backing.” After one client has successfully logged, the port permits the other clients to piggy-back onto the initial client’s log on, so that they can forward packets through the port without

being authentication.

Note, however, that should the client who performed the initial log on fail to periodically reauthenticate or log out, the authenticator port reverts to the unauthenticated state. It bars all further traffic to and from all of the clients until the initial client or another client logs on.

Figure 116 is an example of this mode. Port 10 is connected to an Ethernet hub or non-authentication compliant switch, which in turn is connected to several supplicants. The switch does not forward the client traffic until one of the clients logs on. Afterwards, it forwards the traffic of all the clients.

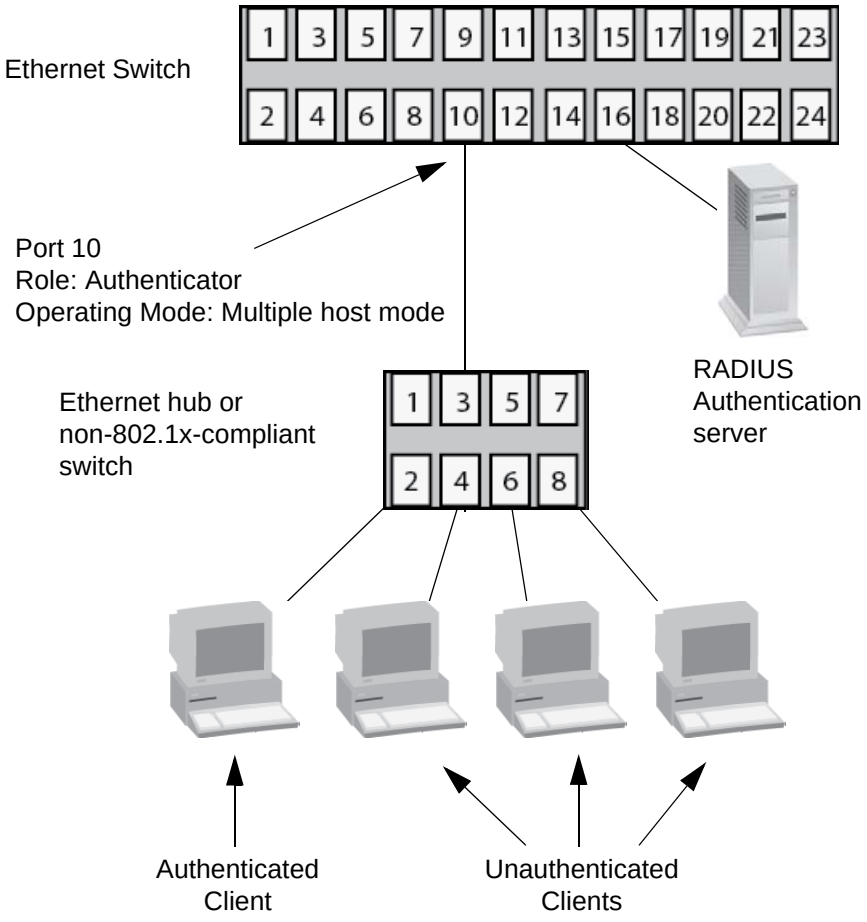

Figure 116. Multiple Host Operating Mode

If the port is set to the 802.1x authentication method, one client must have 802.1x client firmware and must provide a username and password during authentication. (The other clients do not need 802.1x client firmware to forward traffic through the port after one client has been authenticated.)

If the port is using MAC address-based or web browser authentication,

802.1 client firmware is not required. The first client to forward traffic through the port is used for authentication. When that client is authenticated, all supplicants have access to the port.

As mentioned earlier, should the client who performed the initial log on fail to reauthenticate when necessary or log out, the port reverts to the unauthenticated state, blocking all traffic to and from all clients. Another client must be authenticated in order for all remaining clients to continue to forward traffic through the port.

Multiple Host Mode

This mode requires the authentication of all the clients on an authenticator port. This mode is appropriate in situations when you want all of the clients to be authenticated on authenticator ports that are supporting more than one client.

If you are using 802.1x or web browser authentication, you must provide each client with a separate username and password combination and the clients must provide their combinations to forward traffic through a switch port.

An example of this authenticator operating mode is illustrated in Figure 117 on page 478. The clients are connected to a hub or non-authentication switch which is connected to an authenticator port on the switch. If the authenticator port is set to 802.1x or web browser authentication, the clients must provide their username and password combinations before they can forward traffic through the switch.

If the authentication method is MAC address-based, the authenticator port uses the MAC addresses of the clients as the username and password combinations. The port accepts and forwards traffic only from those clients whose MAC addresses have been entered on the RADIUS server and denies access to all other users.

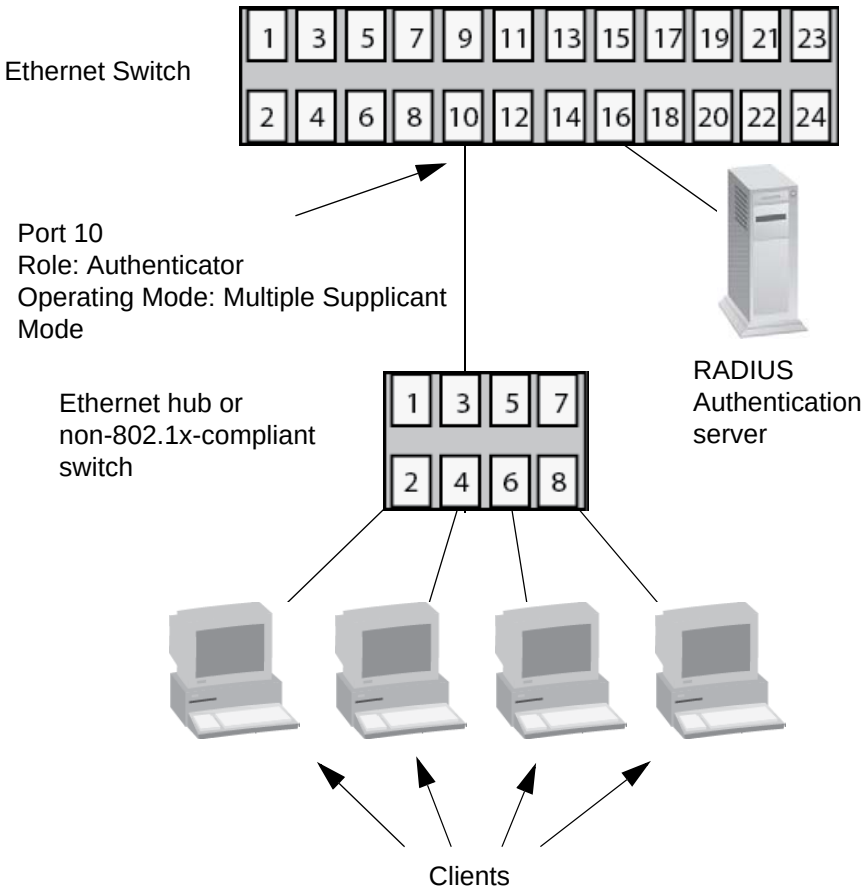

Figure 117. Multiple Supplicant Mode

Supplicant and VLAN Associations

One of the challenges to managing a network is accommodating end users who roam. These are individuals whose work requires that they access the network resources from different points at different times. The difficulty arises in providing them with access to the same network resources and, conversely, restricting them from unauthorized areas, regardless of the workstation from where they access the network. A closely related issue is where a workstation is employed at various times by different individuals with unique requirements in terms of network resources and security levels.

Providing network users with access to their network resources while also maintaining network security is often achieved with VLANs. As explained in Chapter 16, “Port-based and Tagged VLANs Overview” on page 177, a VLAN is an independent traffic domain where the traffic generated by the nodes within the VLAN is restricted to nodes of the same VLAN, unless there is a router or Layer 3 device. Different users are assigned to different VLANs depending on their resource requirements and security levels.

The problem with a port-based VLAN is that VLAN membership is determined by the port on the switch to which the device is connected. If a different device that needs to belong to a different VLAN is connected to the port, the port must be manually moved to the new VLAN using the management software.

With port authentication, you can link a username and password combination or MAC address to a specific VLAN so that the switch automatically moves the port to the appropriate VLAN when a client logs on. This frees you from having to reconfigure VLANs as end users access the network from different points or where the same workstation is used by different individuals at different times.

To use this feature, you have to enter a VLAN identifier, along with other information, when you create a supplicant account on the RADIUS server. The server passes the identifier to the switch when a user logs on with a valid username and password combination or MAC address, depending on the authentication method. The information to provide on the RADIUS server is outlined in “Supplicant VLAN Attributes on the RADIUS Server” on page 480.

How the switch responses when it receives VLAN information during the authentication process can differ depending on the operating mode of an authenticator port.

Single Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the single host mode:

- If the switch receives a valid VLAN ID or VLAN name from the RADIUS server, it moves the authenticator port to the designated guest VLAN and changes the port to the authorized state. Only the authenticated supplicant is allowed to use the port. All other supplicants are denied entry.
- If the switch receives an invalid VLAN ID or VLAN name from the RADIUS server (e.g., the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multiple Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the multiple host mode:

- If the switch receives a valid VLAN ID or VLAN name from the RADIUS server, it moves the authenticator port to the designated VLAN and changes the port to the authorized state. All clients are allowed access to the port and the same VLAN after the initial authentication.
- If the switch receives an invalid VLAN ID or VLAN name from the RADIUS server (e.g., the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multiple Supplicant Mode

The initial authentication on an authenticator port running in the multiple supplicant mode is handled in the same fashion as with the Single operating mode. If the switch receives a valid VLAN ID or name from the RADIUS server, it moves the authenticator port to the designated VLAN and changes the port to the authorized state.

How the switch handles subsequent authentications on the same port depends on how you set the Secure VLAN parameter. Your options are as follows:

- If you activate the Secure VLAN feature, only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with different VLAN assignments or with no VLAN assignment are denied access to the port.
- If you disable the Secure VLAN feature, all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication.

Supplicant VLAN Attributes on the RADIUS Server

The following information must be entered as part of a supplicant's account on the RADIUS server when associating a supplicant to a VLAN.

- Tunnel-Type
  The protocol to be used by the tunnel specified by Tunnel-Private-Group-Id. The only supported value is VLAN (13).

- Tunnel-Medium-Type
  The transport medium to be used for the tunnel specified by Tunnel-Private-Group-Id. The only supported value is 802 (6).
- Tunnel-Private-Group-ID
  The ID of the tunnel the authenticated user should use. This must be the name of VID of the VLAN of the switch.

Guest VLAN

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a supplicant. However, you can configure an authenticator port to be a member of a Guest VLAN when no supplicant is logged on. Any client using the port is not required to log on and has full access to the resources of the Guest VLAN.

