User Manual

SUN-1000SFPM

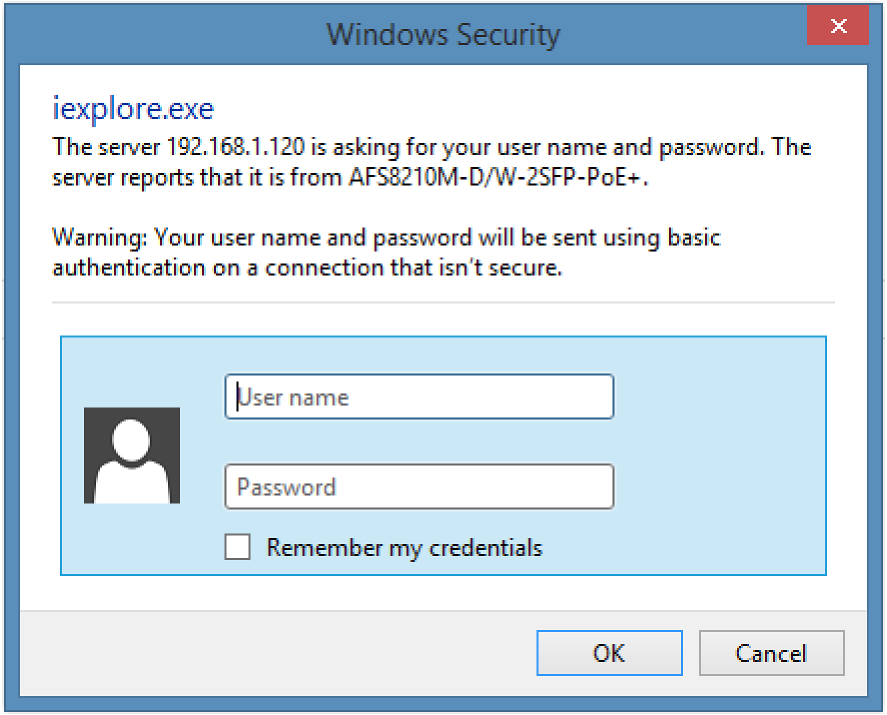
Industrial Management Fiber Switch

English

Content

1. Web-Based Management

Input the IP address that appears on the label into browser and the login screen will pop up as Fig. 18.



The server 192.168.1.120 is asking for your user name and password. The server reports that it is from AFS8210M-D/W-2SFP-PoE+.

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

Fig. 18 Login Screen

Default User Name:	admin
Default Password:	(no password)

Then click “OK”, you will enter the first page of the system.

