SW24MGSFP

10/100/1000 Mbps + 2 Gb SFP

Web Smart Ethernet Switch

User Manual

Version 1.0 (January 2011)

TABLE OF CONTENTS

PACKING LIST

Before you start to install the SW24MGSFP Ethernet Switch, make sure the package contains the following items:

1. Ethernet switch	
2. Mounting hardware (2 “L” brackets and 8 screws)	
3. Four rubber feet	
4. Console cable	

5. Power cable	
6. User's manual CD	

PRODUCT OVERVIEW

Features

- Complies with IEEE802.3, IEEE802.3u and IEEE802.3ab standards
- Twenty-four 10/100/1000 Mb auto-negotiation RJ45 ports supporting Auto-MDI/MDIX
- Two 1000 Mb fiber SFP (Mini GBIC) interfaces that multiplex with RJ45 port 1 and port 2, with higher priority than RJ45 port 1 and port 2
- Supports IEEE802.3x flow control for full-duplex, backpressure flow control for half-duplex
- Up to 48 Gbps backplane bandwidth with support for non-blocking wire-speed forwarding
- Store and forward architecture and integrated 8K MAC address table
- Supports up to 24 VLAN groups for 802.1q VLAN
- Supports up to 24 trunks with up to 16 ports in a trunk
- Supports IGMP(Internet Group Management Protocol)
- Supports SNMP(v1,v2)
- Supports port bandwidth control
- Supports QoS (Quality of Service)
- Supports port-based access control (IEEE 802.1X)
- Supports source IP filter per port to block unwanted access
- Supports broadcast storm smart control
- Supports port mirror
- Support Web Smart and console manager
- Supports HTTP switch system software upgrading, configuration file, backup and reset function
- Supports circuit diagnoses
- Supports flow statistic function, dynamic display switch port receiving - transferring data package situation
- Standard 19" rack mount (1U) steel case with internal power supply

HARDWARE INSTALLATION

Location

Choose a suitable location for the rack mountable switch, considering the following requirements:

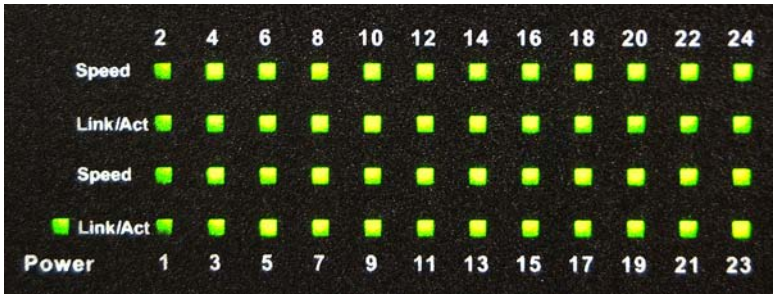
- Suitable power source
- Keep it away from heat sources and sunlight
- Keep it away from electromagnetic interference
- Allow 10 cm space above the unit for good ventilation

Installation

1. Remove the backing paper from the rubber feet and stick one in each of the indicated locations on the bottom of the switch.

2. Attach the “L” brackets to the front corners of the switch using the mounting screws.

3. Place the switch in a standard EIA 19" rack. Adjust the mounting brackets so the holes align with the mounting holes in the rack and fasten the switch to the rack (NOTE: screws are not provided with the switch for this purpose).
4. Plug the power cable into the socket at the rear of the switch and an appropriate power source. The switch will adjust the input voltage automatically within the input range indicated on the rear panel.
5. The switch performs a self-test (all LED indicators on the status panel flash then sweep from left to right).



When the lights turn off, the test is finished and the switch is ready for use.

6. To connect data sources, plug one end of an Ethernet cable into one of the numbered RJ45 ports of the switch and connect the other end to the source. Category 3, 4 or 5 cables can be used, however Category 5 is recommended.

Caution: Do not connect a phone line to the RJ-45 port; phone signals will damage the unit.

LED Indicators

When the power to the switch is on, the following indicators show system status:

LED	Status	Indication
Power	On	Power on
	Off	Power Off
Link/Act	On	Port connected
	Off	Port not connected
	Flashing	Data frames transmitting
Speed	On	Transmission rate 1000 Mbps
	Off	Transmission rate 10/100 Mbps

CONFIGURATION

Connection

1. Connect a standard Ethernet cable between any of the numbered ports on the switch and the Ethernet connector of the PC that will be used to configure the switch parameters.

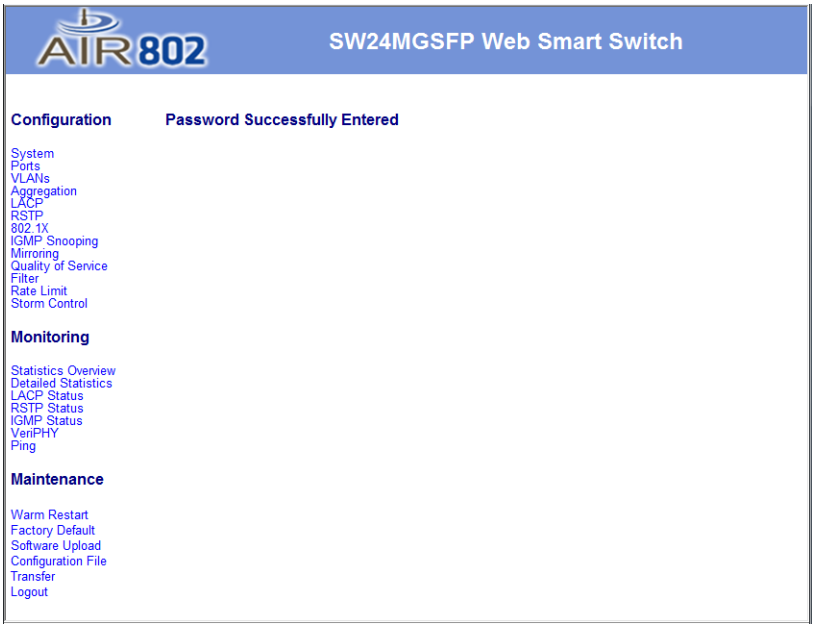
   NOTE: Do not connect the Ethernet cable to the Console port on the front of the switch. The Console port is used for a serial connection only (see Command Line Interface section).

2. Set the network configuration of the PC to any static IP address on the 192.168.2.x subnet except 192.168.2.1 and set the subnet mask to 255.255.255.0.

   NOTE: The Ethernet interface of the PC used to configure the switch must be set to a static IP address on the 192.168.2.x subnet. The default IP address of the switch is 192.168.2.1.

3. Open a Web browser and enter the address http://192.168.2.1. The switch's login window appears.

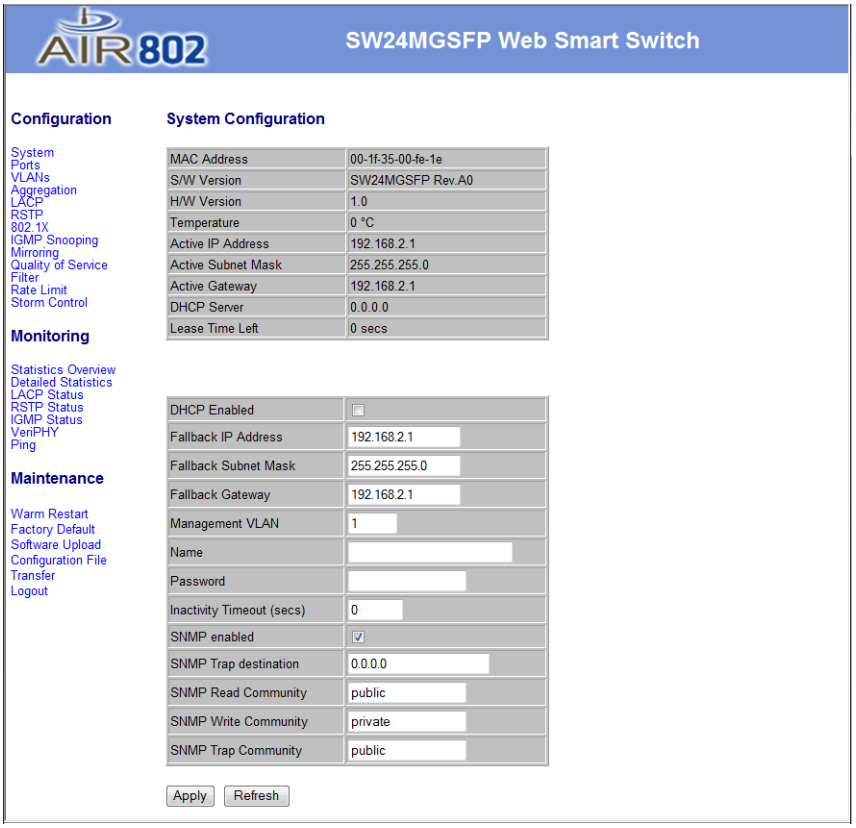
Enter the password for the switch (the default for a new switch is no password, leave the password field blank). Click **Apply**. The configuration window appears.



The system configuration options are listed in the Configuration menu at the left side of the screen. Click on a menu item to open the corresponding configuration screen.

The following sections explain these options.

