WSG18SFP Switch

User Manual

Version: 01/01/2011

Introduction

Product Overview

This switch is equipped with 16 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP Open Slots. It is designed for easy installation and high performance in an environment where traffic is on the network and the number of users increases continuously. The compact rigid 19" rack-mount size is specifically designed for small to medium workgroups. It can be installed where the space is limited; moreover, it provides smooth network migration, the network capacity can be upgraded easily. In addition, the switch has comprehensive features such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

Web Management Features

Configuration
Administrator
Port Configuration
VLAN Setting
Trunking
Link Aggregation
Raid Spanning Tree
802.1X
IGMP Snooping
Port Mirroring
QoS Setting
Filter
Rate Limit
Storm Control
Monitoring
Statistics Overview
Detailed Statistics
LACP Status
RSTP Status
IGMP Status
VeriPHY
Ping
Maintenance
Reboot Device (Warm Restart)
Load Default Setting (Factory Default)
Firmware Updating (Software Upload)

Backup/Recovery (Configuration File Transfer)
Logout

Specifications

- Standard
  IEEE 802.3 10BaseT
  IEEE 802.3u 100BaseTX
  IEEE 802.ab 1000BaseT
  IEEE 802.3z 1000BaseSX/LX
  IEEE 802.3x Flow Control
  IEEE 802.1x Port-based Network Access Control
  IEEE 802.1Q VLAN Tagging
  IEEE 802.3ad Link Aggregation
  IEEE 802.1d Spanning tree protocol
  IEEE 802.1w Rapid Spanning tree protocol
  IEEE 802.1p Class of service, Priority Protocols

- Number of Port
  16 x 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP Open Slots

Mechanical

- LED Indicator
  Per Port: LINK/ACT
  UTP Port 1~16: 1000M
  SFP Port 1~16:: ACT
  Per Unit: Power

- Power Input: 100~240V/AC, 50~60HZ

- Product Dimensions/ Weight
  44 × 220 × 440 mm (H × D x W) / 3kg

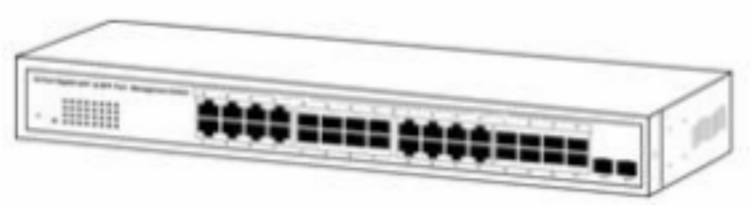
Performance

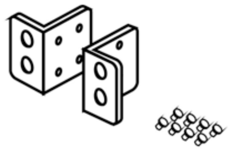
MAC Address: 8K
Buffer Memory: 500 KB
Jumbo Frames: 9K
Transmission Method: Store and Forward

Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- ➤ One PoE Gigabit Ethernet Switch
- ➤ One AC Power Cord
- ➤ User Manual CD
- ➤ One Rack-mount kit





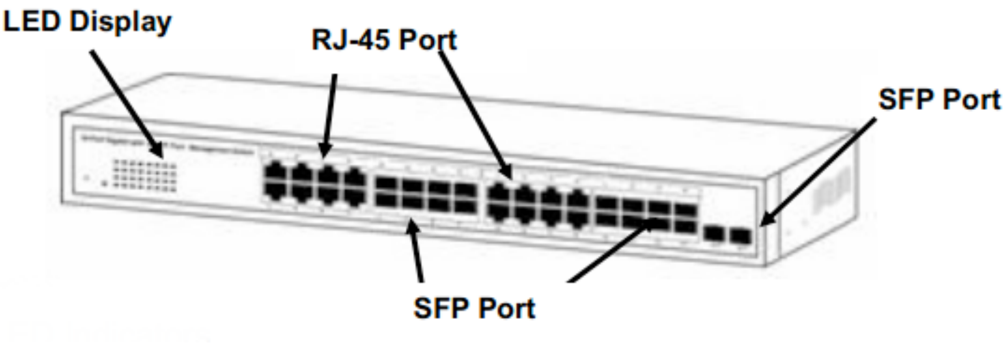
Hardware Description

Physical Dimensions/ Weight

44 × 220 × 440 mm (H × W × D) / 3KG

Front Panel

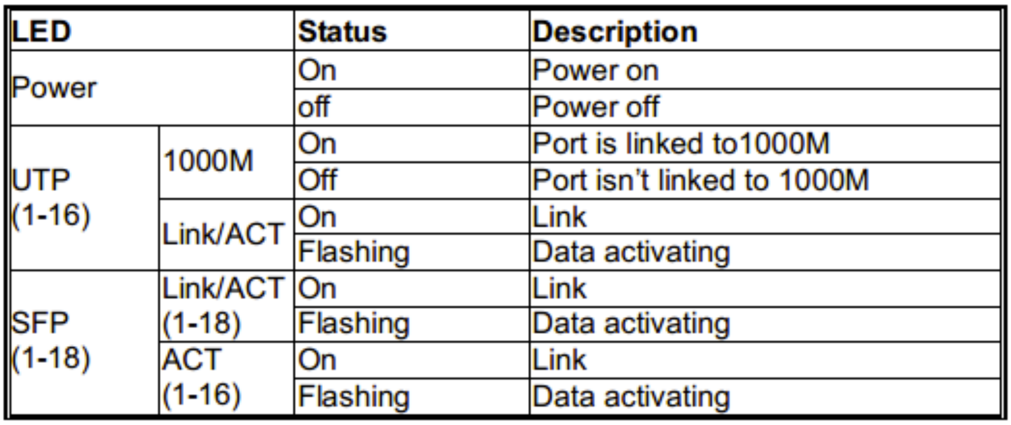
The front Panel consists of 16 x 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP open slots. The LED Indicators are also located on the front panel.



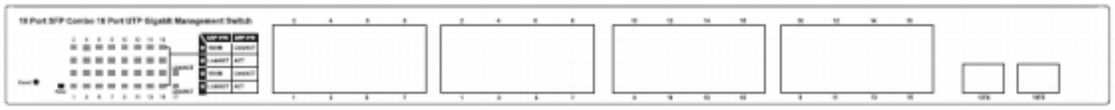
LED Indicators

The LED Indicators present real-time information of the operation status.

Table 1-1 LED Indicators

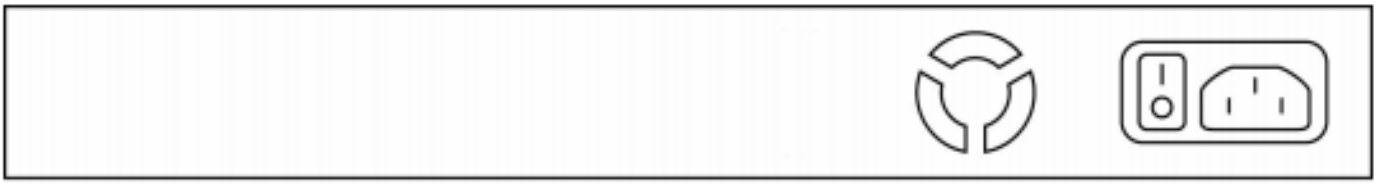


LED		Status	Description
Power		On	Power on
		off	Power off
UTP (1-16)	1000M	On	Port is linked to1000M
		Off	Port isn't linked to 1000M
	Link/ACT	On	Link
		Flashing	Data activating
SFP (1-18)	Link/ACT (1-18)	On	Link
		Flashing	Data activating
	ACT (1-16)	On	Link
		Flashing	Data activating



Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.



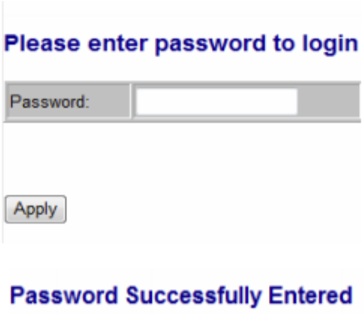
Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough of space to attach the cables, power cord and allow air circulation. Use twisted pair cable to connect this switch to your PC.

Software Description

Open the web browser, and type in the URL: 192.168.2.1. You see the login screen. The factory default did not set up a password, so you can just click the Apply button. The login process is completed and "Password successfully entered" appears on the screen.