First page when entering the system: seen as Fig. 19

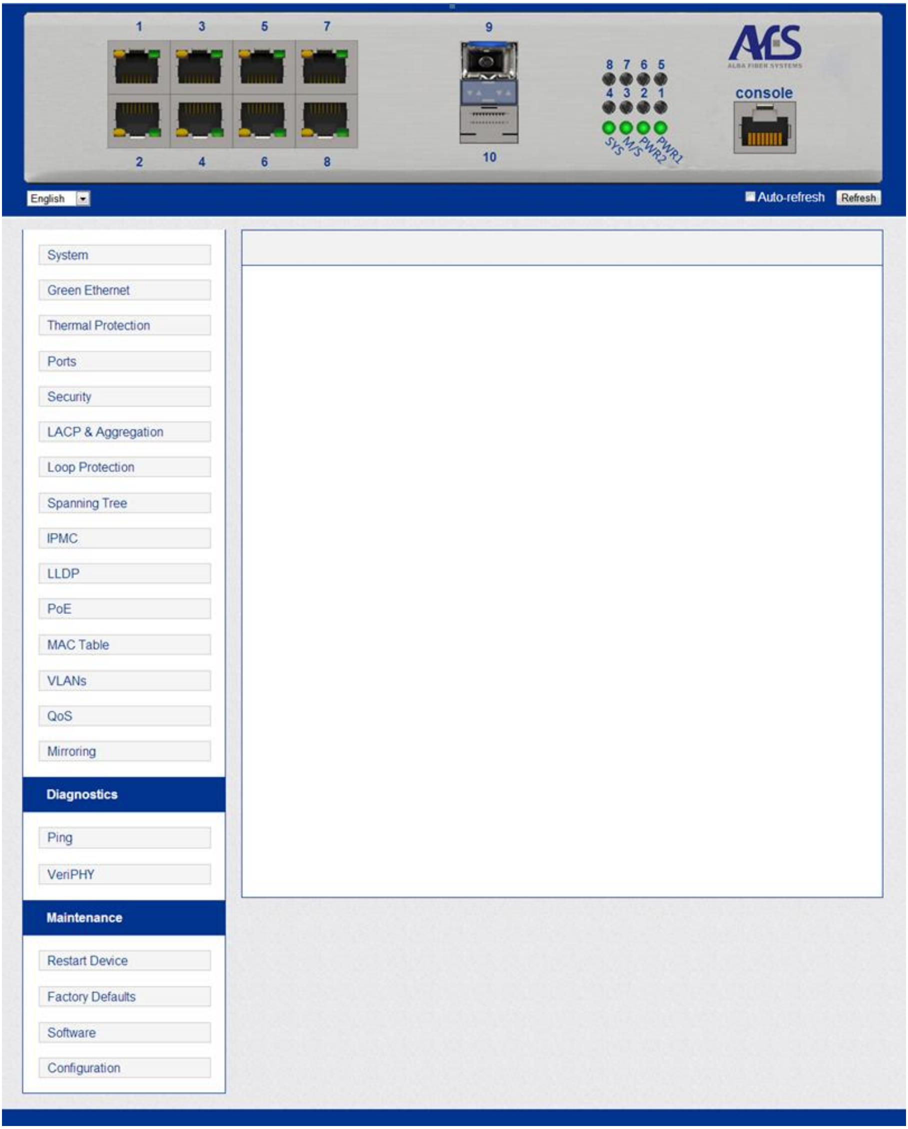


Fig. 19

2. Systems

2.1 System Information Configuration

Configuring memorial name and information for the switch, such as contact information, system name, location of the switch, and time zone offset.

PATH

Web	System, Information
CLI	**System>**

PARAMETERS

These parameters are displayed:

■ System Contact – Administrator responsible for the system. (Maximum length: 255 characters)

■ System Name – Name assigned to the switch system. (Maximum length: 255 characters)

■ System Location – Specifies the system location. (Maximum length: 255 characters)

■ System Time zone Offset (minutes) – Sets the time zone as an offset from Greenwich Mean Time (GMT). Negative values indicate a zone before (east of) GMT, and positive values indicate a zone after (west of) GMT.

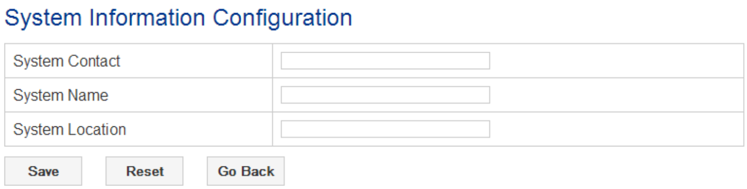
WEB INTERFACE

To configure system information:

1. Click System, and then Information.
2. Specify the contact information for the system administrator, as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.

3. Click Save.

Fig. 20: System Information Configuration


System Information Configuration

System Contact	
System Name	
System Location	

Fig. 20 System Information Configuration

CLI COMMANDS

Configure the memorial information for the switch.

Contact	Configure system contact
Name	Configure device name
Location	Configure system location
Time zone	Configure system time zone
Setup	Setup system information

2.2 IP Configuration

This function used to control the switch CPU port traffic, which used for management. The IP address for the switch is obtained via DHCP by default for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

NOTE: An IPv4 address for this switch is obtained via DHCP by default. If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.2.10 and subnet mask 255.255.255.0. You can manually configure a specific IP address, or direct the device to obtain an address from a DHCP server. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the CLI program.

PATH

Web	System, IP
CLI	**IP>**

PARAMETERS

These parameters are displayed:

IP Configuration

● **DHCP Client** – Specifies whether IP functionality is enabled via Dynamic Host Configuration Protocol (DHCP). If DHCP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP values can include the IP address, subnet mask, and default gateway. (Default: Enabled)

● **IP Address** – Address of the VLAN specified in the VLAN ID field. This should be the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

● **IP Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

● **IP Router** – IP address of the gateway router between the switch and management stations that exist on other network segments.

● **VLAN ID** – ID of the configured VLAN. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4095; Default: 1)

● **DNS Server** – A Domain Name Server to which client requests for mapping host names to IP addresses are forwarded.

IP DNS Proxy Configuration

● **DNS Proxy** – If enabled, the switch maintains a local database based on previous responses to DNS queries forwarded on behalf of attached clients. If the required information is not in the local database, the switch forwards the DNS query to a DNS server, stores the response in its local cache for future reference, and passes the response back to the client.

