FS900M Series

Fast Ethernet Switches

Management Software
Web Browser User’s Guide

613-002073 Rev. A

UCD-SNMP

Net-SNMP

License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd.

to the project since 2001.

An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

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 the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS 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.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

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

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

---- Part 5: Sparta, Inc copyright notice (BSD) -----

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS 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.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

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 Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS 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.

Mathopd

Copyright 1996 - 2004 Michiel Boland. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``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 AUTHOR 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

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

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Figures

Tables

Preface

This guide explains how to use the web browser management interface in the Allied Telesis FS900M Series of Fast Ethernet switches to configure the features and view statistics. The preface contains the following sections:

- ❒ “Safety Symbols Used in this Document” on page 18
- ❒ “Contacting Allied Telesis” on page 19

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 FS900M Series of Fast 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 FS900M Series of Fast Ethernet Switches:

❒ AT-FS909M

❒ AT-FS917M

❒ AT-FS926M

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 25. 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
- Rapid Spanning Tree Protocol (STP compatible)
- Loop Detection Frame
- IGMP v3 Snooping
- MLD v2 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
- 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

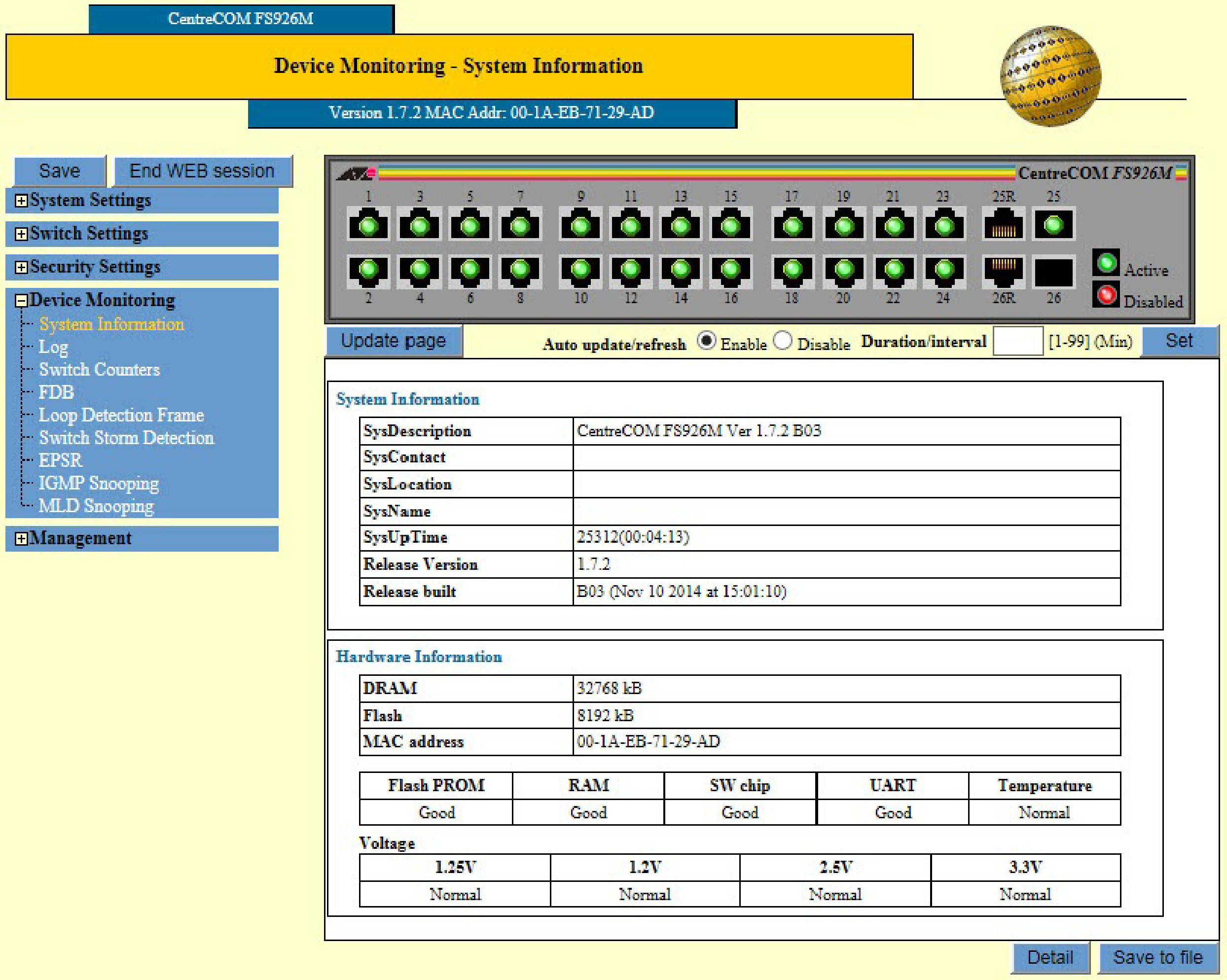
There are several differences between the command line and web browser interfaces. The differences are listed in Table 2.

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.



System Information

SysDescription	CentreCOM FS926M Ver 1.7.2 B03
SysContact	
SysLocation	
SysName	
SysUpTime	25312(00:04:13)
Release Version	1.7.2
Release built	B03 (Nov 10 2014 at 15:01:10)

Hardware Information

DRAM	32768 kB
Flash	8192 kB
MAC address	00-1A-EB-71-29-AD

Flash PROM	RAM	SW chip	UART	Temperature
Good	Good	Good	Good	Normal

Voltage

1.25V	1.2V	2.5V	3.3V
Normal	Normal	Normal	Normal

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 27.

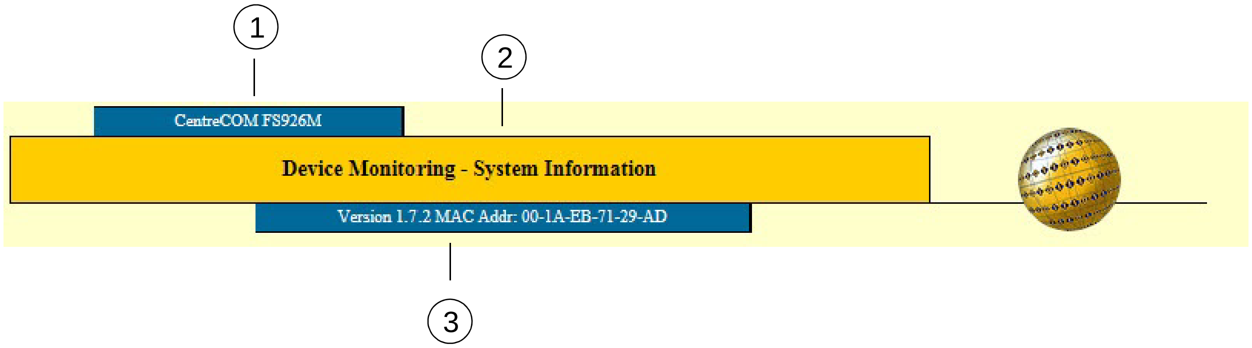

1
2
CentreCOM FS926M
Device Monitoring - System Information
Version 1.7.2 MAC Addr: 00-1A-EB-71-29-AD
3

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 28.

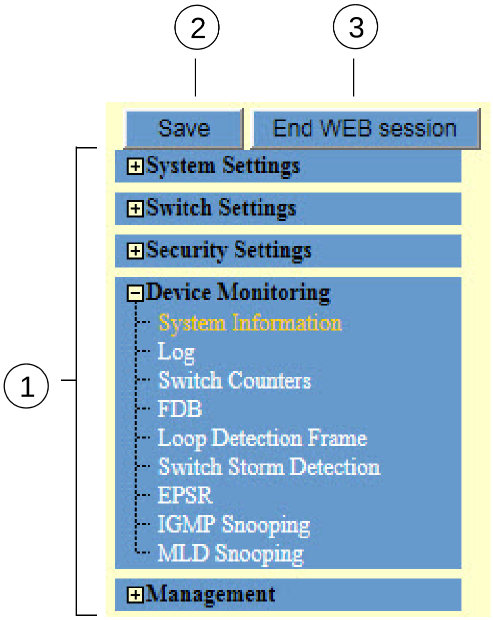


Figure 3. Main Menu

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 30.
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 in the web browser interface of the switch 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

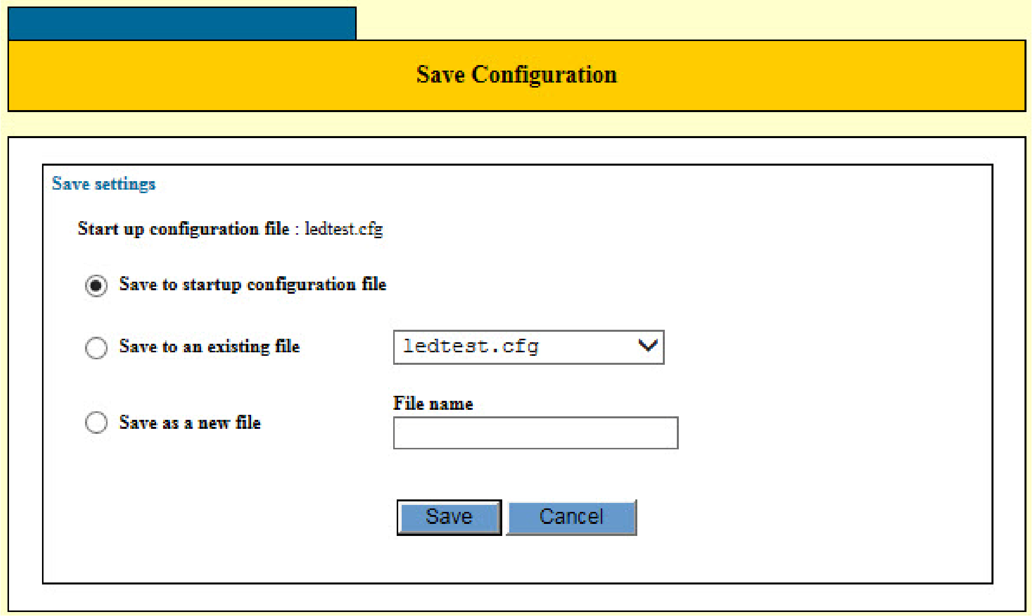
Management windows with adjustable parameters have Apply or Set buttons. After changing a parameter setting of a feature, you have to click one of these buttons to activate your change on the switch. Your changes are not implemented on the switch until you click the buttons.

Save Button

The switch stores its parameter settings in a configuration file in its file system. The file contains the settings of those parameters that have been changed from their default settings. 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 28.)

When you click the Save button, the switch displays the Save Configuration window, shown in Figure 4 on page 30.



Save Configuration

Save settings

Start up configuration file : ledtest.cfg

● Save to startup configuration file

○ Save to an existing file ledtest.cfg

○ Save as a new file File name:

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 likely to use most often.

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 32, “Configuration and Operating System Files” on page 373.

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

Please review the following information before starting a web browser management session on the switch:

- The default setting for the HTTP server on the switch is disabled. You have to enable the server with the ENABLE HTTP SERVER command from the command line interface of a local or Telnet management session before you can manage the switch with a web browser.
- The switch comes with the default IP address 192.168.1.1. You may use the default address for web browser management.

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 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.

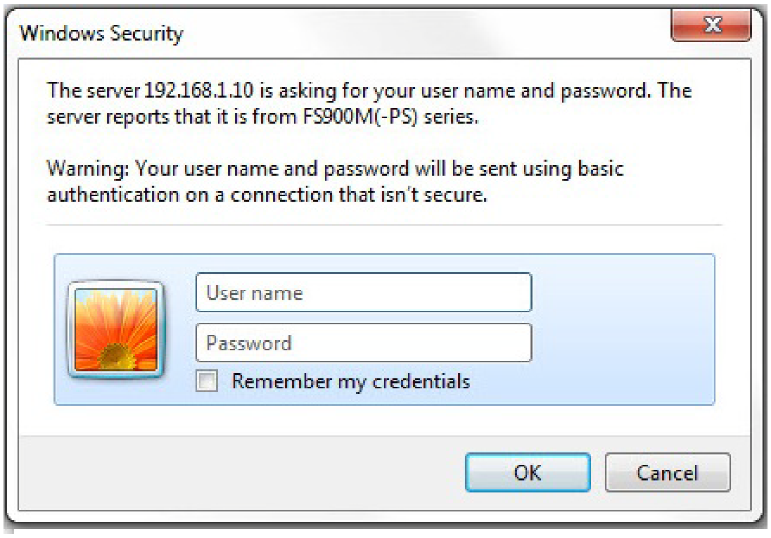
2. Connect the Ethernet network port on your computer to any of the Ethernet ports on the switch.

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 33.



Windows Security

The server 192.168.1.10 is asking for your user name and password. The server reports that it is from FS900M(-PS) series.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

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 26.

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 28. 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

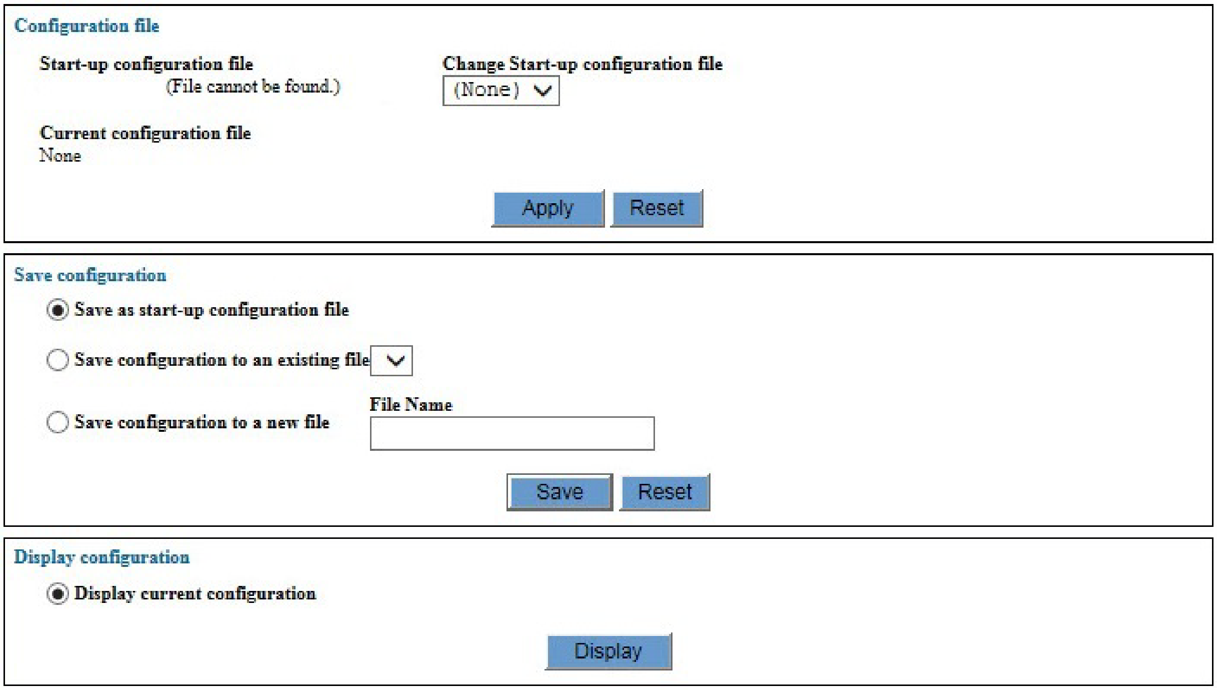
Your first step should be to create a configuration file in the file system of the switch. The device uses the file to store its parameter settings so that you do not have to reenter them when you power off or reset the unit. To create a configuration file, perform the following procedure:

1. Start a web browser management session on the switch. For instructions, refer to “Starting a Management Session” on page 32.

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.



Configuration file

Start-up configuration file
(File cannot be found.)

Change Start-up configuration file
(None)

Current configuration file
None

Save configuration

● Save as start-up configuration file

○ Save configuration to an existing file

○ Save configuration to a new file

File Name

Display configuration

● Display current configuration

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 32, "Configuration and Operating System Files" on page 373.

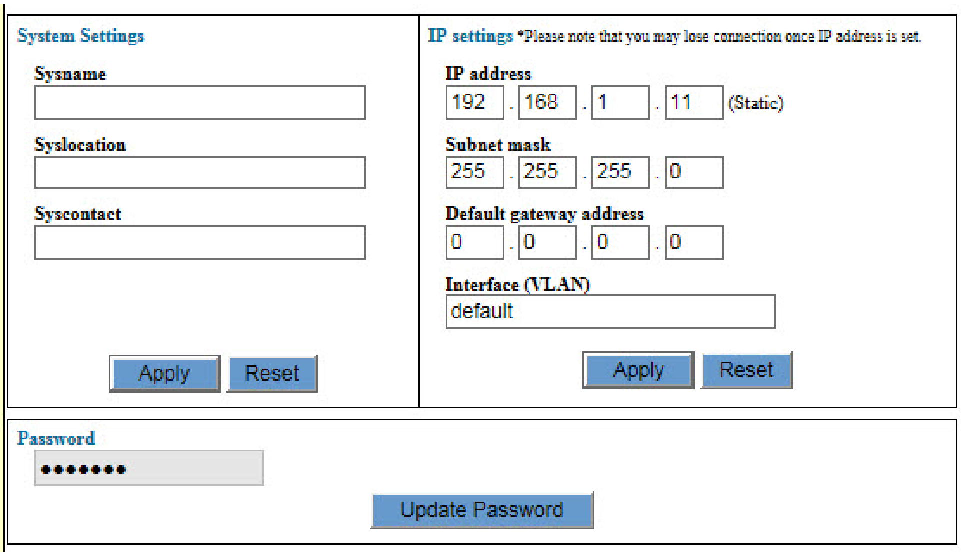
Changing the Manager Password

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.



System Settings

Sysname:

Syslocation:

Syscontact:

IP settings *Please note that you may lose connection once IP address is set.

IP address: 192 . 168 . 1 . 11 (Static)

Subnet mask: 255 . 255 . 255 . 0

Default gateway address: 0 . 0 . 0 . 0

Interface (VLAN): default

Password: •••••••

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.

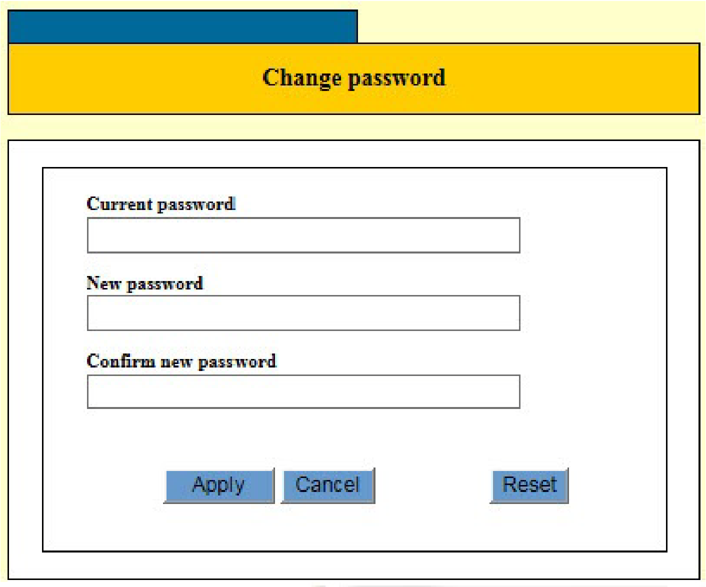


Figure 8. Change Password Window

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.

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.

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.

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

Parameter	Description
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

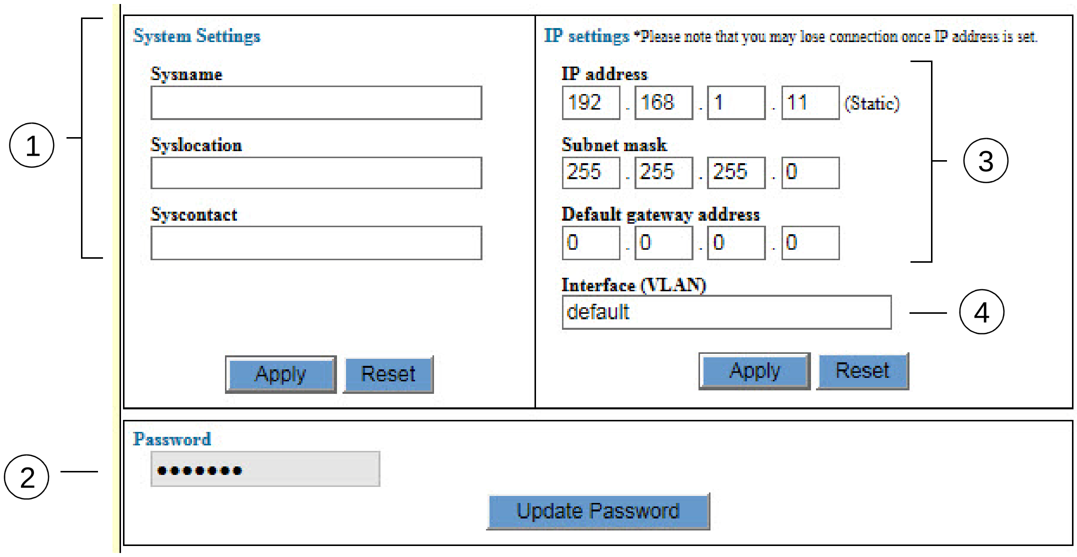
The system window is used to perform the following management tasks:

- 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.

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.



System Settings

Sysname:

Syslocation:

Syscontact:

IP settings *Please note that you may lose connection once IP address is set.

IP address: 192 . 168 . 1 . 11 (Static)

Subnet mask: 255 . 255 . 255 . 0

Default gateway address: 0 . 0 . 0 . 0

Interface (VLAN): default

Password: •••••••

Figure 9. System Settings - System Window

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

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 42.

Table 8. Switch Settings - System Window (Continued)

Section	Description
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 44.
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 46.
4	Use this field to specify the management VLAN on the switch. For instructions, refer to “Specifying the Management VLAN” on page 48.

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 40.

3. Configure the Sysname, Syslocation, and Syscontact parameters in the window in Figure 9 on page 40.

   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 40.

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

   The Password window is shown in Figure 10.

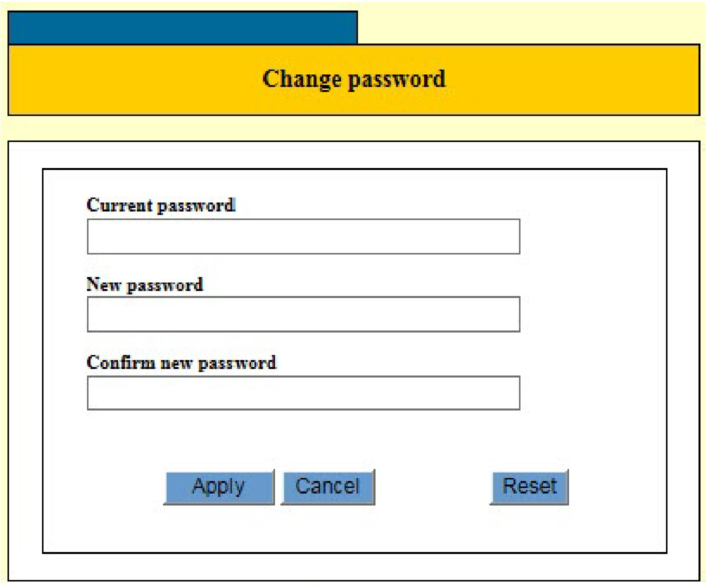


Figure 10. Change Password Window

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-FS900M 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 40.

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 47.

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 14, “Port-based and Tagged VLANs Overview” on page 151 and Chapter 15, “Port-based and Tagged VLANs” on page 165.
- ❒ 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 40.

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.

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.

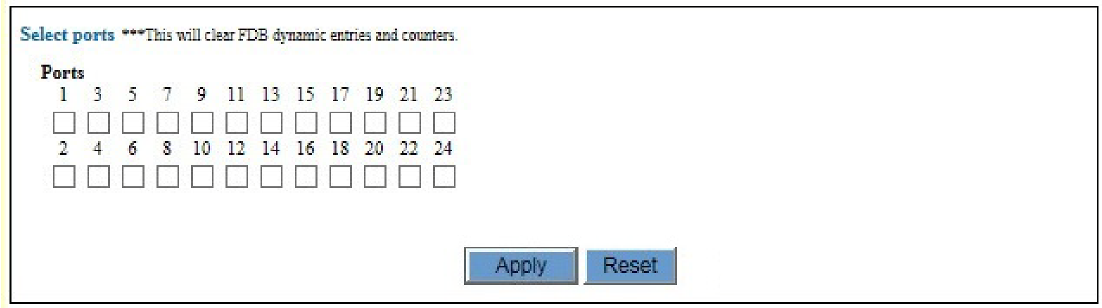
Resetting Ports

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.



Select ports ***This will clear FDB dynamic entries and counters.

Ports

1	3	5	7	9	11	13	15	17	19	21	23
□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24
□	□	□	□	□	□	□	□	□	□	□	□

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

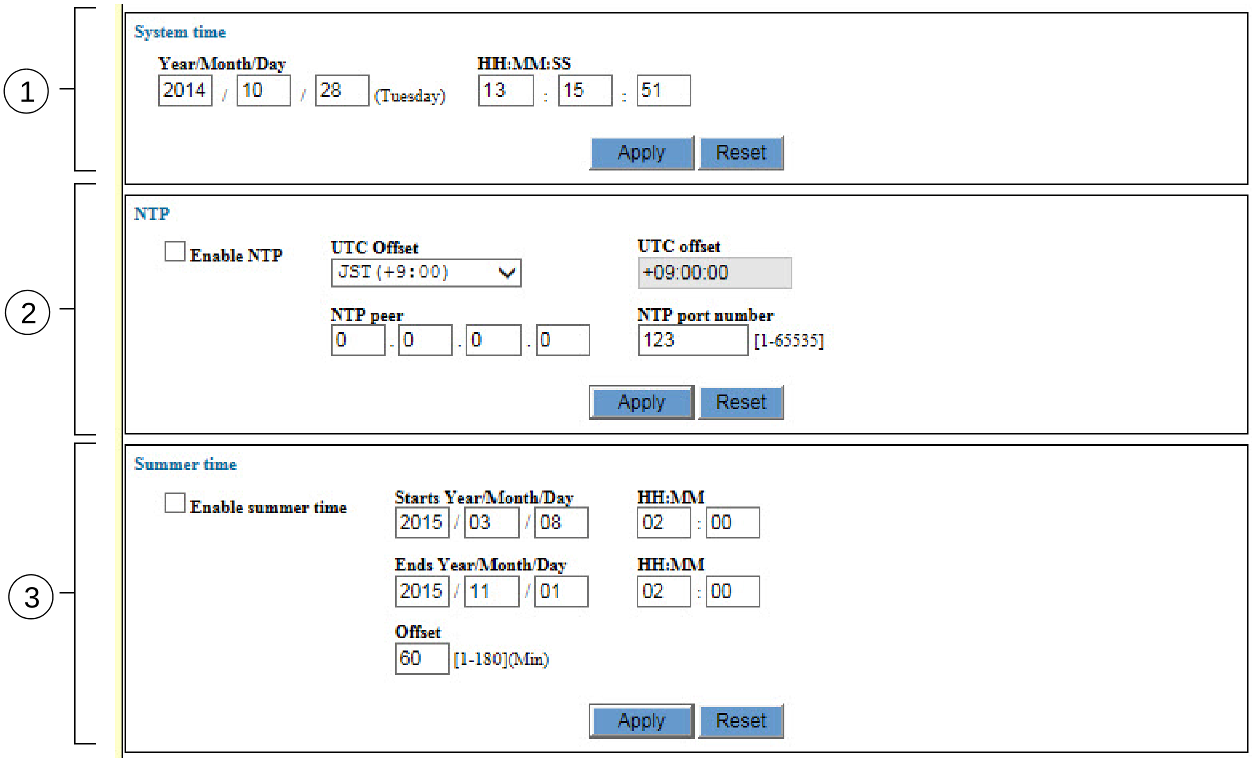
This chapter contains the following sections:

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.



System time

Year/Month/Day 2014 / 10 / 28 (Tuesday)

HH:MM:SS 13 : 15 : 51

NTP

□ Enable NTP

UTC Offset JST (+9:00)

UTC offset +09:00:00

NTP peer 0 . 0 . 0 . 0

NTP port number 123 [1-65535]

Summer time

□ Enable summer time

Starts Year/Month/Day 2015 / 03 / 08

HH:MM 02 : 00

Ends Year/Month/Day 2015 / 11 / 01

HH:MM 02 : 00

Offset 60 [1-180](Min)

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 54.

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 55.
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 57

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 52.

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 46.
- 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 46.
- 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 52.

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 52.

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” on page 60
- “Displaying the Event Log Window” on page 61
- “Configuring the Event Log” on page 63
- “Displaying or Saving the Event Messages in the Event Log” on page 66
- “Deleting Messages in the Event Log” on page 70

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 71.

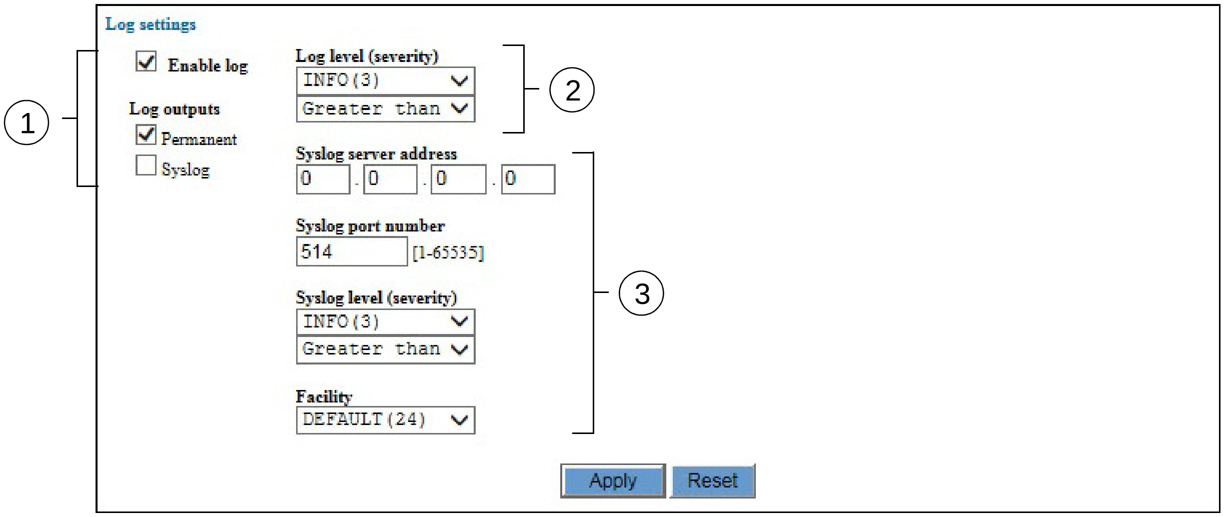
Displaying the Event Log Window

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.



Log settings

☑ Enable log

Log outputs

☑ Permanent

□ Syslog

Log level (severity): INFO(3)

Greater than

Syslog server address: 0 . 0 . 0 . 0

Syslog port number: 514 [1-65535]

Syslog level (severity): INFO(3)

Greater than

Facility: DEFAULT(24)

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 63.
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 63.

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 71.

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 51.

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 61.

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 64.

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 65.

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.

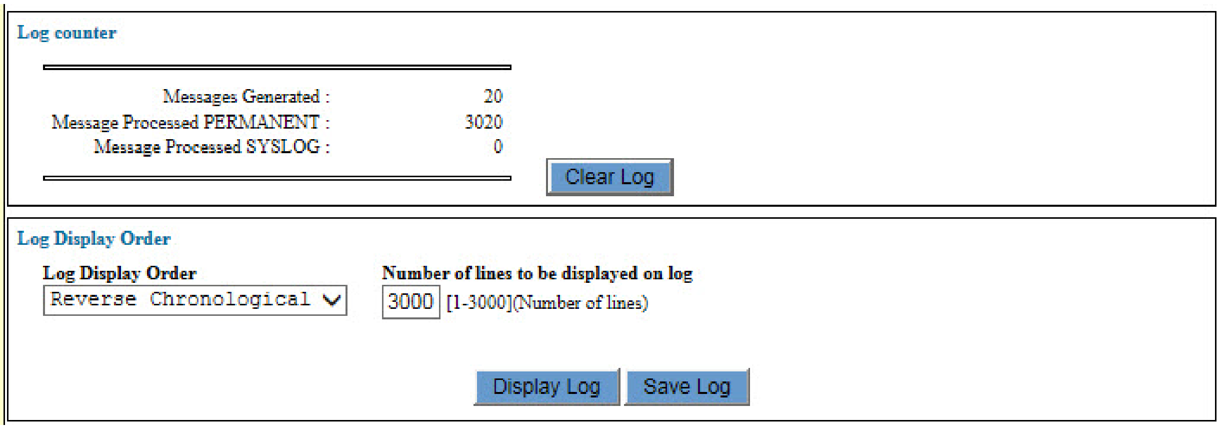
Displaying or Saving the Event Messages in the Event Log

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.



Log counter

Messages Generated : 20
Message Processed PERMANENT : 3020
Message Processed SYSLOG : 0

Log Display Order

Log Display Order: Reverse Chronological
Number of lines to be displayed on log: 3000 [1-3000](Number of lines)

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 63.
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.

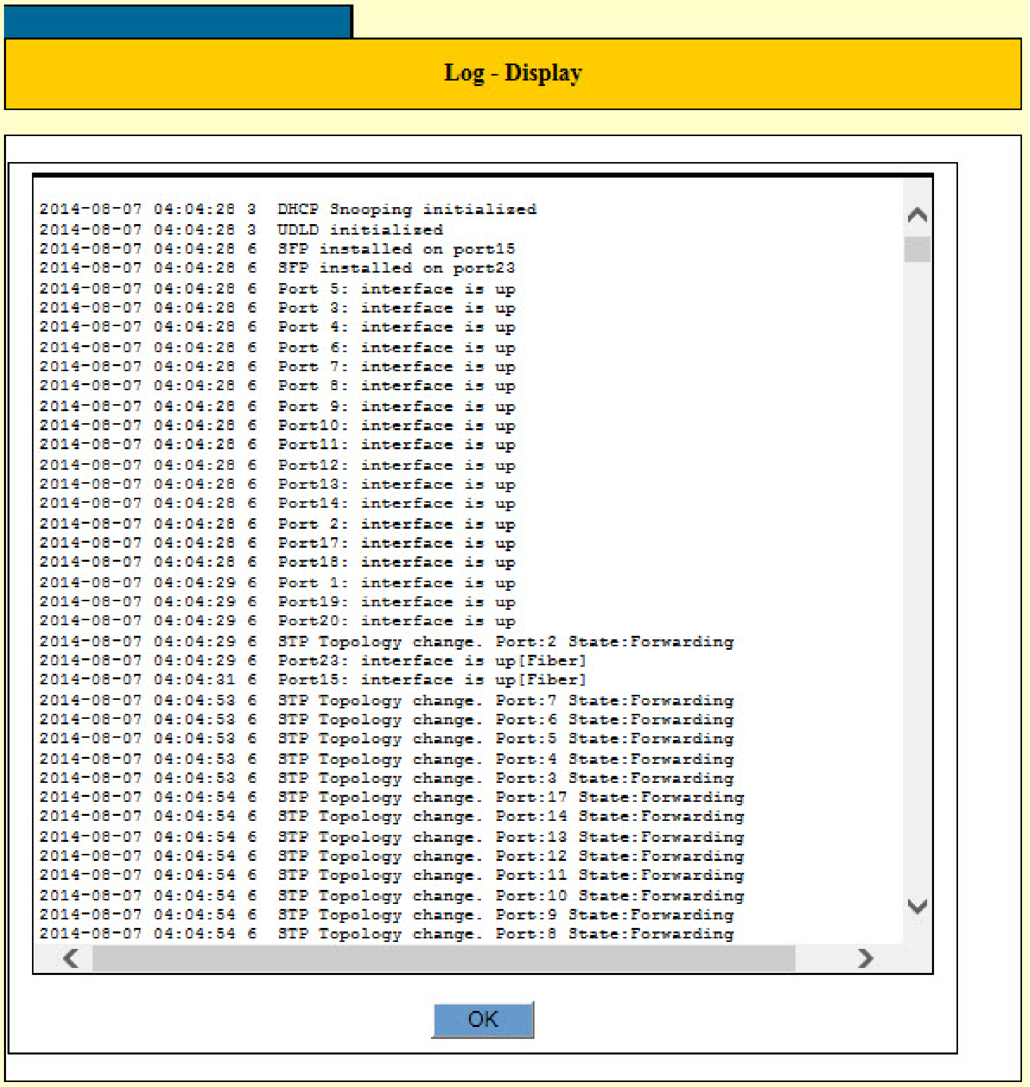
3. Use the Display Order pull-down menu to specify the order in which the messages in the event log are to be displayed on your screen or saved in a file. Your options are listed in Table 20.