Login



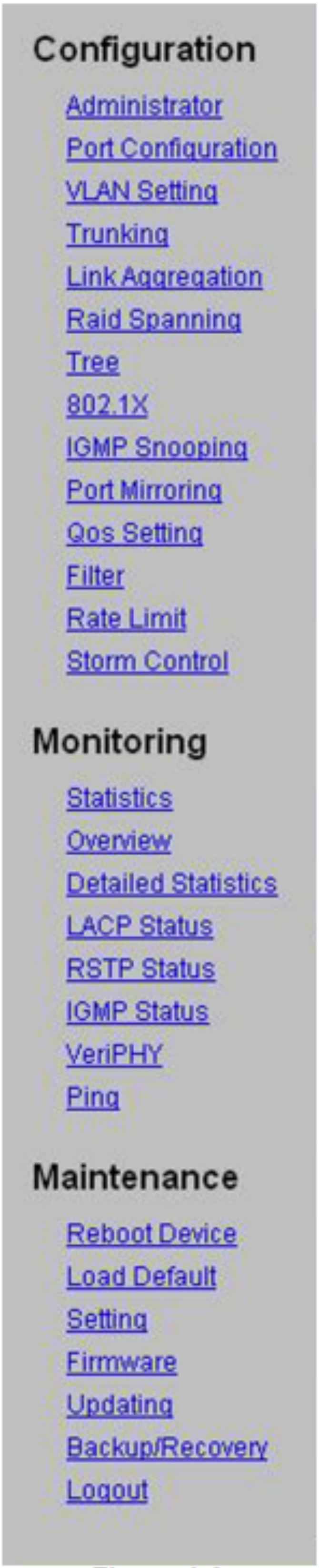
Please enter password to login

Password:

Password Successfully Entered

Figure 1-1

After the user login, the right side of website shows all functions (Fig. 1-2).



Configuration
Administrator
Port Configuration
VLAN Setting
Trunking
Link Aggregation
Raid Spanning
Tree
802.1X
IGMP Snooping
Port Mirroring
Qos Setting
Filter
Rate Limit
Storm Control
Monitoring
Statistics
Overview
Detailed Statistics
LACP Status
RSTP Status
IGMP Status
VeriPHY
Ping
Maintenance
Reboot Device
Load Default
Setting
Firmware
Updating
Backup/Recovery
Logout

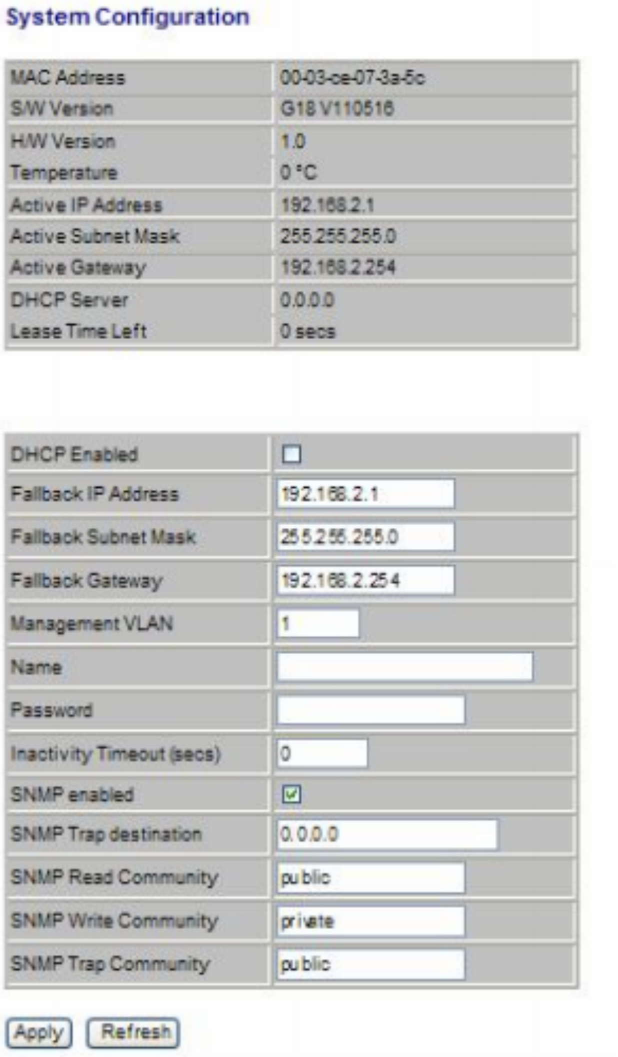
Figure 1-2

Configuration

Administrator

System Configuration

This page shows system configuration information.



System Configuration

MAC Address	00-03-ce-07-3a-5c
S/W Version	G18 V110516
H/W Version	1.0
Temperature	0 °C
Active IP Address	192.168.2.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.2.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	□
Fallback IP Address	192.168.2.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.2.254
Management VLAN	1
Name	
Password	
Inactivity Timeout (secs)	0
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

Figure 2-1

- ➤ MAC Address: hardware address assigned by manufacturer (default).
- ➤ S/W Version: switch's firmware version.
- ➤ H/W Version: switch's Hardware version.
- ➤ DHCP Enabled: click to enable DHCP
- ➤ Fallback IP address: assign the IP address manually, the default IP is 192.168.2.1
- ➤ Fallback Subnet Mask: assign the subnet mask to the IP address
- ➤ Fallback Gateway: assign the network gateway, the default gateway is 0.0.0.0.

- Management VLAN: ID of the configured VLAN (1-4094) to manage the switch. By default, all ports on the switch are members of VLAN 1. However, if the management VLAN is changed, the management station should be attached to a port belonging to this VLAN.
- Name: type in a new user name (default value is 'admin').
- Password: type in a new password (default value is 'admin').
- SNMP Enabled: enables or disables SNMP on the switch. Supports SNMP version 1and 2c management clients.
- SNMP Trap Destination: IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are issued by the switch to specified trap managers. Specify trap managers so that key events are reported by this switch to your management station.
- SNMP Read Community: community string serves as a password and allows access to the SNMP database on this switch.
- SNMP Trap Community: community string sent with the notification operation.

Ports Configuration

Port configuration ensures access to a switch port based on MAC address, limits the total number of devices using a switch port and protects against MAC flooding attacks.

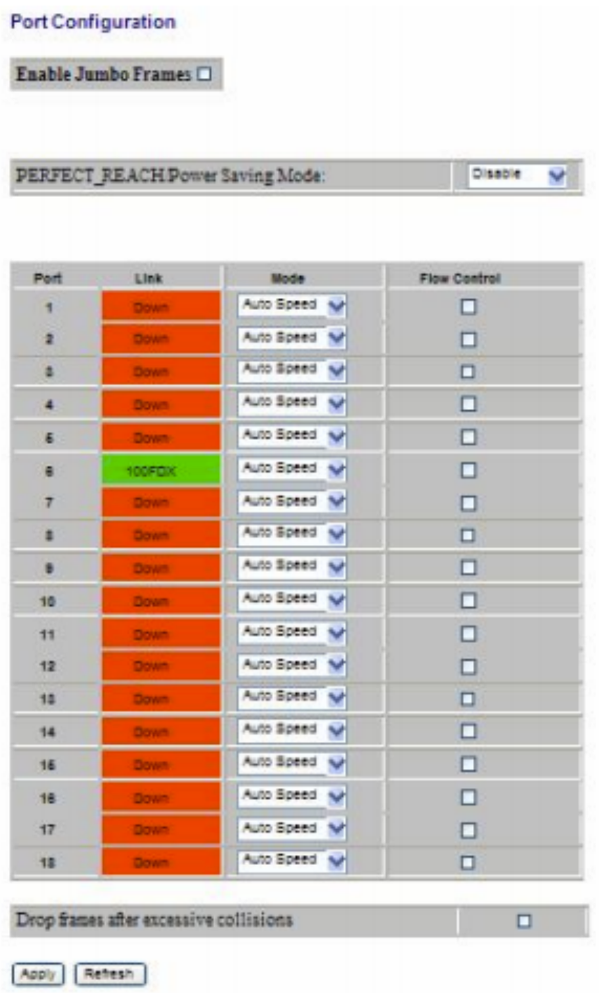
Port Configuration

In Port Configuration, you can set and view the operation mode for each port.

- Enable Jumbo Frames: This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- Power Saving Mode: Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

- Mode: allow user to manually set the port speed as Auto, 10 half, 10 Full, 100 Half, 100 Full, 1000 Full or Disabled. Press Apply button to complete the configuration procedure.



Port Configuration

Enable Jumbo Frames □

PERFECT_REACH Power Saving Mode: Disable

Port	Link	Mode	Flow Control
1	Down	Auto Speed	□
2	Down	Auto Speed	□
3	Down	Auto Speed	□
4	Down	Auto Speed	□
5	Down	Auto Speed	□
6	100FDX	Auto Speed	□
7	Down	Auto Speed	□
8	Down	Auto Speed	□
9	Down	Auto Speed	□
10	Down	Auto Speed	□
11	Down	Auto Speed	□
12	Down	Auto Speed	□
13	Down	Auto Speed	□
14	Down	Auto Speed	□
15	Down	Auto Speed	□
16	Down	Auto Speed	□
17	Down	Auto Speed	□
18	Down	Auto Speed	□

Drop frames after excessive collisions □

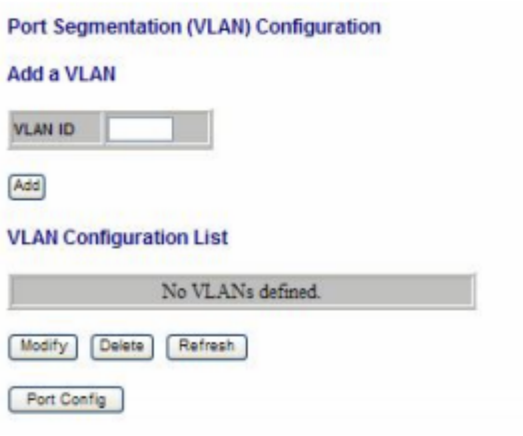
Figure 2-2

VLAN Setting

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic, so that only the members of the same VLAN receive traffic from each other. Basically, creating a VLAN is logically equivalent to connecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

Port Segmentation (VLAN) Configuration

- VLAN ID: ID of configured VLAN (1-4094, no leading zeroes).
- VLAN Configuration List: Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.



Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID

VLAN Configuration List

No VLANs defined.

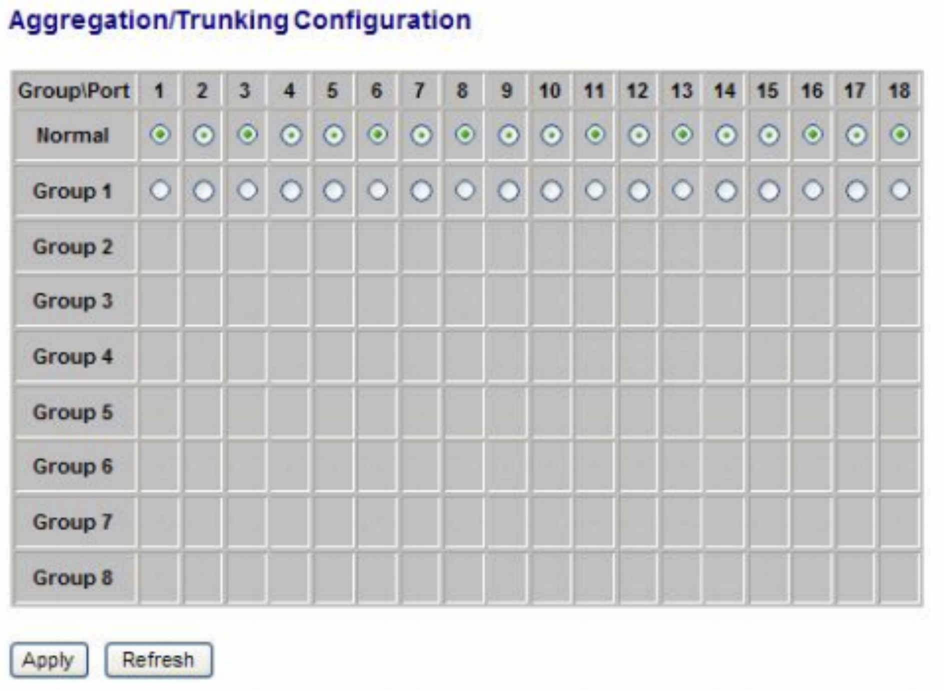
Figure 2-3

Trunking

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a method called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

Aggregation / Trunking Configuration

To assign a port to a trunk, click on the required trunk number, then click Apply.



Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Group 1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 2																		
Group 3																		
Group 4																		
Group 5																		
Group 6																		
Group 7																		
Group 8																		

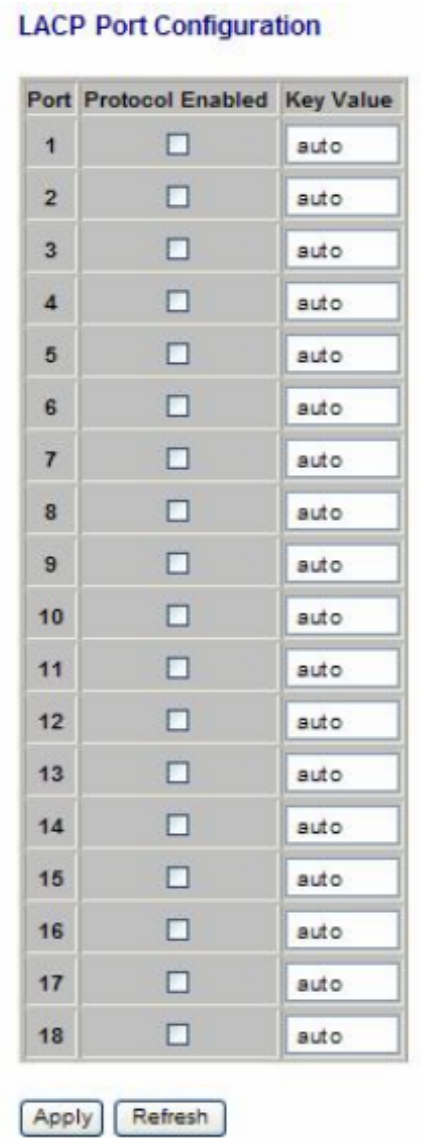
Figure 2-4

Link Aggregation (LACP)

IEEE 802.3ad Link Aggregation Control Protocol (LACP) increases bandwidth by automatically aggregating several physical links together as a logical trunk and providing load balancing and fault tolerance for uplink connections.

LACP Port Configuration

- ➤ Port: Port number.
- ➤ Enabled: Enables LACP on the associated port.
- ➤ Key Value: Configures a port's LACP administration key. The port administrative key should be set to the same value for ports belonging to the same link aggregation group (LAG). If this administrative key is not set when an LAG is formed (i.e., it has the null value of 0), this key is automatically set to the same value as the one used by the LAG.



LACP Port Configuration

Port	Protocol Enabled	Key Value
1	□	auto
2	□	auto
3	□	auto
4	□	auto
5	□	auto
6	□	auto
7	□	auto
8	□	auto
9	□	auto
10	□	auto
11	□	auto
12	□	auto
13	□	auto
14	□	auto
15	□	auto
16	□	auto
17	□	auto
18	□	auto

Figure 2-5

Raid Spanning Tree

IEEE 802.1w Rapid Spanning tree protocol (LACP) provides a loop-free network and redundant links to the core network with rapid convergence to ensure faster recovery from failed links, enhancing overall network stability and reliability.

RSTP System Configuration

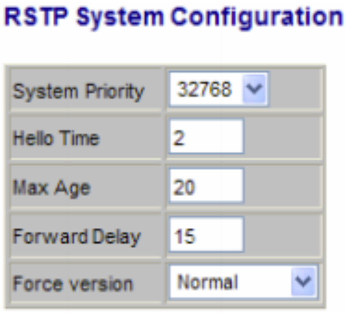
➤ System Priority: This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. If all devices have the same priority, the device with the lowest MAC address becomes the root device. Number between 0-61440 in increments of 4096. Therefore, there are 16 values.

➤Hello Time: Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1-10 (default is 2).

➤ Max Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. It also means the maximum life time for a BPDU frame. Number between 6-40 (default is 20).

➤ Forward Delay: The maximum time (in seconds) the root device waits before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30 (default is 15).

➤ Force Version: Set and show the RSTP protocol to use. Normal - use RSTP, Compatible - compatible with STP



RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal

Figure 2-6-1

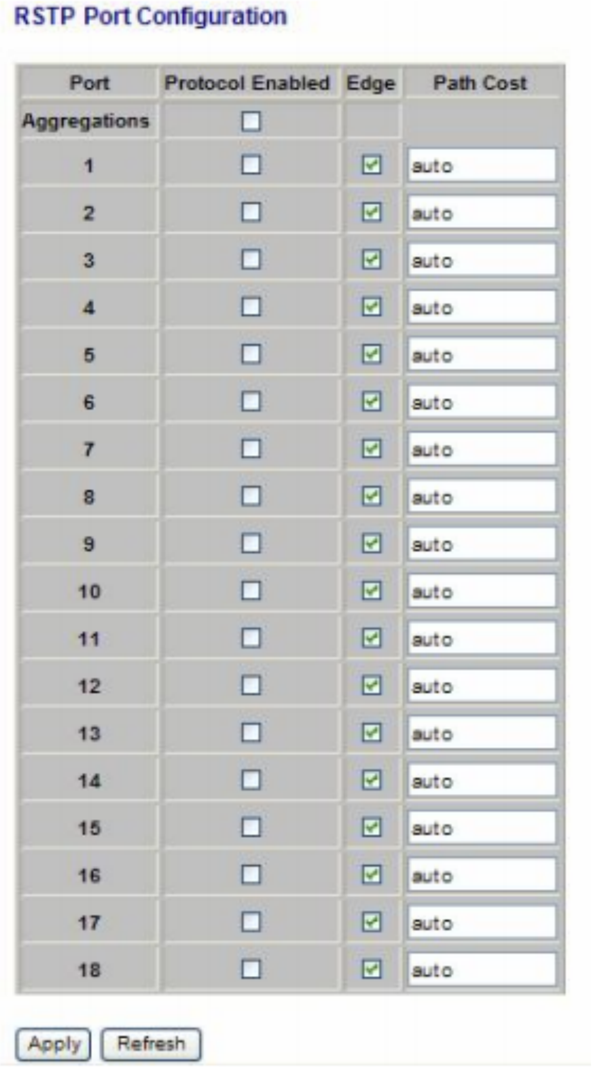
RSTP Port Configuration

➤ Port: The port ID. It cannot be changed. Aggregations mean any configured trunk group.

