AT-IA810M

INDUSTRIAL ETHERNET SWITCH

Web GUI User Guide

Contents

Preface

This manual is the Web Graphic User Interface (GUI) user guide for the AT-IA810M Industrial Ethernet Switch. The instructions in this guide explain how to configure the switch using the Web GUI.

This preface contains the following sections:

❐ "Safety Symbols Used in this Document" on page 10
❐ "Contacting Allied Telesis" on page 11

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
Warnings inform you that an eye and 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 & Services section of 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 questions in our knowledge database, check support tickets, learn about Return Merchandise Authorization (RMA), and 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 an RMA request via our interactive support center.

❐ Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.

❐ Software Updates - Download the latest software releases for your product.

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

Chapter 1
Getting Started

This chapter provides an overview of the AT-IA810M industrial switch and how to perform basic operations.

It contains the following sections:

Management Interfaces

The AT-IA810M industrial switch can be managed only through the Web Graphic User Interface (GUI).

Default Settings   The switch is shipped from the factory with the following settings:

❑   IP address: 192.168.1.1

❑   HTTP service: enabled

Guidelines for the Web Graphic User Interface (GUI)   Here are the guidelines accessing the switch via the Web GUI.

❑   Microsoft Internet Explorer 6 or above.

❑   JavaScript must be enabled on the Internet Explorer.

To enable JavaScript, see "Enabling JavaScript" on page 15.

Manager Accounts   You must log on to manage the switch. The switch comes with one manager account:

❑   User name: `manager`

❑   Password: `friend`

Enabling JavaScript

To access the AT-IA810M switch, JavaScript for your Windows Internet Explorer must be enabled. You can enable JavaScript only when accessing the AT-IA810M switch.

> **Note**
> When JavaScript is already enabled, you do not have to change the setting.

To enable JavaScript only for the AT-IA810M switch, perform the following procedure:

1. Open the Windows Internet Explorer.

2. Click **Tools** from the menu bar.

3. Select **Internet options** from the drop-down menu.

   The Internet Options window appears.

4. Click the **Security** tab on the Internet Options window.

   The Internet Options window appears. See Figure 1.
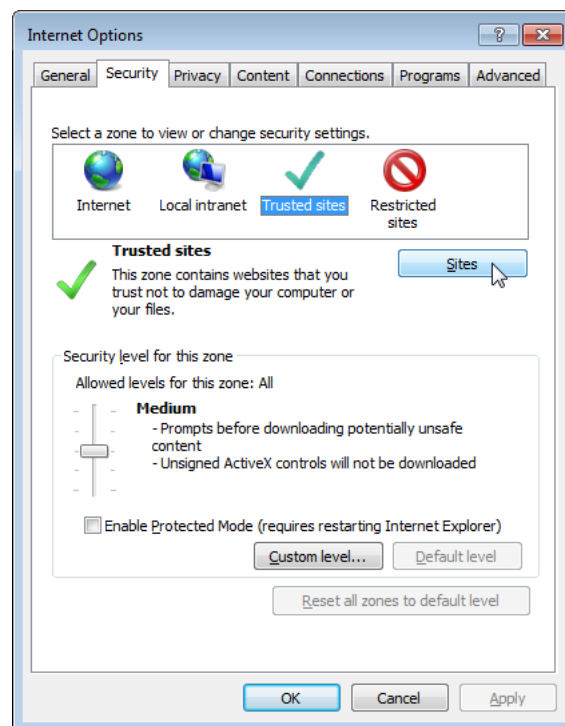
Figure 1. Internet Options Window Security Tab

5. Select the **Trusted sites** icon in the box and press the **Sites** button.

The Trusted sites window appears. See Figure 2.
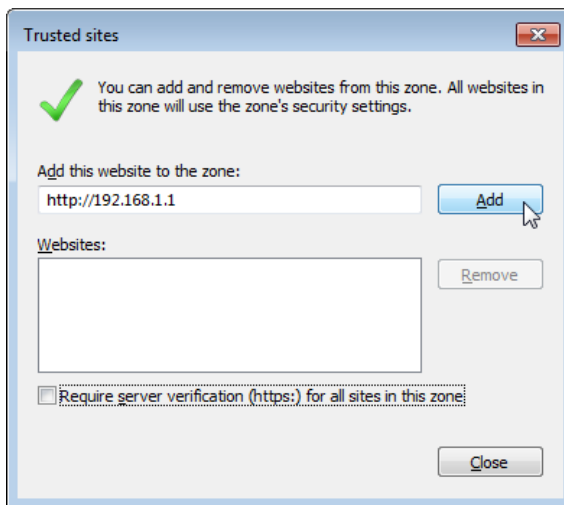
Figure 2. Trusted Sites Window

6. Enter the IP address of the AT-IA810M switch and check the checkbox of "Require server verification (https:) for all sites in this zone."

7. Click **Add**.

The Security Settings Internet Zone window appears. See Figure 3.
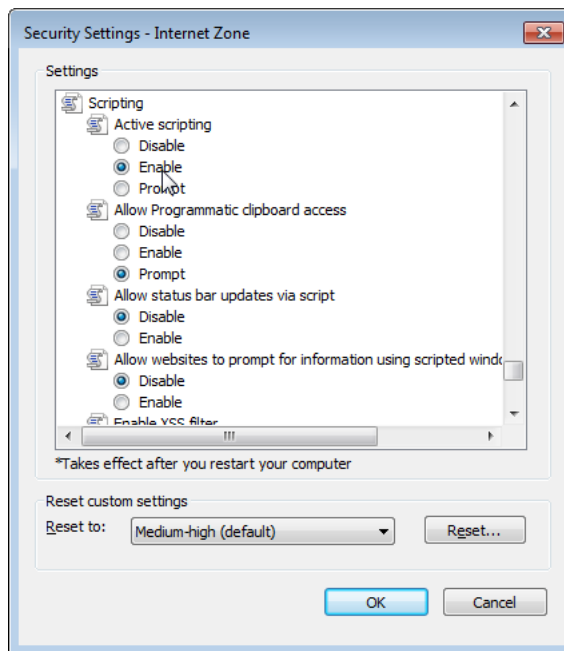
Figure 3. Security Settings Window

8. Change the setting of Active scripting to **Enable**.

9. Click **OK**.

10. Restart the Internet Explorer.

    JavaScript is enabled only when you access the AT-IA810M switch.

Starting and Ending a Management Session

To manage the switch, select one of the following:

- ❑ "Starting an Initial Management Session, next
- ❑ "Starting a Management Session" on page 20
- ❑ "Ending a Management Session" on page 20

Starting an Initial Management Session

When you access the switch for the first time, Allied Telesis recommends the following actions:

- ❑ Change the switch's IP address
- ❑ Change the system name
- ❑ Save changes to the current startup configuration file.

To access the switch for the first time, perform the following procedure:

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

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

2. Open Internet Explorer 6 or above.

3. Enter the switch's default IP address:192.168.1.1.

   The login prompt window appears. See Figure 4.

Figure 4. AT-IA810M switch Login

4. Enter the user name and password.

The following are the default settings:

❑ User name: `manager`

❑ Password: `friend`

5. Click **OK**.

The switch displays the Device Monitoring - System Information page as shown in Figure 5.

Figure 5. Device Monitoring - System Information Page

6. To change the IP address, see "Changing the IP Addresses" on page 26.

7. To change the system name, see "Modifying the SysName, SysLocation, and SysContact" on page 24.

8. Go to "Saving the Changes to a Configuration File" on page 21.

To save the changes to the current startup configuration file, select "Save to startup configuration file."

Starting a Management Session

To start a Web browser management session, perform the following procedure:

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

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

2. Open Internet Explorer 6 or above.

3. Enter the IPv4 address of the switch on the Internet Explorer's URL.

4. Enter the user name and password.

   The login prompt window appears. See Figure 4 on page 18.

5. Enter the user name and password.

   The following are the default settings:

   ❑ User name: `manager`
   ❑ Password: `friend`

6. Press **OK**.

   The switch displays the Device Monitoring - System Information page. See Figure 5 on page 19.

Ending a Management Session

To end a Web browser management session, click the **End WEB session** button above the main menu on the left. See Figure 5 on page 19.

Buttons on the Web GUI

This section describes the Apply, Set, Reset, and Save buttons that you see throughout the Web GUI.

Apply and Set Buttons

Management pages with adjustable parameters have Apply or Set buttons. After changing a parameter setting of a feature, you must click one of these buttons to activate your change on the switch. After you apply or set your changes, they are entered in the running configuration.

Reset Button

The Web management pages also have a Reset button. Use this button to discard your changes to the parameter settings in the page. Note that 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 or Set button is used.

Save Button

When you make a change in the parameter settings and click the Apply or Set button, the change is entered in the running configuration. To save the running configuration to a configuration file, you must use the Save button. The running configuration is deleted when the switch is powered off or reset.

When you make a change in the parameter settings and the change has not been saved to any configuration file, the Save button at the top-left corner of the Web page is displayed in red. After you save the change, the Save button is displayed in green.

The switch does not automatically store your change, instead, you must specify the configuration file where you want your change to be stored.

Saving the Changes to a Configuration File

To save the running configuration to a configuration file, perform the following procedure,

1. Click **Save**.

   The Save Configuration window appears. See Figure 6 on page 22.
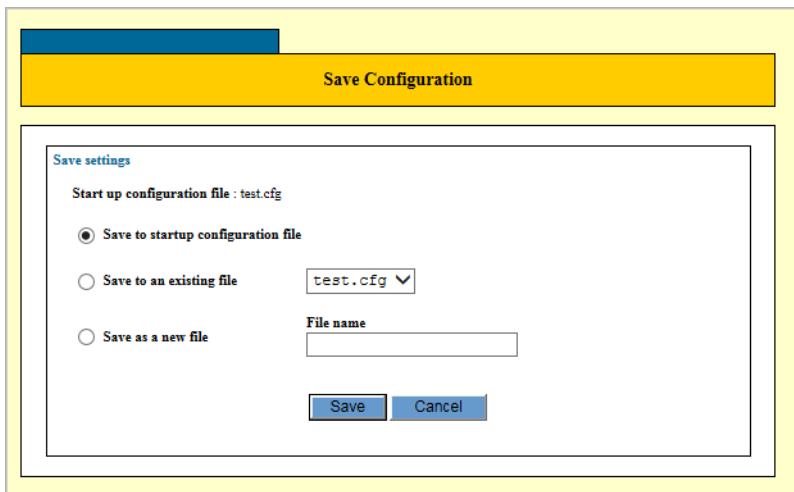
Figure 6. Save Configuration Window

2. Select one of the options described in Table 1.

Table 1. Save Configuration Options

Field	Description
Save to startup configuration file	Saves the running configuration to the current start-up configuration file. To see which configuration file is currently designated as the start-up configuration file, see "Displaying the Start-up and Current Configuration Files" on page 245.
Save to an existing file	Saves the running configuration to a selected configuration file in the file system. To use this option, select a desired configuration file from the pull-down menu.
Save as a new file	Stores the running configuration in a new configuration file and saves the new file in the switch. Enter the filename for a 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.

3. Click **Save**.

Chapter 2
System Settings

This chapter contains the following sections:

System

From the System Settings page, you can assign or modify the Sysname, Syslocation, Syscontact, IP settings, and login password. These values are used for Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.

Modifying the SysName, SysLocation, and SysContact

To assign or modify the SysName, SysLocation, and SysContact, perform the following procedure:

1. From the Navigation pane, go to System Settings > System.

    The System Settings page is displayed. See Figure 7.
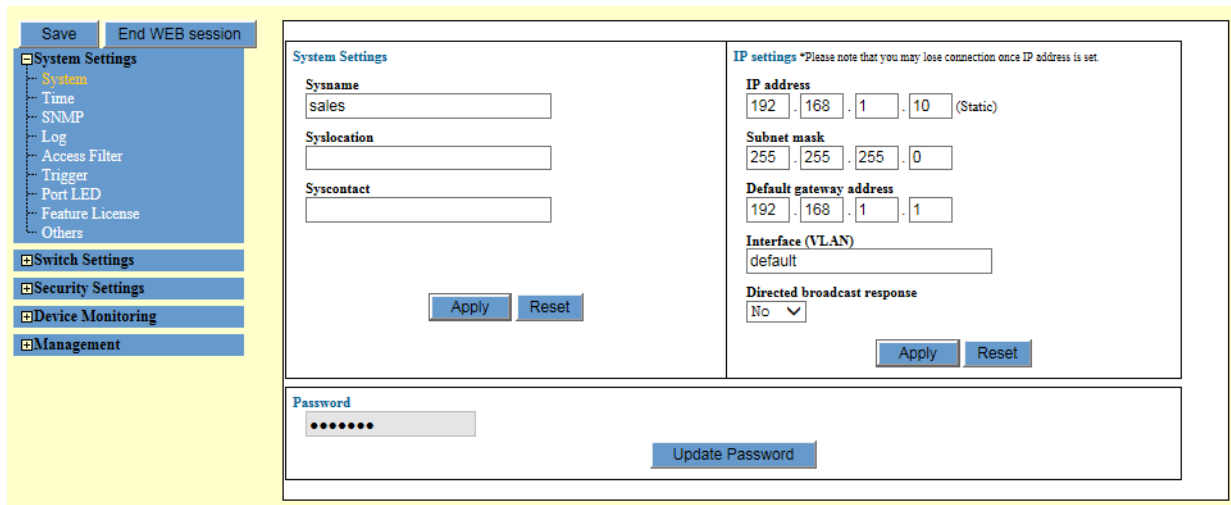
Figure 7. System Settings Page

2. Specify the following items described in Table 2.

Table 2. System Settings

Field	Description
Sysname	Specify a system name, which can be accessed by SNMP managers. The name can be from 1 to 39 characters and include spaces and special characters, such as dashes and asterisks. The default is no name specified. This parameter is optional.
Syslocation	Specify a system location, which can be accessed by SNMP managers. The location can be from 1 to 20 characters and include spaces and special characters, such as dashes and asterisks. The default is no location specified. This parameter is optional.

Table 2. System Settings (Continued)

Field	Description
Syscontact	Specify a system contact, which can be accessed by SNMP managers. The contact information can be from 1 to 20 characters and include spaces and special characters, such as dashes and asterisks. The default is no information specified. This parameter is optional.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Specifying Management VLAN

Review the following information before changing the management Virtual Local-Area Network (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 "Port-based VLAN Overview" on page 258 and "Tagged VLAN Overview" on page 262.

❐ 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. From the Navigation pane, go to System Settings > System.

    The System Settings page is displayed. See Figure 7 on page 24.

2. Select the Interface (VLAN) field and enter the name or VID of the new management VLAN. You can specify only one VLAN.

3. Click **Apply** 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.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Changing the IP Addresses

To change the IPv4 address and related information, perform the following procedure:

Note

Changing the IP address of the switch interrupts the session. To resume a management session, start with a newly assigned IP address.

1. From the Navigation pane, go to System Settings > System.

    The System page is displayed. See Figure 7 on page 24.

2. Specify the following items described in Table 3.

Table 3. IP Settings

Field	Description
IP address	Specify the IPv4 address of the switch to be remotely managed.
Subnet mask	Specify the subnet mask of the IPv4 address of the switch.
Default gateway address	Specify the default gateway address of the switch.
Interface (VLAN)	Specify the management VLAN.
Directed broadcast response	Select "Yes" to respond to broadcast PING queries, and "No" to ignore them.

3. Click **Apply.**

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Changing the Password

To change the password of the manager account on the switch, perform the following procedure:

Note
After Changing the password, you must log on again.

---

1. From the Navigation pane, go to System Settings > System.

   The System page is displayed. See Figure 7 on page 24.

2. Click **Update Password**.

   The system displays the Change password window. See Figure 8.

Figure 8. Change Password Window

3. Specify the three fields described in Table 4 on page 27.

Table 4. Password Window

Field	Description
Current Password	Enter the current manager password.
New Password	Specify the new manager password. The password can be from 0 to 16 alphanumeric characters. The password is case-sensitive. ⚠️ **Caution** Do not use spaces or special characters, such as * and ! in a password if you manage the switch from a web browser. Some web browsers may not handle special characters in passwords.

Table 4. Password Window (Continued)

Field	Description
Confirm New Password	Reenter the new manager password.

4. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

---

5. Log on using the new password.

   The username is 'manager" and the password is the newly assigned password.

Time

From the System Time page, you can set the system time manually or by Network Time Protocol (NTP). In addition, you can enable or disable Daytime Saving Time.

Setting the System Time Manually

To set the system time manually, perform the following procedure:

1. From the Navigation pane, go to System Settings > Time.

    The System Time page is displayed. See Figure 9.

Figure 9. System Time Page

2. Change Year/Month/Day and Hour/Minute/Second in the fields.

    Note
    Ensure that NTP is disabled by unchecking the **Enable NTP**.

3. Click **Apply**.

    Note
    To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

**Configuring the
NTP Client**

To set the system time by NTP, you must configure the NTP client. To configure the NTP client, perform the following procedure:

> **Note**
> Once you configure the NTP client and enable NTP, the switch polls the NTP server for the date and time whenever the switch is powered on, reset, or a change is made to any parameters in the NTP fields.

1. From the Navigation pane, go to System Settings > Time.

   The System Time page is displayed. See Figure 9 on page 29.

2. Changes the fields described in Table 5.

Table 5. NTP Settings

Field	Description
Enable NTP	Enable the NTP client by checking the **Enable NTP** checkbox. Uncheck to disable the NTP client. By default, the NTP client is disabled.
UTC Offset	Use the pull-down menu to select the difference between the UTC and local time.
NTP Peer	Specify the IP address of the NTP server.
NTP port number	Specify the listening port number for the NTP client. The range is 1 to 65535. The default is 123.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

**Configuring
Daylight Saving
Time**

You can apply Daylight Saving Time to the device. To configure the Daylight Saving Time, perform the following procedure:

1. From the Navigation pane, go to System Settings > Time.

   The System Time page is displayed. See Figure 9 on page 29.

2. Changes the fields in the Summer Time section described in Table 6 on page 31.

Table 6. Summer Time Settings

Field	Description
Enable Summer Time	Enable or disable Daylight Saving Time (DST) on the switch. DST is enabled when the **Enable Summer Time** checkbox is checked. The default setting is disabled with this checkbox unchecked.
Starts Year/Month/Day HH:MM	Specify the start date and time for DST. The years must have four digits.
Ends Year/Month/Day HH:MM	Specify the end date and time for DST. The year must have four digits.
Offset	Specify the number of minutes that the clock is to move forward at the start of DST and to move back at the return to Standard Time (ST). The range is 1 to 180 minutes. The default is 60 minutes.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

SNMP

The Simple Network Management Protocol (SNMP) is another way 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 instead of management sessions through a web browser.

> **Note**
> The switch supports SNMPv1 and SNMPv2c.

Here are the main steps to setting SNMP:

1. Enable SNMP on the switch. The default setting is disabled.

2. Create one or more community strings.

3. Load the Allied Telesis MIBs for the switch onto your SNMP management workstation.

   The MIBs are available from the Allied Telesis website.

Modifying SNMP Settings

To configure the SNMP basic settings, perform the following procedure:

1. From the Navigation pane, go to System Settings > SNMP.

   The SNMP page is displayed. See Figure 10 on page 33.

Figure 10. SNMP Page

2.   Modify the fields described in Table 7.

Table 7. SNMP Basic Settings

Field	Description
Enable SNMP	Enable or disable SNMP by checking or unchecking the **Enable SNMP** checkbox. The default setting is disabled.
SNMP port number	Specify the UDP port number for SNMP. The range is 1 to 65535. The default is 161.
Trap port number	Specify the UDP port number for SNMP traps. The range is 1 to 65535. The default is 162.
Select traps	Select the traps that the community strings are permitted to send by checking each checkbox. The default is no selected traps.
Enable Link trap (Interface)	Select designated ports for link traps. The switch sends link traps when a link state is changes on the designated ports.

3.   Click **Apply**.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Observing SNMP Communities

To view SNMP communities, perform the following procedure:

1. From the Navigation pane, go to System Settings > SNMP.

    The SNMP page is displayed. See Figure 10 on page 33.

    The fields are described in Table 8.

Table 8. SNMP Community

Field	Description
Community name	Displays the community name.
Status	Displays the status of the community string. The status are: ❒ Enabled- Network Manager can use the community string to manage the switch. ❒ Disabled - Network Manager cannot use the community string.
Trap	Displays whether the status of the traps of the community string. The status are: ❒ Enabled - The community string can sent traps. ❒ Disabled - The community string cannot sent traps.
Access Privilege	Displays the access mode of the community. The access modes are: ❒ Read-only - The community string can be used to view, but not change the values of the MIBs on the switch. ❒ Read-write - The community string cannot 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: ❒ Yes - The community has an open status. Any management workstation can use it. ❒ No - The community has a closed status. It can be used only by those workstations whose IP addresses are assigned to it.

Adding a New SNMP Community

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

1. From the Navigation pane, go to System Settings > SNMP.

   The SNMP page is displayed. See Figure 10 on page 33.

2. Click **Add** at the bottom of the page.

   The SNMP page is displayed. See Figure 11.

Figure 11. SNMP Community - Add Window

3. Configure the parameters in the window for the new community.

   The fields are described in.Table 9.

Table 9. SNMP Community - Add

Field	Description
Community name	Enter a community name. The name can be up to 32 alphanumeric characters. No spaces or special characters (such as /, #, or &) are allowed.

Table 9. SNMP Community - Add (Continued)

Field	Description
Enable this community	Check the box to enable the community or uncheck the box to disable it. The status are: ❒ Enable - Network Manager can use the community string to manage the switch. ❒ Disable - Network Manager cannot use the community string.
Manager Stations	Specify the IP addresses of up to four management workstations for a community with a closed access. A community with a closed status can only be used by the management workstations listed here. To set the community to be closed, see the "Open Access" field. **Note** Entering manager IP addresses for a community string with an open status has no affect on the community string.
Access Mode	Select one of the access modes for the community. The access modes are: ❒ 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	Check the box to set the community to be open, or uncheck the box to set the community to be closed. The status are: ❒ Open - The community has an open status. Any management workstation can use it. ❒ Closed - The community has a closed status. It can be used only by those workstations whose IP addresses are assigned to it.
Send trap to this community	Check the box to allow the switch to use the community to send traps, or uncheck the box to *not* allow the switch to use the community to send traps.
Trap receivers	Specify 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.

Table 9. SNMP Community - Add (Continued)

Field	Description
Traps	Select traps that the switch is to send using the community. A trap is enabled when the box is checked and disabled when the box is unchecked. The traps selected in this window must also be selected in the System Settings - SNMP window. See Figure 10 on page 33.

4. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting an SNMP Community

To delete an SNMP community, perform the following procedure:

1. From the Navigation pane, go to System Settings > SNMP.

   The SNMP page is displayed. See Figure 10 on page 33.

2. Select an SNMP community from the SNMP Community list that you want to delete.

3. Click **Delete**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Editing an SNMP Community

To edit the properties of an SNMP community, perform the following procedure:

1. From the Navigation pane, go to System Settings > SNMP.

   The SNMP page is displayed. See Figure 10 on page 33.

2. Select an SNMP community in the SNMP Community list that you want to edit.

3. Click **Edit**.

   The SNMP community Edit window appears.

4. Modify the fields as needed. The fields are described in Table 9 on page 35.

> **Note**
> You cannot edit the community name.

5. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Log

The switch generates event messages to help you identify and solve system problems.You can store these event messages in an event log on the switch. These event messages are retained even when you reset or power cycle the switch. In addition, the syslog client on the switch can send event messages to a syslog server.

From the Log page, you can configure that the system stores the specified log messages on the switch and/or sends the specified log messages to a Syslog server.

> **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, see "Time" on page 29.

Viewing the Log Settings

To view the current log settings on the switch, perform the following procedure:

1. From the Navigation pane, click System Settings > Log.

   The Log Settings page is displayed. See Figure 12.

Figure 12. Log Settings Page

2. The fields are described in Table 10 on page 40.

Table 10. Log

Field	Description
Enable Log	Enable or disable the event log and/or syslog client.
Log outputs	Select the type of log to enable. You can select both options. The options are: ❏ Permanent - The system stores event messages in the event log on the switch. ❏ Syslog - The syslog client sends the log messages to the syslog server. **Note** You must check **Enable Log** if you select at least one option.
Log Level (Severity)	This fields are for the messages stored in the switch. Select one severity level of the log messages and select one option that represents the range of messages to be stored in the event log. The severity levels are described in Table 11 on page 42 and the range options are in Table 12 on page 42.
Syslog server address	Specify the IPv4 address of the Syslog server that the Syslog client sends log messages.
Syslog port number	Specify the port number for the Syslog server. The range is from 1 to 655335. The default value is 514.
Syslog Level (Severity)	These fields are specified for the messages that are sent to the Syslog server. Select one severity level of the log messages. See Table 11 on page 42. Select one option that represents the range of messages to be stored in the event log. See Table 12 on page 42.
Facility	Select a facility code for the event messages. The switch adds the code to the messages when transmitting them to the syslog server. The options are described in Table 13 on page 43.

Storing Event Messages on the Switch

To store the specified event messages in the event log on the switch, perform the following procedure:

1. From the Navigation pane, click System Settings > Log.

    The Log Settings page is displayed. See Figure 12 on page 39.

2. Check the Enable log checkbox.

3. Check the Permanent checkbox for Log outputs.

4. Select the options from the Log level (severity) pull-down menus. The options are described in Table 10 on page 40.

5. Click **Apply**.

    > **Note**
    > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Sending Event Messages to a Syslog Server

To send the specified event messages to the Syslog server, perform the following procedure:

1. From the Navigation pane, click System Settings > Log.

    The Log Settings page is displayed. See Figure 12 on page 39.

2. Check the Enable log checkbox.

3. Check the Syslog checkbox for Log outputs.

4. Select the options from the Syslog level (severity) pull-down menus.

    The options are described in Table 11 and Table 12 on page 42.

5. Select one of the Facility codes from the pull-down menu.

    See Table 13 on page 43.

6. Click **Apply**.

    > **Note**
    > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

**Log Levels
(Severity)**

Table 11 explains about the log levels (severity) that you can select.

Table 11. Log Level (Severity)

Severity Level	Description
CRITICAL (7)	Even messages of this level contain information about critical failures that have affected switch operations.
URGENT (6)	Event messages of this level contain information about possible pending failures that require immediate attention.
IMPORTANT (5)	Event messages of this level contain information about possible pending failures.
NOTICE (4)	Event messages of this level contain information about events that do not affect switch operations.
INFO (3)	Event messages of this level contain information about events that do not affect switch operations.
DETAIL (2)	Event messages of this level contain information about events that do not affect switch operations.
TRIVIAL (1)	Event messages of this level contain information about events that do not affect switch operations.
DEBUG (0)	Event messages of this level contain debug information.

**Log Level
(Severity) Ranges**

Table 12 explains about the log level (severity) ranges that you can select.

Table 12. Log Level (Severity) Range Options

Range Option	Description
Less than	Designates 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.

Table 12. Log Level (Severity) Range Options (Continued)

Range Option	Description
Greater Than	Designates 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	Designates 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	Designates 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.

Facility Codes   Table 13 explains about facility codes that you can select.

Table 13. Facility Codes

Facility Value	Facility Code	Description
DEFAULT	24	Default value
LOCAL7	23	Local use 7 (local7)
LOCAL6	22	Local use 6 (local6)
LOCAL5	21	Local use 5 (local5)
LOCAL4	20	Local use 4 (local4)
LOCAL3	19	Local use 3 (local3)
LOCAL2	18	Local use 2 (local2)
LOCAL1	17	Local use 1 (local1)
LOCAL0	16	Local use 0 (local0)
CRON2	15	Clock daemon

Table 13. Facility Codes (Continued)

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

Access Filter

Access Filter allows 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 switch 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 is allowed to manage the switch, you might configure Access Filter so that only your workstation can be used to remotely manage the switch.

Each management interface has its own filter. The different filters are listed in Table 14.

Table 14. Access Filters

Management Interface Filter	Description
SNMP	Approves the workstations to access the switch through SNMP.
FTP	Approves workstations to upload or download files to the file system in the switch with FTP or TFTP.
Telnet	Not supported
HTTP	Approves workstations to access switch through Web browsers.
ICMP	Approves workstations to identify the switch using the PING utility.
GLOBAL	Approves workstations to access switch using all the interfaces listed above.

Note
If you enabled the HTTP or GLOBAL 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.

Enabling Access Filter

To enable Access Filter, perform the following procedure:

1. From the Navigation pane, go to System Settings > Access Filter.

    The Access Filter page is displayed. See Figure 13 on page 46.
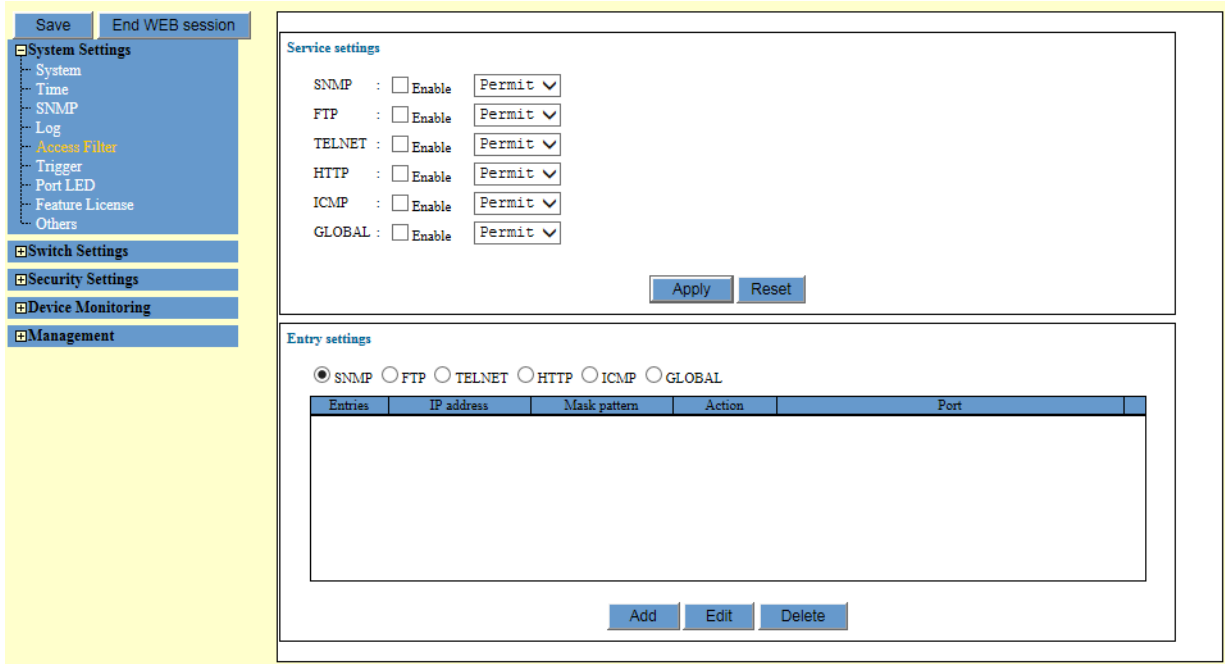
Figure 13. Access Filter Page

2. Check the checkbox of a management interface under the Service settings section. You can check multiple management interfaces as required.

3. Specify whether workstations are permitted or denied use of the management interface. The options are:

   ❒ 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.

4. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Adding Filter Entries

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

1. From the Navigation pane, go to System Settings > Access Filter.

   The Access Filter page is displayed. See Figure 13 on page 46.

2. Select one of the management interfaces by checking its radio button in the Entry settings section.

   Only one interface can be selected at a a time.

3. Click **Add**.

   The Add Access Filter page appears. See Figure 14.

Figure 14. Add Access Filter Window

4. Configure the fields as needed. The fields are described in Table 15.

Table 15. Add Access Filter

Field	Description
Services	Displays the name of a management interface. This parameter cannot be changed. To manage a different filter, close this window and repeat step 2.

Table 15. Add Access Filter (Continued)

Field	Description
IP Address	Specify the IPv4 address of a computer to be allowed or denied access to the corresponding management interface on the switch. Here is the IP address guideline: You may enter only one address.You may enter the address of a specific computer (e.g., 192.168.2.76) or a subnet (e.g., 192.168.2.0).
Mask pattern	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 is the mask guideline: You may specify only one mask. As an example, the mask for the IP address of a specific workstation, such as 192.168.2.76, would be 255.255.255.255
Action	Select 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 Access Filter page. Here is an example. If you are configuring the FTP filter with the main FTP action set to Deny. The filter denies FTP access to all workstations, but permits access to those workstations specified with filter entries. Consequently, you create filter entries with the Permit action for those workstations to be allowed to use FTP to manage the switch. Here is another example. If you are configuring the SNMP filter with the main SNMP action set to Permit. The filter permits SNMP access to all workstations, but denies access to those workstations specified with filter entries. Consequently, you create filter entries with an action of Deny for those workstations to be denied use of SNMP to manage the switch.
Port	Select the port(s) of the workstation for the filter entry. You may assign a filter entry to more than one port.

5. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting Filter Entries

To delete filter entries, perform the following procedure:

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

2. From the Navigation pane, select System Settings > Access Filter.

    The Access Filter page is displayed. See Figure 13 on page 46.

3. In the Entry Setting field select on of the filters by checking its radio button.

    The switch displays the entries of the selected filter.

4. Click **Delete**.

    The switch displays a confirmation prompt.

5. Click **OK**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Trigger

Triggers perform specific actions on the switch automatically at scheduled times.Three available actions are described Table 16.

Table 16. Trigger Actions

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

Note
Once you create a trigger with a Port off action on the management port, you lose access to the switch when a trigger starts and disables the management port. You cannot log in until the trigger ends.

Trigger Guidelines

Here are guidelines for triggers:

❒ The switch can have up to ten triggers.

❒ Triggers with the **LED Off** action or **Port Off** action can be assigned to individual ports.

❒ If you set a trigger with the Port off action on the management port, the web session stops when the trigger starts on a schedule time. You must wait to log in again until the trigger ends.