System



This screen displays the current status of the following:

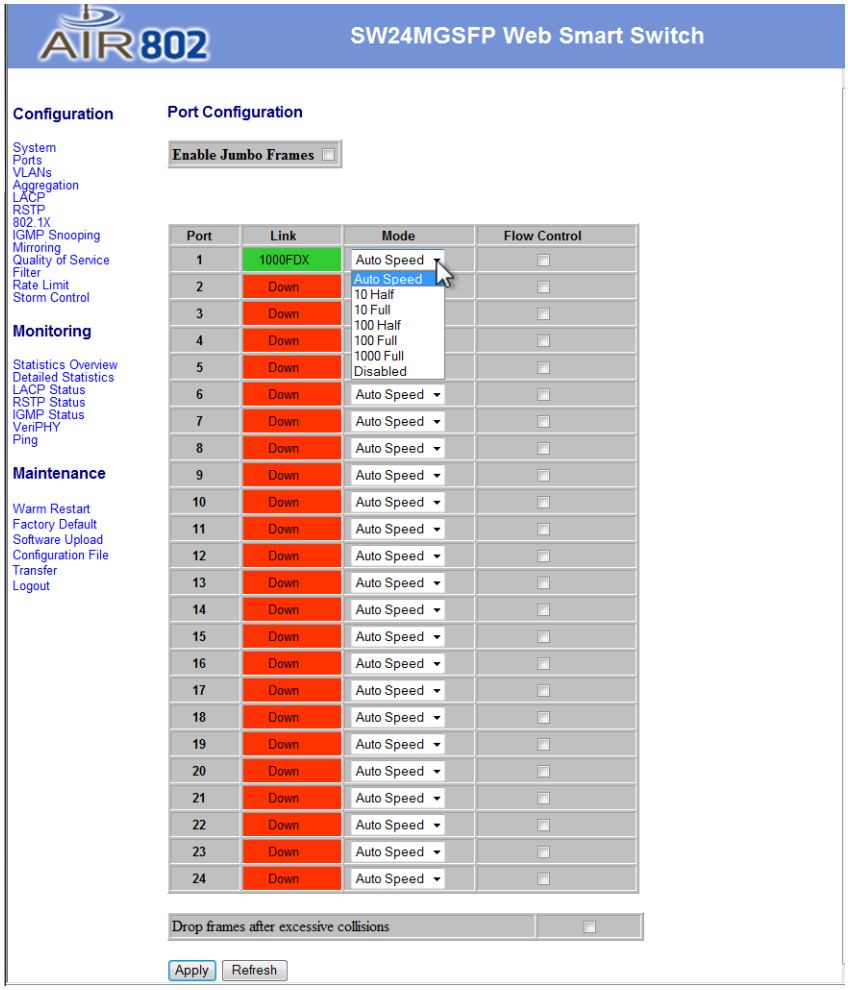
- MAC address: Display the current switch MAC address.
- Software Version: Display the switch software version.
- Hardware Version: Display the switch hardware version.
- Temperature: This item is non-functional.
- Active IP Address: 192.168.2.1 (default)
- Active Subnet Mask: 255.255.255.0 (default)
- Active Gateway: 192.168.2.1 (default)
- DHCP Server：0.0.0.0 (default)
- Lease Time Left：0 (default)

It also shows the current settings for the following.

- DHCP Enabled
- Fallback IP Address
- Fallback Subnet Mask
- Fallback Gateway
- Management VLAN
- Name
- Password
- Inactivity Timeout (secs)
- SNMP enabled
- SNMP Trap destination
- SNMP Read Community
- SNMP Write Community
- SNMP Trap Community

To change a setting, click the check box or enter a new value in the text box.

Ports

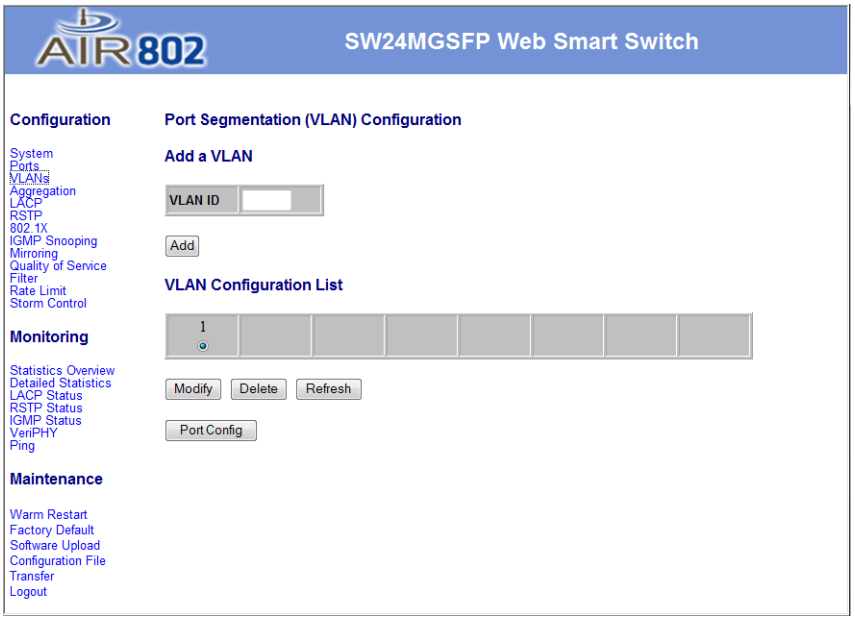


The Ports screen displays the status of each input port Link (active connection with green background, port Down by red background).

To set the operating Mode for individual ports, click the arrow at the right side of the selection box and choose a setting: Auto Speed (default), 10M half-duplex, 10M full-duplex, 100M half-duplex,100M full-duplex, 1000M full-duplex, or Disabled.

To enable or disable flow control, click the check box to enter a check mark (Enabled) or remove the check mark (Disabled).

VLAN

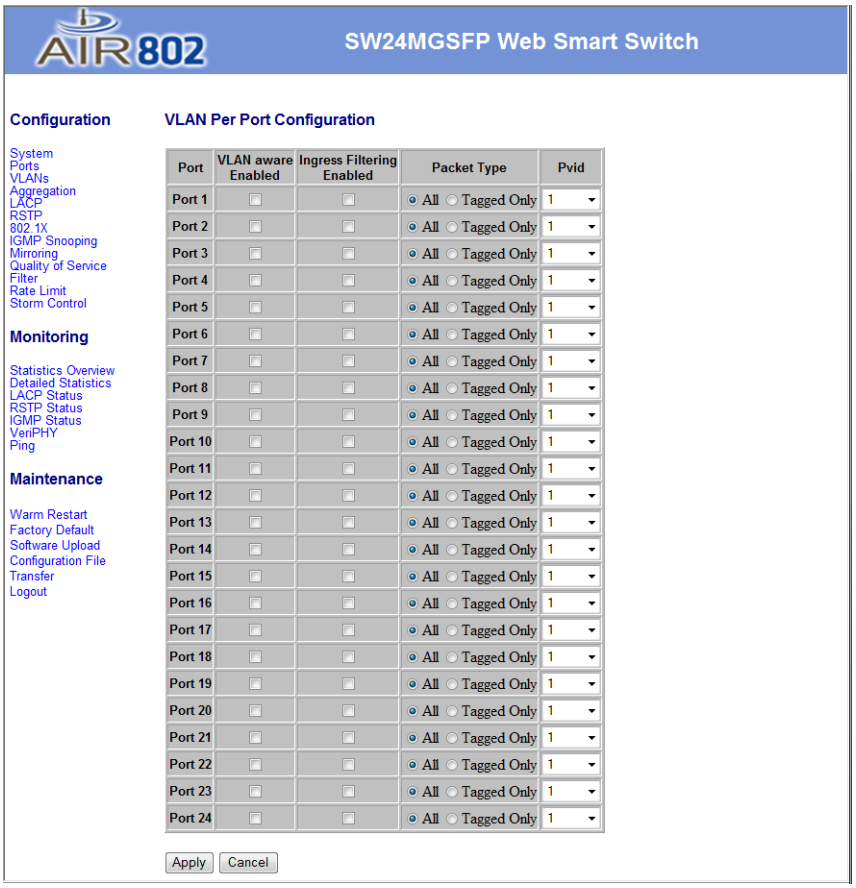


The VLAN screen allows configuration of up to 24 VLAN groups for 802.1q VLAN.

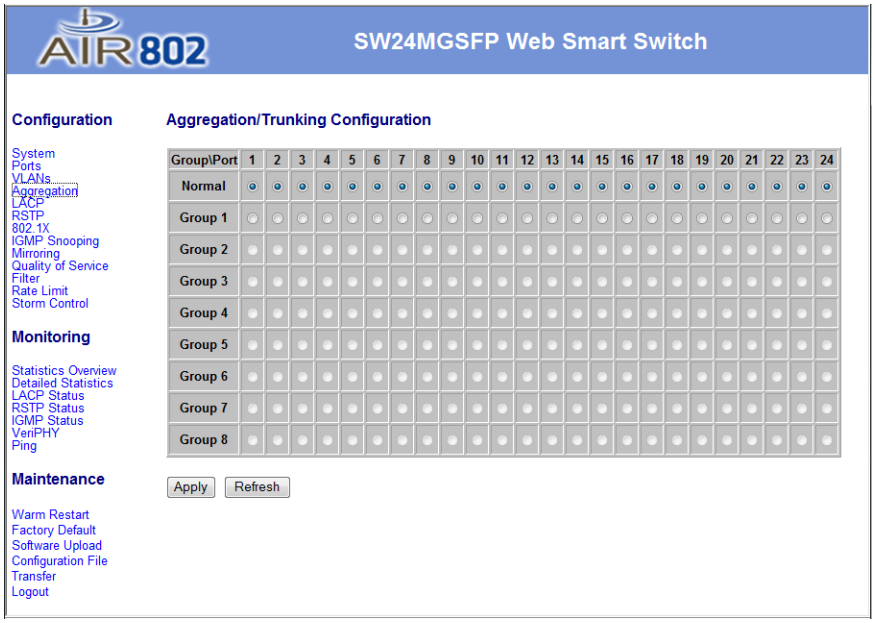
To add a VLAN, enter an ID for the group and click **Add**. Click the selection box beside each port to be added to the group to place a check mark in the box, then click **Apply**.