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 68.



```
2014-08-07 04:04:28 3  DHCP Snooping initialized
2014-08-07 04:04:28 3  UDLD initialized
2014-08-07 04:04:28 6  SFP installed on port15
2014-08-07 04:04:28 6  SFP installed on port23
2014-08-07 04:04:28 6  Port 5: interface is up
2014-08-07 04:04:28 6  Port 3: interface is up
2014-08-07 04:04:28 6  Port 4: interface is up
2014-08-07 04:04:28 6  Port 6: interface is up
2014-08-07 04:04:28 6  Port 7: interface is up
2014-08-07 04:04:28 6  Port 8: interface is up
2014-08-07 04:04:28 6  Port 9: interface is up
2014-08-07 04:04:28 6  Port10: interface is up
2014-08-07 04:04:28 6  Port11: interface is up
2014-08-07 04:04:28 6  Port12: interface is up
2014-08-07 04:04:28 6  Port13: interface is up
2014-08-07 04:04:28 6  Port14: interface is up
2014-08-07 04:04:28 6  Port 2: interface is up
2014-08-07 04:04:28 6  Port17: interface is up
2014-08-07 04:04:28 6  Port18: interface is up
2014-08-07 04:04:29 6  Port 1: interface is up
2014-08-07 04:04:29 6  Port19: interface is up
2014-08-07 04:04:29 6  Port20: interface is up
2014-08-07 04:04:29 6  STP Topology change. Port:2 State:Forwarding
2014-08-07 04:04:29 6  Port23: interface is up[Fiber]
2014-08-07 04:04:31 6  Port15: interface is up[Fiber]
2014-08-07 04:04:53 6  STP Topology change. Port:7 State:Forwarding
2014-08-07 04:04:53 6  STP Topology change. Port:6 State:Forwarding
2014-08-07 04:04:53 6  STP Topology change. Port:5 State:Forwarding
2014-08-07 04:04:53 6  STP Topology change. Port:4 State:Forwarding
2014-08-07 04:04:53 6  STP Topology change. Port:3 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:17 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:14 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:13 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:12 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:11 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:10 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:9 State:Forwarding
2014-08-07 04:04:54 6  STP Topology change. Port:8 State:Forwarding
```

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 64.
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 66.

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 46.
- 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 46.
- 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 61.

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 stops 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 64. 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 65.
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 alert

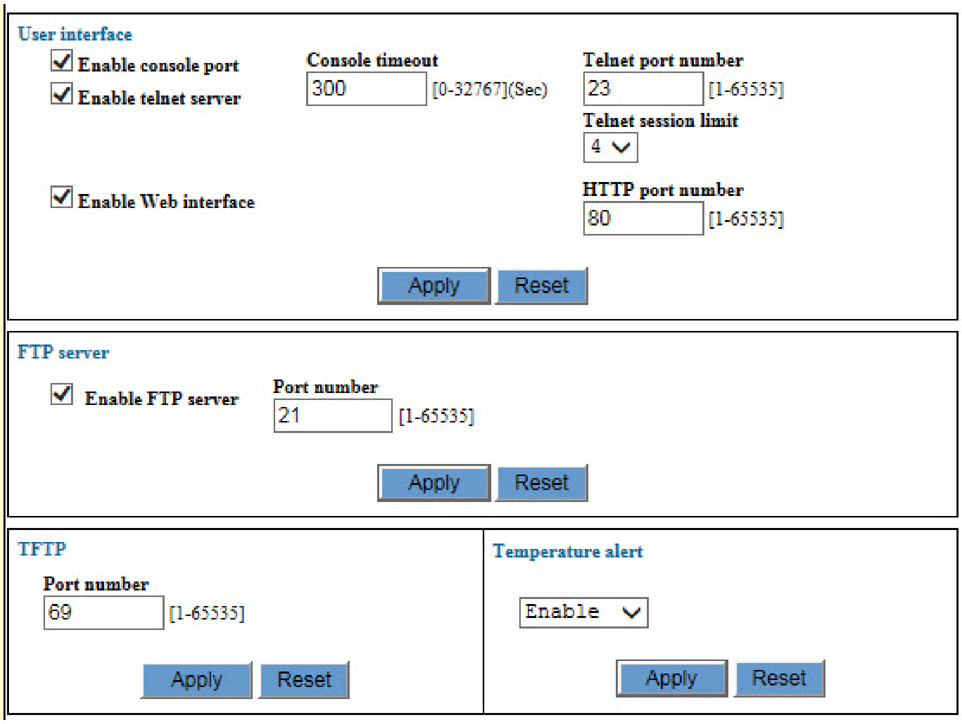
Configuring the Management Tools and Alerts

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.



User interface

☑ Enable console port

☑ Enable telnet server

Console timeout: 300 [0-32767](Sec)

Telnet port number: 23 [1-65535]

Telnet session limit: 4

☑ Enable Web interface

HTTP port number: 80 [1-65535]

FTP server

☑ Enable FTP server

Port number: 21 [1-65535]

TFTP

Port number: 69 [1-65535]

Temperature alert: Enable

Figure 16. System Settings - Others Window

The parameters in the window are defined in Table 24 on page 80.

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 Interface	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	
Temperature Alert	Use this option to enable or disable the temperature alert. When the alert is enabled, the switch sends a trap if the internal temperature of the unit exceeds 40° C.

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” on page 84

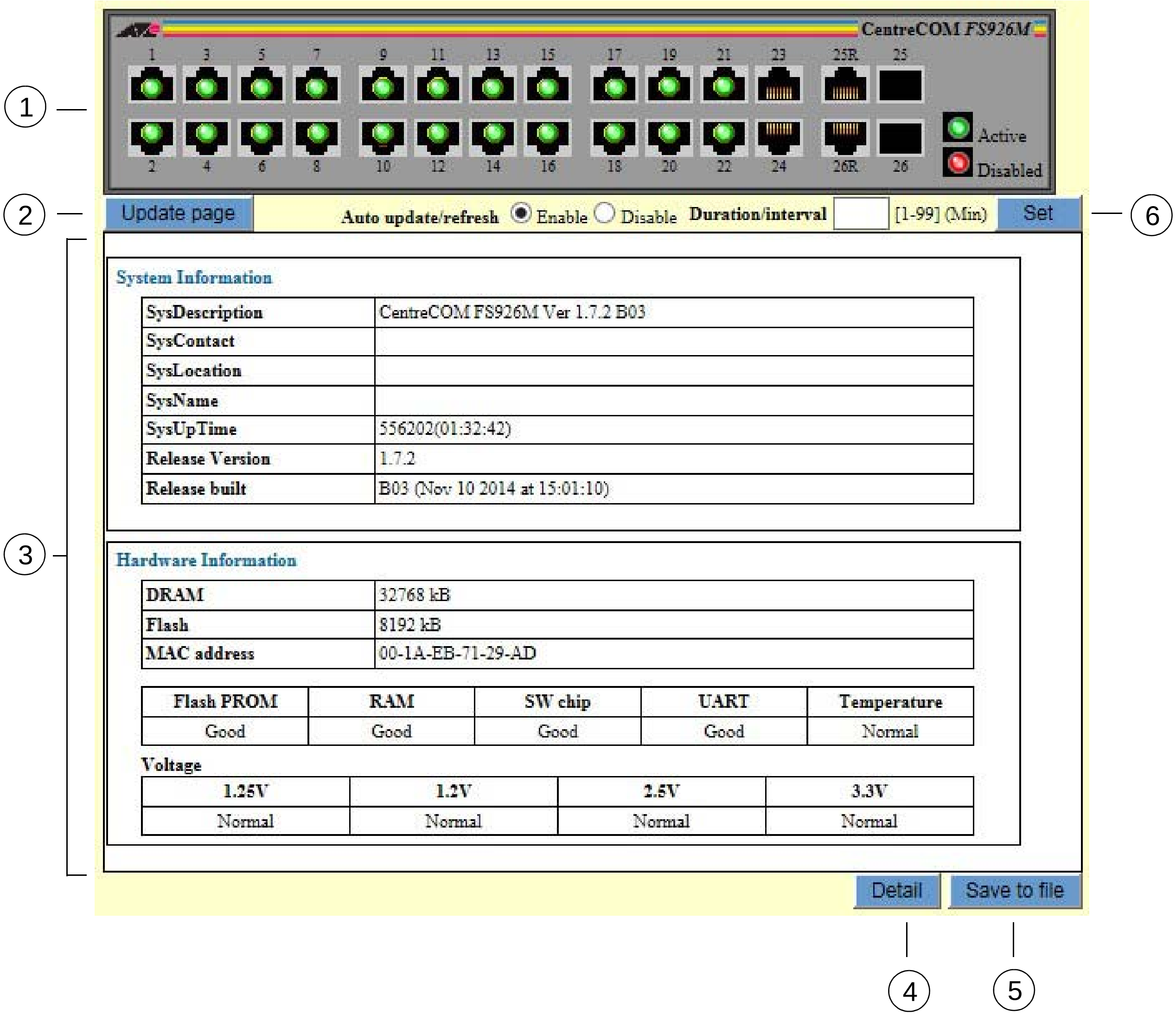
❒ “Displaying Statistics Counters” on page 89

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.



Auto update/refresh ● Enable ○ Disable Duration/interval [1-99] (Min)

System Information

SysDescription	CentreCOM FS926M Ver 1.7.2 B03
SysContact	
SysLocation	
SysName	
SysUpTime	556202(01:32:42)
Release Version	1.7.2
Release built	B03 (Nov 10 2014 at 15:01:10)

Hardware Information

DRAM	32768 kB
Flash	8192 kB
MAC address	00-1A-EB-71-29-AD

Flash PROM	RAM	SW chip	UART	Temperature
Good	Good	Good	Good	Normal

Voltage

1.25V	1.2V	2.5V	3.3V
Normal	Normal	Normal	Normal

Figure 17. Device Monitoring - System Information Window

The sections in the window are defined in Table 25.

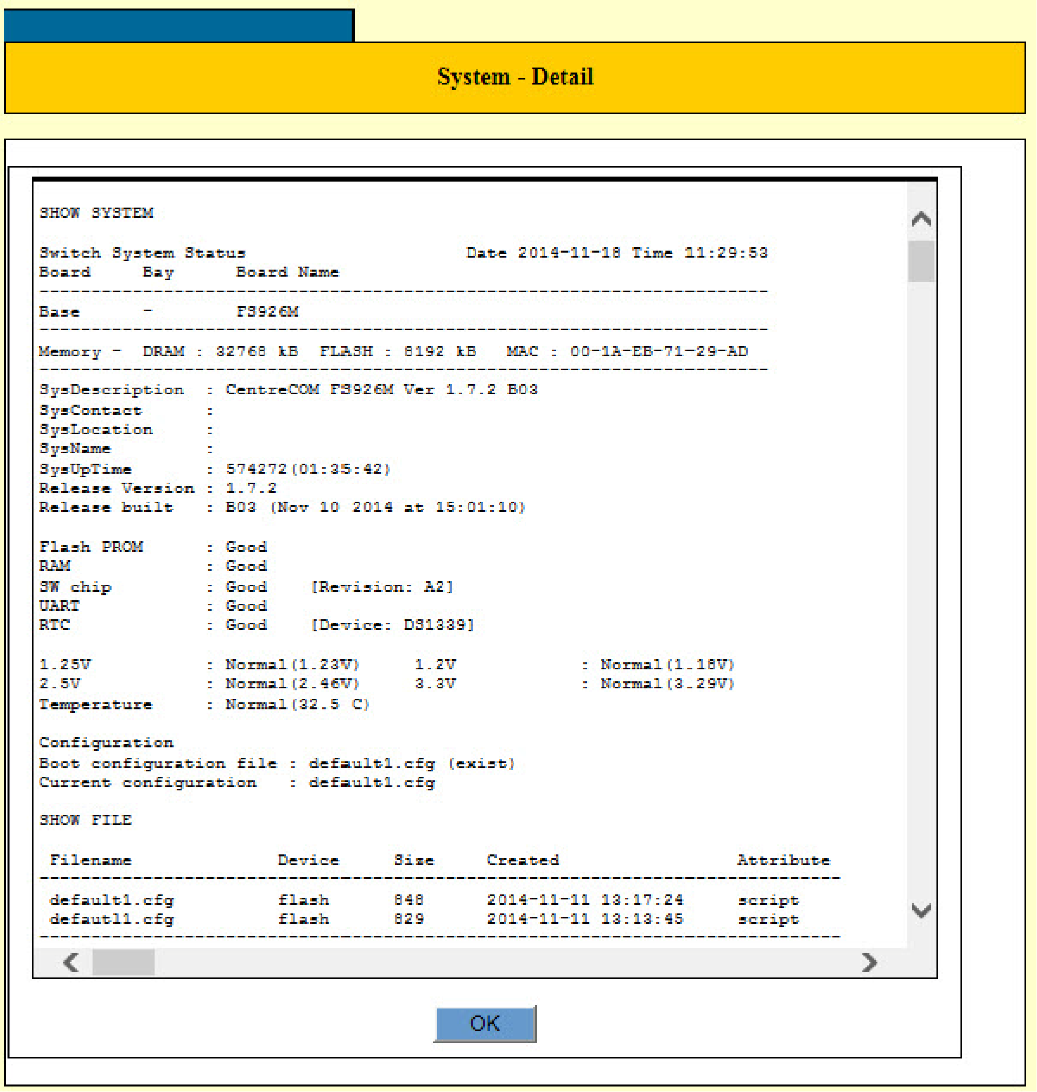
Table 25. Device Monitoring - System Information Window

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 87.
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 85.
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 86.
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 88.

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 86.

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



```
SHOW SYSTEM

Switch System Status                     Date 2014-11-18 Time 11:29:53
Board     Bay      Board Name
----------------------------------------------------------------------
Base      -        FS926M
----------------------------------------------------------------------
Memory -  DRAM : 32768 kB  FLASH : 8192 kB   MAC : 00-1A-EB-71-29-AD
----------------------------------------------------------------------
SysDescription  : CentreCOM FS926M Ver 1.7.2 B03
SysContact      :
SysLocation     :
SysName         :
SysUpTime       : 574272(01:35:42)
Release Version : 1.7.2
Release built   : B03 (Nov 10 2014 at 15:01:10)

Flash PROM      : Good
RAM             : Good
SW chip         : Good    [Revision: A2]
UART            : Good
RTC             : Good    [Device: DS1339]

1.25V           : Normal(1.23V)     1.2V            : Normal(1.18V)
2.5V            : Normal(2.46V)     3.3V            : Normal(3.29V)
Temperature     : Normal(32.5 C)

Configuration
Boot configuration file : default1.cfg (exist)
Current configuration   : default1.cfg

SHOW FILE

 Filename              Device     Size     Created                 Attribute
-----------------------------------------------------------------------------
 default1.cfg          flash      848      2014-11-11 13:17:24     script
 defautl1.cfg          flash      829      2014-11-11 13:13:45     script
-----------------------------------------------------------------------------
```

Figure 18. System - Detail Window

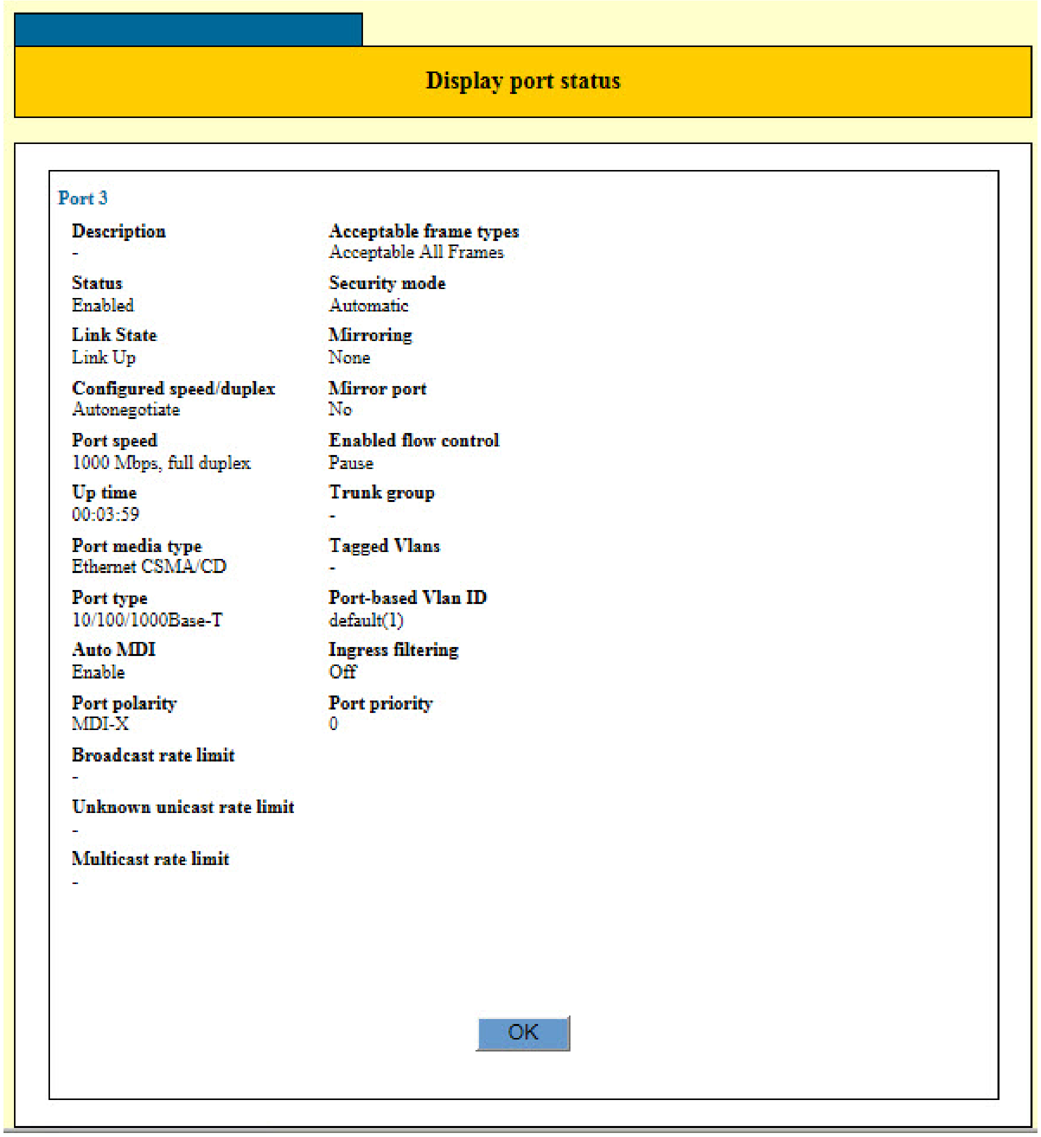
Save to File Button

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 34 on page 114.



Port 3

Description
-

Status
Enabled

Link State
Link Up

Configured speed/duplex
Autonegotiate

Port speed
1000 Mbps, full duplex

Up time
00:03:59

Port media type
Ethernet CSMA/CD

Port type
10/100/1000Base-T

Auto MDI
Enable

Port polarity
MDI-X

Broadcast rate limit
-

Unknown unicast rate limit
-

Multicast rate limit
-

Acceptable frame types
Acceptable All Frames

Security mode
Automatic

Mirroring
None

Mirror port
No

Enabled flow control
Pause

Trunk group
-

Tagged Vlans
-

Port-based Vlan ID
default(1)

Ingress filtering
Off

Port priority
0

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.

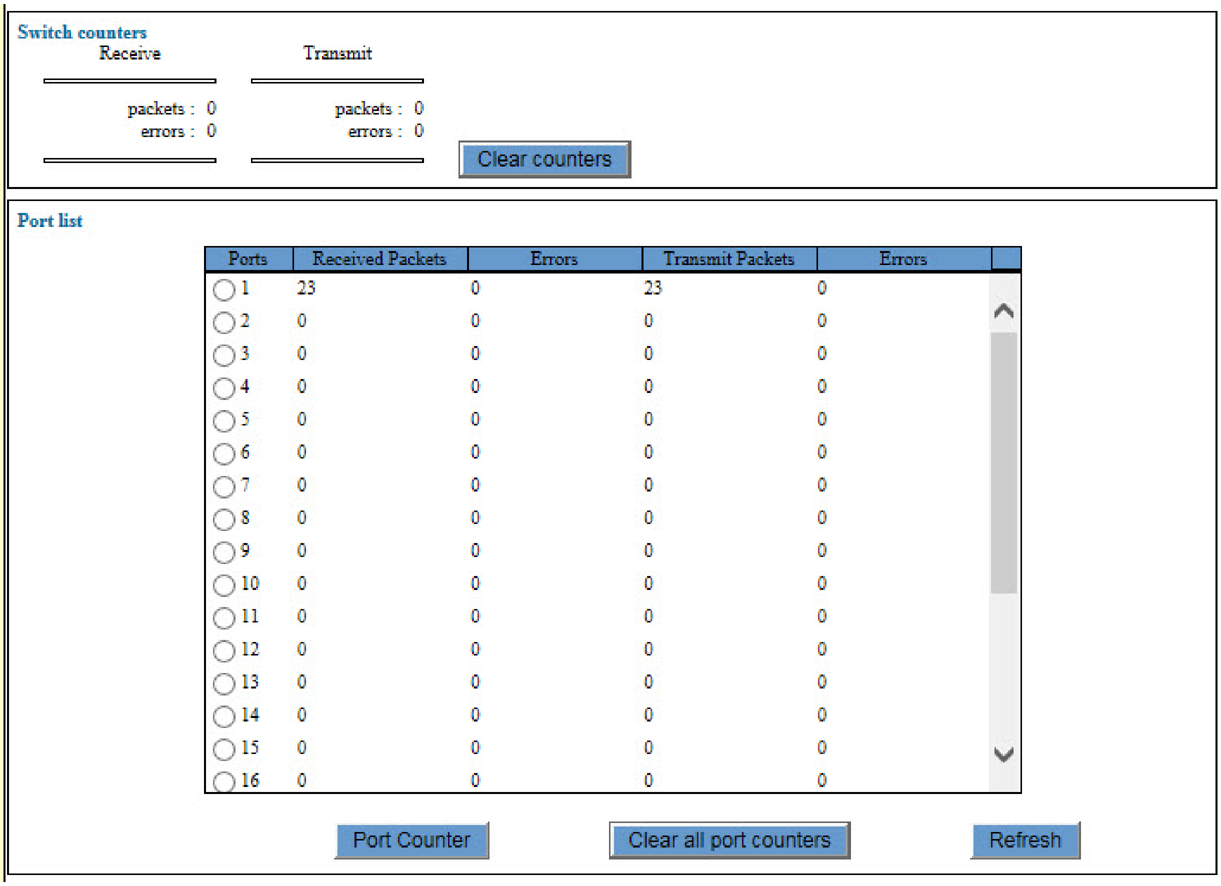
Table 26. Automatic Refresh Option in the Device Monitoring

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.



Switch counters

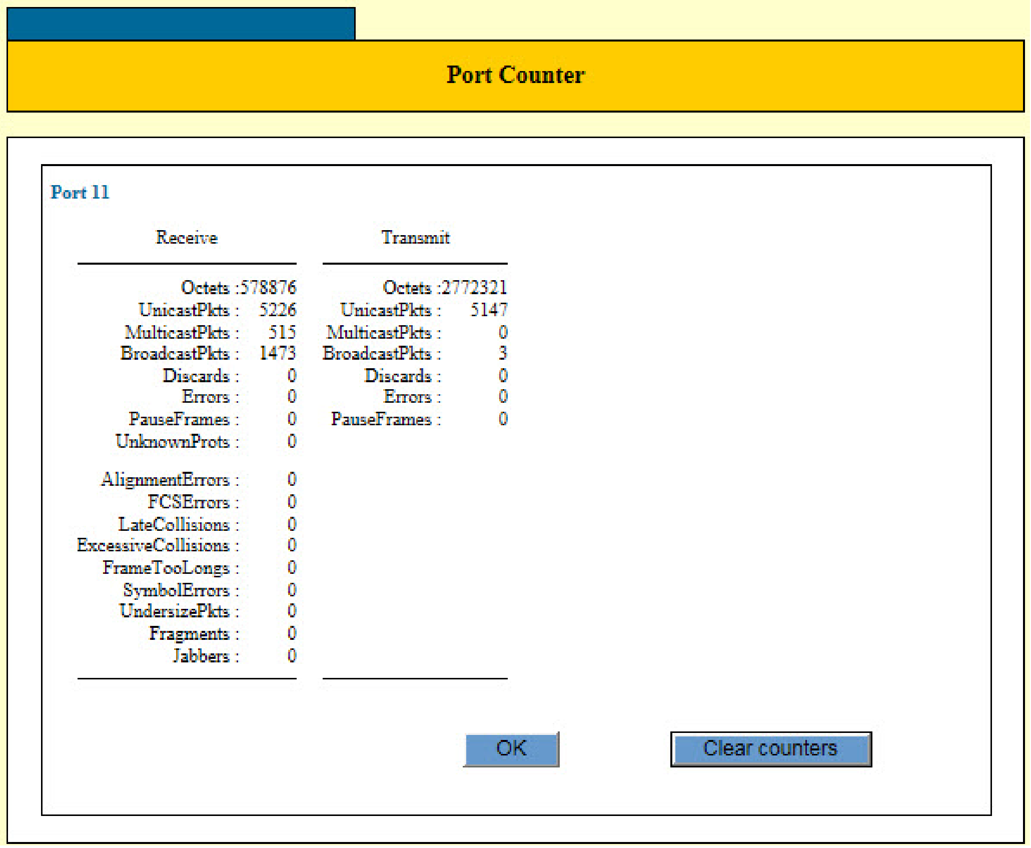
	Receive	Transmit
packets :	0	0
errors :	0	0

Port list

Ports	Received Packets	Errors	Transmit Packets	Errors
○ 1	23	0	23	0
○ 2	0	0	0	0
○ 3	0	0	0	0
○ 4	0	0	0	0
○ 5	0	0	0	0
○ 6	0	0	0	0
○ 7	0	0	0	0
○ 8	0	0	0	0
○ 9	0	0	0	0
○ 10	0	0	0	0
○ 11	0	0	0	0
○ 12	0	0	0	0
○ 13	0	0	0	0
○ 14	0	0	0	0
○ 15	0	0	0	0
○ 16	0	0	0	0

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 90.



Port Counter

Port 11

Receive		Transmit	
Octets :	578876	Octets :	2772321
UnicastPkts :	5226	UnicastPkts :	5147
MulticastPkts :	515	MulticastPkts :	0
BroadcastPkts :	1473	BroadcastPkts :	3
Discards :	0	Discards :	0
Errors :	0	Errors :	0
PauseFrames :	0	PauseFrames :	0
UnknownProts :	0		
AlignmentErrors :	0		
FCSErrors :	0		
LateCollisions :	0		
ExcessiveCollisions :	0		
FrameTooLongs :	0		
SymbolErrors :	0		
UndersizePkts :	0		
Fragments :	0		
Jabbers :	0		

Figure 21. Port Counter Window

Chapter 8

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 sections:

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 46.
- ❒ 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.

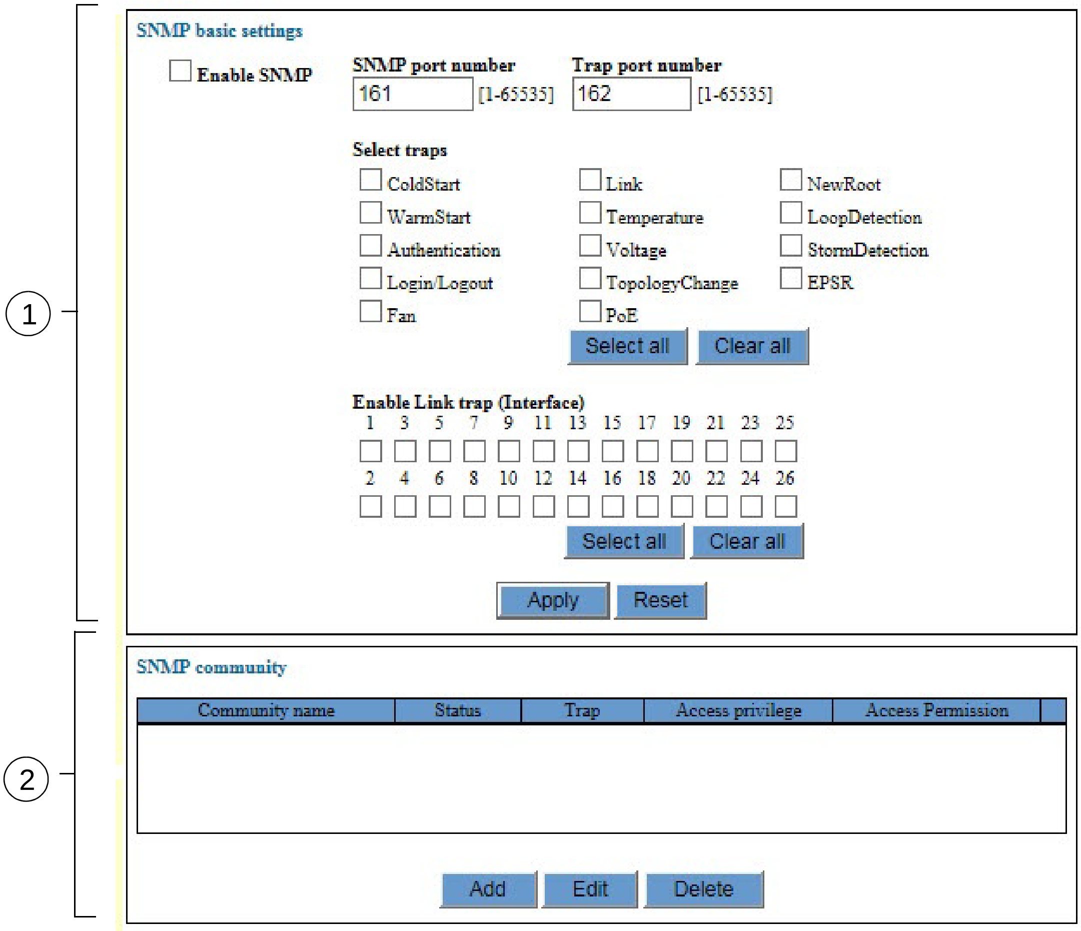
Displaying the SNMP Window

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 22.



SNMP basic settings

□ Enable SNMP

SNMP port number: 161 [1-65535]

Trap port number: 162 [1-65535]

Select traps

□ ColdStart □ Link □ NewRoot
□ WarmStart □ Temperature □ LoopDetection
□ Authentication □ Voltage □ StormDetection
□ Login/Logout □ TopologyChange □ EPSR
□ Fan □ PoE

Enable Link trap (Interface)

1	3	5	7	9	11	13	15	17	19	21	23	25
□	□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24	26
□	□	□	□	□	□	□	□	□	□	□	□	□

SNMP community

Community name	Status	Trap	Access privilege	Access Permission

Figure 22. System Settings - SNMP Window

The sections in the window are described in Table 27.

Table 27. 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 28.

Table 28. 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.

Table 28. SNMP Community Table (Continued)

Column	Description
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.
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 22 on page 93.

3. Configure the parameters in the SNMP Basic Settings section of the window. The parameters are described in Table 29.

Table 29. 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

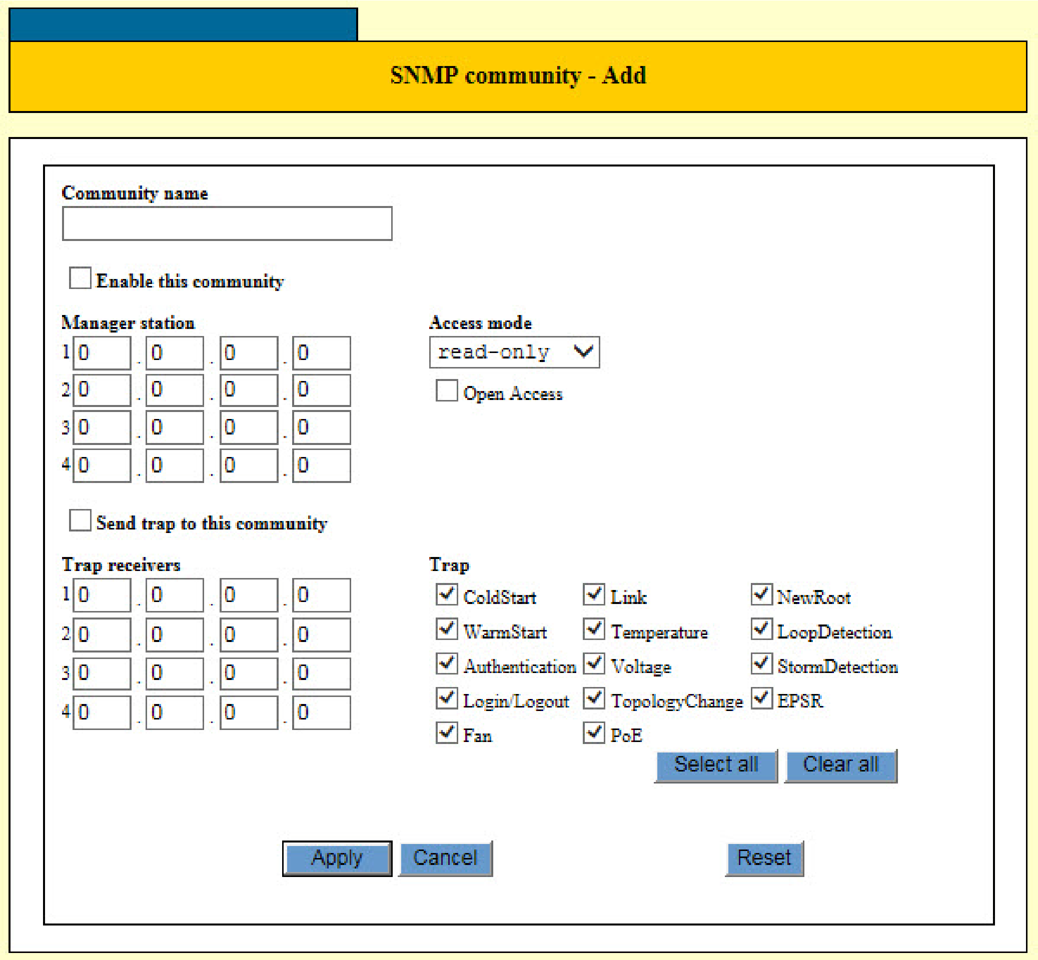
To add new SNMP community strings, perform the following procedure:

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 22 on page 93.

3. Click the Add button at the bottom of the window.

   The SNMP Community - Add window is shown in Figure 23.



SNMP community - Add

Community name

☐ Enable this community

Manager station

1 0 . 0 . 0 . 0
2 0 . 0 . 0 . 0
3 0 . 0 . 0 . 0
4 0 . 0 . 0 . 0

Access mode: read-only

☐ Open Access

☐ Send trap to this community

Trap receivers

1 0 . 0 . 0 . 0
2 0 . 0 . 0 . 0
3 0 . 0 . 0 . 0
4 0 . 0 . 0 . 0

Trap

☑ ColdStart ☑ Link ☑ NewRoot
☑ WarmStart ☑ Temperature ☑ LoopDetection
☑ Authentication ☑ Voltage ☑ StormDetection
☑ Login/Logout ☑ TopologyChange ☑ EPSR
☑ Fan ☑ PoE

Figure 23. SNMP Community - Add Window

4. Configure the parameters in the window for the new community. The parameters are described in Table 30 on page 98.

Table 30. 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 disable 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 30. 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 22 on page 93.

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 22 on page 93.
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 parameters are defined in Table 30 on page 98. 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 22 on page 93.

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 9

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” on page 104
- “Configuring Port Parameters” on page 107
- “Displaying Port Configurations” on page 113

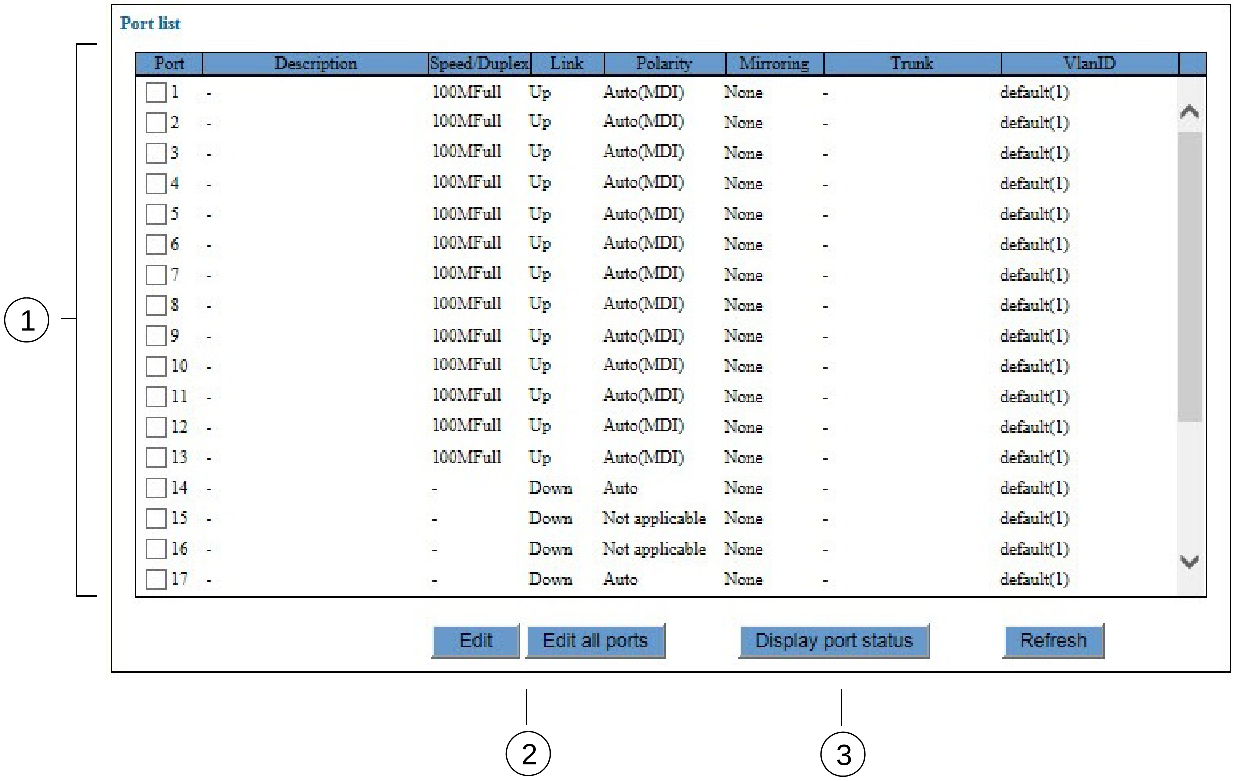
Displaying the Port Parameters Window

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 24.