➤ Enabled: Click on the tick-box to enable/disable the RSTP protocol for the port.

➤ Edge: Expect the port to be an edge port (linking to an end station) or a link to another STP device.

➤ Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP path cost on the port. Number between 0 - 200000000. 0 means auto generated path cost.



RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	□		
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto
5	□	☑	auto
6	□	☑	auto
7	□	☑	auto
8	□	☑	auto
9	□	☑	auto
10	□	☑	auto
11	□	☑	auto
12	□	☑	auto
13	□	☑	auto
14	□	☑	auto
15	□	☑	auto
16	□	☑	auto
17	□	☑	auto
18	□	☑	auto

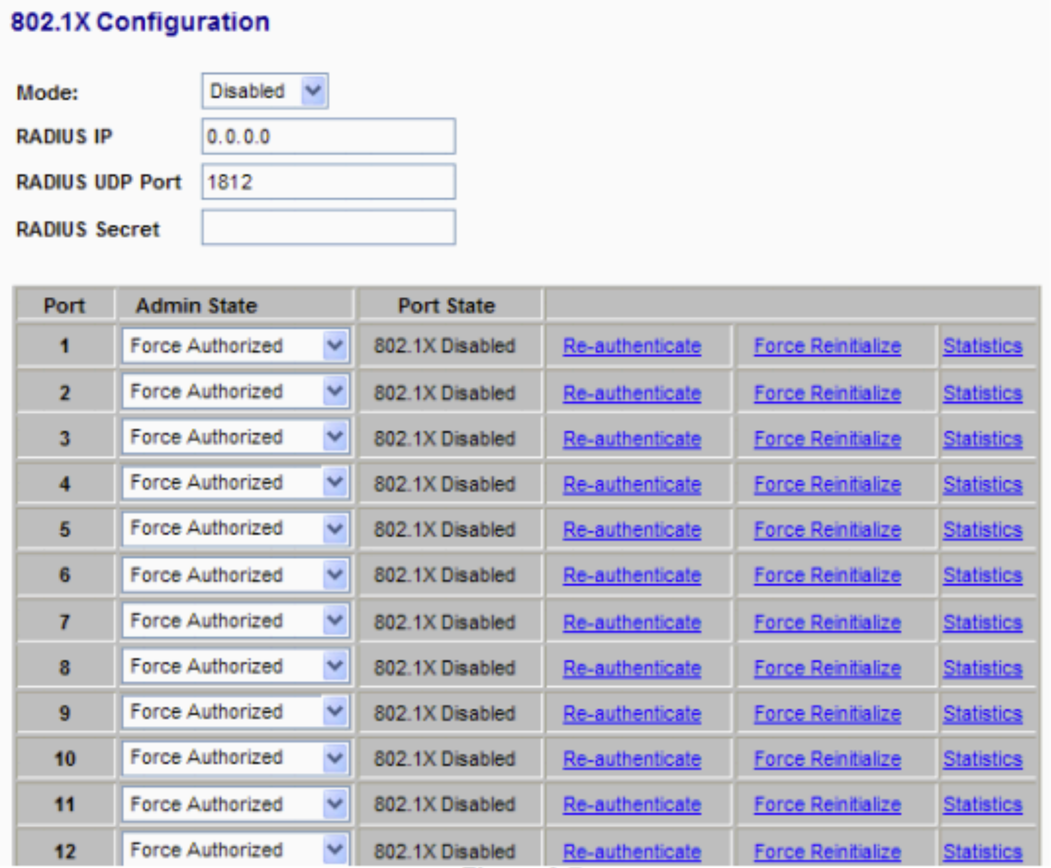
Figure 2-6-2

802.1X

802.1X provides port-based authentication, which involves communication between a supplicant, authenticator, and authentication server. Port refers to a single point of attachment to the LAN infrastructure. Supplicant is often software on a client device, such as a laptop; authenticator is a network device, such as an Ethernet switch or wireless access point; authentication server is typically a host running software supporting the RADIUS and EAP protocols.
Port-based Network access control (PNAC) ensures that all the users are authorized before being granted an access to the network. User authentication is carried out using any standard-based RADIUS server.

802.1X Configuration
Mode: Enables or disables 802.1X globally for all ports. The 802.1X protocol should be enabled globally for the switch before the port settings are active (Default: Disabled)
RADIUS IP: Address of authentication server
RADIUS UDP Port: Network port of authentication server used for authentication messages (Range: 1-65535; Default: 1812)

RADIUS Secret: Sets the text string used for encryption between the switch and the RADIUS server. This key is used to authenticate logon access for the client. Do not use blank spaces in the string. (Max. length: 48 characters).



802.1X Configuration

Mode:	Disabled
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin State	Port State			
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
10	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
11	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
12	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics

Figure 2-7

IGMP Snooping

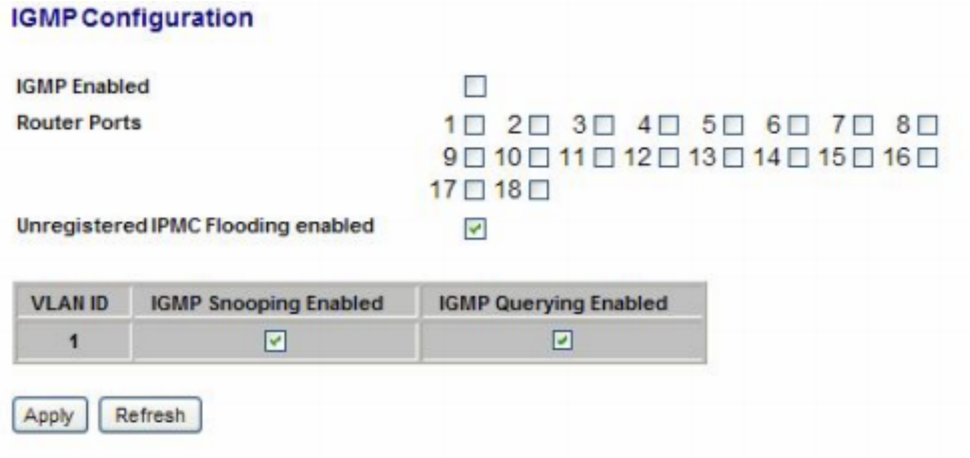
IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer3 IGMP packets sent in a multicast network.

When IGMP Snooping is enabled, it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry. It prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to the subscribers only.

IGMP Configuration

➤ IGMP Enabled: When enabled, the switch monitors network traffic to determine which hosts want to receive multicast traffic.

- Router Ports: Set if ports are connecting to the IGMP administrative routers.
- Unregistered IPMC Flooding enabled: Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic floods when enabled, and forward to router-ports when disabled.
- IGMP Snooping Enabled: When enabled, the port monitors network traffic to determine which hosts want to receive the multicast traffic.
- IGMP Querying Enabled: When enabled, the port can serve as Querier which is responsible for asking hosts if they want to receive multicast traffic.



IGMP Configuration

IGMP Enabled □

Router Ports 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □

Unregistered IPMC Flooding enabled ☑

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	☑

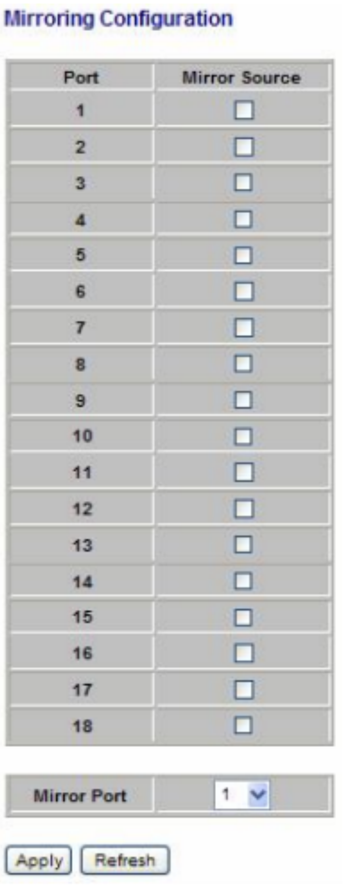
Figure 2-8

Port Mirroring

Port Mirroring is used on a network to send a copy of network packets seen on one switch port (or an entire VLAN) 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.

Mirroring Configuration

- Port to Mirror to: The port that "duplicates" or "mirrors" the traffic on the source port. Only incoming packets can be mirrored. Packets are dropped when the available egress bandwidth is less than ingress bandwidth.
- Ports to Mirror: Select the ports that you want to mirror from this section of the page. A port is mirrored when the "Mirroring Enabled" check-box is checked.