To **Modify**, **Delete**, or **Refresh** a group, click the button below the group and then click the button for the required action.

To configure individual VLAN ports, click **Port Config**.



Aggregation

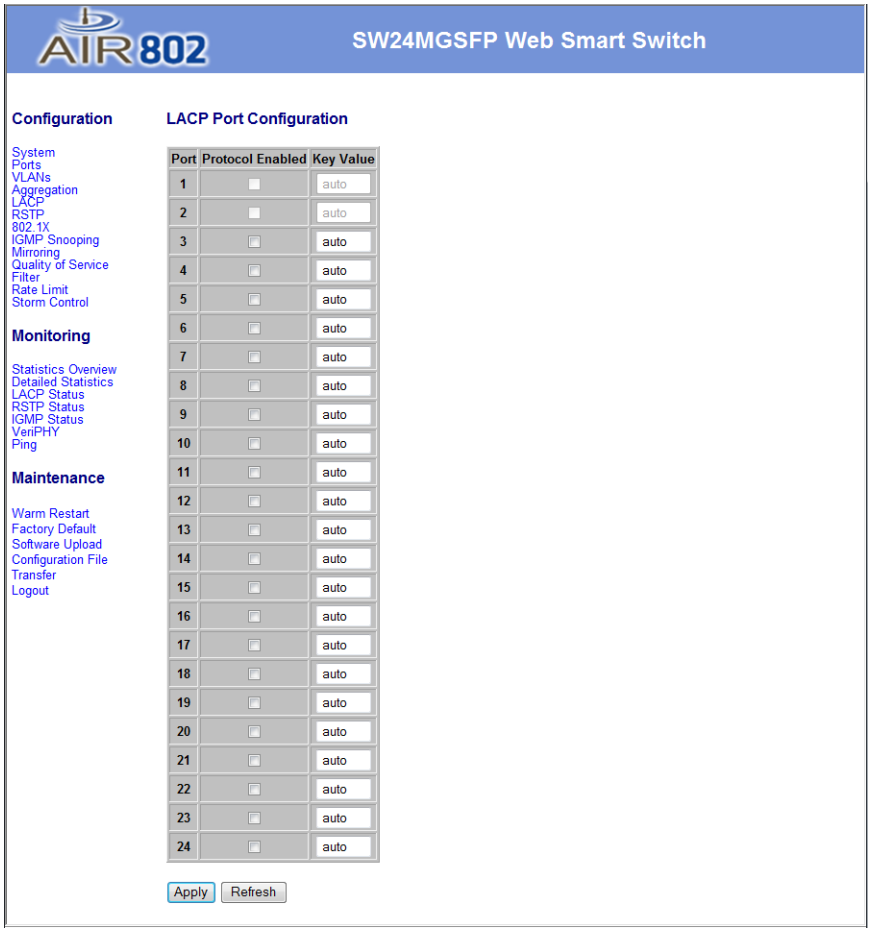


Link aggregation or “trunking” allows use of multiple network ports in parallel to increase the link speed beyond the limits of a single port and increases redundancy for higher availability.

To create a trunk group, click the button corresponding to each port to be added to the group, then click **Apply**.

NOTE: A trunk group cannot span the VLAN; all the trunk members must be in the same VLAN. Two trunk groups cannot be connected together and two switches cannot be connected by two trunk passages. These will make the network cycle and stop the network.

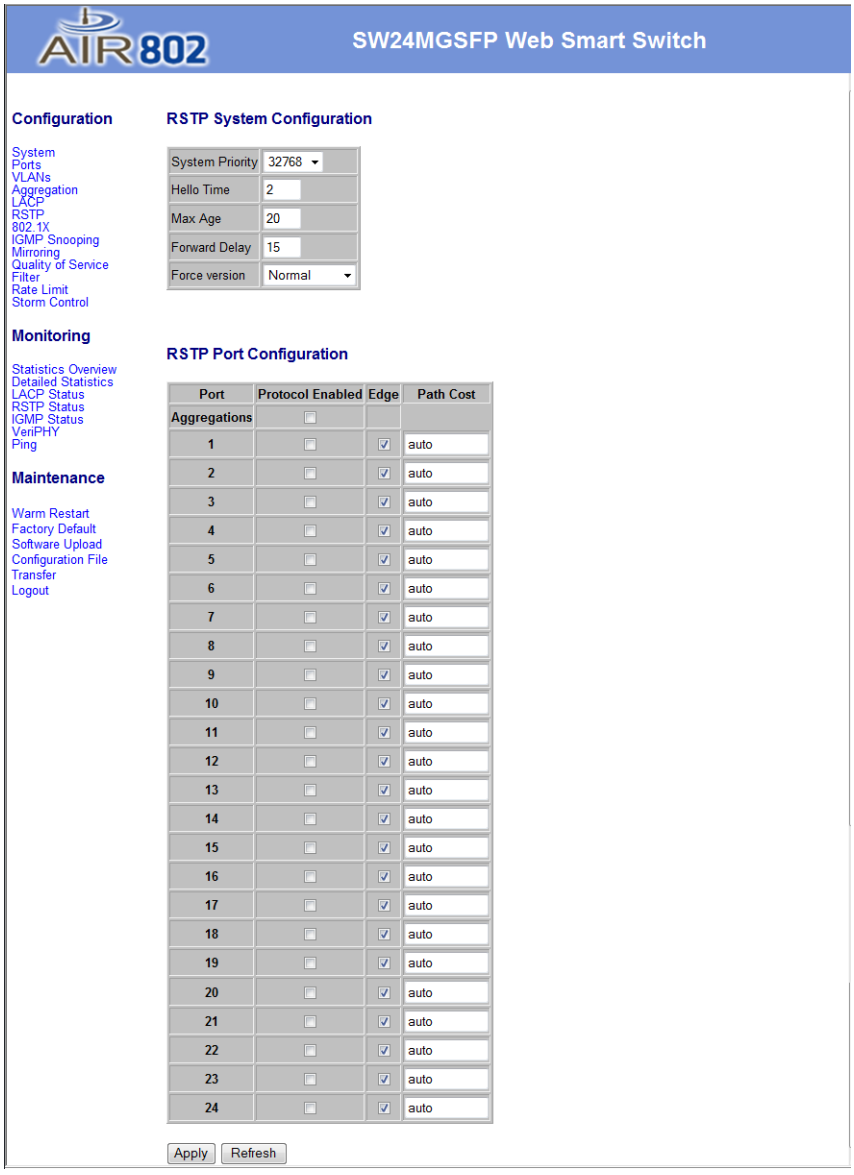
LACP



LACP (IEEE 802.3ad Link Aggregation Control Protocol) allows automatic aggregation between switches. It negotiates automatic bundling of links by sending LACP packets to the peer.

Click the check box beside each port to be enabled for LACP to place a check mark in the box, then click **Apply**. To disable LACP, click check boxes to remove the check mark, then click **Apply**.

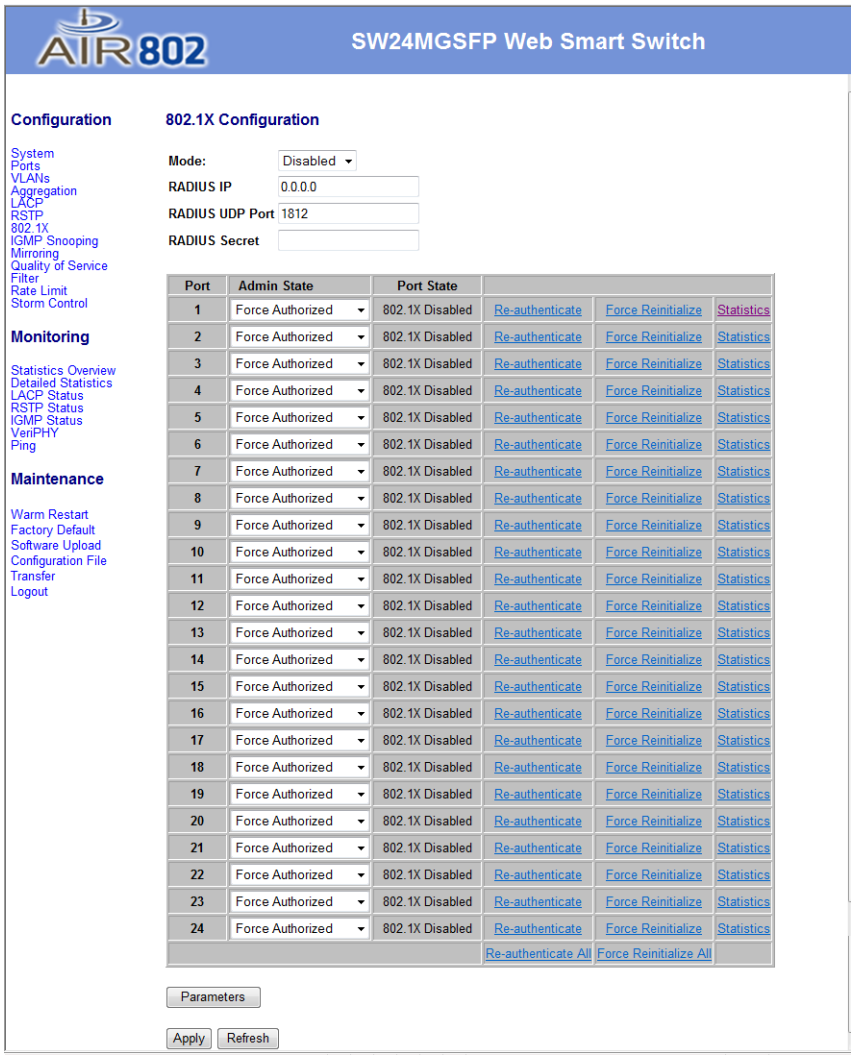
RSTP



RSTP (Rapid Spanning Tree Protocol) is a network protocol that prevents bridge loops in the network and creates spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops or the need for manual enabling/disabling of these backup links.