Viewing Triggers

To view the existing triggers, perform the following procedure:

1. From the Navigation pane, go to System Settings > Trigger.

   The Trigger page is displayed. See Figure 15 on page 51.
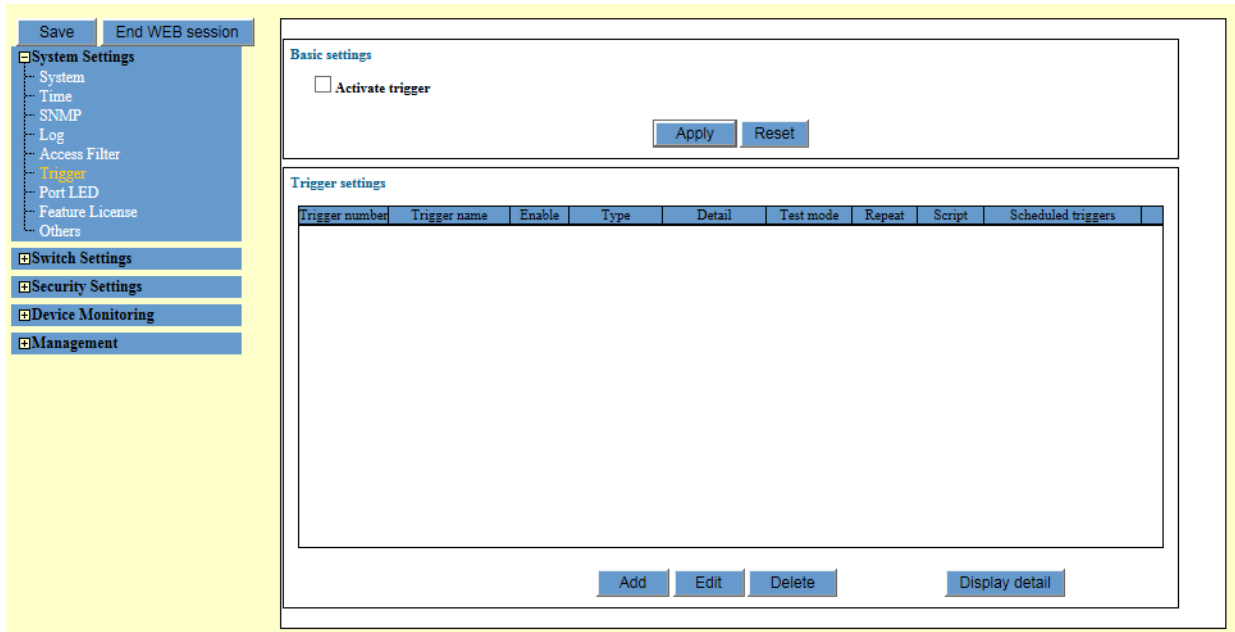
Figure 15. Trigger Page

2. Observe the trigger information displayed in the Trigger settings on the page. The fields are described in Table 17.

Table 17. Trigger Settings

Field	Description
Trigger Number	Displays the ID number of the trigger.
Trigger Name	Displays the name of the trigger.
Enable	Displays whether the trigger is enabled or disabled.
Type	Displays the action.
Detail	Displays the schedule of the trigger.
Test mode	Not available
Repeat	Not available
Script	Not available
Scheduled Triggers	Displays the start and end days or dates of the trigger.

3. For more information, click **Display Detail**.

The Trigger detail page is displayed. See Figure 16 on page 52.
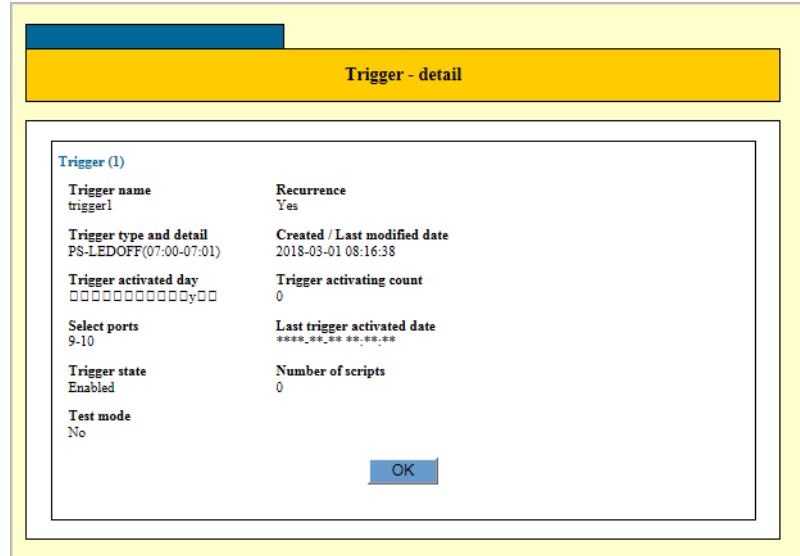
Figure 16. Trigger Detail Page

The fields in the window are defined in Table 18.

Table 18. Trigger - Detail Window

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

Table 18. Trigger - Detail Window (Continued)

Field	Description
Last Trigger Activated Date	Displays the date and time when the trigger was last activated. The field will contain asterisks if the trigger has not been activated.
Number of Scripts	Not used. The status is always 0.

Enabling the Trigger Feature

To enable the trigger feature, perform the following procedure:

1. From the Navigation pane, go to System Settings > Trigger.

   The Trigger page is displayed. See Figure 15 on page 51.

2. Check the checkbox of Activate trigger under Basic settings.

3. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Adding Triggers

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

1. From the Navigation pane, go to System Settings > Trigger.

   The Trigger page is displayed. See Figure 15 on page 51.

2. Click **Add**.

   The Trigger settings - Add page is displayed. See Figure 17 on page 54.
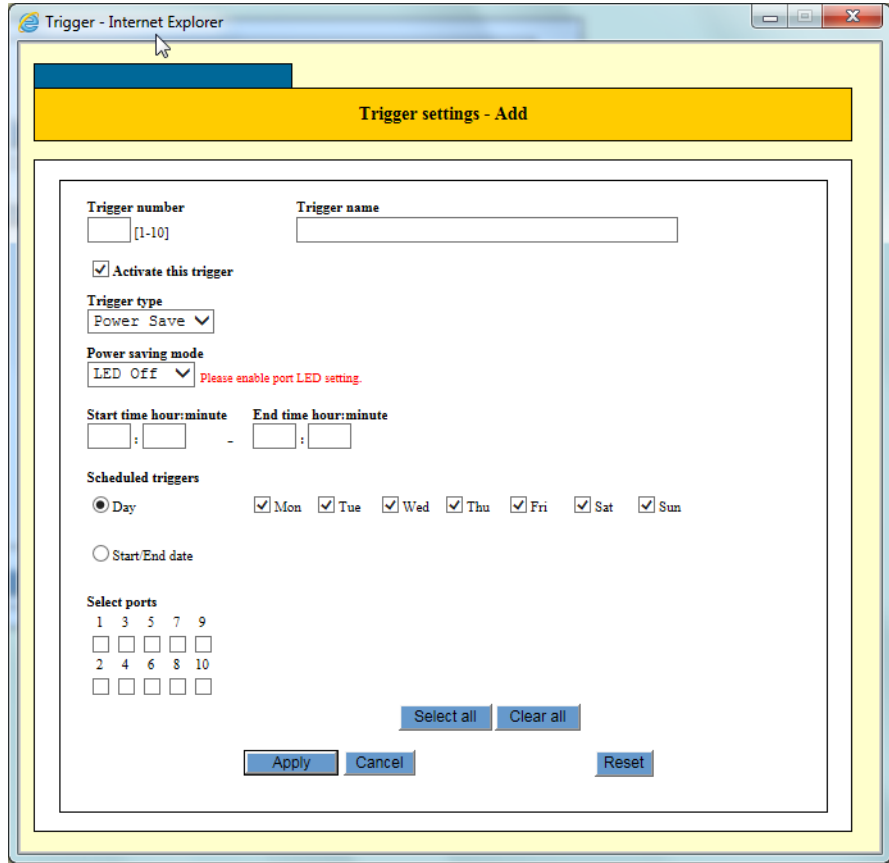
Figure 17. Trigger settings - Add Window

3. Configure the parameters on the page described in Table 19.

Table 19. Trigger Settings

Field	Description
Trigger Number	Assign an ID number to the trigger. The range is 1 to 10.
Trigger Name	Assign a name to the trigger. A name can have up to 40 alphanumeric characters. A name may contain spaces.
Activate This Trigger	Enable or disable the trigger.
Trigger Type	Specify the trigger type. The only selection is "Power Save."
Power Saving Mode	Specify the action of the trigger. See Table 16 on page 50 for the available actions.
Start Time	Specify the start time of the function. Enter the hours and minutes in 24-hour format.

Table 19. Trigger Settings (Continued)

Field	Description
End Time	Specify the end time of the function. The hours are entered in 24-hour format.
Scheduled Triggers - Day	Specify the days of the week when the function is to be performed. A day is selected when its checkbox has a check mark and not selected when the checkbox is empty.
Scheduled Triggers- Start/end Date	Specify the start and end dates of the trigger. The date format is shown here: yyyy:mm:dd The year must have four digits. For example, to specify the start and end dates November 9 to 11, 2014, you enter: 2018/11/9 - 2018/11/11.
Select Ports	Assign the ports of the trigger. You may assign a trigger to more than one port. A port is selected when its dialog box has a check mark and not selected when its dialog box is empty.

4. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying Triggers

To modify a trigger, perform the following procedure:

1. From the Navigation pane, go to System Settings > Trigger.

   The Trigger page is displayed. See Figure 15 on page 51.

2. Select a trigger that you want to modify.

3. Click **Edit**.

   The Trigger settings - Edit page is displayed.

4. Modify the fields. The fields are described in Table 19 on page 54.

Note

You are not allowed to change the ID number.

---

5. Click **Apply**.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting Triggers To delete a trigger, perform the following procedure:

1. From the Navigation pane, go to System Settings > Trigger.

    The Trigger page is displayed. See Figure 15 on page 51.

2. Select a trigger that you want to delete.

3. Click **Delete**.

    The switch displays a confirmation prompt.

4. Click **OK**.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Port LED

Each copper port on the switch has two LEDs: the Link/Activity LED and the Speed/Duplex mode LED. The Link/Activity LED displays the link and activity status of the port; the Speed/Duplex mode LED can display either the speed or duplex mode, but not both at the same time.

From the Port LED page, you can turn on and off the port LEDs on the switch and specify the Speed/Duplex mode LED to display either the speed or the duplex mode. In addition, you can configure the LED of a port to turn off when the ingress traffic falls below a defined threshold level to identify ports that periodically experience low traffic.

Displaying the Port LEDs Settings

To displays the port LEDs, perform the following procedure:

1. From the Navigation pane, go to System Settings > Port LED.

   The Port LED page is displayed. See Figure 18.

Figure 18. Port LED Page

2. Observe the fields described in Table 20 on page 58.

Table 20. Port LED

Field	Description
Status	
LED mode	Displays the LED mode for all ports on the switch. The options are "LED on" and "LED off."
Basic settings	
LED mode	You change the LED mode for all ports on the switch. The options are:
	❑ LED on: Turns on the Link/Activity and Speed/Duplex mode LEDs.
	❑ LED off: Turns off the Link/Activity and Speed/Duplex mode LEDs.
	❑ Speed LED: Sets the Speed/Duplex mode LEDs to display port speeds.
	❑ Duplex LED: Sets the Speed/Duplex mode LEDs to display the Duplex mode.
Port settings	
Port	Displays the port number and its checkbox.
LED action	Displays the port's LED action. The options are:
	❑ LED on
	❑ LED off
Receiving rate threshold (Kbps)	Displays the receiving rate threshold defined on the port.
Receiving rate (Kbps)	Displays the receiving rate on the port.
Link	Displays the link status of the port.
Power save mode	Displays the setting of the Power save mode of the port.
LED status	Displays the LED status of the port.

Modify the LED Mode on the Switch

To modify the LED mode on the switch, perform the following procedure:

1. From the Navigation pane, go to System Settings > Port LED.

   The Port LED page is displayed. See Figure 18 on page 57.

2. Modify the LED mode in the Basic settings section using the pull-down menu. See the description of the LED mode in Table 20.

Note

The LED mode in the Basic settings section applies all the ports on the switch. If you want to set the LED mode for a specific port, go to "Modify the LED Mode on a Port" on page 60.

---

3. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Setting the Traffic Thresholds

To identify ports that periodically experience low traffic, you can configure the LED of a port to turn off when the ingress traffic falls below a defined threshold level for about thirty seconds. The LED remains off even if the traffic exceeds the threshold again.

To set the ingress traffic threshold to identify ports that experience low traffic, perform the following procedure:

1. From the Navigation pane, go to System Settings > Port LED.

   The Port LED page is displayed. See Figure 18 on page 57.

2. Do one of the following options:

   ❏ Select one or more ports by clicking the port checkbox(es), then click Edit.

   ❏ Click Edit all ports.

   The switch displays a Port LED - Port settings page. See Figure 19.

Figure 19. Port LED - Port Settings Page

3. Select Off in the LED action field.

4. Select Enable in Enable the Receiving rate threshold field.

5. Specify the Receiving rate threshold in Kbps.

6. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modify the LED Mode on a Port

To modify the LED mode on the switch, perform the following procedure:

1. From the Navigation pane, go to System Settings > Port LED.

   The Port LED page is displayed. See Figure 18 on page 57.

2. Do one of the following options:

   ❏ Select one or more ports by clicking the checkbox(es), then click **Edit**.

   ❏ Click **Edit all ports**.

   The switch displays the Port LED - Port settings page for the ports you selected. See Figure 19 on page 59 as an example.

3. Modify the LED action, either On or Off.

4. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Feature License

> **Note**
> Currently, this feature is not available.

User Interfaces, FTP, and TFTP

You can manage the switch by enabling or disabling the FTP server and TFTP server from the Others page.

⚠ **Caution**

Do not disable HTTP Server. When it is disabled, you lose the connection and cannot manage the switch.

Enabling Management Tools

To enable management tools, perform the following procedure:

1. From the Navigation pane, go to System Settings > Others.

   The Others page is displayed. See Figure 20.

Figure 20. Others Page

2. Configure the fields described in Table 21

Table 21. Others

Field	Description
User interface	
Enable console port	Not supported
Console timeout	Not supported

Table 21. Others (Continued)

Field	Description
Enable telnet server	Not supported
Telnet port number	Not supported
Telnet session limit	Not supported
Enable Web interface	Enable HTTP Server on the switch. By default, HTTP Server is enabled. ⚠️ **Caution** Do not disable HTTP Server. When it is disabled, you lose the connection to manage the switch.
HTTP port number	Displays the TCP port number for the HTTP server. The value is 80. You cannot change the value.
FTP server	
Enable FTP server	Enable or disable 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. By default, FTP Server is enabled.
Port number	Specify the TCP port number for FTP Server. The range is 1 to 65535. The default value is 21.
TFTP	
Port number	Specify the TCP port number for TFTP Server. The range is 1 to 65535. The default value is 69.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Chapter 3
Switch Settings

This chapter includes the following topics:

Ports

From the Ports page, you can enable or disable the power saving mode, view port parameters and status, and edit port settings.

Enabling the Power Saving Mode

The power saving mode reduces the overall power usage of the switch by decreasing the amount of power the switch provides to ports that have not established links to network devices. You can save power usage by enabling the Eco-friendly mode.

❒ This feature is activated at the switch level. You cannot enable it on individual ports.

❒ This feature does not affect the network operations of the ports.

❒ When this feature is enabled on the switch, ports may take up to three seconds to initially establish links with the network devices.

To enable the Eco-friendly mode, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Port.

   The Port Settings page is displayed. See Figure 21.
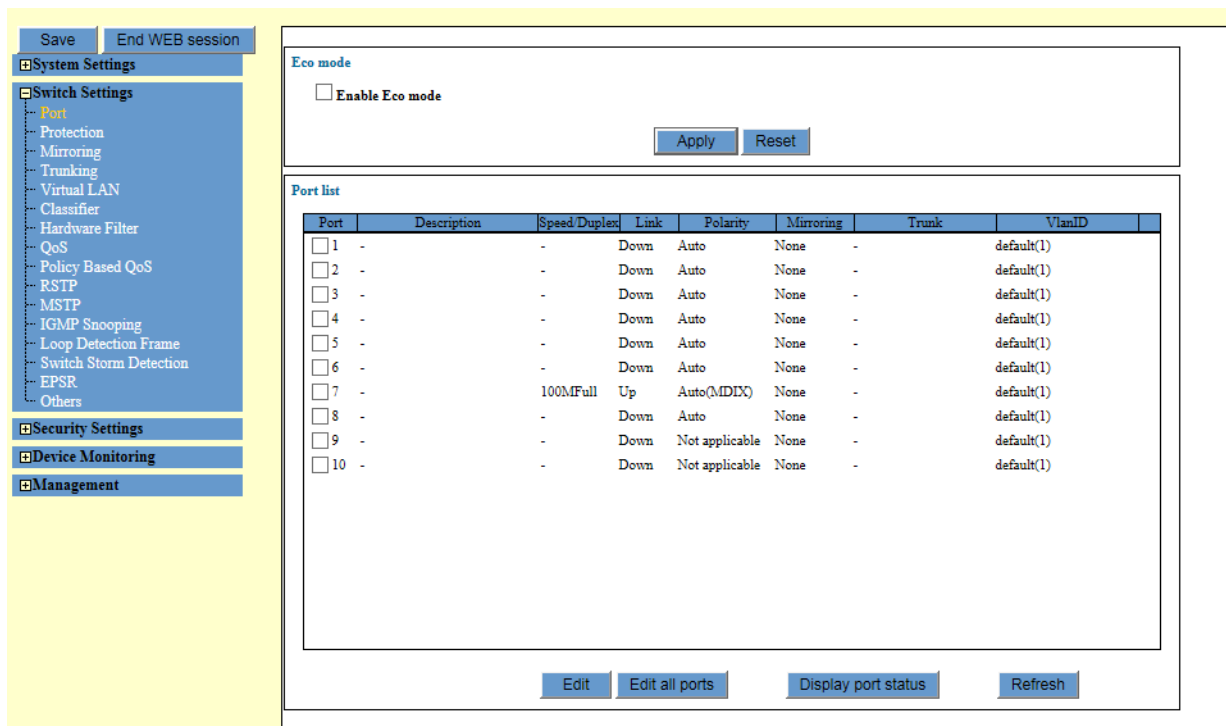
Figure 21. Port Settings Page

2. Check the Enable Eco mode checkbox to enable the Power saving mode.

3. Click **Apply**.

The Eco-friendly mode is now enabled.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Displaying Port Settings

To display the port parameters and status, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Port.

   The Port List section is displayed. See Figure 21 on page 66.

2. Observe the fields as described in Table 22.

Table 22. Ports

Field	Description
Port	Displays the port number and checkbox.
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: ❑ Up: The port has established a link to a network device. ❑ Down: The port has not established a link to a network device or the port is disabled with the Disable (Down) link state. > **Note** > A port in the spanning tree discarding state has an Up state. Also, a port that is disabled with the Enable (Up) link state has an Up state.
Polarity	Displays the current MDI state of a port.

Table 22. Ports (Continued)

Field	Description
Mirroring	Displays whether a port is a member of a port mirror. The possible states are: ❒ Mirror: The 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. ❒ None: The port is not a member of a port mirror. ❒ Rx: The port is a source port of the port mirror. The switch is copying its ingress traffic to the mirror port. ❒ Tx: The port is a source port of the port mirror. The switch is copying its egress traffic to the mirror port. ❒ Both: The 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 the port is a trunk member. The column is empty if the port is not a member of any port trunk.
VlanID	Displays the name and VID of the VLAN where a port is an untagged member.

3. To update the information, click **Refresh**.

Editing Port Parameters

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

1. From the Navigation pane, go to Switch Settings > Port.

   The Port List section is displayed. See Figure 21 on page 66.

2. Check the checkbox of the port that you want to edit.

3. Click **Edit**.

   The Port setting page appears. See Figure 22 on page 69.

   Note
   When you click **Edit all ports**, the Edit page displays parameters for all the ports.
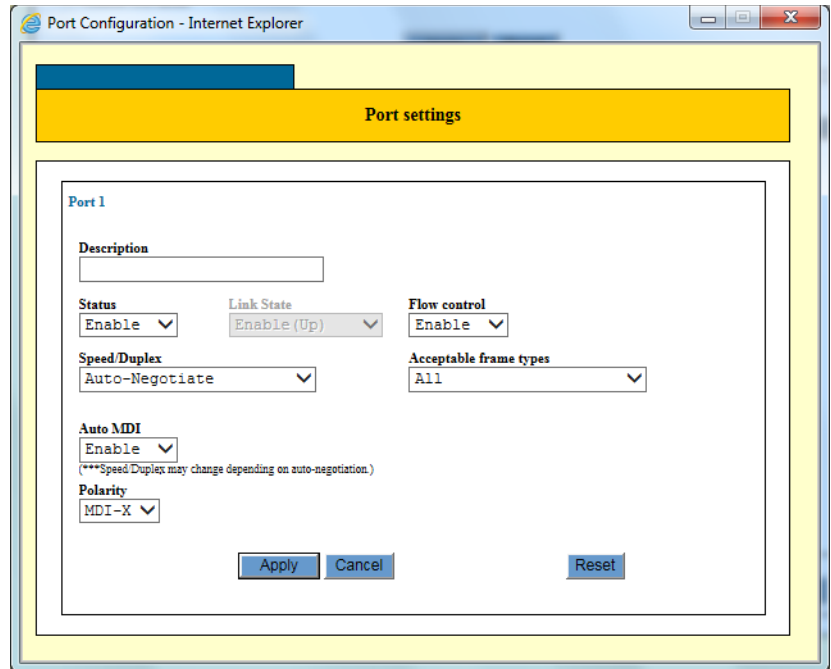
Figure 22. Port Settings Page

4. Edit the fields described in Table 23.

Note

You might lose access to the switch when you change the configuration of the management port. For example, when you disable the management port, you lose the connection and cannot manage the switch.

Table 23. Port Settings

Field	Description
Description	Assigns a name to the port. A name can be 1 to 20 alphanumeric characters. Spaces are allowed in a name, but not special characters, such as * or @. The default value is none.

Table 23. Port Settings (Continued)

Field	Description
Status	Enables or disables a port. A disabled port does not accept or forward frames. You may disable a port to prevent unauthorized use if the port is unused. The options are: ❏ Enabled - The port forwards ingress and egress packets. This is the default setting. ❏ Disabled - The port does not forward any ingress or egress packets.
Link state	Select he link status of a disabled port. **Note** This field is only available when the port is disabled with the Status field. The options are: ❏ 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	Specify the speed and duplex mode of the port. You may select Auto-negotiation so that the port configures its speed and duplex mode automatically. The default value of a copper port is Auto-negotiation. The default value of a fiber port is 100Mbps in the full-duplex mode.

Table 23. Port Settings (Continued)

Field	Description
Auto MDI	This is the PHY spec of this DUT for copper port. If the port speed is fixed, auto MDI is disable and the polarity is MDIX. Enable or disable Auto MDI. **Note** This field is not applicable to fiber ports. The options are: ❏ Enabled - The MDI/MDIX wiring configuration is set automatically. This is default setting for copper ports. ❏ Disabled - Use the Polarity field to set the wiring configuration manually.
Polarity	This is the PHY spec of this DUT for copper port. If the port is a trunk port, the user cannot change the configuration of auto-MDI and polarity. Specify the wiring configuration of a port when Auto MDI is disabled. The selections are MDI and MDIX.
Flow control	Enables or disables Flow Control. The 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. **Note** This field is not applicable to fiber ports. It only applies to copper ports operating in full-duplex mode. The options are: ❏ Enabled - Flow Control is enabled on the port. This is the default setting. ❏ Disabled - Flow Control is disabled on the port.

Table 23. Port Settings (Continued)

Field	Description
Acceptable frame types	Specify whether the port accepts untagged packets as well as tagged packets. The options are: ❒ All - The port forwards both ingress tagged and untagged packets. This is the default setting. ❒ Tagged Packets Only - The port accepts ingress tagged packets and discards untagged packets.

5. Click **Apply**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Displaying Port Status

To display the port status on the switch, perform the following procedure:

Note
You can display the status for multiple ports at a time.

1. From the Navigation pane, go to Switch Settings > Port.

   The Port List section is displayed. See Figure 21 on page 66.

2. Check the checkbox of the port that you want to view the status.

3. Click **Display port status**.

   The Display port status page appears. See Figure 23.
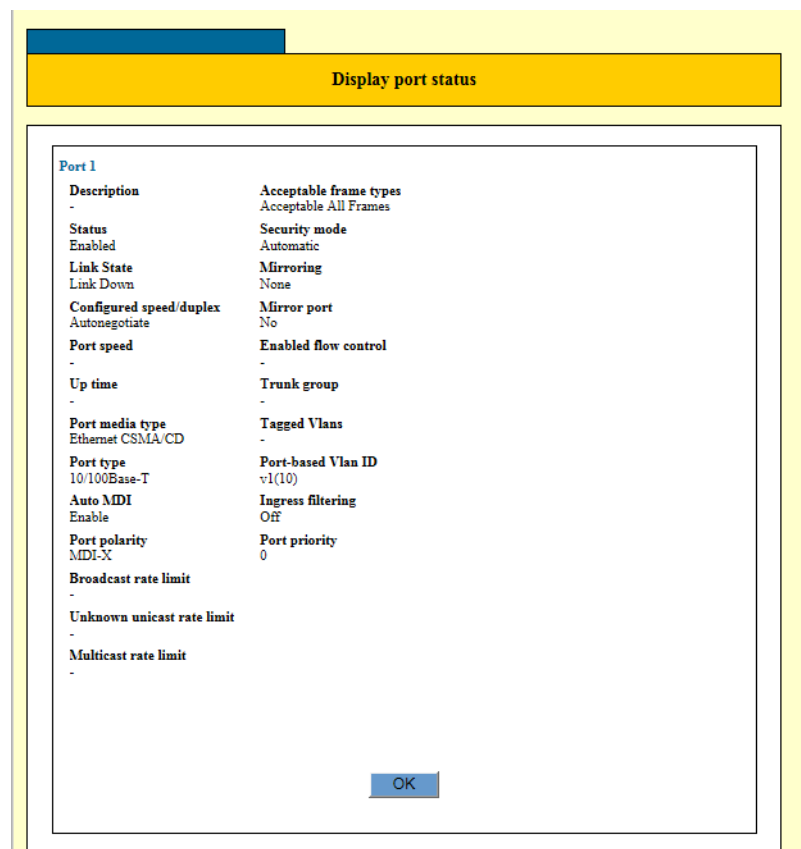
Figure 23. Display Port Status Page

4. Observe the fields described in Table 24 on page 74.

Table 24. Display Port Status

Field	Description
Description	Displays the port description.
Status	Displays whether the port is enabled or disabled. The states are: ❑ Enabled - The port can forward ingress and egress packets. ❑ Disabled - The port cannot forward ingress and 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 is Ethernet CSMA/DC for twisted pair ports.
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 "Packet Storm Protection" on page 76.
Acceptable Frame Types	Displays whether a port is accepting both tagged and untagged packets or only tagged packets. The states are: ❑ Acceptable All Frames - The port is accepting both tagged and untagged packets. ❑ Admit Only VLAN-tagged Frames - The port is accepting only tagged packets.
Security Mode	Displays the security mode of the port.
Mirroring	Displays whether the port is a source port of a port mirror.

Table 24. Display Port Status (Continued)

Field	Description
Mirror Port	Displays whether the port is acting as a port mirror.
Enabled Flow Control	Displays whether Flow Control is enabled on the port. **Note** This field only applies to ports operating in full-duplex mode. The states are: ❑ - - Flow Control is not enabled or the port is not connected to an active network device. ❑ Pause - Flow Control is enabled.
Trunk Group	Displays the name of the trunk group to which the port belongs. This field is empty if the port is not a member of a trunk group.
Tagged VLANs	Displays the VIDs of the VLANs where the port is a tagged member.
Port-based VLAN ID	Displays the name and VID where the port is an untagged member.
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 states are: ❑ Off - Ingress filtering is disabled. ❑ On - Ingress filtering is enabled.
Port Priority	Displays the priority value assigned to ingress untagged packets on the port.

5. Click **OK**.

Packet Storm Protection

Packet Storm Protection allows you to set a threshold for the maximum number of ingress broadcast, multicast, or unknown unicast packets on the ports. When Packet Storm Protection is enabled, packets above the threshold are discarded by the switch to protect the network from packet storms.

Guidelines for Packet Storm Protection

Here are guidelines to configuring Packet Storm Protection:

❏ The switch supports only one threshold value in bps.

❏ You may activate packet filtering on the individual ports.

❏ To enable Packet Storm Protection, you must enable the broadcast rate limit. The following list shows the combinations of effectively enabled Packet Storm Protection:

- The broadcast rate limit is on

- The broadcast and multicast rate limits are on

- The broadcast and unknown unicast rate limits are on

- All of the rate limits are on

Displaying the Packet Storm Protection Settings

To display the Packet Storm Protection settings on ports, perform the following procedure:

1. From the Navigation pane, click Switch Settings > Protection.

The Packet Storm Protection page is displayed. See Figure 24.
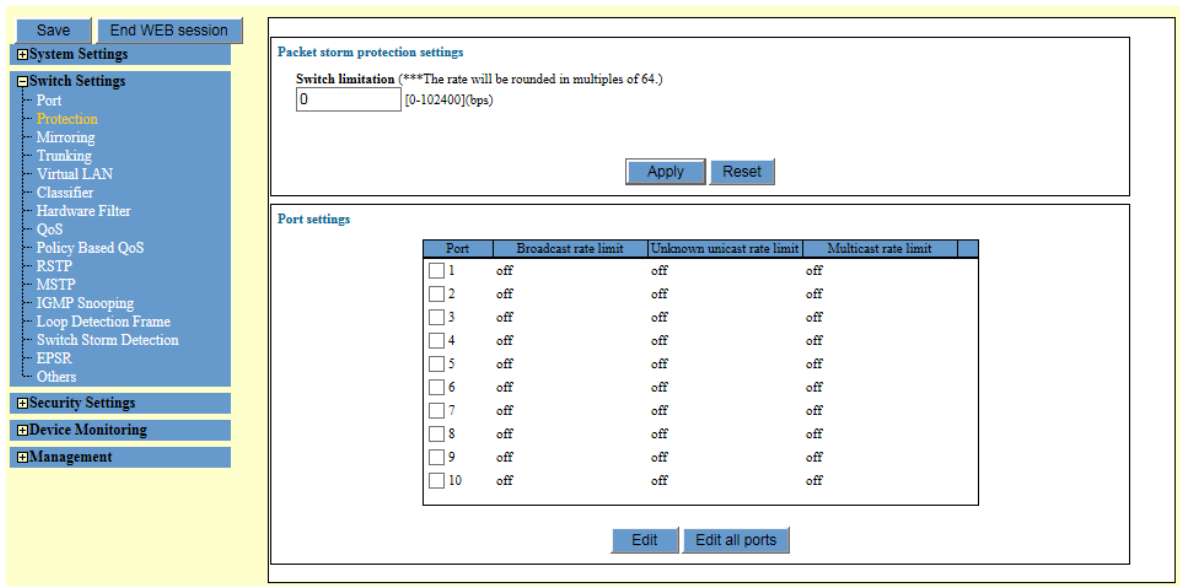
Figure 24. Packet Storm Protection Page

2. Observe the fields described in Table 25.

Table 25. Packet Storm Protection Port Settings

Field	Description
Port	Displays a port number and checkbox.
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.

Adjusting the Threshold Limit for Packet Filtering

To adjust the threshold limit for packet filtering, perform the following procedure:

1. From the Navigation pane, click Switch Settings > Protection.

    The Packet Storm Protection page is displayed. See Figure 24 on page 76.

2. Enter a new value in the Switch Limitation field.

    Note
    The range is 0 to 1,024,000 bps. The switch automatically rounds off the value to a multiple of 64 bps.

3. Click **Apply**.

    The new threshold limit value is now in effect.

    Note
    To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Enabling or Disabling Packet Storm Protection on Ports

You can enable or disable Packet Storm Protection on the broadcast rate limit, unknown rate limit, and multicast rate limit on each port.

To enable or disable Packet Storm Protection, perform the following procedure:

1. From the Navigation pane, click Switch Settings > Protection.

   The Packet Storm Protection page is displayed. See Figure 24 on page 76.

2. Select one or more ports by checking the checkbox(s).

   Note
   To edit the Packet Storm Protection settings on all the ports at once, click **Edit all ports**.

3. Click **Edit**.

   The Packet Storm Protection - Edit page is displayed. See Figure 25.
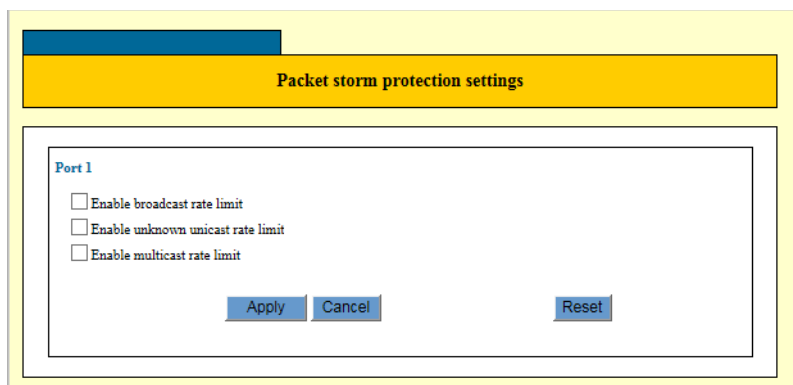
Figure 25. Packet Storm Protection Enable or Disable Page

4. Enable or disable Packet Storm Protection on the broadcast rate limit, unknown unicast rate limit, and/or multicast rate limit.

5. Click **Apply**.

   The Packet storm protection conditions are applied for the ports you selected.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Port Mirroring

Port Mirroring 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. Port Mirroring can be used to troubleshoot network problems or to investigate possible unauthorized network access.

To use the feature, you must 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.

Guideline for Port Mirroring

Here are guidelines to using Port Mirroring:

❐ 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.

Note
The performance and speed of the switch is not affected by Port Mirroring.

Enabling Mirroring

To enable mirroring, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Mirroring.

   The Mirroring Settings page is displayed. See Figure 26 on page 80.
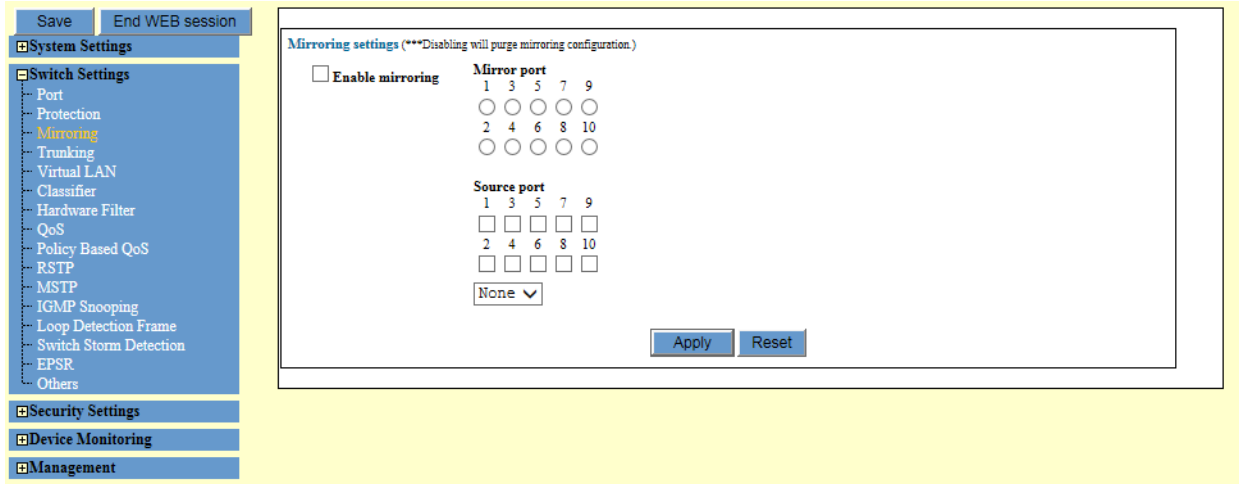
Figure 26. Mirroring Settings Page

2. Configure Port Mirroring in the fields as described in Table 26.

Table 26. Mirroring Settings

Fields	Description
Enable Mirroring	Enable or disable the mirror function on the switch.
Mirror Port	Select a mirror port. You can designate only one port as a mirror port.
Source Port	Select source one or more source ports. You can select multiple source ports except the port that is selected as the mirror port.
Traffic to be monitored	Select one of the following option from the pull-down menu: ❏ 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.