Mirroring Configuration

Port	Mirror Source
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□
11	□
12	□
13	□
14	□
15	□
16	□
17	□
18	□

Mirror Port: 1

Figure 2-9

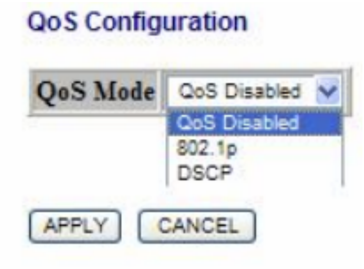
QoS Setting

In QoS Mode, select QoS Disabled, 802.1p, or DSCP to configure the related parameters.

QoS Configuration

- ➤ Strict: Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- ➤ WRR: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)

  *Note: WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page



QoS Configuration

QoS Mode: QoS Disabled

Figure 2-10-1

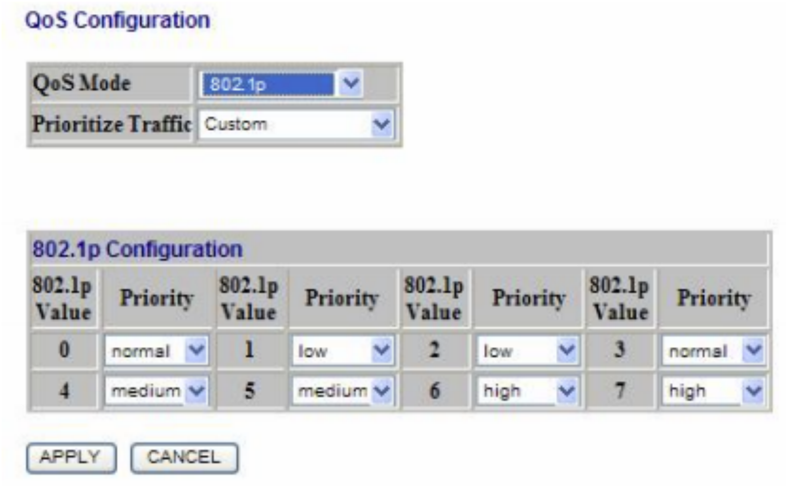
QoS Mode: QoS Disabled

When the QoS Mode is set to QoS Disabled, the following table is displayed.

QoS Mode: 802.1p

Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0 - 7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

When the QoS Mode is set to 802.1p, the 802.1p Configuration table is displayed as shown below.



QoS Configuration

QoS Mode	802.1p
Prioritize Traffic	Custom

802.1p Configuration

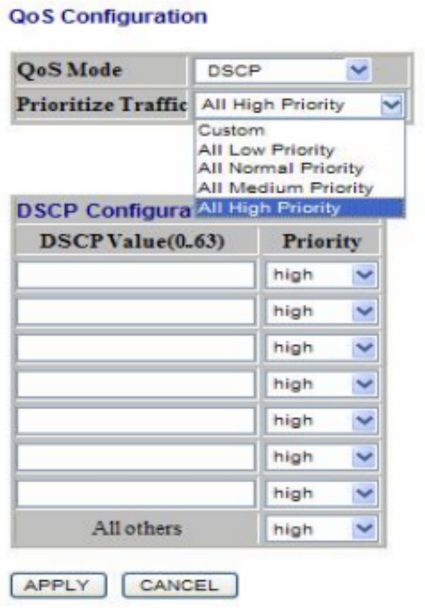
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

Figure 2-10-2

QoS Mode: DSCP

DSCP: Packets are prioritized using the DSCP (Differentiated Services Code Point) value. The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings map all DSCP values to the high priority egress queue.
You can use the Prioritize Traffic drop-down list to quickly set the values in the DSCP Configuration table to a common priority queue. Use Custom if you want to set each value individually.

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.



QoS Configuration

QoS Mode	DSCP
Prioritize Traffic	All High Priority

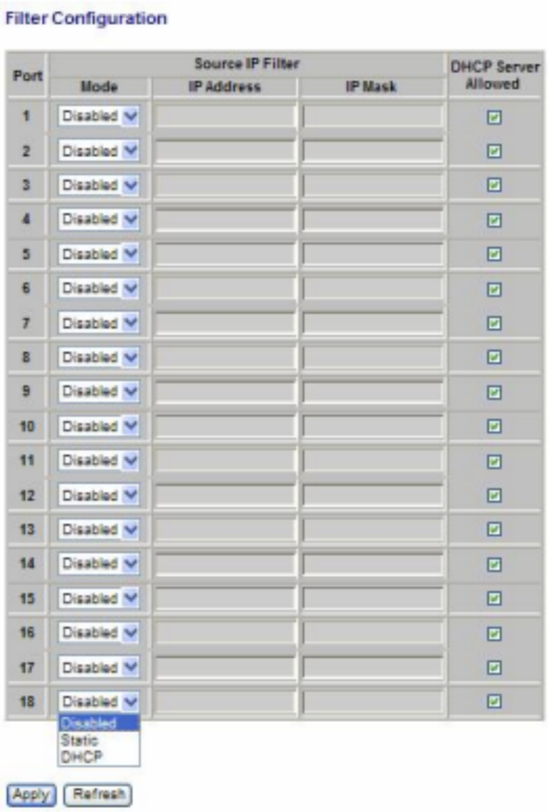
DSCP Configura

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Figure 2-10-3

Filter Configuration

Administrators can easily assign IP addresses to the ports of the switch. Press Apply button after you make the changes.



Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			☑
2	Disabled			☑
3	Disabled			☑
4	Disabled			☑
5	Disabled			☑
6	Disabled			☑
7	Disabled			☑
8	Disabled			☑
9	Disabled			☑
10	Disabled			☑
11	Disabled			☑
12	Disabled			☑
13	Disabled			☑
14	Disabled			☑
15	Disabled			☑
16	Disabled			☑
17	Disabled			☑
18	Disabled			☑

Figure 2-11

Source IP Filter:

Mode: There are three modes, by default it's "disabled"

Disabled: Allow all IP network addresses to login to this switch and to manage it.

Static: Only configured IP network addresses (IP with IP mask) are allowed to login to this switch and to manage it. Only the the received IP packets containing configured source network addresses can be forward by the switch.

Note: In this mode, the received packets are filtered except the IP packets with configured source network addresses.

For example:

1. *IP Address: 192.168.3.2, IP Mask: 255.255.255.0; Network address 192.168.3.x (254 IP Addresses) can be forwarded on this port*
2. *IP Address: 192.168.3.2, IP Mask: 255.255.255.255; Only IP 192.168.3.2 can be forwarded on the port.*

DHCP: Allow the IP Address received from DHCP server to login to this switch and manage it. Only the IP packets containing the source IP are allowed to be forwarded through the switch.

IP Address: IP Address, it can be one IP Address or a LAN

IP Mask: IP Subnet Mask, related to the IP Address

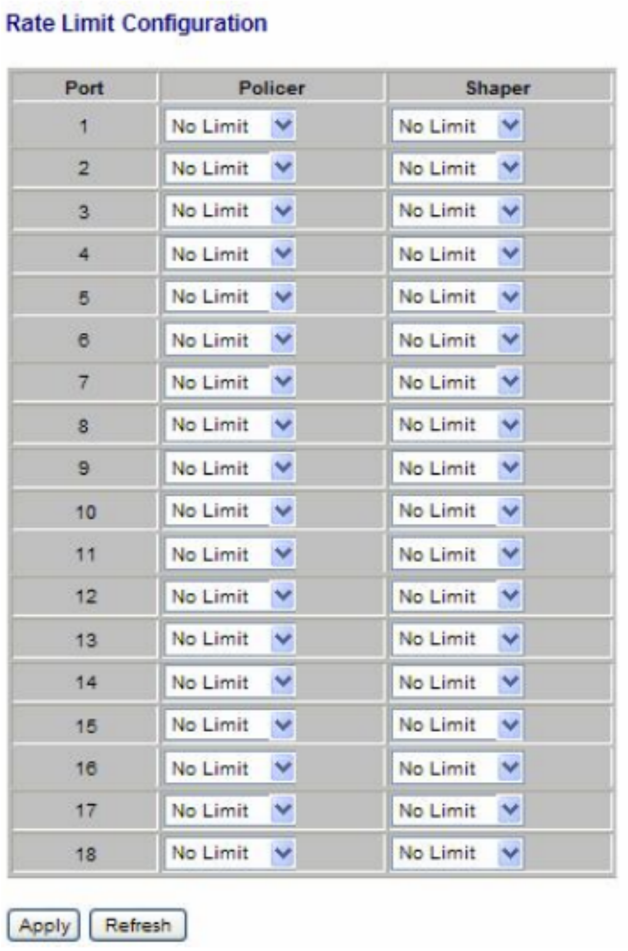
DHCP Server Allowed: Tick off the check-box under the port x to allow the DHCP Server on this Port, valid port is Port 1-18.

Rate Limit Configuration

Select the Port number.