If the switch receives 802.1x packets on the port, signalling that a supplicant is logging on, it moves the port to its predefined VLAN and places it in the unauthorized state. The port remains in the unauthorized state until the log on process between the supplicant and the RADIUS server is completed. When the supplicant logs off, the port automatically returns to the Guest VLAN.

Note
The Guest VLAN feature is only supported on an authenticator port in the Single operating mode.

RADIUS Accounting

The switch supports RADIUS accounting for switch ports in the Authenticator role. This feature sends information to the RADIUS server about the status of the supplicants so that you can monitor network activity and use.

The switch sends accounting information to the RADIUS server when the following events occur:

- Supplicants log on
- Supplicants logs off
- Authenticator ports change states during active supplicant sessions (for example, a port is reset or is changed from the Authenticator role to None role while a supplicant is logged on)

The event information sent to the RADIUS server includes:

- The port number where an event occurred.
- The date and time when an event occurred.
- The number of packets transmitted and received by a switch port during a supplicant's session. (This information is sent only when a client logs off.)

You can also configure the accounting feature to send interim updates so you can monitor which clients are still active.

Here are the guidelines to using the accounting feature:

- The management software supports the Network level of accounting, but not the System or Exec.
- This feature is only available on Authenticator ports.
- You must configure 802.1x Port-based Network Access Control as explained in this chapter and designate the Authenticator ports.
- You must configure the RADIUS client.

General Steps

Here are the general steps to implementing port authentication and RADIUS accounting on the switch:

1. You must install a RADIUS server on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesis. Funk Software Steel-Belted Radius and Free Radius have been verified as fully compatible with the switch's management software.

   Note
   This feature is not supported with the TACACS+ authentication protocol.

2. You must create accounts on the server for the supplicants:

   - To create an account for a supplicant connected to an authenticator port set to the 802.1x or web browser authentication mode, enter a username and password combination. The maximum length for a username is 38 alphanumeric characters and spaces, and the maximum length for a password is 16 alphanumeric characters and spaces.
   - To create an account for a supplicant connected to an authenticator port set to the MAC address-based authentication mode, enter the MAC address of the node used by the supplicant as both its username and password.

3. Those clients connected to an authenticator port set to 802.1x authentication must have 802.1x client software. Microsoft WinXP client software and Meeting House Aegis client software have been verified as fully compatible with the switch's management software. (Clients of MAC address or web browser-based authentication do not require 802.1x client software.)

4. You must configure the RADIUS client on the switch by entering the IP addresses and encryption keys of the authentication servers on your network. For instructions, refer to Chapter 39, "RADIUS Client" on page 459.

5. You must configure the port access control settings on the switch, as explained in Chapter 41, "Port Authentication" on page 487.

Guidelines

Here are the general guidelines to this feature:

- Ports that are configured for authentication do not support dynamic MAC address learning.
- A port that is connected to a RADIUS authentication server must not be set to the authenticator role because an authentication server cannot authenticate itself.
- The authentication method of an authenticator port can be 802.1x, MAC address, or web browser-based authentication.
- Supplicants connected to authenticator ports set to 802.1x authentication must have 802.1x client software.
- Supplicants do not need 802.1x client software for MAC address or web browser-based authentication.
- The logon credentials for 802.1x and web browser supplicants are not tied to the MAC addresses of an end node. This allows end users to use the same logon credentials when working at different workstations.
- The MAC addresses of authenticated clients are added to the MAC address table as authenticated addresses. They remains in the table until the clients log off the network or fail to reauthenticate, at which point they are removed. The addresses are not timed out, even if the nodes are inactive.

Note
End users of port authentication should be instructed to always log off at the conclusion of every work session. This can prevent unauthorized individuals from accessing the network through unattended network workstations.

- Authenticator and supplicant ports must be untagged ports. They cannot be tagged ports.
- Authenticator ports cannot use MAC address-based port security. For further information, refer to Chapter 37, “MAC Address-based Port Security Overview” on page 447.
- Authenticator ports cannot be members of static port trunks or the port mirror.
- The Guest VLAN feature requires that the designated VLAN already exist on the switch.
- The Guest VLAN can be a port-based or tagged VLAN.
- The switch supports EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP and EAP-PEAP authentication.

- The switch must have an management IP address to communicate with the RADIUS server. For background information, refer to “Changing the IP Address Configuration” on page 48.

Here are the guidelines to adding VLAN assignments to supplicant accounts on a RADIUS server:

- The VLAN can be either a port-based or tagged VLAN.
- The VLAN must already exist on the switch.
- A client can have only one VLAN associated with it on the RADIUS server.
- When a supplicant logs on, the switch port is moved as an untagged port to the designated VLAN.

Chapter 41

Port Authentication

This chapter contains instructions on how to configure the port authentication feature on the switch. The chapter contains the following procedures:

Note
For background information, refer to Chapter 40, “Port Authentication Overview” on page 471

Displaying the Port Authentication Window

To view the Port Authentication window, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118.

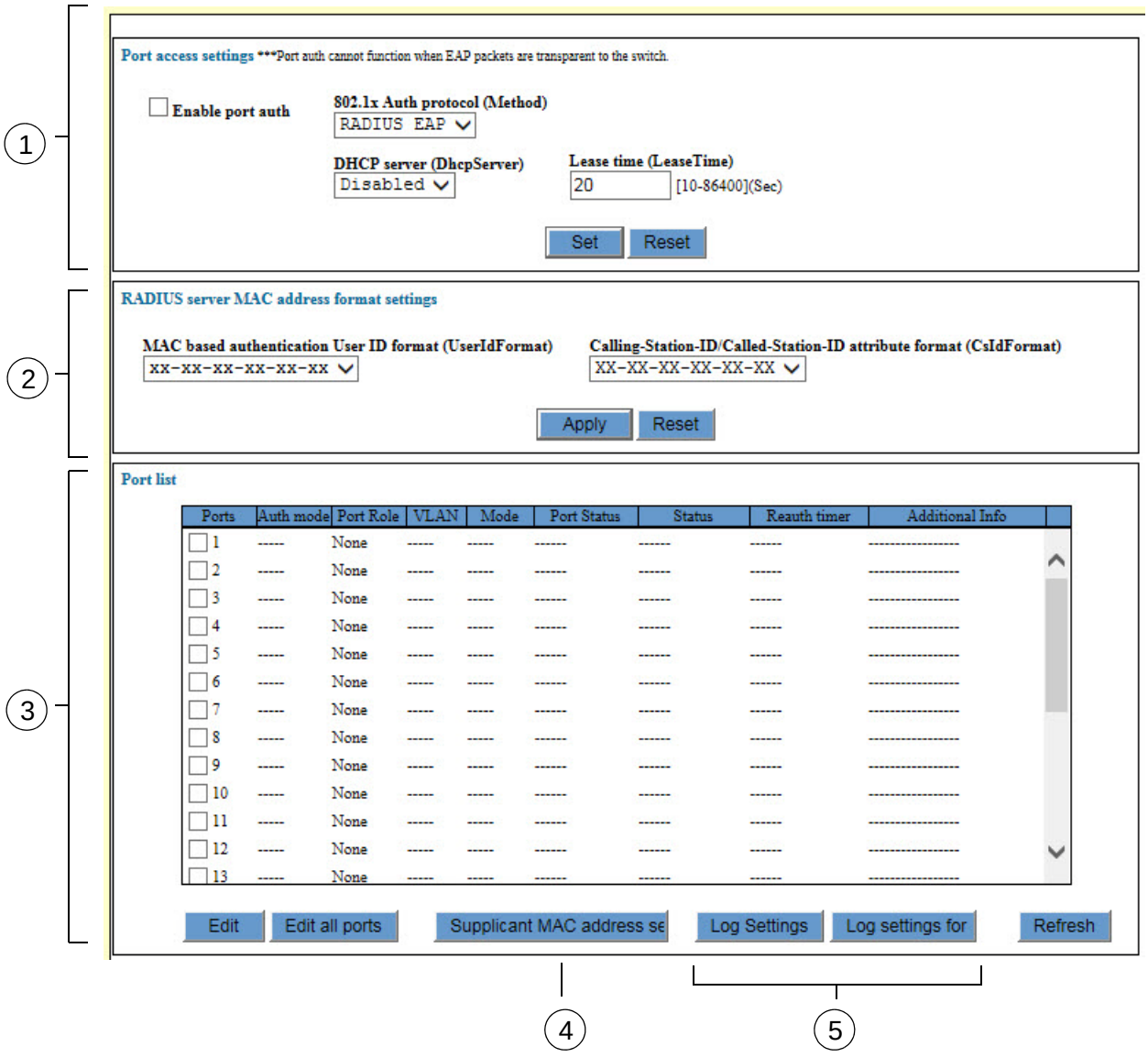

Figure 118. Security Settings - Port Authentication Window

The sections in the Security Settings - Port Authentication window are defined in Table 126.

Table 126. Security Settings - Port Authentication Window

Section	Description
1	Use this section to enable or disable port authentication on the switch or to configure the basic settings. Refer to "Enabling Port Authentication on the Switch" on page 492 or "Disabling Port Authentication on the Switch" on page 518.
2	Use this section to specify the format of the MAC addresses when the switch sends them to the RADIUS server. This section applies only to MAC address-based authentication. Refer to "Enabling Port Authentication on the Switch" on page 492.
3	Use this section to view or configure the authenticator or supplicant settings on the ports. Refer to "Configuring Authenticator Ports" on page 495 or "Configuring Supplicant Ports" on page 508.
4	Use this button to manage non-authenticated network devices. Refer to "Designating Non-authenticated Network Devices" on page 514.
5	Use the Log Settings or Log Settings for All Ports button to configure the switch to enter events in the event log when clients log on the authenticator ports. Refer to "Configuring Log Events for Authenticator Ports" on page 512

The Port List table in the window displays port status information. The information is described in Table 127.

Table 127. Port List Table in the Security Settings - Port Authentication Window

Column	Description
Port	Displays the port number.

Table 127. Port List Table in the Security Settings - Port Authentication Window (Continued)

Column	Description
Auth Mode	Displays the authentication mode of the port. The options are listed here: 8021x - 802.1X authentication MACBASE - MAC address authentication Web - Web browser authentication
Port Role	Displays the port access role. The possible roles are listed here: Auth - Authenticator role Supp - Supplicant role None - No role
VLAN	Displays the VID of the VLAN where the port is currently an untagged member.
Mode	Displays the operating mode of an authenticator port. The mode can be Single or Multiple. For background information, refer to “Authenticator Port Operating Modes” on page 475. This column does not distinguish between single mode and single mode with piggybacking.
Port Status	Displays the port status, as follows: Authorized - At least one supplicant has logged on the port. Unauthorized - No supplicants have logged on the port.