3. Click **Apply**.

Port Mirroring with your settings are now active on the switch.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

4. Connect a data analyzer to the mirror port to monitor the traffic on the source ports.

Disabling Mirroring

To disable Port Mirroring, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Mirroring.

   The Mirroring Settings page is displayed. See Figure 26 on page 80.

2. Uncheck the checkbox to disable Port Mirroring.

3. Click **Apply**.

   Port Mirroring is now disabled.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Trunking

Port Trucks are groups of two to eight ports that act as single virtual link between the switch and other network devices. Port Trucks 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.

Guidelines for Port Trunks

Here are guidelines for static port trunks:

❑ The switch can support up to eight static port trunks at one time.

❑ A port trunk can have up to eight ports.

❑ A port trunk cannot have both twisted pair and 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 5-7) or nonconsecutive (for example, ports 2, 4, 6).

❑ The ports of a port trunk must be members of the same VLAN.

❑ Before creating a port trunk, set the speed, duplex mode, flow control settings the same on all the ports to be in the trunk.

❑ After setting a port trunk, do not change the parameter settings of any port in the trunk without changing the same settings on the other ports.

❑ You may use 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 trunks, a trunk on one device might not be compatible with the same feature on a device from a different manufacturer. Allied Telesis recommends using this feature only between Allied Telesis network devices.

Displaying Trunk Settings

To display trunk settings on the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Trunking.

   The Trunk settings page is displayed. See Figure 27 on page 83.
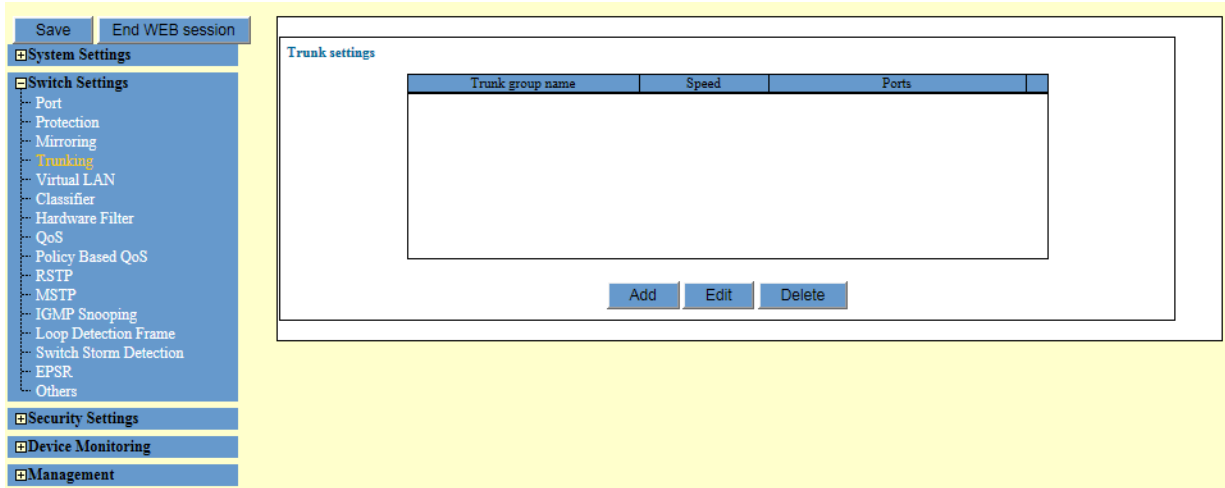
Figure 27. Trunk Settings Page

2. Observed the fields described in Table 27.

Table 27. Trunk Settings

Field	Description
Trunk group name	Displays the name of a port trunk.
Speed	Displays the speed of the trunk.
Ports	Displays the member ports of the trunk.

Guidelines for Trunking Data

Here are the guidelines for trunking data:

❑ The master port is the smallest part of port number in the port set as a trunk group.

❑ The flooding packet (bc/mc/dlf) is always output from a master port.

❑ The mirror port and ports belonging to other trunk groups cannot be designated in a member port.

❑ You cannot make a port including configuration in security belong to a trunk group.

❑ When the ports are in a different configuration in the (m)STP,EPSR function, the ports cannot belong to the same trunk group.

❑ When the configuration of ports are different in loop detection (or storm protection), you cannot add the port to an identical trunk group.

❑ You must make the setting of FLOW control (disable/enable) the same setting in the same trunk group.

Creating a Port Trunk

To create a new port trunk on the switch, perform the following procedure:

1. Disconnect all the data cables from the ports of the trunk.

    ⚠ **Caution**
    Disconnect all the data cables from the ports of the trunk before adding or removing ports from the trunk, or deleting a trunk from the switch. leaving the cables connected can form a loop in your network topology, which can result in a broadcast storm and poor network performance.

2. From the Navigation pane, go to Switch Settings > Trunking.

    The Trunk settings page is displayed. See Figure 27 on page 83.

3. Click **Add**.

    The Trunk settings - Add page appears. See Figure 28 on page 84.

Figure 28. Trunk Settings - Add Page

4. Configure the parameters as described in Table 28.

Table 28. Trunk Settings

Field	Description
Trunk group name	Specify a name for the new trunk. The name can be up to 20 alphanumeric characters. Spaces or special characters, such as * and @, are *not* allowed. Each trunk must have a unique name.
Speed	Select the speed of the ports in the trunk from the pull-down menu, either 100Mbps or 10Mbps.

Table 28. Trunk Settings (Continued)

Field	Description
Ports	Specify port members of the trunk by checking on the checkboxes of the ports. One port trunk can have up to eight ports.

5. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

6. Configure the ports on the remote device for Port Trunking.

7. Connect the cables to the ports of the trunk on the switch and the remote device.

    The port trunk is ready for network operation.

Modifying a Port Trunk

To modify an existing port trunk, perform the following procedure:

1. Disconnect all the data cables from the ports of the trunk.

> ⚠ **Caution**
> Disconnect all the data cables from the ports of the trunk before adding or removing ports from the trunk, or deleting a trunk from the switch. leaving the cables connected can form a loop in your network topology, which can result in a broadcast storm and poor network performance.

2. From the Navigation pane, go to Switch Settings > Trunking.

    The Trunk settings page is displayed. See Figure 29 on page 89.

3. Select a trunk that you want to edit the settings.

4. Click **Edit**.

    The Trunk settings - Edit page appears.

5. Modify the parameters described in Figure 28 on page 84.

6. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more
> information, see "Saving the Changes to a Configuration File" on
> page 21.

7. Configure the ports with the same port and trunking parameters on the remote device if necessary.

8. Reconnect the cables to the ports of the trunk between the switch and the remote device.

   The port trunk is ready for network operation.

Deleting a Port Trunk

To delete a existing port trunk, perform the following procedure:

1. Disconnect all the data cables from the ports of the trunk.

> ⚠️ **Caution**
> Disconnect all the data cables from the ports of the trunk before
> adding or removing ports from the trunk, or deleting a trunk from the
> switch. leaving the cables connected can form a loop in your
> network topology, which can result in a broadcast storm and poor
> network performance.

2. From the Navigation pane, go to Switch Settings > Trunking.

   The Trunk settings page is displayed. See Figure 29 on page 89.

3. Select the trunk that you want to delete.

4. Click **Delete**.

   A confirmation page appears.

5. Click **OK** to confirm.

6. Reconnect the cables as needed.

> **Note**
> To save your changes into a configuration file, click **Save**. For more
> information, see "Saving the Changes to a Configuration File" on
> page 21.

Port-based and Tagged VLAN

A VLAN consists of a group of ports that form an independent traffic domain on one or more Ethernet switches. You can create and configure VLANs by assigning untagged and tagged ports to VLANs. Port-based VLANs is associated with untagged ports; IEEE802.1Q VLAN tagging is associated with tagged ports.

> **Note**
> For information about VLAN, see Appendix A, "VLANs Overview" on page 255. To configure Protected Ports VLAN, see "Protected Ports VLAN" on page 95.

Guidelines to Adding or Removing Ports from VLANs

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

Here are 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 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. 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 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 Configuration

To display the VLAN settings on the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

   The Virtual LAN Settings page is displayed. See Figure 29.
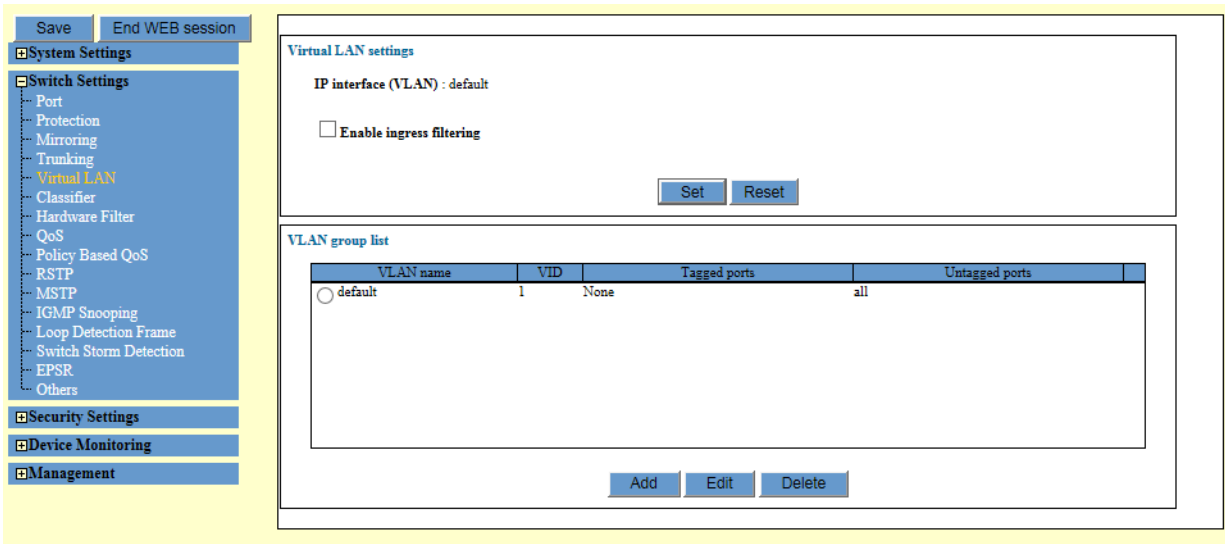
Figure 29. Virtual LAN Settings Page

2. Observe the fields as described in Table 29 on page 89.

Table 29. Virtual LAN Settings

Field	Description
Virtual LAN Settings	
IP interface (VLAN)	Displays the name of the VLAN that is assigned the switch's IP address to, which is the switch's management VLAN.
Enable ingress filtering	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.
VLAN Group List	
VLAN name	Displays the name of a VLAN and its radio button to select the VLAN.
VID	Displays the identifier of the VLAN. The VID of the default VLAN is always 1.
Tagged ports	Displays the tagged ports of the VLAN. These ports are for IEEE802.1Q VLAN tagging.
Untagged ports	Displays the untagged ports of the VLAN. These ports are for a port-based VLAN.

Creating a Port-based or Tagged VLAN

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

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

   The Virtual LAN settings page is displayed. See Figure 29 on page 88.

2. Examine the VLAN table and do one of the following:

   ❒ If the ports are untagged members of the default VLAN or no member of any VLANs, go to step 3.

   ❒ If a port is currently untagged members of a VLAN other than the default VLAN, you must remove the port from their current untagged VLAN assignment to return them to the default VLAN. Go to "Modifying a Port-based or Tagged VLAN Configuration" on page 92.

3. Click **Add**.

   The VLAN settings - Add page appears. See Figure 30 on page 90.
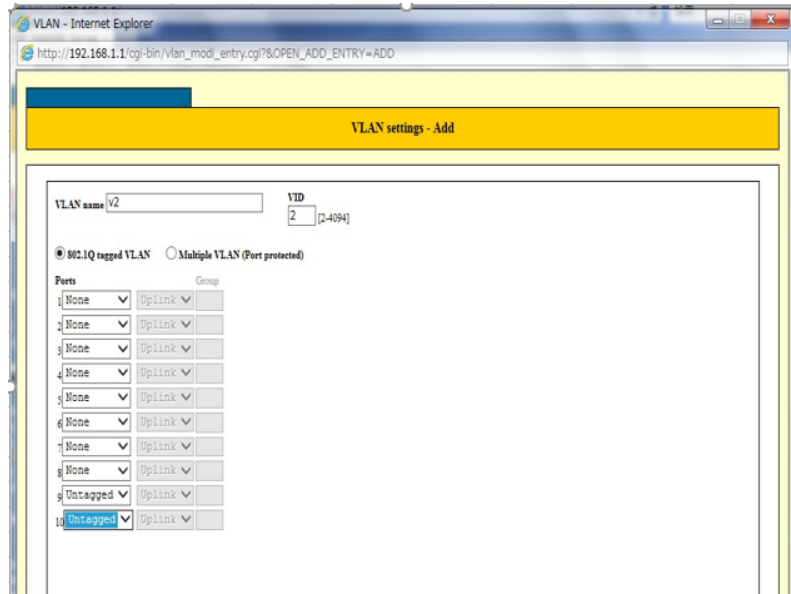
Figure 30. VLAN Settings - Add Window

4. Configure the parameters as described in Table 30.

Table 30. VLAN Settings

Field	Description
VLAN Name	Specify a name for a new VLAN. The name can be up to 20 alphanumeric characters. Spaces or special characters, such as * and @, are *not* allowed. If the VLAN is par of a larger VLAN that spans multiple switches, then the name of the VLAN must be the same on each switch where nodes of the VLAN are connected.
VID	Assign a VID to a new VLAN. A VLAN must have a VID. The range is 2 to 4094. The default is the next available VID number on the switch. If the VLAN is part of a larger VLAN that spans multiple switches, then the VID for the VLAN must be the same on each switch. The switch is only aware of its own VIDs and not those being used by other devices in the network.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.

Table 30. VLAN Settings (Continued)

Field	Description
802.1Q tagged VLAN	Select this option to create a new VLAN and assign ports as tagged or untagged.
Multiple VLAN (Port Protected)	This field is not used for port-based or tagged VLANs. For protected ports VLANs, see "Protected Ports VLAN" on page 95.
Ports	Designate ports as tagged or untagged ports of the VLAN. A VLAN can contain from one port to all the ports on the switch. The options are: ❐ None - Designate ports as no member of the new VLAN. This is the default setting. ❐ Untagged - Add a port as an untagged port of the new VLAN. ❐ Tagged - Add a port as a tagged port of the new VLAN.
Uplink	This field is not used for port-based or tagged VLANs.
Group	This field is not used for port-based or tagged VLANs.

5. Click **OK**.

6. Here are a couple points to consider:

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

   For example, let's assume that you want to create a new VLAN called Sales with untagged ports 1 to 5 that already belong as untagged ports in a VLAN called Accounting. In this situation you have to remove the ports from the Accounting VLAN before adding them to the new VLAN. For instructions on how to remove untagged ports from VLANs, see "Modifying a Port-based or Tagged VLAN Configuration" on page 92.

   ❐ 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.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a Port-based or Tagged VLAN Configuration

Before modifying a port-based or tagged VLAN configuration, review "Guidelines to Adding or Removing Ports from VLANs" on page 87.

To add or remove ports from a port-based or IEEE 802.1Q tagged VLA on the switch, perform the following procedure:

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

Note
If you delete the member port of the management VLAN, you cannot access the DUT from the GUI. (There is no error.)

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

   The Virtual LAN settings page is displayed. See Figure 29 on page 88.

2. Mark the radio button for the VLAN you want to add or remove tagged or untagged ports.

3. Click **Edit**.

   The VLAN settings - Edit page appears. See Figure 31 on page 93.

Figure 31. VLAN Settings - Edit Page

4. Modify the parameters in the window as needed. The parameter are described in Table 30 on page 90.

5. Click **OK**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting a Port-based or Tagged VLAN

Before deleting a port-based or tagged VLAN, review the following information:

❒ 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 7 on page 24. The management VLAN is called Interface (VLAN).

❒ 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 VLANs from the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

   The Virtual LAN settings page is displayed. See Figure 29 on page 88.

2. Select the radio button of the VLAN you want to delete.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK** to confirm.

   Here are a couple items to consider:

   ❒ If you see the message "Cannot delete VLAN when contains IP Interface," you tried to delete the management VLAN, which is not permitted. Designate another VLAN as the management VLAN. For instructions, see "Changing the IP Addresses" on page 26. The management VLAN is called Interface (VLAN).

   ❒ 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.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Protected Ports VLAN

This procedure explains how to create a new protected ports VLAN. Review the following information before creating a protected ports 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 82 on page 266 and Table 83 on page 266.

❏ For guidelines on changing the VLAN assignments of ports, see "Guidelines to Adding or Removing Ports from VLANs" on page 87.

Note

For information about VLAN, see Appendix A, "VLANs Overview" on page 255. To configure Port-based and Tagged VLAN, see "Port-based and Tagged VLAN" on page 87.

Guidelines for Protected Ports VLAN

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.

❏ When using multiple VLAN and tag VLAN, it is treated as multiple.

❏ A group can be a member of only one protected ports VLAN at a time.

Displaying the VLAN Configuration

To display the VLAN settings on the switch, see "Modifying a Port-based or Tagged VLAN Configuration" on page 92.

Changing VLAN Configuration

❐ You cannot control DUT with an uplink port for management VLAN.

❐ When using multiple VLANs and tag VLANs, it is treated with multiple.

❐ VLAN priority (this is a limitation).

❐ Default VLAN (VID=1) cannot be used as a Protected Port VLAN.

❐ Uplink port can communicate for CPU (SNMP, GUI, syslog, NTP).

❐ You cannot use uplink port to communicate with a client port to CPU (NTP, SNMP, GUI, syslog, etc.).

❐ You cannot make changes in the group number and untag/ tagged at the same time. Change it separately. For example, when "untag->Tagged" is changed in the group number at the same time, the result is a configuration with untag/default.

Creating a Protected Ports VLAN

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

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

2. Examine the VLAN table 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 member of any VLANs, go to step 3.

   ❐ If a port is currently untagged members of a VLAN other than the default VLAN, you must remove the port from their current untagged VLAN assignment to return them to the default VLAN. For instructions, see "Modifying a Port-based or Tagged VLAN Configuration" on page 92.

3. Click **Add**.

Figure 32. VLAN Settings - Add Protected Ports VLAN

4. Configure the parameters as described in Table 30.

Note
You may create only one VLAN at a time.

Table 31. VLAN Settings

Field	Description
VLAN Name	Specify a name for a new VLAN. The name can be up to 20 alphanumeric characters. Spaces or special characters, such as * and @, are *not* allowed. If the VLAN is part of a larger VLAN that spans multiple switches, then the name of the VLAN must be the same on each switch where nodes of the VLAN are connected.

Table 31. VLAN Settings (Continued)

Field	Description
VID	Assign a VID to a new VLAN. A VLAN must have a VID. The range is 2 to 4094. The default is the next available VID number on the switch. If the VLAN is part of a larger VLAN that spans multiple switches, then the VID for the VLAN must be the same on each switch. The switch is only aware of its own VIDs and not those being used by other devices in the network.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.
802.1Q tagged VLAN	This option is not used with protected ports VLANs. For tagged VLANs, see "Port-based and Tagged VLAN" on page 87.
Multiple VLAN (Port Protected)	Select this option to designate the new VLAN as a protected ports VLAN. Selecting the option activates the client and uplink columns in the window.
Ports	Designate ports as tagged or untagged ports of the VLAN. A VLAN can contain from one port to all the ports on the switch. The options are: ❒ None - Designate ports as no member of the new VLAN. This is the default setting. ❒ Untagged - Add a port as an untagged port of the new VLAN. ❒ Tagged - Add a port as a tagged port of the new VLAN.

Table 31. VLAN Settings (Continued)

Field	Description
Uplink	Designate the uplink port of the new protected ports VLAN. A protected ports VLAN can have only one uplink port. **Note** This field is initially greyed out. It becomes active when you select the Multiple VLAN (port protected) option. **Note** Do not control DUT with Uplink port for management VLAN.
Group	Assign group numbers to the ports of the new VLAN. The range is 1 to 65535. **Note** This field is initially greyed out. It becomes active when you select the Multiple VLAN (port protected) option.

Figure 33 is an example of how the VLAN Settings - Add window would look for the protected ports VLAN detailed in Table 56 on page 207 and Table 57 on page 207.
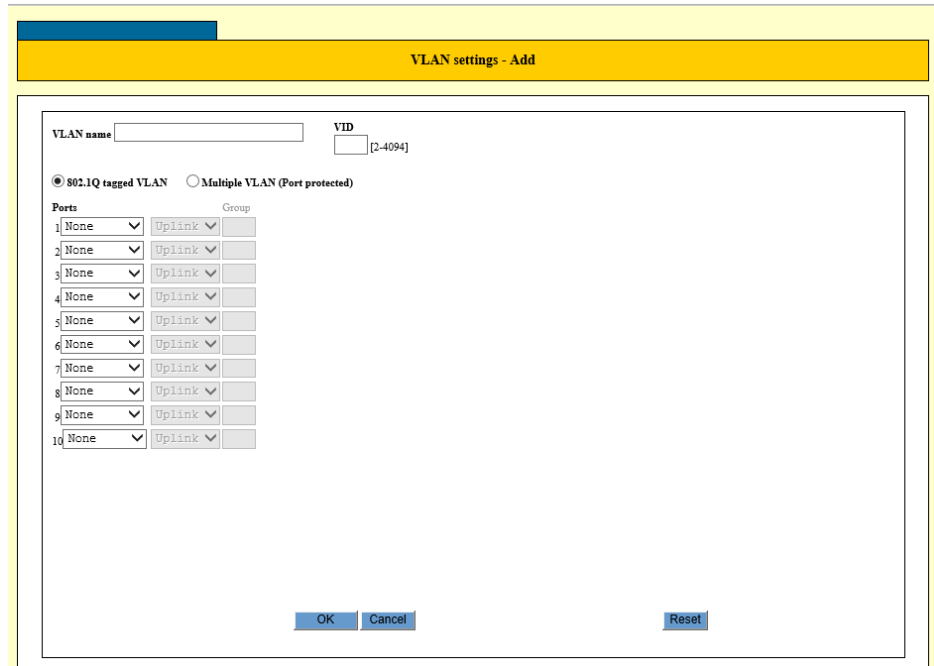
Figure 33. VLAN Settings - Add Page for Protected Ports VLAN

5. Click **OK**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying the Protected Ports VLAN Configuration

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

> **Note**
> For guidelines on changing the VLAN assignments of ports, see "Guidelines to Adding or Removing Ports from VLANs" on page 87.

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

    The Virtual LAN settings page is displayed. See Figure 29 on page 88.

2. Mark the radio button for the VLAN you want to add or remove tagged or untagged ports.

3. Click **Edit**.

    The VLAN settings - Edit page appears. See Figure 31 on page 93.

4. Modify the parameters in the window as needed. The parameter are
   described in Table 31 on page 97.

5. Click **OK**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more
> information, see "Saving the Changes to a Configuration File" on
> page 21.

Deleting a Protected Ports VLAN

To delete a protected ports VLANs from the switch, perform the following
procedure:

1. From the Navigation pane, go to Switch Settings > Virtual LAN.

   The Virtual LAN settings page is displayed. See Figure 29 on page 88.

2. Select the radio button of the VLAN you want to delete.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK** to confirm.

   Here are some items to consider:

   ❒ If you see the message "Cannot delete VLAN when it contains IP
   Interface," you tried to delete the management VLAN, which is not
   permitted. Designate another VLAN as the management VLAN.
   For instructions, see "Changing the IP Addresses" on page 26. The
   management VLAN is called Interface (VLAN).

   ❒ 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

> **Note**
> To save your changes into a configuration file, click **Save**. For more
> information, see "Saving the Changes to a Configuration File" on
> page 21.

Rapid Spanning Tree Protocol (RSTP)

Spanning Tree Protocols are designed to build a loop-free logical topology for Ethernet networks by detecting and blocking loops in the networks. A data loop exists when two or more nodes can transmit data to each other over more than one data path in a network. Data loops can cause broadcast storms that can significantly reduce network performance. Where multiple paths exist, a spanning tree protocol places the extra paths in a standby or block mode by disabling ports, so that there is only one active path.

Note
For more information about RSTP, see Appendix B, "Rapid Spanning Tree Protocol Overview" on page 269.

Rapid Spanning Tree Protocol (RSTP) is an enhancement of the original STP. The switch does not come with the STP version; however, RSTP is fully compatible with STP.

Displaying the RSTP Settings

To display the RSTP settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > RSTP.

   The RSTP status is displayed. See Figure 34.
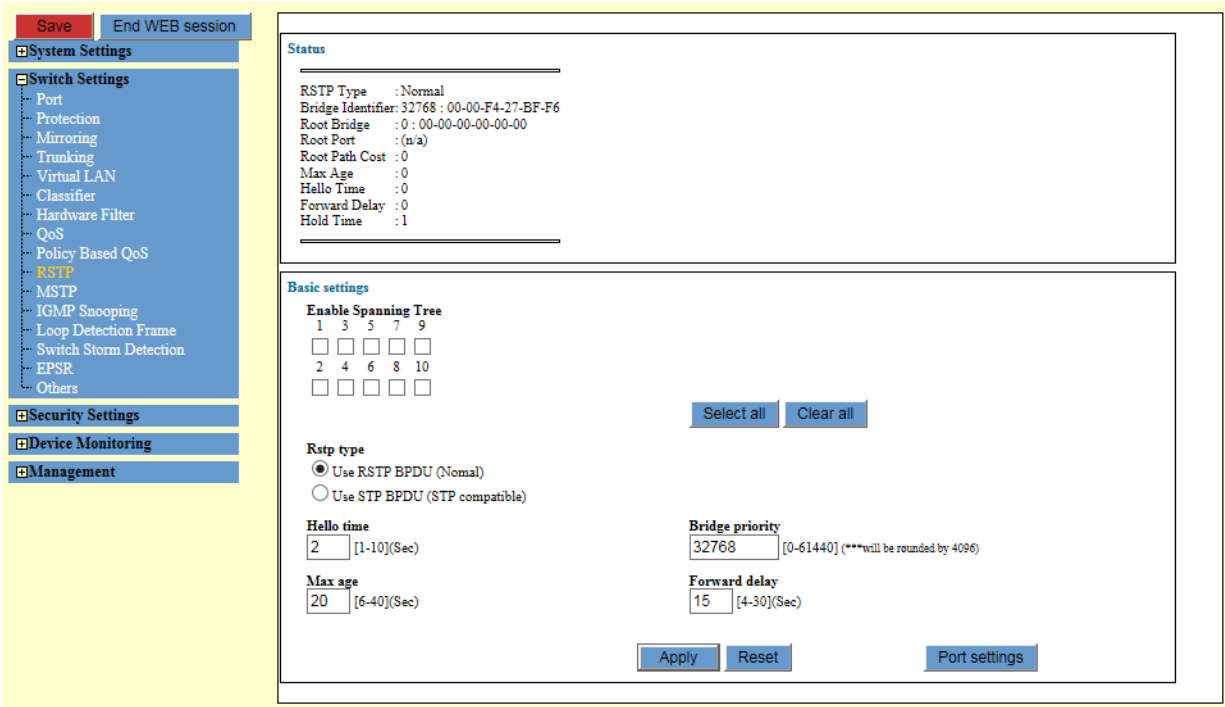
Figure 34. RSTP Page

2. Observe the status fields described in Table 32.

Table 32. RSTP Status

Field	Description
RSTP Type	Displays whether the bridge is operating with RSTP or in an STP-compatible mode. The options are: ❒ 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.
Bridge Identifier	Displays the switch's bridge priority value and MAC address, separated by a colon (:).
Root Bridge	Displays the bridge identifier of the root bridge of the spanning tree domain. Here is the guidelines for the root bridge field: ❒ Root bridge is zero if the spanning tree protocol is not enabled on any of the ports on the switch. ❒ Root bridge is same as the Bridge Identifier parameter if the switch 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. Root Port is "n/a" if the 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. Path cost is the sum of the port costs between the switch (a bridge) and the root bridge. A port cost is typically based on port speed; however, the port cost is adjustable. The faster the port, the lower the port cost. Root Path Cost is 0 if the switch is the root bridge of the spanning tree domain or if RSTP is not activated on any of the ports.

Table 32. RSTP Status (Continued)

Field	Description
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.
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 transmissions 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.

Modifying RSTP Bridge Settings

To create a new flow group, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > RSTP.

2. Change the fields described in Table 33 on page 105.

Table 33. RSTP Basic Settings

Field	Description
Enable Spanning Tree	Enable or disable RSTP on a port.
RSTP type	Select one of the options to control whether the bridge operates with RSTP or in an STP-compatible mode. The options are: ❐ 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	Specify 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.
Bridge priority	Specify 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. Bridge priority can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority.

Table 33. RSTP Basic Settings (Continued)

Field	Description
Max age	Specify 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)).
Forward delay	Specify 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.

3. Click **Apply**.

The RSTP bridge setting changes are in effect.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Displaying RSTP Ports Settings

To create a new flow group, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > RSTP.

The RSTP status and settings are displayed. See Figure 34 on page 102.

2. Click **Port settings** at the bottom on the page.

The Port settings page is displayed. See Figure 35 on page 107.

Figure 35. RSTP Port Settings Page

3. Observe the status fields described in Table 34.

Table 34. RSTP Port Settings

Field	Description
Port	Displays the port number and its checkbox.
RSTP status	Displays whether RSTP is enabled or disabled on the port.
Status	Displays the RSTP port state. The port state can be Discarding, Learning, or Forwarding.
Role	Displays the RSTP port role. The port role can be a Root or Designated.
Edge	Displays whether the port is a edge port or non-edge port.
P2P	Displays the setting for the P2P port.
Version	Displays the version of the STP.
Cost	Displays the cost of the port.

Configuring RSTP Ports Settings

To configure the RSTP port settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > RSTP.

   The RSTP status and settings are displayed. See Figure 34 on page 102.

2. Click **Port settings** at the bottom of the page.

   The Port settings page is displayed. See Figure 35 on page 107.

3. Check the checkbox of the port that you want to configure. You may configure more than one port at a time.

4. Click **Edit**.

   The Port settings - Edit page is displayed. See Figure 36.

Figure 36. RSTP Port Settings - Edit Page

5. Change the fields described in Table 35 on page 109.

Table 35. RSTP Port Settings

Field	Description
Priority	Specify 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 (Cost)	Specify 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 default setting is Automatic detect, which sets the port cost depending on the speed of the port. To specify as Automatic detect, specify 0. The range is 0 to 20,000,000. Default values are: ❐ 2,000,000 for 10 Mbps ports ❐ 200,000 for 100 Mbps ports ❐ 20,000 for 1 Gbps ports
Point-to-Point	Specify the port as a point-to-point port. The options are Yes, No, and Auto-Detect.
Edge Port (Edge)	Specify whether the port is functioning as an edge port.

6. Click **Apply**.

   The RSTP bridge setting changes are in effect.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Multiple Spanning Tree Protocol (MSTP)

Spanning Tree Protocols are designed to build a loop-free logical topology for Ethernet networks. Multiple Spanning Tree Protocol (MSTP) is an extension or an evolution of RSTP. MSTP is fully compatible with STP and RSTP.

Single STP or RSTP does not work efficiently in a network containing more than one VLAN. If a link is blocked, all VLANs are blocked. To overcomes this limitation with other enhancements, MSTP enables grouping and mapping VLANs into different spanning tree instances. Each instance, which is called Multiple Spanning Tree Instance (MSTI), defines a single forwarding topology for an exclusive set of VLANs.

> **Note**
> For more information about MSTP, see Appendix C, "Multiple Spanning Tree Protocol Overview" on page 279.

Multiple Spanning Tree Instance (MSTI)

MSTI is an individual spanning tree domain in MSTP. An MSTI can span any number of switches.

To create an MSTI, assign it a number (MSTI ID), define the scope of the MSTI by assigning one ore more VLANs. The MSTI can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time. A port can be a member of more than one MSTI at a time if the port is a tagged member of one or more VLANs assigned to different MSTIs.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTIID of 0. The CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP bridges in a network.

When you create a new port-based or tagged VLAN, the VLAN is by default associated with the CIST. The default VLAN is also associated with CIST by default. You cannot delete the CIST, or change the ID.

Multiple Spanning Tree Region

An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. The characteristics are:

❑ MST Region Name (ConfigName)

❑ Revision (RevisionLevel)

❑ VLANs

❑ VLAN Associations

Displaying the MSTP Settings

To display the flow groups, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

   The MSTP status are displayed. See Figure 37.

Figure 37. MSTP Page

2. Observe the status fields described in Table 36.

Table 36. MSTP Status

Field	Description
Protocol Version	Displays the MSTP protocol version. The options are: ❒ Normal - The ports on the switch are using MSTP, except those ports that are receiving STP or RSTP BPDU packets. This is the default setting. ❒ Force STP Compatible - The bridge is using the MSTP parameters, but the ports are sending only STP BPDU packets.

Table 36. MSTP Status (Continued)

Field	Description
Bridge Identifier	Displays the identifier of the switch. The identifier consists of the switch's bridge priority value and MAC address, separated by a slash (/).
Root Bridge	Displays the 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. **Note** The root bridge is zero if MSTP is disabled on the switch. **Note** The root bridge is same as the Bridge Identifier if the switch is the root bridge of the spanning tree domain.
Root Path Cost	Displays the path cost from the switch to the root bridge of the MSTP domain. The root path cost is 0 if the switch is the root bridge of the spanning tree domain or if MSTP is not activated on any of the ports.
Max Age	Displays the maximum length of time the bridges in the spanning tree region retain bridge protocol data units (BPDUs).
Max Hops	Displays the maximum number of hops before BPDUs are deleted. The Max Hop counter in a BPDU is decremented every time a BPDU crosses an MSTP region boundary. After the counter reaches zero, a BPDU is deleted.
Hello Time	Displays the time interval between generating and sending configuration messages by all bridges in the spanning tree domain.
Forward Delay	Displays the amount of time the bridge waits before changing to a new state, such as becoming the new root bridge after a change to the network topology.

Enabling or Disabling MSTP on the Ports

To enable or disable MSTP on the ports, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

    The MSTP status are displayed. See Figure 37 on page 111.

2. Check the checkboxes of the port numbers in the Basic Settings section in the middle of the MSTP page.

    To disable MSTP, uncheck the checkboxes of the port numbers.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Configuring the MSTP Bridge

To configure the MSTP bridge, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

    The MSTP status are displayed. See Figure 37 on page 111.

2. Configure the MSTP bridge on the fields described in Table 37.

Table 37. MSTP Bridge Settings

Field	Description
MST Region Name (ConfigName)	Specify a name for the MST region. The name can be from 0 (zero) to 32 alphanumeric characters in length. The name is case-sensitive. The name must be the same on all of the bridges in a region. Examples of a configuration name include Sales Region and Production Region. The default region name is the MAC address of the switch.
Hello time	Specify the time interval for the bridge between generating and sending configuration messages. The range is 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of a region.