Port list

Port	Description	Speed/Duplex	Link	Polarity	Mirroring	Trunk	VlanID
□ 1	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 2	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 3	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 4	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 5	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 6	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 7	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 8	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 9	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 10	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 11	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 12	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 13	-	100MFull	Up	Auto(MDI)	None	-	default(1)
□ 14	-	-	Down	Auto	None	-	default(1)
□ 15	-	-	Down	Not applicable	None	-	default(1)
□ 16	-	-	Down	Not applicable	None	-	default(1)
□ 17	-	-	Down	Auto	None	-	default(1)

Figure 24. Switch Settings - Port Window

The sections in the window are described in Table 31.

Table 31. Switch Settings - Port Window

Section	Description
1	Use the table to view the operational status of the ports. The columns are defined in Table 32 on page 105.

Table 31. Switch Settings - Port Window (Continued)

Section	Description
2	Use the buttons to configure the settings of the ports. For instructions, refer to “Configuring Port Parameters” on page 107.
3	Use this button to view port configurations. Refer to “Displaying Port Configurations” on page 113.

The current operational states of the ports are displayed in the Port List table in the window. The columns in the table are described in Table 32.

Table 32. 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 some 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 32. 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 12, “Port Mirroring” on page 135. 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 13, “Static Port Trunks” on page 141.
VlanID	Displays the name and VID of the VLAN where a port is an untagged member.

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.

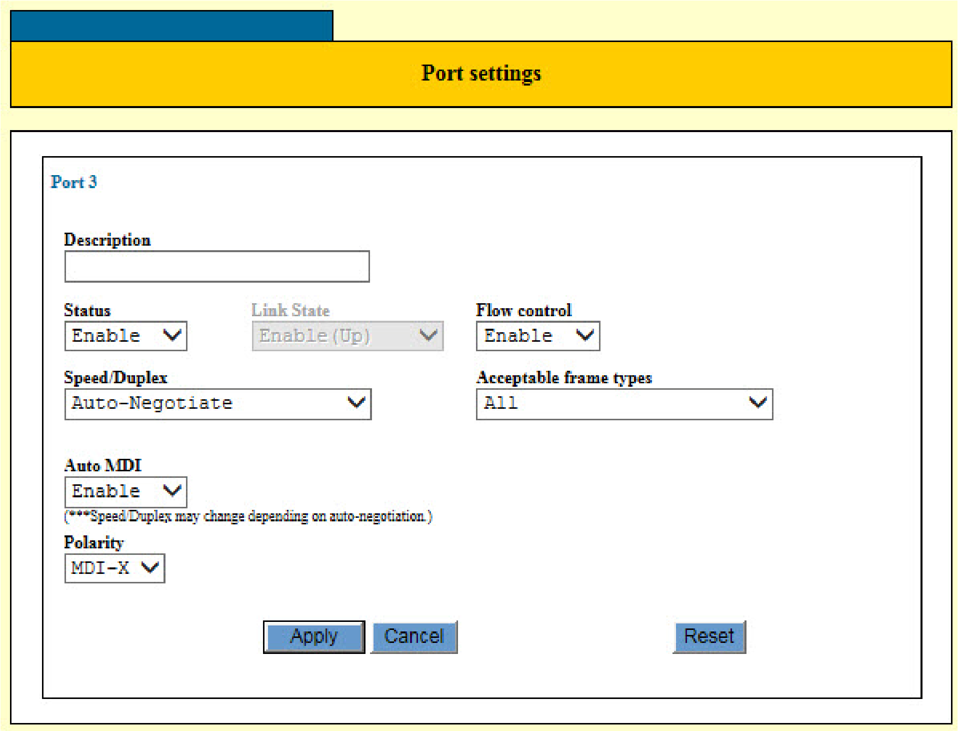
   The Switch Settings - Port window is shown in Figure 24 on page 104.

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 25.



Port settings

Port 3

Description

Status: Enable

Link State: Enable (Up)

Flow control: Enable

Speed/Duplex: Auto-Negotiate

Acceptable frame types: All

Auto MDI: Enable

(***Speed/Duplex may change depending on auto-negotiation.)

Polarity: MDI-X

Figure 25. 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 33.

Table 33. 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 33. 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 111.
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 112. 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 33. 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 151. 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 33. 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:

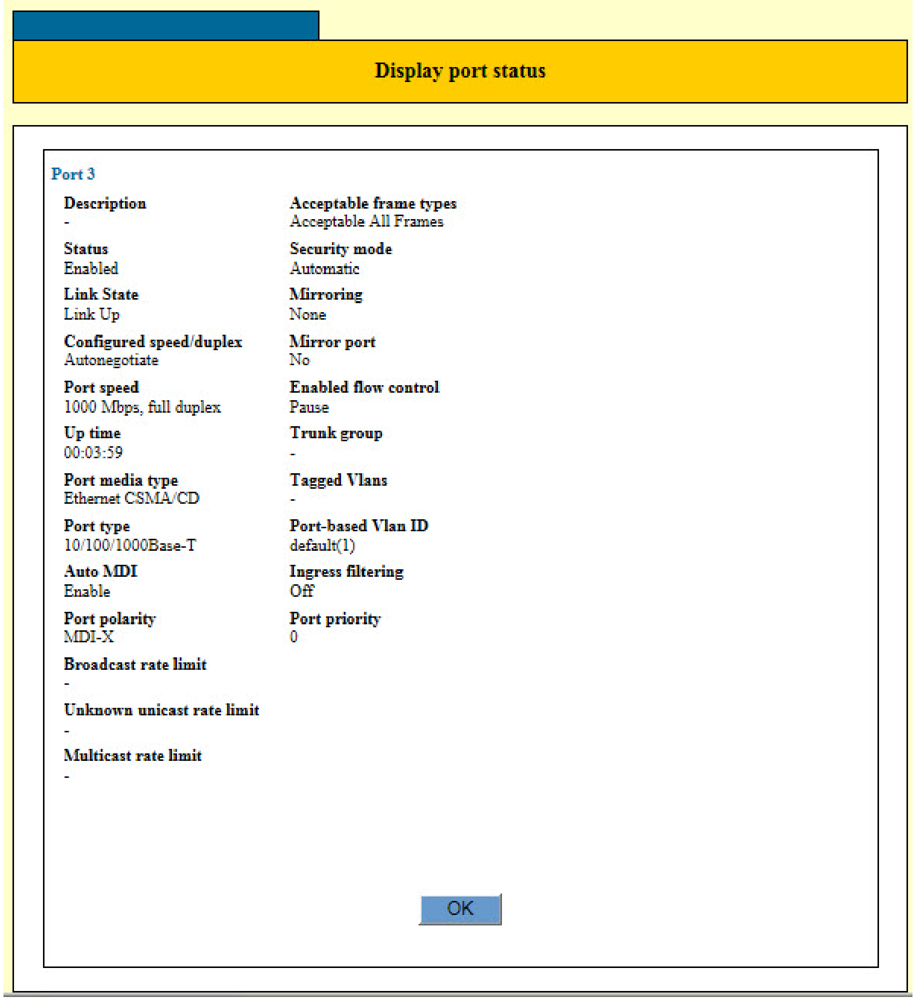
1. Expand the Switch Settings menu in the main menu.

2. Select the Port Settings option from the Switch Settings menu.The Switch Settings - Port window is shown in Figure 24 on page 104.

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 26.



Display port status

Port 3

Description
-

Status
Enabled

Link State
Link Up

Configured speed/duplex
Autonegotiate

Port speed
1000 Mbps, full duplex

Up time
00:03:59

Port media type
Ethernet CSMA/CD

Port type
10/100/1000Base-T

Auto MDI
Enable

Port polarity
MDI-X

Broadcast rate limit
-

Unknown unicast rate limit
-

Multicast rate limit
-

Acceptable frame types
Acceptable All Frames

Security mode
Automatic

Mirroring
None

Mirror port
No

Enabled flow control
Pause

Trunk group
-

Tagged Vlans
-

Port-based Vlan ID
default(1)

Ingress filtering
Off

Port priority
0

Figure 26. Display Port Status Window

The parameters in the window are described in Table 34.

Table 34. 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 11, “Packet Storm Protection” on page 129.

Table 34. 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 151.
Security Mode	Displays the security mode of the port. For background information, refer to Chapter 28, “MAC Address-based Port Security” on page 303.
Mirroring	Displays whether the port is a source port of a port mirror. For background information, refer to Chapter 12, “Port Mirroring” on page 135.
Mirror Port	Displays whether the port is acting as a port mirror. For background information, refer to Chapter 12, “Port Mirroring” on page 135.
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 34. 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 13, “Static Port Trunks” on page 141.
Tagged VLANs	Displays the VIDs of the VLANs where the port is a tagged member. For background information, refer to Chapter 14, “Port-based and Tagged VLANs Overview” on page 151.
Port-based VLAN ID	Displays the name and VID where the port is an untagged member. For background information, refer to Chapter 14, “Port-based and Tagged VLANs Overview” on page 151.
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 168.
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 204.

Chapter 10
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:

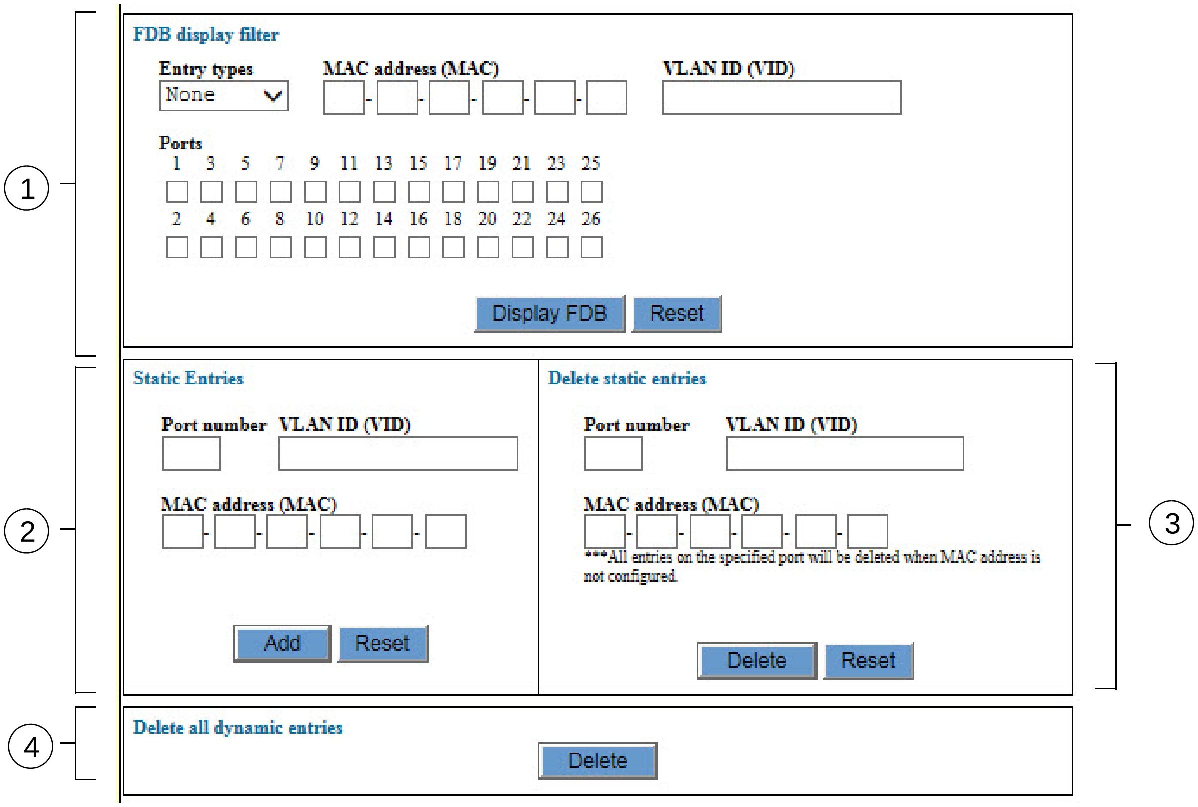
Displaying the MAC Address Window

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 27.



FDB display filter

Entry types: None

MAC address (MAC)

VLAN ID (VID)

Ports

Static Entries

Port number

VLAN ID (VID)

MAC address (MAC)

Delete static entries

Port number

VLAN ID (VID)

MAC address (MAC)

***All entries on the specified port will be deleted when MAC address is not configured.

Delete all dynamic entries

Figure 27. Device Monitoring - FDB Window

The sections in the window are described in Table 35.

Table 35. 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 120.

Table 35. 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 123.
3	Use this section to delete static MAC addresses from the switch. For instructions, refer to “Deleting Static Unicast Addresses” on page 124
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 125.

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 27 on page 118. 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 36.

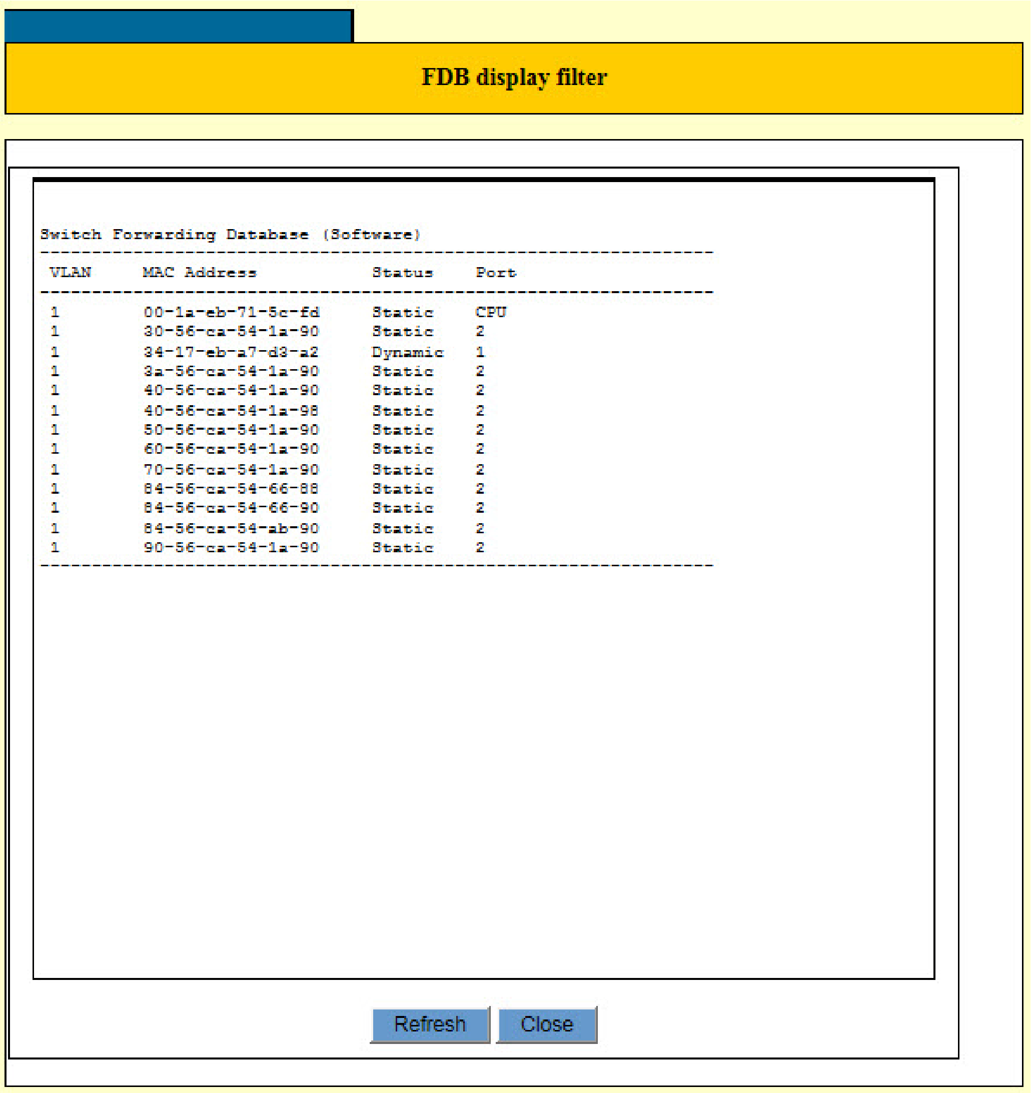
Table 36. FDB Display Filter

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 36. 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 168.
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 28 on page 122.



```
Switch Forwarding Database (Software)
---------------------------------------------------------------------
 VLAN      MAC Address            Status     Port
---------------------------------------------------------------------
 1         00-1a-eb-71-5c-fd      Static     CPU
 1         30-56-ca-54-1a-90      Static     2
 1         34-17-eb-a7-d3-a2      Dynamic    1
 1         3a-56-ca-54-1a-90      Static     2
 1         40-56-ca-54-1a-90      Static     2
 1         40-56-ca-54-1a-98      Static     2
 1         50-56-ca-54-1a-90      Static     2
 1         60-56-ca-54-1a-90      Static     2
 1         70-56-ca-54-1a-90      Static     2
 1         84-56-ca-54-66-88      Static     2
 1         84-56-ca-54-66-90      Static     2
 1         84-56-ca-54-ab-90      Static     2
 1         90-56-ca-54-1a-90      Static     2
---------------------------------------------------------------------
```

Figure 28. FDB Display Filter Window

Adding Static Unicast MAC Addresses

This 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 27 on page 118.
3. Configure the parameters in the Static Entries section of the window, as needed. The variables are described in Table 37. 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 37. 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 27 on page 118. 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 27 on page 118.

3. Click the Delete button in the bottom section of the window.

   The switch does not display a confirmation prompt.

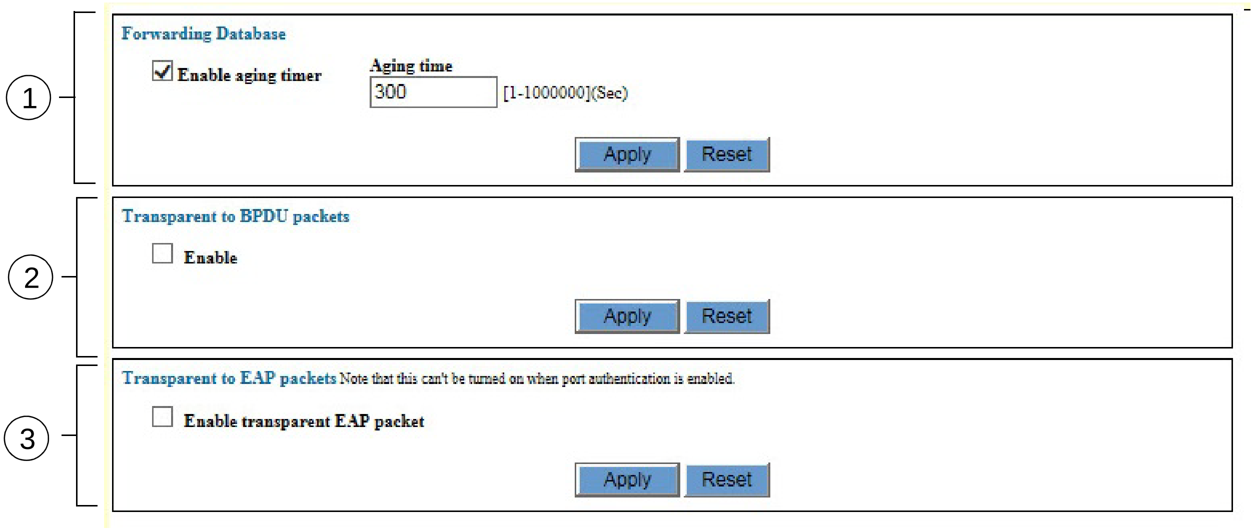
Changing the Aging Timer

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 29.



Forwarding Database

☑ Enable aging timer

Aging time: 300 [1-1000000](Sec)

Transparent to BPDU packets

□ Enable

Transparent to EAP packets Note that this can't be turned on when port authentication is enabled.

□ Enable transparent EAP packet

Figure 29. Switch Settings - Others Window

The sections in the window are described in Table 38.

Table 38. 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 38. 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. For instructions, refer to “Enabling or Disabling BPDU Transparency for RSTP” on page 229.
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 371.

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 11

Packet Storm Protection

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

Introduction

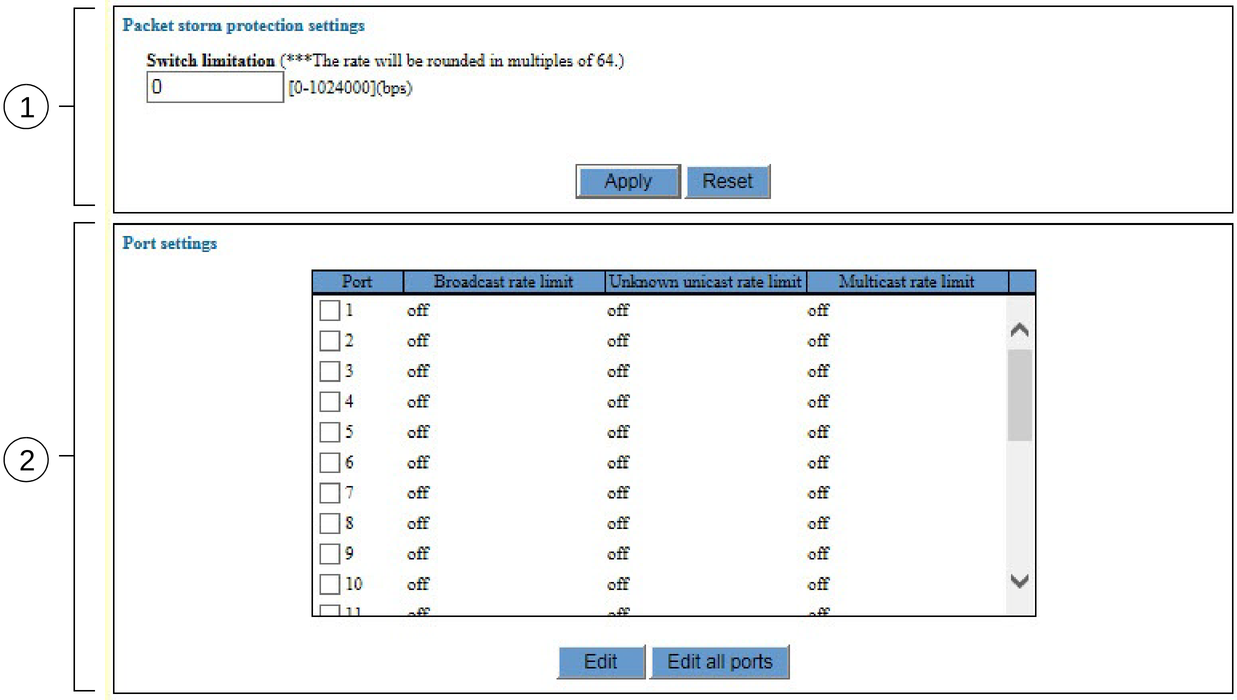
The packet storm protection feature allows you to set a threshold for the maximum number of ingress broadcast, multicast, or unknown unicast packets on the ports. Packets above the threshold are discarded by the switch. The switch supports only one threshold setting, which is set in bits per second (bps). 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 30.



Packet storm protection settings

Switch limitation (***The rate will be rounded in multiples of 64.)

0 [0-1024000](bps)

Port settings

Port	Broadcast rate limit	Unknown unicast rate limit	Multicast rate limit
□ 1	off	off	off
□ 2	off	off	off
□ 3	off	off	off
□ 4	off	off	off
□ 5	off	off	off
□ 6	off	off	off
□ 7	off	off	off
□ 8	off	off	off
□ 9	off	off	off
□ 10	off	off	off
□ 11	off	off	off

Figure 30. Switch Settings - Protection Window

The sections in the window are described in Table 39.

Table 39. 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 133.

The columns in the table in the window are defined in Table 40.

Table 40. 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.

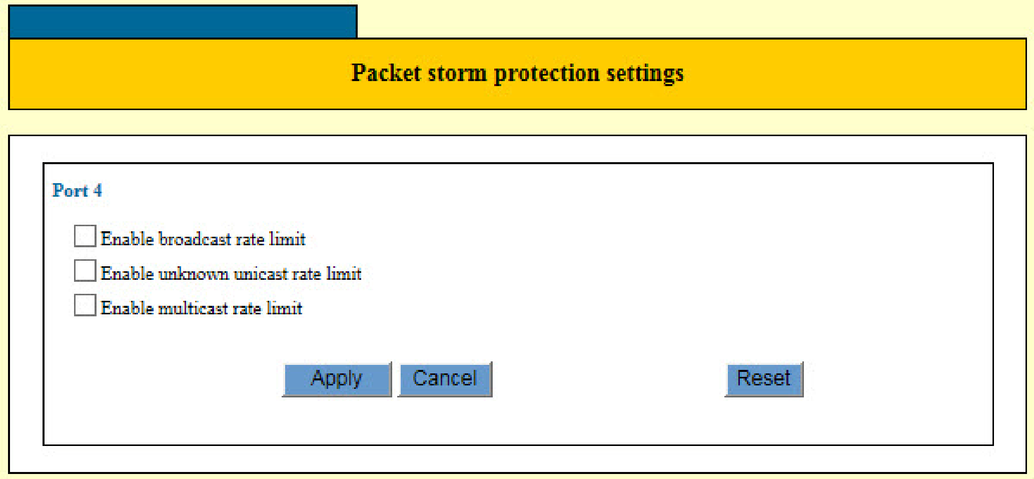
Configuring Packet Storm Protection

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 30.
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 31.



Packet storm protection settings

Port 4

□ Enable broadcast rate limit
□ Enable unknown unicast rate limit
□ Enable multicast rate limit

Figure 31. 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 12

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:

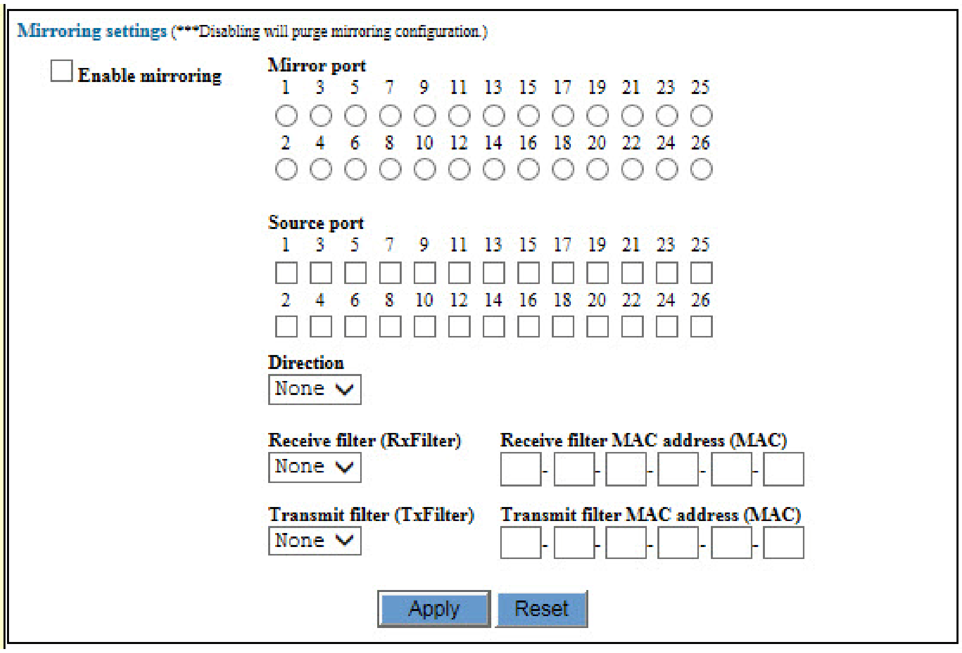
- The switch supports only one port mirror at a time.
- The port mirror can have only one mirror port.
- The mirror port must be a member of the default VLAN.
- The mirror port cannot be a member of a static port trunk.
- The port mirror can have more than one source port. This allows you to monitor 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 32.



Mirroring settings (***Disabling will purge mirroring configuration.)

□ Enable mirroring

Direction: None

Receive filter (RxFilter): None

Transmit filter (TxFilter): None

Figure 32. Switch Settings - Mirroring Window

3. Configure the parameters in the window.

   The parameters are defined in Table 41.

Table 41. Switch Settings - Mirroring Window

Parameter	Description
Enable Mirroring	Use this parameter to enable or disable the port mirroring feature. The feature is enabled when the dialog box has a check mark and disabled when the box is empty.
Mirror Port	Use this parameter to designate the mirror port. This is the port to which the switch copies the traffic from the source ports. You may designate only one mirror port.

Table 41. Switch Settings - Mirroring Window (Continued)

Parameter	Description
Source Port	Use this parameter to designate the source port. The traffic on the source port is copied to the mirror port. You may designate more than one source port.
Direction	Use this option to identify the traffic to be copied from the source ports to the mirror port. The options are listed 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. This is the default setting. You may not select None.
Receive Filter (RxFilter)	Use this parameter to mirror ingress traffic with a specified source or destination MAC address. For this filter to work, the Direction parameter has to be set to Rx or Both. The options are listed here: None - The ingress filter is disabled. The mirror feature copies all ingress traffic on the source ports. SA - The mirror feature copies only those ingress packets that have the specified MAC address as the source address. DA - The mirror feature copies only those ingress packets that have the specified MAC address as the destination address.

Table 41. Switch Settings - Mirroring Window (Continued)

Parameter	Description
Receive Filter MAC Address (MAC)	Use this parameter to specify the MAC address for the Receive Filter parameter. When the Receive Filter parameter is set to SA or DA, the mirror feature copies only those ingress packets on the source ports that have the specified MAC address as the source or destination address, respectively.
Transmit Filter (TxFilter)	Use this parameter to mirror egress traffic with a specified source or destination MAC address. For this filter to work, the Direction parameter has to be set to Tx or Both. The options are listed here: None - The ingress filter is disabled. The mirror feature mirrors all egress traffic. SA - The mirror feature copies only those egress packets that have the specified MAC address as the source address. DA - The mirror feature copies only those egress packets that have the specified MAC address as the destination address.
Transmit Filter MAC Address (MAC)	Use this parameter to specify the MAC address for the Transmit Filter parameter. When the Transmit Filter parameter is set to SA or DA, the mirror feature copies only those egress packets on the source ports that have the specified MAC address as the source or destination address, respectively.

4. 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.

5. 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 32 on page 137.

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 13

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

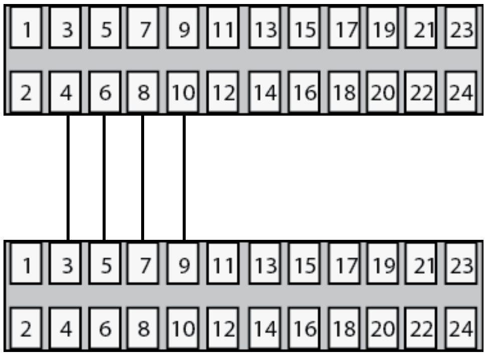


Figure 33. Static Port Trunk Example

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 107.

- ❒ The ports of a trunk cannot be authenticator or supplicant ports in port authentication. For further information, refer to Chapter 30, "Port Authentication Overview" on page 325 or Chapter 31, "Port Authentication" on page 343.
- ❒ 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:

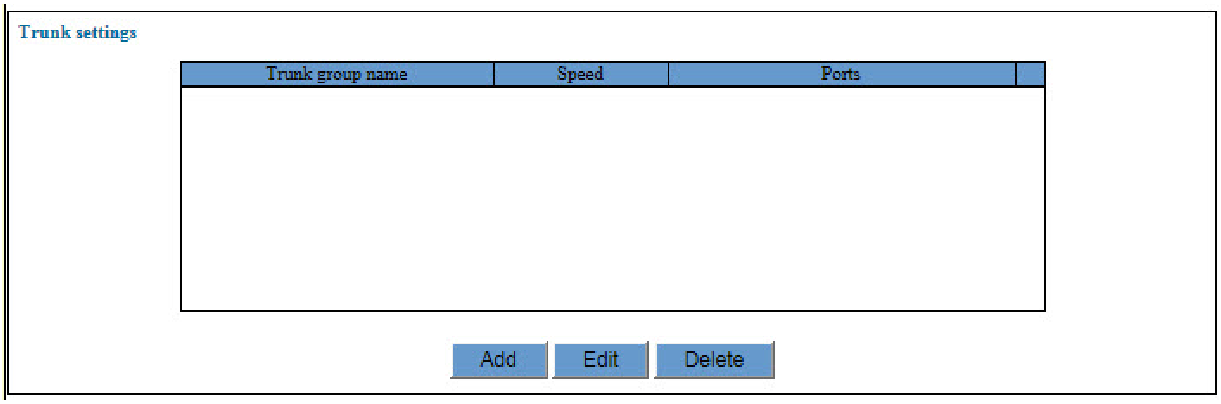
- ❐ Check that the parameter settings are the same on all of the ports that are to be in the trunk. For instructions, refer to “Configuring Port Parameters” on page 107.
- ❐ Check that the ports are members of the same VLAN. For instructions, refer to “Displaying the VLAN Window” on page 168.
- ❐ If 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 107.

⚠ **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 34.



Trunk settings

Trunk group name	Speed	Ports

Figure 34. Switch Settings - Trunking Window

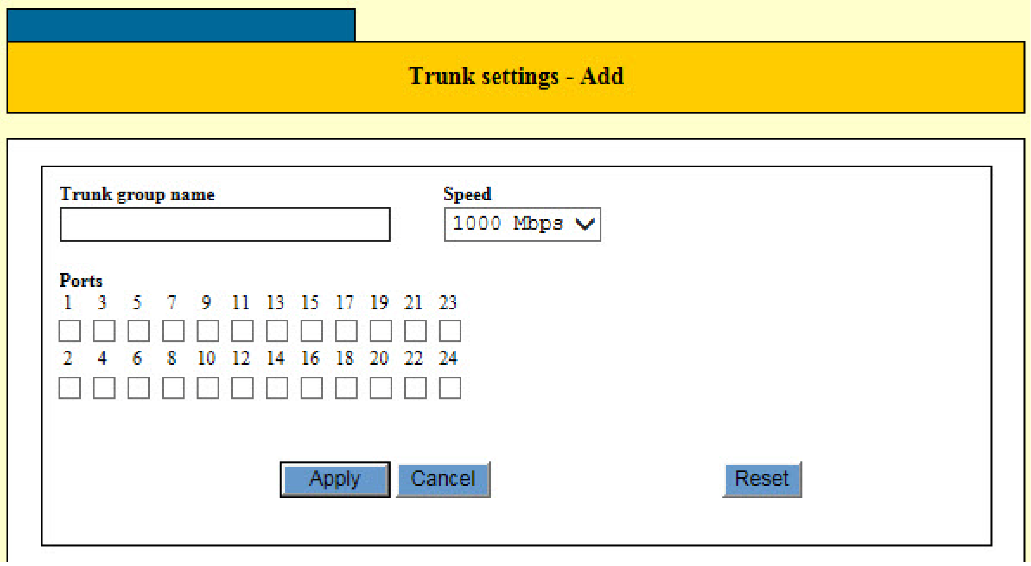
The table in the window displays the specifications of the existing trunks. The columns in the window are described in Table 42.

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 35.



Trunk settings - Add

Trunk group name

Speed: 1000 Mbps

Ports

1	3	5	7	9	11	13	15	17	19	21	23
□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24
□	□	□	□	□	□	□	□	□	□	□	□

Figure 35. 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 107.
- ❐ 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 168.

⚠ **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.

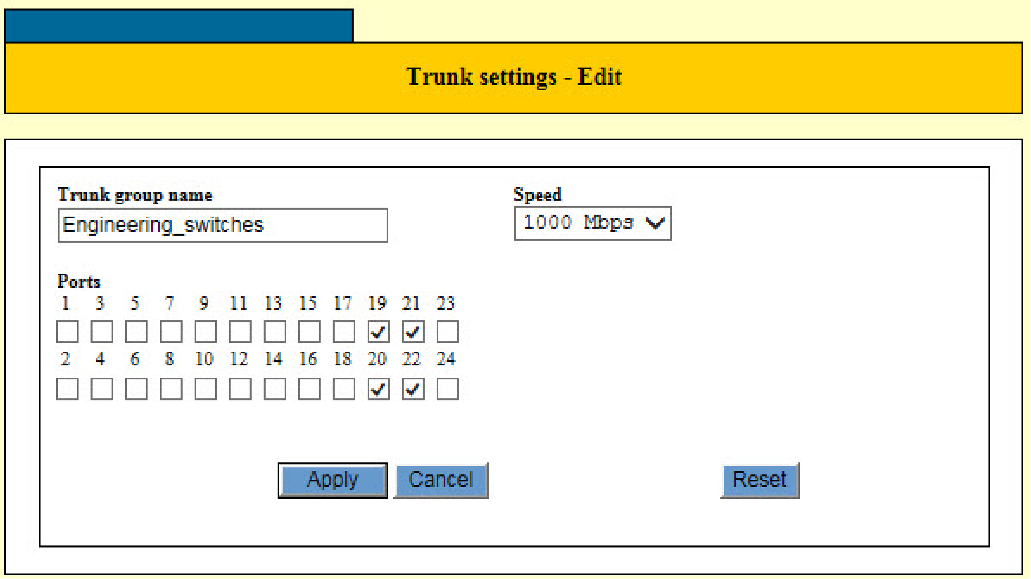
To modify a static port trunk, perform the following procedure:

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 34 on page 144.