Table 127. Port List Table in the Security Settings - Port Authentication Window (Continued)

Column	Description
Status	Displays port status. The status field is dependent on the port role. The possible status values for authenticator ports are listed here: Aborting Authenticated Authenticating Connecting Disconnected Force_Auth Force_Unauth Held Initialize The possible status values for supplicant ports are listed here Acquired Authenticated Authenticating Connecting Disconnected Held Logoff
Reauth Timer	Displays the amount of time remaining before the supplicant has to reauthenticate.
Additional Info	Displays the MAC address of an authenticated node on an authenticator port with a status of Authenticated.

Enabling Port Authentication on the Switch

To enable port authentication or to configure the basic parameters in sections 1 and 2 of the port authentication window (refer to Figure 118 on page 488), perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Port Authentication window is shown in Figure 118 on page 488.
3. Configure the parameters in the top section of the window, as needed. The parameters are described in Table 128.

Table 128. Port Access Settings

Parameter	Description
Enable Port Auth	Use this option to enable or disable port authentication on the switch. The feature is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default setting is disabled.
802.1X Authentication Protocol (Method)	Use this option to view the authentication method of the authentication server. RADIUS EAP is the only available selection.
DHCP server (DhcpServer)	Use this option to enable or disable the DCHP server on the switch. The server is used with web browser authentication to assign temporary IP addresses to supplicants for use during the authentication process. Do not enable the DHCP server if you are not using web browser authentication. The server is not used for 802.1X or MAC address authentication.

Table 128. Port Access Settings (Continued)

Parameter	Description
Lease Time (LeaseTime)	Use this option to specify the lease time for the temporary IP addresses the switch assigns to supplicants who are using web browser authentication. The range is 10 to 86400 seconds. The default is 20 seconds. The value should be as short as possible to ensure that supplicants apply for new IP addresses immediately after the completion of the authentication processes. The lease time applies only to web browser authentication. It does not apply to 802.1X or MAC address authentication.

4. Click the Set button.

5. To permanently save your changes in the configuration file, click the Save button above the main menu.

6. If supplicants will be using the MAC addresses of their workstations for authentication, configure the two parameters in the middle section of the window. The parameters are described in Table 129.

Table 129. RADIUS Server MAC Address Format Settings

Parameter	Description
MAC based authentication User ID Format (UserIdFormat)	Use this parameter to specify how the switch is to format the MAC addresses of supplicants when forwarding them to a RADIUS server for authentication. The format specified here needs to match the format you plan to use when you enter the MAC addresses as the usernames and passwords for the user accounts on the RADIUS server. You can configure the switch to send the addresses with the hexadecimal letters (A to F) in all uppercase or lowercase. You may group the digits in groups of two or four and separated with hyphens, colons, or periods, or with no separators.

Table 129. RADIUS Server MAC Address Format Settings

Parameter	Description
Calling-Station-ID/Called-Station-ID attribute format (CsId Format)	Use this parameter to specify the format of the MAC addresses of the supplicants when the switch adds them to attributes 30 (Called-Station-ID) and 31 (Calling-Station-ID) in RADIUS packets. The same MAC address format is used for both attributes.

7. Click the Apply button.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring Authenticator Ports

To configure a port as an authenticator port, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.
3. In the Port List table at the bottom of the window, click the dialog box of the port that is to be an authenticator port. You may configure more than one port at a time.
4. Click the Edit button. To configure all of the ports, click the Edit All Ports button.

   The switch displays the Port Settings window.
5. Click the Authenticator dialog circle at the top of the window to designate the port as an authenticator port.
6. Click the Apply button.

   The switch displays the Port Authentication - Port Settings window for authenticator ports. Refer to Figure 119 on page 496.

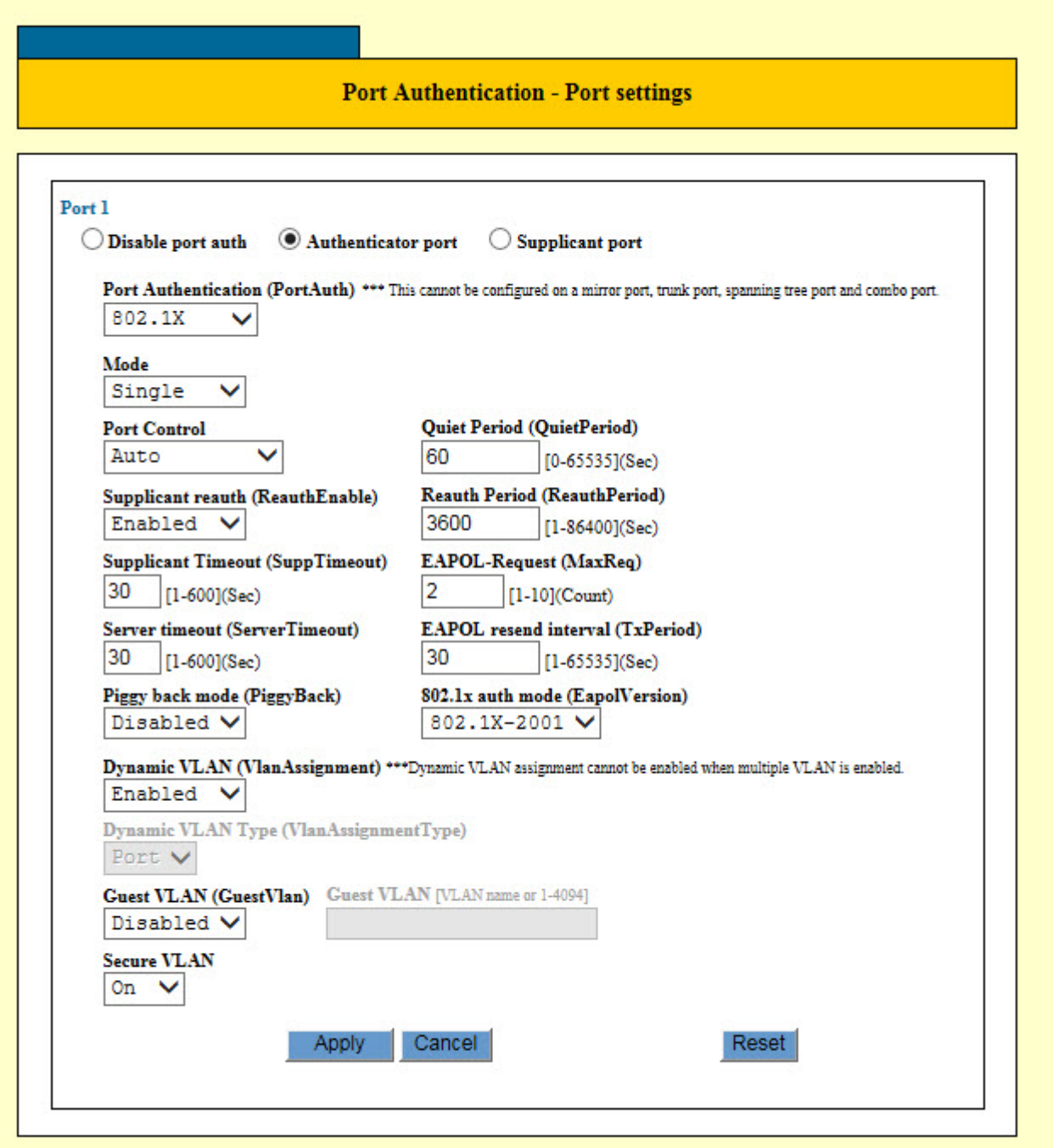

Figure 119. Port Authentication - Port Settings Window for Authenticator Ports

7. Configure the authenticator port parameters: The parameters are described in Table 130 on page 497.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports

Parameter	Description
Port Authentication (PortAuth)	Use this parameter to set the mode of an authenticator port. The possible settings are listed here: 802.1x: Specifies 802.1x username and password as the authentication method on an authenticator port. Supplicants must provide, either manually or automatically, usernames and passwords when they log on to an authenticator port in this mode. This authentication method requires 802.1x client software on the supplicant nodes. MAC Based: Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames from a supplicant and automatically sends it to the authentication server as the username and password of the supplicant. Supplicant nodes do not need 802.1x client software for this authentication method. Web Browser - Specifies web browser authentication.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Mode	Use this parameter to set the supplicant mode of an authenticator port. The possible settings are listed here: Single: Configures an authenticator port to accept only one authentication. This mode should be used together with the piggy-back mode. When an authenticator port is set to the Single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port. Multiple: Configures an authenticator port to accept up to 20 authentications. An authenticator port in this mode requires that all of its clients have logon credentials.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Port Control	Use this parameter to set the operational mode of an authenticator port. The possible settings are listed here: Auto - Activates port authentication. Clients must provide logon credentials to forward traffic through the port. This is the default setting. ForceUnauth **-** Causes the port to remain in the unauthorized state, ignoring all attempts by clients to authenticate. The switch cannot provide authentication services to the client through the interface ForceAuth - Disables port authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without authentication of a client. A supplicant connected to an authenticator port set to force-authorized must have 802.1x client software if the port's authenticator mode is 802.1x. Though the force-authorized setting prevents an authentication exchange, the supplicant must still have the client software to forward traffic through the port.
Quiet Period (QuietPeriod)	Use this parameter to set the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Supplicant Reauth (ReauthEnabled)	Use this parameter to control whether the client must periodically reauthenticate. The possible settings are listed here: Enabled - The client must periodically reauthenticate. The time period between reauthentications is set with the Reauth Period option. This is the default setting. Disabled - The client is not required to reauthenticate after the initial authentication, unless there is a change to the status of the link between the supplicant and the switch or the switch is reset or power cycled.
Reauth Period (ReauthPeriod)	Use this parameter to specify the time period in seconds between reauthentications of the client when the Supplicant Reauth option is set to Enabled. The range is 1 to 65,535 seconds. The default value is 3600 seconds.
Supplicant Timeout (SuppTimeout)	Use this parameter to set the switch-to-client retransmission time for the EAP-request frame. The range is 1 to 600 seconds. The default value is 30 seconds. This parameter is only available with 802.1x authentication. It is not available with MAC address or web browser authentication.
EAPOL-Request (MaxReq)	Use this parameter to specify the maximum number of times the switch retransmits an EAP Request packet to the client before it times out the authentication session. The range is 1 to 10 retransmissions. The default value is 2 retransmissions. This parameter is only available with 802.1x authentication. It is not available with MAC address or web browser authentication.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Server Timeout (ServerTimeout)	Sets the timer used by the switch to determine authentication server timeout conditions. The range is 1 to 600 seconds. The default value is 30 seconds. This parameter is available with 802.1x and web browser authentications. It is not available with MAC address authentication.
EAPOL Resend Interval (TxPeriod)	Use this parameter to set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds. The default value is 30 seconds. This parameter is only available with 802.1x authentication. It is not available with MAC address or web browser authentication.
Pibbyback Mode (PiggyBack)	Use this parameter to control who can use the switch port in cases where there are multiple clients (e.g., the port is connected to an Ethernet hub). The possible settings are listed here: Enabled - The port allows clients to piggy-back onto the initial client's authentication. The port forwards packets from all of it clients after one client has been authenticated. Disabled - The switch port forwards only those packets from the client who was authenticated and discards packets from all other users. This parameter is only available with 802.1x authentication. It is not available with MAC address or web browser authentication.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
802.1x Auth Mode (EapolVersion)	Use this parameter to specify the version of 802.1x. The settings are listed here: 802.1X-2001 802.1X-2004 This parameter is only available with 802.1x authentication. It is not available with MAC address or web browser authentication.
Dynamic VLAN (VlanAssignment)	Use this parameter to control whether an authenticator port uses the VLAN assignment returned by a RADIUS server. For background information, refer to “Supplicant and VLAN Associations” on page 479. The parameter options are listed here: Enabled: Specifies that the authenticator port is to use the VLAN assignment returned by the RADIUS server when a supplicant logs on. This is the default setting. The port automatically moves to the designated VLAN after the supplicant successfully logs on. Disabled: Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even if the RADIUS server returns a VLAN assignment when a supplicant logs on. This is the default setting.
Dynamic VLAN Type (VlanAssignmentType)	Use this parameter to specify the dynamic VLAN type. The choices are Port and User (MAC address).