Table 37. MSTP Bridge Settings (Continued)

Field	Description
Max Age Time (MaxAge)	Specify the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs. All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called BPDUs. For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds. Be sure to follow these rules when selecting a value for the maximum age: MaxAge must be greater than (2 x (HelloTime + 1)) MaxAge must be less than (2 x (ForwardingDelay - 1))
Revision (RevisionLevel)	Specify the revision level of an MSTP region. This is an arbitrary number you assign to a region. The revision level must be the same on all of the bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 65535.
Forward Delay Time (ForwardDelay)	Specify the waiting period for a bridge when it changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.
Max Number of Hops (MaxHops)	Specify the maximum number of hops before BPDUs are deleted. The Max Hop counter in a BPDU is decremented every time a BPDU crosses an MSTP region boundary. After the counter reaches zero, a BPDU is deleted.

Table 37. MSTP Bridge Settings (Continued)

Field	Description
MSTP Type (ProtocolVersion)	Specify the bridge to the MSTP or STP-compatible mode. The options are: ❐ MSTP - The bridge operates all of the ports in MSTP, except those ports that receive STP or RSTP BPDU packets. This is the default setting. ❐ STP Compatible mode - The bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. Selecting this option deletes all of the spanning tree instances on the switch

3. Click **Apply**.

   The MSTP bridge is in effect.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying the CIST Priority

The CIST priority value is used to determine the root bridge of the bridged network. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the lowest MAC address becomes the root bridge.

To modify the CIST priority, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

   The MSTP status are displayed. See Figure 37 on page 111.

2. In the CIST/MST instance list at the bottom of the page, click the checkbox of the CIST entry.

3. Click **Edit**.

   The MSTP Instance - Edit window is displayed. See Figure 38 on page 116.
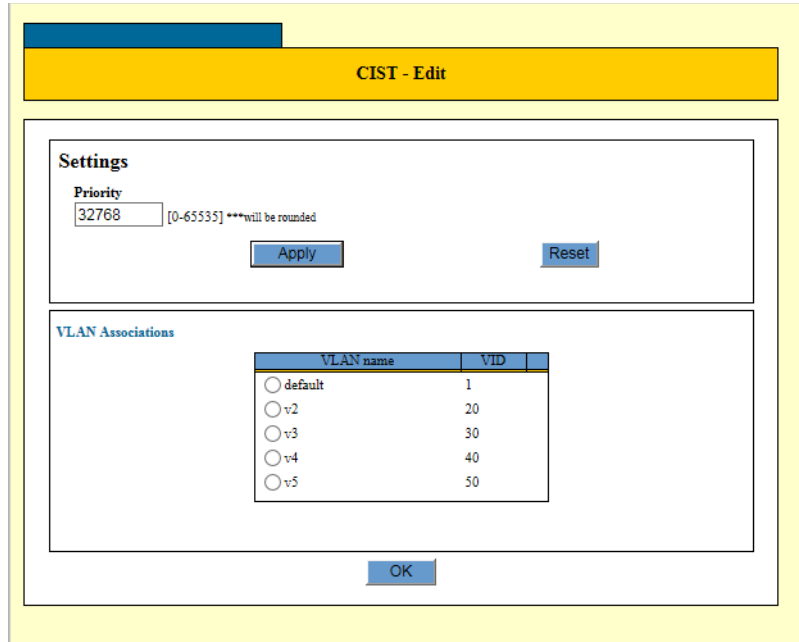
Figure 38. CISP Instance - Edit Window

4. Change the CIST priority in the fields described in Table 38.

Table 38. CIST Instance - Edit

Field	Description
Priority	Specify the CIST priority for the switch. The range is 0 to 65535 in increments of 4096. The default value is 32768. A value that is not an increment of 4096 is automatically rounded down.
VLAN Associations	Displays the VLANs associated to the CIST. VLANs are removed from the CIST when you associate them with MST instances and are returned to the CIST when you remove them from MST instances.

5. Click **Apply**.

6. Click **OK**.

The new CISP priority is in effect.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Configuring MSTP

To configure MSTP, you specify two types of port parameters: MSTI-specific parameters and generic parameters.

The MSTI-specific parameters are set on a per MSTI basis. When a port that is a member of more than one MSTI, each instance can have different parameter values. The MSTI-specific parameters are:

- ❐ Internal path cost
- ❐ Port priority

Generic port parameters are set once on a port and apply to all MSTIs that the port is assigned. The generic parameters are:

- ❐ External path cost
- ❐ Point-to-point port
- ❐ Edge port
- ❐ Port priority

Adding an MST Instance

To add an MST instance, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

   The MSTP status are displayed. See Figure 37 on page 111.

2. In the CIST/MST instance list at the bottom of the page, click **Add**.

   The MST Instance - Add window is displayed. See Figure 39.

Figure 39. MST Instance - Add Window

3. Configure an MST instance in the fields described in Table 39.

Table 39. MST Instance -Add

Field	Description
Priority	Specify the MST priority. The range is 0 to 65535 in increments of 4096. The default value is 32768. A value that is not an increment of 4096 is automatically rounded down.
VLAN Associations	Displays a list of VLANs associated the MST instance. To delete a VLAN, select the radio button of the VLAN and click **Delete**.
VLAN Settings	To associate a VLAN to the MST instance, enter a VLAN name and click **Add**.

4. Click **OK**.

The new MST instance is configured.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying an MST Instance

To edit an MST instance, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

The MSTP status are displayed. See Figure 37 on page 111.

2. In the CIST/MST instance list at the bottom of the page, select an MST instance that you want to modify.

3. Click **Edit**.

The MST Instance - Edit window is displayed. See Figure 40 on page 119.

Figure 40. MST Instance - Edit Window

4. Modify an MST instance in the fields described in Table 39 on page 118.

5. Click **OK**.

   The MST instance is modified.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Displaying MSTP Port Settings

To display the flow groups, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

   The MSTP status are displayed. See Figure 41 on page 120.
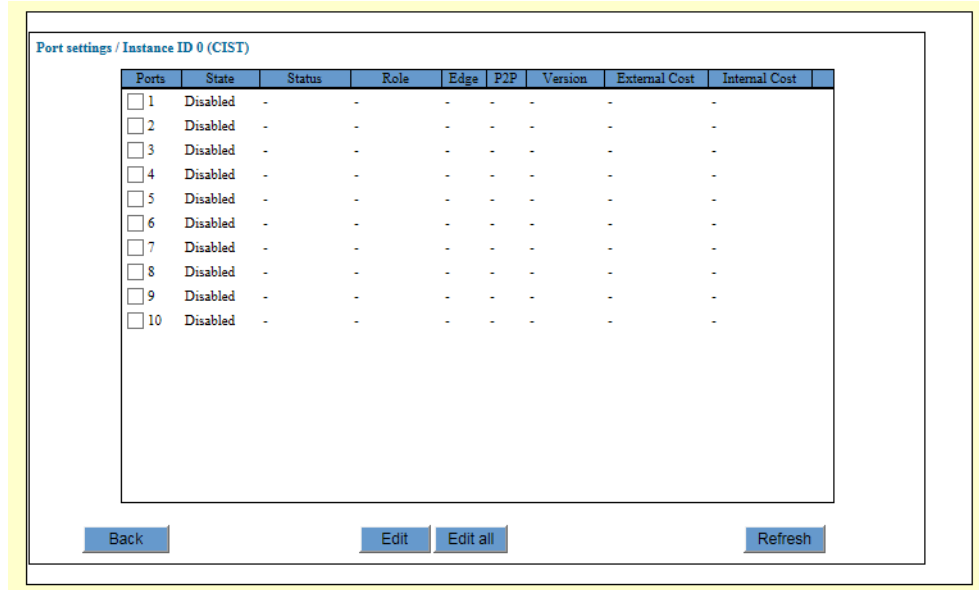
Figure 41. MSTP Port Settings Page

2. Observe the status fields described in Table 40.

Table 40. MSTP Status

Field	Description
Ports	Displays the port number.
State	Displays whether MSTP is enabled or disabled on the port.
Status	Displays the MSTP state of the port. The options are: ❒ Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission. ❒ Learning - The port is enabled for receiving, but not forwarding packets. ❒ Forwarding - Normal operation. ❒ Disabled - The port has not established a link with an end node.

Table 40. MSTP Status (Continued)

Field	Description
Role	Displays the MSTP role of the port. The roles are: ❒ Root - The port that is connected to the root switch, directly or through other switches, with the least path cost. ❒ Alternate - The port offers an alternate path in the direction of the root switch. ❒ Backup - The port on a designated switch that provides a backup for the path provided by the designated port. ❒ Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch. ❒ Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called "master" when the CIST role is "root."
Edge	Displays whether the port is an edge port or not.
P2P	Displays whether the port is a point-to-point port or not.
Version	Displays whether the port is operating in MSTP mode or STP-compatible mode.
External Cost	Displays the external cost of the port.
Internal Cost	Displays the internal cost of the port.

Configuring MSTP

To configure MSTP, specify two types of port parameters: MSTI-specific parameters and generic parameters. When configuring MSTI-specific values, select an appropriate MST instance. When configuring generic port parameters, select the CIST entry.

The MSTI-specific parameters are set on a per MSTI basis. When a port that is a member of more than one MSTI, each instance can have different parameter values. The MSTI-specific parameters are:

❒ Port priority

❒ Internal path cost

Generic port parameters are set once on a port and apply to all MST instances that the port is assigned to. The generic parameters are:

❐ Port priority

❐ External path cost

❐ Point-to-point port

❐ Edge port

To configure MSTP ports, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > MSTP.

   The RSTP status and settings are displayed. See Figure 37 on page 111.

2. In the CIST/MST instance list at the bottom of the page, do one of the following:

   ❐ To configure MSTI-specific parameters for ports, select an MST instance. You may select only one MST instance.

   ❐ To configure the port parameters in CIST, which include the generic port parameters, select the CIST entry in the list.

3. Click **Port Settings**.

   An example of the Port settings page is displayed. See Figure 41 on page 120.

4. Select ports that you want to configure the MST instance or CIST entry.

5. Click **Edit**.

   When selecting an MST instance on step 2, the MST Instance - Port settings window is displayed. See Figure 42.
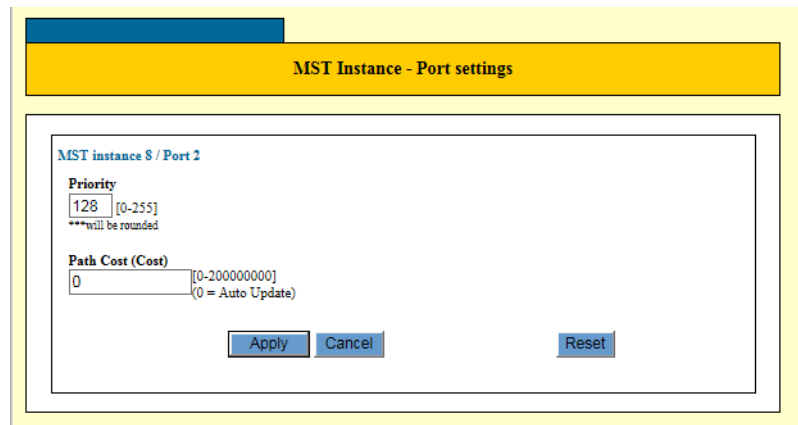
Figure 42. MST Instance - Port Settings Window

When selecting the CIST entry on step 2, the MST Instance - Port settings window is displayed. See Figure 43.

Figure 43. CIST Instance - Port Settings Window

6. Configure the parameters described in the status fields described in Table 41 on page 124.

Table 41. MST/CIST Port Settings

Field	Description
Priority	Specify the priority parameter for a port. The priority is used as a tie breaker when two or more ports have equal costs to the regional root bridge. The range is 0 to 255 in increments of 16. The default value is 128.
External Path Cost	Specify the cost of a port that is connected to a bridge that is a member of another MSTP region or an STP or RSTP domain. The range is 0 to 200,000,000. The value 0 activates the Auto setting, which sets the value according to port speed. Here are the MSTP port costs with the Auto setting when a port is not a member of a trunk. ❑ 10 Mbps - 2,000,000 ❑ 100 Mbps - 200,000 ❑ 1000 Mbps - 20,000 Here are the MSTP port costs with the Auto setting when a port is a member of a trunk. ❑ 10 Mbps - 20,000 ❑ 100 Mbps - 20,000 ❑ 1000 Mbps - 2,000

Table 41. MST/CIST Port Settings (Continued)

Field	Description
Internal Path Cost	Specify the cost of a port that is connected to a bridge that is a member of the same MSTP region. The range is 0 to 200,000,000. The value 0 activates the Auto setting, which sets the value according to port speed. Here are the MSTP port costs with the Auto setting for a port that is not a member of a trunk. ❐ 10 Mbps - 2,000,000 ❐ 100 Mbps - 200,000 ❐ 1000 Mbps - 20,000 Here are the MSTP port costs with the Auto setting for a port that is a member of a trunk. ❐ 10 Mbps - 20,000 ❐ 100 Mbps - 20,000 ❐ 1000 Mbps - 2,000
Point-to-point	Specify whether the port is a point-to-point port. The options are Yes, No, and Auto-Detect.
Edge port (Edge)	Specify whether the port is functioning as an edge port. The options are Yes and No.

7. Click **Apply**.

   The MST/CIST port settings are in effect.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

IGMP Snooping

IGMP Snooping monitors IGMP communications among devices and optimizes multicast traffic. A switch floods multicast traffic to all the ports in a broadcast domain. Flooding multicast traffic can cause a significant amount of traffic to be sent unnecessarily. IGMP Snooping prevents this flooding by maintaining a map of which links need which IP multicast streams.

There are three versions of IGMP: versions 1, 2, and 3. The AT-IA810 switch supports only version 1 and version 2.

One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group.

In version 1 it stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a time-out value, it assumes that the host node no longer wants to receive multicast frames, and removes it from the membership list of the multicast group.

In version 2 a host node exits from a multicast group by sending a leave request. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

The IGMP snooping feature allows the switch to monitor the flow of queries from routers and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups.

Without IGMP snooping a switch would have to flood multicast packets out all of its ports, except the port on which it received the packets. Such flooding of packets can negatively impact network performance.

The switch maintains its list of multicast groups through an adjustable timeout value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Modifying the IGMP Snooping Settings

To change the IGMP Snooping settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > IGMP Snooping.

   The IGMP Snooping settings are displayed. See Figure 44 on page 127.

Figure 44. IGMP Snooping Page

2. Change the fields described in Table 42.

Table 42. IGMP Snooping Settings

Field	Description
Enable IGMP Snooping	Enable or disable IGMP Snooping. By default, IGMP is disabled.
Time out	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. This parameter also controls the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

Table 42. IGMP Snooping Settings (Continued)

Field	Description
Number of Maximum Multicast Groups	Specify the maximum number of IGMP multicast groups the switch can learn. This parameter is useful with networks that contain a large number of multicast groups. The range is 1 to 255 groups. The default is 64 multicast groups.
Router port	Specify the manner by which the switch is to learn the ports where the multicast routers are located. The choices are listed here: ❑ Auto - Enables the switch to automatically identify the router ports. This is the default setting. ❑ None - Sets the mode to manual without any router ports specified. ❑ Select - Manually designate the router ports. If you choose Select, use the list of ports below the Router Port pull-down menu to designate the router ports. A check mark in a checkbox indicates that the port is a router port while an empty check mark indicates that the port is not a router port.

3. Click **Apply**.

   The IGMP Snooping settings are modified.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Displaying an IP Multicast Address List

To display the IGMP Snooping settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > IGMP Snooping.

   The IGMP Snooping settings are displayed. See Figure 44.

2. Observe the fields described in Table 43 on page 129.

Table 43. IP Multicast Address List

Field	Description
IP multicast address	Displays an IP multicast address on the switch.
Router port	Displays the router ports of the multicast address.

Adding an IP Multicast Address

To add an IP multicast address to the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > IGMP Snooping.

   The IGMP Snooping settings are displayed. See Figure 44 on page 127.

2. Click **Add**.

   The IP multicast address - Add window is displayed. See Figure 45.

Figure 45. IP Multicast Address - Add Window

3. Change the fields described in Table 44 on page 130.

Table 44. IP Multicast Address - Add

Field	Description
IP multicast address (MCGroup)	Specify an IP multicast address add to the switch. If you want to enter a range of addresses, enter the lowest address of the range.
Count (Number)	Specify the number of consecutive multicast addresses starting with the IP address that you specified in the IP multicast address field.
Router ports (RouterPort)	Assign the router ports of the new static multicast address.

4. Click **Add**.

5. Click **OK**.

   The new IP multicast address is added to the switch.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying an IP Multicast Address

To change IP Multicast address settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > IGMP Snooping.

   The IGMP Snooping settings are displayed. See Figure 44.

2. In the IP multicast address list, select an IP multicast address.

3. Click **Edit**.

   The IP multicast address - Edit window is displayed.

4. Specify the fields described in Table 44 on page 130.

5. Click **OK**.

   The multicast address is modified.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting an IP Multicast Address

To change the IGMP Snooping settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > IGMP Snooping.

   The IGMP Snooping settings are displayed. See Figure 44 on page 127.

2. In the IP multicast address list, select an IP multicast address.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK**.

   The multicast address is deleted.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Loop Detection Frame

The IA810M switch has the Loop Detection feature that uses Loop Detection Frames to detect loops and apply selected protection mechanisms to limit the adverse effects of any network loop.

A loop exists when a network node can communicate with another node over more than one data path. The problem with wiring loops in Ethernet networks is that they can cause broadcast storms that consume network bandwidth and reduce network performance. The feature can perform several actions if it detects a loop in the wiring topology of a network.

The actions that a port can perform when a loop is detected are:

❑ Port disable

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.

❑ Link down

Disables the port and link to block all traffic. It also enters a message in the event log.

❑ BC discard

Disables 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.

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 Loop Detection Frame Settings on the Ports

To display Loop Detection Frame settings on the ports, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Loop Detection Frame.

   The Loop Detection Frame page is displayed. See Figure 46.

Figure 46. Loop Detection Frame Page

2. Observe the fields. The fields are described in Table 45 on page 134.

Table 45. Loop Detection Frame Port List

Field	Description
Port	Displays the port number and its checkbox.
Loop	Displays whether a loop has been detected on the port. The possible states are: ❏ -- - 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.
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. Here are some guidelines: ❏ 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 enable the port manually, see "Editing Port Parameters" on page 68.

Table 45. Loop Detection Frame Port List (Continued)

Field	Description
Port State	Displays the current state of the port. The possible states are: ❐ 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. To enable the port manually, see "Editing Port Parameters" on page 68.
Link Status	Displays the link state. The possible states are: ❐ 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: ❐ 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.

3. To update the display, click **Refresh**.

Enabling or Disabling Loop Detection Frame

To enable or disable Loop Detection Frame, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Loop Detection Frame.

    The Loop Detection Frame page is displayed. See Figure 46 on page 133.

2. Check the checkbox of the ports that you want to enable Loop Detection Frame on. You can enable Loop Detection Frame on multiple ports at a time.

3. Uncheck the checkbox of the ports that you want to disable Loop Detection Frame on. You can disable Loop Detection Frame on multiple ports at a time.

4. Click **Apply**.

   The Loop Detection Frame is either enabled or disabled.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Configuring Loop Detection Frame on Ports

To configure Loop Detection Frame on the ports, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Loop Detection Frame.

   The Loop Detection Frame page is displayed. See Figure 46 on page 133.

2. Check the checkbox of the ports you want to modify the settings. You can select multiple ports.

3. Click **Edit**.

   Note
   If you want to modify the settings of all the ports, click the Edit all ports button.

   The LDF Port settings page is displayed. See Figure 47 on page 137.

Figure 47. Loop Detection Frame Port Settings Page

4. Configure the parameters as needed. The parameters are described in Table 46.

Table 46. Loop Detection Frame Port Settings

Field	Description
Frame Action (Action)	Specifies the action of the switch if it detects a loop on a port. The options are: ❑ 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. **Note** Do not select LinkDown on the management port. You lose access to the switch when a loop occurs.

Table 46. Loop Detection Frame Port Settings

Field	Description
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: ❑ 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
Traffic class list	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. To enable the port manually, see "Editing Port Parameters" on page 68. **Note** If you select Disable on this field with the PortDisable/LinkDown on the Frame Action, you lose access to the switch when a loop occurs and the access does not resume even after the loop resolves.

5. Click **Apply**.

The Loop Detection Frame is modified on the ports you selected.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Switch Storm Detection

The IA810M switch has the Storm Detection feature that prevents LAN interfaces from being disrupted by a broadcast storm, which potentially swamps the network. You set high and low rate thresholds for the ingress packets for each port and actions for the port to take when 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.

The actions that a port can perform in response to a threshold violation are:

❐ Port disable

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.

❐ Link down

Disables the port and link to block all traffic. It also enters a message in the event log.

❐ BC discard

Disables 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.

Guidelines for Switch Storm Detection

Here are the guidelines for using Switch Storm Detection:

❐ 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, see "Editing Port Parameters" on page 68.

❐ 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 Switch Storm Detection Settings on the Ports

To display Switch Storm Detection settings on the ports, perform the following procedure.

1. From the Navigation pane, go to Switch Settings > Switch Storm Detection.

   The Switch Storm Detection page is displayed. See Figure 48 on page 142.
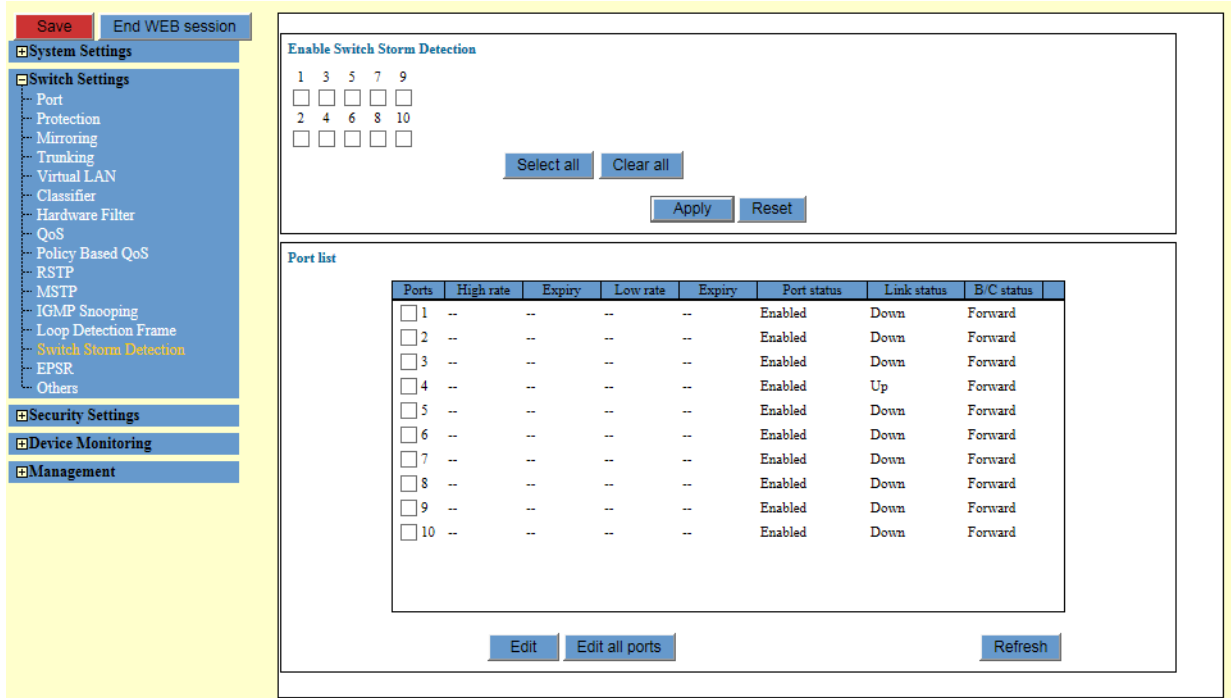
Figure 48. Switch Storm Detection Page

2. Observe the fields. The fields are described in Table 47.

Table 47. Switch Storm Detection Port List

Field	Description
Port	Displays the port number and its checkbox.
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 47. Switch Storm Detection Port List (Continued)

Field	Description
Expiry	Displays the amount of time remaining before the action for the high rate threshold expires. Here are some guidelines: ❒ 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 enable the port manually, see "Editing Port Parameters" on page 68.
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. ❒ 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.

Table 47. Switch Storm Detection Port List (Continued)

Field	Description
Port Status	Displays the current state of the port. The possible states: ❒ Enabled - The port is enabled. **Note** A port with a threshold action of PortDisable, BC Discard, or None has a Port Status of Enabled even when 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. To enable the port manually, see "Editing Port Parameters" on page 68.
Link Status	Displays the link state. The possible states are: ❒ 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. ❒ Down(Act) - The switch has 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. The possible states are: ❒ 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.

3. To update the display, click **Refresh**.

Enabling or Disabling Switch Storm Detection

To enable or disable Switch Storm Detection on each port, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Switch Storm Detection.

2. The Switch Storm Detection page is displayed. See Figure 48 on page 142.

3. Check the checkbox of the ports that you want to enable Switch Storm Detection.

   You can enable Switch Storm Detection on multiple ports at a time.

4. Uncheck the checkbox of the ports that you want to disable Switch Storm Detection.

   You can disable Switch Storm Detection on multiple ports at a time.

5. Click **Apply**.

   The Switch Storm Detection is either enabled or disabled.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Configuring Switch Storm Detection on Ports

To configure Switch Storm Detection on ports, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Switch Storm Detection.

2. The Switch Storm Detection page is displayed. See Figure 48 on page 142.

3. Check the checkbox of the ports you want to modify the settings. You can select multiple ports.

4. Click **Edit**.

   Note
   If you want to modify the settings of all the ports, click the Edit all ports button.

   The Switch Storm Detection - Port Settings page is displayed. See Figure 49 on page 146.
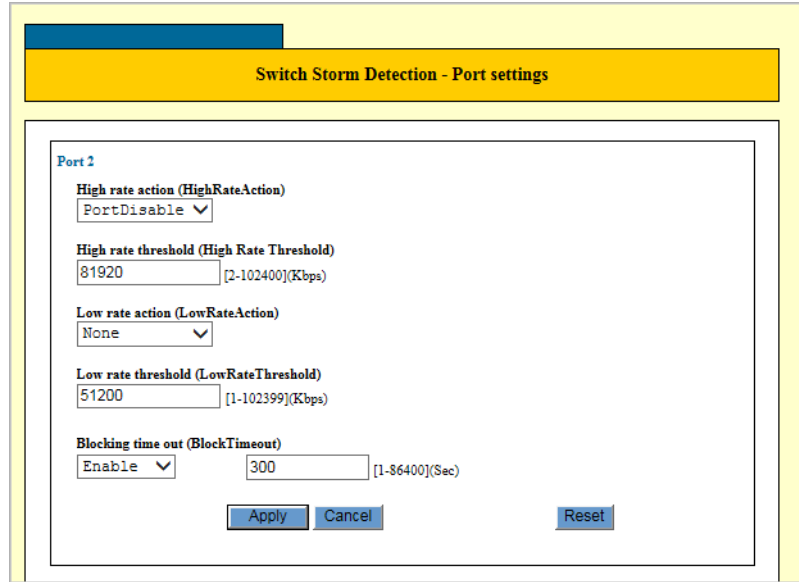
Figure 49. Switch Storm Detection - Port Settings Page

5. Specify the parameters as needed. The parameters are described in Table 48.

Table 48. Switch Storm Detection - Port Settings

Field	Description
High Rate Action (HighRateAction)	Specify the action of a port if the high packet rate threshold is crossed. The options are: ❑ 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)	Specify 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)	Specify the action of a port if the low packet rate threshold is crossed. The actions are the same as for the high rate action. The default setting is None.

Table 48. Switch Storm Detection - Port Settings (Continued)

Field	Description
Low Rate Threshold (LowRateThreshold)	Specify the low packet rate threshold, in kilobits per second. The range is 1 to 1023999 Kbps. The default is 512000 Kbps.
Blocking Time Out (BlockTimeout)	Specify 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. To change a port setting, see "Editing Port Parameters" on page 68.

6. Click **Apply**.

The Switch Storm Detection is configured on the ports you selected.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

EPSR

Ethernet Protection Switching Ring (EPSR) operates on physical rings of switches, not on meshed networks. EPSR prevents a loop in a ring of switches by blocking data transmission across one port.

In EPSR, each ring of switches forms an EPSR domain. One of the domain's switches is the master note and the others are transit nodes. Each node connects to the ring via tow ports.

One or more data VLANs sends data around the ring, and a control VLAN sends EPSR messages. A physical ring can have more than one EPSR domain, but each domain operates as a separate logical group of VLANs and has its own control VLAN and master node. On the master node, one port is the primary port and the other is the secondary port. When all the nodes in the ring are up, EPSR prevents loops by blocking the date VLAN on the secondary port.

Displaying EPSR Domain List

To display a list of EPSR domains, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > EPSR.

   The EPSR Domain list is displayed. See.Figure 50.
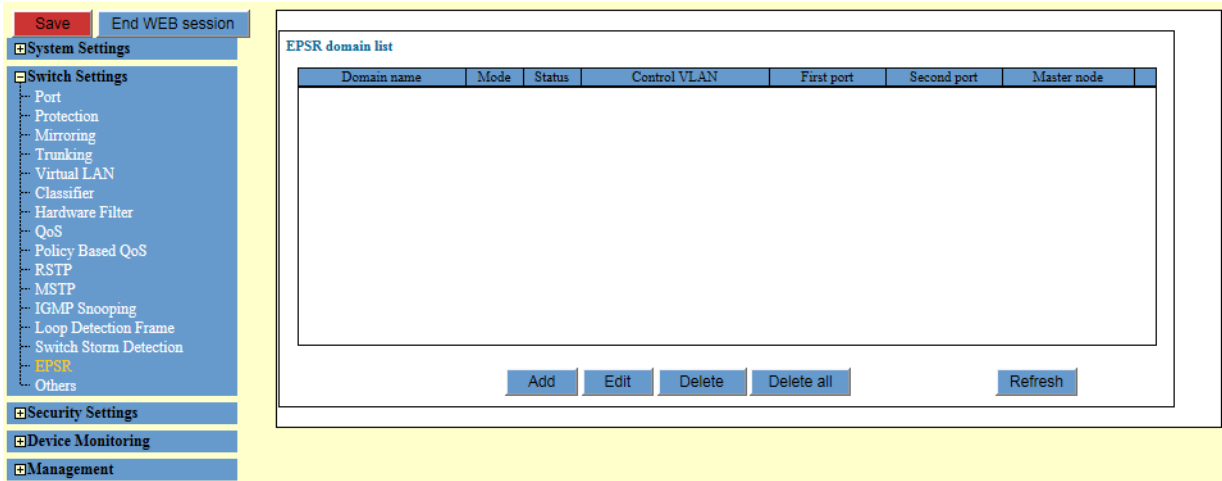
Figure 50. EPSR Domain List

2. Observe the fields described in Table 49 on page 149.

Table 49. EPSR Domain List

Field	Description
Domain Name	Displays the name of the domain.
Mode	Displays the mode of the domain. The option is only Aware.
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.
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 create an EPSR domain, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > EPSR.

    The EPSR Domain list is displayed in Figure 50 on page 148.

2. Click **Add** on the page.

    The EPSR Domain - Add page appears. See Figure 51 on page 150.

Figure 51. EPSR Domain - Add Page

3.   Specify the parameters as described in Table 50.

Table 50. EPSR Domain - Add

Field	Description
Enable This Domain	Enable or disable the domain. To enable the domain, check the checkbox. To disable the domain, uncheck the checkbox.
EPSR Domain Name (EpsrDomainName)	Specify the EPSR domain name. The name can be up to 15 characters. Spaces are not allowed.
Mode	Specify the EPSR mode of the domain. The option is only Aware.

Table 50. EPSR Domain - Add (Continued)

Field	Description
Delete Multicast Address (DeleteMcast)	Enable or disable controlling the deletion of multicast addresses from the MAC address table. The options are: ❒ Enabled - The switch deletes dynamic IPv4 multicast addresses learned by IGMP snooping from the MAC address table. The switch does not delete static multicast addresses. ❒ Disabled - The switch does not delete IPv4 multicast addresses.
Control VLAN (ControlVlan)	Specify the name or VID of the control VLAN. You may specify only one VLAN.

4. Click **Apply**.

   The EPSR domain is created.

5. Click the Data VLAN field and enter the name or VID of the data VLAN of the EPSR instance.

6. Click **Add**.

   The data VLAN of the EPSR instance is added.

7. Repeat steps 5 and 6 to add more data VLANs to the domain, as needed.

8. Click **OK**.

   Additional data VLANs are added to the domain.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying an EPSR Domain

To modify an EPSR domain, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > EPSR.

   The EPSR Domain list is displayed in Figure 50 on page 148.

2. Select an EPSR domain that you want to modify its settings. You can select multiple ports.

3. Click **Edit**.

   The EPSR Domain - Edit page appears.

4. Change the fields as needed. The Fields are described in Table 50 on page 150.

5. Click **Apply**.

   The EPSR domain is modified with the changes you selected.

Adding Data VLANs

To add data VLANs to the domain, perform the following procedure:

1. 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.

2. Click **Add**.

   The data VLAN is added to the domain.

3. Repeat steps 1 and 2 to add more data VLANs as needed.

Deleting Data VLANs

To delete data VLANs from the domain, perform the following procedure:

1. In the Data VLAN list section, check the checkbox of the data VLAN you want to delete.

2. Click **Delete**.

   The data VLAN is deleted from the domain.

   > **Note**
   > To delete all the data VLANs of the domain, click the Delete All button.

Completing the EPSR Domain Modifications

To implement adding VLANs to the EPSR domain or/and deleting VLANs from the EPSR domain:

1. Click **OK**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting an EPSR Domain

To delete an EPSR Domain, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > EPSR.

   The EPSR Domain list is displayed in Figure 50 on page 148.

2. Check the checkbox of the EPSR that you want to delete.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK**.

   The EPSR domain is deleted.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Aging Timer for Forwarding Database, BPDU Transparency, and EAP Transparency

From the Other page in the Switch Settings section, you can enable or disable Aging Timer, BPDU transparency, and EAP transparency.

Enabling Aging Timer for Forwarding Database

To enable the aging timer for the Forwarding database and adjust the timer, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Others.