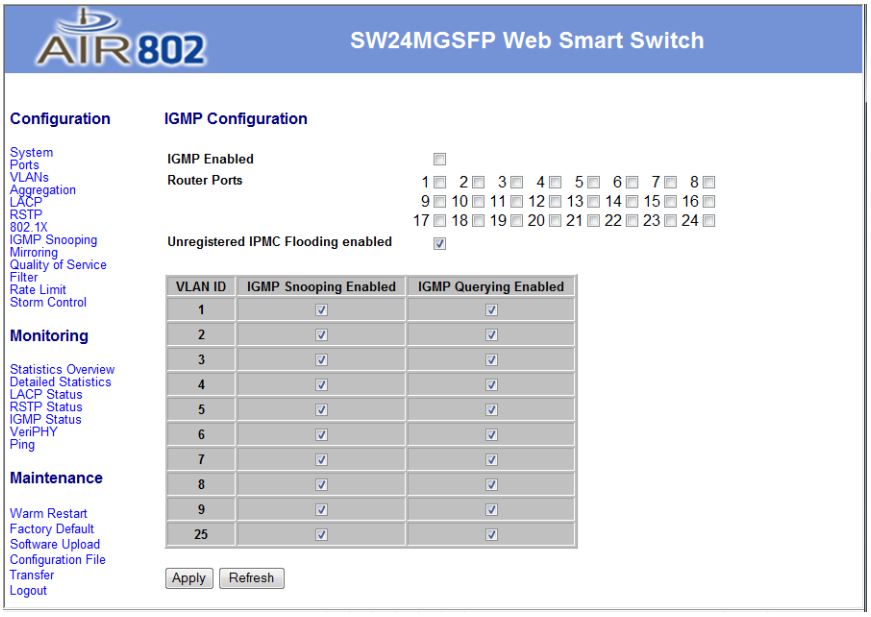
If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Click the check box to add a check mark.

802.1x



This screen displays and allows configuration of 802.1X processes for each port of the switch.

IGMP Snooping

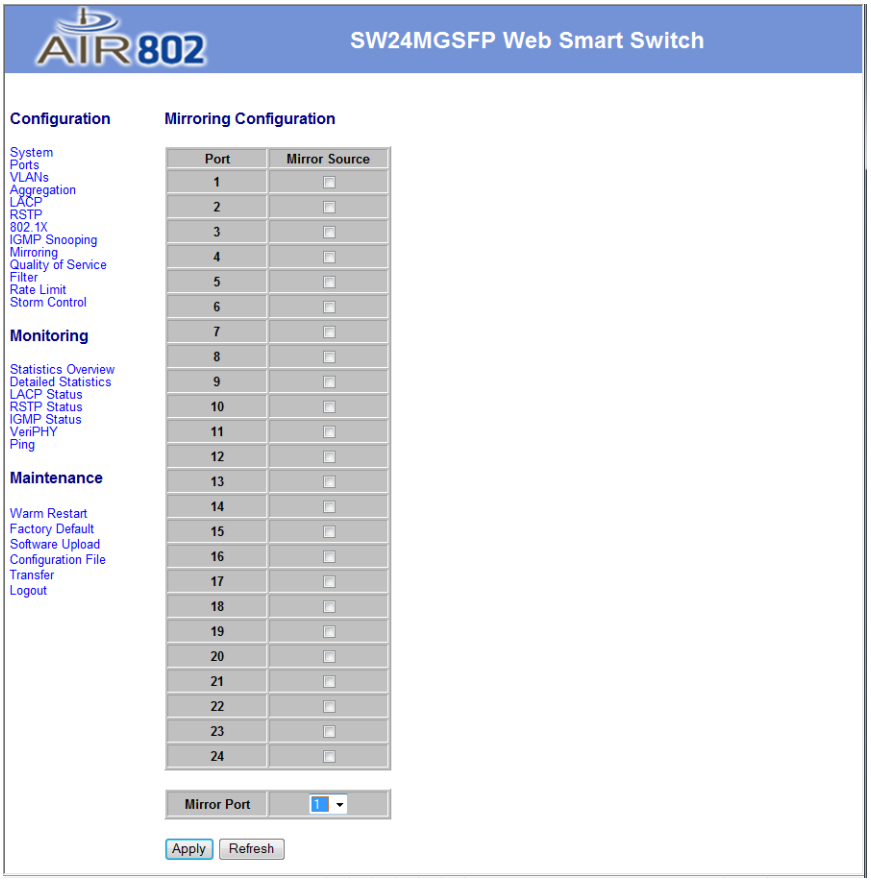


IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic in order to prune multicast traffic from links that do not contain a multicast listener (an IGMP client), preventing unnecessary load on host devices.

When enabled, IGMP snooping will function in each statically defined VLAN (i.e., VLANs stored in non-volatile configuration memory). The IGMP snooping module listens to IP multicast router IGMP queries and IGMP reports from hosts, and updates the switch device MAC table with IP multicast group MAC addresses and port masks according to the received reports. If no IP multicast router is present in an IGMP enabled VLAN, the switch will perform the querying itself in that particular VLAN.

The switch querying functionality can be enabled and disabled per VLAN. The switch must be setup for IP management in order for the querying to work.

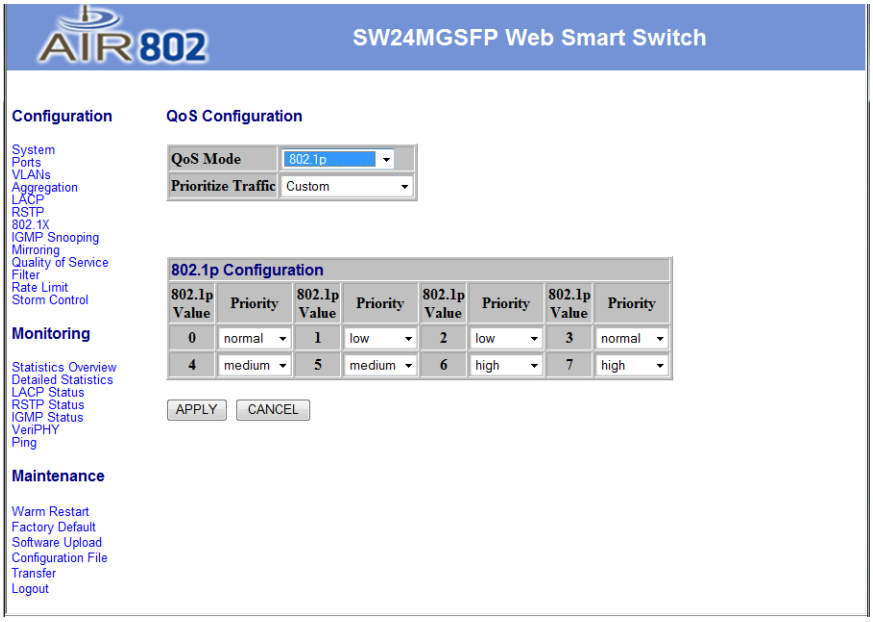
Mirroring

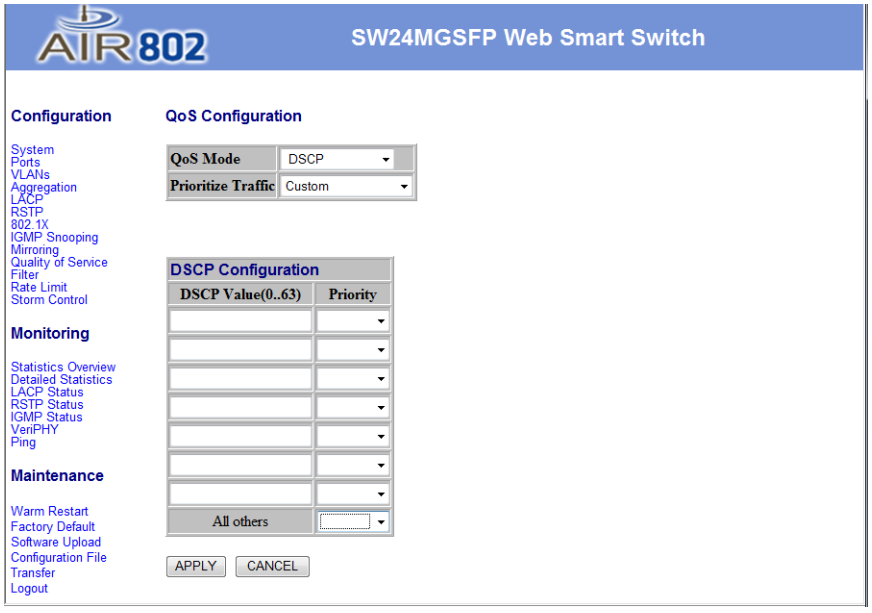


Port mirroring sends a copy of network packets seen on one switch port to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Monitor port bandwidth should be greater than or equal to the monitored port bandwidth.