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 36 on page 148.



Trunk settings - Edit

Trunk group name: Engineering_switches

Speed: 1000 Mbps

Ports

1	3	5	7	9	11	13	15	17	19	21	23
□	□	□	□	□	□	□	□	□	☑	☑	□
2	4	6	8	10	12	14	16	18	20	22	24
□	□	□	□	□	□	□	□	□	☑	☑	□

Figure 36. Trunk Settings - Edit Window

4. Modify the parameters in the window, as needed. The parameters are described in Table 43 on page 145.

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 section 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 34 on page 144.
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 14

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 16, “Protected Ports VLANs Overview” on page 179.

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 158.

- 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 158.

Port-based Example 1

Figure 37 on page 157 illustrates an example of one switch with three port-based VLANs. (The default VLAN is not shown in the following examples.)

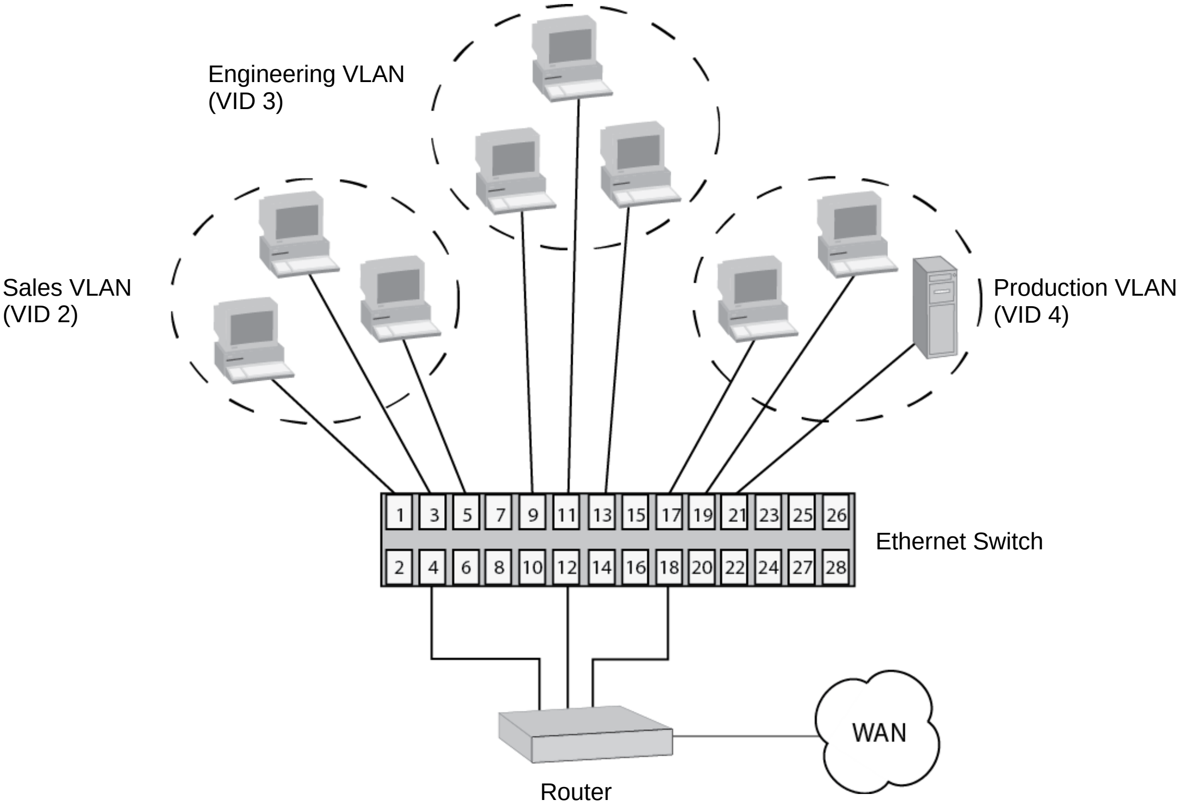


Figure 37. Port-based VLAN - Example 1

Table 44 lists the port assignments of the Sales, Engineering, and Production VLANs on the switch.

Table 44. 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 38 is another example of port-based VLANs. In this example, two VLANs, Sales and Engineering, span two switches.

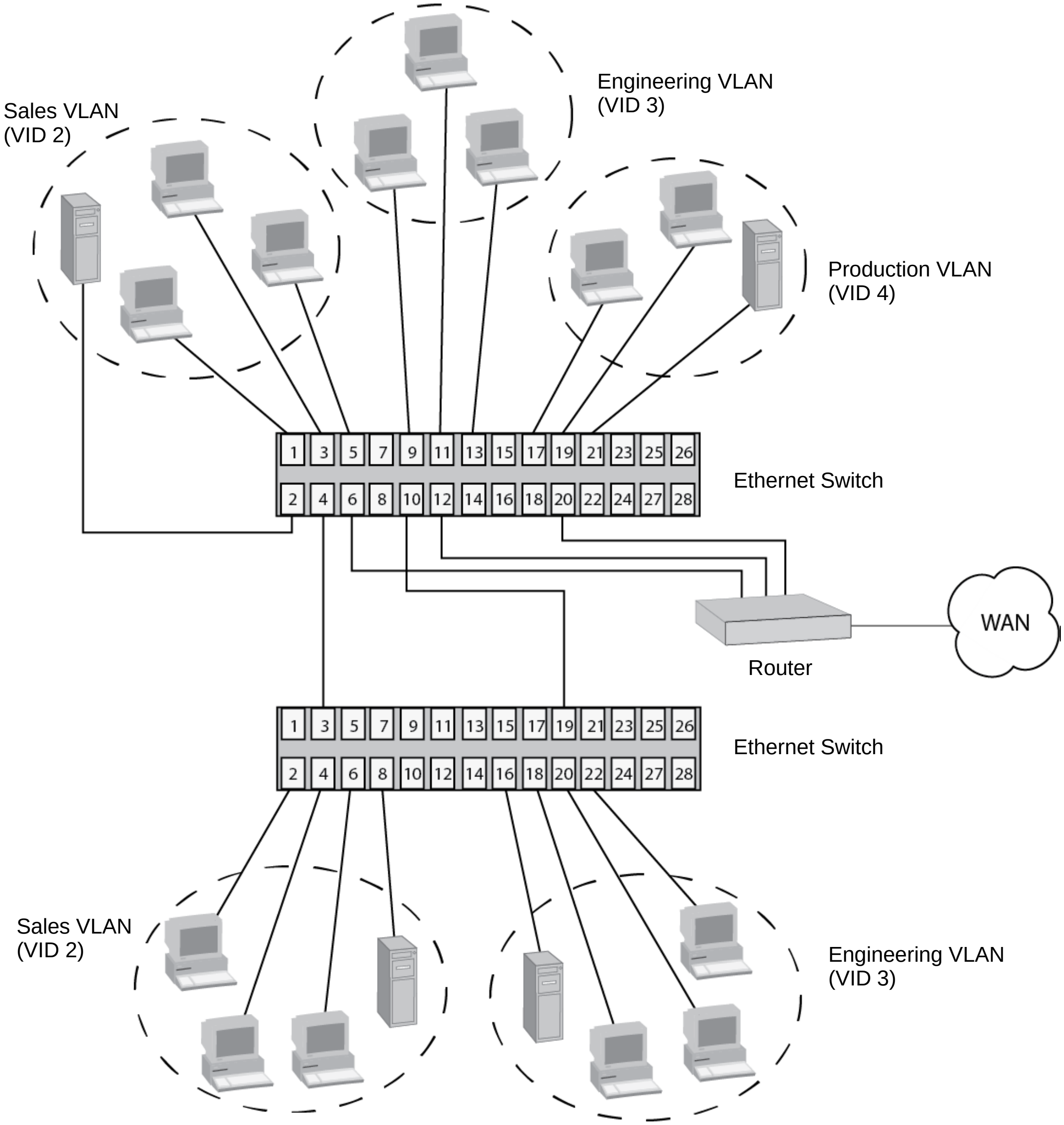


Figure 38. Port-based VLAN - Example 2

Table 45 on page 159 lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

Table 45. 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 154, 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 154 and “VLAN Identifier” on page 154.

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 39 on page 162 illustrates how tagged ports can be used to interconnect IEEE 802.1q-based products.

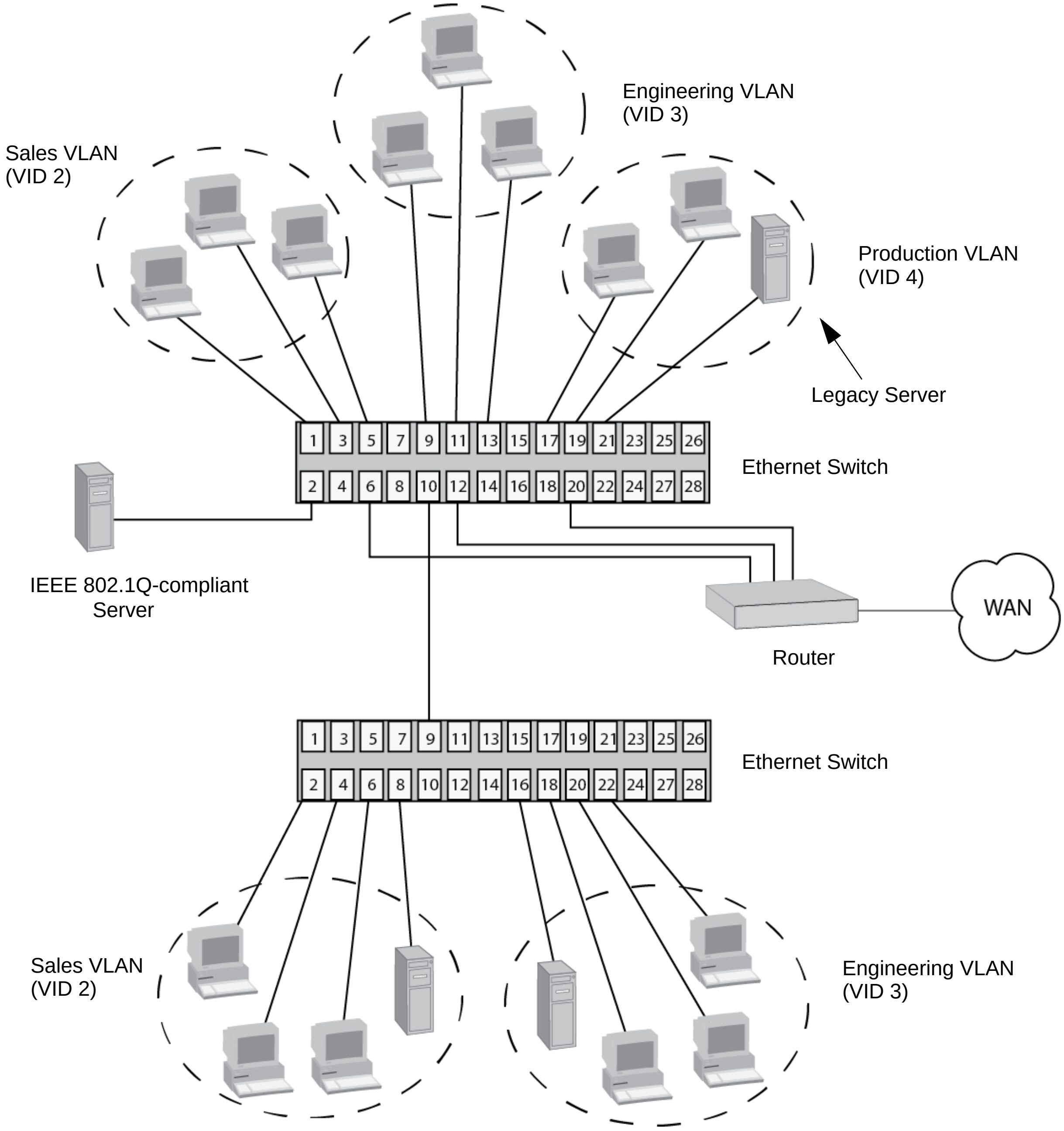


Figure 39. Example of a Tagged VLAN

The port assignments of the VLANs are described in Table 46 on page 163.

Table 46. 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, 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 158. 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 158 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 15

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 usually 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 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

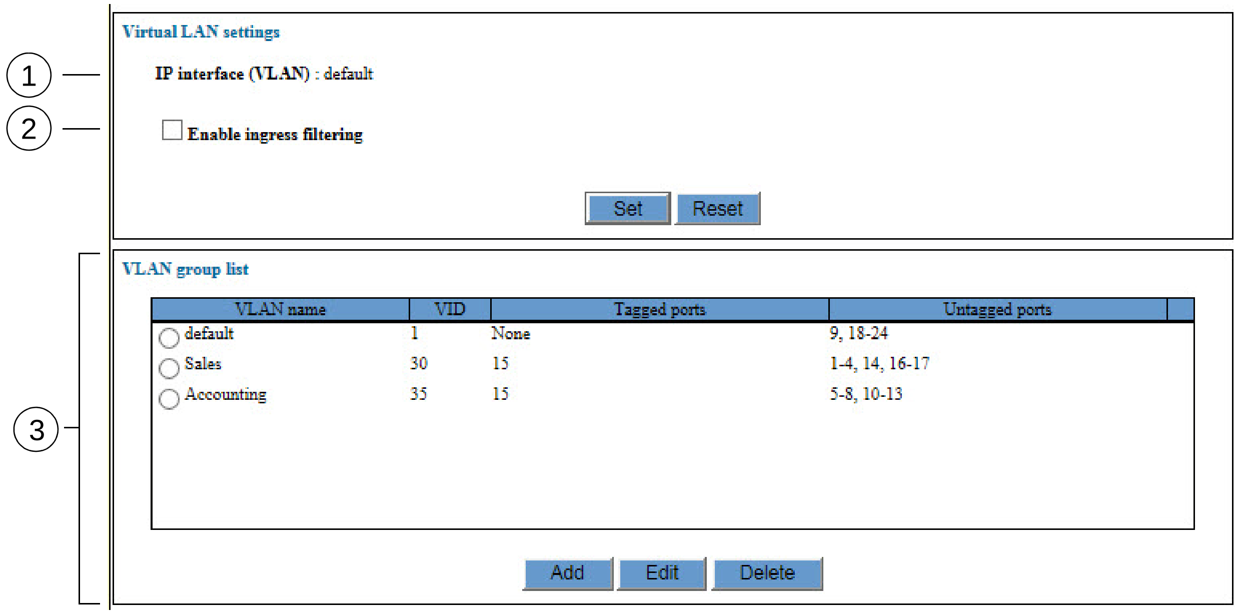
other tagged and untagged VLAN assignments, because a tagged port can be a member of more than one VLAN at a time.

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 40.



Virtual LAN settings

IP interface (VLAN) : default

□ Enable ingress filtering

VLAN group list

VLAN name	VID	Tagged ports	Untagged ports
○ default	1	None	9, 18-24
○ Sales	30	15	1-4, 14, 16-17
○ Accounting	35	15	5-8, 10-13

Figure 40. Switch Settings - Virtual LAN Window

The items in the window are described in Table 47.

Table 47. 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 48,
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 47. 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 170, “Modifying a Port-based or Tagged VLAN” on page 175, and “Deleting a VLAN” on page 177.

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 48.

Table 48. 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 166.

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

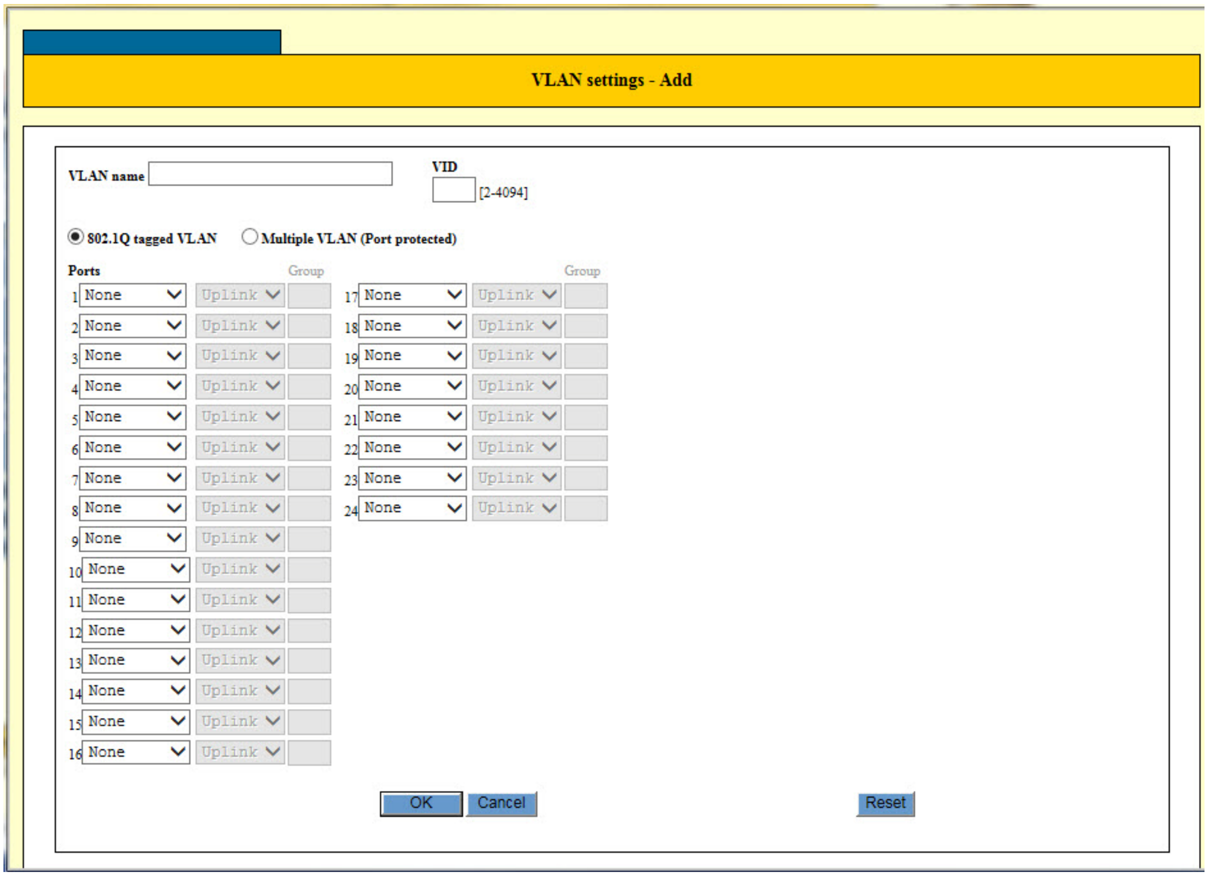
1. Expand the Switch Settings menu in the main menu.
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 40 on page 168.
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 175.
4. Click the Add button at the bottom of the window.

   The VLAN Settings - Add window is shown in Figure 41 on page 171.



VLAN settings - Add

VLAN name

VID [2-4094]

● 802.1Q tagged VLAN ○ Multiple VLAN (Port protected)

Ports		Group			Group
1 None	Uplink		17 None	Uplink	
2 None	Uplink		18 None	Uplink	
3 None	Uplink		19 None	Uplink	
4 None	Uplink		20 None	Uplink	
5 None	Uplink		21 None	Uplink	
6 None	Uplink		22 None	Uplink	
7 None	Uplink		23 None	Uplink	
8 None	Uplink		24 None	Uplink	
9 None	Uplink				
10 None	Uplink				
11 None	Uplink				
12 None	Uplink				
13 None	Uplink				
14 None	Uplink				
15 None	Uplink				
16 None	Uplink				

Figure 41. VLAN Settings - Add Window

5. Configure the parameters in the window to create the new VLAN. The parameters are described in Table 49.

Table 49. 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 49. 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 49. 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 some 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 175.

   ❐ 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 166.

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.

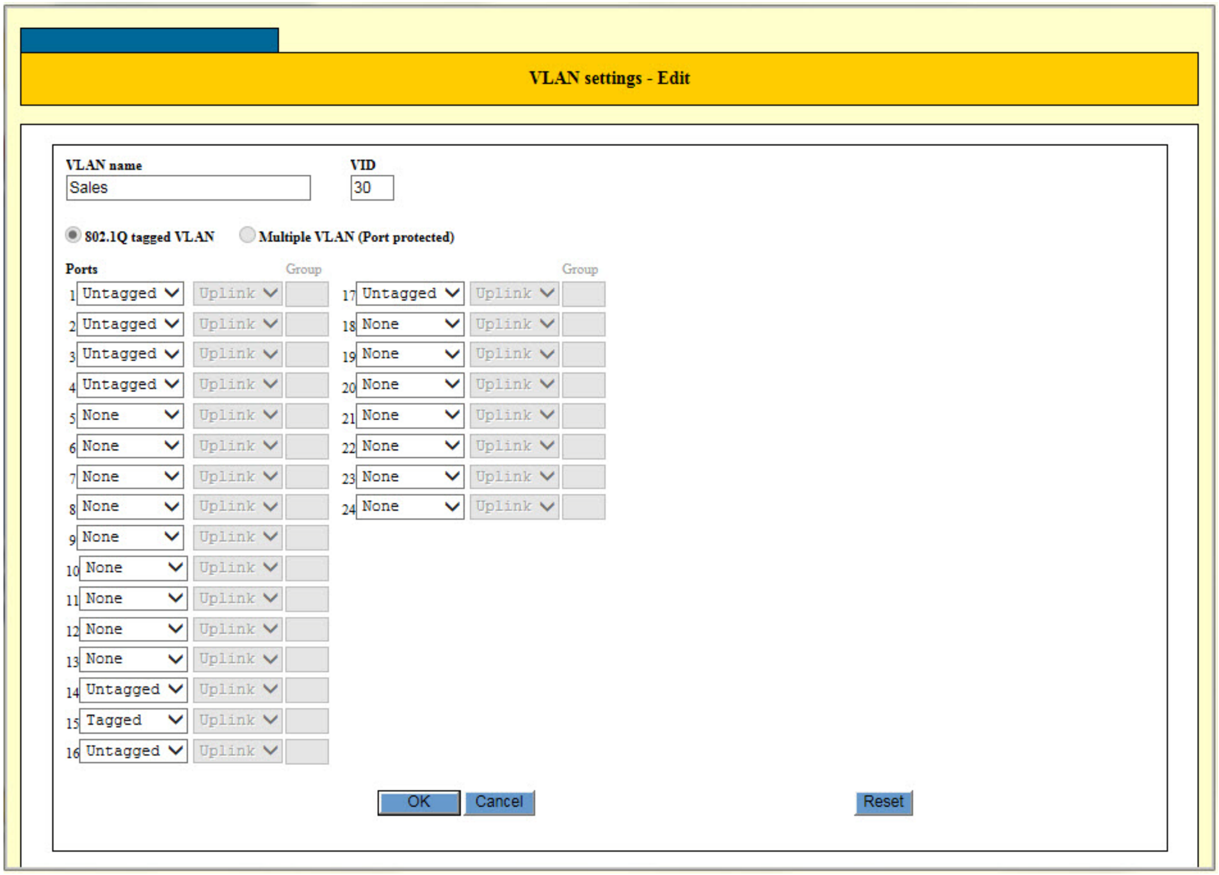
2. Select the Virtual LAN option from the Switch Settings menu.

   The Switch Settings - Virtual LAN window is shown in Figure 40 on page 168.

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 42 on page 176.



VLAN settings - Edit

VLAN name: Sales

VID: 30

● 802.1Q tagged VLAN ○ Multiple VLAN (Port protected)

Ports			Group				Group
1	Untagged	Uplink		17	Untagged	Uplink	
2	Untagged	Uplink		18	None	Uplink	
3	Untagged	Uplink		19	None	Uplink	
4	Untagged	Uplink		20	None	Uplink	
5	None	Uplink		21	None	Uplink	
6	None	Uplink		22	None	Uplink	
7	None	Uplink		23	None	Uplink	
8	None	Uplink		24	None	Uplink	
9	None	Uplink					
10	None	Uplink					
11	None	Uplink					
12	None	Uplink					
13	None	Uplink					
14	Untagged	Uplink					
15	Tagged	Uplink					
16	Untagged	Uplink					

Figure 42. VLAN Settings - Edit Window

5. Modify the parameters in the window, as needed. The parameters are described in Table 49 on page 171.

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 40.
- ❒ 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 40.
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 48.

- ❐ 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 16

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 14, "Port-based and Tagged VLANs Overview" on page 151.

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 50 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 51 lists the different groups in the VLAN and the ports of the groups.

Table 50. 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 51. 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 17

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 50 on page 181 and Table 51 on page 181.
- ❐ For guidelines on changing the VLAN assignments of ports, refer to “Guidelines to Adding or Removing Ports from VLANs” on page 166.

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 168.

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 175 or “Modifying a Protected Ports VLAN” on page 188.

4. Click the Add button.

   The VLAN Settings - Add window is shown in Figure 41 on page 171.

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 52 on page 185.

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.

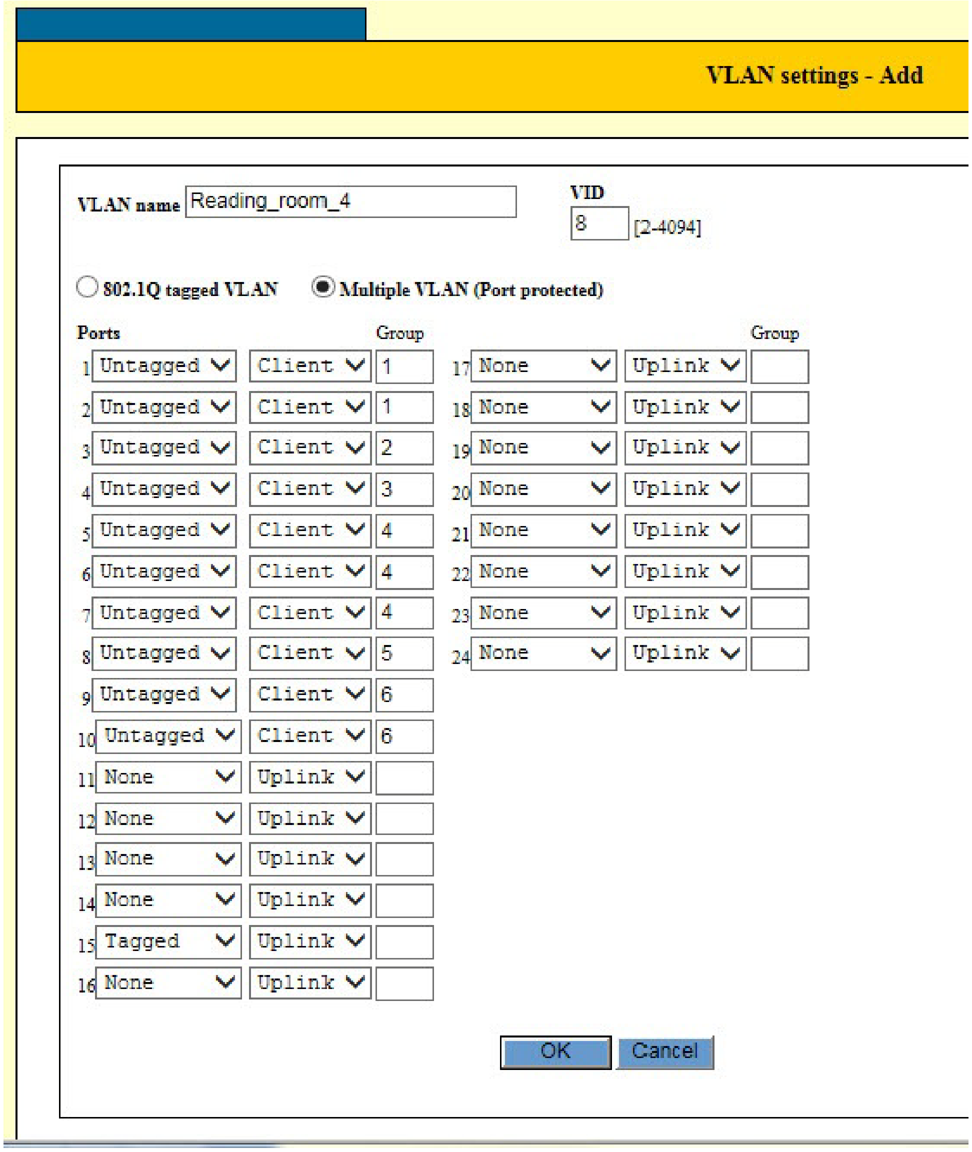
Table 52. VLAN Settings - Add Window for Protected Ports VLAN

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 52. 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 43 on page 187 is an example of how the VLAN Settings - Add window would look for the protected ports VLAN detailed in Table 50 on page 181 and Table 51 on page 181.



VLAN settings - Add

VLAN name Reading_room_4

VID 8 [2-4094]

○ 802.1Q tagged VLAN ● Multiple VLAN (Port protected)

Ports			Group				Group
1	Untagged	Client	1	17	None	Uplink	
2	Untagged	Client	1	18	None	Uplink	
3	Untagged	Client	2	19	None	Uplink	
4	Untagged	Client	3	20	None	Uplink	
5	Untagged	Client	4	21	None	Uplink	
6	Untagged	Client	4	22	None	Uplink	
7	Untagged	Client	4	23	None	Uplink	
8	Untagged	Client	5	24	None	Uplink	
9	Untagged	Client	6				
10	Untagged	Client	6				
11	None	Uplink					
12	None	Uplink					
13	None	Uplink					
14	None	Uplink					
15	Tagged	Uplink					
16	None	Uplink					

Figure 43. 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 166.

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 168.
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 52 on page 185.
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 40.
- ❒ 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 168.

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 48.

- ❐ 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 18

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 160, 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 53 on page 193 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 53. 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 54.

Table 54. 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 54. 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 55 on page 196 shows the default values for the queues.

Table 55. 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 19

Quality of Service

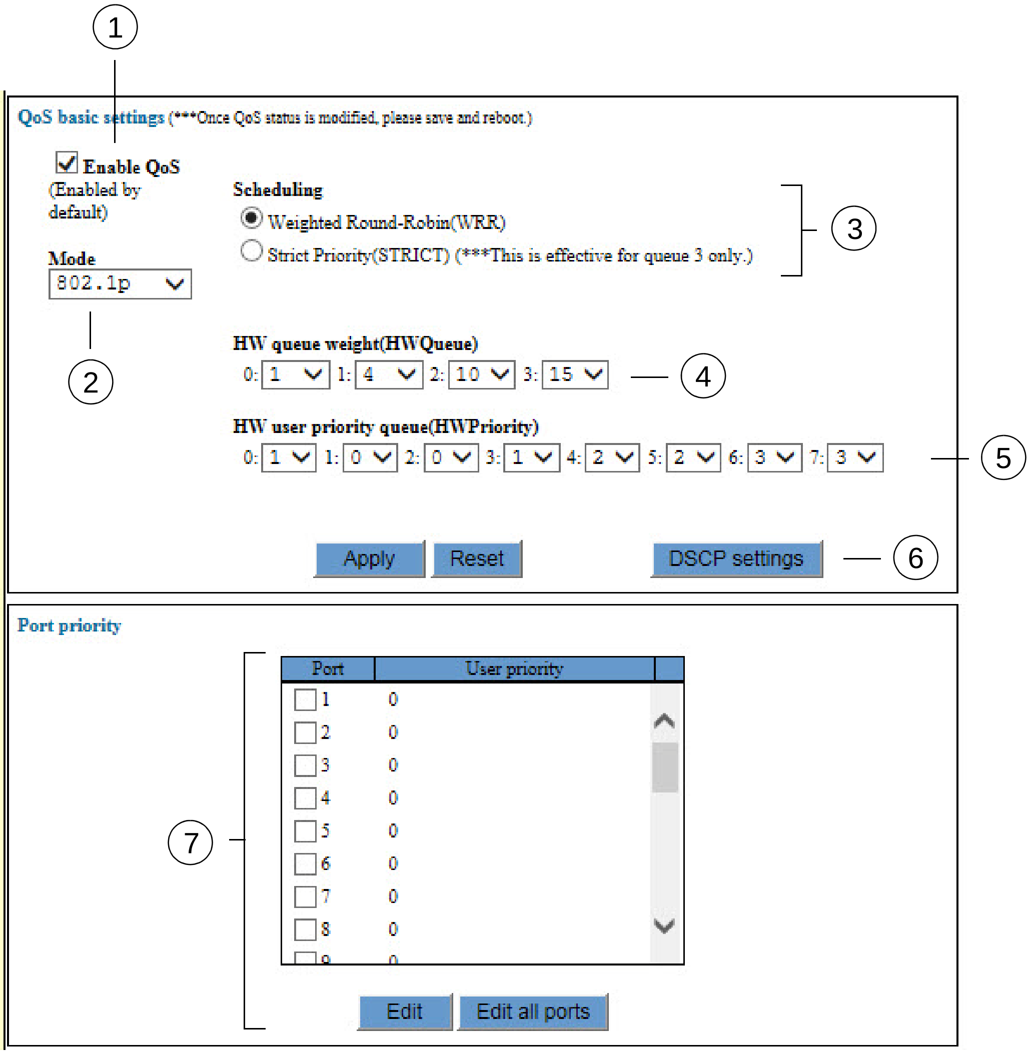
This chapter explains how to configure the Class of Service portion of Quality of Service (QoS). This chapter contains the following procedures:

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 44.



QoS basic settings (***Once QoS status is modified, please save and reboot.)

☑ Enable QoS (Enabled by default)

Mode: 802.1p

Scheduling
- ● Weighted Round-Robin(WRR)
- ○ Strict Priority(STRICT) (***This is effective for queue 3 only.)

HW queue weight(HWQueue)

0: 1   1: 4   2: 10   3: 15

HW user priority queue(HWPriority)

0: 1   1: 0   2: 0   3: 1   4: 2   5: 2   6: 3   7: 3

Port priority

Port	User priority
□ 1	0
□ 2	0
□ 3	0
□ 4	0
□ 5	0
□ 6	0
□ 7	0
□ 8	0
□ 9	0

Figure 44. Switch Settings - QoS Window

The sections in the window are described in Table 56 on page 199.

Table 56. 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 method of packet prioritization. The options are listed here: DIFFSERV - 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 195. For instructions on how to set the feature, refer to “Configuring Egress Packet Scheduling” on page 200.
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 195. For instructions on how to set the feature, refer to “Configuring Egress Packet Scheduling” on page 200.
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 192. For instructions on how to set the feature, refer to “Mapping CoS Priorities to Egress Queues” on page 201.
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 202.
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 192. For instructions, refer to “Setting the Priority Values for Ingress Untagged Packets” on page 204.

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 44 on page 198.

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 195.

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 192. 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 44 on page 198. 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 53 on page 193.

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:

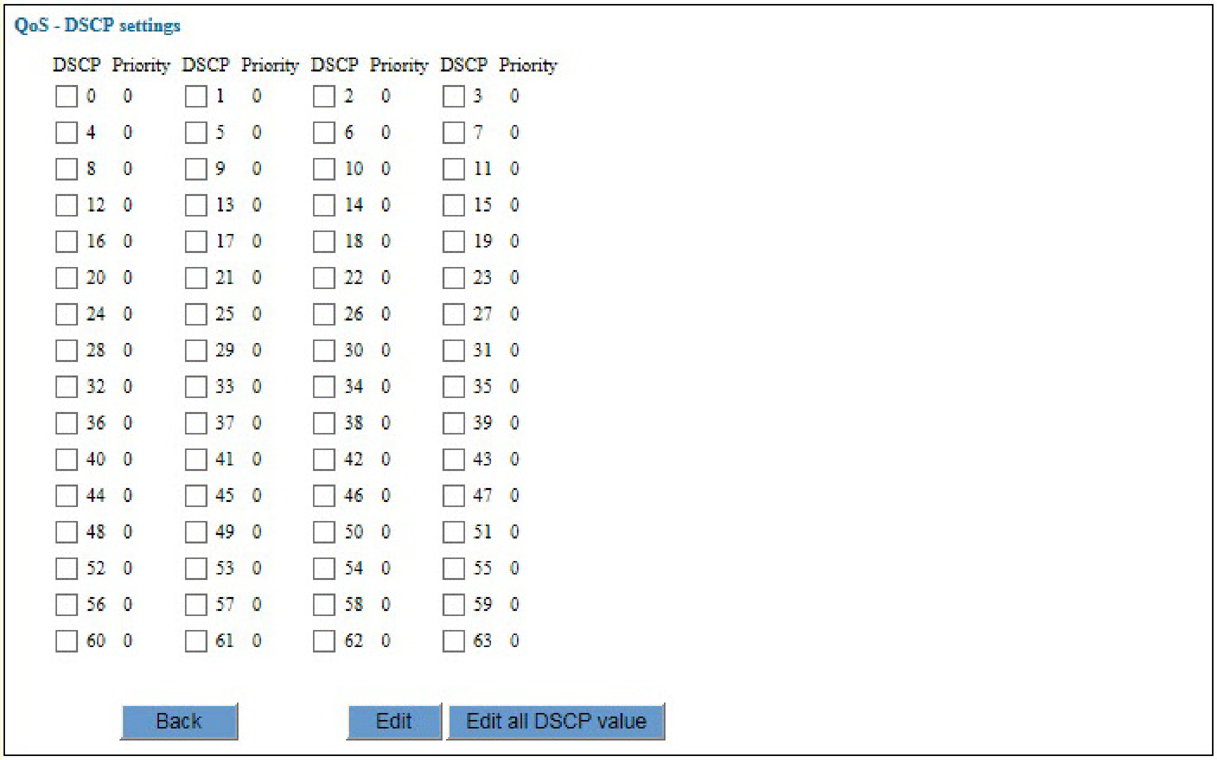
1. Expand the Switch Settings menu in the main menu.