   The Others page is displayed. See Figure 52.
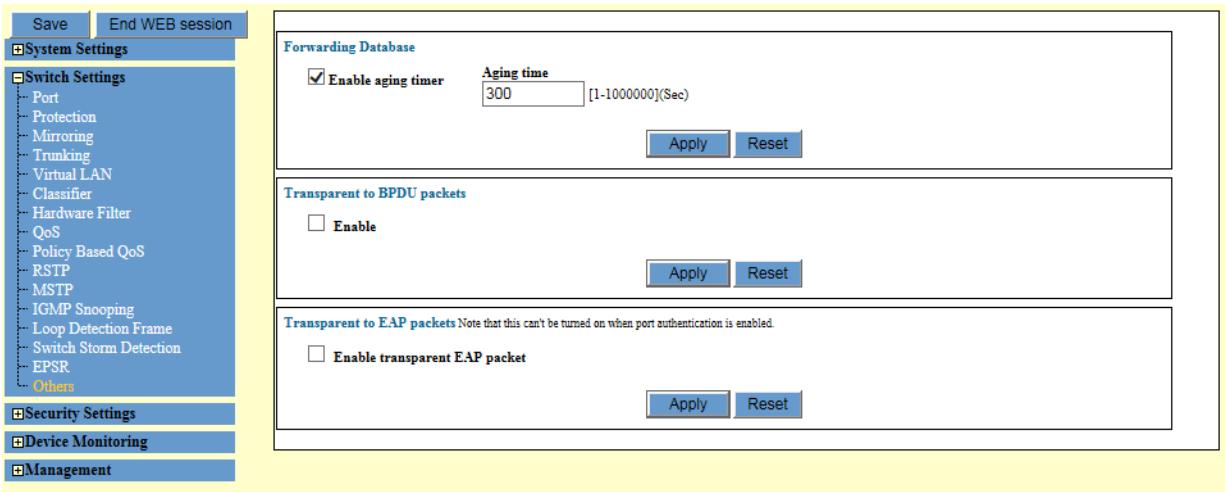
Figure 52. Others page

2. Configure the aging timer for the Forwarding database in the fields described in Table 51.

Table 51. Forwarding Database

Field	Description
Enable aging timer	Enable or disable the aging timer for the forwarding database.
Aging time	Adjust the aging timer. The range is 1 to 1,000,000 seconds. The default value is 300 seconds.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Enabling BPDU Transparency

You can specify the switch to forward BPDU packets even when RSTP is disabled. Network devices with STP enabled use BPDUs to transmit STP-related information to each other. By default, the switch discards all BPDU packets when RSTP is disabled.

To enable BPDU transparency, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Others.

   The Others page is displayed. See Figure 52 on page 154.

2. Enable the Transparent to BPDU packets.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Enabling EAP Transparency

You can specify the switch to forward the EAP packets if the default setting is disabled.

To enable EAP transparency, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Others.

   The Others page is displayed. See Figure 52 on page 154.

2. Enable the Transparent to EAP packets.

3. Click **Apply**.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Chapter 4
Quality of Service

This chapter includes the following topics:

Quality of Service (QoS) Overview

QoS is a set of techniques or mechanisms for managing network resources to ensure high-quality performance for critical applications. Traditionally, the concept of quality in networks meant that all network was treated equally. The concept of QoS is based on the idea that requirements of some applications and users are more critical than others, which means that some traffic needs to be put a high priority.

The switch uses QoS policies to control QoS service delivery. A QoS policy consists of a collection of user defined traffic. According to QoS policies, the switch sorts packets into various traffic and allocates resources to direct these traffic according to bandwidth or priority settings in the policy. The policy contains traffic classes, flow groups, and classifiers.

QoS Policy Configuration

To configure a QoS policy, you must:

❏ Create *classifiers* to sort packets into traffic flows. To configure classifiers, see "Classifier" on page 168.

❏ Create *flow groups* and add classifiers to them. Flow groups are groups of classifiers, which group together similar traffic flows. You can apply QoS traffic prioritization to flow groups. To configure flow groups, see "Flow Groups" on page 182.

❏ Create *traffic classes*, add flow groups to them, and apply the maximum and guaranteed bandwidth for the matching traffic. To configure traffic classes. see "Traffic Classes" on page 187.

❏ Create QoS *policies*, add traffic classes and associate ports to them. Policies are groups of traffic classes. The QoS policy defines a QoS solution for a port or group of ports.

QoS Policy Guidelines

Here is a list of QoS policy guidelines:

❏ A classifier may be assigned to many flow groups; however, assigning a classifier more than one within the same policy may lead to undesirable results. A classifier may be used successfully in many different policies.

❏ A flow group may have multiple classifiers, but must be assigned at least one classifier.

❏ A flow group may be assigned to only one traffic class.

❏ A traffic class may have many flow groups.

❏ A traffic class may be assigned to only one policy.

❏ A QoS policy may have multiple traffic classes.

❏ A QoS policy may have only one policy.

□   A QoS policy that is associated to any port is inactive.

□   A QoS policy must have at least one action defined in the flow group, traffic class, or policy itself. A QoS policy without an action is invalid.

□   The switch can store up to 64 flow groups.

□   The switch can store up to 64 traffic classes.

□   The switch can store up to 64 QoS policies.

Attaching the String to the QoS Policy in the Port

After assigning traffic class to the QoS policy, attach the string to QoS policy in the port. (The Flooding packet cannot use policy map's filter.)

classifier--->flow group--->traffic class---> QoS policy--> switch port

1. Create a QoS policy

2. Create the traffic class: Traffic class is assigned to the QoS policy.

3. Create flow group: Flow group is assigned to the traffic class.

4. Create the classifier: Classifier is assigned to the flow group.

5. Assign the QoS policy to the switch port.

IEEE 802.1p Priority Levels and Egress Priority Queues

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

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

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

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

CoS applies mainly to tagged packets because, in addition to carrying VLAN information, these packets can also contain a priority level that

indicates how important (delay sensitive) a packet is in comparison to other packets. The switch refers to this number when determining a packet's priority level.

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

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

When a tagged packet arrives on a port, the switch examines its priority value to determine which egress priority queue the packet should be directed to on the egress port. Table 52 on page 219 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Note
QOS mappings are applied at the switch level (DSCP, cos, weight, scheduling)

Table 52. 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 53.

Table 53. 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
6	Q3
7	Q3

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.

Note
The QoS function does not work for these type of packets:
1. DVMRP packet (IGMP Snooping enabled)
2. VSRP packet (STP/MSTP or EPSR, aware enabled)
3. LDF sent from other equipment (A LDF detection function in QoS)

From the QoS basic settings page, you can configure QoS basics; enabling or disabling QoS on the switch, setting the packet queue scheduling, queue weight, queue priority, and user priority on each port.

Note

To make the new QoS configuration effective, when you change the QoS configuration, reboot the switch.

Displaying QoS Basic Settings

To display basic QoS settings, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > QoS.

   The QoS basic settings page is displayed. See Figure 53.
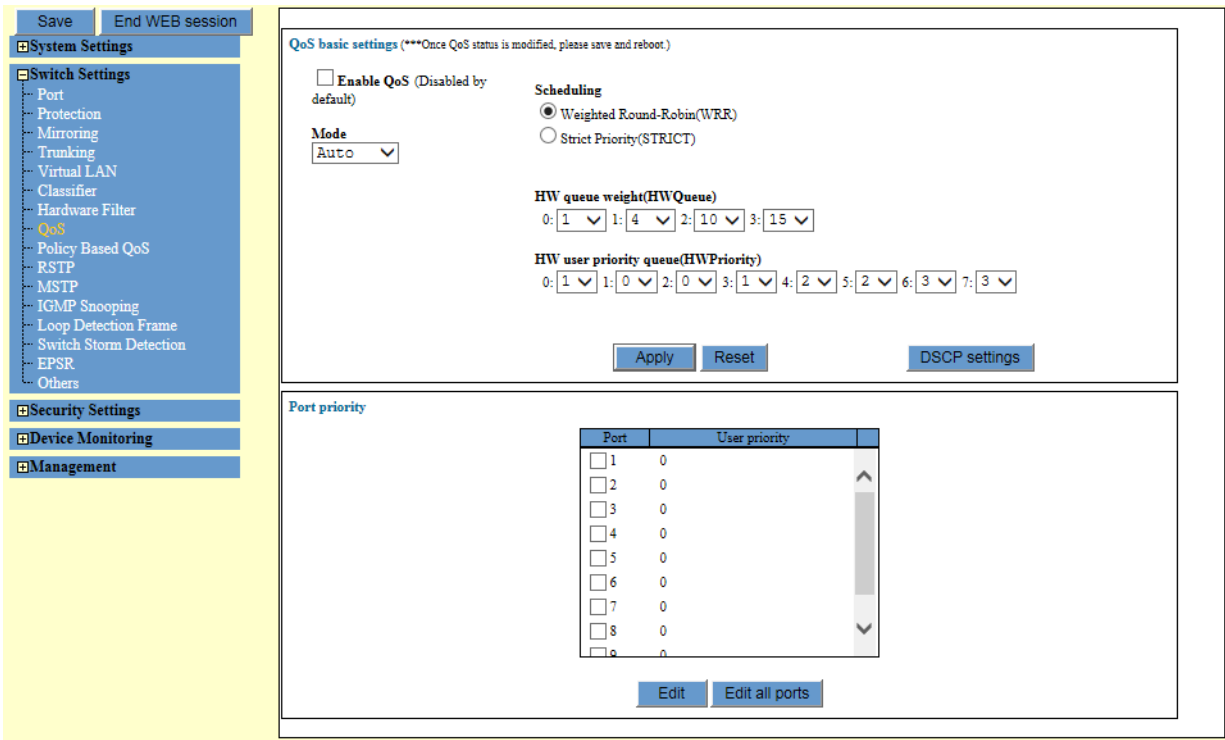
Figure 53. QoS Basic Settings Page

2. Observe the fields described in Table 54 on page 163. The page displays the current settings of the QoS.

Table 54. QoS Basic Settings

Field	Description
QoS basic settings	
Enable QoS	Enable or disable QoS on the switch.
Mode	Displays the manner in which packets are prioritized. The options are: ❐ Auto - Packet priority is based on the DSCP value, IEEE802.1p priority tab, and port priority, in that order. ❐ 802.1p - Packet priority is based only on the IEEE802.1p priority tag.
Scheduling	Displays packet queue scheduling. The schedule controls the order in which ports transmit packets from their egress packet queues. The options are: ❐ Weighted Round-Robin - A port transmits a set number of packets from each queue in a round robin fashion. Each queue has a chance to transmit traffic. ❐ Strict priority (STRICT) - A port transmits all of the packets out of the higher priority queues before transmitting the packets in the lower priority queues. High priority packets are always handled before low priority packets.
HW queue weight (HW Queue)	Displays the maximum number of packets that the switch is to transmit from the egress queues on a port before moving to the next queue. These values are applied only when you select the weighted round robin in scheduling. The default queue weight for each queue are: ❐ Q0 (lowest) - 1 packet ❐ Q1 - 4 packets ❐ Q2 - 10 packets ❐ Q3 - 15 packets

Table 54. QoS Basic Settings (Continued)

Field	Description
HW user priority queue (HW Priority)	Displays the mappings of CoS priority values to egress packet queues. Class of Service (CoS) applies to tagged packets because these packets with VLAN information contain a priority level that indicates how important (delay sensitive) a packet is in comparison to other packets. The switch refers to this number determining a packet's priority level. The default IEEE802.1p priority level to port priority queues are: ❏ Priority level 0 - Port Queue Q1 ❏ Priority level 1 - Port Queue Q0 (lowest) ❏ Priority level 2 - Port Queue Q0 ❏ Priority level 3 - Port Queue Q1 ❏ Priority level 4 - Port Queue Q2 ❏ Priority level 5 - Port Queue Q3 ❏ Priority level 6 - Port Queue Q3 ❏ Priority level 7 - Port Queue Q3 (highest) By default, all untagged packets are assigned to a priority of 0 and are placed in a port's Q2 egress queue. **Note** Queue Q3 is the highest priority. You must set the weight of Queue Q3 (price:1-15) as the biggest value. (The same value of weight can be set.) **Note** Mappings are applied at the switch level. They cannot be set on a per-port basis.
Port Priority	
Port	Displays the port number and its radio button to select.

Table 54. QoS Basic Settings (Continued)

Field	Description
User priority	Displays the CoS priority value for the ports. The priority values determine which hardware queues store ingress untagged packets.

Setting the Priority Values for DSCP Packets

To modify the mapping of Differentiated Services Code Point (DSCP) values to queues, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > QoS.

   The QoS basic setting page is displayed. See Figure 53 on page 162.

2. Click **DSCP settings**.

   The DSCP Settings page appears. See Figure 54.

Figure 54. QoS - DSCP Settings Window

3. Click the checkbox of the DSCP number whose association to a queue you want to change.

   You can change more than one DSCP value at a time.

4. Click **Edit**.

   Another QoS DSCP Settings page appears. See Figure 55 on page 166.
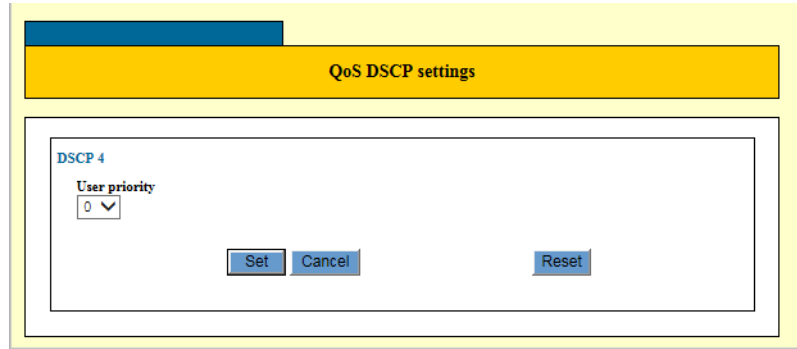
Figure 55. QoS DSCP Settings Window

Note
To change priorities of all DSCP values at a time, click **Edit all DSCP values**.

5. Select the new user priority for the selected DSCP value.

6. Click **Set**.

7. Reboot the switch when you complete changes on QoS. To reboot the switch, see "Reboot" on page 254.

Note
To make the new QoS configuration effective, reboot the switch.

Setting the Priority for Untagged Packets on a Port

You can set a user priority for untagged packets on a port.

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

1. From the Navigation pane, go to Switch Settings > QoS.

   The QoS basic setting page is displayed. See Figure 53 on page 162.

2. In the Port Priority section, click the checkbox of the port whose user priority value you want to change.

   Note
   You can configure more than one port at a time.

3. Click **Edit**.

   The QoS - Port Settings page appears. See Figure 56.
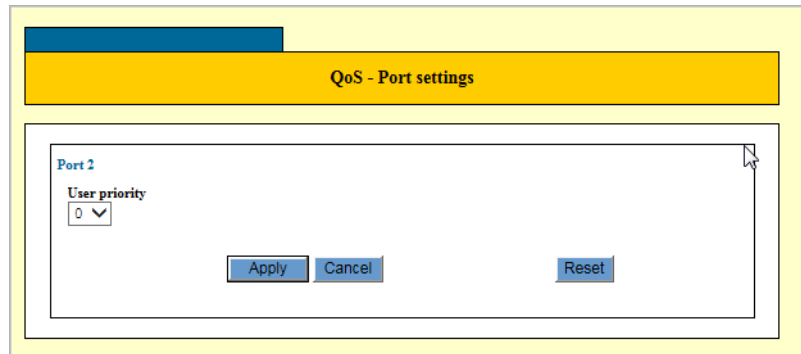
Figure 56. QoS - Port Settings Window

4. Select the new user priority for the selected ports.

   The new priority level applies to all ingress untagged packets on the specified port.

5. Click **Apply**.

   The new user priority for the selected ports that you have entered is in effect.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

6. Reboot the switch when you complete changes on QoS. To reboot the switch, see "Reboot" on page 254.

   > **Note**
   > To make the new QoS configuration effective, reboot the switch.

Classifier

A classifier is an object type that identifies a particular type of traffic. After creating a classifier, assign it to QoS policies or hardware filters to regulate the various traffic flows that pass through the switch.

To assign a classifier to a QoS policy, see "Quality of Service (QoS) Overview" on page 158. To assign a classifier to a hardware filter, see "Hardware Filter" on page 177.

Classifier Guidelines

Here are the guidelines for classifiers:

- ❑ Each classifier represents a separate traffic flow.

- ❑ The variables within a classifier are linked by AND. The more variables you define within a classifier, the more specific it becomes in terms of the flow it defines. For instance, specifying both a source IP address and a TCP destination port within the same classifier defines a traffic flow that relates to IP packets containing both the designated source IP address and the TCP destination port. There are, however, some restrictions on combining variables in the same classifier. For the restrictions, refer to "Classifier Criteria" on page 235.

- ❑ You can apply the same classifier to more than one QoS policy.

- ❑ A classifier without any defined variables applies to all packets.

- ❑ You cannot create two classifiers that have the same settings. There can be only one classifier for any given type of traffic flow.

- ❑ A classifier can have a maximum of eight defined criteria, not including the classifier ID number and description.

- ❑ The switch can store up to 256 classifiers. However, the maximum number of classifiers you can assign to active QoS policies at any one time will be from 14 to 127. The number depends on several factors, such as the number of ports to which the classifiers are assigned and the types of criteria defined in the classifiers.

- ❑ You cannot modify a classifier if it belongs to a QoS policy that is assigned to a port. You must remove the port assignments from the policy and reassign them after modifying the classifier.

- ❑ You cannot delete a classifier that is assigned to a QoS policy. You have to remove a classifier from all of its QoS policy assignments before you can delete it.

Displaying Classifiers

To display classifiers defined on the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Classifier.

   The Classifier list page is displayed. See Figure 57.
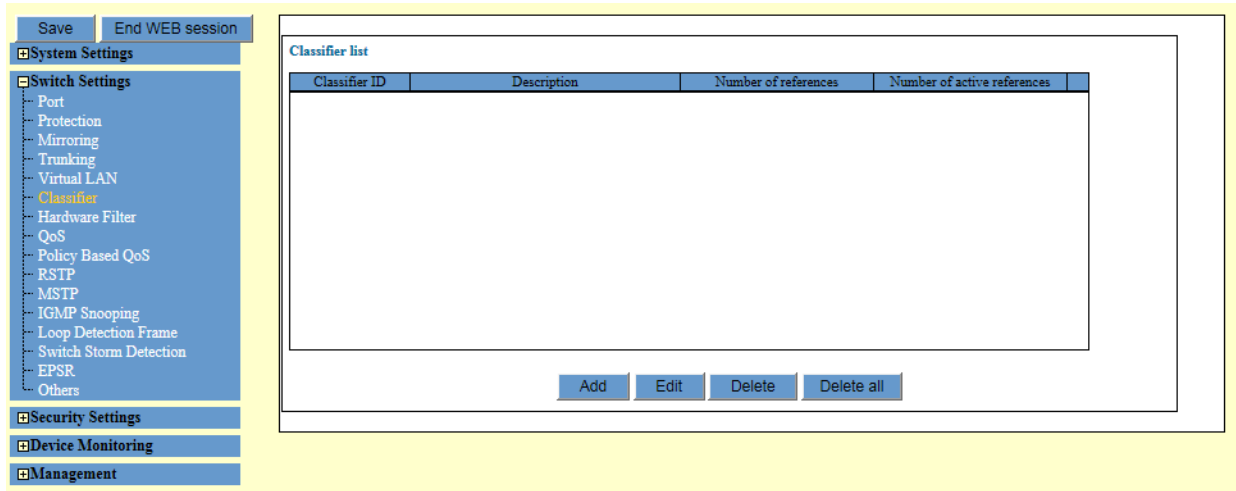
Figure 57. Classifier List Page

2. Observed the fields described in Table 55.

Table 55. Classifier

Field	Description
Classifier ID	Displays the ID number of a classifier.
Description	Displays the description of a classifier.
Number of references	Displays the number of QoS policies to which the classifier is currently assigned. If this field is 0, the classifier is not assigned to any policies.
Number of active references	Displays the number of active QoS policies to which the classifier is currently assigned. A QoS policy is active if it is assigned to at least one port, and inactive if it is not assigned to any ports.

Creating a Classifier

To create a new classifier, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Classifier.

   The Classifier page is displayed. See Figure 57 on page 169.

2. Click **Add**.

The Classifier - Add page appears. See Figure 58.

Figure 58. Classifier - Add Page

3. Configure the parameters as described in Table 56 on page 170.

Table 56. Classifier Settings

Field	Description
Classifier ID	Specify an ID number for a new classifier. Each classifier on the switch must have a unique ID number. The range is 1 to 9999.
Description	Specify a description for a new classifier. A description can be up to 31 alphanumeric characters. Spaces are allowed.
Destination MAC Address	Specify a traffic flow by its destination MAC address.

Table 56. Classifier Settings (Continued)

Field	Description
Destination MAC Address Mask	Specify a mask for the destination MAC address. The mask is used to define the destination MAC address as referring to a single node or a range of nodes with consecutive MAC addresses. The values in the mask can be either of the following: ❒ F - Indicates the parts of the destination MAC address the switch should filter on. ❒ 0 (zero) - Indicates the parts of the destination MAC address the switch should ignore.
Source MAC Address	Specify a traffic flow by its source MAC address.
Source MAC Address Mask	Specify a mask for the source MAC address. The mask is used to define the source MAC address as referring to a single node or a range of nodes with consecutive MAC addresses. The values in the mask can be either of the following: ❒ F - Indicates the parts of the destination MAC address the switch should filter on. ❒ 0 (zero) - Indicates the parts of the destination MAC address the switch should ignore.
Frame Format	Specify a traffic flow by its Ethernet format. The options are: ❒ Any - Specifies all Ethernet format types. This is the default value. ❒ ETHII-Untagged - Specifies Ethernet II untagged packets. ❒ ETHII-Tagged - Specifies Ethernet II tagged packets. ❒ 802.2-Untagged - Specifies Ethernet 802.2 untagged packets. ❒ 802.2-Tagged - Specifies Ethernet 802.2 tagged packets.

Table 56. Classifier Settings (Continued)

Field	Description
User Priority	Specify a traffic flow by the user priority level in tagged Ethernet frames. The range is 0 to 7.
Protocol Field	Specify a traffic flow by the protocol specified in the Ethertype field of the MAC header in an Ethernet II frame. The options are: ❏ IP ❏ ARP ❏ RARP ❏ Others - Enter the protocol number in the Ethertype field of the MAC header in Ethernet II frames. Enter the number in decimal or hexadecimal format. The decimal range is 1536 to 65535. The hexadecimal range is 0x600 to 0xFFFF.
Virtual LAN	Specify a traffic flow of tagged packets by the VLAN ID number. Specify the VLAN by its name or VID. The VID range is 1 to 4094. Only one VLAN is allowed.
TOS Field	Specify a traffic flow by the Type of Service value. The range is 0 to 7.
DSCP Field Value	Specify a traffic flow by the DSCP (DiffServ Code Point) value. The range is 0 to 63.
IP Protocol Field	Specify a traffic flow by the IP Layer 3 protocol. The options are: ❏ TCP ❏ UDP ❏ ICMP ❏ IGMP ❏ Others - Enter an IP Layer 3 protocol number in the field next to the pull-down menu. The number must be entered in hexadecimal format. The number must be preceded by "0x". The range is 0x00 to 0xFF.

Table 56. Classifier Settings (Continued)

Field	Description
Source IP Address	Specify a traffic flow by a source IP address. The address can be for a specific node or subnet.
Source IP Address Mask	Specify a mask for the source IP address. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask "255.255.255.0".
Destination IP Address	Specify a traffic flow by a destination IP address. The address can be for a specific node or subnet.
Destination IP Address Mask	Specify a mask for the destination IP address. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. For example, the subnet address 149.11.11.0 would have the mask "255.255.255.0".
TCP Source Port	Specify a traffic flow by a source TCP port. This field requires that the IP Protocol Field be set to TCP.
TCP Destination Port	Specify a traffic flow by a destination TCP port. This field requires that the IP Protocol Field be set to TCP.
UDP Source Port	Specify a traffic flow by a source UDP port. This field requires that the IP Protocol Field be set to UDP.
UDP Destination Port	Specify a traffic flow by a destination UDP port. This field requires that the IP Protocol Field be set to UDP.

Table 56. Classifier Settings (Continued)

Field	Description
TCP Flags	Specify a traffic flow by a TCP flag. This field requires that the IP Protocol Field be set to TCP. The options are: ❒ URG - Urgent ❒ ACK - Acknowledgment ❒ PSH - Push ❒ RST - Reset ❒ SYN - Synchronization ❒ FIN - Finish

4. Click **Apply**.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a Classifier

To modify an existing classifier, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Classifier.

   The Classifier list page is displayed. See Figure 57 on page 169.

2. Select a classifier that you want to modify the settings.

3. Click **Edit**.

   The Classifier - Edit page appears. See Figure 59 on page 175.

Figure 59. Classifier - Edit Page

4. Change the fields. They are described in Table 56 on page 170.

5. Click **Apply**.

   The changes that you have entered are in effect.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

   > **Note**
   > If the value is 0, you may continue with the next step to delete the classifier. If the value is 1 or more, do not continue. The classifier is assigned to one or more QoS policies. You have to remove the classifier from the policies before you can delete it.

Deleting a Classifier

To delete a existing classifier, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Classifier.

The Classifier list page is displayed. See Figure 57 on page 169.

2. Select the classifier that you want to delete.

3. Click **Delete**.

    A confirmation page appears.

4. Click **OK** to confirm.

    Note
    To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Hardware Filter

Hardware Filter is a hardware-based packet-filtering feature. It is also called Access Control List (ACL). Because hardware filters are hardware-based, they put no load on the CPU of the switch and have no affect on the throughput of the switch.

A hardware filter consists of classifiers, an action, and ports that the hardware filter is applied to. The switch compares a packet with every hardware filter before it compares the packet with any QoS flow group. If the packet matches a hardware filter, the switch takes the action specified by that hardware filter and skips the rest of the comparison process.

If a packet matches both a hardware filter and a QoS flow group, the packet only gets matched against the hardware filter. It bypasses the QoS process. For this reason, Allied Telesis only recommends combining hardware filters and QoS if all your hardware filters result in traffic being dropped.

Displaying Hardware Filters

To display hardware filters defined on the switch, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Hardware Filter.

   The Entry list page is displayed. See Figure 60.
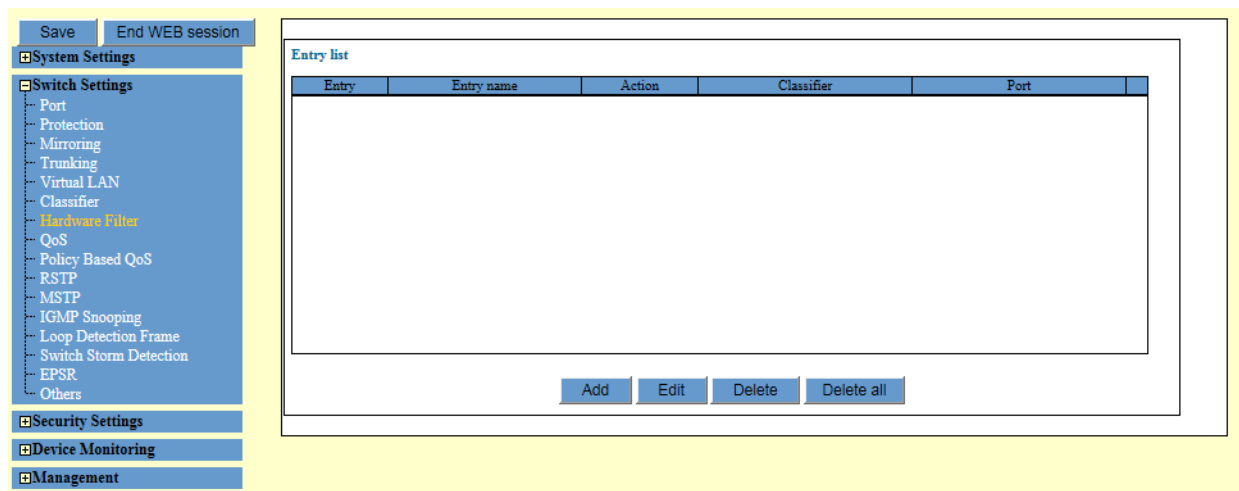
Figure 60. Hardware Filter Entry List Page

2. Observe the fields described in Table 57 on page 178.

Table 57. Hardware List Entry

Field	Description
Entry	Displays the entry number of a hardware filter.
Entry name	Displays the name of the hardware filter.
Action	Displays the assigned action that the switch takes when a packet matches the hardware filter.
Classifier	Displays a list of classifiers assigned to the hardware filter.
Port	Display a list of ports that the hardware filter is applied to.

Creating a Hardware Filter

To create a hardware filter, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Hardware Filter.

   The Entry list page is displayed. See Figure 60 on page 177.

2. Click **Add**.

   The Hardware Filter - Add page appears. See Figure 61.
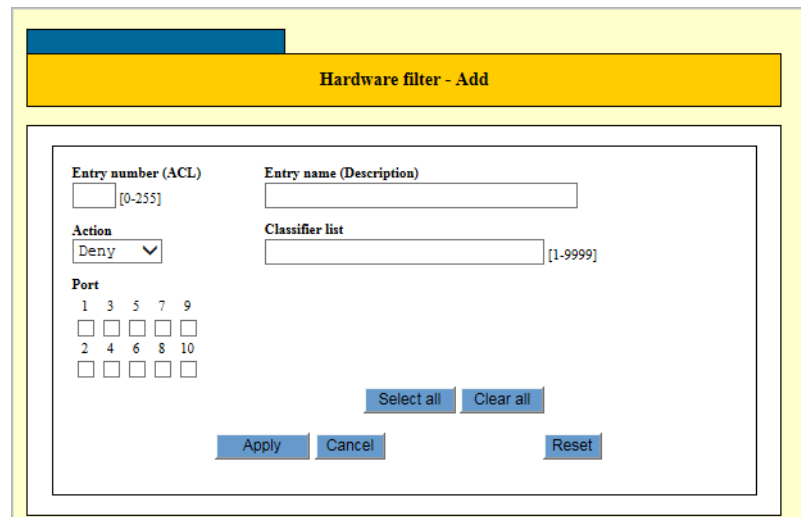
Figure 61. Hardware Filter- Add Page

3. Configure the parameters as described in Table 56 on page 170.

Table 58. Hardware Filter

Field	Description
Entry number (ACL)	Specify a number for the new hardware filter, or Access Control List (ACL). The range is 0 to 255.
Entry Name (Description)	Description for entry (length: 1~31 characters, empty:no error).
Action	Select an action that the switch takes when a packet matches the hardware filter. The options are: ❏ Deny - Discards the packet. ❏ Permit - Allows the packet.
Classifier List	Applied ACL for entry (ID=1 to 9999). Maximum length is 128 characters, multiple classifier or empty:no error.
Port	1. When you assign Action="deny" to management VLAN in hardware filter, you fail in control of DUT. 2. When you want to change a used classifier, you must release the hardware filter that is assigned to the port. 3. When you want to delete a used classifier, you must release the hardware classifier that is assigned to the hardware filter.

4. Click **Apply**.

The configuration that you have entered is in effect.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a Hardware Filter

To modify an existing hardware filter, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Hardware Filter.

   The Hardware Filter Entry list page is displayed. See Figure 60 on page 177.

2. Select a hardware filter that you want to modify the settings.

3. Click **Edit**.

    The Hardware Filter - Edit page appears. See Figure 62 on page 180.

Figure 62. Hardware Filter- Edit Page

4. Change the fields. They are described in Table 57 on page 178.

5. Click **Apply**.

    The modifications that you have entered are in effect.

    Note
    To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting a Hardware Filter

To delete a existing hardware filter, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Hardware Filter.

    The Entry list page is displayed. See Figure 60 on page 177.

2. Select the hardware filter that you want to delete.

3. Click **Delete**.

    A confirmation page appears.

4. Click **OK** to confirm.

    The hardware filter is deleted.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Flow Groups

A flow group groups similar traffic flow together and specify more specific QoS controls. A flow group consists of a set of QoS parameters and a group of classifiers.

Displaying Flow Groups

To display the flow groups, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

    The flow group list is displayed in the bottom section of the page as shown in Figure 63.
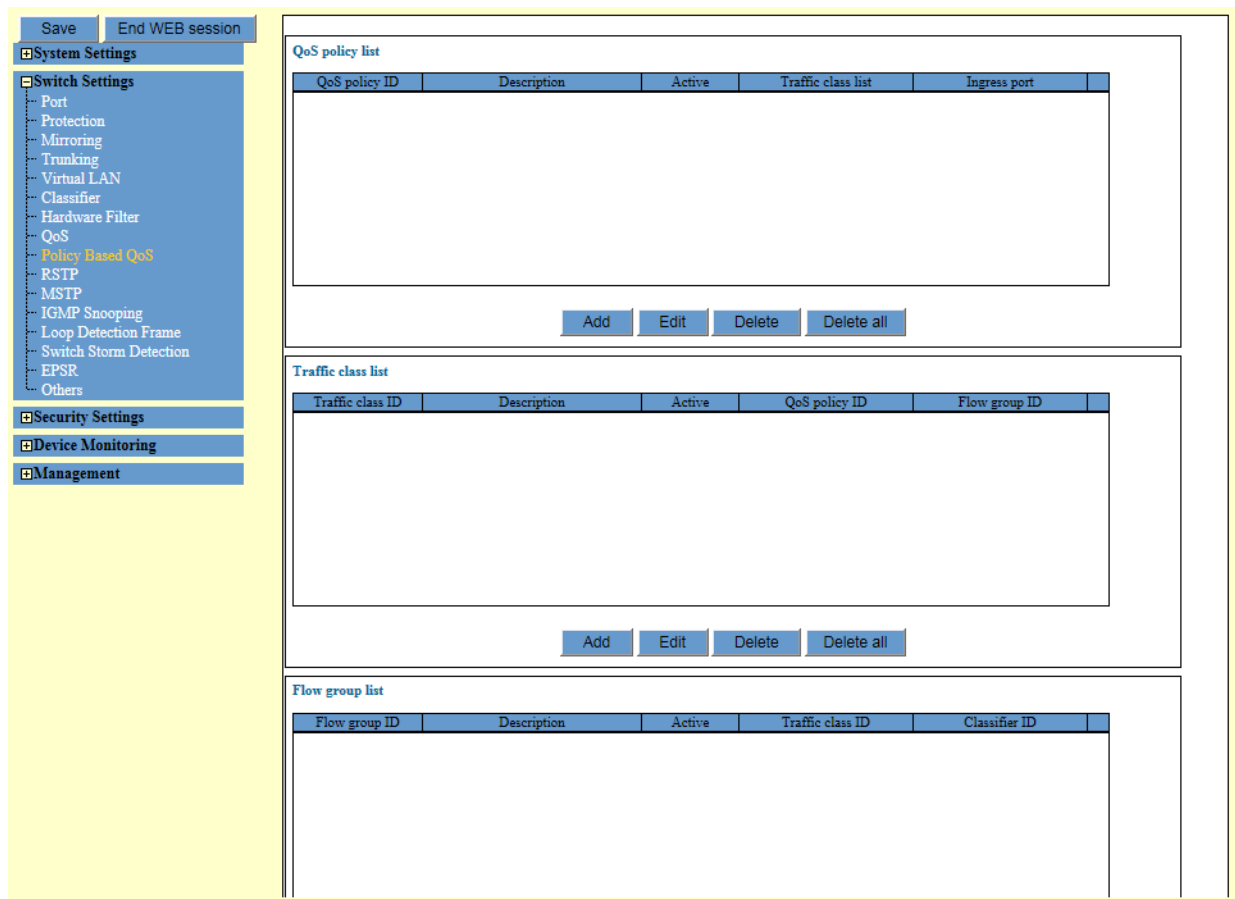
Figure 63. QoS Policy, Traffic Class, and Flow Group Lists Page

2. Observe the fields described in Table 61 on page 196.

Adding a Flow Group

To create a new flow group, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Flow Group list is displayed in the bottom section. See Figure 63 on page 182.

2. Click **Add** in the Flow Group List section of the page.

   The Flow Group - Add page appears. See Figure 64.