Policer: Set up the ingress bandwidth limit. Incoming traffic is discarded if the rate exceeds the value entered. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1-18 is 128-3968 kbps. Default: No Limit

Shaper: Set up the egress bandwidth limit. Outgoing traffic is discarded if the rate exceeds the value entered. Pause frames are generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1-18 is 128-3968. Default: No limit



Rate Limit Configuration

Port	Policer	Shaper
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit

Figure 2-12

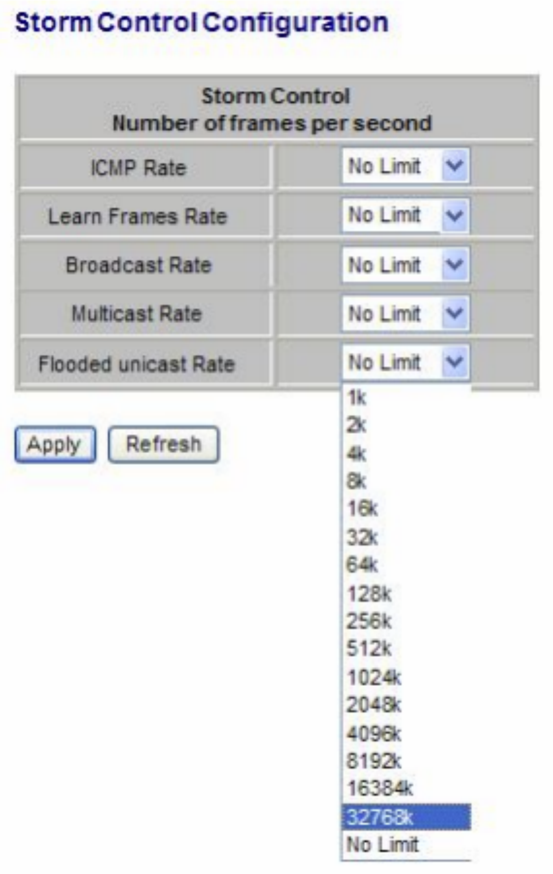
Storm Control

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold are dropped then.

Storm Control Configuration

Storm control is used to block unnecessary multicast and broadcast frames that reduce switch's performance. When the function is enabled and Storm Control rate settings are detected as exceeded, the unnecessary frames are dropped. There are five types of traffic which can be rate limited, including ICMP Rate, Learn Frames Rate, Broadcast Rate, Multicast Rate and Flooded unicast Rate. The setting range is 1k-32768k per second. Default of four Rates is No Limit.



Storm Control Number of frames per second	
ICMP Rate	No Limit
Learn Frames Rate	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Flooded unicast Rate	No Limit

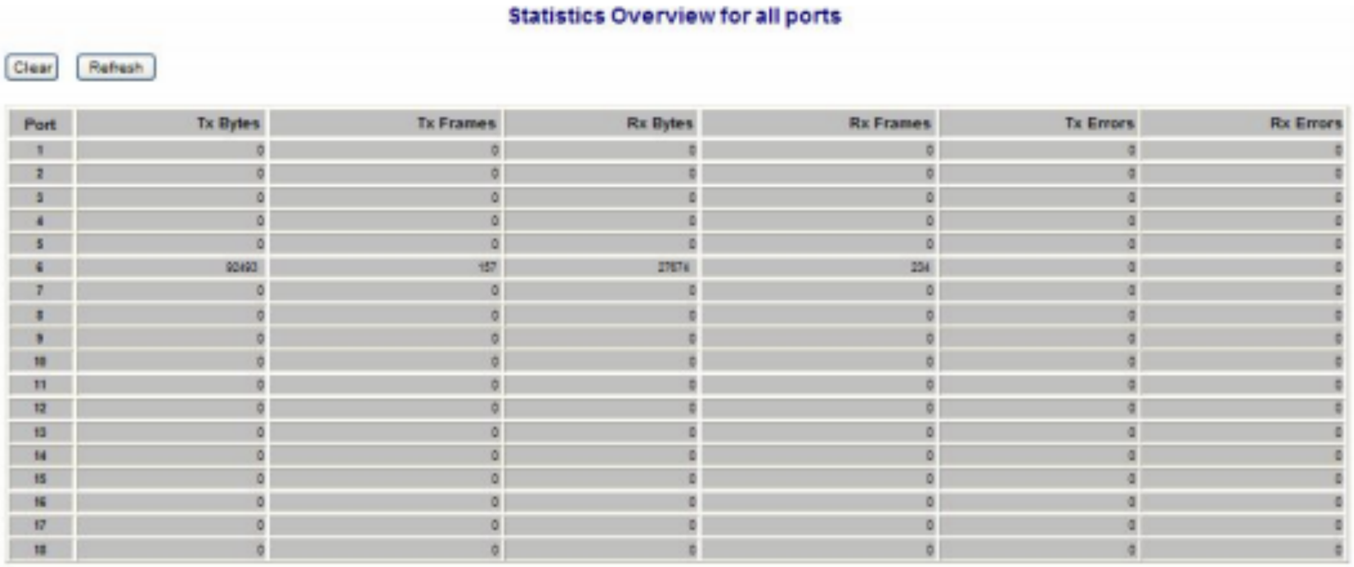
Figure 2-13

After completing the function's setting, press Apply button.

Monitorning

Statistic Overview

Statistic Overview for all ports
You can mirror traffic from any source port to a target port for real-time analysis.



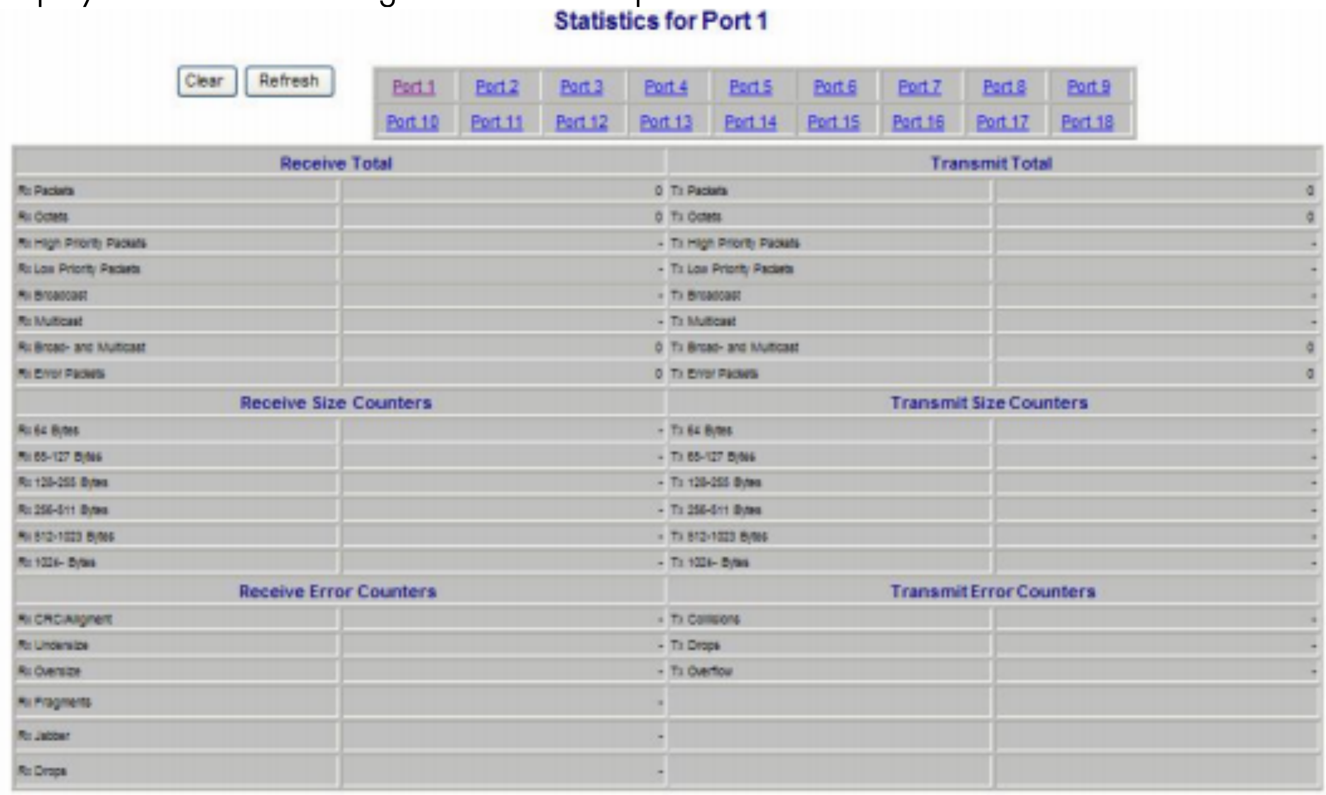
Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	90493	157	27874	234	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0

Figure 3-1

Detailed Statics

Display the detailed counting number of each port's traffic.