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

   The Switch Settings - QoS window is shown in Figure 44 on page 198.

3. Click the DSCP Settings button.

   The switch displays the DSCP Settings - QoS window, shown in Figure 45.



QoS - DSCP settings

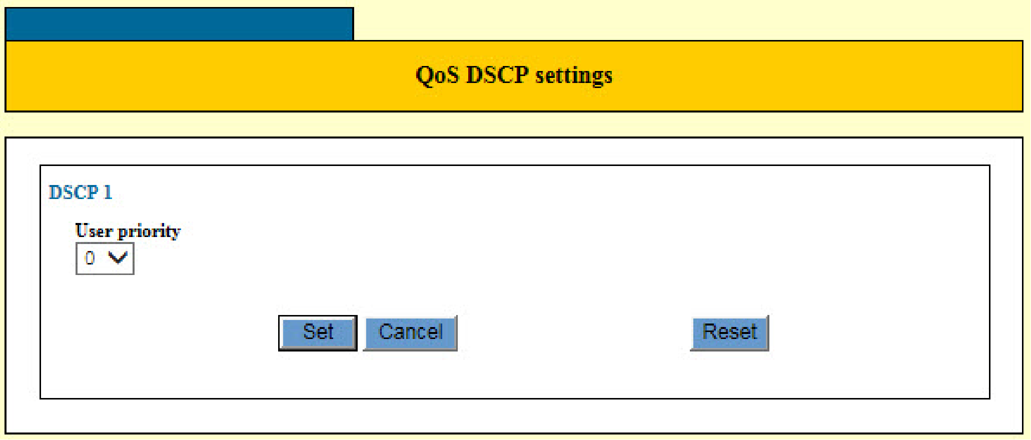
DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
□ 0	0	□ 1	0	□ 2	0	□ 3	0
□ 4	0	□ 5	0	□ 6	0	□ 7	0
□ 8	0	□ 9	0	□ 10	0	□ 11	0
□ 12	0	□ 13	0	□ 14	0	□ 15	0
□ 16	0	□ 17	0	□ 18	0	□ 19	0
□ 20	0	□ 21	0	□ 22	0	□ 23	0
□ 24	0	□ 25	0	□ 26	0	□ 27	0
□ 28	0	□ 29	0	□ 30	0	□ 31	0
□ 32	0	□ 33	0	□ 34	0	□ 35	0
□ 36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

Figure 45. 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 46 on page 203.



QoS DSCP settings

DSCP 1

User priority
0

Figure 46. 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 201.

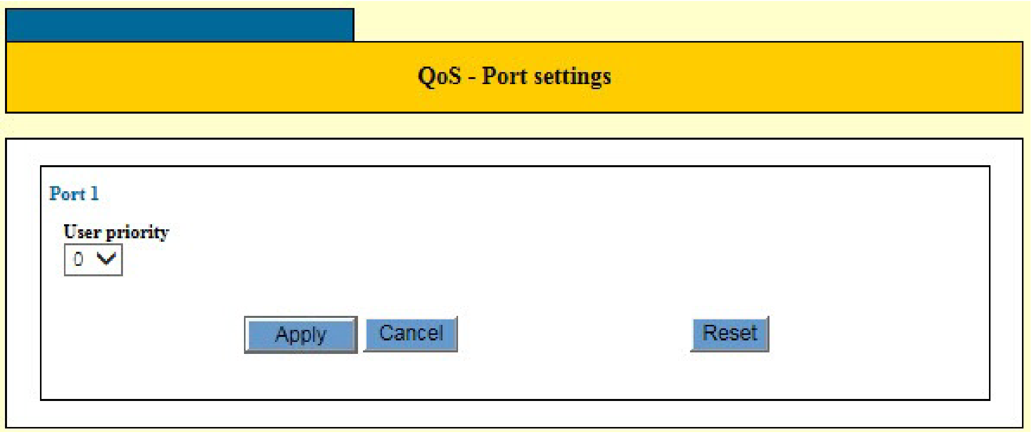
To change the CoS priority level on a port, perform the following procedure:

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 44 on page 198.

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 47.


QoS - Port settings

Port 1

User priority: 0

Figure 47. 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 20

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

RSTP is 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, the spanning tree protocol places the extra paths in a standby or blocking mode by disabling ports, so that there is only one active path.

The spanning tree protocol can also activate redundant paths if active main paths go down. This enables the protocol to maintain network connectivity between different parts of a network in the event of a failure of a primary path.

RSTP on the switch has an STP-compatible mode that makes it compatible with legacy devices that only support the original Spanning Tree Protocol (STP).

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 of 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 57 lists the RSTP port costs with Auto-Detect.

Table 57. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 58 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 58. 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 48 illustrates two switches that are connected with one data link of point-to-point ports operating in full-duplex mode.

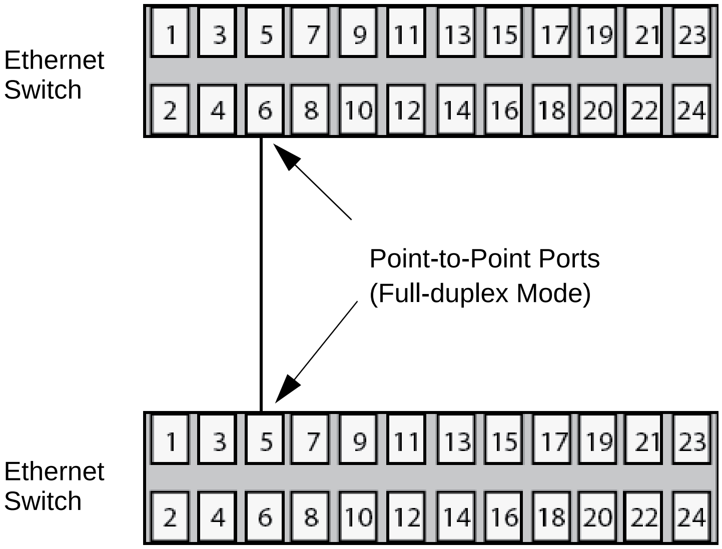


Figure 48. Point-to-Point Ports

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 49 on page 213 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.

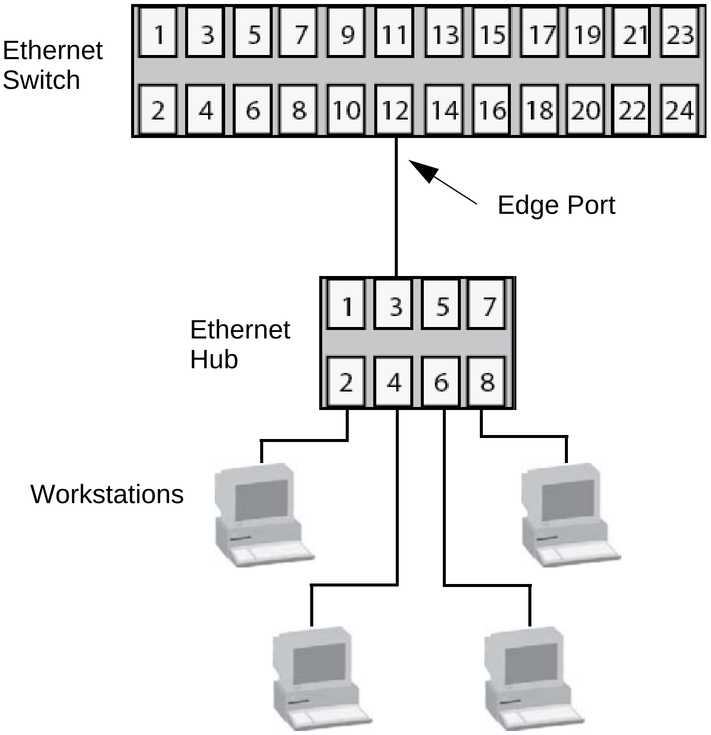


Figure 49. Edge Port

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 50 illustrates a port functioning as both a point-to-point and edge port.

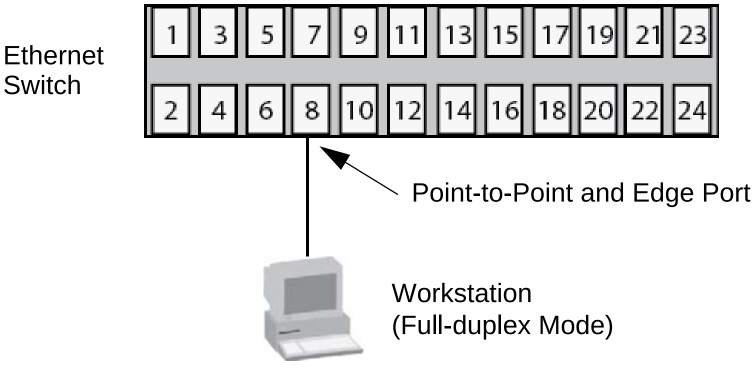


Figure 50. Point-to-Point and Edge Port

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 51. 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.

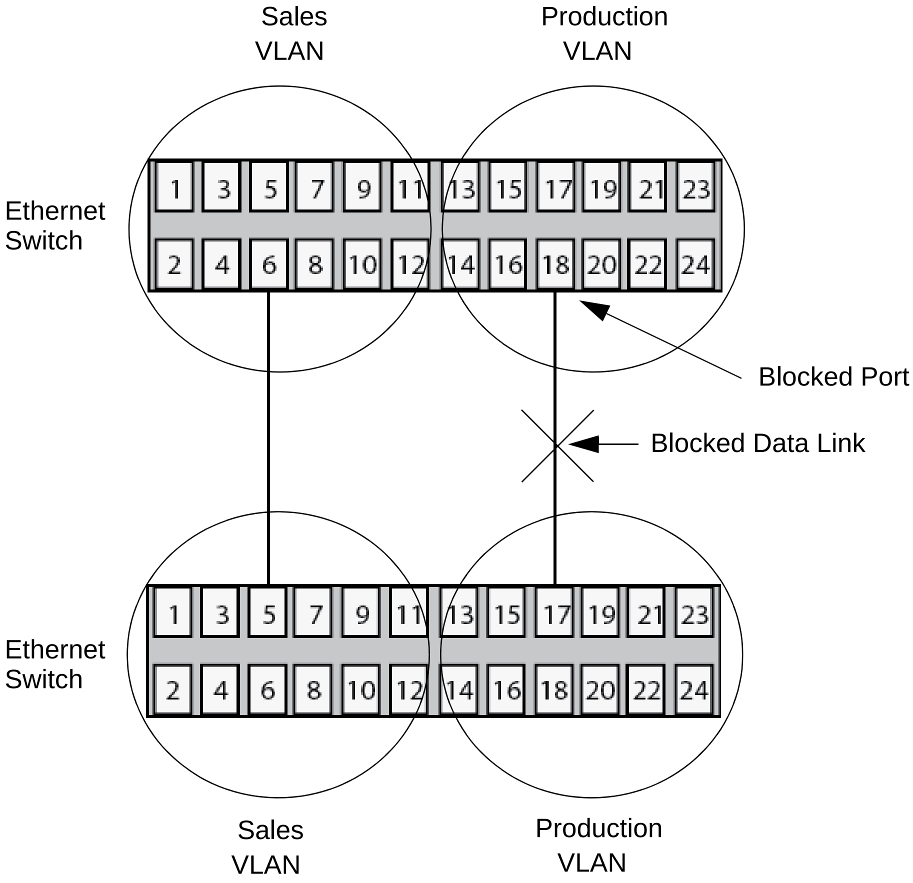


Figure 51. VLAN Fragmentation

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 14, “Port-based and Tagged VLANs Overview” on page 151.)

Chapter 21

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

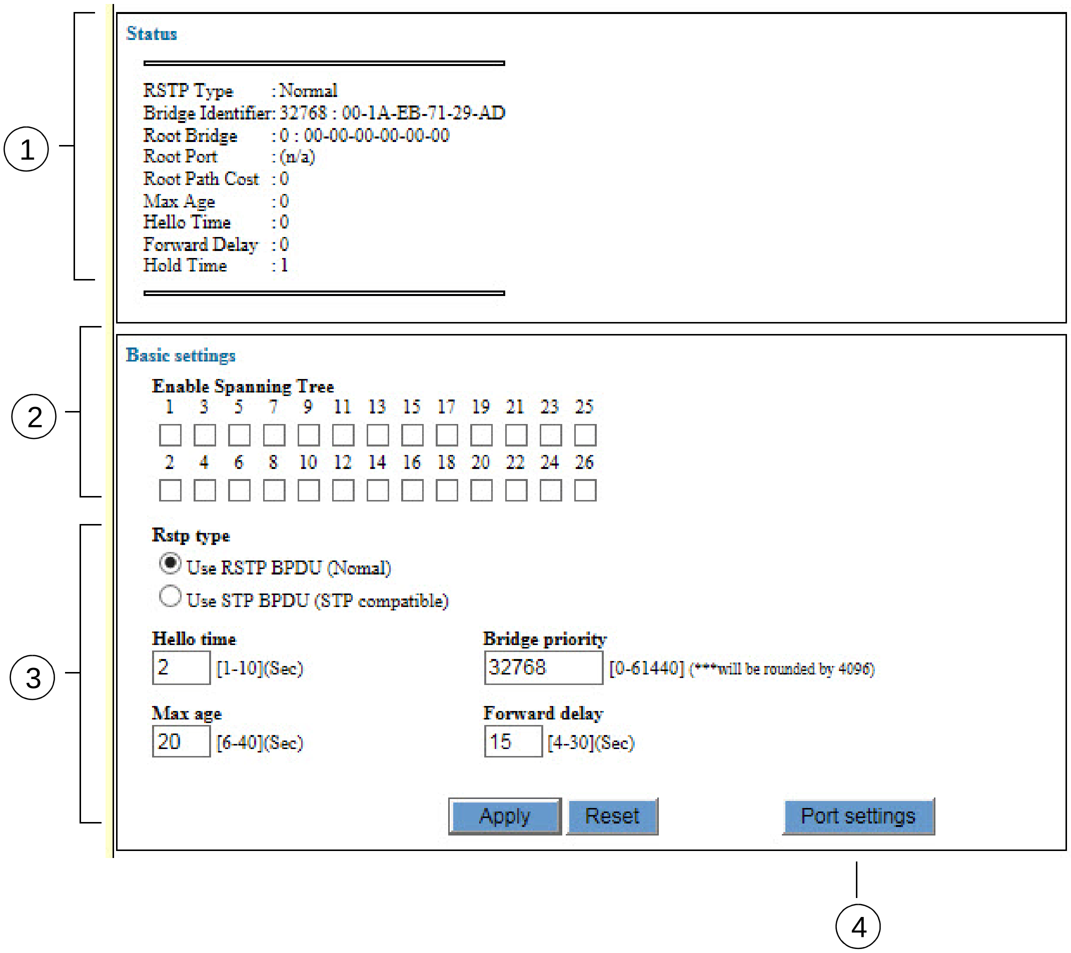
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience or an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

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 52.



Status

```
RSTP Type          : Normal
Bridge Identifier: 32768 : 00-1A-EB-71-29-AD
Root Bridge        : 0 : 00-00-00-00-00-00
Root Port          : (n/a)
Root Path Cost     : 0
Max Age            : 0
Hello Time         : 0
Forward Delay      : 0
Hold Time          : 1
```

Basic settings

Enable Spanning Tree

1	3	5	7	9	11	13	15	17	19	21	23	25
□	□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24	26
□	□	□	□	□	□	□	□	□	□	□	□	□

Rstp type

● Use RSTP BPDU (Nomal)

○ Use STP BPDU (STP compatible)

Hello time: 2 [1-10](Sec)

Bridge priority: 32768 [0-61440] (***will be rounded by 4096)

Max age: 20 [6-40](Sec)

Forward delay: 15 [4-30](Sec)

Figure 52. Switch Settings - RSTP Window

The sections in the Switch Settings - RSTP window are defined in Table 59 on page 219.

Table 59. 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 60 on page 219.
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 228.
3	Use the options in this section to configure the RSTP bridge settings. Refer to “Configuring RSTP Bridge Settings” on page 222.
4	Use this button to configure the RSTP port settings. Refer to “Configuring RSTP Port Settings” on page 225.

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 60.

Table 60. 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 60. 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 60. 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 52 on page 218.
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 52 on page 218 and the parameters are described in Table 61.

Table 61. 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 61. 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 61. 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:

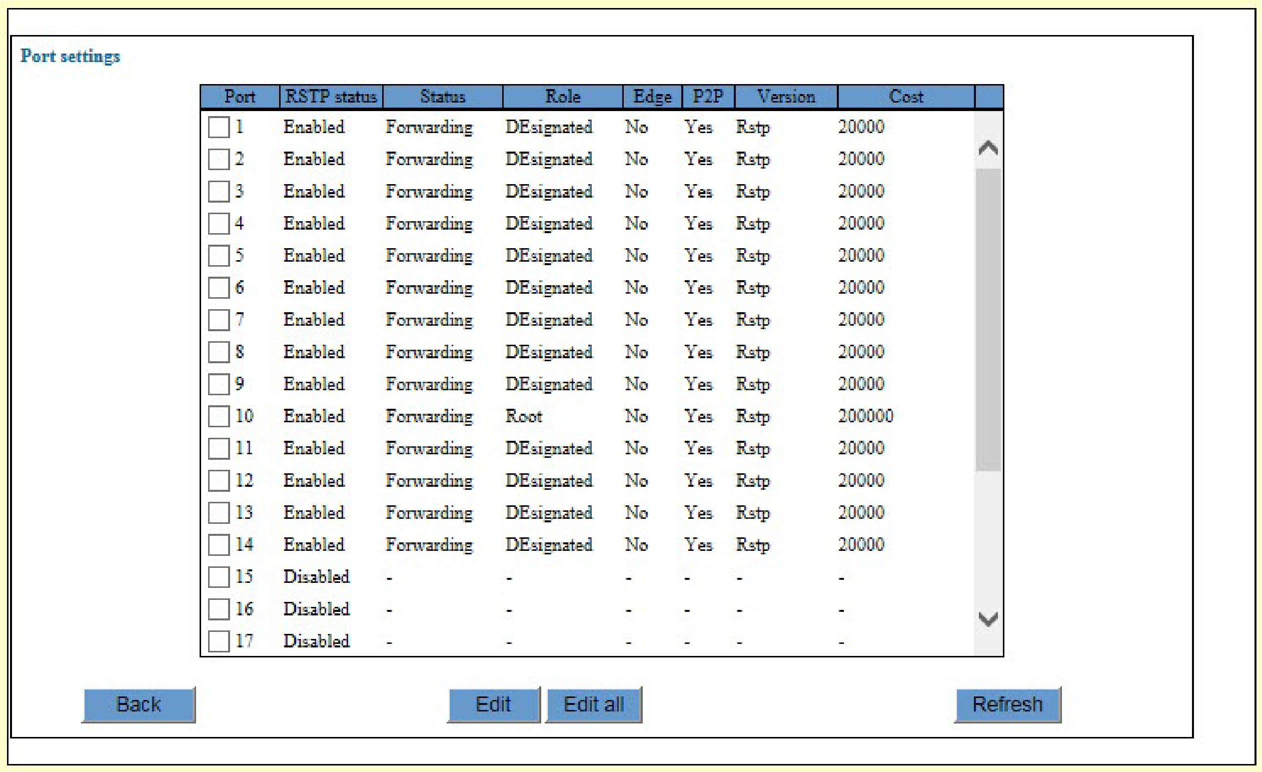
1. Expand the Switch Settings menu in the main menu.

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

   The Switch Settings - RSTP window is shown in Figure 52 on page 218.

3. Click the Port Settings button at the bottom of the window.

   The switch displays the RSTP Port Parameters window. Refer to Figure 53.



Port settings

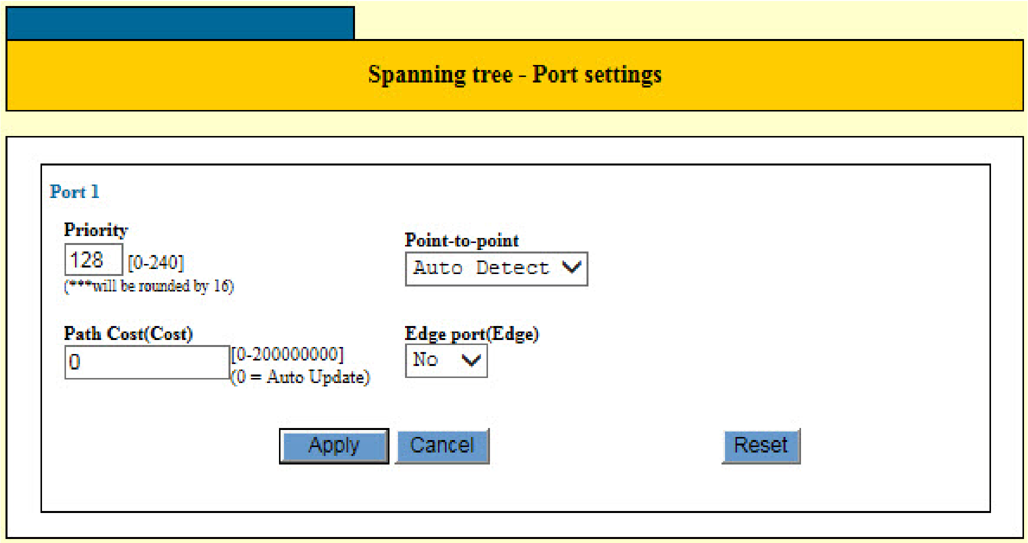
Port	RSTP status	Status	Role	Edge	P2P	Version	Cost
□ 1	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 2	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 3	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 4	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 5	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 6	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 7	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 8	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 9	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 10	Enabled	Forwarding	Root	No	Yes	Rstp	200000
□ 11	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 12	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 13	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 14	Enabled	Forwarding	DEsignated	No	Yes	Rstp	20000
□ 15	Disabled	-	-	-	-	-	-
□ 16	Disabled	-	-	-	-	-	-
□ 17	Disabled	-	-	-	-	-	-

Figure 53. 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 54 on page 226.



Spanning tree - Port settings

Port 1

Priority

128 [0-240]

(***will be rounded by 16)

Point-to-point

Auto Detect

Path Cost(Cost)

0 [0-200000000]

(0 = Auto Update)

Edge port(Edge)

No

Figure 54. Spanning Tree - Port Settings Window

6. Configure the parameters, as needed. The parameters are described in Table 62.

Table 62. 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 62. 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 52 on page 218.

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 211, 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 on the switch. 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 228,

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 29 on page 126.

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 22

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 a specific action 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.

The feature can perform one of several actions if it detects a loop in the wiring topology of a network. The actions are defined in Table 63.

Table 63. 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.

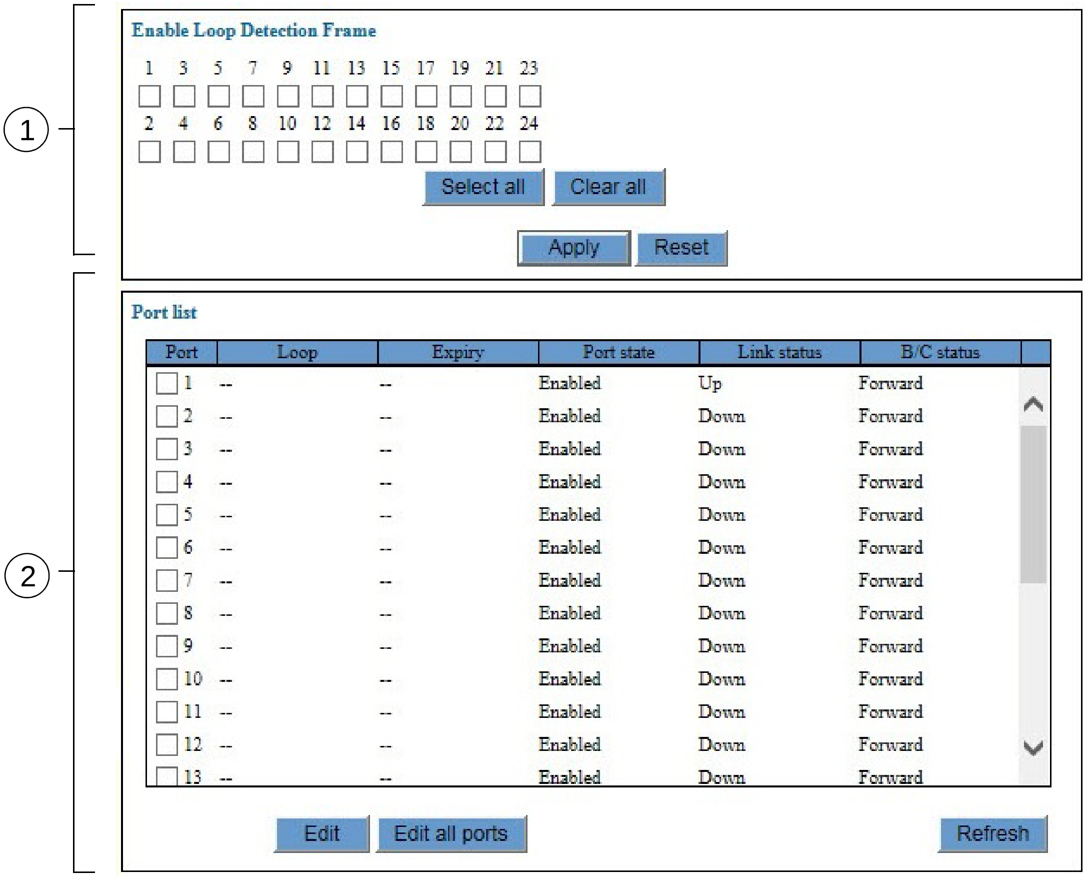
Displaying the Loop Detection Frame Window

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 55.



Port	Loop	Expiry	Port state	Link status	B/C status
□ 1	--	--	Enabled	Up	Forward
□ 2	--	--	Enabled	Down	Forward
□ 3	--	--	Enabled	Down	Forward
□ 4	--	--	Enabled	Down	Forward
□ 5	--	--	Enabled	Down	Forward
□ 6	--	--	Enabled	Down	Forward
□ 7	--	--	Enabled	Down	Forward
□ 8	--	--	Enabled	Down	Forward
□ 9	--	--	Enabled	Down	Forward
□ 10	--	--	Enabled	Down	Forward
□ 11	--	--	Enabled	Down	Forward
□ 12	--	--	Enabled	Down	Forward
□ 13	--	--	Enabled	Down	Forward

Figure 55. Switch Settings - Loop Detection Frame Window

The sections in the window are described in Table 64 on page 234.

Table 64. 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 237.
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 238. The columns in the table are described in Table 65.

The Port List table displays the current state of the Loop Detection Frame feature on the ports. The columns are described in Table 65.

Table 65. 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 65. 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 107, 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 107.

Table 65. 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 238.

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 55 on page 233.
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.

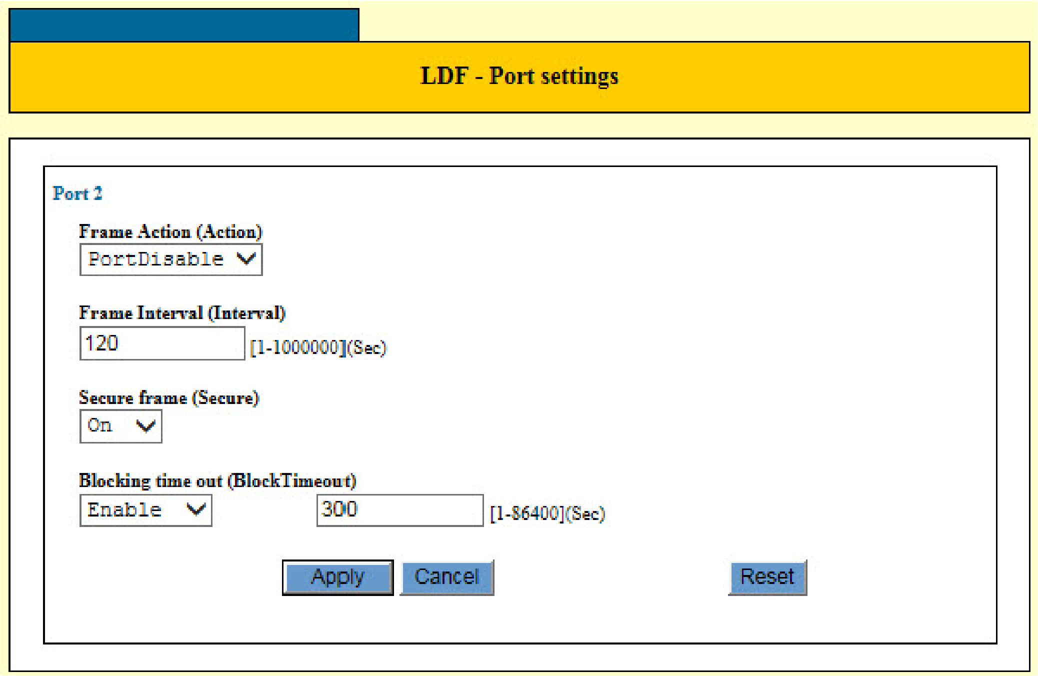
2. Select the Loop Detection Feature option from the Switch Settings menu.

   The Switch Settings - Loop Detection Feature window is shown in Figure 55 on page 233.

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 56.



LDF - Port settings

Port 2

Frame Action (Action)
PortDisable

Frame Interval (Interval)
120 [1-1000000](Sec)

Secure frame (Secure)
On

Blocking time out (BlockTimeout)
Enable 300 [1-86400](Sec)

Figure 56. LDF - Port Settings Window

5. Configure the parameters, as needed. The parameters are described in Table 66 on page 239.

Table 66. 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 66. 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 107, 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.

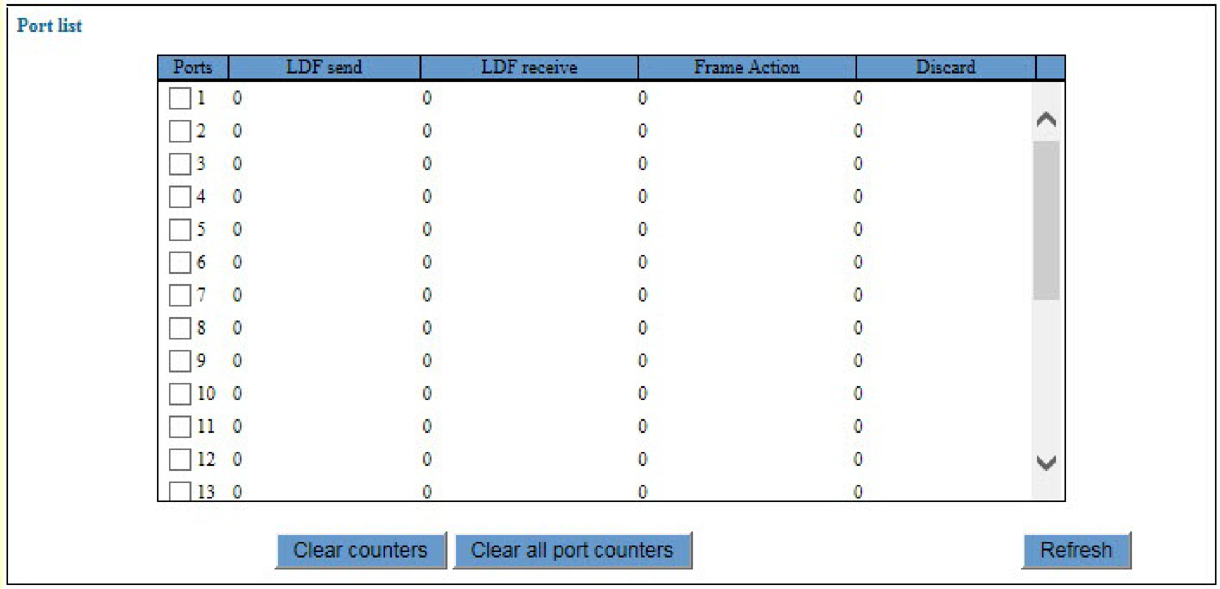
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

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 57.



Ports	LDF send	LDF receive	Frame Action	Discard
□ 1	0	0	0	0
□ 2	0	0	0	0
□ 3	0	0	0	0
□ 4	0	0	0	0
□ 5	0	0	0	0
□ 6	0	0	0	0
□ 7	0	0	0	0
□ 8	0	0	0	0
□ 9	0	0	0	0
□ 10	0	0	0	0
□ 11	0	0	0	0
□ 12	0	0	0	0
□ 13	0	0	0	0

Figure 57. Device Monitoring - Loop Detection Frame Window

The columns in the table are described in Table 67.

Table 67. 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 67. 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 23

IGMP Snooping

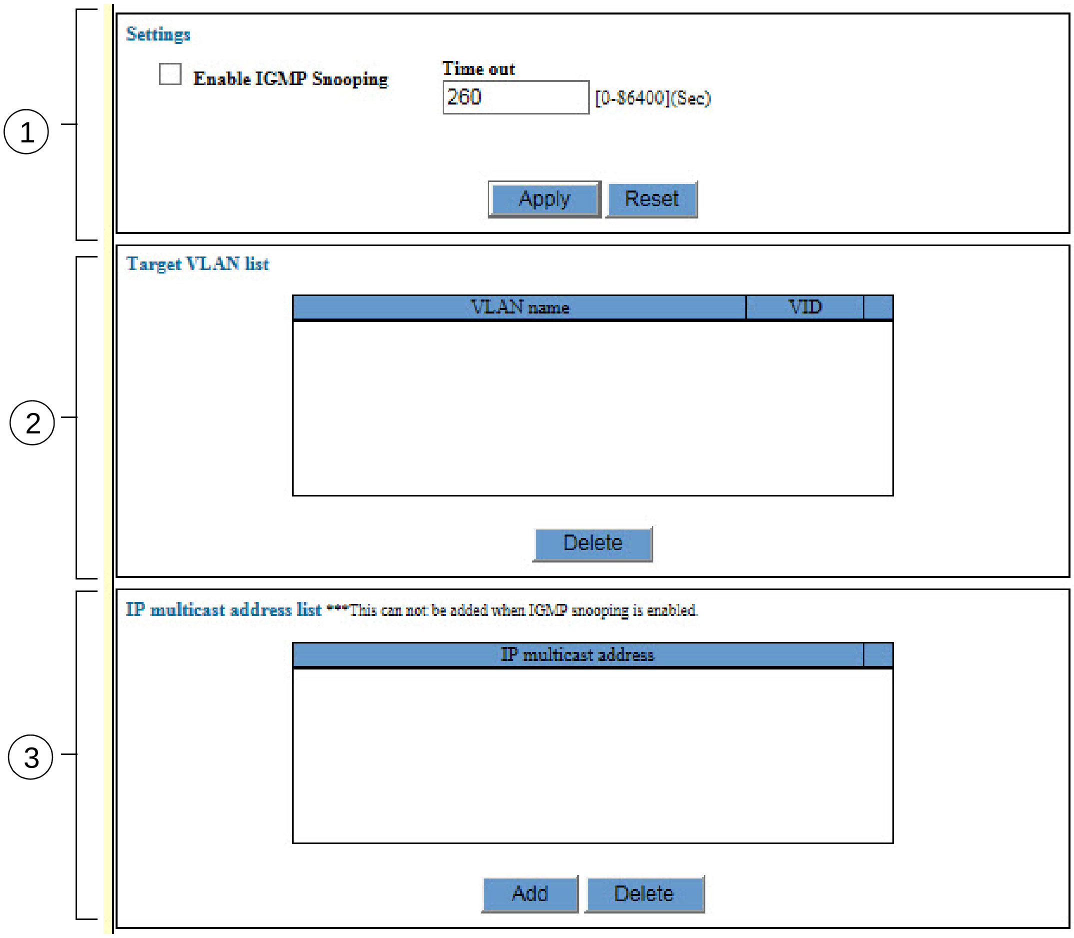
This chapter contains the configuration instructions for the IGMP snooping feature on the switch. The procedures are listed here:

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 58.



Settings

□ Enable IGMP Snooping

Time out: 260 [0-86400](Sec)

Target VLAN list

VLAN name	VID

IP multicast address list ***This can not be added when IGMP snooping is enabled.

IP multicast address

Figure 58. Switch Settings - IGMP Snooping Window

The sections in the window are described in Table 68.

Table 68. Switch Settings - IGMP Snooping Window

Section	Description
1	Use this section to enable or disable IGMP snooping, or to configure the timeout parameter. Refer to “Enabling or Disabling IGMP Snooping” on page 246.

Table 68. Switch Settings - IGMP Snooping Window (Continued)

Section	Description
2	Use this section to view the names and VIDs of the VLANs with multicast addresses. VLANs without multicast addresses are not included in the table. You may also use this section to delete multicast addresses. For instructions, refer to “Deleting All the Static Multicast Addresses of a VLAN” on page 251.
3	Use this section to view and manage the multicast addresses on the switch. The section displays the multicast address of only one VLAN at a time. To view the multicast addresses of a VLAN, select the VLAN in the Target VLAN List section of the window. For instructions, refer to “Adding Static Multicast Addresses” on page 248 or “Deleting Static Multicast Addresses” on page 250.

Enabling or Disabling IGMP Snooping

To enable or disable IGMP snooping or to configure the timeout parameter, 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 58 on page 244.

3. Configure the parameters in the top part of the window.

   The parameters are defined in Table 69.

Table 69. 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.

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

This procedure explains how to add static multicast addresses to the switch.