Figure 64. Flow Group - Add Page

3. Specify the parameters as described in Table 59.

Table 59. Flow Group - Add

Field	Description
Flow Group ID	Specify an ID number to a flow group. Each flow group on the switch must have a unique ID number. The range is from 0 to 1023.
Description	Specify a description to the flow group. A description can have up to 31 alphanumeric characters. Spaces are allowed.
Mark Value	Specify a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

Table 59. Flow Group - Add (Continued)

Field	Description
Priority	Specify a new user 802.1p priority value for the packets. The range is 0 to 7. You can specify a new priority value at both the flow group and traffic class levels. If you specify a new user priority value at both levels, the value in the flow group here overrides the value in Traffic Class. If you want the packets to retain the new value when they exit the switch, change Remark Priority to Yes.
Remark Priority	Select one of the following options: ❒ Yes - Replaces the user priority value in the packets with the new value specified in the Priority parameter when the packets leave the switch. ❒ No - Does not replace the user priority value. This is the default setting.
ToS	Specify a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. New ToS values can be set in flow groups, traffic classes, and policies. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.
Move ToS to Priority	Select one of the following options: ❒ Yes - Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. ❒ No - Does not replace the ToS priority field. This is the default setting.
Move Priority to ToS	Select one of the following options: ❒ Yes - Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. ❒ No - Does not replace the ToS priority field. This is the default setting.
Classifier List	Adds the classifier to the flow group. The classifier must already exist on the switch. A flow group can have more than one classifier. Separate multiple classifiers with comma or spaces.

4. Click **Set**.

The new flow group is created.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a Flow Group

To modify a flow group, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Flow Group list is displayed in the bottom section. See Figure 63 on page 182.

2. Select a flow group that you want to modify the settings.

3. Click **Edit**.
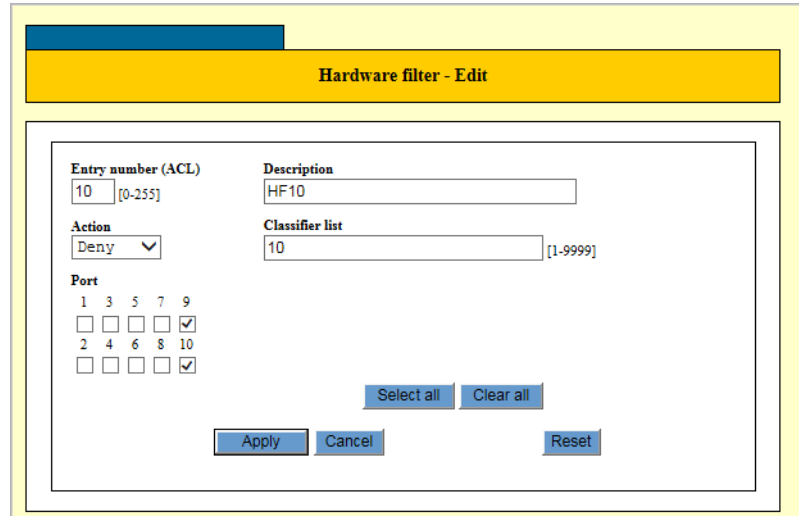
   The Flow Group - Edit page appears. See Figure 65.

Figure 65. Flow Group- Edit Page

4. Change the fields. They are described in Table 59 on page 183.

5. Click **Apply**.

   The modifications to the flow group are in effect.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

> **Note**
> If the flow group is already part of a QoS policy assigned to one or more switch ports, you have to modify the policy by removing the port assignments before you can modify (delete) the flow group. You can reassign the ports to the policy after modifying the flow group.

Deleting a Flow Group

To delete a flow group, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Flow Group list is displayed in the bottom section. See Figure 63 on page 182.

2. Select the flow group that you want to delete.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK**.

   The flow group is deleted.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Traffic Classes

A traffic class consists of a set of QoS parameters and a group of flow groups. Traffic can be prioritized, marked with ToS and DSCP, and bandwidth limited.

> **Note**
> This function restricts a band of the transfer rate of the data including L2 header to the frame forwarded actually. An overhead (preamble of an Ethernet frame) is not included in the biggest bandwidth by setting MAXBANDWIDTH. An error is so big that the frame size in packet is small, and the maximum of the error is about 1.5 times.

Displaying Traffic Classes

To display the traffic classes, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Traffic Class list is displayed in the middle section on the page. See Figure 63 on page 182.

2. Observed the fields described in Table 61 on page 196.

Adding a Traffic Class

To create a new traffic class, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Traffic Class list is displayed in the middle section. See Figure 63 on page 182.

2. Click the Add button in the Traffic Class List section of the page.

   The Traffic Class - Add page appears. See Figure 66.

Figure 66. Traffic Class - Add Page

3. Specify the parameters as described in Table 60 on page 188.

Table 60. Traffic Class - Add

Field	Description
Traffic Class ID	Specify an ID number to the traffic class. Each traffic class on the switch must have a unique ID number. The range is from 0 to 511.
Description	Assign a description to the traffic class. A description can have up to 15 alphanumeric characters. Spaces are allowed.
Exceed Action	Select the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth. The options are: ❑ Drop: Traffic exceeding the bandwidth is discarded. This is the default setting. ❑ Remark: Packets are forwarded after replacing the DSCP value with the new value specified in Exceed Remark Value.
Exceed Remark Value	Specify the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The range is 0 to 63. The default value is 0.

Table 60. Traffic Class - Add (Continued)

Field	Description
Mark Value	Specify a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level.
Max Bandwidth	Specify the maximum available bandwidth for the traffic class. The range is 0 to 1016 Mbps. This parameter determines the maximum rate at which the ingress port accepts packets belonging to the traffic class before either dropping or remarking occurs, depending on the Exceed Action parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discard packets before they can be classified. The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16). If this option is set to 0 (zero), all traffic that matches the traffic class is dropped. However, an access control list can be created to match the traffic that is marked for dropping, or a subset of it, and given an action of permit, to override this. This functionality can be used to discard all but a certain type of traffic.

Table 60. Traffic Class - Add (Continued)

Field	Description
Burst Size	Specify the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. The default is 512 Kbps.

The token bucket is used in situations where you set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded.Tokens are added to the bucket at the same rate as the traffic class' maximum bandwidth, set with option 6, Max Bandwidth. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at the same rate.

If the amount of traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic is discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added.

To use this parameter you must specify a maximum bandwidth with the Max Bandwidth parameter. Specifying a token bucket size without also entering a maximum bandwidth serves no function. |

Table 60. Traffic Class - Add (Continued)

Field	Description
Priority	Specify the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7. The value 0 is the lowest priority and the value 7 is the highest priority. Incoming frames are mapped into one of four Class of Service (CoS) queues based on the priority value. If you specify a new user priority value and in Flow Group, the value in Flow Group overwrites the value here.
Remark Priority	Select one of the following options: Yes - The packets replace the user priority value with the new value specified in the Priority field. No - The packets retain their preexisting priority value when they leave the switch.
ToS	Specify a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A ToS value can be set at all three levels: flow group, traffic class, and policy. The ToS value in a flow group overrides the value specified at the traffic class or policy level, while the ToS value in a traffic class overrides the value in a policy.
Move ToS to Priority	Use this parameter to replace the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. The options are: ❒ Yes: Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. ❒ No: Does not replace the preexisting 802.1p priority level. This is the default.

Table 60. Traffic Class - Add (Continued)

Field	Description
Move Priority to ToS	Use this parameter to replace the value in the ToS priority field with the 802.1p priority field on IPv4 packets. The options are: ❏ Yes: Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. ❏ No: Does not replace the ToS priority field. This is the default.
Flow Group List	Specify the flow group for the traffic class. A traffic class can have more than one flow group. Separate multiple flow groups with commas or spaces.

4. Click **Set**.

The new traffic class is created.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a Traffic Class

To modify a existing traffic class, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Traffic Class list is displayed in the middle section. See Figure 63 on page 182.

2. Select a traffic class that you want to modify the settings.

3. Click **Edit**.

   The Traffic Class - Edit page appears. See Figure 67 on page 193.

Figure 67. Traffic Class- Edit Page

4.   Change the fields. They are described in Table 60 on page 188.

5.   Click **Set**.

The changes to the traffic class are in effect.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

> **Note**
> If the traffic class to be modified is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can modify (edit) the traffic class. You can reassign the ports back to the policy after you have finished modifying the traffic class.

Deleting a Traffic Class

To delete a existing traffic class, perform the following procedure:

1.   From the Navigation pane, go to Switch Settings > Policy Based QoS.

The Traffic Class list is displayed in the middle section. See Figure 63 on page 182.

2.   Select a traffic class that you want to delete.

3.   Click **Delete**.

A confirmation page appears.

4. Click **OK**.

The traffic class is deleted.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Quality of Service (QoS) Policy

From the Policy Base QoS page, you can display a list of QoS policies, add a new QoS policy, modify, and delete QoS policies.

Displaying QoS Policies

To display a list of QoS policies, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The QoS policy list is displayed in the bottom section on the page. See Figure 68.

Figure 68. QoS Policy, Traffic Class, and Flow Group Lists Page

2. Observe the fields described in Table 61 on page 196.

Table 61. QoS Policy, Traffic Class, and Flow Group Lists

Field	Description
QoS Policy List	
QoS policy ID	Displays the ID number of a policy.
Description	Displays the description of the policy.
Active	Displays the status of the policy. The status of a policy can be active or inactive. A policy has an active status when it is associated to at least one switch port and an inactive state when it is not associated to any switch ports.
Traffic class list	Displays the traffic classes associated to the policy.
Ingress port	Displays the ingress ports associated to the policy.
Traffic Class List	
Traffic Class ID	Displays the ID number of a traffic class.
Description	Displays the description of the traffic class.
Active	Displays the state of the traffic class. The state of a traffic class can be active or inactive. A traffic class has an active status if it belongs to a policy that is associated to at least one switch port.
QoS Policy ID	Displays a QoS policy of the traffic class.
Flow Group ID	Displays a flow group of the traffic class.
Flow Group List	
Flor Group ID	Displays the ID number of a flow group.
Description	Displays the description of the flow group.
Active	Displays the status of a flow group. The status can be active or inactive. A flow group is active if it is part of a policy that is associated to a switch port. A flow group is inactive if it is not part of any policies or if the policies are not associated to any ports.
Traffic Class ID	Displays the ID numbers of the traffic classes the belong to the flow groups.
Classifier ID	Displays the classifiers that belong to the flow group.

Adding a QoS Policy

To create a new QoS policy, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Flow Group list is displayed in the bottom section. See Figure 68 on page 195.

2. Click **Add** in the QoS policy section of the page.

   The QoS Policy - Add page appears. See Figure 69.

Figure 69. QoS Policy - Add Page

3. Specify the parameters as described in Table 62.

Table 62. QoS Policy- Add

Field	Description
Policy ID (Policy)	Assign an ID number to a QoS policy. Each QoS policy on the switch must have a unique ID number. The range is from 0 to 255.
Description (Description)	Specify a description to the QoS policy. The description can have up to 31 alphanumeric characters. Spaces are allowed.

Table 62. QoS Policy- Add (Continued)

Field	Description
Remark IP DSCP field value (RemarkInDscp)	Specify whether the DSCP values in the ingress packets are overwritten. The options are: ❒ None - The DSCP values in the packets are not overwritten. ❒ All - The DSCP values in the packets are overwritten.
IP DSCP field value (InDespOverWrite)	Specify a replacement value to write into the DSCP field of a packet. The range is 0 to 63. The new DSCP value can be set at all three levels: flow group, traffic class, and QoS policy. A DSCP value specified in a flow group overwrites a DSCP value specified in a traffic class or QoS policy. A DSCP value specified in a QoS policy is used only when no value is specified in a flow group or traffic class.
IP ToS field value (TOS)	Specify a replacement value for the Type of Service (ToS) field of a packet. to write into the DSCP (TOS) field of the packets. The range is 0 to 7. A ToS value can be set at all three levels: flow group, traffic class, and QoS policy. A ToS value specified in a flow group overwrites a ToS value specified in a traffic class or QoS policy. A ToS value specified in a QoS policy is used only when no value is specified in a flow group or traffic class.
Apply ToS to priority (MoveToStoPriority)	Specify whether the value in the 802.1p priority field is replaced with the value in the ToS priority field on IPv4 packets. The options are: ❒ Yes - Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. ❒ No - Does not replace the preexisting 802.1p priority. This is the default.

Table 62. QoS Policy- Add (Continued)

Field	Description
Apply priority to ToS (MovePrirorytoToS)	Specify whether the ToS priority value is replaced with the 802.1p priority value in IPv4 packets. The options are: ☐ Yes - Replaces the priority value in the ToS priority field with the 802.1p priority field in IPv4 packets. ☐ No - Does not replace the ToS priority field. This is the default setting.
Mirroring (SendtoMirror)	Copy the traffic that meets the criteria of the policy's classifiers to a destination mirror port. The options are: ☐ Yes - Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by configuring a mirror port. To configure a mirror port, see "Port Mirroring" on page 79. ☐ No - Does not copy the traffic to a destination mirror port. This is the default setting.
Traffic class list (TrafficClassList)	Specify the traffic class for the QoS policy. The traffic class must exist. A QoS policy can have more than one traffic class. Separate multiple traffic class ID numbers with commas or spaces.
Ingress port (IngressPort)	Specify the ingress port of the QoS policy. A QoS policy can be assigned to more than one ingress port. Separate multiple port numbers with commas or spaces. A port can be an ingress port of only one QoS policy at a time.

Table 62. QoS Policy- Add (Continued)

Field	Description
Egress Port (EgressPort)	Specify the egress port of the QoS policy. You can enter only one egress port. A port can be an egress port of only one QoS policy at a time. A port that is an egress port of a QoS policy must be removed from it's current QoS policy assignment before the port can be added to another policy.
Redirect port (RedirectPort)	Specify a port where the traffic is to be redirected. Traffic that matches the defined traffic flow is redirected to the specified port. You can specify only one port.

4. Click **Set**.

    The new QoS policy is in effect.

> **Note**
> To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Modifying a QoS Policy

To modify a QoS policy, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

    The Flow Group list is displayed in the bottom section. See Figure 68 on page 195.

2. Select a QoS policy that you want to modify the settings.

3. Click **Edit**.

    The QoS Policy - Edit page appears. See Figure 70 on page 201.

Figure 70. QoS Policy - Edit Page

4. Change the fields described in Table 62 on page 197.

5. Click **Apply**.

   The QoS policy changes that you selected are in effect.

   > **Note**
   > To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Deleting a QoS Policy

To delete a QoS policy, perform the following procedure:

1. From the Navigation pane, go to Switch Settings > Policy Based QoS.

   The Flow Group list is displayed in the bottom section. See Figure 68 on page 195.

2. Select the QoS policy that you want to delete.

3. Click **Delete**.

   A confirmation page appears.

4. Click **OK**.

   The QoS policy is deleted.

Note
To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Chapter 5
Security

This chapter includes the following topics:

❑ "Port Security" on page 204

Port Security

The AT-IA810 switch has the MAC address-based port security feature, which filters packets at ports whether the system forwards or discards ingress packets based on source MAC addresses of the packets.

Guidelines to Port Security

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

❐ Packets are filtered on the ingress ports. By default, the security mode is Automatic.

❐ A port can have only one security mode at a time.

❐ The static and dynamic addresses on a port are deleted from the MAC address table when the security mode is changed to Automatic from one of the other security modes.

Displaying the Port Security List

To display the port security list, perform the following procedure:

1. From the Navigation pane, go to Security Settings > Port Security.

   The Port Security page is displayed. See Figure 71.
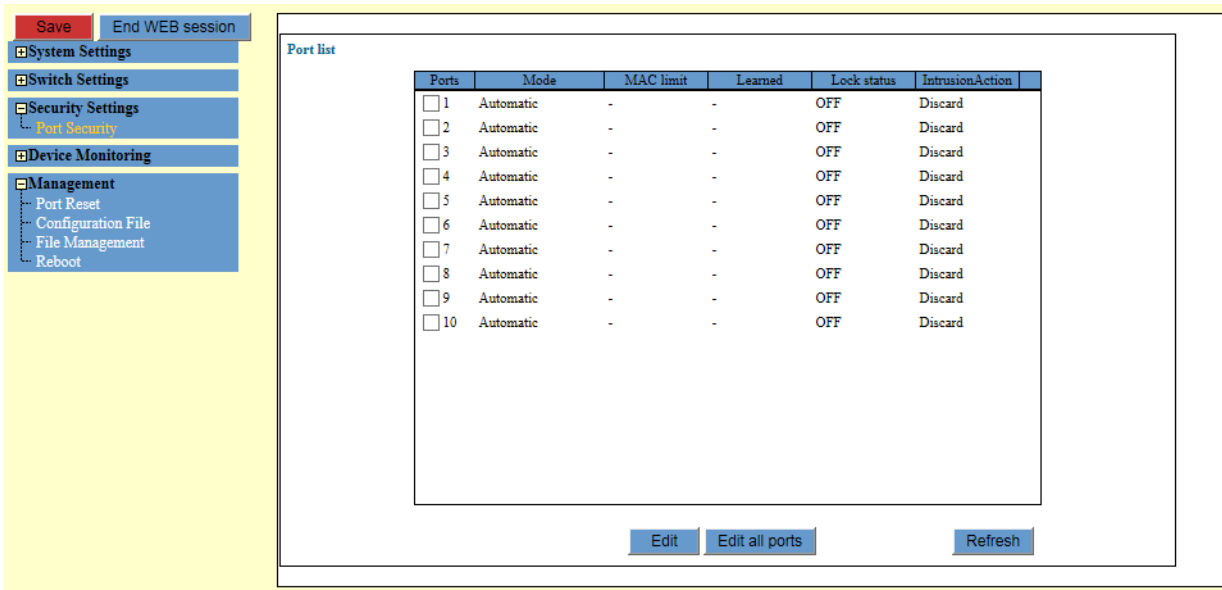
Figure 71. Port Security Page

2. Observe or specify the fields described in Table 63 on page 205.

Table 63. Port Security

Field	Description
Port	Displays the port number and its checkbox.
Mode	Displays the security mode. The options are: ❒ **Automatic**- Disables Port Security on the port. This is the default setting. The static and dynamic addresses on the MAC address table when the security mode is changed to Automatic. ❒ **Secured** - Stops the switch from learning and storing new source MAC addresses. The system converts the dynamic addresses on the MAC address table into static MAC addresses.The port forwards only packets whose source addresses match the static MAC addresses on the MAC address table. ❒ **Limited** - Deletes all of the dynamic MAC addresses from the MAC address table and the switch starts learning new addresses up to the defined maximum. Static addresses added to the port before the feature is enabled are retained. These static addresses are not counted against the maximum number. The dynamic addresses that the port learn are added as static addresses in the MAC address table. ❒ **Dynamic Limited** - Works the same as the Limited mode except how the system handle the dynamic MAC addresses. The source MAC addresses learned by the port in the Dynamic Limited mode are entered as dynamic addresses in the MAC address table and, consequently, are deleted from the table when the devices are inactive.
MAC limit	Displays the maximum number of dynamic MAC addresses the port is allowed to learn. This field applies only to the Limited and Dynamic Limited security modes.
Learned	Displays the number of dynamic MAC addresses the port has already learned. This column applies only to the Limited and Dynamic Limited security modes.

Table 63. Port Security (Continued)

Field	Description
Lock status	Displays whether the port can learn new dynamic MAC addresses. The lock statuses for a port in the Limited or Dynamic Limited security mode are: ❒ Off: The port can learn more dynamic MAC addresses because it has not learned its maximum number of addresses. ❒ On: The port cannot learn any more MAC addresses because it has learned its maximum number of addresses. **Note** The lock status for ports in the Secured mode is always On because ports in that security mode are not allowed to learn new dynamic MAC addresses.
Intrusion Action	Displays an intrusion action that the port takes when receiving an invalid frame. The options are: ❒ Discard - Discards invalid frames. ❒ Disable - Disables the port. The link on the port remains up, but the port stops forwarding traffic. **Note** Do not specify Disable on the management port. You lose access to the switch when the port receives an invalid frame. ❒ Trap - Discards invalid frames and send SNMP traps. SNMP must be enabled on the switch. ❒ Log - Discards invalid frames and enters messages in the event log.

Modifying Security Settings on Ports

To modify security settings on ports, perform the following procedure:

1. From the Navigation pane, go to Security Settings > Port Security.

   The Port Security page is displayed. See Figure 71 on page 204.

2. Check the checkbox of the port you want to modify its security settings.

3. Click **Edit**.

   The Port Security settings window appears. See Figure 72.

Figure 72. Port Security Settings Page

4. Configure the parameters as described in Table 63 on page 205.

   Note
   See the Intrusion action field for Violation (IntrusionAction).

5. Click **Apply**.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

   Note
   If used mode is 'dynamic limited', intrusion action is fixed 'discard' for intrusion action. If user uses else mode (automatic, secured, limited), the user can select all intrusion actions.

Chapter 6
Device Monitoring

This chapter includes the following topics:

System Information

You can view basic system and port information from the System Information page. In addition, you can specify the page to be updated automatically or save the information to a file.

Displaying Port Configuration

To display port parameter settings:

1. Click on a port in the image of the front panel.

   The switch displays the Display Port Status window. See Figure 73. The parameters can be viewed one port at a time.
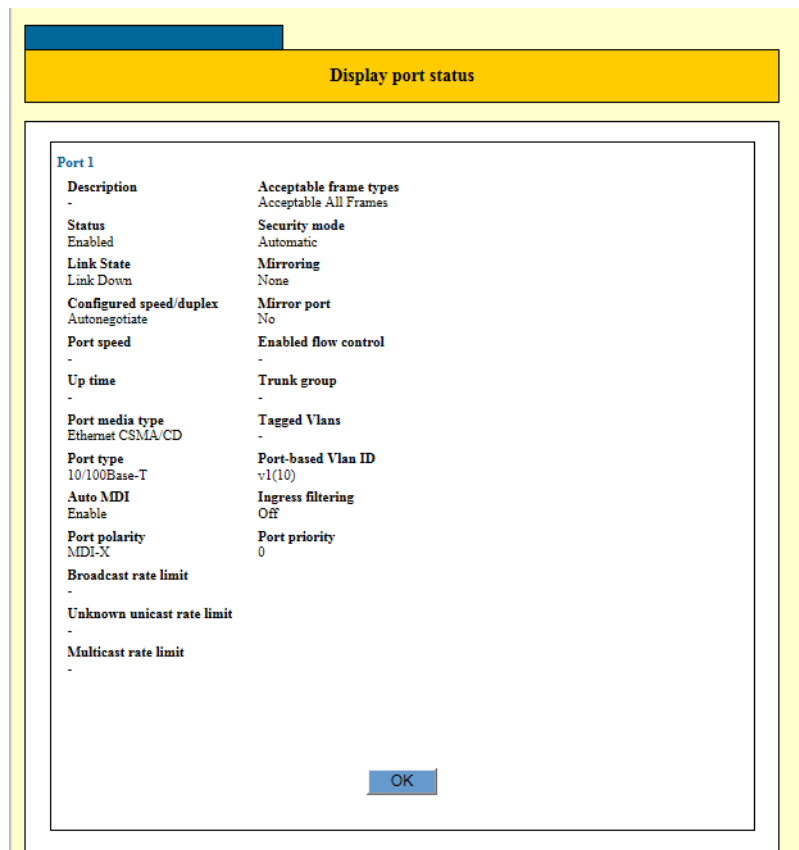
Figure 73. Display Port Status Page

Viewing System Information, Hardware Information, and Average CPU Usage

To view System Information, Hardware Information, and Average CPU usage, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > System Information.

   The System Information page is displayed. See Figure 74.

Figure 74. System Information Page

2. Observe the settings described in Table 64 on page 211.

Table 64. System Information

Field	Description
System Information	
SysDescription	Displays the description of the management software, which is accessed by SNMP managers.
Syscontact	Displays the contact information, which is accessed by SNMP managers.

Table 64. System Information (Continued)

Field	Description
SysLocation	Displays the location of the switch, which is accessed by SNMP managers.
SysName	Displays the name of the switch, which is accessed by SNMP managers.
SysUpTime	Displays the system up time, which is accessed by SNMP managers.
Release Version	Displays the version of the management software.
Release Built	Displays the date of the management software.
Hardware Information	
DRAM	Displays the size of the DRAM.
Flash	Displays the size of the Flash.
MAC address	Displays the MAC address of the device.
Flash PROM	Displays the status of the FLASH PROM.
RAM	Displays the status of the RAM.
SW chip	Displays the status of the software chip.
UART	Displays the status of the UART.
Temperature	Displays the status of the device.
Voltage	Displays the status for 1.2V.
	Displays the status for 2.5V(A).
	Displays the status for 2.5V(B).
	Displays the status for 3.3V.
Average CPU Usage	
Last second	Displays the CPU usage for the last second.
Last minute	Displays the CPU usage for the last minute.
Last 5 minutes	Displays the CPU usage for the last 5 minutes.
Last 15 minutes	Displays the CPU usage for the last 15 minutes.

Viewing the Detail Information

To view System Information, Hardware Information, and Average CPU usage, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > System Information.

   The System Information page is displayed. See Figure 74 on page 211.

2. Click **Detail.**

   The System - Detail page is displayed. See Figure 75.
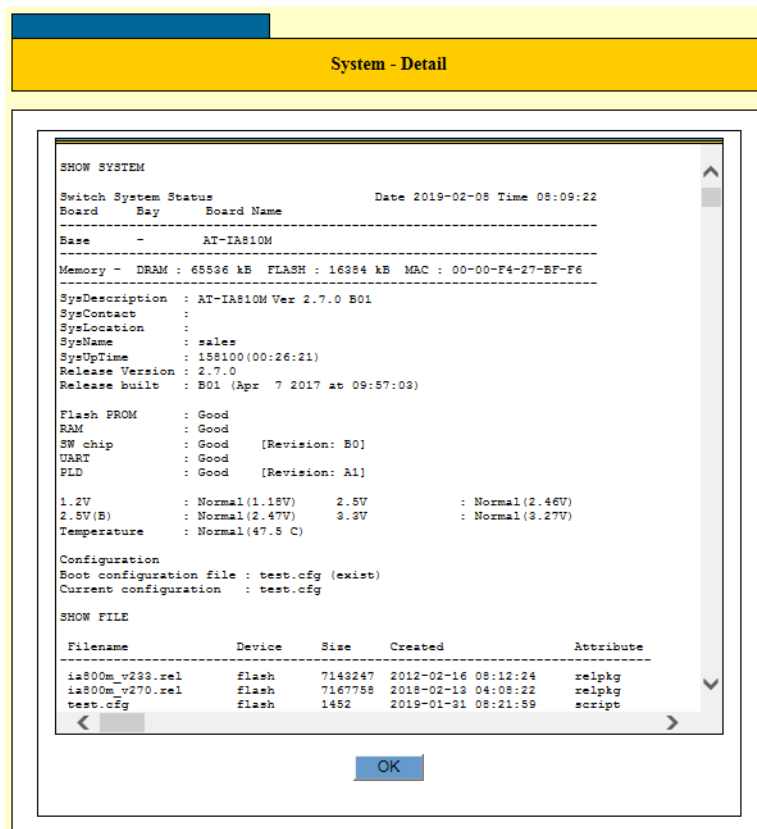
Figure 75. System - Detail Page

3. Click **OK.**

**Saving
Information to a
File**

By clicking **Detail**, you can save the displayed information to a file on your workstation or a network server. You might be asked to provide this file if you contact Allied Telesis for assistance in resolving a technical problem.

To save the detail system information to a file, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > System Information.

   The System Information page is displayed. See Figure 74 on page 211.

2. Click **Save to file.**

   Your Web browser prompts you to select a location to save.

3. Follow the instructions from your browser.

**Refreshing the
Window**

To update information displayed on the Web page, click **Update** in the upper left corner of the display table. The **Update** button immediately updates the information in the switch image and table.

In addition to the **Update** button, you can specify the switch automatically to update the switch information periodically.

To set the switch automatically to update the display, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > System Information.

   The System Information page is displayed. See Figure 74 on page 211.

2. Specify the settings described in Table 65.

Table 65. Auto Update

Field	Description
Auto update/ refresh	Enable or disable the automatic update option. The default setting is enabled.
Duration/interval	Specify how frequently the switch updates the page when you enable the auto update feature. The range is 1 to 99 minutes. The default setting is 1minute.

3. Click **Set**.

Note

To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Log

You can view the log counters and event messages that are stored on the switch. In addition, you can save the event messages to a file on your network and delete them.

Viewing the Log Counters

To view the log counters, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Log.

    The Log counter and Log Display Order page is displayed. See Figure 76.
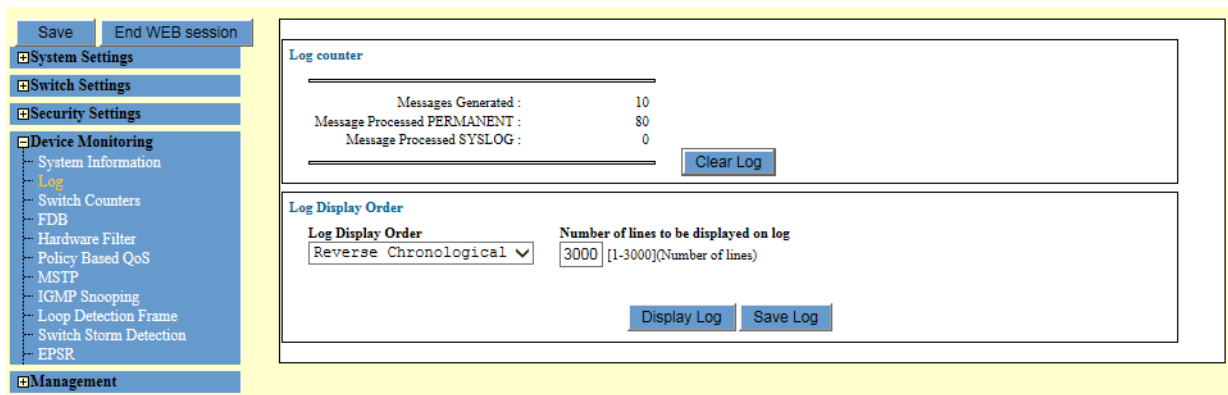
Figure 76. Log Counter and Log Display Order Page

2. Observe he following fields described in Table 66.

Table 66. Log Counters

Field	Description
Messages Generated	Displays the number of the event messages that the switch generated since the beginning of this session.
Message Processed PERMANENT	Displays the number of the event messages stored in the event log on the switch.
Message Processed SYSLOG	Displays the number of the event messages that the syslog client sent to the designated syslog server.

3. Click **Clear Log** as needed:

    The clear log refreshes the display on this page.

Viewing the Port List

To view the event messages stored on the switch, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Log.

   The Log counter and Log Display Order page is displayed. See Figure 76 on page 216.

2. Specify the items described in Table 67.

Table 67. Log Display Order

Field	Description
Log Display Order	Select a way to display or save the event messages from the event log. The options are: ❑ Reverse Chronological ❑ Chronological ❑ Latest
Number of Lines to be displayed	Specify how many lines of the event messages that you want to display or save. The range is 1 to 3000 lines. The default value is 3000.

3. Click **Display Log**.

Saving the Event Messages to a File

To save the event messages in the event log to a file on your network, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Log.

   The Log counter and Log Display Order page is displayed. See Figure 76 on page 216.

2. Specify the items described in Table 67.

3. Click **Save Log**.

   Your Web browser prompts you to open or save the file. See Figure 77.

Do you want to open or save **log_192.168.1.10_20180315-054725.txt** from **192.168.1.10**? Open Save ▾ Cancel ✕
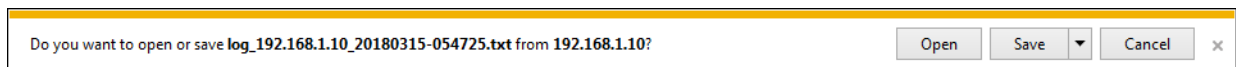
Figure 77. Save Log

4. Follow the instructions from your browser.

Switch Counters

The switch keeps statistics counters that become useful when your are troubleshooting network problems. You can view the log counters and event messages that are stored on the switch. In addition, you can save the event messages to a file on your network and delete them.

Viewing the Switch Counters

To view the switch counters, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Switch Counters.

   The Switch counters and Port list page is displayed. See Figure 78.
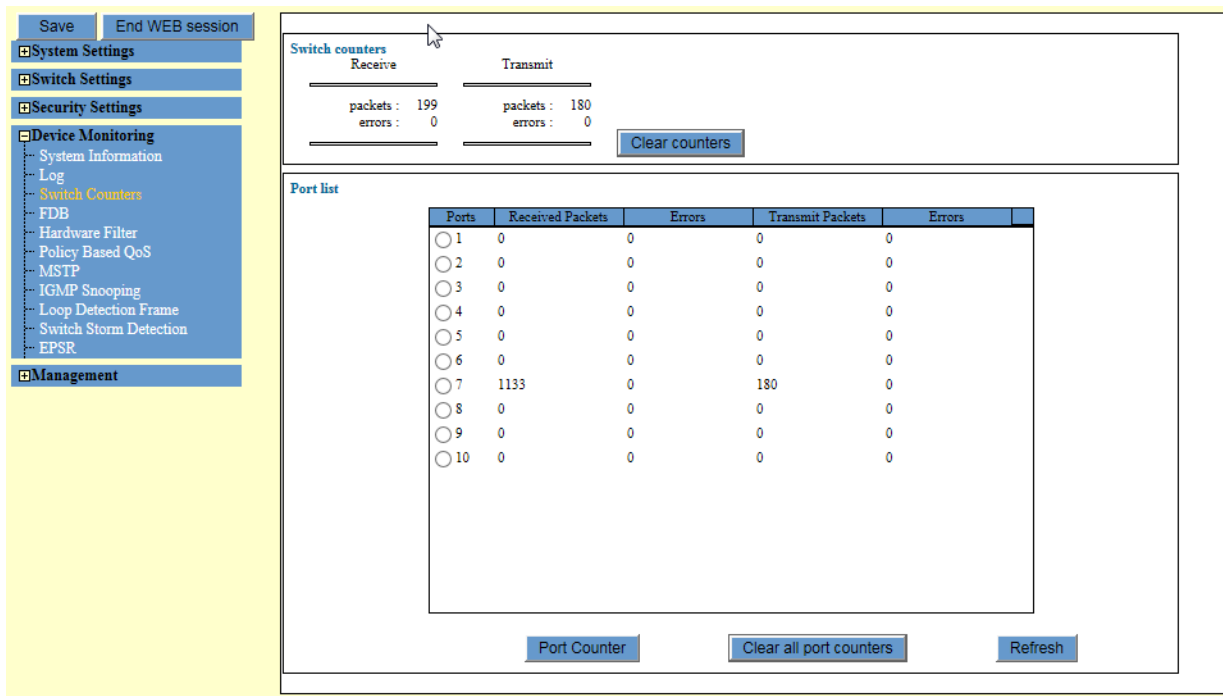
Figure 78. Switch Counters and Port List Page

2. Observe the fields described in Table 68.

Table 68. Switch Counters

Field	Description
Receive	
packets:	Displays the number of the packets that the switch received.
errors	Displays the number of the errors that the switch revived.