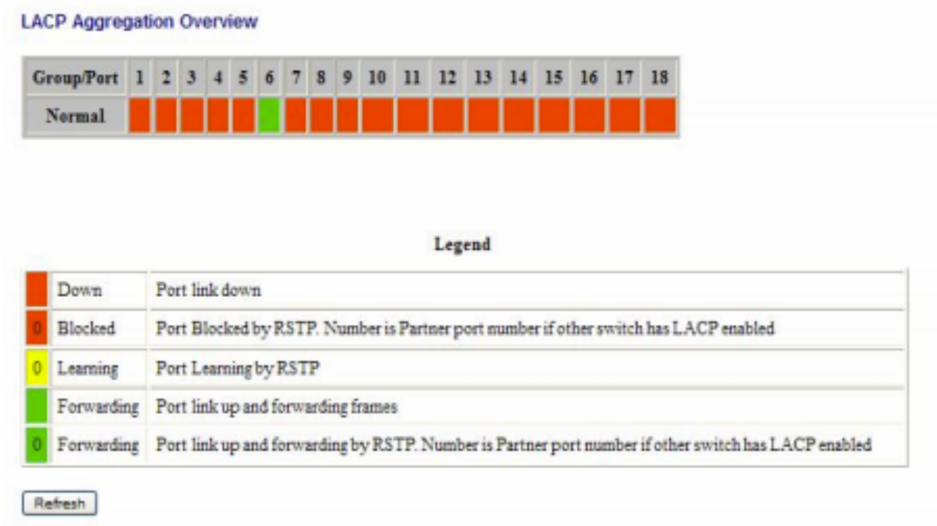
Statistics for Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	0	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Alignment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Figure 3-2

LACP Status

LACP Aggregation Overview



LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Normal	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

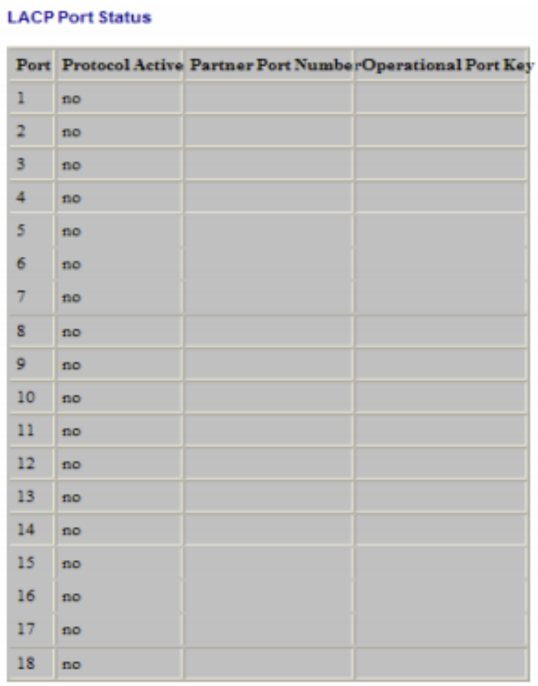
Legend

🟥	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
🟩	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Figure 3-3-1

- ➤ Port: Port number.
- ➤ Port Active: Shows if the port is a member of an active LACP group.
- ➤ Partner Port Number: A list of the ports attached to the remote end of this LAG link member.
- ➤ Operational Port Key: Current operational value of the key used by this LAG.

LACP Port Status



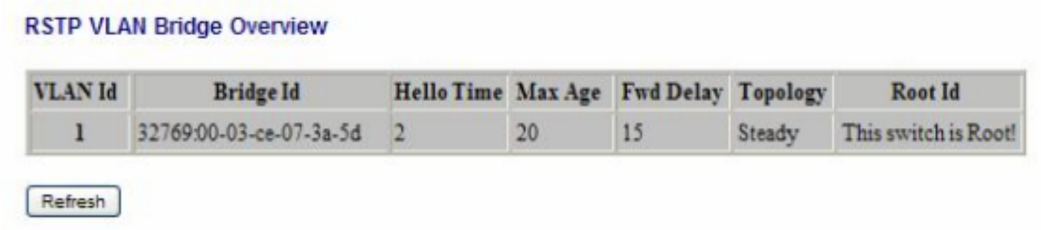
LACP Port Status

Port	Protocol Active	Partner Port Numbe	rOperational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		
9	no		
10	no		
11	no		
12	no		
13	no		
14	no		
15	no		
16	no		
17	no		
18	no		

Figure 3-3-2

RSTP Status

RSTP VLAN Bridge Overview



RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-03-ce-07-3a-5d	2	20	15	Steady	This switch is Root!

Figure 3-4-1

Bridge ID: Show the switch's current bridge priority setting and bridge ID which stands for the MAC address of the switch

Hello Time: Interval (in seconds) with which the root device transmits configuration message

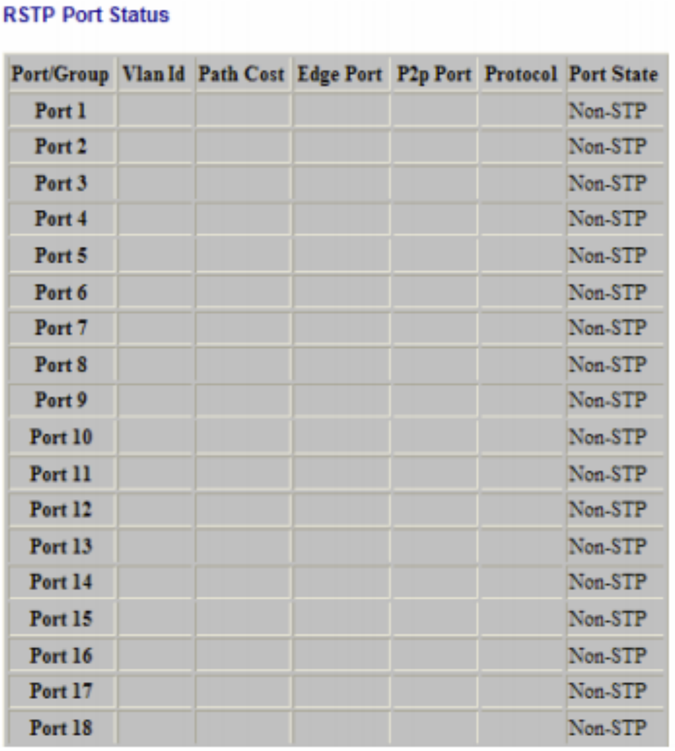
Max Age: The max. time (in seconds) a device waits without receiving configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages with regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from the device ports attached to the network.

Fwd Delay: The max. time (in seconds) the root device waits before changing state (i.e. discarding to learning to forwarding). This delay is required because every device should receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen to conflicting information that makes it return to a discarding state; otherwise, temporary data loops can occur.

Topology: Indicates if spanning tree topology is steady or undergoing reconfiguration. (The time required for reconfiguration is extremely short, so no values other than "steady" state are likely to be seen in this field)

Root ID: The priority and MAC address of the device in the Spanning Tree that the switch has accepted as the root device. Each port has been connected to the root device.

<ins>RSTP Port Status</ins>



RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP
Port 10						Non-STP
Port 11						Non-STP
Port 12						Non-STP
Port 13						Non-STP
Port 14						Non-STP
Port 15						Non-STP
Port 16						Non-STP
Port 17						Non-STP
Port 18						Non-STP

Figure 3-4-2

- ➤ Port/Group: The number of a port or the ID of a static trunk.
- ➤ Path Cost: The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower is the media, the higher is the cost.
- ➤ Edge Port: Shows if this port is functioning as an edge port, either through manual selection (see the RSTP Port Configuration table) or auto-detection. Note that if the switch detects another bridge connected to this port, the manual setting for Edge Port will be overridden, and the port functions as a point-to-point connection instead.
- ➤ P2P Port: Shows if this port is functioning as a Point-to-Point connection. The switch can automatically determine if the interface is attached to a point-to-point link or to shared media. If shared media is detected, the switch assumes that it is connected to two or more bridges.
- ➤ Protocol: Shows the spanning tree protocol functioning on this port, either RSTP or STP (STP-compatible mode).

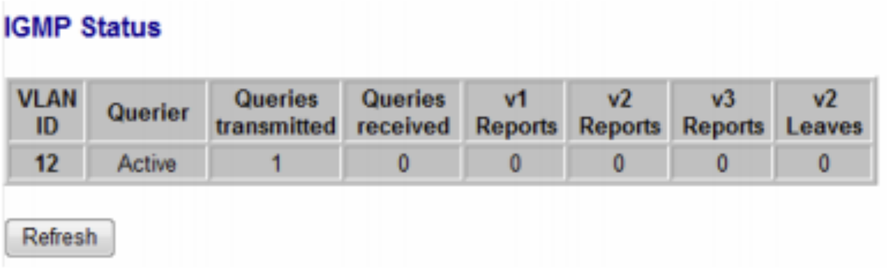
IGMP Status

IGMP Status

IGMP Status shows the IGMP Snooping statistics for the whole switch.