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Guest VLAN (GuestVlan)	Use this parameter to control the Guest VLAN feature on an authenticator port. For background information, refer to "Guest VLAN" on page 482. The possible settings are listed here: Enabled - Enables the Guest VLAN feature on an authenticator port. An authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN. Disabled - Disables the feature.
Guest VLAN (VLAN Name or 1-4094)	Use this parameter to specify the Guest VLAN. You may specify a Guest VLAN by its name or VID.This option is only available when the Guest VLAN (GuestVlan) parameter is enabled. This parameter is only supported when the supplicant mode of an authenticator port is set to the single mode. The parameter is not supported when the supplicant mode of an authenticator port is set to the multiple mode.

Table 130. Port Authentication - Port Settings Window for Authenticator Ports (Continued)

Parameter	Description
Secure VLAN	Use this parameter to control the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode. The possible settings are listed here: On: Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting. Off: Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

8. Click the Apply button to activate your changes on the switch.

9. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring the Web Authentication Server

You have to perform this procedure if you plan to use the web browser authentication method on any of the authenticator ports on the switch. This procedure is not required for the 802.1x or MAC address-based authentication method. This procedure allows you to configure the following parameters:

- Enable or disable the web authentication server on the switch.
- Specify the server's port software number.
- Specify a web page to which supplicants are directed after they successfully log on.
- Specify the messages in the logon window. Refer to Figure 121 on page 507.

To configure the web authentication server, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Port Authentication window is shown in Figure 118 on page 488.
3. Click the Web Server button.

   The switch displays the Security Settings - Web Authenticator Server window, shown in Figure 120 on page 506.

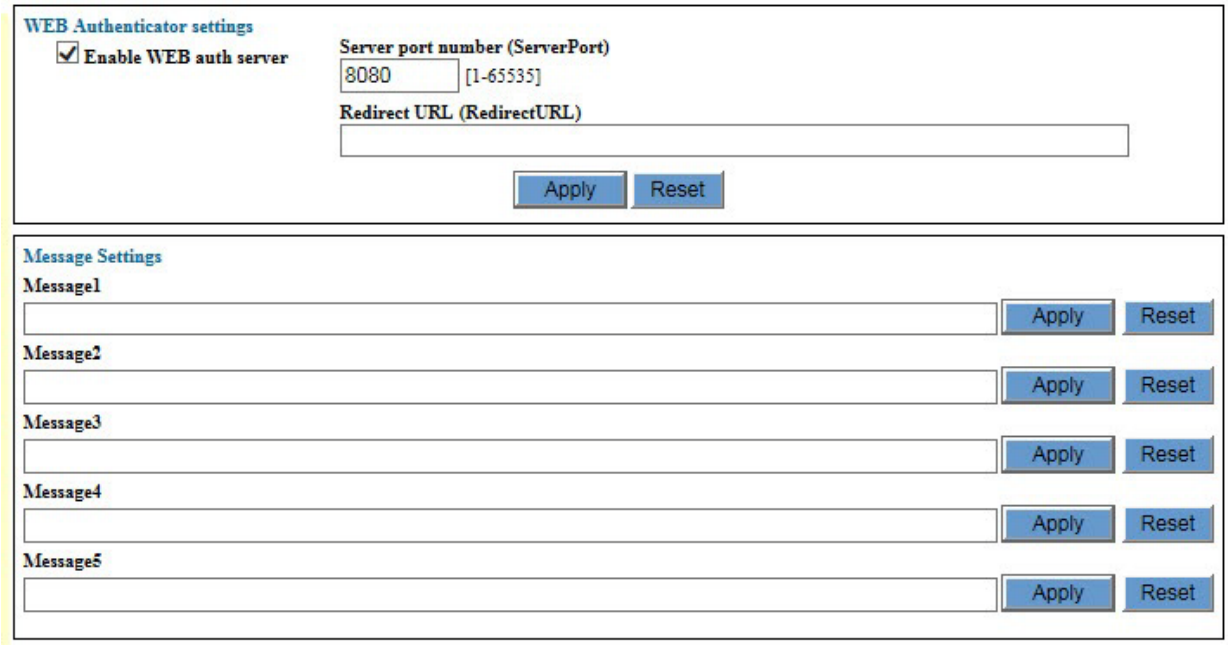

Figure 120. Security Settings - Web Authenticator Window

4. Configure the parameters in the window. They are described in Table 131.

Table 131. Security Settings - Web Authenticator Window

Parameter	Description
Web Server Authentication	Use this option to enable or disable web authentication. Web authentication is enabled when the dialog box has a check mark and disabled when the dialog box is empty.
Server Port	Use this option to specify the HTTP port number of the web authentication server. The range is 1 to 65535. The default is 8080.
Redirect URL	Use this option to specify the URL of the web page to which supplicates are redirected to after successfully logging on with web authentication.
Messages	Use these options to enter the messages to be displayed on the web authentication login screen. Refer to Figure 121 on page 507.

Figure 121 identifies the locations of the messages in the logon window for web browser authentication.

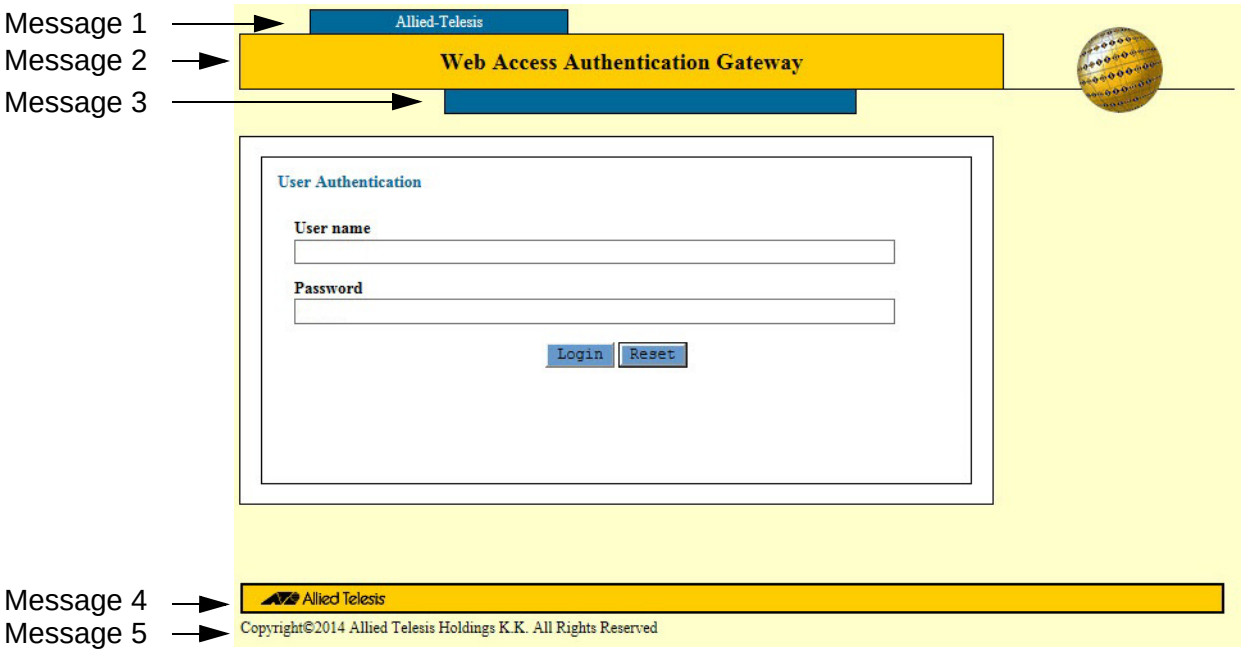

Figure 121. Locations of the Messages in the Web Access Authentication Gateway

5. Click the Apply button.

6. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring Supplicant Ports

To configure a port as a supplicant port, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.
3. In the Port List table, click the dialog box of the port you want to configure. You may configure more than one port at a time.
4. Click the Edit button. To configure all of the ports, click the Edit All Ports button.

   The switch displays the Port Authentication - Port Settings window.
5. Click the Suppliant dialog circle at the top of the window.

   The switch displays the Port Authentication - Port Settings window for supplicant ports. Refer to Figure 122 on page 509.