Table 68. Switch Counters (Continued)

Field	Description
Transmit	
packets:	Displays the number of the packets that the switch transmitted.
errors	Displays the number of the errors that the switch transmitted.

3. Click **Clear counters** as needed:

   The clear counters deletes the counters.

Viewing the Port List

To view a list of port counters, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Switch Counters.

   The Port list is displayed. See Figure 78 on page 218.

2. Observe the following items described in Table 69.

Table 69. Port List

Field	Description
Port	Displays the port number. Select the radio button to display additional port counters.
Received Packets	Displays the number of the packets that the switch received.
Errors	Displays the number of the errors that the switch revived.
Transmit Packets	Displays the number of the packets that the switch transmitted.
Errors	Displays the number of the errors that the switch transmitted.

3. Click one of the following buttons as needed:

   ❒ **Port Counter —** Click this button to view additional port counters. See "Viewing Additional Port Counters" on page 220.

   ❒ **Clear counters —** Deletes all the port counters.

   ❒ **Refresh —** Updates the counters.

**Viewing
Additional Port
Counters**

To view additional port counters, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Switch Counters.

   The Port list is displayed. See Figure 78 on page 218.

2. Select a port that you want to view additional port counters by marking its radio button.

   The Port counter window is displayed. See Figure 79.
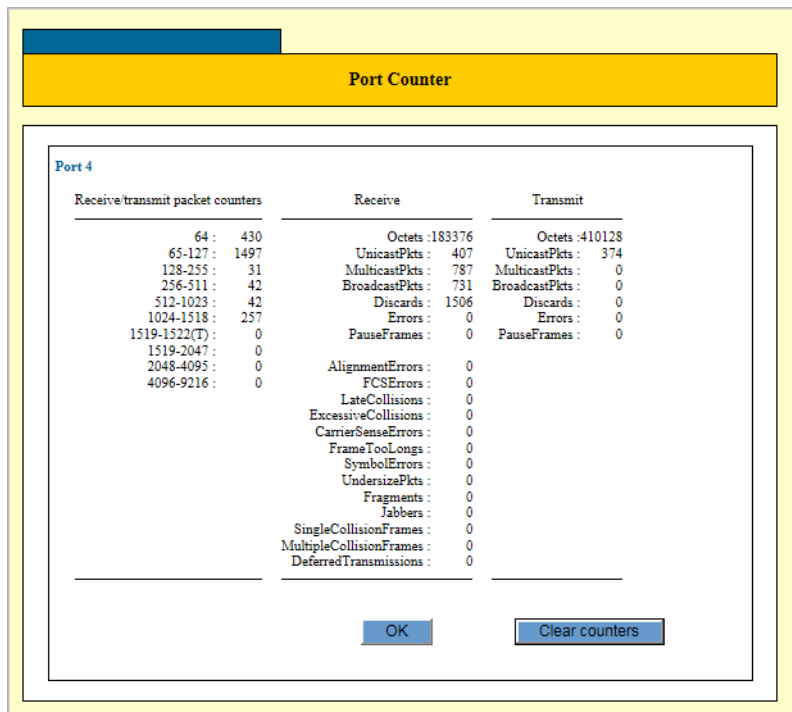
Figure 79. Port Counter Window

3. Click the following buttons as needed:

   ❑ **OK —** Closes the window.

   ❑ **Clear counters —** Deletes all additional counters on the page.

Forwarding Database (FDB)

From the FDB page, you can display a list of MAC addresses in the MAC address table, add static MAC addresses, delete static MAC addresses, and delete all of the dynamic MAC addresses from the MAC address table.

Displaying a List of MAC Addresses

To display a list of MAC Addresses in the MAC address table, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > FDB.

    The FDB page is displayed. See Figure 80.

Figure 80. Device Monitoring > FDB Page

2. Do one of the following:

    ❒ To view all the MAC addresses in the table, leave the FDB display filter options at the default settings.

    ❒ To filter the table for specific MAC addresses to display, specify the parameters in the FDB display filter section. The parameters are described in Table 70 on page 222.

Table 70. DFB Display Filter

Field	Description
Entry Types	Select an option form the pull-down menu to display categories of MAC addresses. The options are: ❑ None - Disables the filter. ❑ Static - Displays static MAC addresses. ❑ Dynamic - Displays dynamic MAC addresses. ❑ Discard - Displays the MAC addresses of nodes that were denied entry to the switch.
MAC Address (MAC)	Specify a MAC address to learn a port on which the switch has learned a particular address.
VLAN Name (ID)	Specify a VLAN name or ID to view the MAC addresses the switch has learned on the ports of a particular VLAN.
Trunk Group	Specify a trunk group name to list the MAC addresses that the switch has learned on the ports of the port trunk.
Ports	Specify ports to list the MAC addresses that the switch has learned on specify ports.

3. Click **Display FDB**.

The switch displays the FDB list window. See Figure 81 on page 223.

```
                              FDB display filter


  Switch Forwarding Database (Software)
  ---------------------------------------------------------------
  VLAN    MAC Address         Status    Port
  ---------------------------------------------------------------
  1       00-00-f4-27-bf-f6   Static    CPU
  1       44-87-fc-4e-36-58   Dynamic   4
  ---------------------------------------------------------------
```
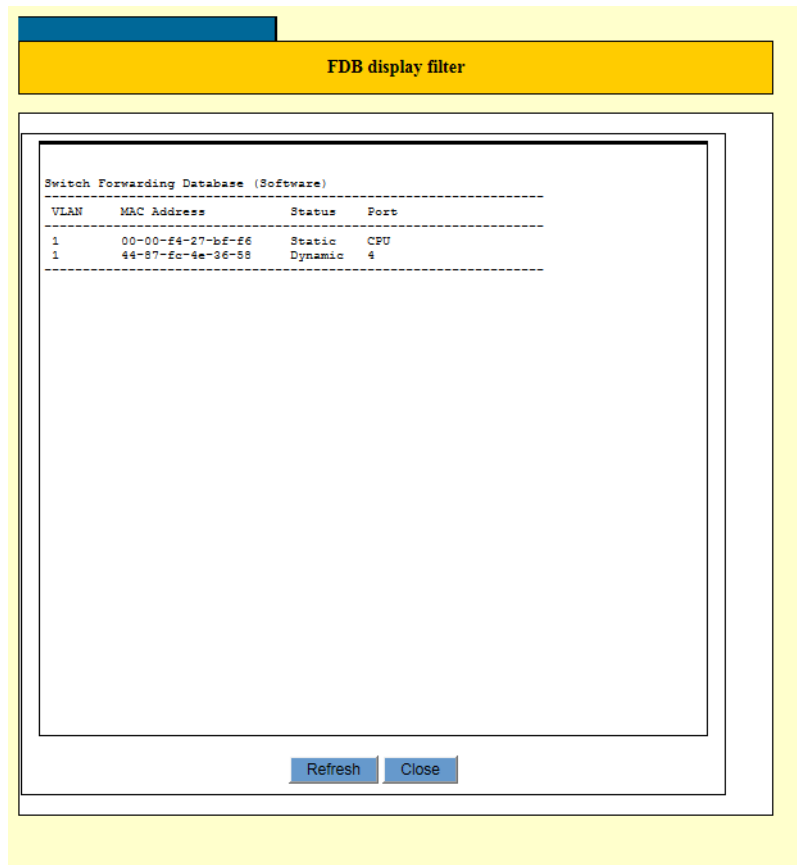
                    [Refresh] [Close]

Figure 81. FDB Display Window

4. Click one of the following buttons:

   ❑ **Close —** Closes the window.

   ❑ **Refresh —** Refreshes the display on this page.

Adding a Static MAC Address

To add static unicast MAC Address in the MAC address table, perform the following procedure:

> **Note**
> You may not add a static multicast MAC address.

1. From the Navigation pane, go to Device Monitoring > FDB.

   The FDB page is displayed. See Figure 80 on page 221.

2. Specify the fields in the Static Entries section. The fields are described in Table 71 on page 224.

Table 71. Static Entries

Field	Description
Port number	Specify the number of the port on the switch where you want to assign the static MAC address.
VLAN Name	Specify the VLAN name or VID where the port is a member.
MAC address	Specify a new MAC address.

3. Click **Add.**

   The new static MAC address is added to the port that you have specified.

Deleting a Static MAC Address

To delete static MAC Address from the MAC address table, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > FDB.

   The FDB page is displayed. See Figure 80 on page 221.

2. Do one of the following:

   ❒ To delete all of the static address assigned to a port on the switch, enter the port number in the Port Number field.

   ❒ To delete a specific MAC address, enter the port number of the address in the Port Number field and the MAC address in the MAC Address (MAC) field.

3. Click **Delete.**

   All of the static MAC addresses are deleted.

Deleting Dynamic MAC Addresses

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

1. From the Navigation pane, go to Device Monitoring > FDB.

   The FDB page is displayed. See Figure 80 on page 221.

2. Click **Delete** in the Delete all dynamic entires section of the page.

   All of the dynamic MAC address entries are deleted from the FDB.

Hardware Filter

From the hardware filter page, you can display a list of hardware filter entries and hardware filter counters.

Displaying Hardware Filter Entries

To display the hardware filter entries on the switch, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Hardware Filter.

   The Entry list is displayed. See Figure 82.
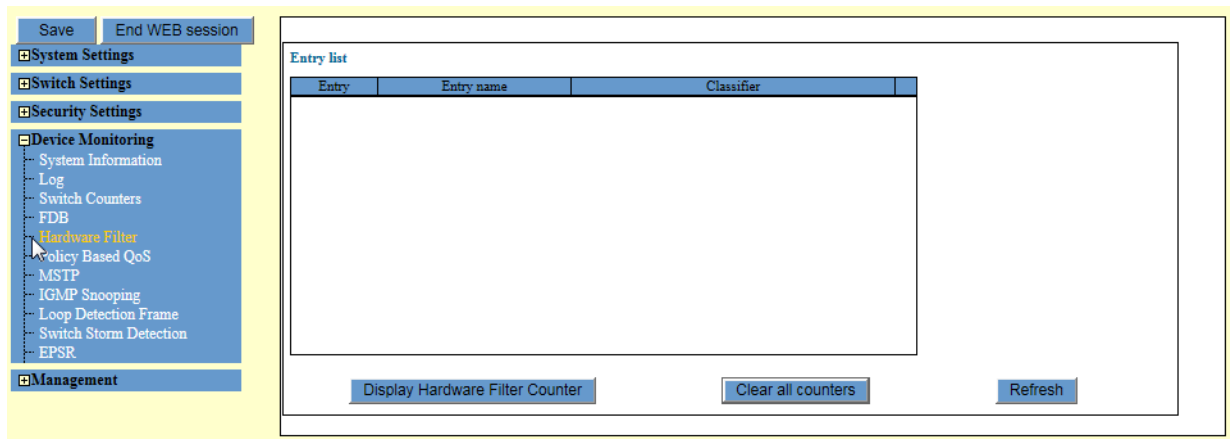
Figure 82. Device Monitoring > Hardware Filter Page

2. Observe the items described in Table 72.

Table 72. Hardware Filter

Field	Description
Entry	Displays the hardware filter number and its checkbox to select.
Entry name	Displays the hardware filter name.
Classifier	Displays a classifier associated to the hardware filter.

Displaying Hardware Filter Counter

To display the hardware filter entries on the switch, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Hardware Filter.

   The Entry list is displayed. See Figure 82 on page 225.

2. Select an entry whose counters you want to view.

3. Click **Display Hardware Filter Counter.**

The Display Hardware filter counters list is displayed. See Figure 83.
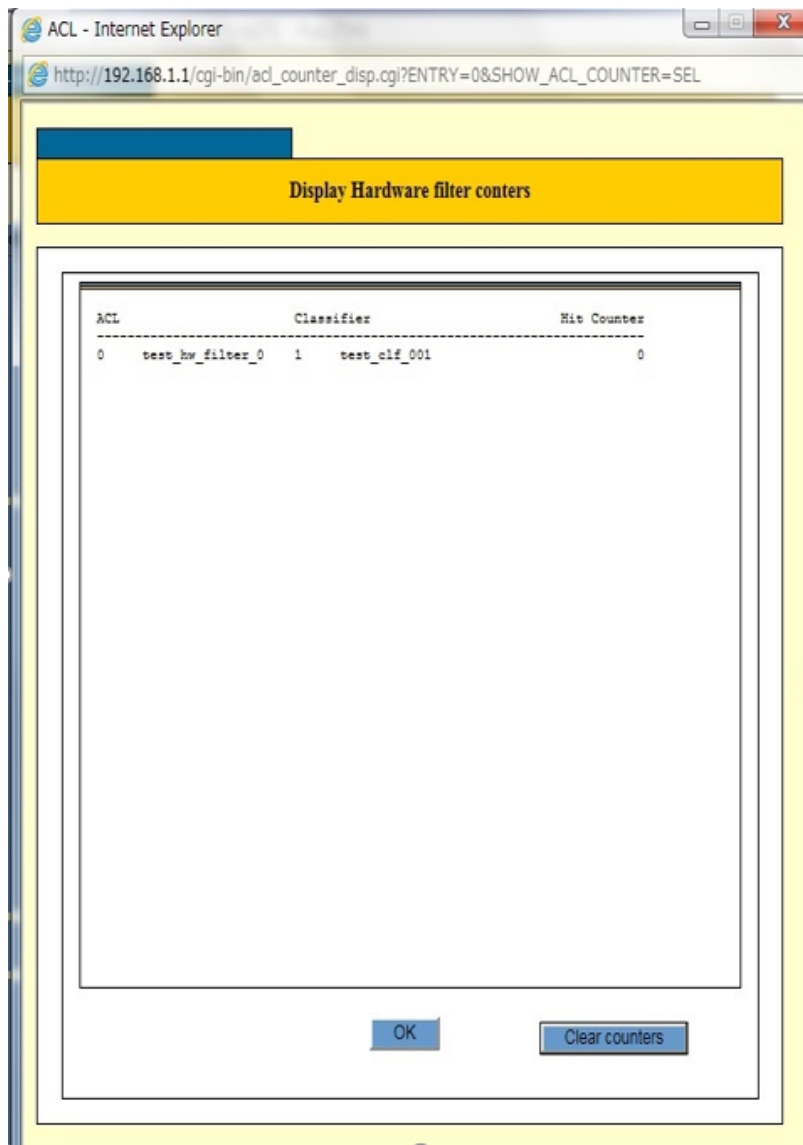
Figure 83. Display Hardware Filter Counters

Clearing All Counters   To delete all of the counters, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Hardware Filter.

The Entry list is displayed. See Figure 82 on page 225.

2. Click **Clear all counters.**

Policy Based QoS

To display statistics on packets processed by the QoS policies, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Policy Based QoS.

   The QoS Policy list page is displayed. See Figure 84.
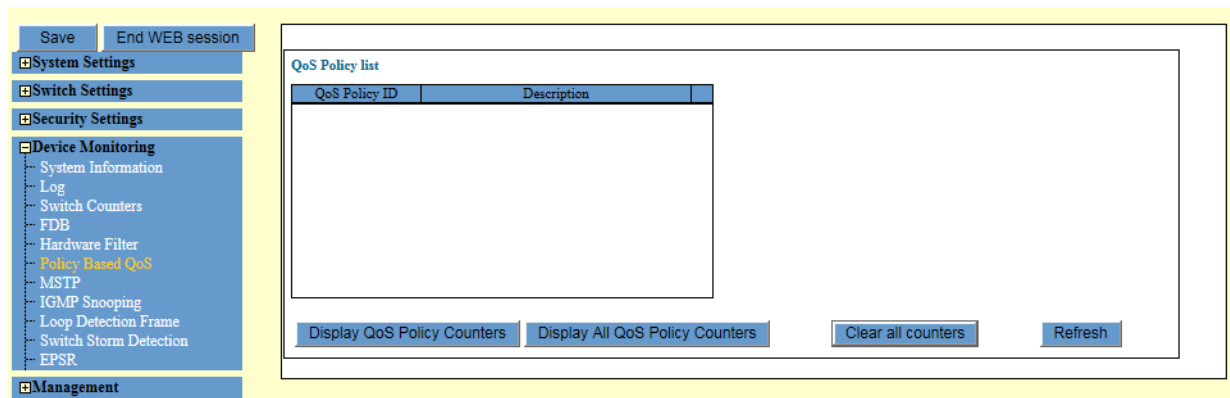
Figure 84. QoS Policy List Page

2. Do one of the following options:

   ❒ To display the statistics of the selected QoS policy, click **Display QoS Policy Counters**.

   ❒ To displays the statistics for all of the QoS policies on the list, click **Display All QoS Policy Counters**.

Displaying QoS Policy Statistics

To display statistics on the number of packets that have been processed by the QoS policies on the switch, perform the following procedure:

1. Expand the Device Monitoring menu in the main menu.

2. Select the Policy Based QoS option from the Device Monitoring menu.

    An example of the Device Monitoring - Policy Based QoS window is shown in Figure 85.
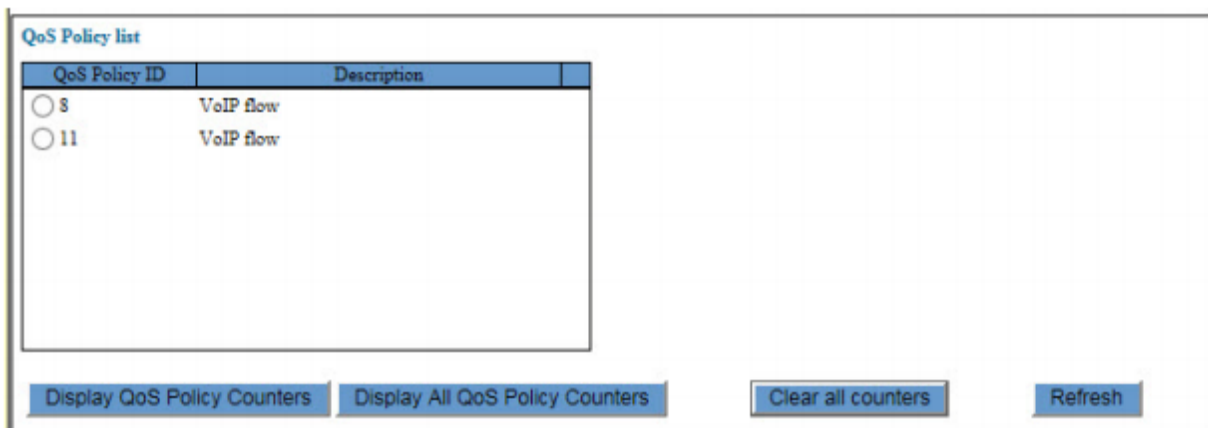
Figure 85. Device Monitoring - Policy Based QoS Window

The window lists the QoS policies on the switch.

3. Do one of the following options:

    □ To display the statistics of the selected QoS policy, click **Display QoS Policy Counters**.

    □ To displays the statistics for all of the QoS policies on the list, click **Display All QoS Policy Counters**.

An example of the QoS Policy Counters window is shown in Figure 86.

QoS Policy Counters

```
Policy/TrafficClass/FlowGroup Classifier                    Hit Counter
------------------------------------------------------------------------
  8    VoIP flow
   18   VoIP flow
     14    VoIP               22    VoIP flow                    0
 11    VoIP flow
   15   VoIP flow
     17    VoIP flow          23    VoIP flow                    0
```
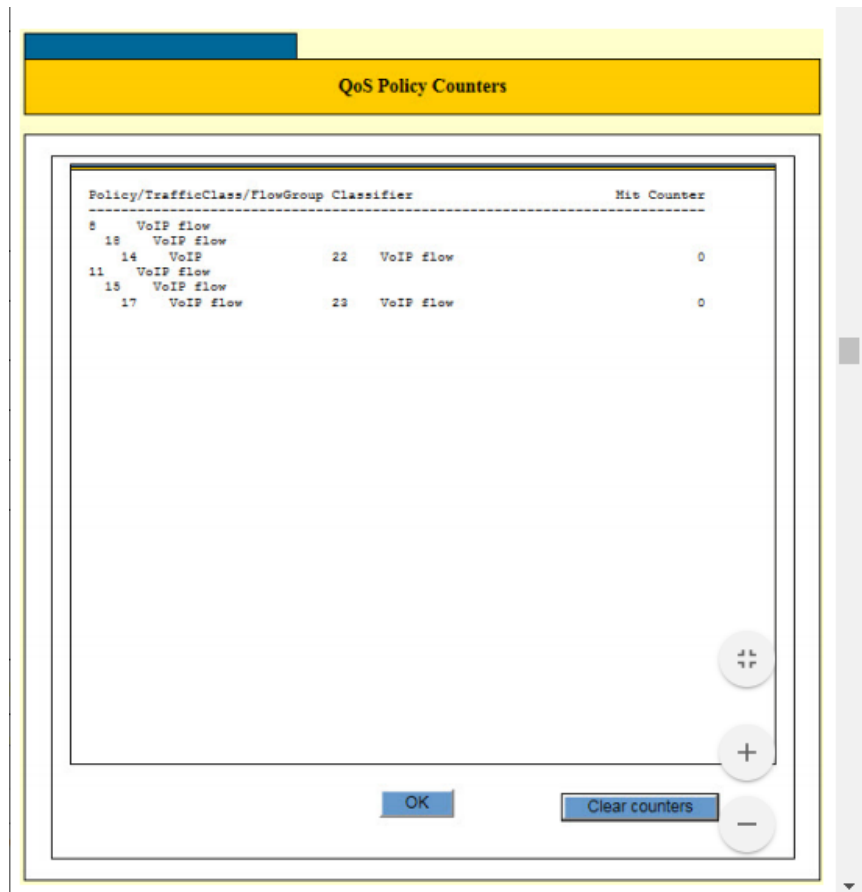
OK   Clear counters

Figure 86. QoS Policy Counters Window

The Hit Counter displays the number of packets a QoS policy has processed.

4. To clear the counters, do one of the following:

    ❒   To clear the counters for all of the policies, click **Clear All Counters** in the Device Monitoring - Policy Based QoS window.

    ❒   To clear the counters for a particular policy, click **Clear Counters** in the QoS Policy Counters window.

MSTP (Multiple Spanning Tree Protocol)

To display statistics on MSTP, perform the following procedure.

1. From the Navigation pane, go to Device Monitoring > MSTP.

    The MSTP Port list page is displayed. See Figure 87.
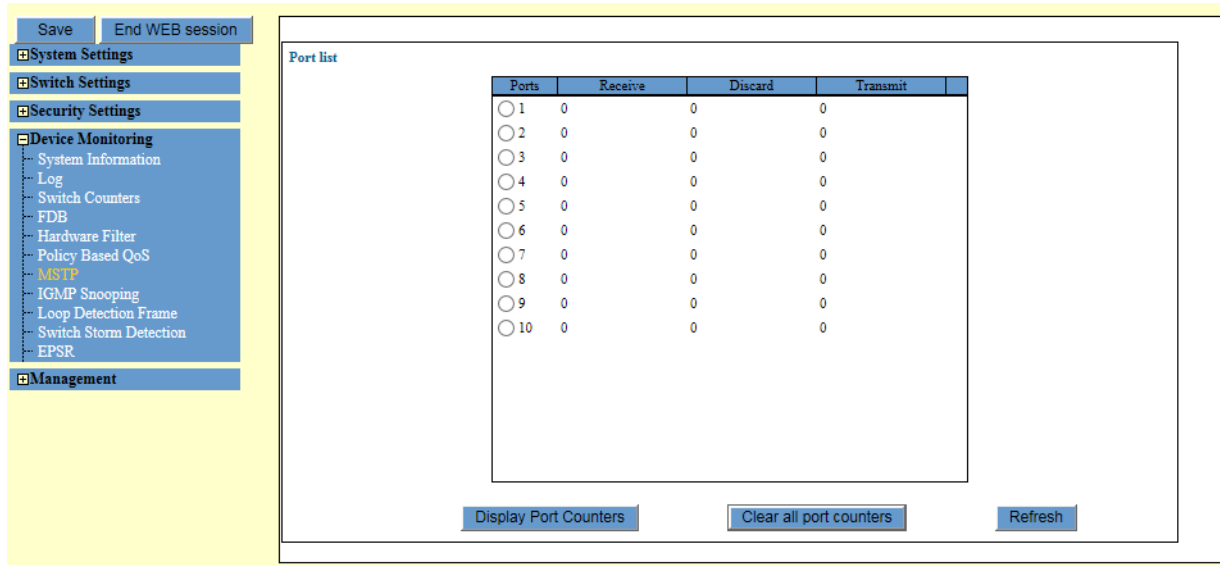
Figure 87. MSTP Port List Page

2. Observe the fields described in Table 73.

Table 73. Manual Channel Plan

Field	Description
Ports	Displays a port number and radio button.
Receive	Displays the total number of STP, RSTP, and MSTP BPDUs that the port has received from other network devices.
Discard	Displays the total number of BPDUs that the port has discarded because they had the wrong Type value.
Transmit	Displays the total number of STP, RSTP, and MSTP BPDUs that the port has transmitted to other network devices.

3. Click one of the following buttons as needed:

❐ **Display Port Counters —** Displays the BPDU statistics on the selected port.

❐ **Display All Port Counters —** Displays the BPDU statistics for all of the ports.

The switch displays the MSTP port counters window.
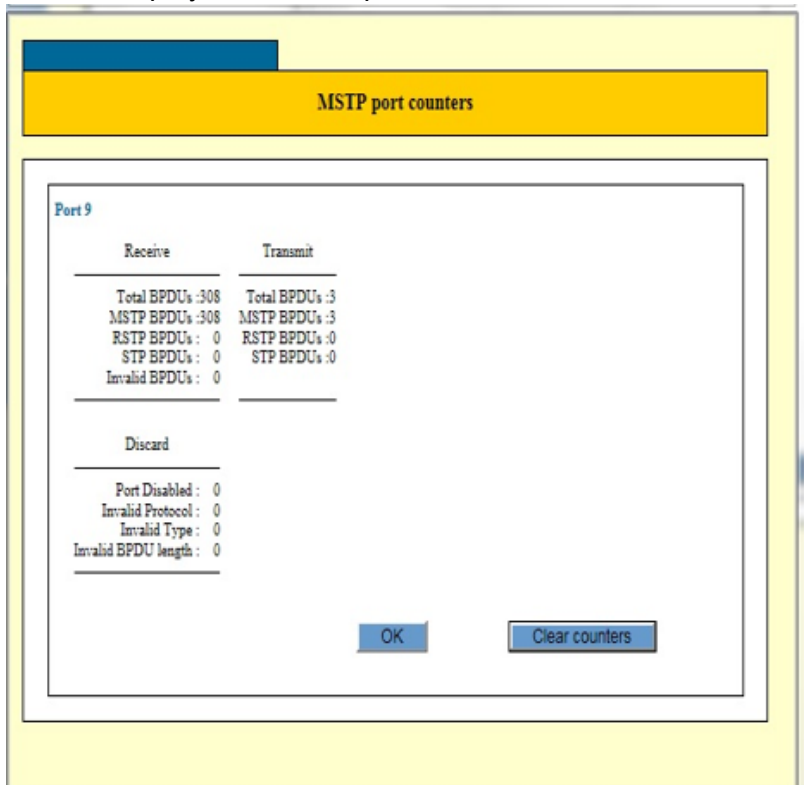
Figure 88. MSTP Port Counters

4. The counters in the table are described in Table 74.

Table 74. MSTI Statistics Window

Statistic	Description
Receive	
Total BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has received from other network devices.
MSTP BPDUs	Displays the total number of MSTP BPDUs the port has received from other network devices.
RSTP BPDUs	Displays the total number of RSTP BPDUs the port has received from other network devices

Table 74. MSTI Statistics Window (Continued)

Statistic	Description
STP BPDUs	Displays the total number of STP BPDUs the port has received from other network devices.
Invalid BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has deleted because they had the wrong type value.
Transmit	
Total BPDUs	Displays the total number of STP, RSTP, and MSTP BPDUs the port has transmitted to other network devices.
MSTP BPDUs	Displays the total number of MSTP BPDUs the port has transmitted to other network devices.
RSTP BPDUs	Displays the total number of RSTP BPDUs the port has transmitted to other network devices
STP BPDUs	Displays the total number of STP BPDUs the port has transmitted to other network devices.
Discard	
Port Disabled	This statistic is not supported. The value is always 0.
Invalid Protocol	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because the values in the protocol ID or protocol version ID fields were incorrect.
Invalid Type	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because they contained the wrong type value.
Invalid BPDU Length	Displays the number of STP, RSTP, and MSTP BPDUs the port has discarded because they were the wrong length.

Internet Group Management Protocol (IGMP)

To display the status of IGMP Snooping, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > IGMP.

    The IGMP Status page is displayed. See Figure 89.
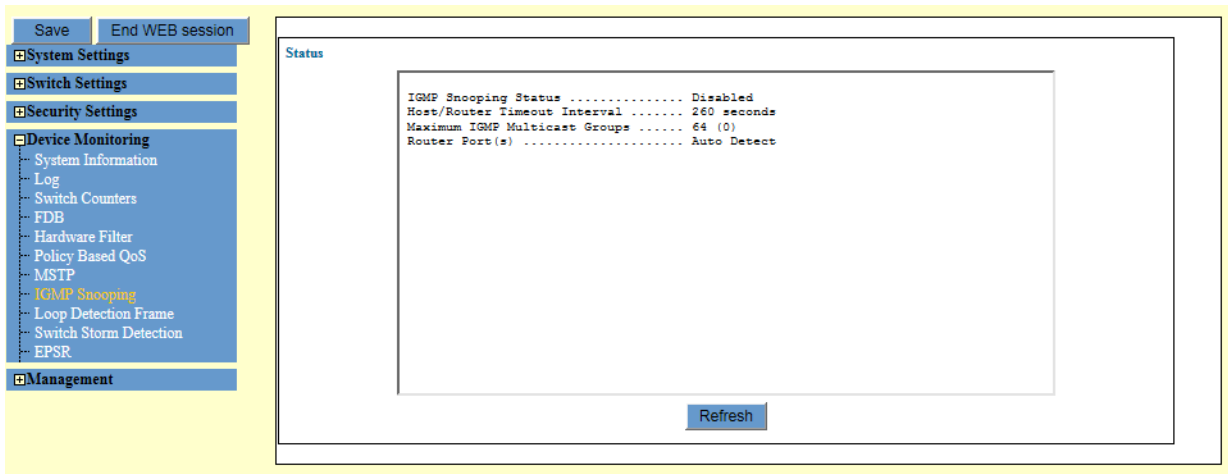
Figure 89. IGMP Status Page

2. Observe the fields described in Table 75.

Table 75. IGMP Status

Field	Description
IGMP Snooping Status	Displays the status of IGMP Snooping, either enabled or disabled.
Host/Router Timeout Interval	Displays the maximum amount of time that 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.
Maximum IGMP Multicast Groups	Displays the maximum number of IGMP multicast groups that switch can learn.

Table 75. IGMP Status

Field	Description
Router Port(s)	Displays the mode the switch is configured for router ports. The options are: ❒ Auto Detect: The switch automatically detects router ports. ❒ Select: Router ports are manually specified. ❒ None: Router ports are not specified.

3. Click **Refresh**, as needed.

Loop Detection Frame

To display the Loop Detection Frame statistics, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Loop Detection Frame.

   The Loop Detection Frame page is displayed. See Figure 90.

Figure 90. Loop Detection Frame Page

2. Observe the fields described in Table 76.

Table 76. Loop Detection Frame

Field	Description
Ports	Displays a port number and checkbox.
LDF send	Displays the number of Loop Detection Frames that the port has transmitted.
LDF receive	Displays the number of Loop Detection Frames that 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.
Discard	Displays the number of ingress Loop Detection Frames the port has discarded.

3. Click the following buttons as needed:

❑ **Clear counters —** Clears the statistics on the selected port(s).

❑ **Clear all port counters —** Clears the statistics for all of the ports.

❑ **Refresh —** Refreshes the display on this page.

Switch Storm Detection

To display statistics on Switch Storm Detection, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > Switch Storm Detection.

   The Switch Storm Detection Port list page is displayed. See Figure 91.

Figure 91. Switch Storm Detection Port List Page

2. Observe the fields described in Table 77.

Table 77. Switch Storm Detection

Field	Description
Port	Displays a port number and checkbox.
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.
Low Rate	Displays the number of times the port has detected a low packet rate threshold violation.

Table 77. Switch Storm Detection (Continued)

Field	Description
Acton	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. Click the following buttons as needed:

❐ **Clear counters —** Clears the statistics on the selected port(s).

❐ **Clear all port counters —** Clears the statistics for all of the ports.

❐ **Refresh —** Refreshes the display on this page.

Ethernet Protection Switching Ring (EPSR)

To display the EPSR status and statistics, perform the following procedure:

1. From the Navigation pane, go to Device Monitoring > EPSR.

   The EPSR Domain List page is displayed. See Figure 92.
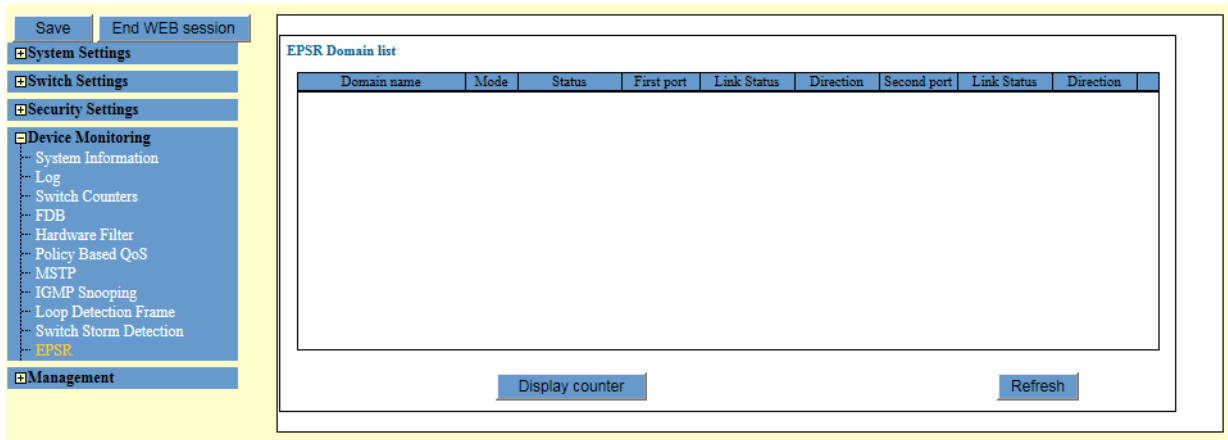
Figure 92. EPSR Domain List Page

2. Observe the fields described in Table 78.

Table 78. EPSR

Field	Description
Domain Name	Displays the name of the EPSR domain.
Mode	Displays the mode of the domain. The option is only Aware.
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.
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.

Table 78. EPSR (Continued)

Field	Description
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 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. Click the following buttons as needed:

   ❑ **Display Counter —** Displays EPSR packet counters.

   ❑ **Refresh —** Refreshes the display on this page.