- ➤ VLAN ID: VLAN ID number.
- ➤ Querier: Shows whether Querying is enabled.
- ➤ Queries transmitted: Shows the number of transmitted Query packets.
- ➤ Queries received: Shows the number of received Query packets.
- ➤ v1 Reports: Shows the number of received v1 Report packets.
- ➤ v2 Reports: Shows the number of received v2 Report packets.
- ➤ v3 Reports: Shows the number of received v2 Report packets.

- ➤ v3 Leave: Shows the number of v3 leave packets received.



IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
12	Active	1	0	0	0	0	0

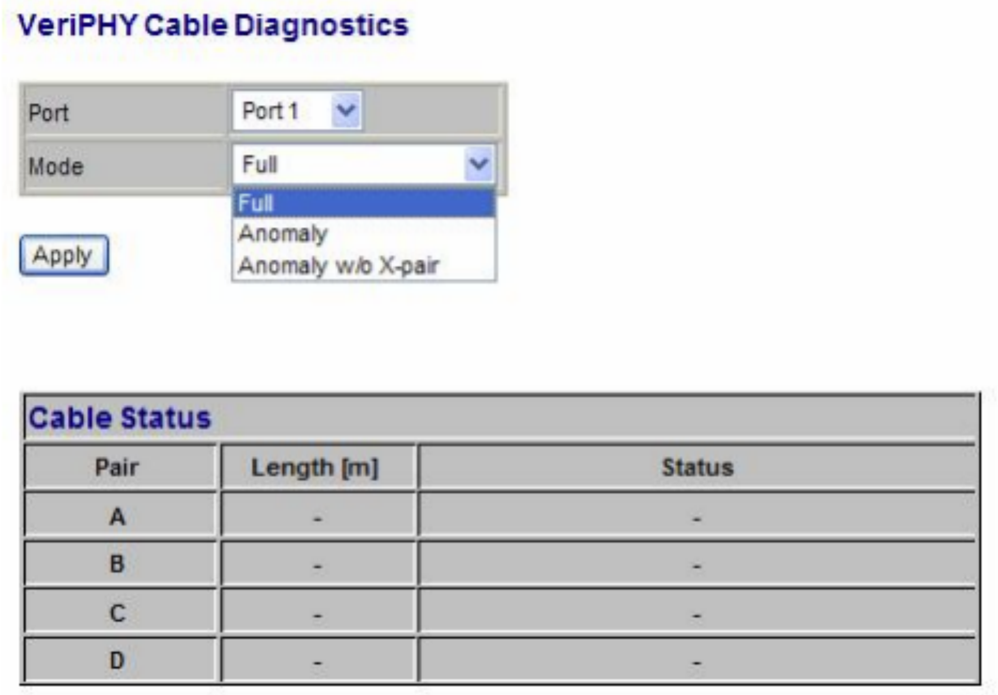
Figure 3-5

VeriPHY

VeriPHY Cable Diagnostics

User can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc..) and feedback a distance to the fault.

- ➤ Cable Diagnostics: Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.
- ➤ Cable Status: Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.



VeriPHY Cable Diagnostics

Port	Port 1
Mode	Full

Cable Status

Pair	Length [m]	Status
A	-	-
B	-	-
C	-	-
D	-	-

Figure 3-6

Ping

This command sends ICMP echo request packets to another node on the network.

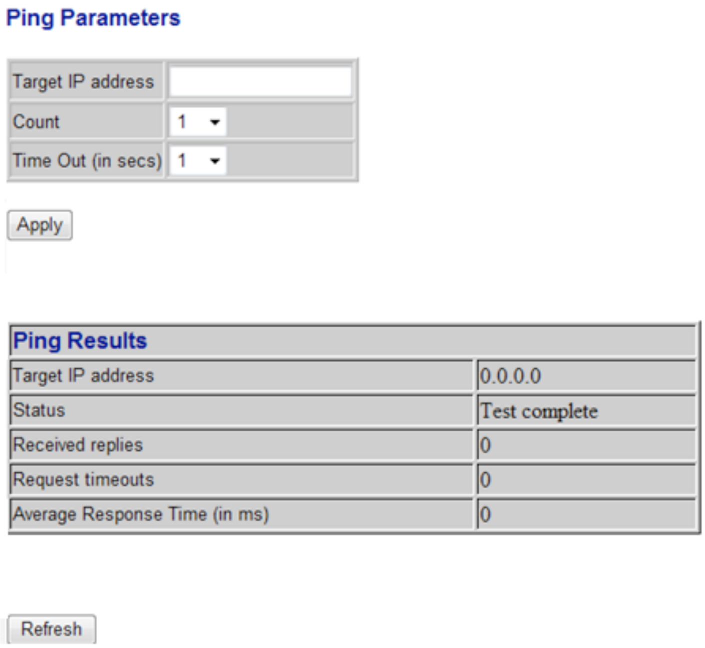
Ping Parameters

- ➤ Target IP Address: IP address of the host
- ➤ Count: Number of packets to send. Select between 1, 5, 10, 20. Default: 1
- ➤ Time Out: setting the time period of host is Ping. Select between 1,5, 10, 20. Default: 1

Use the ping command to see if another site on the network can be reached.
The following are some results of the ping command:

- ➤ Normal response: The normal response occurs in one to ten seconds, depending on network traffic.
- ➤ Destination does not respond: If the host does not respond, a "timeout" appears in ten seconds.
- ➤ Destination unreachable: The gateway for this destination indicates that the destination is unreachable.
- ➤ Network or host unreachable: The gateway found no corresponding entry in the route table.

Press <Esc> to stop pinging.



Ping Parameters

Target IP address	
Count	1
Time Out (in secs)	1

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

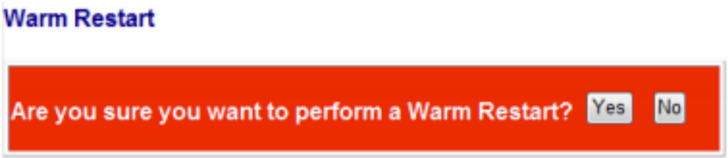
Figure 3-7

Maintenance

There are many ways to reboot the switch, such as power up, hardware reset, software reset. Press RESET button situated on the front panel to reset the device and to retrieve default settings. After upgrading software, reboot the device to apply new configuration. The procedure of software reset is explained below.

Reboot Device (Warm Restart)

Press Yes button to restart the switch, the reset is complete when the power lights stop blinking.



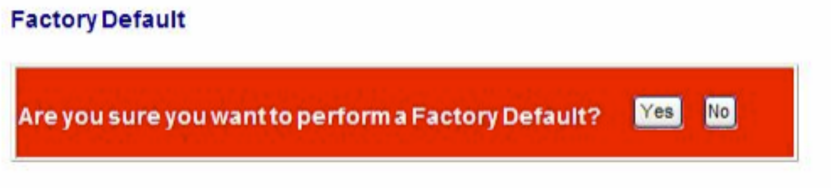
Warm Restart

Are you sure you want to perform a Warm Restart?

Figure 4-1

Load Default Setting (Factory Default)

Factory Default retrieves default settings and replaces the current configuration. Except IP address setting, all settings are restored to the factory defaults. If you want to restore all configurations including the IP address, press “RESET” button situated on the front panel.



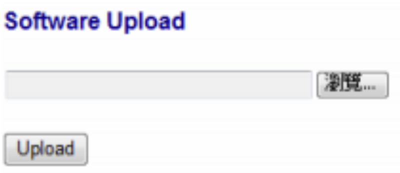
Factory Default

Are you sure you want to perform a Factory Default?

Figure 4-2

Firmware Updating (Software upload)

Select “Upgrade Firmware” from the Tools drop-down list then click on the “Browse” button to select the firmware file. Click the APPLY button to upgrade the selected switch firmware file. You can download firmware files from the Support section of your local supplier.



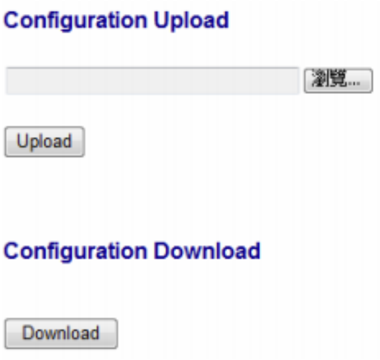
Software Upload

Figure 4-3

Backup/Recovery (Configuration File Transfer)

Configuration file transfer allows you to save the switch’s current configuration or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station. Select “Upload” the configuration file to save a configuration or

"Download" to restore a configuration. Use the Browse button to choose a file location on the web management station, or to find a saved configuration file.



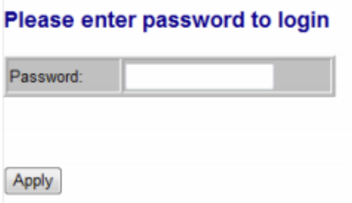
Configuration Upload

Configuration Download

Figure 4-4

Logout

The administrator has write access for all parameters governing the onboard agent. User should therefore assign a new administrator password as soon as possible, and store it in a safe place.



Please enter password to login

Password:

Figure 4-5

Contacts

Italy: +39 0461.1715112 support@wildix.com	**France:** +33 176 747 980 support@wildix.fr