Quality of Service

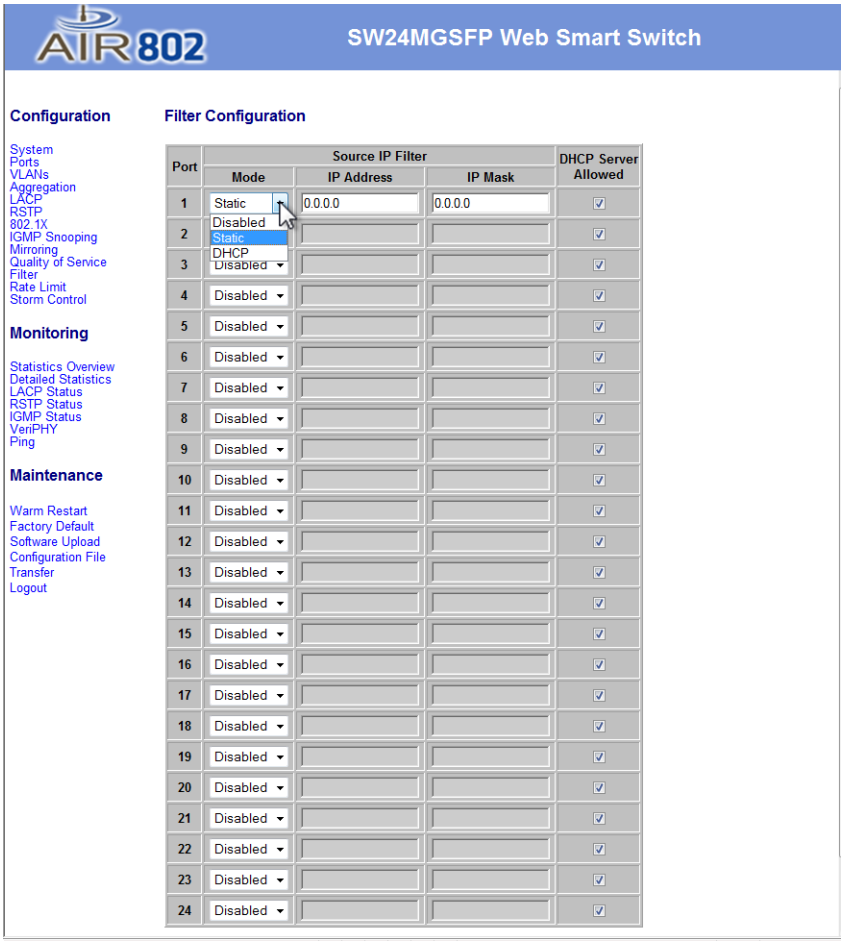




Quality of Service (QoS) allows prioritization of network traffic elements to guarantee the bandwidth relationship between individual applications or protocols.

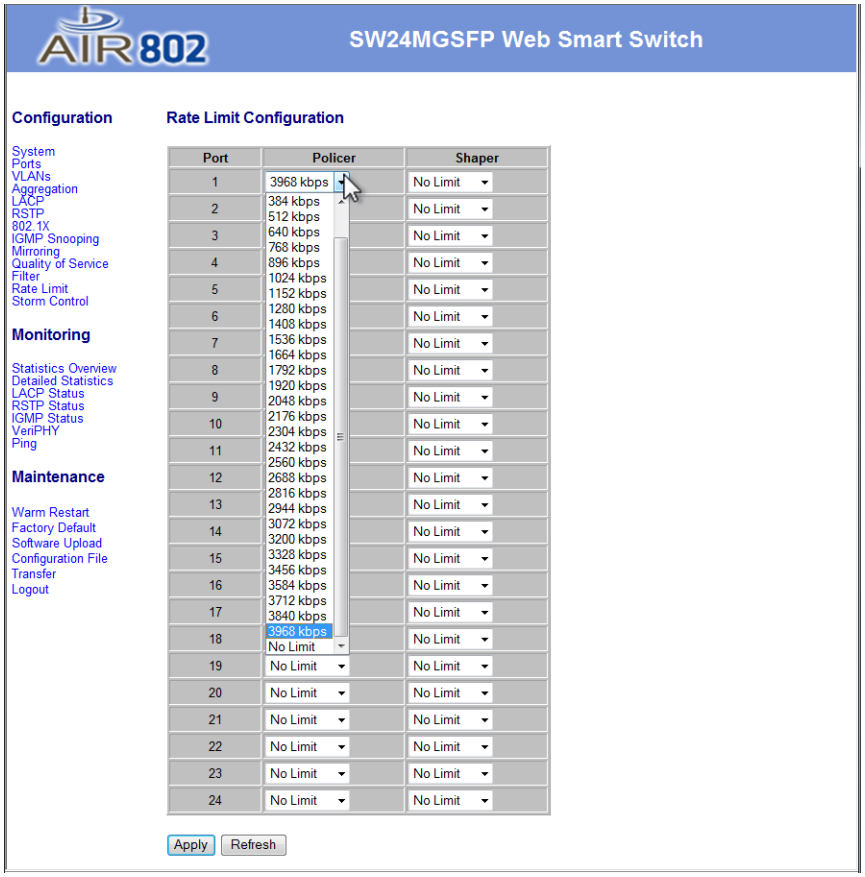
Select either **802.1p** or **DSCP** (Differentiated Services Code Point) mode from the QoS Mode drop-down box, enter settings as required, then click **APPLY**.

Filter



Filter lets you set a Source IP filter for any port to block unwanted access. Select either Static or DHCP Mode from the drop-down box. If you select Static Mode, enter the IP Address and IP Mask in the appropriate areas.

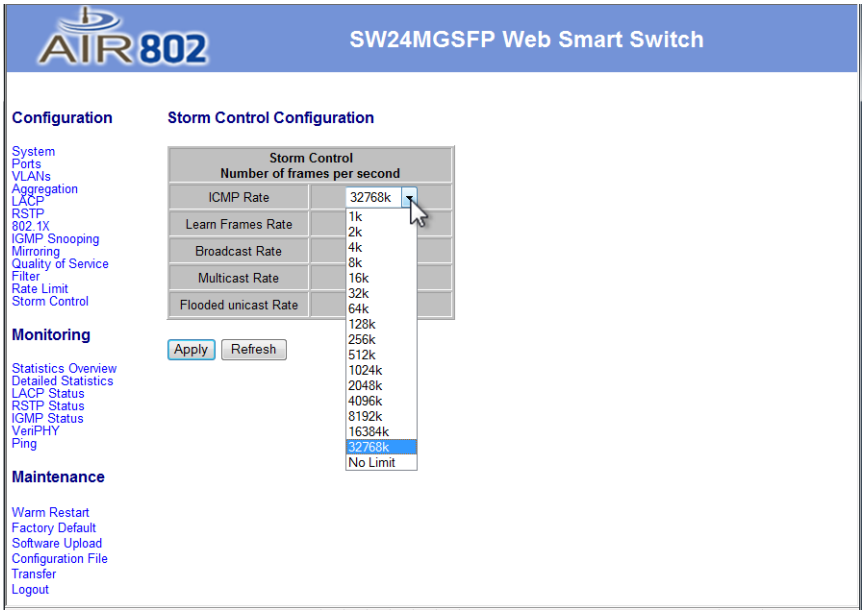
Rate Limit



Rate limits are used to control the transmit rate at which traffic enters and exits the switch ports to prevent ports from occupying too much bandwidth.

Select **Policer** and **Shaper** rates from 128 kbps to 3968 kbps for each port and then click **Apply**.

Storm Control



Storm control prevents the network from being disrupted by a “broadcast storm”, which occurs when broadcast packets flood the subnet, creating excessive traffic and degrading network performance. You can configure storm control to rate limit broadcast traffic and unknown unicast traffic at a specified level and to drop packets when the specified traffic level is exceeded.

Select each rate from the drop-down list and then click **Apply**.

Notes:

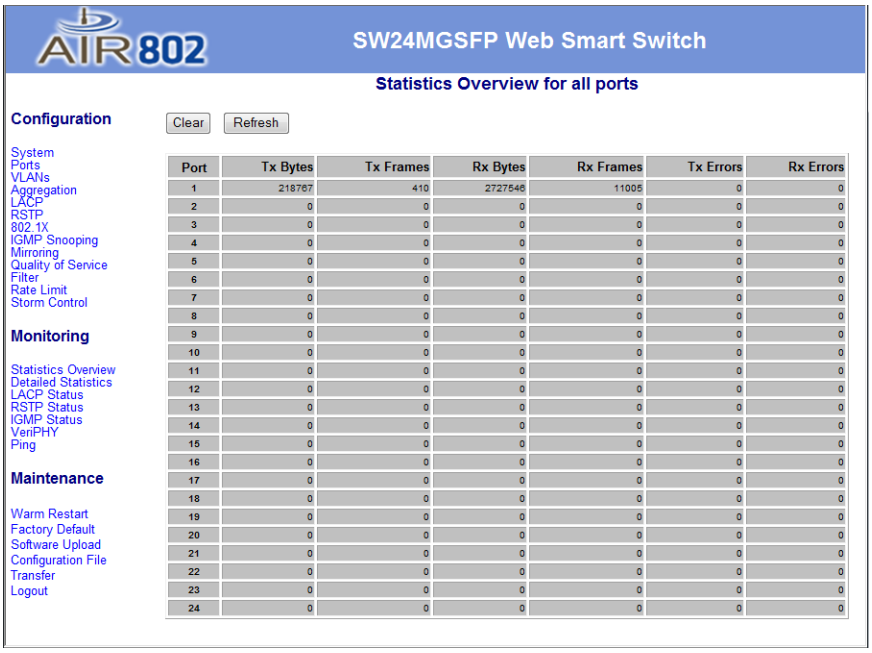
- ICMP (Internet Control Message Protocol) carries network status information. Example is the “ping” utility that probes remote hosts.
- Broadcast packets are sent to all network hosts.
- Multicast packets are sent to a group of hosts.
- Unicast packets are sent to one host.