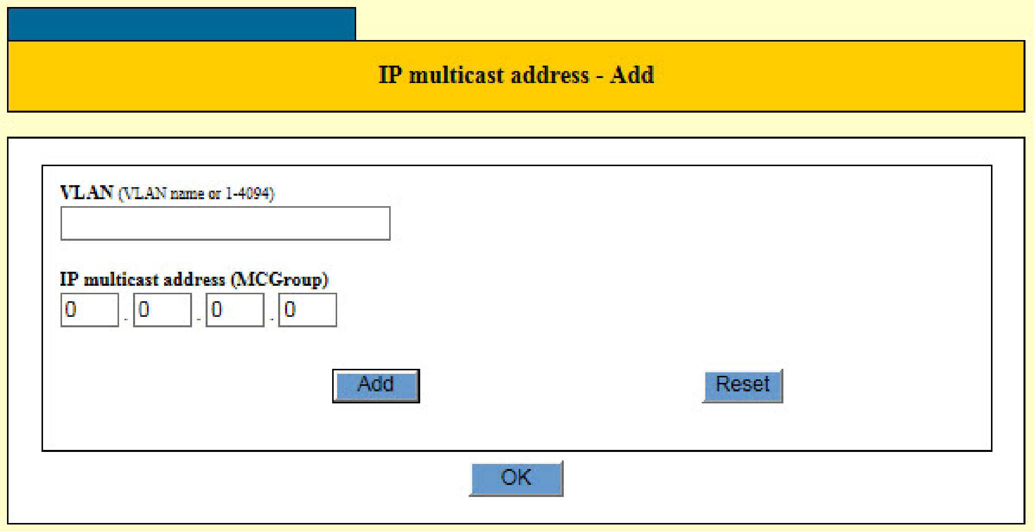
Note
IGMP snooping has to be disabled when you add addresses. To disable IGMP snooping, refer to “Enabling or Disabling IGMP Snooping” on page 246.

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 58 on page 244.
3. In the Add button in the IP Multicast Address List section of the window.

   The IP Multicast Address - Add window is shown in Figure 59.



IP multicast address - Add

VLAN (VLAN name or 1-4094)

IP multicast address (MCGroup)
0 . 0 . 0 . 0

Figure 59. IP Multicast Address - Add Window

4. Configure the parameters in the window, as needed. The parameters are defined in Table 70 on page 249.

Table 70. IP Multicast Address - Add Window

Parameter	Description
VLAN	Use this parameter to specify the name or VID of the VLAN of the multicast address. The VLAN must already exist on the switch. You may specify only one VLAN.
IP Multicast Address (MCGroup)	Use this parameter to enter the multicast address.

5. Click the Add button.

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

Deleting Static Multicast Addresses

To delete specific 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 58 on page 244.
3. In the Target VLAN List table of the window, click the dialog circle of the VLAN with an multicast address to be deleted.

   You may select only one VLAN at a time. The multicast addresses of the selected VLAN are displayed in the IP Multicast Address List section of the window.
4. In the IP Multicast Address List section of the window, click the dialog circle of an address you want to delete.

   You may delete only one multicast address at a time.
5. Click the Delete button beneath the IP Multicast Address List section of the window.
6. At the confirmation prompt, click OK.

   The switch deletes the multicast address.
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.

Deleting All the Static Multicast Addresses of a VLAN

To delete all of the static multicast addresses of a VLAN on 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 58 on page 244.

3. In the Target VLAN List table of the window, click the dialog circle of the VLAN whose multicast addresses are to be deleted.

   You may select only one VLAN at a time.

4. Click the Delete button beneath the Target VLAN List table in the window.

5. At the confirmation prompt, click OK.

   The switch removes the VLAN from the Target VLAN List table and deletes its multicast addresses.

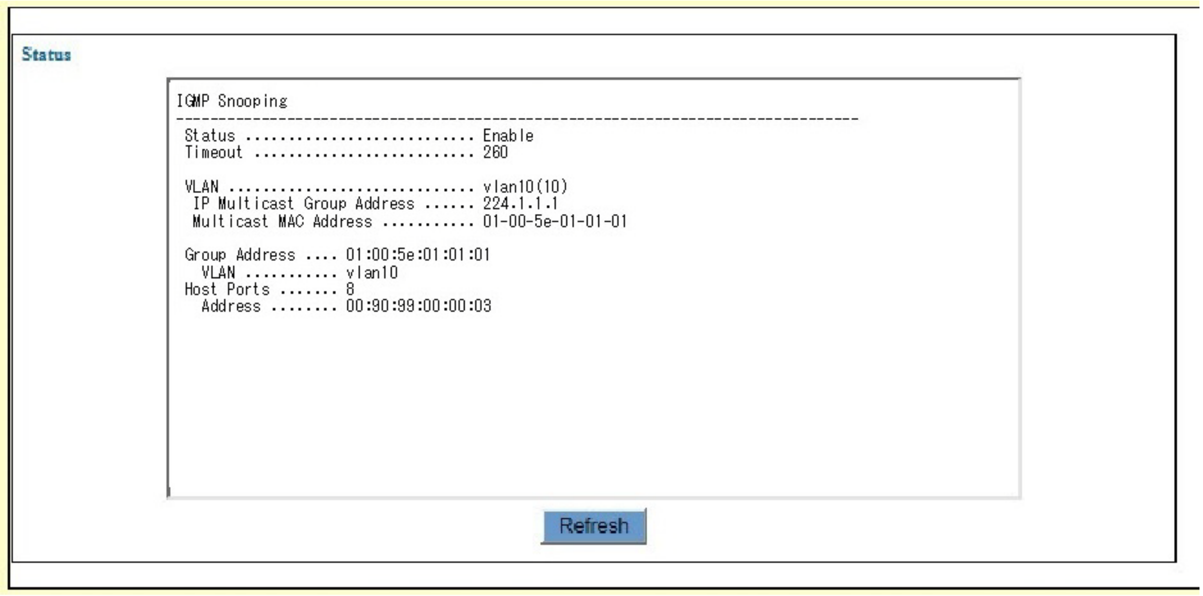
6. To permanently save your changes in the configuration file, click the Save button above the main menu.

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 60.



```
IGMP Snooping
--------------------------------------------------------------------------------
 Status ........................... Enable
 Timeout .......................... 260

 VLAN ............................. vlan10(10)
  IP Multicast Group Address ...... 224.1.1.1
  Multicast MAC Address ........... 01-00-5e-01-01-01

 Group Address .... 01:00:5e:01:01:01
   VLAN ........... vlan10
 Host Ports ....... 8
   Address ........ 00:90:99:00:00:03
```

Figure 60. Device Monitoring - IGMP Snooping Window

Chapter 24

MLD Snooping

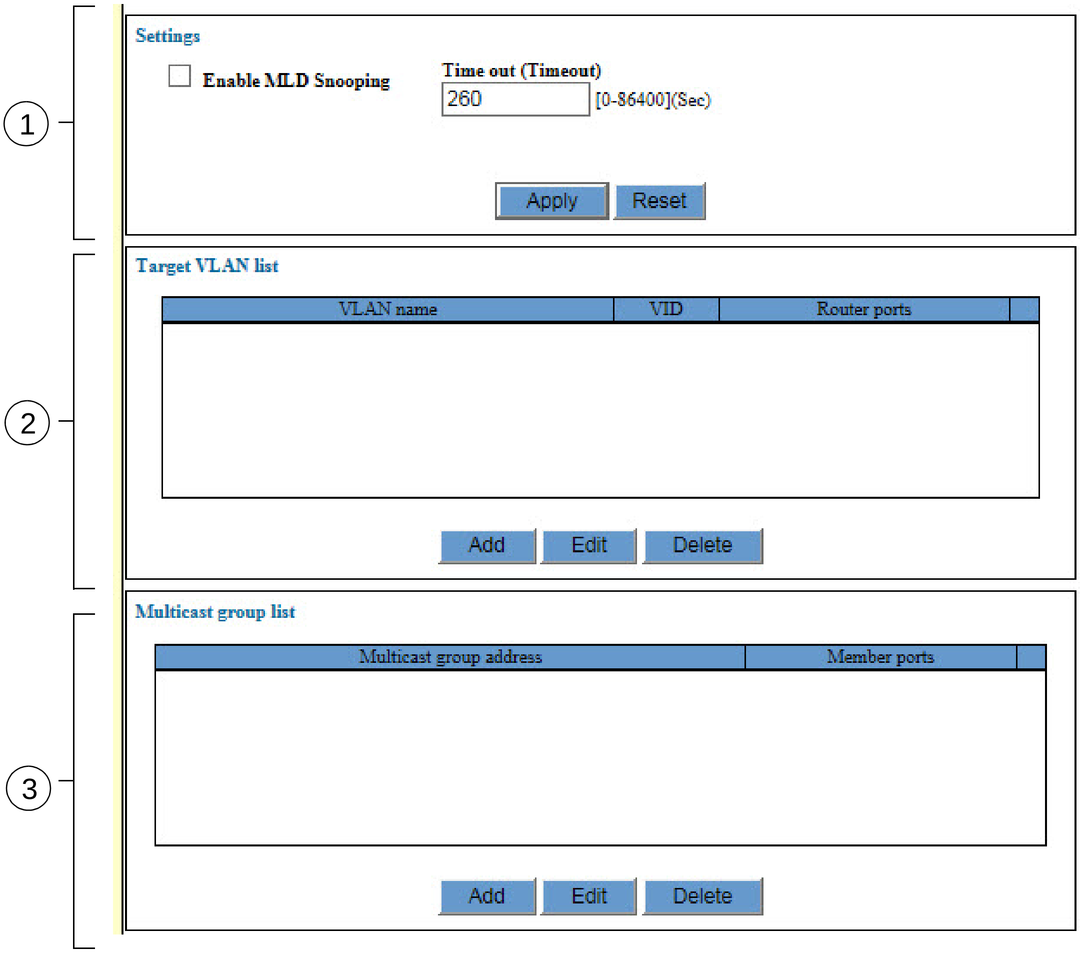
This chapter describes how to configure the MLD snooping feature on the switch. The sections in the chapter are listed here:

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 61.



Settings

☐ Enable MLD Snooping

Time out (Timeout) 260 [0-86400](Sec)

Figure 61. Switch Settings - MLD Snooping Window

The sections in the window are described in Table 71 on page 255.

Table 71. 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 "Enabling or Disabling MLD Snooping" on page 257.
2	Use this section to add or delete VLANs with multicast groups or to designate router ports. Refer to "Adding Multicast Addresses" on page 259 or "Deleting Multicast Addresses" on page 265.
3	Use this section to add, edit, or delete IPv6 multicast addresses or to designate ports with host nodes. Refer to "Adding Multicast Addresses" on page 259, "Editing Multicast Addresses" on page 263, or "Deleting Multicast Addresses" on page 265.

The Target VLAN List table in the middle section of the window lists the names and VIDs of the VLANs with multicast groups. It also displays the port numbers of the routers in the VLANs. The columns in the table are described in Table 72.

Table 72. Target VLAN List Table

Column	Description
VLAN Name	Displays the name of a VLAN with one or more multicast groups.
VID	Displays the VID of a VLAN.
Router Ports	Displays the port in a VLAN on the switch where a multicast router is connected.

The Multicast Group List table in the bottom portion of the window lists the IPv6 multicast addresses of the VLANs and the ports connected to host nodes of the addresses. The table can display the multicast addresses of only one VLAN at a time. To display the multicast addresses of a VLAN, click the dialog circle of the corresponding VLAN in the Target VLAN List section of the window. The columns in the Multicast Group List Default table are described in Table 73 on page 256.

Table 73. Multicast Group List Default Table

Column	Description
Multicast Group Address	Displays the multicast addresses the switch has learned or that were entered manually.
Member Ports	Displays the ports to which host nodes are connected.

Enabling or Disabling MLD Snooping

To enable or disable MLD snooping or to configure the timeout parameter, 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 61 on page 254.

3. Configure the parameters in the top part of the window.

   The parameters are defined in Table 74.

Table 74. 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.
Time out (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.

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 Multicast Addresses

To add 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 61 on page 254.

> **Note**
> If the VLAN of the multicast group is not listed in the Target VLAN List table in the window, perform steps 3 to 5 to add it. If the VLAN is already listed in the table, go to step 6.

3. In the Target VLAN List section of the window, click the Add button.

   The switch displays the MLD Snooping Settings - Add window, shown in Figure 62.

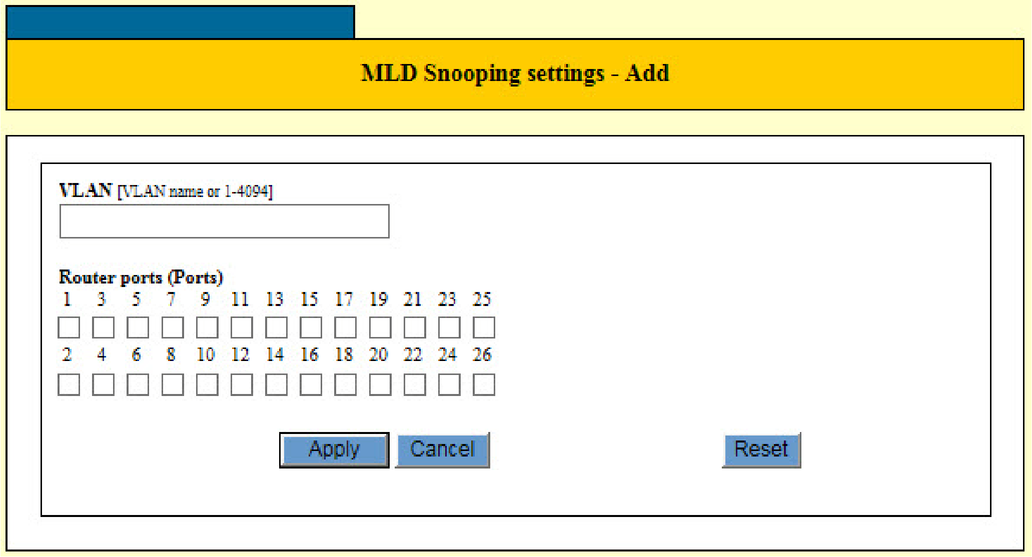


Figure 62. MLD Snooping Settings - Add Window

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

   The parameters are defined in Table 75 on page 260.

Table 75. MLD Snooping Settings - Add Window

Parameter	Description
VLAN (VLAN name or 1 - 4094)	Use this parameter to specify the name or VID of a VLAN for a multicast group. You may specify only one VLAN and it must already exist on the switch.
Router ports (Ports)	Use this parameter to specify the port to which the multicast router is connected to the switch. You may designate more than one router port. A router port must be a tagged or untagged member of the VLAN.

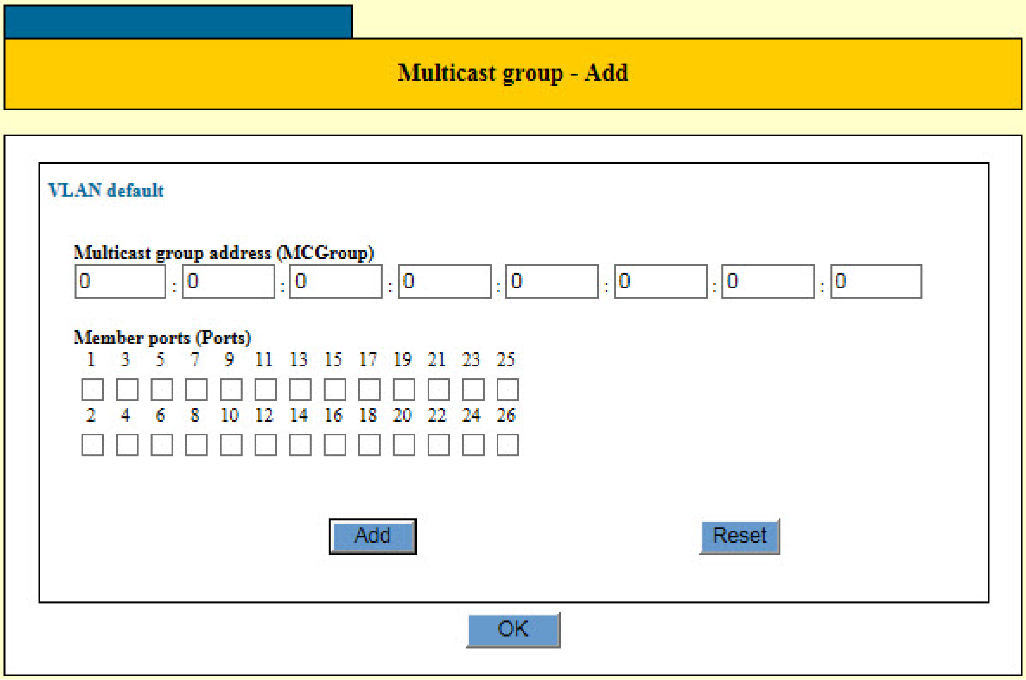
5. Click the Apply button.

   The VLAN is added to the Target VLAN List table.

6. In the Target VLAN List section of the window, click the dialog circle of the VLAN where you want to add the multicast address. You may select only one VLAN.

7. In the Multicast Group List Default section of the window, click the Add button.

   The Multicast Group - Add window is shown in Figure 63.



Multicast group - Add

VLAN default

Multicast group address (MCGroup)

0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Member ports (Ports)

1	3	5	7	9	11	13	15	17	19	21	23	25
□	□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24	26
□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 63. Multicast Group - Add Window

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

   The parameters are defined in Table 76.

Table 76. Multicast Group - Add Window

Parameter	Description
Multicast Group Address (MCGroup)	Use this parameter to specify the new IPv6 multicast address. Here are the guidelines to the parameter: You may enter only one address at a time. You may not enter a range of addresses.
Member Ports (Ports)	Use the list of ports to designate the ports that are connected to host nodes of a multicast address. A port is selected when its dialog box has a check mark and not selected when the box is empty. Here are the guidelines to this parameter: The ports have to be members of the selected VLAN. You may not designate a router port. If you want the switch to automatically detect the host ports, do not select any ports in the window.

9. Click the Apply button to add the multicast address to the switch.

10. Click the OK button to close the Multicast Group - Add window.

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

Editing Router Ports of VLANs

To change the router port of a multicast VLAN, perform the following procedure:

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

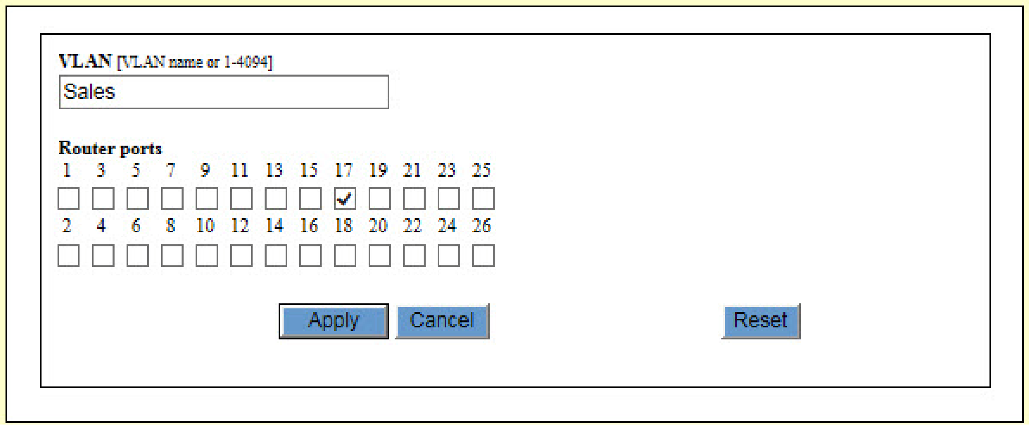
2. Select the MLD Snooping option from the Switch Settings menu.

   The Switch Settings - MLD Snooping window is shown in Figure 61 on page 254.

3. In the Target VLAN List section of the window, click the dialog circle of the VLAN with the multicast address whose router port you want to change. You may edit only one VLAN at a time.

4. Click the Edit button beneath the Target VLAN List section.

   The switch displays the MLD Snooping Settings - Edit window. An example of the window is shown in Figure 64.



VLAN [VLAN name or 1-4094]

Sales

Router ports

1	3	5	7	9	11	13	15	17	19	21	23	25
□	□	□	□	□	□	□	□	☑	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24	26
□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 64. MLD Snooping Settings - Edit Window

5. Edit the list of router ports of the VLAN, as needed.

   A VLAN may have more than one router port. You must designate at least one router port. You may not change the VLAN.

6. Click the Apply button.

   The change is applied to the VLAN.

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

Editing Multicast Addresses

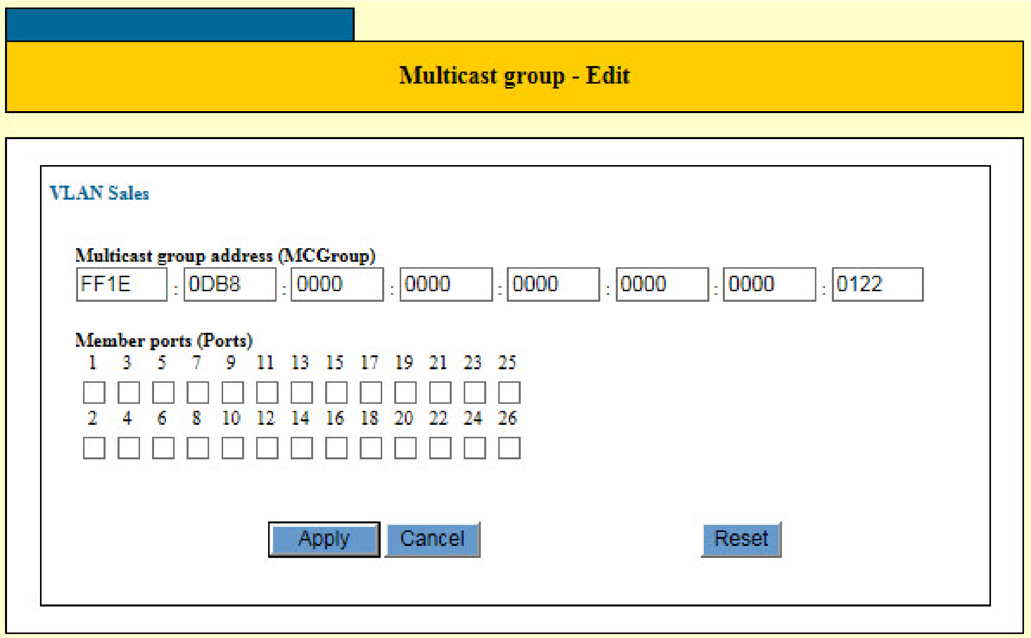
To change the host ports of IPv6 multicast addresses, perform the following procedure:

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 61 on page 254.

3. In the Target VLAN List section of the window, click the dialog circle of the VLAN with the multicast address whose host ports you want to change.
4. In the Multicast Group List Default section of the window, click the dialog circle of the multicast address you want to change.

   The switch displays the Multicast Group - Edit window. An example of the window is shown in Figure 63.



Multicast group - Edit

VLAN Sales

Multicast group address (MCGroup)

FF1E : 0DB8 : 0000 : 0000 : 0000 : 0000 : 0000 : 0122

Member ports (Ports)

1	3	5	7	9	11	13	15	17	19	21	23	25
□	□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24	26
□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 65. Multicast Group - Edit Window

5. Adjust the host ports in the Member Ports (Ports) section of the window, as needed. Here are the guidelines:

   - You may not change the multicast address.
   - You may select more than one host port.

- Host ports have to be members of the VLAN selected in step 3.
- You may not select a router port.
- Do not designate any ports as host ports if you want the switch to automatically determine the host ports.

6. Click the Apply button to add the multicast address to the switch.

7. Click the OK button to close the Multicast Group - Add window.

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

Deleting Multicast Addresses

To delete 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 61 on page 254.
3. In the Target VLAN List section of the window, click the dialog circle of the VLAN containing the multicast address you want to delete.
4. In the Multicast Group List 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.
5. Click the Delete button beneath the Multicast Group List section.

   The switch displays a confirmation prompt.
6. Click the OK button to delete the multicast address.
7. To permanently save your changes in the configuration file, click the Save button above the main menu.

Deleting All the Multicast Addresses of a VLAN

To delete all of the multicast addresses of a VLAN, 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 61 on page 254.

3. In the Target VLAN List section of the window, click the dialog circle of the VLAN containing the multicast address you want to delete.

4. In the Target VLAN List section of the window, click the Delete button.

   The switch displays a confirmation prompt.

5. Click the OK button to delete all the multicast address of the VLAN.

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

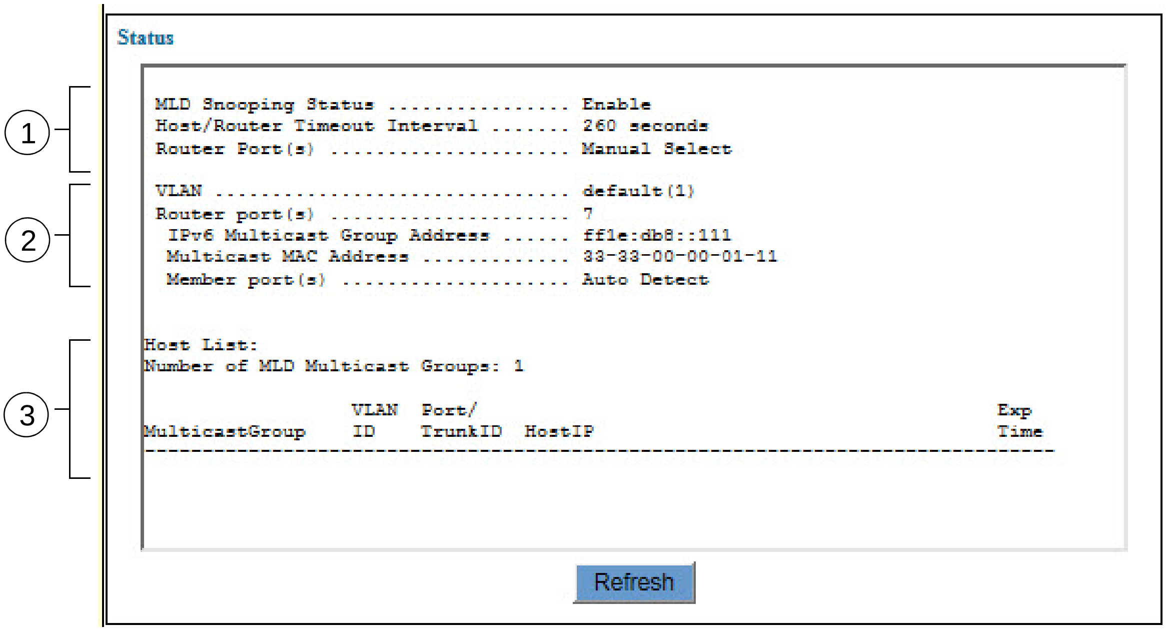
Displaying Multicast Addresses

To display the IPv6 multicast addresses in 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 66.



```
 MLD Snooping Status ................. Enable
 Host/Router Timeout Interval ....... 260 seconds
 Router Port(s) ..................... Manual Select

 VLAN ............................... default(1)
 Router port(s) ..................... 7
  IPv6 Multicast Group Address ...... ff1e:db8::111
  Multicast MAC Address ............. 33-33-00-00-01-11
  Member port(s) .................... Auto Detect


Host List:
Number of MLD Multicast Groups: 1

                  VLAN  Port/                                            Exp
MulticastGroup    ID    TrunkID  HostIP                                  Time
------------------------------------------------------------------------------
```

Figure 66. Device Monitoring - MLD Snooping

The fields in section 1 contain the current settings for MLD snooping and are defined in Table 74 on page 257. (The Router Port(s) parameter is not adjustable. You have to manually designate the router ports when adding the VLANs to the Target VLAN List. For instructions, refer to “Adding Multicast Addresses” on page 259.)

Section 2 displays the specifications of the multicast addresses.

Section 3 lists the host nodes of the addresses. The columns in the table are defined in Table 77 on page 268.

Table 77. 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 25

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 78.

Table 78. 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 107. To enable a port from the command line interface, use the ENABLE SWITCH PORT command.

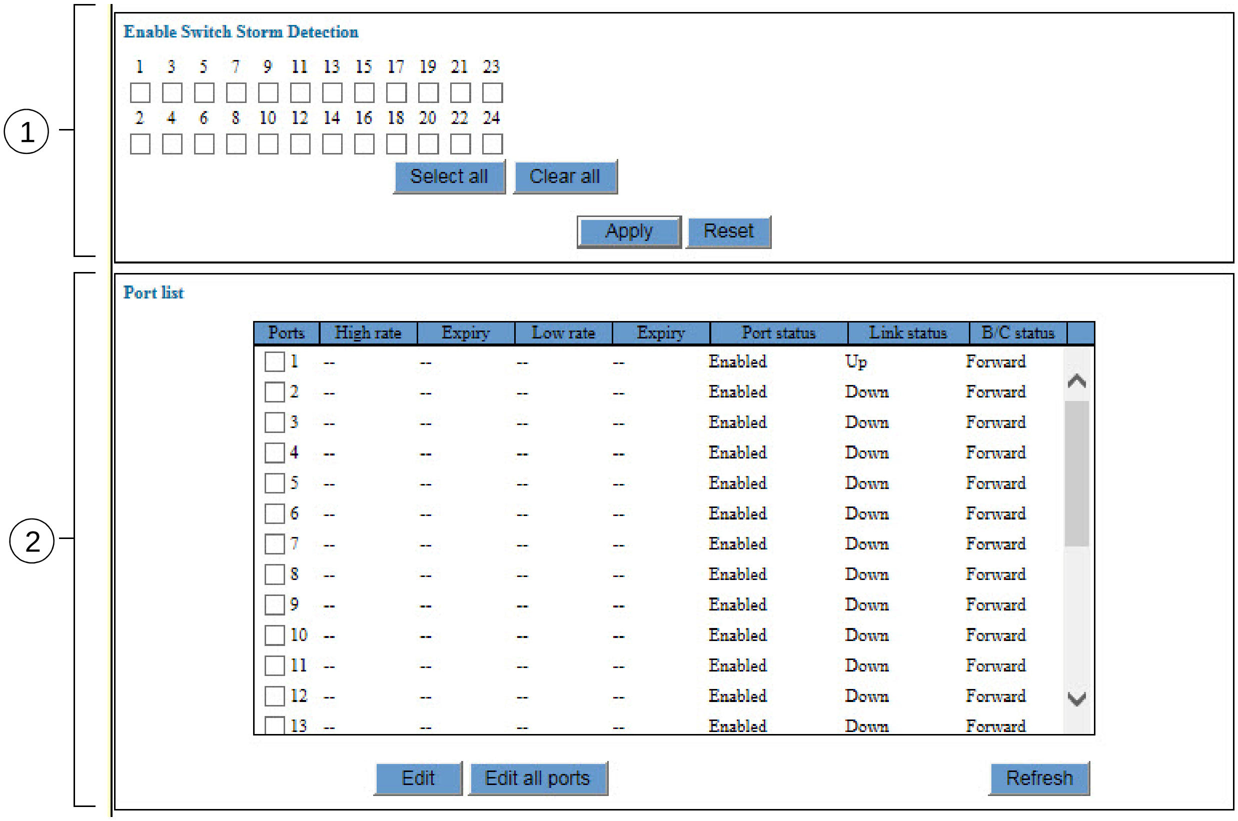
- You may apply packet rate thresholds to the ports of a static port trunk, but the action should be either LinkDown or None.
- The time duration for the LinkDown action should not be less than 60 seconds.The action may not work correctly if the time duration is less than 60 seconds.

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 67.



Ports	High rate	Expiry	Low rate	Expiry	Port status	Link status	B/C status
□ 1	--	--	--	--	Enabled	Up	Forward
□ 2	--	--	--	--	Enabled	Down	Forward
□ 3	--	--	--	--	Enabled	Down	Forward
□ 4	--	--	--	--	Enabled	Down	Forward
□ 5	--	--	--	--	Enabled	Down	Forward
□ 6	--	--	--	--	Enabled	Down	Forward
□ 7	--	--	--	--	Enabled	Down	Forward
□ 8	--	--	--	--	Enabled	Down	Forward
□ 9	--	--	--	--	Enabled	Down	Forward
□ 10	--	--	--	--	Enabled	Down	Forward
□ 11	--	--	--	--	Enabled	Down	Forward
□ 12	--	--	--	--	Enabled	Down	Forward
□ 13	--	--	--	--	Enabled	Down	Forward

Figure 67. Switch Settings - Switch Storm Detection Window

The sections in the window are described in Table 79 on page 273.

Table 79. 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 277.
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 80. For instructions on how to configure the port parameters, refer to “Configuring Switch Storm Detection” on page 278.

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 80.

Table 80. 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 80. 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 107, 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 80. 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 107.
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 80. 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 278.

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 67 on page 272.
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.

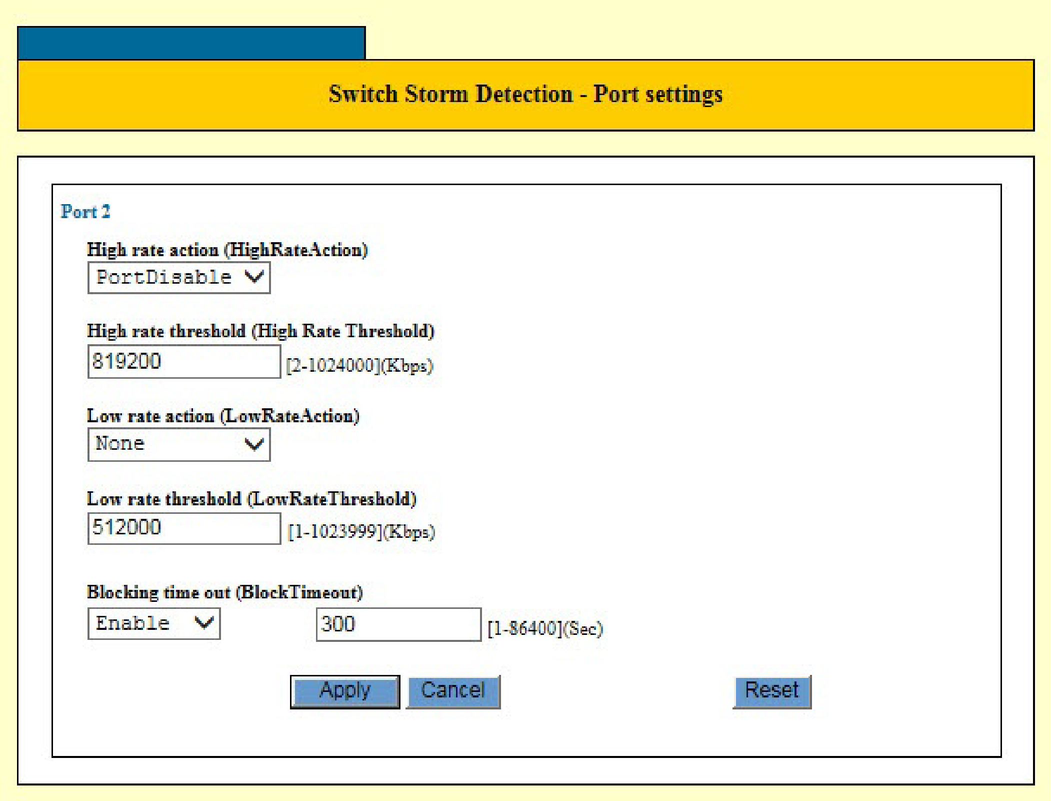
2. Select the Switch Storm Detection option from the Switch Settings menu.

   The Switch Settings - Switch Storm Detection window is shown in Figure 67 on page 272.

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 68.



Switch Storm Detection - Port settings

Port 2

High rate action (HighRateAction)
PortDisable

High rate threshold (High Rate Threshold)
819200 [2-1024000](Kbps)

Low rate action (LowRateAction)
None

Low rate threshold (LowRateThreshold)
512000 [1-1023999](Kbps)

Blocking time out (BlockTimeout)
Enable 300 [1-86400](Sec)

Figure 68. Switch Storm Detection - Port Settings Window

5. Configure the parameters, as needed. The parameters are described in Table 81.

Table 81. 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 81. 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 107, 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.

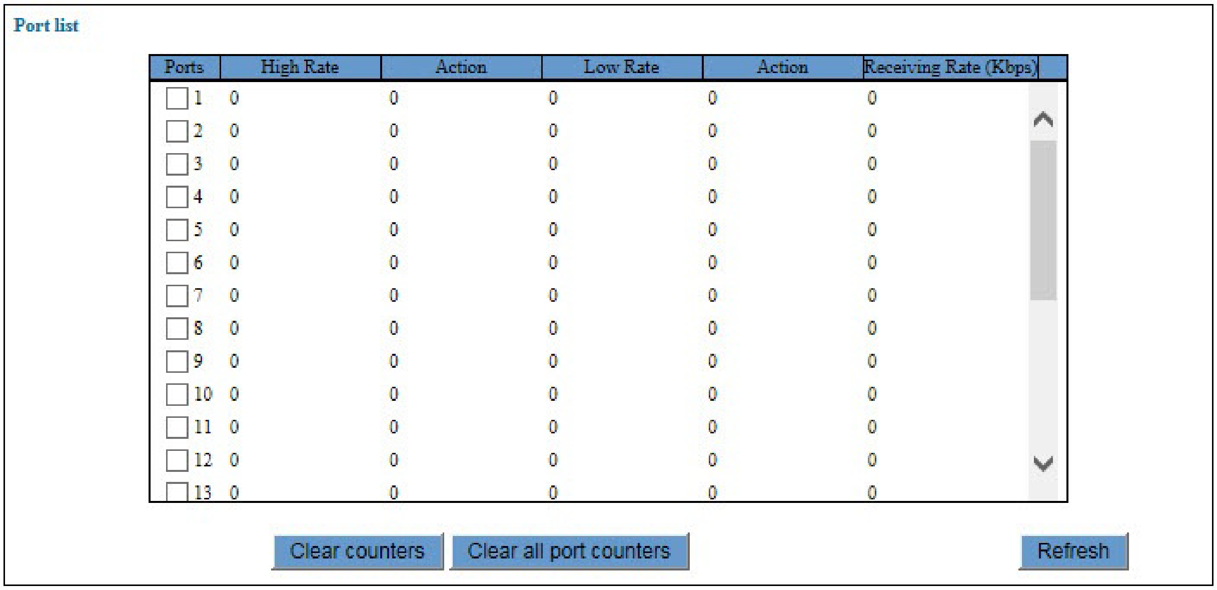
Displaying Statistics for Switch Storm Detection

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 69.