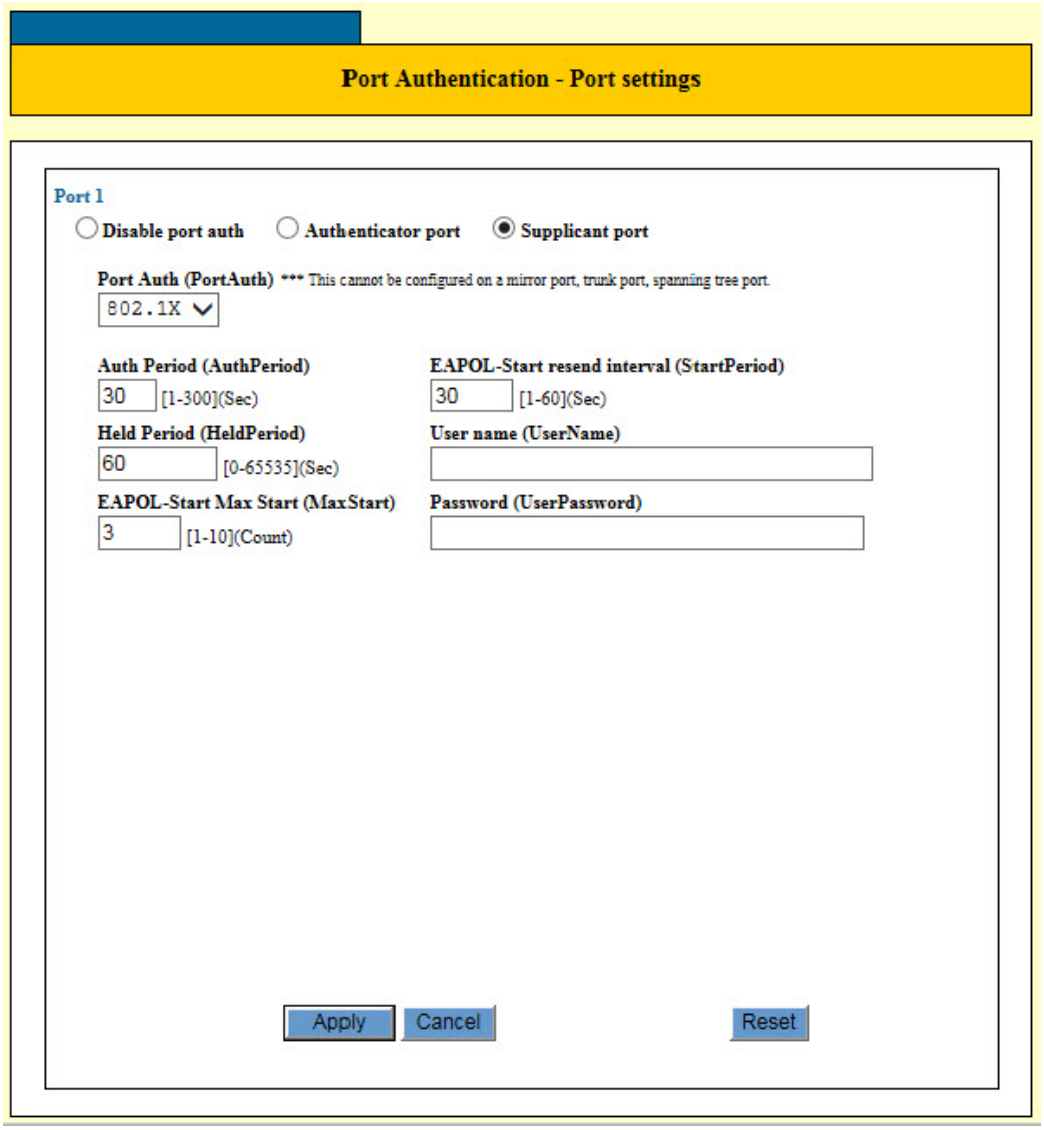

Figure 122. Port Authentication - Port Settings Window for Supplicant Ports

6. Configure the supplicant parameters, as needed: The parameters are described in Table 132 on page 509.

Table 132. Port Authentication - Port Settings window for Supplicant Ports

Parameter	Description
Port Auth (PortAuth)	Use this parameter to specify the type of port authentication. The only option is 802.1X.

Table 132. Port Authentication - Port Settings window for Supplicant Ports

Parameter	Description
Auth Period (AuthPeriod)	Use this parameter to specify the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 300 seconds. The default is 30 seconds.
EAPOL-Start Resend Interval (StartPeriod)	Use this parameter to specify the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60 seconds. The default is 30 seconds.
Held Period (HeldPeriod)	Use this parameter to specify the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535 seconds. The default value is 60 seconds.
User Name (UserName)	Use this parameter to specify the username for the switch port. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case sensitive.
EAPOL-Start Max Start (MaxStart)	Use this parameter to specify the maximum number of times the supplicant sends EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

Table 132. Port Authentication - Port Settings window for Supplicant Ports

Parameter	Description
Password (UserPassword)	Use this parameter to specify the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case sensitive.

7. After configuring the supplicant parameters. click the Apply button to implement your changes.

8. To permanently save your changes in the configuration file, click the Save button above the main menu.

Configuring Log Events for Authenticator Ports

The switch can add events to the event log when users log onto your network through the authenticator ports. The events become a record of when users enter or exit your network. You may specify the supplicant actions that cause events to be stored in the event log. The actions may be specified separately for the three authentication methods: 802.1X, MAC address, and web browser.

To configure the authentication actions that add events to the event log, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.
3. In the List Ports table in the window, click the dialog boxes of the authenticator ports where you want to set the event log actions.
4. Click the Log Settings button. To configure all of the ports, click the Log Settings for All Ports button.

   The switch displays the Authentication Log Settings window, shown in Figure 123.

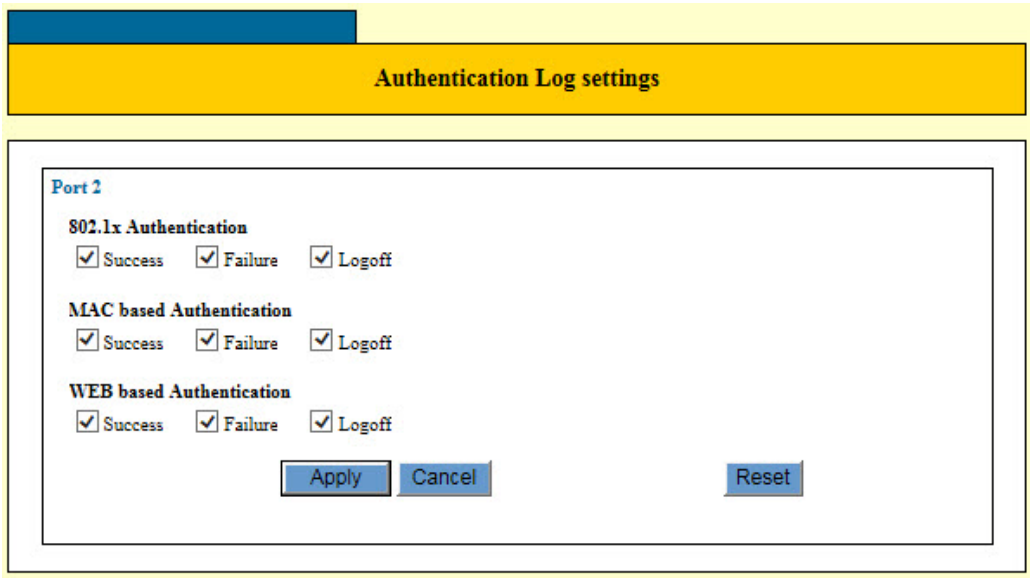

Figure 123. Authentication Log Settings Window

5. Configure the options in the window. The options are described in Table 133 on page 513.

Table 133. Authenticator Log Settings Window

Action	Description
Success	Activate this option if you want the switch to add events to the event log when supplicants successfully log on the switch using an authentication method. The option is active when the dialog box has a check mark.
Failure	Activate this option if you want the switch to add events to the event log when supplicants are unsuccessful when they log on the switch using an authentication method. The option is active when the dialog box has a check mark.
Log off	Activate this option if you want the switch to add events to the event log when supplicants log off the switch. The option is active when the dialog box has a check mark.

6. After configuring the parameters. click the Apply button to implement your changes.

7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Designating Non-authenticated Network Devices

Network devices that are connected to authenticator ports on the switch are usually required to provide logon credentials for validation by a RADIUS server before the switch begins to forward their traffic. However, your network might have network devices that you do not want the switch to authenticate. The solution for these devices, which might include network servers or printers, is to designate them as non-authenticated network devices. These devices can forward traffic through authenticator ports without having to provide logon credentials. You designate non-authenticated network devices by adding their MAC addresses as approved supplicant addresses to the authenticator ports.

Here are the guidelines to the feature.

- The feature is supported on authenticator ports set to Auto authentication.
- You must configure a port as an authentication port with Auto authentication before adding the MAC addresses of the non-authenticated devices.
- When a MAC address of a non-authenticated device is added to an authenticator port, the corresponding network device can only communicate with the switch through that port. If you move the device or rewire the switch such that the device is connected to a different port, the switch blocks its traffic.
- The MAC address of a non-authenticated device is added as a static address to the MAC address table when the device initially begins to forward traffic through the switch. Consequently, the address is not deleted from the table when the device is inactive.
- You may add up to 10 MAC addresses of non-authenticated devices to an authenticator port.
- You may not specify a range of MAC addresses or multicast or broadcast addresses.
- A device can be registered as a non-authenticated device on only one authenticator port at a time.

To manage the MAC addresses of non-authenticated network devices, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.

3. In the Port List table, click the dialog box of the authentication port where you want to add MAC addresses of non-authenticated devices.

   You may configure only one port at a time. The selected port must already be set to Auto authenticator. For instructions, refer to "Configuring Authenticator Ports" on page 495.

4. Click the Supplicant MAC Address Settings button.

   The Port Authentication - Supplicant MAC Address Settings window is shown in Figure 124.

   Note
   If your web browser does not display the window, there may be a compatibility problem. You might need to add the IP address of the switch to the compatibility view of your web browser.

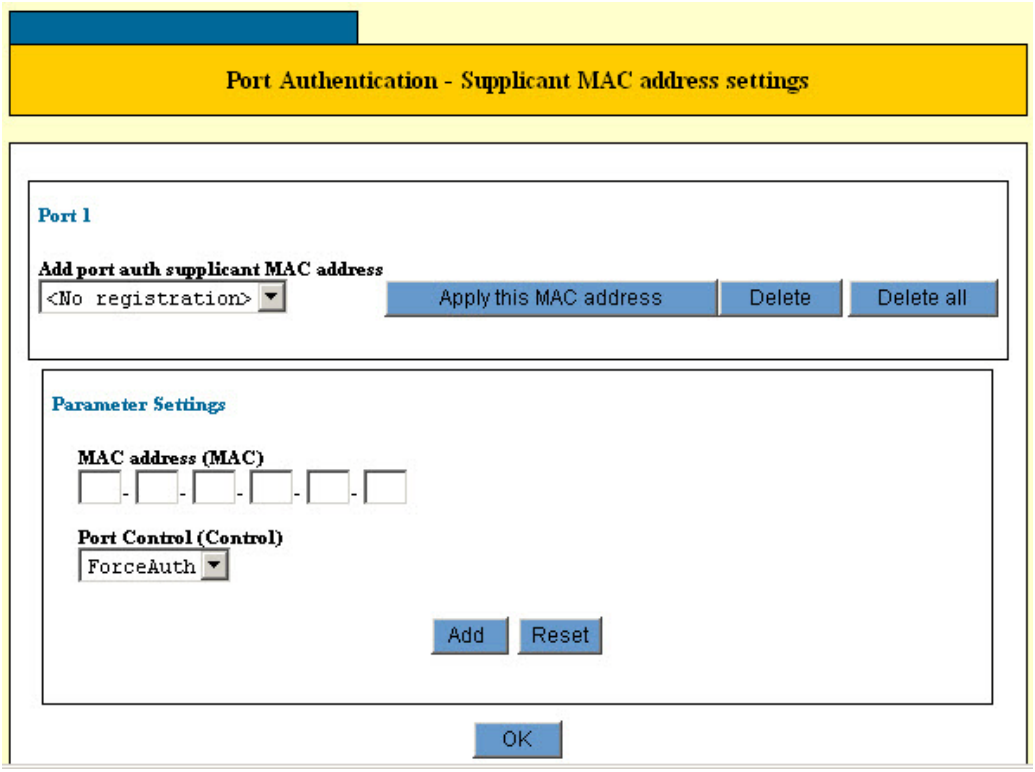

Figure 124. Port Authentication - Supplicant MAC Address Settings

5. To add a MAC address of a non-authenticated device, perform the following steps:

   a. Enter the address in the MAC Address (MAC) fields.