Monitoring

The system monitoring options are listed in the Monitoring menu at the left side of the screen. Click on a menu item to open the corresponding monitoring screen.

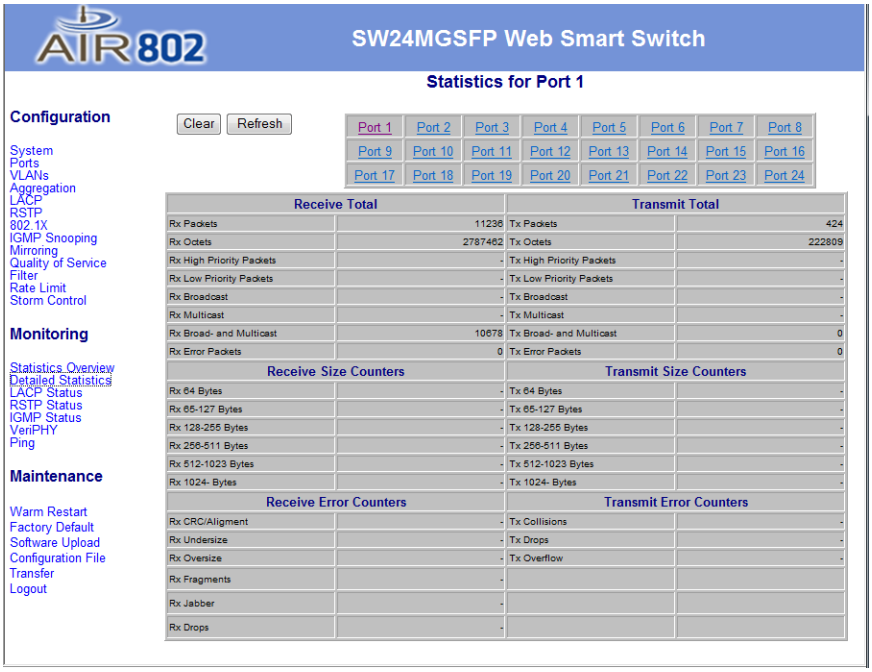
The following sections explain these options.

Statistics Overview



The Statistics screen displays transmit (Tx) and receive (Rx) information for all ports, including Bytes, Frames and Errors.

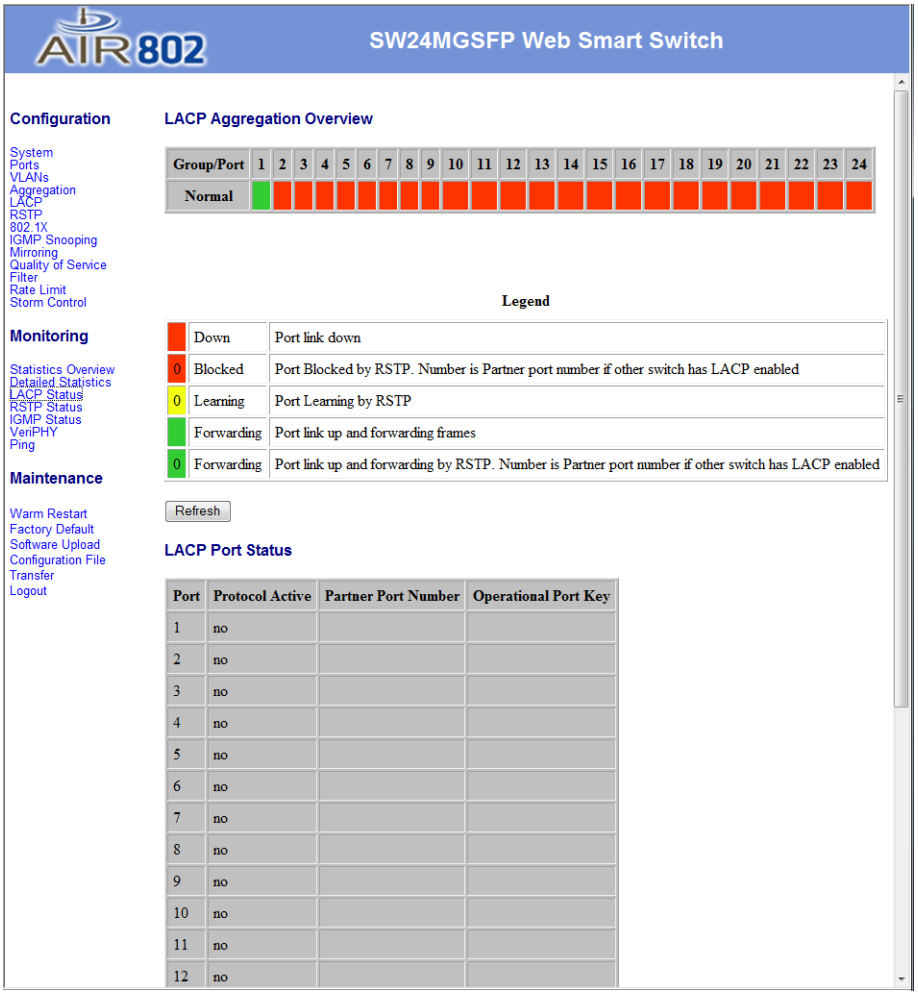
Detailed Statistics



The Detailed Statistics screen display detailed transmit and receive information for a specific port.

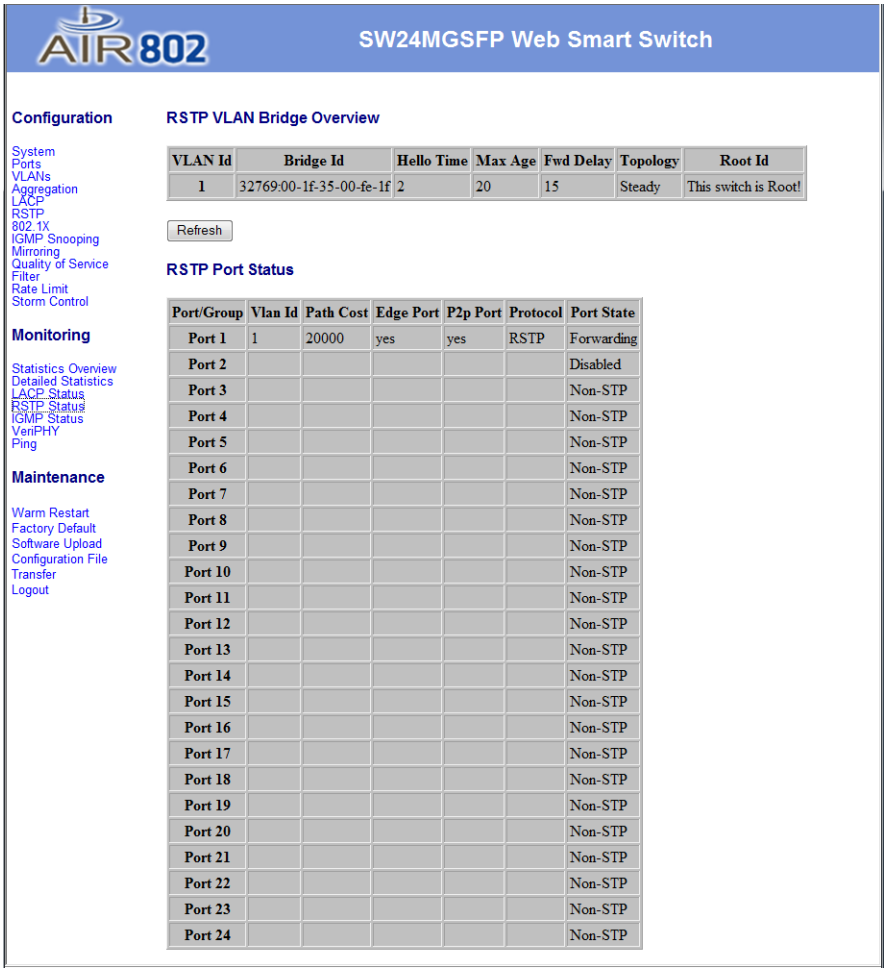
Click on a port number at the top of the screen to view the information for that port.

LACP



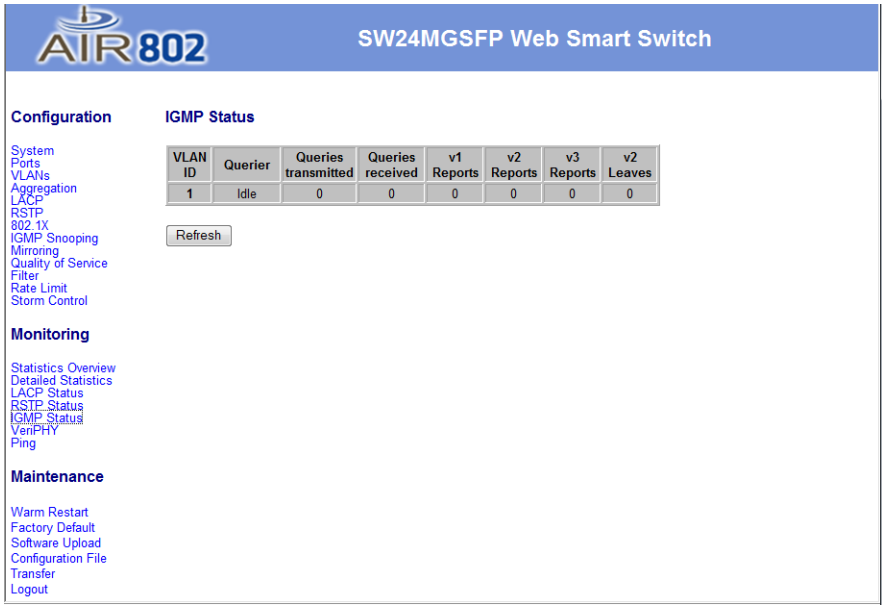
The Link Aggregation Control Protocol (LACP) screen displays the status of aggregated ports.