Ports	High Rate	Action	Low Rate	Action	Receiving Rate (Kbps)
□ 1	0	0	0	0	0
□ 2	0	0	0	0	0
□ 3	0	0	0	0	0
□ 4	0	0	0	0	0
□ 5	0	0	0	0	0
□ 6	0	0	0	0	0
□ 7	0	0	0	0	0
□ 8	0	0	0	0	0
□ 9	0	0	0	0	0
□ 10	0	0	0	0	0
□ 11	0	0	0	0	0
□ 12	0	0	0	0	0
□ 13	0	0	0	0	0

Figure 69. Device Monitoring - Switch Storm Database Window

The columns in the table are defined in Table 82.

Table 82. 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 82. Device Monitoring - Switch Storm Database Window (Continued)

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 26

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 70.

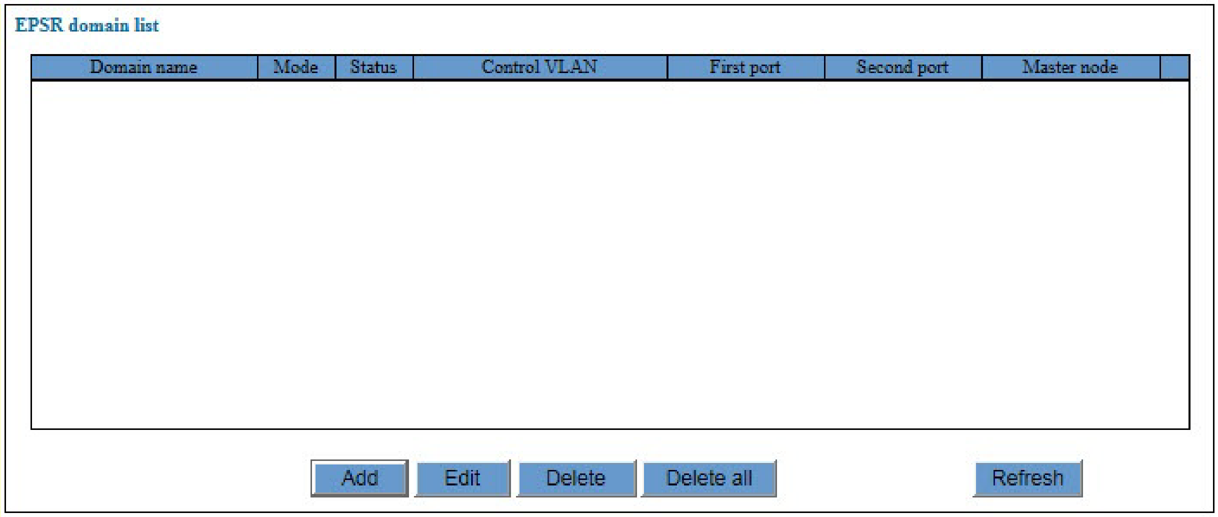


Figure 70. Switch Settings - EPSR Window

The columns in the window are described in Table 83.

Table 83. 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 83. 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:

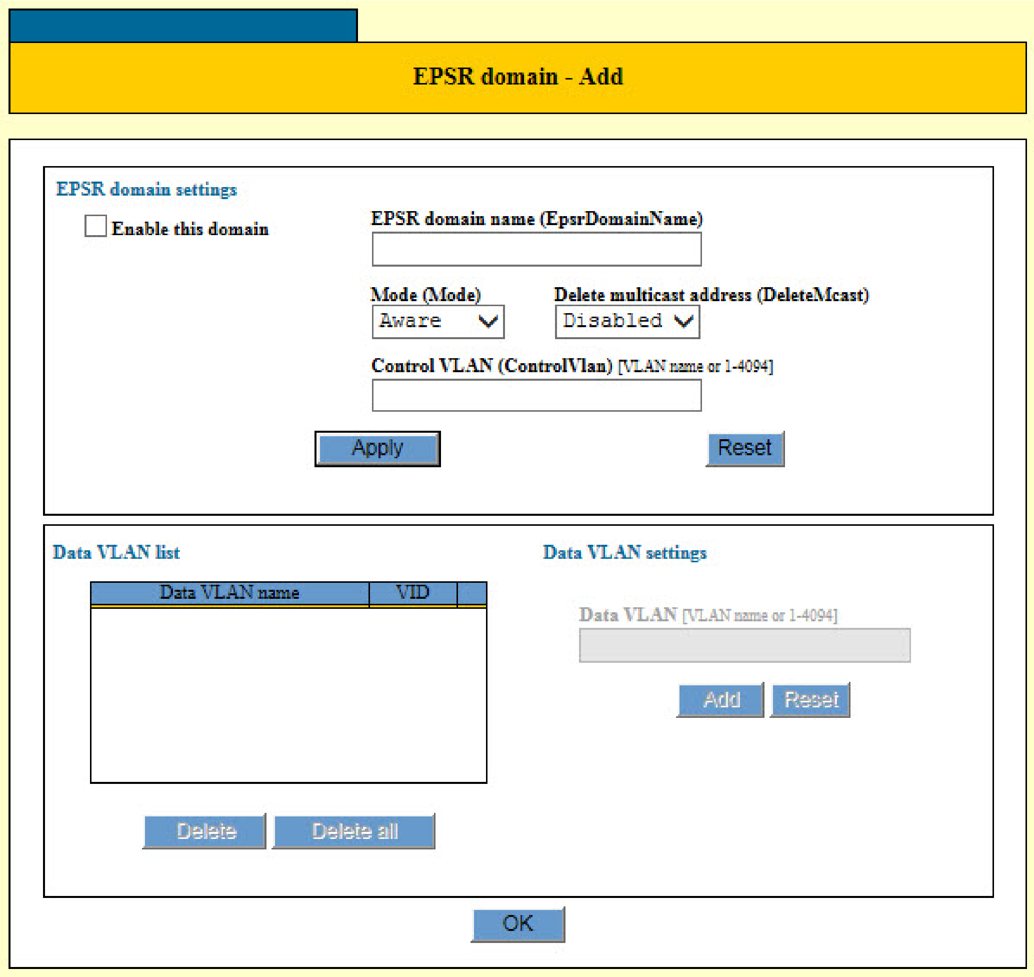
1. Expand the Switch Settings menu in the main menu.

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

   The EPSR window is shown in Figure 70 on page 284.

3. Click the Add button.

   The EPSR Domain - Add window is shown in Figure 71.



EPSR domain - Add

EPSR domain settings

□ Enable this domain

EPSR domain name (EpsrDomainName)

Mode (Mode): Aware

Delete multicast address (DeleteMcast): Disabled

Control VLAN (ControlVlan) [VLAN name or 1-4094]

Data VLAN list

Data VLAN name	VID

Data VLAN settings

Data VLAN [VLAN name or 1-4094]

Figure 71. EPSR Domain - Add Window

4. Configure the parameters in the window, as needed. The parameters are defined in Table 84 on page 287.

Table 84. 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 84 to complete the domain.

7. Click the Add button.

   The VLAN is added to the Data VLAN List table.

8. Repeat steps 6 and 7 if you need to add more data VLANs to the domain.

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 70 on page 284.

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 84 on page 287.
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 84 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 needed.

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 70 on page 284.

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 72.

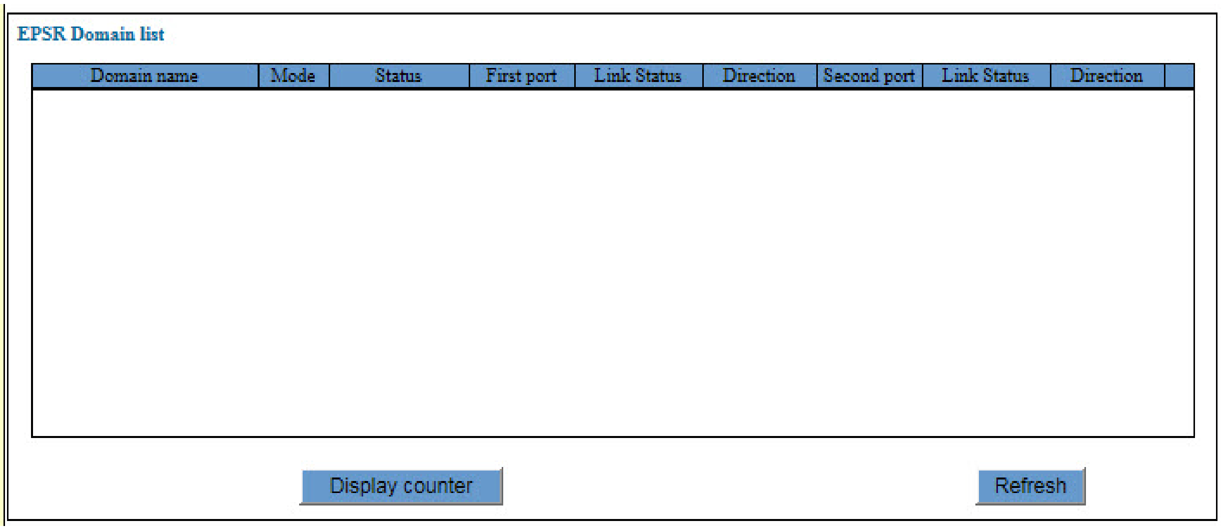


Figure 72. Device Monitoring - EPSR Window

The columns in the window are described in Table 85.

Table 85. 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 85. 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 27

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 sections:

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 managed the device.

Each management interface has its own filter. The different filters are listed in Table 86.

Table 86. 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 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 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 possible unauthorized workstations, which you are not likely to know.

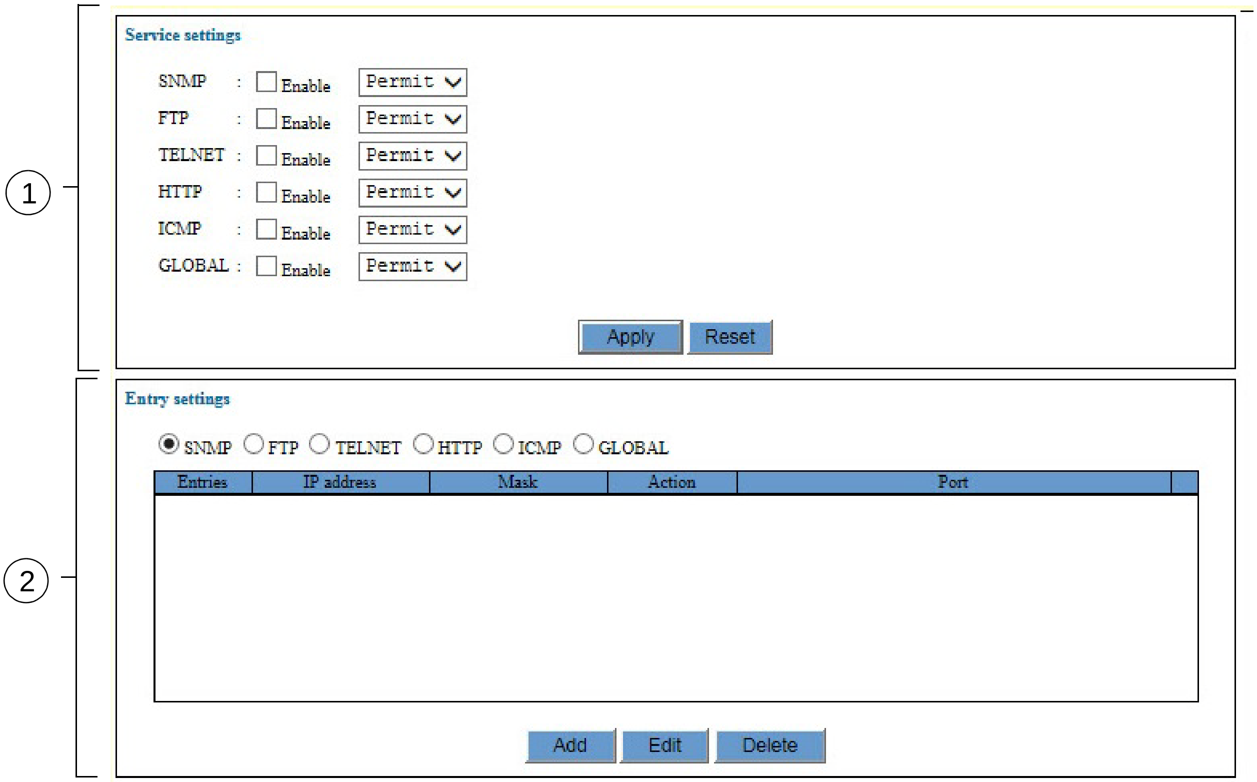
Each management interface has a main filter and individual filter entries. The main filter dictates whether the switch permits or denies access to the switch using the interface. For example, if the Telnet main filter is set to deny, than the switch does not allow any workstation to access the unit using 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 73.



Service settings

SNMP : □ Enable Permit

FTP : □ Enable Permit

TELNET : □ Enable Permit

HTTP : □ Enable Permit

ICMP : □ Enable Permit

GLOBAL : □ Enable Permit

Entry settings

● SNMP ○ FTP ○ TELNET ○ HTTP ○ ICMP ○ GLOBAL

Entries	IP address	Mask	Action	Port

Figure 73. System Settings - Access Filter Window

The sections in the window are defined in Table 87.

Table 87. 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 the Access Filters” on page 298.

Table 87. 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 299 or “Deleting Filter Entries” on page 302

Enabling or Disabling the 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 299.

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 73 on page 296.

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

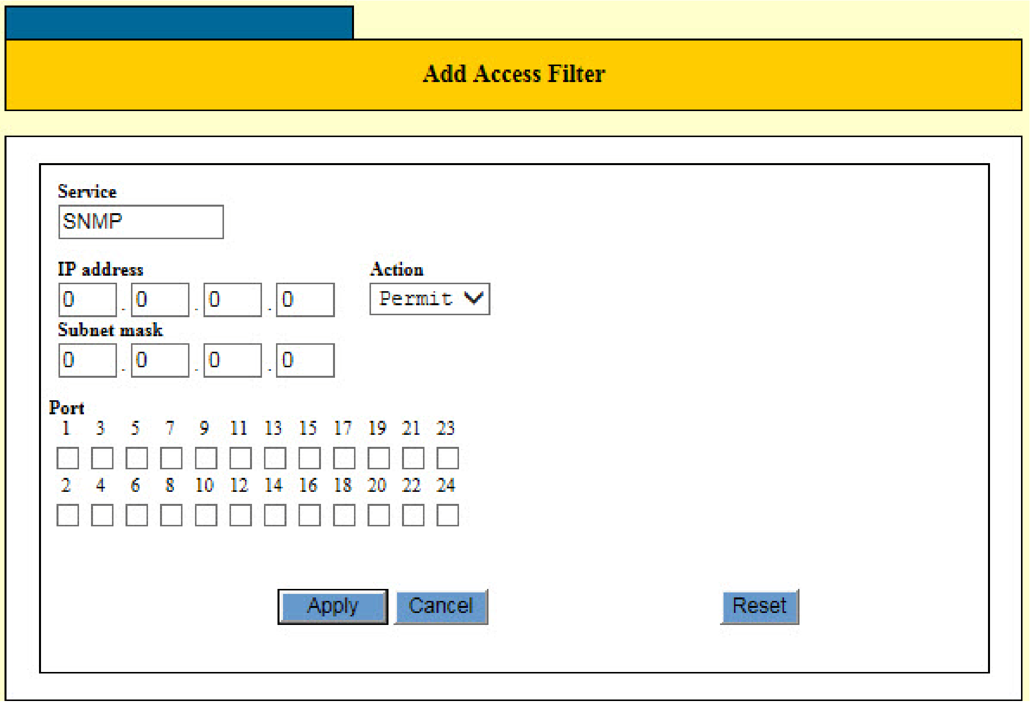
To add a new filter entry, perform the following procedure:

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 73 on page 296.

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 74.



Add Access Filter

Service: SNMP

IP address: 0 . 0 . 0 . 0

Action: Permit

Subnet mask: 0 . 0 . 0 . 0

Port

1	3	5	7	9	11	13	15	17	19	21	23
□	□	□	□	□	□	□	□	□	□	□	□
2	4	6	8	10	12	14	16	18	20	22	24
□	□	□	□	□	□	□	□	□	□	□	□

Figure 74. Add Access Filter Window

5. Configure the parameters, as needed.

   The filters are defined in Table 88 on page 300.

Table 88. 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, is 255.255.255.255. As another example, the mask for the subnet 149.132.45.0 is 255.255.255.0.

Table 88. 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 73 on page 296.

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 28

MAC Address-based Port Security

This chapter explains how to configure the MAC address-based security feature on the ports on the switch. The sections in the chapter are listed here:

Introduction

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 30, “Port Authentication Overview” on page 325. 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 switch deletes all of the static and dynamic addresses on a port 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. Packets with unknown MAC addresses are discarded.

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.

As 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 packets from 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 stops learning new addresses and 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.

As 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 similar to Limited security mode in that it allows ports to learn up to a defined number of MAC addresses and to forward packets of only those network devices. After learning their maximum number of MAC addresses, ports discard packets with unknown addresses.

The difference between the Limited and Dynamic Limit modes relates to how they handle dynamic MAC addresses. With the Limited security level, the switch automatically converts dynamic addresses into static addresses as it adds them to the MAC address table. Consequently, they are never deleted from the table even when network devices are inactive. In contrast, source MAC addresses learned by ports in this security level are entered as dynamic addresses in the MAC address table and 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 can learn a new dynamic address.

Note
The Dynamic Limited security level does not support static addresses. You cannot activate this security level on ports that have static MAC addresses. Additionally, you cannot add static addresses to ports on which this security level has been activated.

Guidelines

Here are the guidelines to MAC address-based port security:

❒ The security feature filters ingress packets, but not egress packets.

❒ You cannot use MAC address-based port security and port authentication on the same port. Authenticator and Supplicant ports have to be set to the Automatic security level, 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.

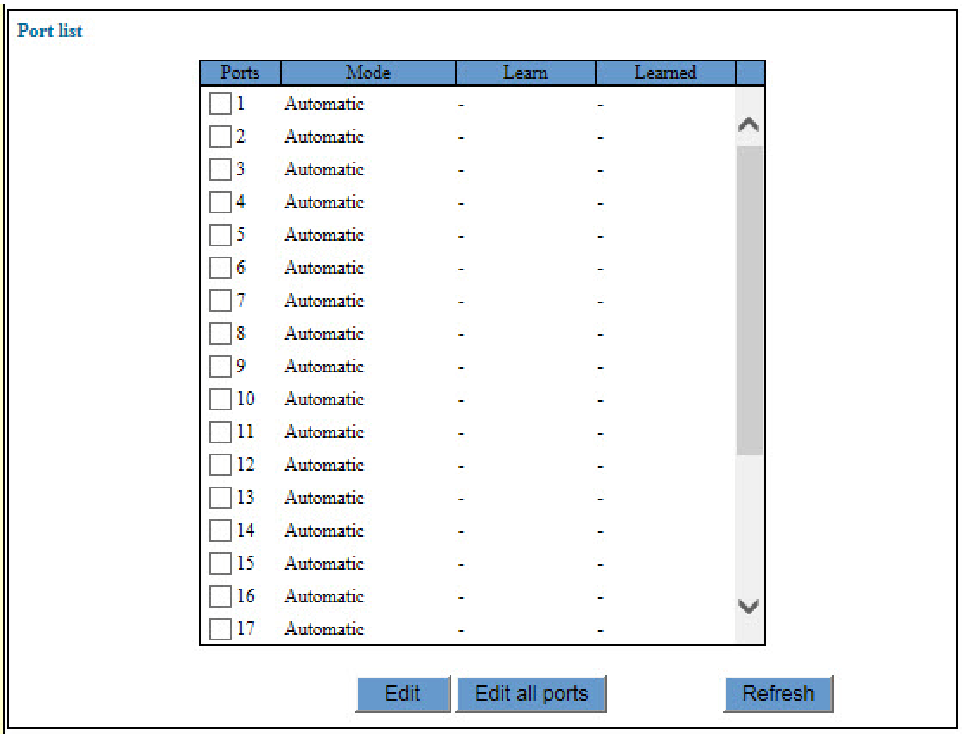
Displaying the MAC Address-based Port Security Window

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 75.



Port list

Ports	Mode	Learn	Learned
□ 1	Automatic	-	-
□ 2	Automatic	-	-
□ 3	Automatic	-	-
□ 4	Automatic	-	-
□ 5	Automatic	-	-
□ 6	Automatic	-	-
□ 7	Automatic	-	-
□ 8	Automatic	-	-
□ 9	Automatic	-	-
□ 10	Automatic	-	-
□ 11	Automatic	-	-
□ 12	Automatic	-	-
□ 13	Automatic	-	-
□ 14	Automatic	-	-
□ 15	Automatic	-	-
□ 16	Automatic	-	-
□ 17	Automatic	-	-

Figure 75. Security Settings - Port Security Window

The table in the window displays the current security settings of the ports. The columns are described in Table 89.

Table 89. 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 “Introduction” on page 304.

Table 89. Security Settings - Port Security Window (Continued)

Column	Description
Learn	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. It does not apply to the Secured mode.

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.

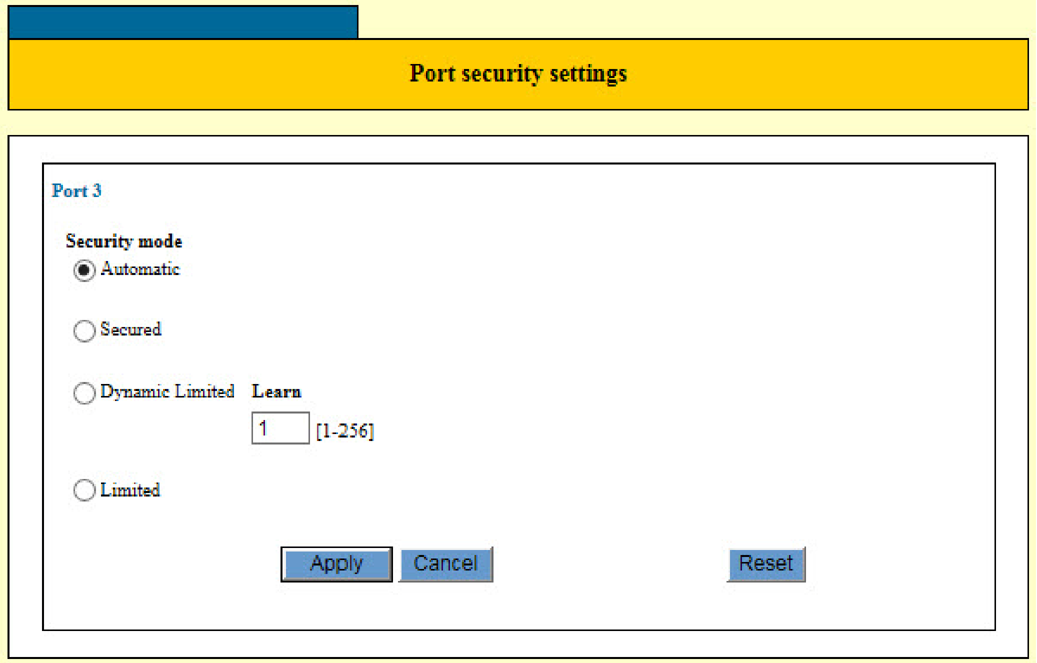
   The Security Settings - Port Security window is shown in Figure 75 on page 308.

3. Click the dialog box of a port. 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 76.



Port security settings

Port 3

Security mode

● Automatic

○ Secured

○ Dynamic Limited Learn 1 [1-256]

○ Limited

Figure 76. Port Security Settings Window

5. Configure the parameters, as needed. The parameters are defined in Table 90.

Table 90. 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 “Introduction” on page 304.
Learn	Use this parameter to specify the maximum number of dynamic MAC addresses a port can learn. This parameter applies to the Dynamic Limited and 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 29

RADIUS Client

This chapter contains instructions on how to configure the RADIUS client on the switch. This chapter contains the following sections:

Introduction

The port authentication feature described in Chapter 31, “Port Authentication” on page 343 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 FS900M Series switches have the client portion of the RADIUS protocol. They do not have a RADIUS server. Consequently, they do not validate 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 46.
- ❐ 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 338.
- 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.

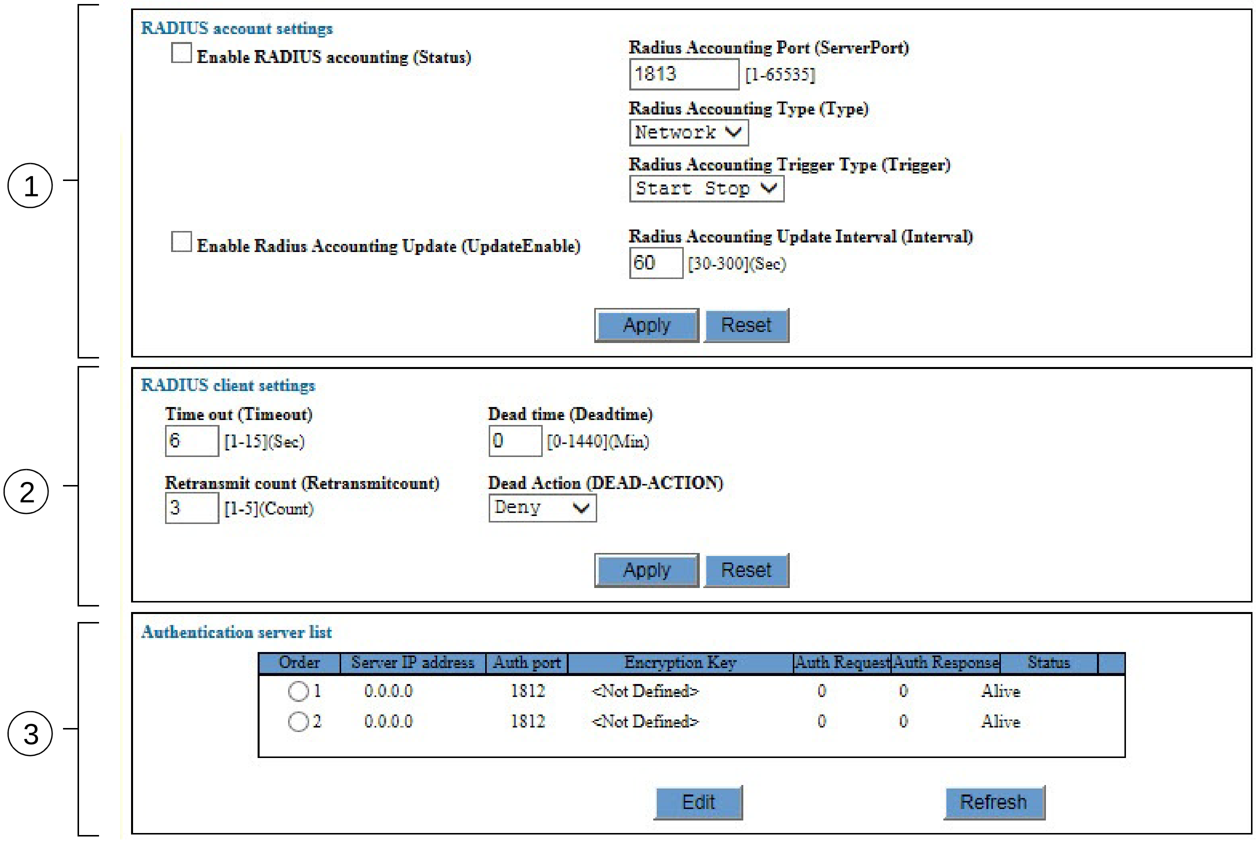
Displaying the RADIUS Client Window

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 77.



RADIUS account settings

□ Enable RADIUS accounting (Status)

Radius Accounting Port (ServerPort)
1813 [1-65535]

Radius Accounting Type (Type)
Network

Radius Accounting Trigger Type (Trigger)
Start Stop

□ Enable Radius Accounting Update (UpdateEnable)

Radius Accounting Update Interval (Interval)
60 [30-300](Sec)

RADIUS client settings

Time out (Timeout)
6 [1-15](Sec)

Dead time (Deadtime)
0 [0-1440](Min)

Retransmit count (Retransmitcount)
3 [1-5](Count)

Dead Action (DEAD-ACTION)
Deny

Authentication server list

Order	Server IP address	Auth port	Encryption Key	Auth Request	Auth Response	Status
○ 1	0.0.0.0	1812	<Not Defined>	0	0	Alive
○ 2	0.0.0.0	1812	<Not Defined>	0	0	Alive

Figure 77. Security Settings - RADIUS Server Window

The sections in the Security Settings - RADIUS Server window are described in Table 91 on page 317.

Table 91. 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 318.
2	Use the parameters in this section to configure the RADIUS client. Refer to “Configuring the RADIUS Client” on page 320.
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 322.

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 338.

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 77 on page 316.

3. Configure the parameters in the RADIUS Account Settings section of the window. The parameters are described in Table 92.

Table 92. 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 92. 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 77 on page 316.
3. Configure the parameters in the RADIUS Client Settings section of the window. The parameters are described in Table 93.

Table 93. 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 93. 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 communications 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.

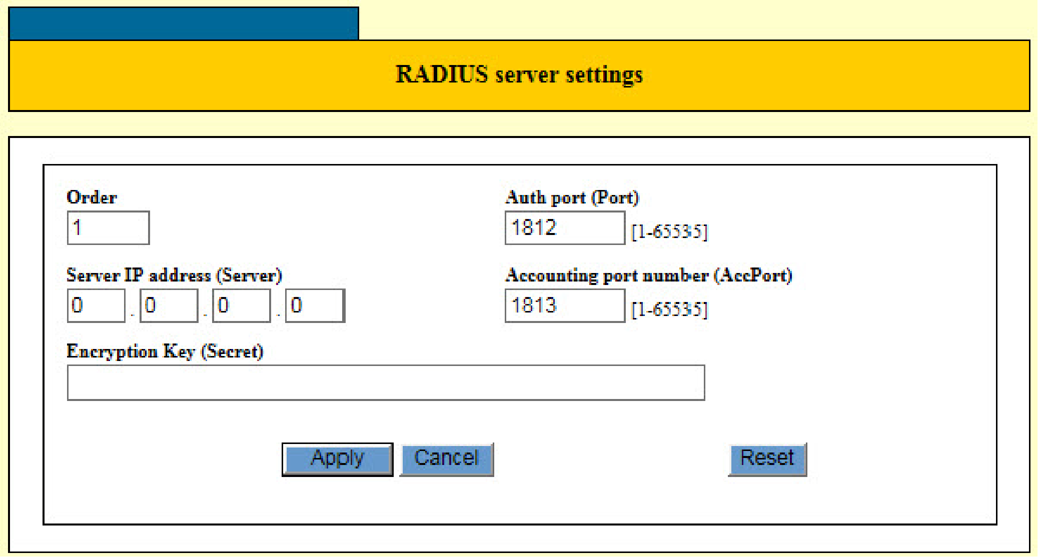
2. Select the RADIUS Server option from the Security Settings menu.

   The Security Settings - RADIUS Settings window is shown in Figure 77 on page 316.

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 78.



Order: 1

Auth port (Port): 1812 [1-65535]

Server IP address (Server): 0 . 0 . 0 . 0

Accounting port number (AccPort): 1813 [1-65535]

Encryption Key (Secret):

Figure 78. RADIUS Server Settings Window

5. Configure the parameters. The parameters are described in Table 94.

Table 94. 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 to 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 30

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. Network users have to 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 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 29, “RADIUS Client” on page 313.

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.

Here are general guidelines to this authentication method:

- The switch supports these authentication methods for 802.1x authentication: EAP-MD5, PEAP (EAP-MSCHAPv2), TLS (with TTLS specified).
- The supplicants must have 802.1x client software.
- This authentication method requires a RADIUS server.

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.

Here are general guidelines to this authentication method:

- MAC address-based authentication supports the PAP authentication method.

- The MAC addresses of the network devices must be entered as the usernames and passwords in the supplicant accounts on the RADIUS server.
- When the switch transmits the MAC addresses of the network devices to the RADIUS server for authentication, it sends the letters “a” to “f” in the hexadecimal addresses in lowercase. Consequently, the letters should be entered in lowercase in the supplicant accounts on the RADIUS server.
- This authentication method requires a RADIUS server.

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.

Here are general guidelines to this authentication method:

- Web browser authentication supports the PAP authentication method.
- You have to enable the web authentication server on the switch.
- The MAC addresses of the network devices must be entered as the usernames and passwords in the supplicant accounts on the RADIUS server.
- This authentication method requires a RADIUS server.

To log on using web browser authentication, supplicants have to enter the IP address of the switch and software port number of the web authenticator server on the switch in the URL field of their web browsers. Here is the format:

http://*ip_address*:*web_server_port_number*

For example, if the IP address of the switch is 149.32.67.12 and the port number of the web authentication server is 8080, supplicants enter the following in the URL fields of their web browsers:

http://149.32.67.12:8080

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 79, 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.

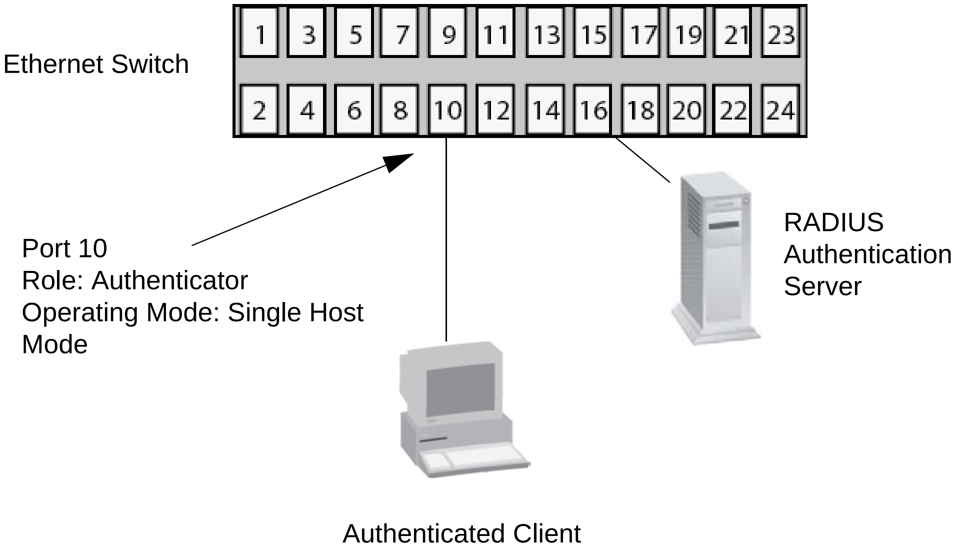


Figure 79. Single Host Mode

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 authenticated.

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 80 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.

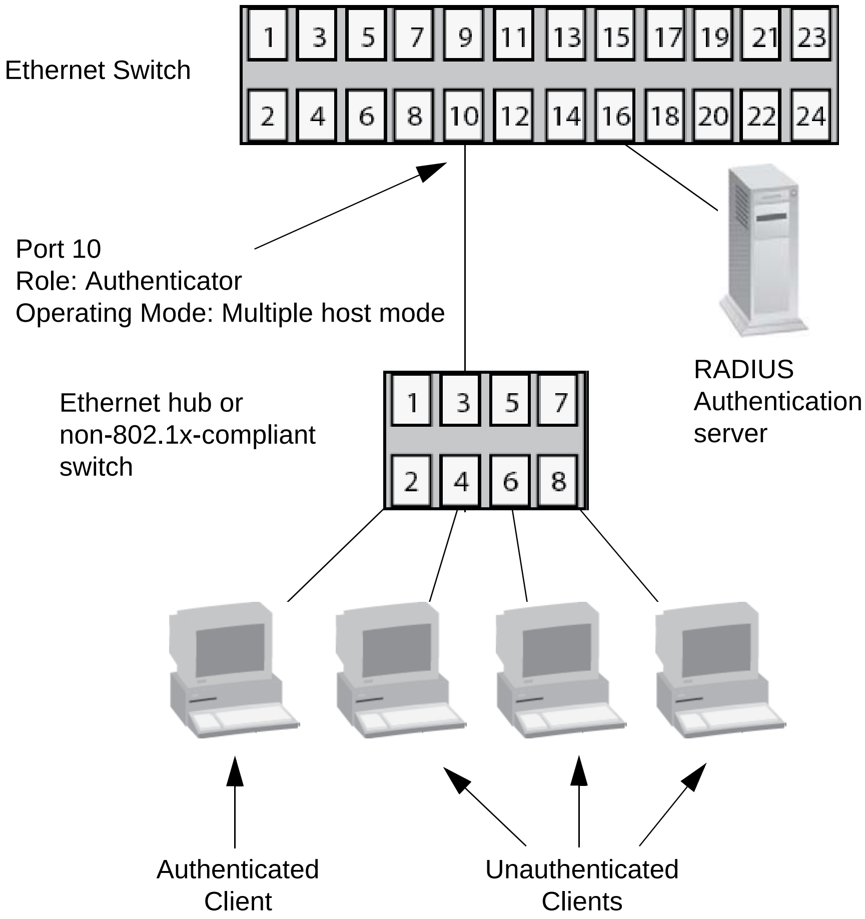


Figure 80. Multiple Host Operating Mode

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 81 on page 333. 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.