Note
The Port Control (Control) parameter cannot be adjusted.

b. Click the Add button.

   The address is added to the Add Port Auth Supplicant MAC Address pull-down menu. The device is now registered as a non-authenticated device on the authenticator port. The device may now forward traffic through the port without providing logon credentials.

6. To modify an address, perform the following steps:

   a. Select the address from the Add Port Auth Supplicant MAC Address pull-down menu.

   b. Click the Apply this MAC Address button.

      The address is displayed in the MAC Address (MAC) fields.

   c. Modify the address.

   d. Click the Add button.

      The address is modified in the Add Port Auth Supplicant MAC Address pull-down menu.

7. To delete selected addresses, perform the following steps:

   a. Select the address from the Add Port Auth Supplicant MAC Address pull-down menu.

   b. Click the Delete button.

      The switch displays a confirmation prompt.

   c. Click OK to delete the address.

8. To delete all of the addresses, perform the following steps:

   a. Click the Delete All button.

      The switch displays a confirmation prompt.

   b. Click OK to delete the addresses.

Disabling Port Authentication on the Ports

To disable port authentication on individual ports, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.
3. In the port table at the bottom of the window, click the dialog box of the port you want to configure. You may configure more than one port at a time.
4. Click the Edit button. To configure all of the ports, click the Edit All Ports button.

   The switch displays the Port Authentication - Port Settings window.
5. Click the Disabled dialog circle at the top of the window.
6. Click the Apply button to implement your changes.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Disabling Port Authentication on the Switch

To disable port authentication on the switch, perform the following procedure:

1. Expand the Security Settings menu in the main menu.
2. Select the Port Authentication option from the Security Settings menu.

   The Security Settings - Port Authentication window is shown in Figure 118 on page 488.
3. Click the Enable Port Auth dialog box in the top section of the window, to remove the check mark.
4. Click the Set button.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Enabling or Disabling EAP Transparency

The switch, at its default settings, discards EAP packets from other network devices if port authentication is disabled. The RADIUS server on your network and the RADIUS client on the switch use EAP packets to accomplish the log on process of clients. In some circumstances, you may want the switch to forward these packets even if it is not using port authentication. You can do this by activating EAP transparency on the switch.

Note
Port authentication must be disabled on the switch before you can enable EAP transparency. For instructions, refer to "Disabling Port Authentication on the Switch" on page 518.

To enable or disable EAP transparency on the switch, perform the following procedure:

1. Expand the Switch Settings menu in the main menu.
2. Select the Others option from the Switch Settings menu.

   The Switch Settings - Others window is shown in Figure 31 on page 138.
3. In the Transparent to EAP Packets section of the window, click the dialog box to enable or disable the EAP transparency feature.

   The feature is enabled when the dialog box has a check mark. The switch forwards EAP packets when the feature is enabled. The feature is disabled when the dialog box is empty. The switch does not forward the packets when the feature is disabled. The default setting is disabled.
4. Click the Apply button to activate your changes on the switch.
5. To permanently save your changes in the configuration file, click the Save button above the main menu.

Chapter 42

Configuration Files

This chapter explains how to manage the configuration files in the file system of the switch. This chapter contains the following procedures:

Introduction

The switch stores its parameter settings in a configuration file in its file system. The switch does not automatically update the file when you configure the parameter settings of a feature. Instead, you have to manually instruct the switch to update the file yourself by clicking the Save button, above the main menu. When you click the button, the switch updates the file with its current parameter settings.

The file system can store more than one configuration file. You might store a history of the parameter settings of the switch in case you need to return the unit to an earlier configuration. However, only one of the configuration files can be active on the switch at one time. This file is referred to as the active configuration file. It is the active configuration file the switch updates when you click the Save button. You may designate which configuration file in the file system is to be the active configuration file.

You may download configuration files from the switch to your management workstation or a network server, as well as upload files back to the switch. You may find this useful in restoring a configuration to a switch, configuring a replacement switch, or transferring the same configuration to different units that are to have similar feature settings.

The web browser interface has two windows for managing configuration files. The first window is the Management - File Management window. In this window you can upload or download configuration files to the switch as well as delete files. Information about this window is found in “Displaying the File Management Window” on page 523. (This window is also used to download new operating system files to the switch, as explained in Chapter 43, “Operating System Files” on page 535.)

The second window is the Management - Configuration File window. This window lets you create new configuration files and designate the active configuration file. For more information, refer to “Displaying the Configuration File Window” on page 525.

Displaying the File Management Window

To display the file management window, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 125.

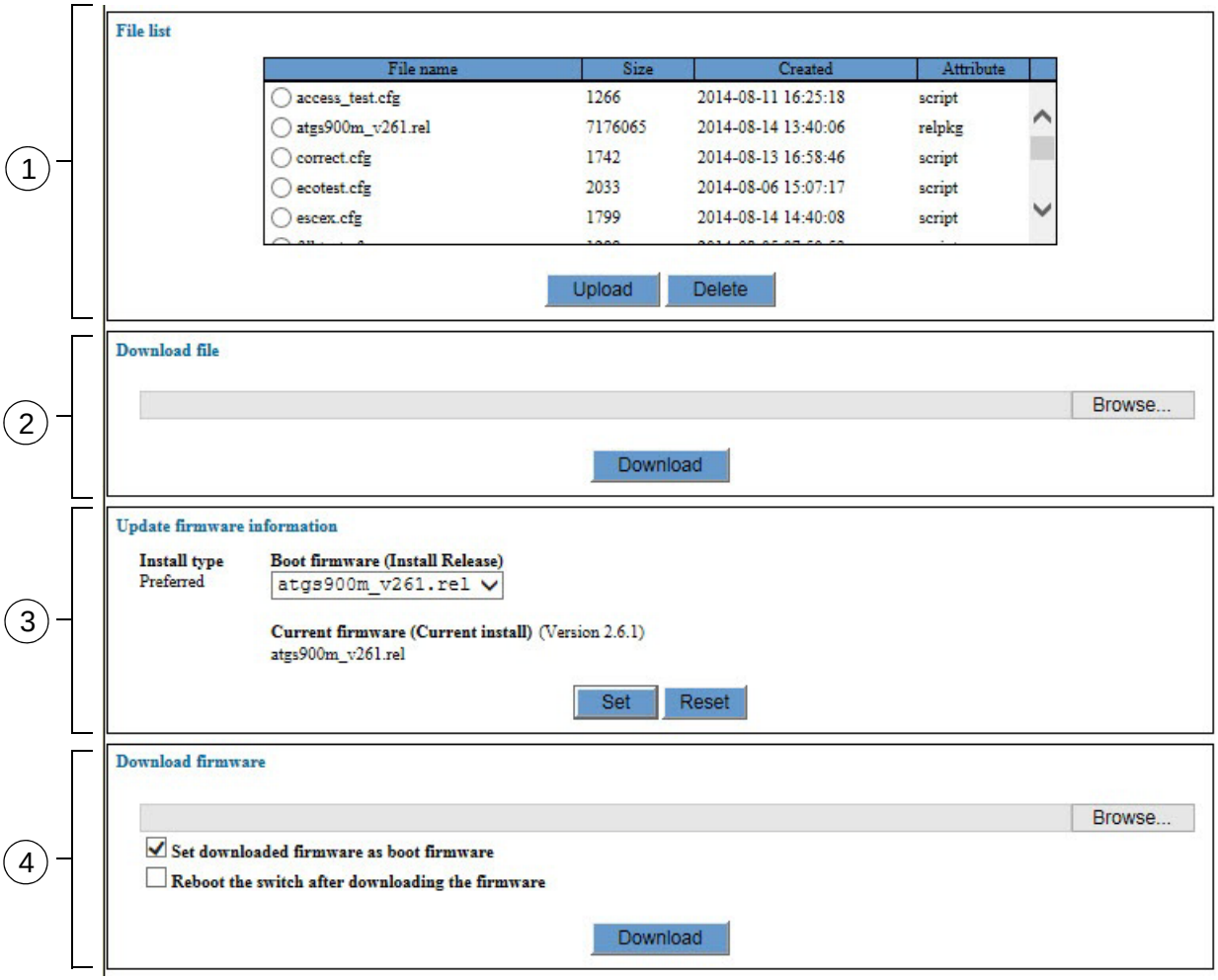

Figure 125. Management - File Management Window

The sections in the window are defined in Table 134 on page 524.

Table 134. Management - File Management Window

Section	Description
1	Use this section of the window to delete configuration files from the file system in the switch or upload configuration files from the switch to your management workstation or a network server. For instructions, refer to “Deleting Configuration Files” on page 532 and “Uploading Configuration Files from the Switch” on page 529. If the switch has two operating system files, you may also use this section to delete the secondary file. For instructions, refer to Chapter 43, “Operating System Files” on page 535.
2	Use this section to download configuration files from your management workstation or network server to the file system in the switch. For instructions, refer to “Downloading Configuration Files to the Switch” on page 530.
3	Use this section to specify the primary (preferred) operating system file for the switch. For instructions, refer to Chapter 43, “Operating System Files” on page 535.
4	Use this section to download a new operating system file for the switch from your management workstation or network server to the file system in the switch. For instructions, refer to Chapter 43, “Operating System Files” on page 535.

Displaying the Configuration File Window

To display the configuration file window, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the Configuration File option from the Management menu.

   The Management - Configuration File window is shown in Figure 126.