RSTP Status



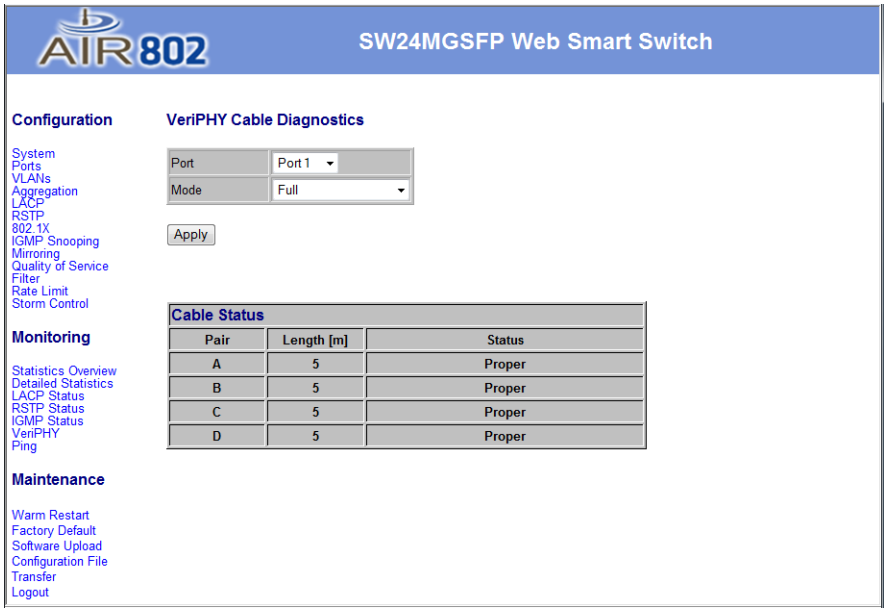
The RSTP (Rapid Spanning Tree Protocol) screen displays the status of RSTP ports.

IGMP Status



The IGMP Status screen displays details of Internet Group Management Protocol (IGMP) network traffic.

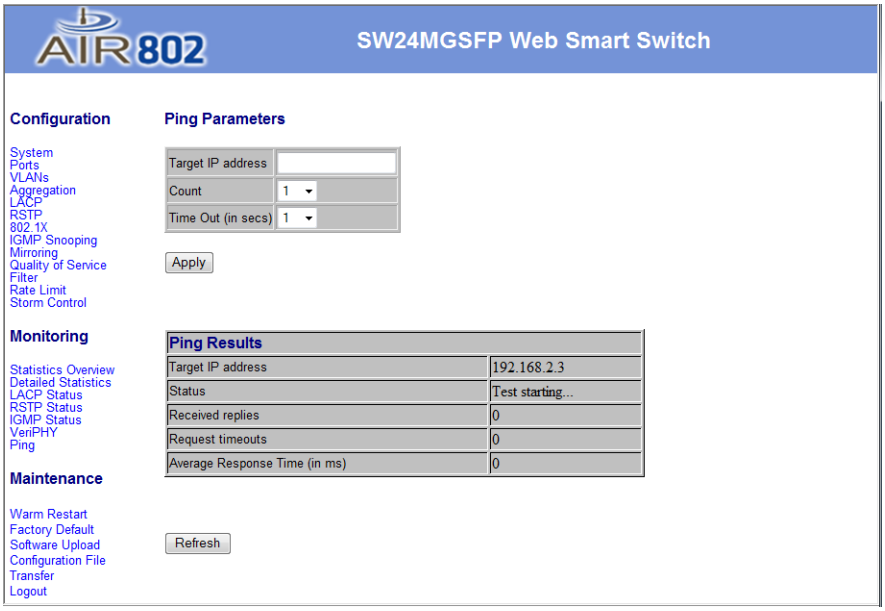
VeriPHY



VeriPHY determines the characteristics of the Ethernet cable attached to any port of the switch. It calculates the cable length and provides status information such as cable termination mismatch, including short and open states; identification of improperly terminated cable pairs, and coupling between cable pairs.

Select a port from the drop-down menu at the top of the screen and click **Apply**.

Ping



Ping is a network administration utility used to test the reachability of a network host and measure the round-trip time for messages sent from the switch to the destination computer.

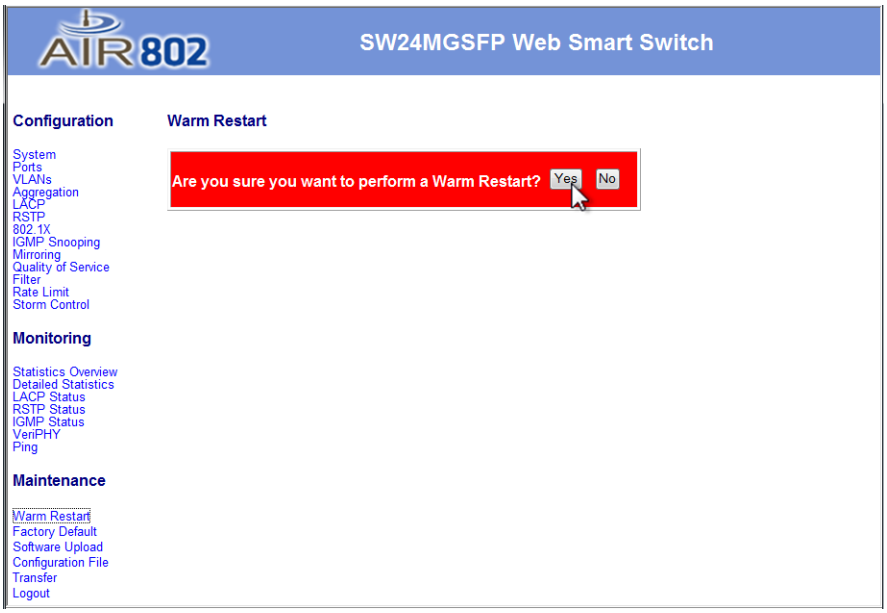
Enter a Target IP address and click **Apply**.

Maintenance

The system maintenance options are listed in the Maintenance menu at the left side of the screen. Click on a menu item to open the corresponding maintenance screen.

The following sections explain these options.

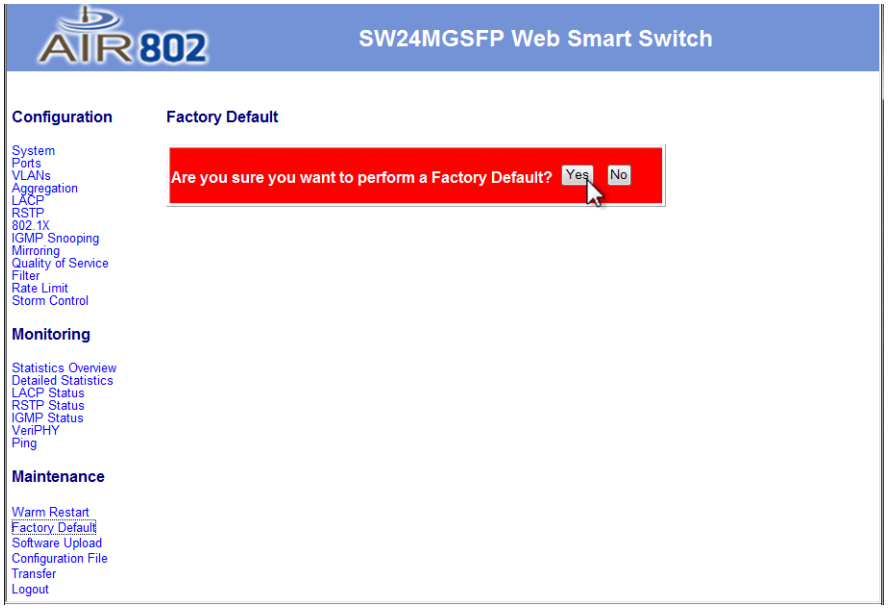
Warm Restart



A warm restart (or “soft reboot”) restarts the switch under software control, without removing power.

Click **Yes** to restart the switch.

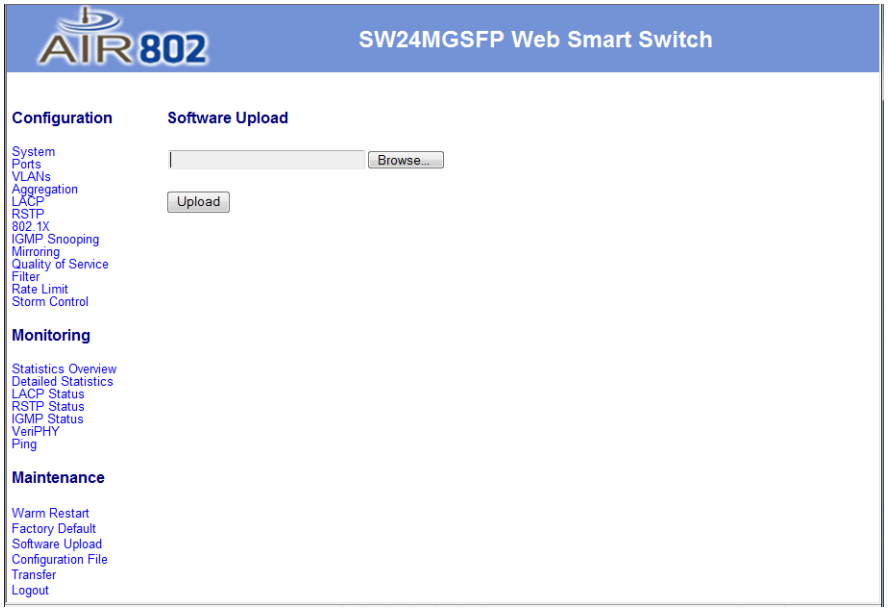
Factory Default



The Factory Default screen lets you restore the switch configuration to the factory default settings.