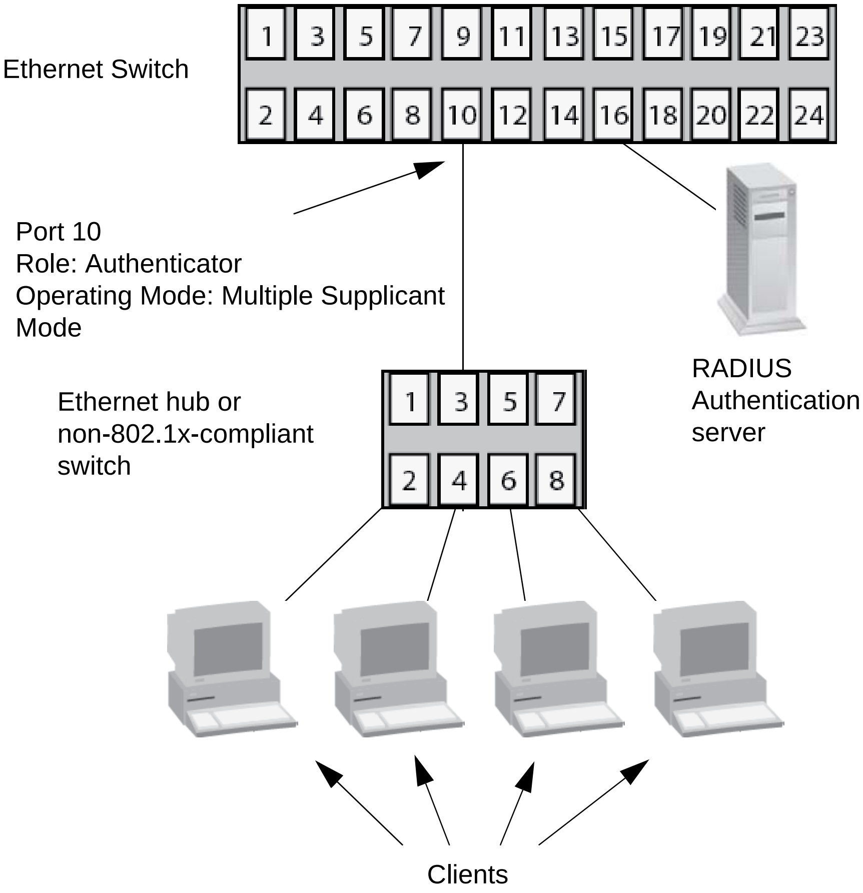

Ethernet Switch
1
3
5
7
9
11
13
15
17
19
21
23
2
4
6
8
10
12
14
16
18
20
22
24
Port 10
Role: Authenticator
Operating Mode: Multiple Supplicant Mode
RADIUS Authentication server
Ethernet hub or non-802.1x-compliant switch
1
3
5
7
2
4
6
8
Clients

Figure 81. 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 14, “Port-based and Tagged VLANs Overview” on page 151, 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 335.

How the switch responds 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 logon 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 log 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 29, “RADIUS Client” on page 313.

5. You must configure the port access control settings on the switch, as explained in Chapter 31, “Port Authentication” on page 343.

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 28, “MAC Address-based Port Security” on page 303.
- Authenticator ports cannot be members of static port trunks or the port mirror.
- The Guest VLAN feature requires that the designated VLAN already exists 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 a management IP address to communicate with the RADIUS server. For background information, refer to "Changing the IP Address Configuration" on page 46.

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 31

Port Authentication

This chapter contains instructions on how to configure the port authentication feature on the switch. The chapter contains the following procedures:

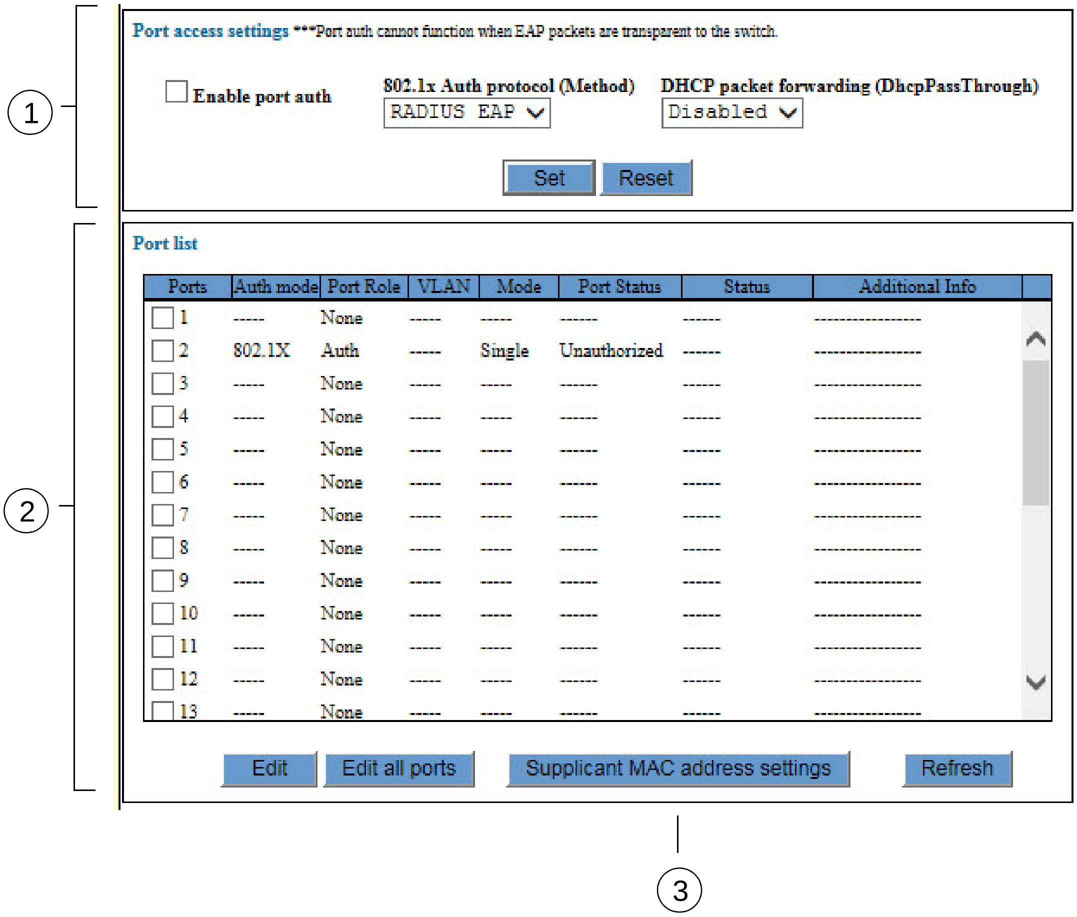
Note
For background information, refer to Chapter 30, “Port Authentication Overview” on page 325.

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 82.



Port access settings ***Port auth cannot function when EAP packets are transparent to the switch.

□ **Enable port auth**

802.1x Auth protocol (Method) RADIUS EAP

DHCP packet forwarding (DhcpPassThrough) Disabled

Port list

Ports	Auth mode	Port Role	VLAN	Mode	Port Status	Status	Additional Info
□ 1	-----	None	-----	-----	------	------	----------------
□ 2	802.1X	Auth	-----	Single	Unauthorized	------	----------------
□ 3	-----	None	-----	-----	------	------	----------------
□ 4	-----	None	-----	-----	------	------	----------------
□ 5	-----	None	-----	-----	------	------	----------------
□ 6	-----	None	-----	-----	------	------	----------------
□ 7	-----	None	-----	-----	------	------	----------------
□ 8	-----	None	-----	-----	------	------	----------------
□ 9	-----	None	-----	-----	------	------	----------------
□ 10	-----	None	-----	-----	------	------	----------------
□ 11	-----	None	-----	-----	------	------	----------------
□ 12	-----	None	-----	-----	------	------	----------------
□ 13	-----	None	-----	-----	------	------	----------------

Figure 82. Security Settings - Port Authentication Window

The sections in the Security Settings - Port Authentication window are defined in Table 95 on page 345.

Table 95. 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 347 or “Disabling Port Authentication on the Switch” on page 370.
2	Use this section to view or configure the authenticator or supplicant settings on the ports. Refer to “Configuring Authenticator Ports” on page 349 or “Configuring Supplicant Ports” on page 362.
3	Use this button to manage non-authenticated network devices. Refer to “Identifying Non-authenticated Network Devices” on page 366.

The Port List table in the window displays port status information. The information is described in Table 96.

Table 96. Port List Table in the Security Settings - Port Authentication Window

Column	Description
Port	Displays the port number.
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.

Table 96. Port List Table in the Security Settings - Port Authentication Window (Continued)

Column	Description
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 330. 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.
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
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 section 1 of the port authentication window (refer to Figure 82 on page 344), 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 82 on page 344.

3. Configure the parameters in the top section of the window, as needed. The parameters are described in Table 97.

Table 97. 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 Auth Protocol (Method)	Use this option to view the authentication method of the authentication server. RADIUS EAP is the only available selection.
DHCP packet forwarding (DhcpPassThrough)	Use this option to enable or disable DHCP packet forwarding. This option applies only to the web browser authentication method. It does not apply to the 802.1x port-based or MAC address-based authentication methods. When the option is enabled, the switch forwards DHCP packets between unauthenticated supplicants and a DHCP server. When the option is disabled, the switch discards the DHCP packets going to or from unauthenticated supplicants.

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

6. Click the Apply button.

7. 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.

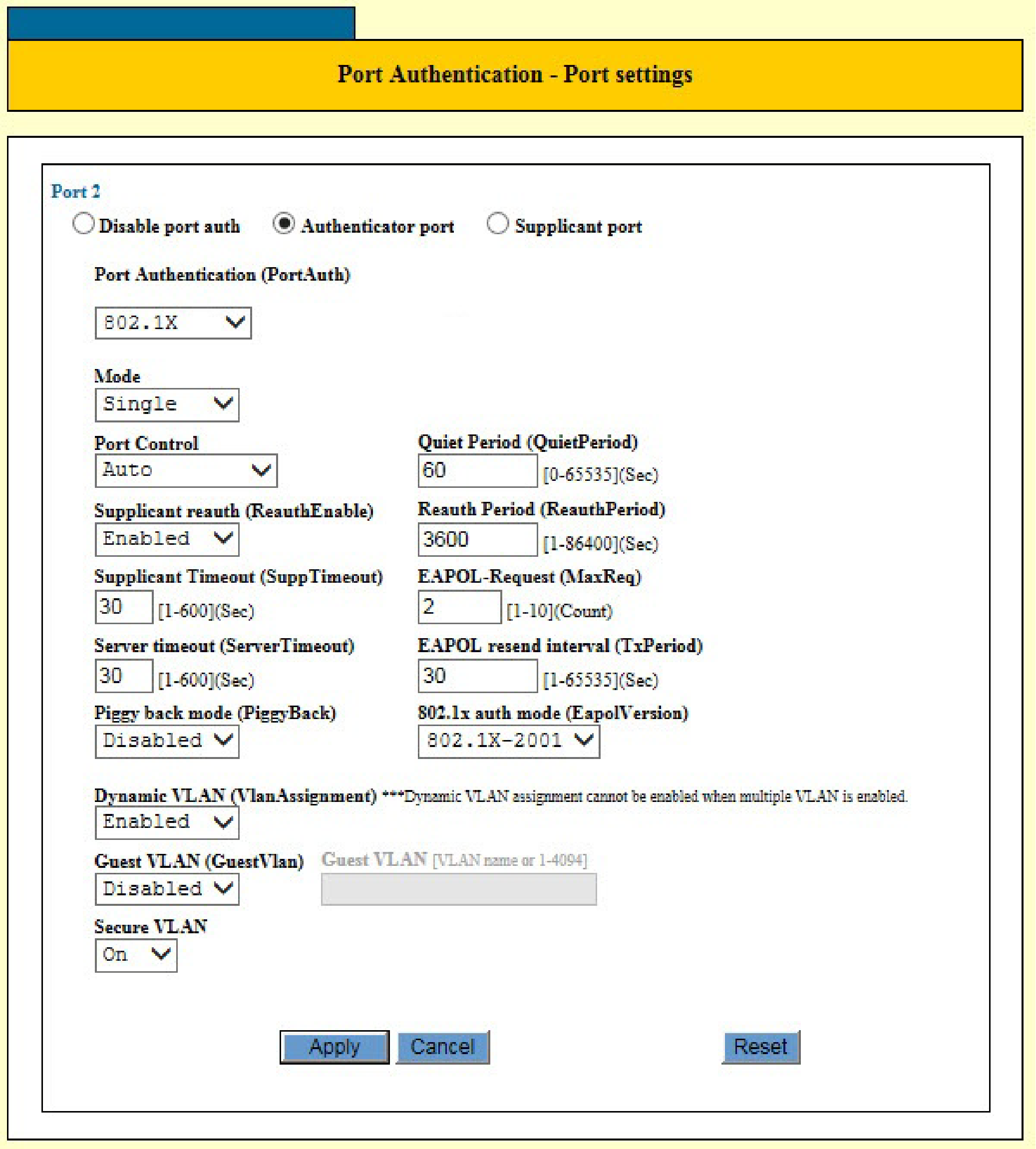
   The Security Settings - Port Authentication window is shown in Figure 82 on page 344.

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 83 on page 350.



Port Authentication - Port settings

Port 2

○ Disable port auth ● Authenticator port ○ Supplicant port

Port Authentication (PortAuth): 802.1X

Mode: Single

Port Control: Auto

Quiet Period (QuietPeriod): 60 [0-65535](Sec)

Supplicant reauth (ReauthEnable): Enabled

Reauth Period (ReauthPeriod): 3600 [1-86400](Sec)

Supplicant Timeout (SuppTimeout): 30 [1-600](Sec)

EAPOL-Request (MaxReq): 2 [1-10](Count)

Server timeout (ServerTimeout): 30 [1-600](Sec)

EAPOL resend interval (TxPeriod): 30 [1-65535](Sec)

Piggy back mode (PiggyBack): Disabled

802.1x auth mode (EapolVersion): 802.1X-2001

Dynamic VLAN (VlanAssignment) ***Dynamic VLAN assignment cannot be enabled when multiple VLAN is enabled.: Enabled

Guest VLAN (GuestVlan): Disabled

Guest VLAN [VLAN name or 1-4094]:

Secure VLAN: On

Figure 83. Port Authentication - Port Settings Window for Authenticator Ports

7. Configure the authenticator port parameters: The parameters are described in Table 98 on page 351.

Table 98. 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. Supplicants must provide usernames and passwords when they log on to an authenticator port in this mode.

Table 98. 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 98. 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 98. 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 98. 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.
Piggyback 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 its clients after one client is authenticated. Disabled - The switch port forwards only those packets from the client who is 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 98. 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 334. 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.

Table 98. 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 337. 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 98. 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:

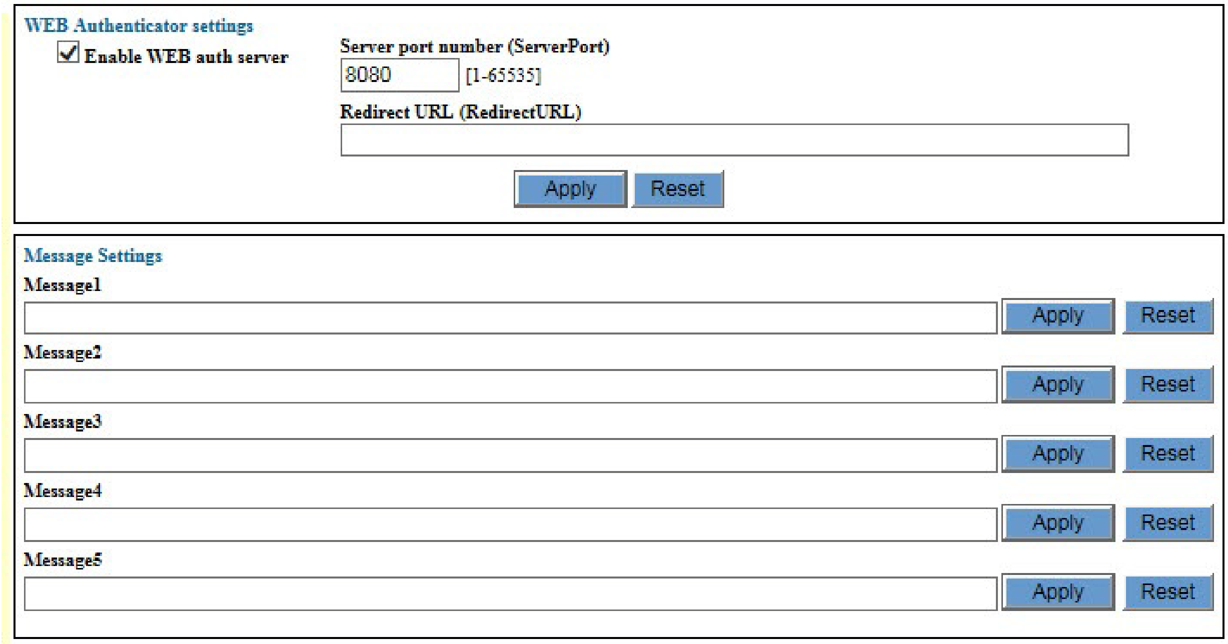
- Enable or disable the web authentication server on the switch.
- Specify the server's port software number.
- Specify a web page to which supplicants are directed after they successfully log on.
- Specify the messages in the logon window. Refer to Figure 85 on page 361.

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 82 on page 344.
3. Click the Web Server button.

   The switch displays the Security Settings - Web Authenticator Server window, shown in Figure 84 on page 360.



WEB Authenticator settings

☑ Enable WEB auth server

Server port number (ServerPort)

8080 [1-65535]

Redirect URL (RedirectURL)

Message Settings

Message1

Message2

Message3

Message4

Message5

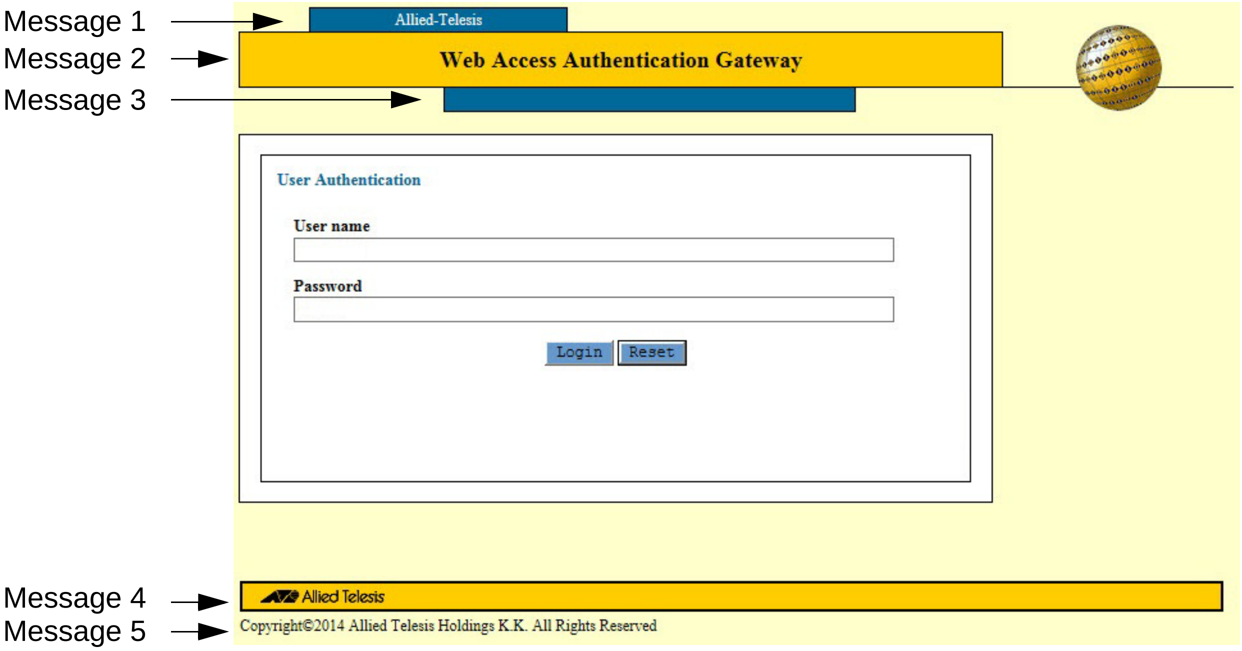
Figure 84. Security Settings - Web Authenticator Window

4. Configure the parameters in the window. They are described in Table 99.

Table 99. 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 for the web authentication server on the switch. 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 supplicants are redirected after successfully logging on with web authentication.
Messages	Use these options to enter the messages that are displayed in the web authentication login screen. Refer to Figure 85 on page 361.

Figure 85 identifies the messages in the logon window of web browser authentication.



Allied-Telesis

Web Access Authentication Gateway

User Authentication

User name

Password

Copyright©2014 Allied Telesis Holdings K.K. All Rights Reserved

Figure 85. Messages in the Web Access Authentication Gateway Window

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 82 on page 344.

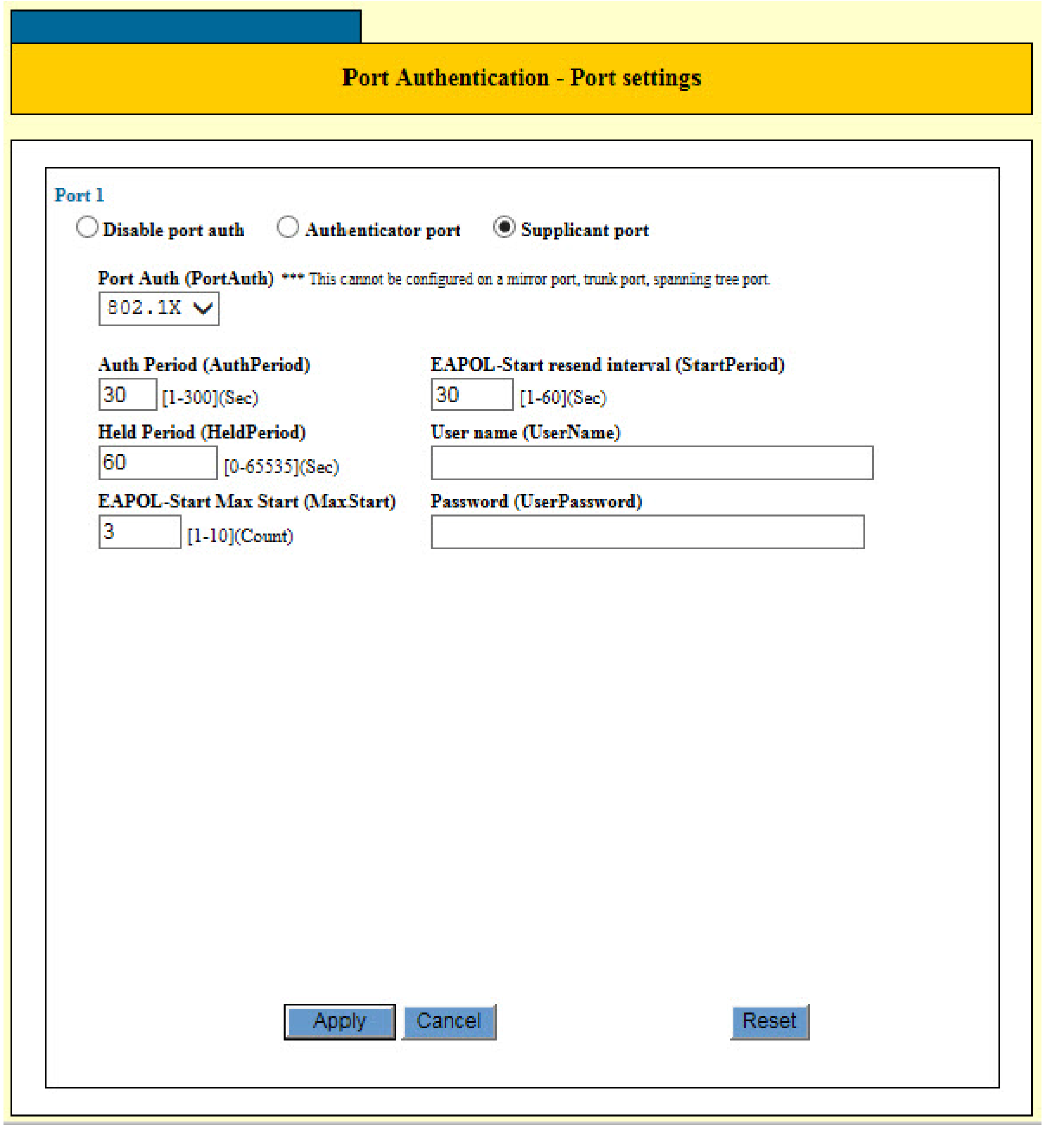
3. In the Port List table, click the dialog box of the port you want to configure. You may configure more than one port at a time.

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 Supplicant dialog circle at the top of the window.

   The switch displays the Port Authentication - Port Settings window for supplicant ports. Refer to Figure 86 on page 363.



Port Authentication - Port settings

Port 1

○ Disable port auth ○ Authenticator port ● Supplicant port

Port Auth (PortAuth) *** This cannot be configured on a mirror port, trunk port, spanning tree port.
802.1X

Auth Period (AuthPeriod)
30 [1-300](Sec)

EAPOL-Start resend interval (StartPeriod)
30 [1-60](Sec)

Held Period (HeldPeriod)
60 [0-65535](Sec)

User name (UserName)

EAPOL-Start Max Start (MaxStart)
3 [1-10](Count)

Password (UserPassword)

Figure 86. Port Authentication - Port Settings Window for Supplicant Ports

6. Configure the supplicant parameters, as needed: The parameters are described in Table 100 on page 363.

Table 100. 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 100. 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 100. 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.

Identifying Non-authenticated Network Devices

You might decide that not all of the network devices require authentication. Perhaps there are some, such as network servers or printers, that should not have to provide logon credentials to forward traffic through the authenticator ports on the switch.

These units are referred to as non-authenticated network devices. The switch forwards their traffic without requiring any authentication when the devices communicate with your network through authenticator ports.

You identify non-authenticated network devices by adding their MAC 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 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 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 82 on page 344.

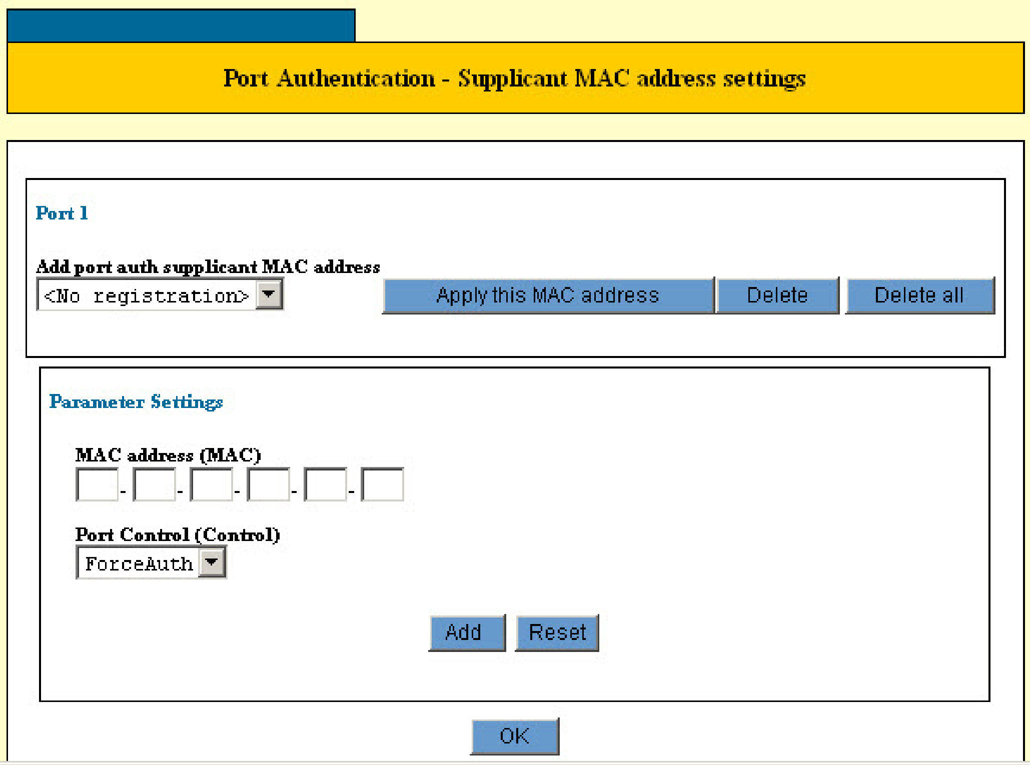
3. In the Port List table, click the dialog box of the authentication port where you want to add MAC addresses of non-authenticated devices.

   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 349.

4. Click the Supplicant MAC Address Settings button.

   The Port Authentication - Supplicant MAC Address Settings window is shown in Figure 87.

Note
If your web browser does not display the window, there may be a compatibility problem. You may need to add the IP address of the switch to the compatibility view of your web browser.



Port Authentication - Supplicant MAC address settings

Port 1

Add port auth supplicant MAC address
<No registration>

Parameter Settings

MAC address (MAC)
□-□-□-□-□-□

Port Control (Control)
ForceAuth

Figure 87. 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 port.

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 82 on page 344.

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 82 on page 344.
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

You may configure the switch to either forward or discard EAP packets when port authentication is disabled. The packets are used by RADIUS servers and clients to communicate with each other when validating the login credentials of supplicants. 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. When EAP transparency is enabled, the switch forwards the packets even though port authentication is disabled.

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 370.

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 29 on page 126.

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 32

Configuration and Operating System Files

This chapter explains how to manage the configuration files in the file system of the switch. This chapter contains the following sections:

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 375. (This window is also used to download new operating system files to the switch. For instructions, refer to “Downloading a New Operating System File to the Switch” on page 384.)

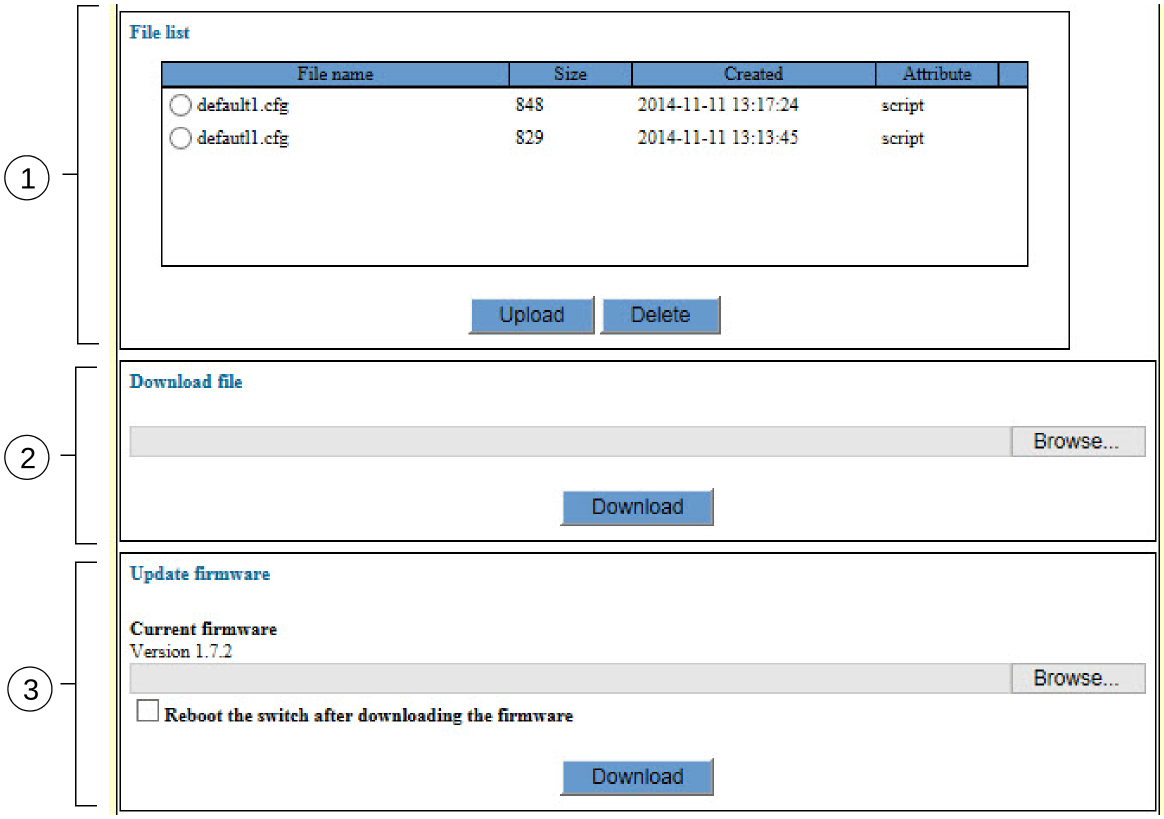
The second window is the Management - Configuration File window. This window lets you create new configuration files and designate the active configuration file. For more information, refer to “Displaying the Configuration File Window” on page 377.

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 88.



File list

File name	Size	Created	Attribute
○ default1.cfg	848	2014-11-11 13:17:24	script
○ defautl1.cfg	829	2014-11-11 13:13:45	script

Download file

Update firmware

Current firmware
Version 1.7.2

□ **Reboot the switch after downloading the firmware**

Figure 88. Management - File Management Window

The sections in the window are defined in Table 101 on page 376.

Table 101. Management - File Management Window

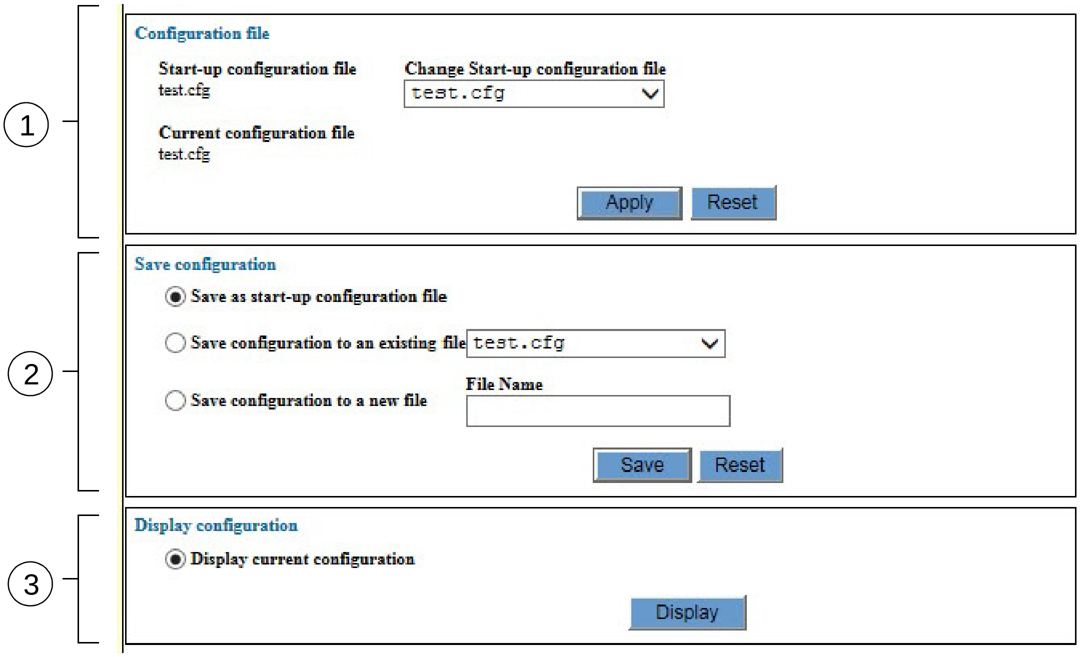
Section	Description
1	Use this section of the window to delete configuration files from the file system in the switch or upload configuration files from the switch to your management workstation or a network server. For instructions, refer to “Deleting Configuration Files” on page 383 and “Uploading Configuration Files from the Switch” on page 380.
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 381.
3	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 “Downloading a New Operating System File to the Switch” on page 384.

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 89.



Configuration file

Start-up configuration file
test.cfg

Change Start-up configuration file
test.cfg

Current configuration file
test.cfg

Save configuration

● Save as start-up configuration file

○ Save configuration to an existing file test.cfg

○ Save configuration to a new file

File Name

Display configuration

● Display current configuration

Figure 89. Management - Configuration File Window

The sections in the window are defined in Table 102.

Table 102. 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 379.
2	Use this section to save the parameter settings to a non-active configuration file or create a new configuration file.
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.

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 Apply 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 Apply 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 88 on page 375.

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 88 on page 375.

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 Apply 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 88 on page 375.

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 without specifying a new active file and reboot the unit, the switch restores the default settings to all of the parameter settings.

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 88 on page 375.

5. In the Update 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. If you want the switch to reboot and begin to use the new operating system file after it downloads the file, select the Reboot the Switch After Downloading the Firmware option.

   If you do not activate the option, the switch continues to use the previous operating system until you reboot it at a later time.

7. Click the Download button.

   The switch downloads the file from your network. If you activated the option in the previous step, the switch reboots after it downloads the file.

8. If the switch reboots, wait for it to initialize its new operating system software.

9. To continue managing the unit, start a new web browser management session.