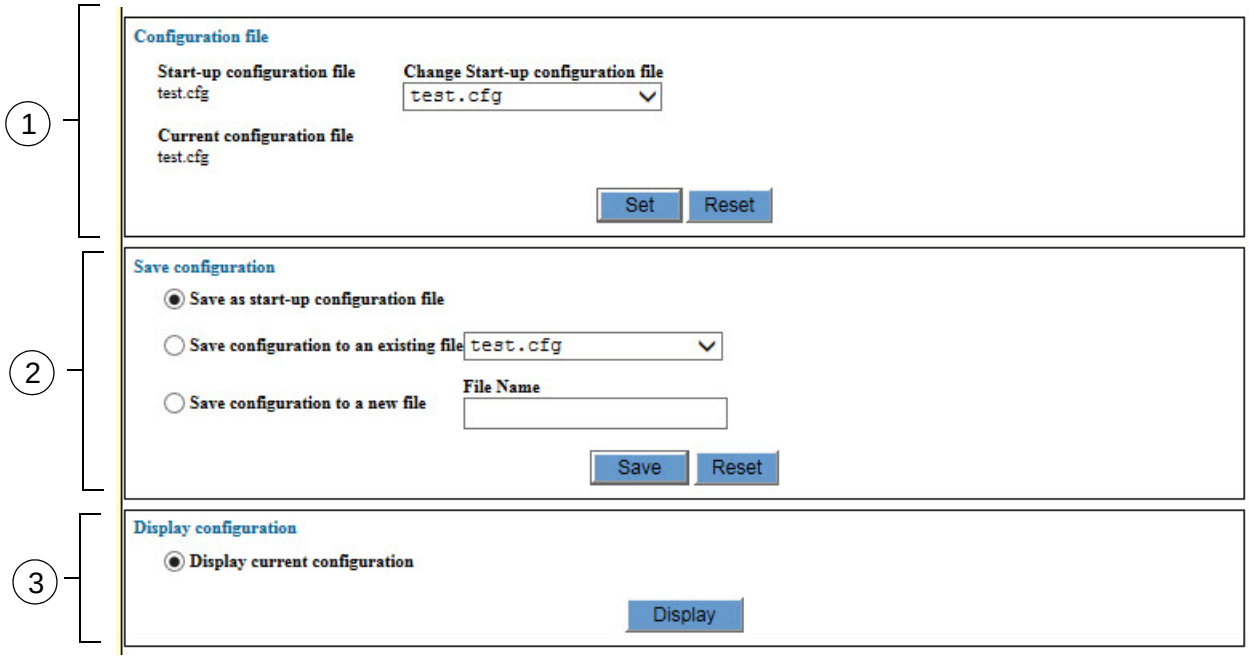

Figure 126. Management - Configuration File Window

The sections in the window are defined in Table 135.

Table 135. Management - Configuration File Window

Section	Description
1	Use this section of the window to designate the active configuration file for the switch. For instructions, refer to “Designating the Active Configuration File” on page 528.
2	Use this section to save the parameter settings to a non-active configuration file or create a new configuration file. For instructions, refer to “Creating a New Configuration File” on page 527.

Table 135. Management - Configuration File Window (Continued)

Section	Description
3	Use this section to display the parameter settings of the switch, in their equivalent command line commands. This selection displays only those parameter settings that have been changed from their default settings. For instructions, refer to “Displaying the Configuration Window” on page 533.

Creating a New Configuration File

To create a new configuration file in which to store the parameter settings of the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the configuration File option from the Management menu.
3. In the Save Configuration section of the window, click the dialog circle of the Save Configuration to a New File option.
4. In the File Name field, enter a name for the new configuration file.

   Here are the guidelines for the filename for a configuration file.

   - ❒ The filename must have the ".cfg" extension.
   - ❒ The filename can be up to twenty characters, including the extension.
   - ❒ Spaces and special characters are not allowed in the filename.

   Filename examples are Sales_switch.cfg and Bldg2_sw4.cfg.
5. Click the Save button.

   The switch adds the new configuration file to the file system and stores its current parameter settings in the file.

   Note
   If you want to designate the new file as the active configuration file on the switch, continue with the next step.

6. In the Configuration File section of the window, select the name of the new configuration file from the pull-down menu for the Change Start-up Configuration File option.

   The pull-down menu displays the names of the configuration files in the file system in the switch. You may select only one configuration file to be the active file.
7. Click the Set button.

   The switch designates the new file as its active configuration file. It now stores the parameter settings in that file whenever you click the Save button above the main menu.

Designating the Active Configuration File

The active configuration file is the configuration file the switch updates in its file system when you click the Save button. You may store more than one configuration file in the file system, but only one file can be the active configuration file at a time.

To designate the active configuration file for the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the Configuration File option from the Management menu.
3. In the Configuration File section of the window, use the pull-down menu in Change Start-up Configuration File option to select the name of the file to be the new active configuration file

   You may choose only one configuration file.
4. Click the Set button.
5. Do one of the following:

   - If you want the switch to reconfigure its parameter settings according to the parameter settings in the new active configuration file, continue with this procedure to reset the switch.

     Note
     Continuing with this procedure is disruptive to network operations because it requires resetting the unit.

   - If you want to overwrite the settings in the new active configuration file with the current settings of the switch, click the Save button above the main menu.
6. From the Management menu, choose the Reboot option.
7. At the confirmation prompt, select OK to reboot the switch or Cancel to cancel the procedure.
8. Wait for the switch to initialize its operating system and configure its parameter settings with the active configuration file.

   At this point the switch is operating with the settings in the new active configuration file.

Uploading Configuration Files from the Switch

This section contains the procedure for uploading configuration files from the file system of the switch to your management workstation or a network server. You might perform this procedure to transfer the configuration of a switch to another switch, or to maintain a history of the configurations of the switch on your management workstation.

To upload configuration files from the file system in the switch to your management workstation or a network server, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 125 on page 523.
3. In the File List section of the window, click the name of the configuration file to be uploaded to your management workstation. You may upload only one file at a time.
4. Click the Upload button.

   The switch displays a confirmation prompt.
5. Click OK to upload the file or Cancel to cancel the procedure.

   If you click OK, the selected configuration file is upload from the switch to your management workstation or network server.

Downloading Configuration Files to the Switch

This section contains the procedure for downloading configuration files from your management workstation or a network server to the file system in the switch. You might perform this procedure to restore an earlier configuration to the switch or to configure the parameter settings of a replacement switch.

To download configuration files from your management workstation or a network server to the file system in the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 125 on page 523.
3. In the Download File section of the window, click the Browse button to locate and select the configuration file stored on your management workstation or network server. You may download only one file at a time.
4. Click the Download button.

   The switch downloads the selected configuration file from your management workstation or network server to the file system in the switch.
5. To confirm the download, check for the name of the file in the File List section of the Management - File Management window.

   Note
   To designate the file as the active configuration file on the switch and to configure the switch with the parameter settings in the file, continue with the next step. This part of the procedure is disruptive to network operations because it requires resetting the unit.
6. Select the Configuration File option from the Management Menu.
7. In the Configuration File section of the window, use the pull-down menu in Change Start-up Configuration File to select the name of the file that you just downloaded onto the switch.
8. Click the Set button.

Note
Do NOT click the Save button. If you do, the switch overwrites the settings in the new configuration file with its current settings.

9. From the Management menu, choose the Reboot option.
10. At the confirmation prompt, select OK to reboot the switch or Cancel to cancel the procedure.
11. Wait for the switch to initialize its operating system and configure its parameter settings with the active configuration file.

    At this point the switch is operating with the settings in the new active configuration file.

Deleting Configuration Files

To delete old or unused configuration files from the file system in the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 125 on page 523.
3. In the File List section of the window, click the name of the configuration file to be deleted. You may delete only one file at a time.
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click OK to delete the file or Cancel to retain it.

   If you click OK, the configuration file is deleted from the file system.

Note
If you delete the active configuration file and reboot the unit without specifying a new active file, the switch restores the default settings to all of the parameter settings.

Displaying the Configuration Window

To display the current configuration of the switch in the equivalent command line commands, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the Configuration File option from the Management menu.

   The Management - Configuration File window is shown in Figure 126 on page 525.
3. Click the display button in the Display Configuration section at the bottom of the window.

   An example of the Configuration window is shown in Figure 127 on page 534. The window displays only those parameters that have been changed from their default values.

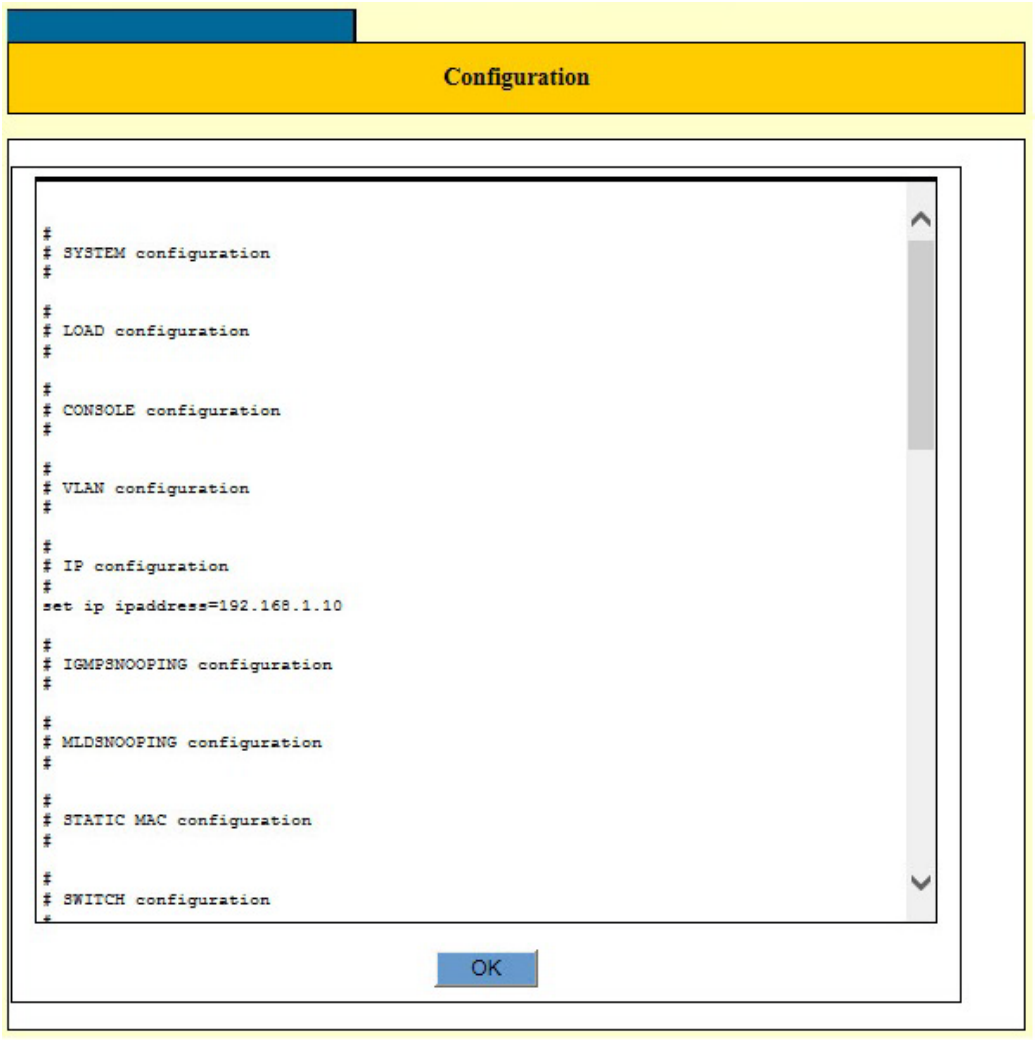

Figure 127. Configuration Window

4. Click the OK button to close the window.

Chapter 43

Operating System Files

This chapter contains instructions on how to manage operating system files. Operating system files contain the management software for the switch. This chapter contains the following procedures:

Introduction

The software operating system for the switch is stored in a file in the file system of the unit. The switch automatically loads its operating system from the file whenever it is reset or powered on.