4. If you click Display Counter, the Display EPSR Counters page is displayed.
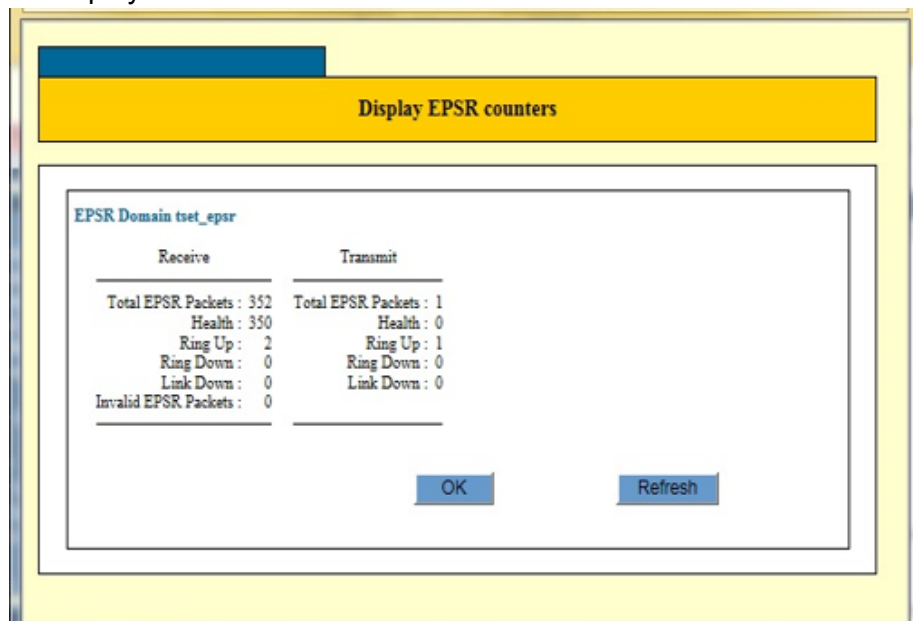
Figure 93. Display EPSR Counters

5. Observe the fields described in Table 79 on page 241.

Table 79. Display EPSR Counters

Name	Description
Receive	
Total EPSR Packets	The total number of the received EPSR control packets
Health	The number of the received Healthcheck messages
Ring Up	The number of the received Ring Up messages
Ring Down	The number of the received Ring Down messages
Link Down	The number of the received Link Down messages
Invalid EPSR Packets	The counter of invalid EPSR control packets
Transmit	
Total EPSR Packets	The total number of the Transmit EPSR control packets
Health	The number of the transmit Healthcheck messages (value is 0)
Ring Up	The number of the transmit Ring Up messages
Ring Down	The number of the transmit Ring Down messages (value is 0)
Link Down	The number of the transmit Link Down messages

Chapter 7
Management

This chapter contains the following sections:

Port Reset

Resetting a port clears the MAC address table for the port and deletes the port statistics counters.

To reset an individual port on the switch, perform the following procedure:

1. From the Navigation pane, go to Management > Port Reset.

    The Port Reset page is displayed. See Figure 94.
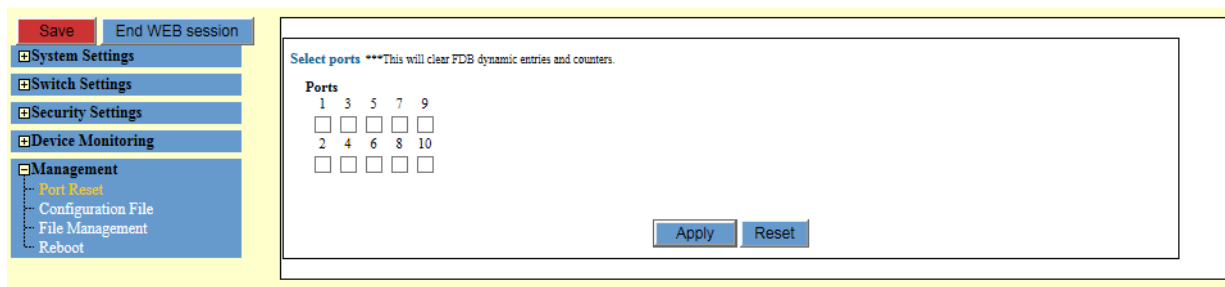
Figure 94. Port Reset Page

2. Check the checkbox of the port you want to reset.

    Note
    You many select multiple ports at a time.

3. Click **Apply**.

Configuration File

You can store multiple configuration files on the switch. You can specify one configuration file as the start-up configuration file, which the switch uses when it is rebooted. In addition, you can specify a new configuration file as the start-up file when you create it.

Note
To display, download, upload, or delete configuration files, go to "File Management" on page 249.

Displaying the Start-up and Current Configuration Files

To display the names of the start-up configuration file and the current configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95.

Figure 95. Configuration File Page

2. Observe the fields described in Table 80.

Table 80. Configuration File Properties

Field	Description
Start-up configuration file	Displays the name of the designated start-up configuration file of the switch.
Current configuration file	Displays the name of the configuration file that the switch is currently running on.

Designating an Existing Configuration File as the Start-up Configuration File

To designate a configuration file stored on the switch as the start-up configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95 on page 245.

2. In the Configuration file section, select a configuration file from the Change Start-up configuration file pull-down menu.

3. Click **Apply**.

   The existing configuration file is now designated as the start-up configuration file.

   Note
   To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

Saving the Running Configuration to the Start-up Configuration File

To save the running configuration, which the switch is currently running on, to the start-up configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95 on page 245.

2. In the Save configuration section, select the Save as start-up configuration file option.

3. Click **Save**.

   The running configuration is now designated as the start-up configuration file.

Saving the Running Configuration to the an Existing Configuration File

To save the running configuration to an existing configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95 on page 245.

2. In the Save configuration section, select the Save configuration to an existing file.

3. Select a configuration file name from the pull-down menu.

4. Click **Save**.

   The running configuration is now saved to the existing configuration file you selected.

Saving the Running Configuration as a New Configuration File

To save the running configuration as a new configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95 on page 245.

2. In the Save configuration section, select configuration to a new file.

3. Enter a file name of the new configuration file.

4. Click **Save**.

   The running configuration is now saved under the new configuration file name that you have entered.

Displaying the Running Configuration

To display the content of the running configuration, perform the following procedure:

1. From the Navigation pane, go to Management > Configuration File.

   The Configuration File is displayed. See Figure 95 on page 245.

2. In the Display configuration section, click **Display**.

   The switch displays the contents of the running configuration. See Figure 96 on page 248 as an example.
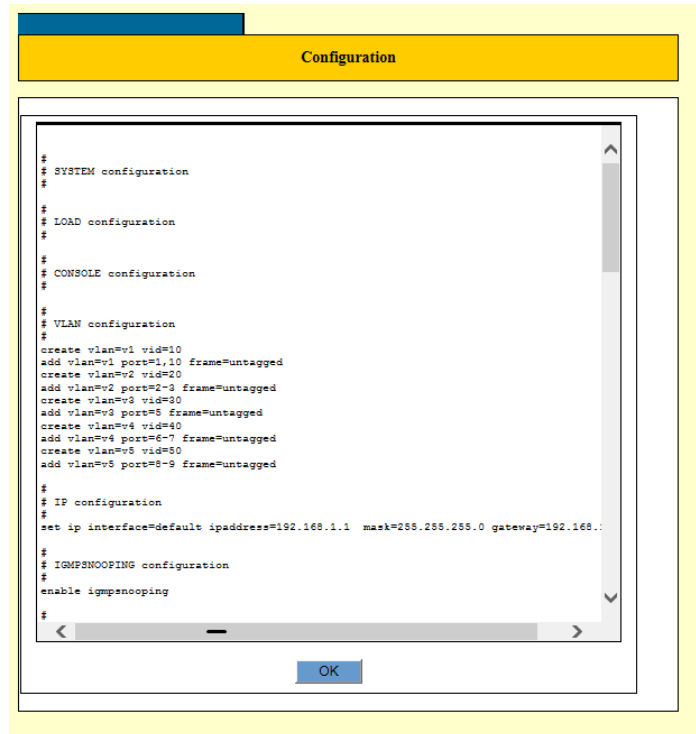
Figure 96. Running Configuration Window

3. Click **OK**.

File Management

The switch stores more than one configuration file. You can store a history of the parameter settings of the switch in case you need to return the unit to an earlier configuration. You can down load configuration files from the switch to your management workstation or a server, as well as upload files back to the switch.

In addition, the switch can store up to two firmware files. Allied Telesis periodically release new operating software for the switch and make it available to the customers on the company web site. You may download it onto your switch.

Displaying a List of Management Files on the Switch

To view a list of management files stored on the switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

   The File Management page is displayed. See Figure 97.

Figure 97. File Management Page

2. Observe a list of management files on the switch. The fields are described in Table 81.

Table 81. Configuration File Properties

Field	Description
File name	Displays the name of a management file.
Size	Display the size of a management file.
Created	Displays the date and time when the management file was created.
Attribute	Displays the attribute of the management file. The file extensions are: ❏ .rel - Firmware ❏ .cfg - configuration file

Uploading Configuration Files to the Management Workstation

To upload configuration files from the switch to your management workstation or network server, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

    The File Management page is displayed. See Figure 97 on page 249.

2. In the File List section, click the name of the configuration file to be uploaded to your management workstation.

    Note
    You many upload only one file at a time.

3. Click **Upload**.

    A confirmation prompt appears.

4. Click **OK**.

    The selected configuration file is uploaded from the switch to your management workstation or network server.

Downloading Configuration Files to the Switch

To download configuration files from the management workstation to the switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

    The File Management page is displayed. See Figure 97 on page 249.

2. In the Download File section, click **Browse** to locate and select the configuration file stored on your management workstation or network server.

Note
You may download only one file at a time.

---

3. Click **Download**.

The switch downloads the selected configuration file from your management workstation or network server to the file system on the switch.

4. To confirm the download, check for the name of the file in the File List section of the Management - File Management page.

Deleting Management Files from the Switch

To delete management files from the switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

The File Management page is displayed. See Figure 97 on page 249.

2. In the File List section, click the name of the management file to be deleted from the switch.

Note
You many upload only one file at a time.

---

3. Click **Delete**.

A confirmation prompt appears.

4. Click **OK**.

Designating the Active Configuration File

To designate the file as the start-up configuration file and configure the switch with the parameter settings in the configuration file, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

The File Management page is displayed. See Figure 97 on page 249.

2. Select the Configuration File option from the Management menu.

3. In the Configuration file section of the page, use the pull-down menu in the Change start-up configuration file to select the name of the file that you just downloaded onto the switch.

4. Click **Set**.

> **Note**
> Do *not* click the Save button. If you save the changes, the switch overwrites the settings in the downloaded configuration file with its current settings.
---

5. Form the Management menu, choose the Reboot option.

6. At the confirmation prompt, click **OK** to reboot the switch or **Cancel** to cancel designating the file as the active configuration file.

   The switch initializes its operating system and configures its parameter settings with the new active configuration file.

Deleting Firmware from the Switch

The file system in the switch can store up to two firmware files. When you have two firmware files on the switch, you must delete one before downloading new firmware to the switch.

To delete a firmware file from switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

2. In the File List section, click the name of the firmware file to be deleted from the switch.

> **Note**
> A firmware file has a .rel extension.
---

3. Click **Delete**.

   A confirmation prompt appears.

4. Click **OK**.

Downloading Firmware to the Switch

To download firmware from the management workstation to the switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

2. In the Download Firmware section, click **Browse** to locate and select firmware stored on your management workstation or network server.

Note
A firmware file has a .rel extension.

---

3. Select one of the following options:

   ❐ Set the downloaded firmware as boot firmware - Next time you reboot, the switch uses the new firmware to reboot.

   ❐ Reboot the switch after downloading the firmware - The switch immediately reboots with the new firmware.

4. Click **Download**.

Designating the Boot Firmware File

To change the current secondary firmware as the boot firmware for the switch, perform the following procedure:

1. From the Navigation pane, go to Management > File Management.

   The File Management page is displayed. See Figure 97 on page 249.

2. In the Update Firmware Information section, select the firmware you want to be the boot firmware from the pull-down list.

3. Click **Set**.

   Next time you reboot, the switch uses the firmware you just selected as the boot firmware.

Reboot

To reboot the switch, perform the following procedure:

Note
If you want to keep your changes, save them before rebooting the switch. To save your changes into a configuration file, click **Save**. For more information, see "Saving the Changes to a Configuration File" on page 21.

1. From the Navigation pane, go to Management > Reboot.

    The Reboot Confirmation Window appears. See Figure 98.
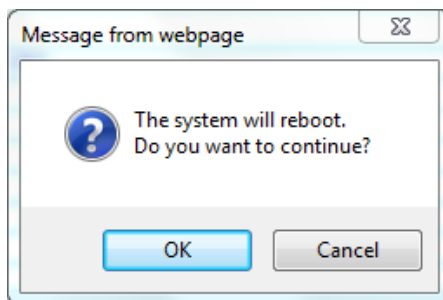
Figure 98. Reboot Confirmation Window

2. Click **OK**.

Appendix A

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 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 262.)

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 261.

❏ The switch can support up to a total of 4094 port-based, tagged, and protected ports VLANs.

❏ 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 261.

Port-based Example 1

Figure 99 illustrates an example of one switch with two VLANs, with the VIDs 10 and 20. The ports are untagged. Consequently, the PVIDs are the same as the VIDs. Both VLANs have one port connected to a router to provide communications between the VLANs as well as a link to the WAN.

Figure 99. Port-based VLAN - Example 1

Port-based Example 2

Figure 100 is an example of two port-based VLANs that span two switches. To prevent VLAN fragmentation, the parts of the VLANs are joined by dedicated, untagged links on the switches. Port 1 on each switch links VLAN 10 and Port 6 links VLAN20.

Switch A					Switch B								
Port	Type	VLAN ID	PVID		Port	Type	VLAN ID	PVID					
1	untagged	10	10	------	1	untagged	10	10					
2	untagged	10	10		2	untagged	10	10					
3	untagged	10	10		3	untagged	10	10					
4	untagged	10	10		4	untagged	10	10	-----	Router	---- WAN		
5	Untagged	20	20		5	Untagged	20	20	-----				
6	Untagged	20	20	- - - -	6	Untagged	20	20					
7	Untagged	20	20		7	Untagged	20	20					
8	Untagged	20	20		8	Untagged	20	20					
9	Untagged	default(1)	default(1)		9	Untagged	default(1)	default(1)					
10	Untagged	default(1)	default(1)		10	Untagged	default(1)	default(1)					

Figure 100. Port-based VLAN - Example 2

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 258, 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 258 and "VLAN Identifier" on page 258.

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 101 illustrates how tagged ports can be used to interconnect IEEE 802.1q-based products.

Switch A					Switch B							
Port	Type	VLAN ID	PVID		Port	Type	VLAN ID	PVID				
1	untagged	10	10		1	untagged	10	10				
2	untagged	10	10		2	untagged	10	10				
3	untagged	10	10		3	untagged	10	10				
4	untagged	10	10		4	untagged	10	10		Router	---- WAN	
5	Untagged	20	20		5	Untagged	20	20				
6	Untagged	20	20		6	Untagged	20	20				
7	Untagged	20	20		7	Untagged	20	20				
8	Tagged	10	10		8	Tagged	10	10				
		20					20					
9	Untagged	default(1)	default(1)		9	Tagged	10	10		Server		
10	Untagged	default(1)	default(1)				20					
					10	Untagged	default(1)	default(1)				

Figure 101. Example of a Tagged VLAN

This example is nearly identical to the "Port-based Example 2" on page 261. Tagged ports have been added to simplify network implementation and management.

One of the tagged ports is port 9 on the switch B. 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 both VLANs can access the server without going through a router or other interconnection device.

Figure 101 illustrates how tagged ports are also used to link the different parts of the VLANs on the two switches. Port 8 on each switch is a tagged member of both VLANs to enable it to carry traffic from both VLANs. The link provides a common connection that allows different parts of the same VLAN to communicate while maintaining data separation between VLANs.

In comparison, the two VLANs in the "Port-based Example 2" on page 261 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.

Protected Ports VLAN 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, see "Port-based VLAN Overview" on page 258 and "Tagged VLAN Overview" on page 262.

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 82 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 10.

Table 82. Example of a Protected Ports VLAN - Part I

Name	Reading_room
VID	8
Client Untagged Ports in VLAN	1-4
Client Tagged Ports in VLAN	none
Uplink Port(s)	10

Table 83 lists the different groups in the VLAN and the ports of the groups.

Table 83. Example of a Protected Ports VLAN - Part II

Client Port(s)	Group Number
1	1
2	2
3	3
4	4

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 for Uplink Port and Client Port

❒ A protected ports VLAN must 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 (all ports are same configuration; tagged or untagged).

❒ The range for the number of groups is 1 to 256 and each group must be assigned a unique group number on the switch.

❒ 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.

❒ When using multiple VLAN and tag VLAN, it is treated with multiple VLAN priority (this is limitation).

❒ When uplink port receives unicast packet, it is forwarded to an appropriate client port according to the address MAC address.

❒ When uplink port receives flooding packet, it is flooded to all client ports.

Appendix B

Rapid Spanning Tree Protocol Overview

This chapter provides background information on the Rapid Spanning Tree Protocol (RSTP). The sections in the chapter are listed here:

Overview

Spanning tree protocols are designed to detect and block loops in the wiring topology of a network. A data loop exists when two or more nodes can transmit data to each other over more than one data path in a network. Data loops can cause broadcast storms that can significantly reduce network performance. Where multiple paths exist, a spanning tree protocol places the extra paths in a standby or blocking mode by disabling ports, so that there is only one active path.

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

There are three versions of the protocol. They are listed here:

❐ Spanning Tree Protocol (STP) - This is the original version of the protocol.The switch does not come with this version; however, the RSTP and MSTP protocols have STP-compatible modes that makes them compatible with STP on legacy devices.

❐ Rapid Spanning Tree Protocol (RSTP) - This version of the protocol is described in this chapter. The instructions for configuring RSTP parameters are found in "Rapid Spanning Tree Protocol (RSTP)" on page 102.

❐ Multiple Spanning Tree Protocol - This version of the spanning tree protocol is intended for large networks. It allows you to group bridges into multiple spanning tree domains, which can increase the speed of the protocol in identifying and resolving loops in a network. Introductory information on the protocol can be found in Appendix C, "Multiple Spanning Tree Protocol Overview" on page 279. The instructions on how to configure the settings are found in "Multiple Spanning Tree Protocol (MSTP)" on page 110.

Note
For detailed information on the Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

Bridge Priority and the Root Bridge

The Rapid Spanning Tree Protocol designates one of the bridges as the root bridge. The root bridge distributes network topology information to the other network bridges and is used by the other bridges to search for redundant paths in the network topology.

A root bridge is selected by the *bridge priority* number, also referred to as the bridge identifier. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number of the switch. You can designate a switch as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge offline, and assign that bridge the second lowest bridge identifier number. The bridge priority has a range 0 to 61440 in increments of 4096.

Path Costs and Port Costs

After the root bridge is selected, the bridges determine if the network contains redundant paths and, if one is found, select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the root port.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by a determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed in the blocking state.

Path cost is determined by evaluating *port costs*. Every port on a bridge participating in the spanning tree protocol has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

The port cost of a port on the switch is adjustable. The range for RSTP is 0 to 20,000,000.

Port cost also has an Auto-Detect feature. This feature allows spanning tree to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting. Table 84 lists the RSTP port costs with Auto-Detect.

Table 84. RSTP Auto-Detect Port Costs

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

Table 85 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 85. 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.

Note
The AT-IA810M switch does not have ports that operate in 1000Mbps.

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 102 illustrates two switches that are connected with one data link of point-to-point ports operating in full-duplex mode.
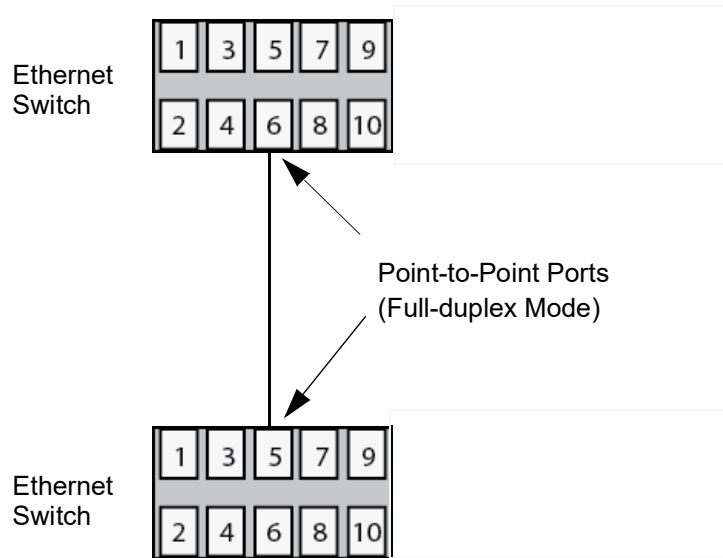
Figure 102. Point-to-Point Ports

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 103 on page 275 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.
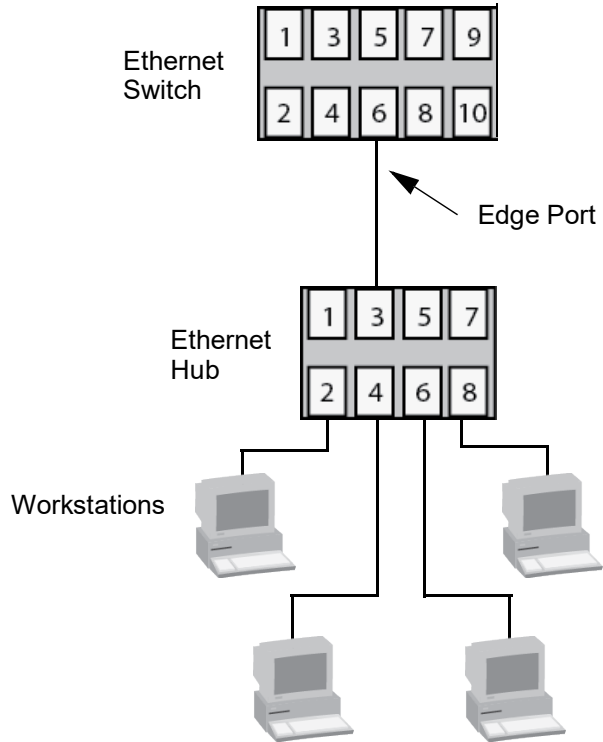
Figure 103. Edge Port

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 104 illustrates a port functioning as both a point-to-point and edge port.
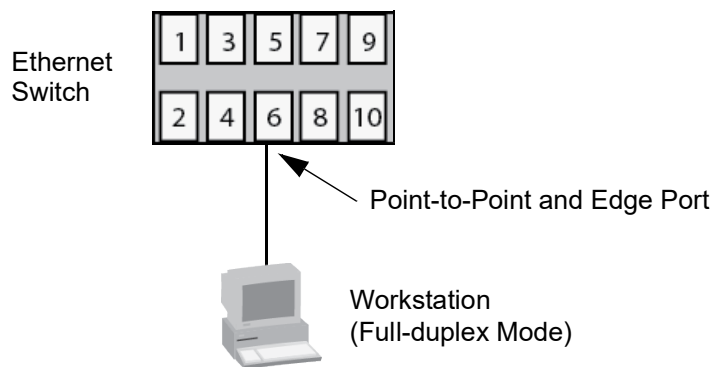
Figure 104. Point-to-Point and Edge Port

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 105. 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.

	SW A			SW B		
	Vlan(Vid)	port		port	Vlan(Vid)	
	sales(2)	1		1	sales(2)	
	sales(2)	2		2	sales(2)	
	sales(2)	3		3	sales(2)	
	sales(2)	4	-----------	4	sales(2)	
	prd(3)	5		5	prd(3)	
	prd(3)	6		6	prd(3)	
	prd(3)	7		7	prd(3)	
	prd(3)	8	-----------	8	prd(3)	
	default(1)	9		9	default(1)	
control vlan	default(1)	10		10	default(1)	control vlan
				port8-port8 : Blocked Data link		
				SW A port8 : Blocked port		

Figure 105. 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 "Tagged VLAN Overview" on page 262.

Appendix C
Multiple Spanning Tree Protocol Overview

This chapter provides background information on the Multiple Spanning Tree Protocol (MSTP). The sections in the chapter are listed here:

Overview

MSTP has the same function as RSTP, which is explained in Appendix B, "Rapid Spanning Tree Protocol Overview" on page 269. It searches for loops in the wiring topology of a network and, where loops exist, blocks bridge ports to prevent broadcast storms. MSTP differs from RSTP in that it lets you group the bridges of a network into multiple spanning tree domains. This can be useful in networks with large number of bridges because it enables the spanning tree protocol to react to and resolve loops more quickly than if all of the bridges are one domain.

The following sections describe some of the terms and concepts related to MSTP.

Note

Do not activate MSTP on the switch without first familiarizing yourself with the following concepts and guidelines. Unlike RSTP, you cannot activate this spanning tree protocol on the switch without configuring the protocol parameters.

Note

The MSTP implementation on the switch complies with the new IEEE 802.1s standard and is compatible with other vendors' compliant 802.1s implementations.

Multiple Spanning Tree Instance (MSTI)

The individual spanning trees domains in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). An MSTI can span any number of switches.

To create an MSTI, you assign it a number, referred to as the MSTI ID. The range is 1 to 15. (The switch is shipped with a default MSTI with an ID of 0. This default spanning tree instance is discussed later in "Common and Internal Spanning Tree (CIST)" on page 286.)

After selecting an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Here are the MSTI guidelines:

- ❐ The switch supports up to 16 spanning tree instances, including the CIST.
- ❐ An MSTI can contain any number of VLANs.
- ❐ A VLAN can belong to only one MSTI at a time.
- ❐ A switch port can belong to more than one spanning tree instance at a time by being an untagged and tagged member of VLANs belonging to different MSTIs. This is possible because a port can be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to "Ports in Multiple MSTIs" on page 281.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called associations. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTIs. In this circumstance, a port might have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port's MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set only once on a port and apply to all the MSTIs where the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to

multiple MSTIs, can have only one external path cost. Another generic parameter designates a port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI in which a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

Multiple Spanning Tree Regions

Another important concept of MSTP is regions. An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. The characteristics are listed here:

- ❒ Configuration name
- ❒ Revision number
- ❒ VLANs
- ❒ VLAN to MSTI ID associations

A configuration name is a name that identifies a region. You must assign each bridge in a region exactly the same name; even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The revision number is an arbitrary number assigned to a region. You might use this number to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that all of the bridges in a region have the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all of the bridges in a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP considers the bridges as residing in different regions.

Figure 106 on page 284 illustrates the concept of regions. It shows one MSTP region with two switches. The switches have the same configuration names and revision levels. They also have the same five VLANs and the VLANs are associated with the same MSTIs.

```
SW_A;IA810M ( 10port SW)

Configuration Name: fig_104_SWA.cfg

<Vlan>

default(VID=1);port1,2 untag port

(IP=192.168.1.20/24)

Sales(VID=2);port 3,4,9-10(tag)

Presales(VID=3);port 5,6,9-10(tag)

Accounting(VID=4);port 7,9-10(tag)


<MSTP>

Region

Revision Level: 1

VLAN to MSTI Associations:

MSTI ID 1

VLAN: Sales (VID 2)

VLAN: Presales (VID 3)

MSTI ID 2

VLAN: Accounting (VID 4)


point-to point ;port 9-10

SW_A is master
```

```
SW_B;IA810M ( 10port SW)

Configuration Name: fig_104_SWA.cfg

<Vlan>

default(VID=1);port1,2 untag port

(IP=192.168.1.25/24)

Sales(VID=2);port 3,4,9-10(tag)

Presales(VID=3);port 5,6,9-10(tag)

Accounting(VID=4);port 7,9-10(tag)


Region

Revision Level: 1

VLAN to MSTI Associations:

MSTI ID 1

VLAN: Sales (VID 2)

VLAN: Presales (VID 3)

MSTI ID 2

VLAN: Accounting (VID 4)


point-to point ;port 9-10
```

Figure 106. Multiple Spanning Tree Region

The switch determines regional boundaries by examining the MSTP BPDUs it receives on the ports. A port that receives an MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for ports connected to bridges running STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a regional root. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root of an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the MSTI priority value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used to determine the regional root of a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority; from 0 to 61,440 in sixteen increments of 4,096.

Region Guidelines

Here are the guidelines for regions.

- A network can contain any number of regions and a region can contain any number of switches.
- A switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.
- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- The regional root of an MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs you create yourself. First, you cannot delete this instance or change its MSTI ID. Second, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The default VLAN is also associated by default with CIST.

Another important difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP bridges in a network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and STP and RSTP bridges, to form one spanning tree for the entire bridged network.

MSTP uses CIST to form the spanning tree of an entire bridged network because CIST can cross regional boundaries, while an MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and STP and RSTP bridges in the bridged network.

The CIST regional root is set with the CIST Priority parameter. This parameter, which functions similar to the RSTP bridge priority value, selects the root bridge for the entire bridged network. If the switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP bridges in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on the switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of an MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all of the rules and guidelines mentioned in earlier sections, and provides a few new ones:

❏ The switch can support up to 16 spanning tree instances, including the CIST.

❏ An MSTI can contain any number of VLANs.

❏ A VLAN can belong to only one MSTI at a time.

❏ An MSTI ID can be from 1 to 15.

❏ The CIST ID is 0. You cannot change this value.

❏ A switch port can belong to more than one spanning tree instance at a time. This allows you to assign a port as an untagged and tagged member of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.

❏ A router or Layer 3 network device is required to forward traffic between VLANs.

❏ A network can contain any number of regions and a region can contain any number of switches.

❏ The switch can belong to only one region at a time.

❏ A region can contain any number of VLANs.

❏ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.

❏ An MSTI cannot span multiple regions.

❏ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.

❏ The regional root of an MSTI must be in the same region as the MSTI.

❏ The CIST must have a regional root for communicating with other regions and single-instance spanning trees.

❏ MSTP is compatible with STP and RSTP.

❏ A port transmits CIST information even when it is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in "Associating VLANs to MSTIs" on page 290.

Note

The MSTP implementation on the switch complies with the IEEE 802.1s standard and is compatible with similar products from other vendors, provided that their products are also compliant with the standard.

Associating VLANs to MSTIs

Allied Telesis, Inc. recommends that you assign all of the VLANs on the switch, including the default VLAN, to an MSTI. You should not leave VLANs assigned to only the CIST. This is to prevent the switch from blocking ports that should be in the forwarding state. The reason for this guideline is explained here.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all of the ports belong to the CIST instance. So CIST is included in the BPDU. If a port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is illustrated in Figure 107. Port 10 in switch A is a member of a VLAN assigned to MSTI ID 7 while port 9 is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 10 to switch B indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from port 9 indicates the port is a member of the CIST and MSTI 10.

		Mater			Back up		
	IP=192.168.1.20	<SW_A>			<SW_B>	IP=192.168.1.25	
connected	Vlan(VID)	port			port	Vlan(VID)	connected
PC_1	default(1)	1			1	default(1)	PC_2
	default(1)	2 -----------	-----------		2	default(1)	
PC_A_1	sales(2)	3			3	sales(2)	PC_B_1
PC_A_2	sales(2)	4			4	sales(2)	PC_B_2
PC_A_3	presale(3)	5			5	presale(3)	PC_B_3
PC_A_4	presale(3)	6			6	presale(3)	PC_B_4
PC_A_5	Accounting(4)	7			7	Accounting(4)	PC_B_5
	default(1)	8			8	default(1)	default(1)
	tagged vid=2,3,4	9 -----------	-----------		10	tagged vid=2,3,4	
	tagged vid=2,3,4	10 -----------	-----------		9	tagged vid=2,3,4	

port9 on SW_A --> port10 on SW_B : Instances: CIST 0 and MSTI 10
port10 on SW_A --> port9 on SW_B : Instances: CIST 0 and MSTI 10

Figure 107. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When switch B receives a packet from switch A, it uses MSTI, not CIST, to determine whether a loop exists. And because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise if you assign some VLANs to MSTIs while leaving others only in CIST. The problem is illustrated in Figure 108 on page 291. The network is the same as the previous example. The difference is that the VLAN containing port 8 on Switch A has not been assigned to an MSTI, and belongs only to CIST with its MSTI ID 0.

		Mater			Back up		
	IP=192.168.1.20	<SW_A>			<SW_B>	IP=192.168.1.25	
connected	Vlan(VID)	port			port	Vlan(VID)	connected
PC_1	default(1)	1			1	default(1)	PC_2
	default(1)	2	-----------	-----------	2	default(1)	
PC_A_1	sales(2)	3			3	sales(2)	PC_B_1
PC_A_2	sales(2)	4			4	sales(2)	PC_B_2
PC_A_3	presale(3)	5			5	presale(3)	PC_B_3
PC_A_4	presale(3)	6			6	presale(3)	PC_B_4
PC_A_5	Accounting(4)	7			7	Accounting(4)	PC_B_5
	default(1)	8			8	default(1)	default(1)
	tagged vid=2,3,4	9	-----------	-----------	10	tagged vid=2,3,4	
	tagged vid=2,3,4	10	-----------	-----------	9	tagged vid=2,3,4	

port9 on SW_A --> port10 on SW_B : Instances: CIST 0 and MSTI 10
port10 on SW_A --> port9 on SW_B : Instances: CIST 0

Figure 108. CIST and VLAN Guideline - Example 2

When port 9 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST. Therefore, switch B uses CIST to determine whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block a port to block the loop.

To avoid this issue, always assign all of the VLANs on the switch, including the Default VLAN, to MSTIs. This guarantees that all of the ports on the switch have an MSTI ID and ensures that loop detection is based on the MSTIs and not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when you connect different MSTP regions or an MSTP region and an STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANS of your network.

As mentioned previously, only the CIST can span regions. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 109. The example shows two switches that reside in different regions. Port 9 in switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 10 is a tagged and untagged member of three different VLANs, all associated to MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop

exists between the regions, and Switch B would block a port.

	IP=192.168.1.20	<SW_A>			<SW_B>	IP=192.168.1.25	
connected	Vlan(VID)	port			port	Vlan(VID)	connected
PC_1	default(1)	1			1	default(1)	PC_2
	default(1)	2 ----------		----------	2	default(1)	
PC_A_1	sales(2)	3			3	sales(2)	PC_B_1
PC_A_2	sales(2)	4			4	sales(2)	PC_B_2
PC_A_3	presale(3)	5			5	presale(3)	PC_B_3
PC_A_4	presale(3)	6			6	presale(3)	PC_B_4
PC_A_5	Accounting(4)	7			7	Accounting(4)	PC_B_5
PC_A_5	Marketing(5)	8			8	default(1)	default(1)
	Accounting(4)	9 ----------		----------	10		
	untag 2/ tagged 3,5	10 ----------		----------	9		
			Resion1	Resion2			

port9 on SW_A	:MSTI 4 VLAN (untagged) port: Accounting
port10 on SW_A:	MSTI 12 VLAN (untagged port): Sales VLAN (tagged port): Presales VLAN (tagged port): Marketing

Figure 109. Spanning Regions - Example 1

There are several ways to address this issue. One way is to have only one MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. Those VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Assume that you have two regions that contain the following VLANS:

Region 1 VLANs
Sales
Presales
Marketing
Advertising
Technical Support
Product Management
Project Management
Accounting

Region 2 VLANs
Hardware Engineering
Software Engineering
Technical Support
Product Management
CAD Development
Accounting

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You could group those VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. After they are grouped, you can connect the VLANs across the regions using a link of tagged ports.