Click **Yes** to return the switch to factory default settings.

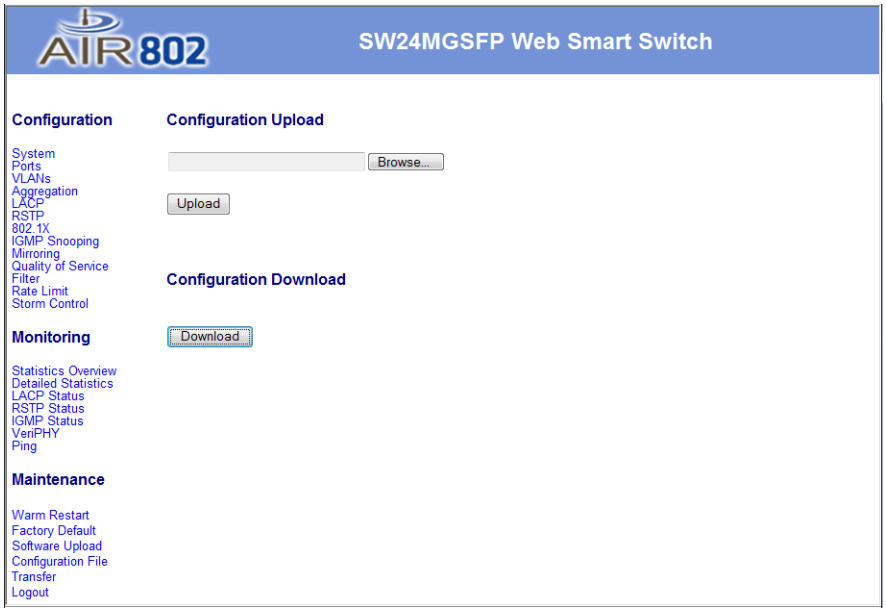
Software Upload



From time to time, updated operating software for you switch may be issued. This software is installed from the Software Upload screen.

Enter the location of the software to be loaded or click **Browse** to navigate to the software location, then click **Upload**.

Configuration File



A configuration file can be used to automatically configure a series of switches with the same settings or restore switch settings when a switch has been replaced.

To upload a saved configuration file, enter the location of the software to be loaded or click **Browse** to navigate to the software location, then click **Upload.**

To save a configuration file, click **Download**. In the pop-up box that appears, click **Save**, navigate to the location where you want to save the file, and click **Save**.

Logout

Click **Logout** to exit the switch software and return to the Login screen.

Command Line Interface

Connection

To use the CLI (Command Line Interface), you require a PC with RS-232 (serial) port; a terminal program such as WinRS (included with Windows 7 and Windows Vista), HyperTerminal (included with Windows XP), or a Telnet program such as PuTTY; and the Console Cable included with the switch. The COM port must be configured for 8 data bits, 1 stop bit, no parity, 115200 baud and no flow control.

Connect the Console Cable between the RS-232 (serial) port of the PC and the Console connector on the front of the switch, then open the terminal program on the PC.

Command Hierarchy

The CLI is hierarchical with two levels: the top level and a group level. The group level consists of the following groups: System, Console, Port, MAC, VLAN, Aggregation, LACP, RSTP, User Group, QoS, Mirror, IP, Dot1X, Debug.

At the top level you can execute a command by entering the full command string, including group, or you may change context to a group by entering the name of the group.

At group level you can enter commands for the particular group you have chosen without specifying the group name or return to the top level by entering the **up** command.

The current level and group is indicated by the prompt. If you are at the top level, the prompt is “>”. If you are at group level, the prompt displays the actual group, e.g., “System>”.

At group level you also have the option of using the slash (/) key to refer to a context relative to the top level, e.g., from the System group you can enter /console to enter the Console group.

Login/Logout Procedures

The CLI login procedure includes a password check, however the factory default for the password is an empty string, which disables the check. Therefore, when the terminal program connects to the switch, you can immediately begin entering commands.

To enable the password check, from the Console level enter

Console Password [**<password>**]

The next time a terminal program attempts to logon to the switch, the password will be required.

To disable the password check, change the password to an empty string, i.e., from the Console level enter

Console Password “”

To logout from the switch, enter **exit** from any level.

Help Utility

At any time while using the CLI you can get help information by pressing the **?** key or entering “help”. The help information displayed depends on the context:

At top level, a list of command groups is displayed.

At group level, a list of the command syntaxes for the current group is displayed.

If the help command is issued for a specific command, the command syntax and a description of the command are shown.

Example 1 — commands at the top level:

> **? <enter>** returns

System	– System commands
Console	– Console commands
Port	– Port commands
MAC	– MAC table commands
VLAN	– VLAN commands
Aggregation	– Aggregation/Trunking commands
LAC	– IEEE802.3ad Link aggregation commands
RSTP	– IEEE802.1w Rapid Spanning Tree commands
User Group	– User Group commands
QoS	– QoS commands/
Mirror	– Mirror commands
IP	– IP commands
Dot1x	– Dot1x commands
Debug	– Debug commands

Example 2 — commands at the Console level:

> **console <enter>**
> **? <enter>** returns

Console Configuration

Console Password [<password>]

Console Timeout [<timeout>]

Console Prompt [<prompt string>]

Example 3 — command syntax:

> **console <enter>**
> **password ? <enter>** returns

Syntax:
Console Password [<password>]

Description:
Set or show the console password. The empty string (“”) disables the password check.

[<password>]: Password string of up to 16 characters.

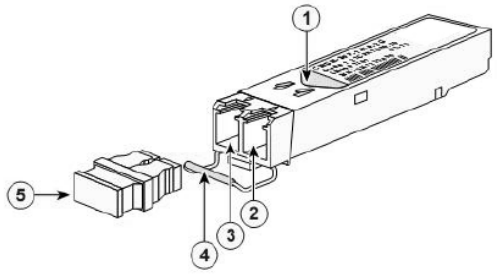
SFP Transceivers

Slots SFP1 and SFP2 on the front of the switch accept SFP (small form-factor pluggable) or Mini-GBIC transceivers that can be used to interface the switch to fiber optic networking cable for gigabit single/multi-mode transmission over distances to 80 km.

Supported optical transceivers include:

SFP-GIG-SX	Gigabit Ethernet optical transceiver (supports 850nm wavelength multi-mode, LC connector). Up to 550 meters through 50/125 μm multi-mode fiber, and up to 275 meters through 62.5/125 μm multi-mode fiber.
SFP-GIG-LX	Gigabit Ethernet optical transceiver(LC connector). Up to 10 km through 1310 nm wavelength single-mode fiber.
SFP-GIG-LH40	Gigabit Ethernet optical transceiver (LC connector). Up to 40 km through 1310 nm wavelength single-mode fiber.
SFP-GIG-LH80	Gigabit Ethernet optical transceiver (LC connector). Up to 80 km through 1550 nm wavelength single-mode fiber.

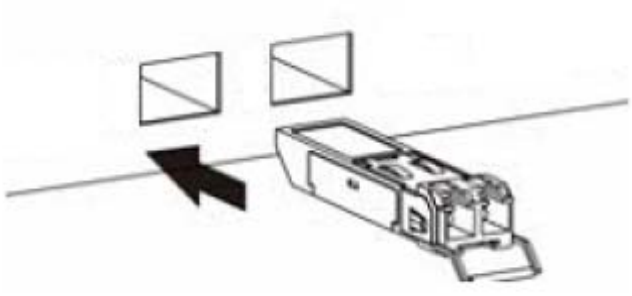
SFP Module Components



1. Specification label
2. Incoming optical signal jack
3. Outgoing optical signal jack
4. Bale-clasp latch
5. Dust plug

SFP Module Installation

1. Remove the module's packaging and the dust plug.
2. Grasp the module between your thumb and index finger, and carefully slide it into one of the SFP slots.



3. Remove the rubber caps from the incoming (Rx) and outgoing (Tx) optical signal cables and insert each cable into the corresponding module connector until it locks into place.

Cautions regarding optical connections:

For maximum transmission distance and to avoid possible damage, only connect fiber optic cables that meet the specifications shown on the specification label.

To avoid contamination, do not touch the optical surfaces.

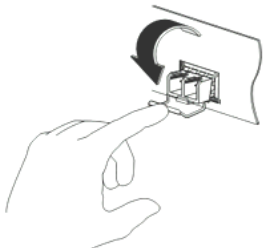
To avoid possible eye damage, do not look directly into an optical interface.

Do not excessively bend optical cables.

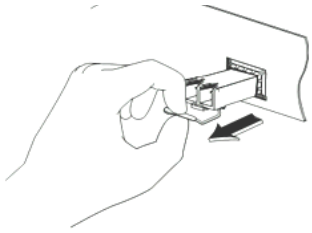
If necessary, clean the fiber-optic connectors using standard procedures.

SFP Module Removal

1. Press the locking tabs on each optical signal cable and remove the cable from the module. Place rubber caps on the connectors to protect them from contamination.
2. Pull the bale-clasp latch out and down to eject the module.



3. Grasp the module between your thumb and index finger, and carefully remove it from the module slot.



4. Place the removed module in an antistatic bag or other protective environment.

Cautions regarding optical connections:

To avoid contamination, do not touch the optical surfaces.

To avoid possible eye damage, do not look directly into an optical interface.

Do not excessively bend optical cables.

If necessary, clean the fiber-optic connectors using standard procedures.


AIR 802 LLC