Allied Telesis may periodically release new operating software for the switch and make it available to our customers on our company web site, as a new operating system file. If you receive a new operating system file, you may download it onto your switch with the instructions in this chapter.

The file system in the switch has sufficient space for two operating software files. A switch that has only one operating software file always uses that file to load its operating system whenever it is reset or powered on.

A switch that has two operating system files in the file system uses one of the files as the primary file and the other is the secondary file. The switch uses the primary file for its operating system and the secondary file only if it encounters a problem with the primary file.

Before you begin to load a new operating system file onto the switch, you should first examine the file system to determine whether there are one or two operating system files. If there are two files, you have to delete one of the files to make room for the new file. (An operating system file can be identified by its “.rel” extension.)

Displaying the File Management Window

To display the file management window, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 128.

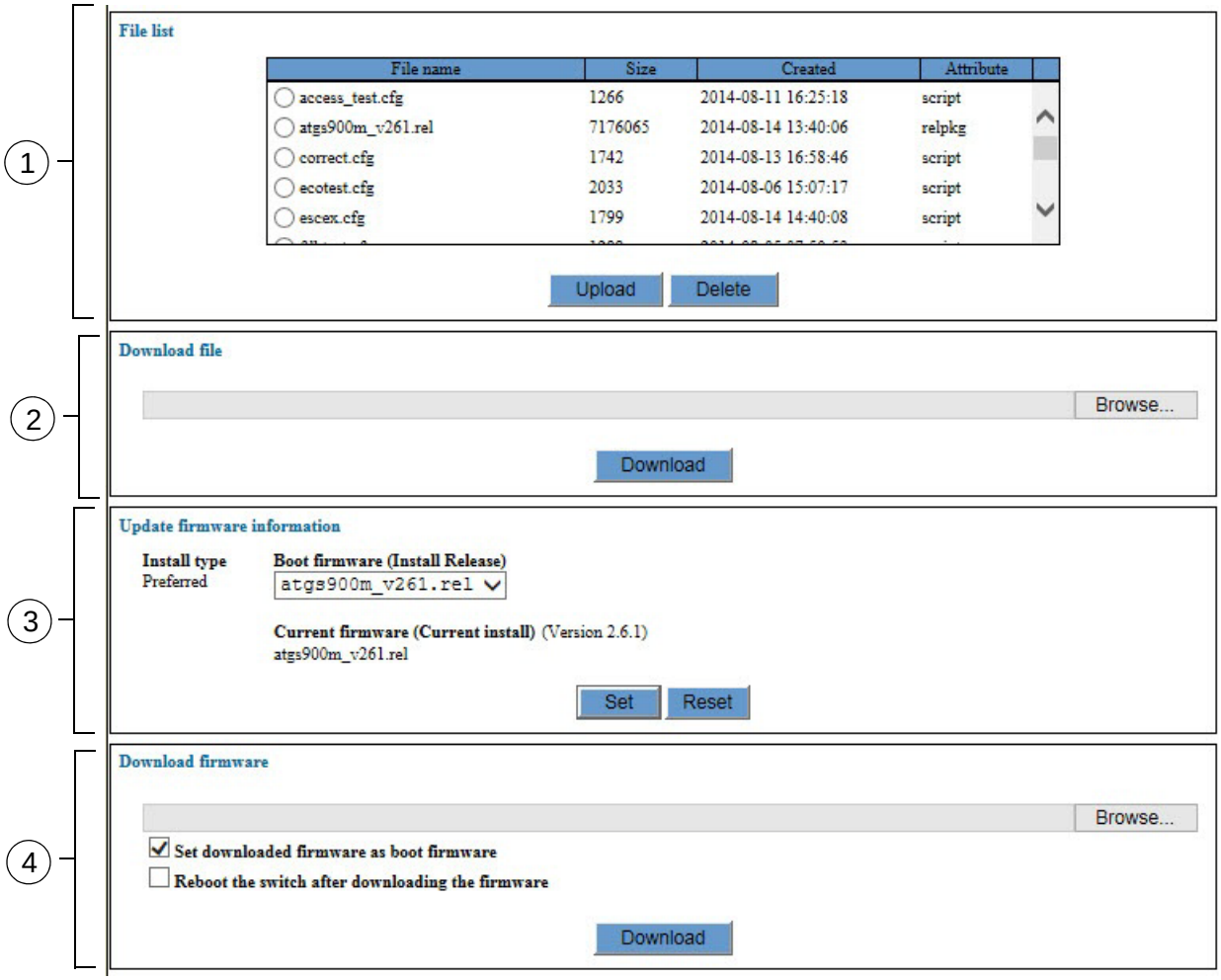

Figure 128. Management - File Management Window

The sections in the window are defined in Table 136 on page 538.

Table 136. Management - File Management Window

Section	Description
1	Use this section of the window to delete operating system files from the file system. For instructions, refer to “Deleting the Secondary Operating System File” on page 539. This section may also be used to delete configuration files or upload configuration files from the switch to your management workstation or a network server. For instructions, refer to Chapter 42, “Configuration Files” on page 521.
2	Use this section to download configuration files from your management workstation or a network server to the switch. For instructions, refer to Chapter 42, “Configuration Files” on page 521.
3	Use this section to specify the active management software on the switch. For instructions, refer to “Designating the Primary Operating System File” on page 542.
4	Use this section to download new firmware to the switch. For instructions, refer to “Downloading a New Operating System File to the Switch” on page 540.

Deleting the Secondary Operating System File

The file system in the switch can store two operating system files. If you want to install a new version of the operating system file on a switch whose file system already contains two files, you have to delete the secondary file to make space for the new file.

> **Note**
> The switch will not allow you to delete the primary operating system file. If you want to retain the secondary file and delete the primary file, you first have to swap the roles of the files, so that the secondary file becomes the primary file. For instructions, refer to "Designating the Primary Operating System File" on page 542.

To delete the secondary operating software file from the file system in the switch, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 128 on page 537.
3. In the File List section of the window, click the name of the secondary operating system file. Operating system files have the ".rel" suffix. (The filename of the primary file is displayed in the Current Firmware field in the Update Firmware Information section of the window.)
4. Click the Delete button.

   The switch displays a confirmation prompt.
5. Click OK to delete the file or Cancel to retain it.

   If you click OK, the secondary operating system file is deleted from the file system in the switch.

Downloading a New Operating System File to the Switch

Allied Telesis may periodically release new firmware for this product and make it available to our customers in an operating system file on our company web site. You may use this procedure to download a new operating system file to the switch.

Note
This procedure is disruptive to network operations because it requires rebooting the switch.

To download a new operating system file from your management workstation or a network server to the switch, perform the following procedure:

1. Obtain the new operating system file for the switch from the Allied Telesis web site or your Allied Telesis sales representative and store it on your management workstation or a network server.
2. Start a web browser management session on the switch.
3. Expand the Management menu in the main menu.
4. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 128 on page 537.
5. In the Download Firmware section of the window, click the Browse button to locate and select the new firmware file on your management workstation or network server.
6. Configure the two download options in the section. The options are described in Table 137 on page 541.

Table 137. Download Firmware Options

Option	Description
Set downloaded firmware as boot firmware	Use this option to control whether you want the new firmware to be the primary operating system file for the switch. The possible settings are listed here: Check mark: A check mark in the dialog box enables the option. The switch downloads the new firmware to its file system and marks it as its primary operating system file. The status of the previous primary file is changed to the secondary file. This is the default setting. No check mark: No check mark disables the option. The switch downloads the new firmware to its file system and marks the file as its secondary operating system file.
Reboot the switch after downloading the firmware	Use this option to control whether the switch is to reboot and begin to use the new operating system file as soon as it downloads it. Check mark: The switch immediately reboots after it downloads the new operating system file, so that it immediately begins to use the firmware. No check mark: The switch downloads the operating system file to its file system but does not reboot. This is the default setting. You might select this option if you want to reboot the switch at a later time.

7. Click the Download button.

   The switch downloads the file from your network and stores it in its file system. Depending on how you configured the options in step 6, the switch might reboot after marking the file as its primary operating system file.

8. If the switch reboots, wait for it to initialize its new operating system software and then start a new web browser management session.

Designating the Primary Operating System File

The switch can have two operating system files in its file system. A switch that has two operating system files uses one of the files as its primary file and the other as the secondary file. The switch uses the primary file for its operating system software whenever it is reset or powered on, and reserves the secondary file for situations where it cannot successfully load the primary file.

The procedure in this section explains how to change the designations of the operating system files, such that the current secondary file becomes the primary file, and the current primary file becomes the secondary file. Here are two situations where you might want to change the designations of the operating system files:

- You might want to designate the secondary file as the new primary file if the current primary file has a problem and you want the switch to stop trying to load it whenever the unit is reset or powered on.
- You might want to designate the secondary file as the primary file if it has a newer version of the operating system than the current primary file. This can happen if you downloaded a newer version of the operating system file to the switch but did not designate it as the primary file during the download procedure.

To designate the secondary operating system file as the primary file, perform the following procedure:

1. Expand the Management menu in the main menu.
2. Select the File Management option from the Management menu.

   The Management - File Management window is shown in Figure 128 on page 537.
3. In the Update Firmware Information section of the window, use the Boot Firmware (Install Release) pull-down menu to select the name of the new primary operating system file for the switch.

   Please note the following information:

   - The pull-down menu should contain no more than two filenames because the file system in the switch cannot store more than two operating system files.
   - The name of the current primary operating system file is displayed under Current Firmware (Current Install).
4. Click the Set button.

Note
At this point, the switch has swapped the roles of the two operating system files. If you want the switch to use the new operating system file, continue with this procedure to reboot the unit.

Note
Continuing with this procedure is disruptive to network operations because it requires rebooting the switch.

5. From the Management menu, choose the Reboot option.
6. At the confirmation prompt, select OK to reboot the switch or Cancel to cancel the procedure.
7. Wait for the switch to initialize its operating system.