CLI COMMANDS

Address	Set up the IP address
Configuration	Display the configuration of the switch
DHCP	If the IP address assigned by DHCP or not
Route	Configure the routing information

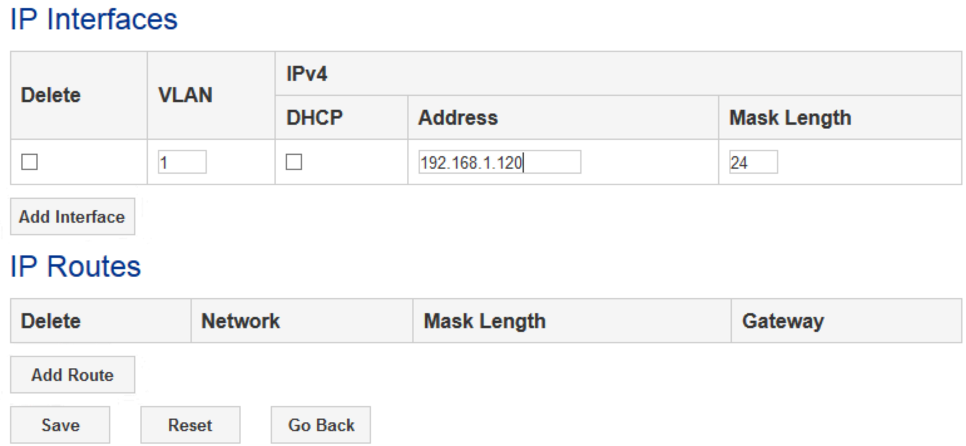
WEB INTERFACE

To configure an IP address:

1. Click System, IP Status, and then click the Edit button at the bottom of the page.

2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Save.

Fig. 21 shows IP Configuration



IP Interfaces

Delete	VLAN	IPv4		
		DHCP	Address	Mask Length
□	1	□	192.168.1.120	24

IP Routes

Delete	Network	Mask Length	Gateway

Fig. 21 IP Configuration

2.3 SNTP Configuration

Use the SNTP Configuration page to specify the Network Time Protocol (SNTP) servers to query for the current time. SNTP allows the switch to set its internal clock based on periodic updates from an NTP time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last boot up.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to five time server IP addresses. The switch will attempt to poll each server in the configured sequence.

PATH

Web	System, SNTP
CLI	**IP/SNTP>**

PARAMETERS

These parameters are displayed:

■**Mode** – Enables or disables SNTP client requests.

■**Server** – Sets the IPv4 address for up to five time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. The polling interval is fixed at 15 minutes

.

CLI COMMANDS

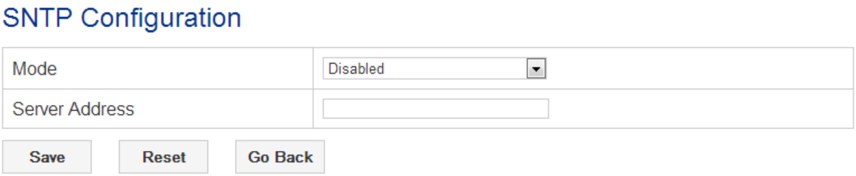
Configuration	Configuration Show SNTP configuration.
Mode	Set or show the SNTP mode to enable or disable.
Server Add	Add the SNTP server entry
Server Delete	Deleted the SNTP server entry

WEB INTERFACE

To configure the SNTP servers:

1. Click System, Information, then click the SNTP button.
2. Enter the IP address of up to five time servers.
3. Click Save.

Fig. 22 SNTP Configuration



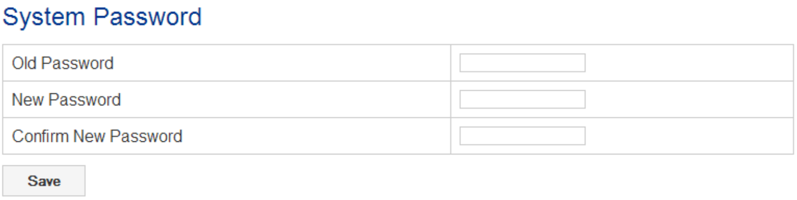
SNTP Configuration

Mode	Disabled
Server Address	

Fig. 22 SNTP Configuration

2.4 System Password

Default Password for entering the system is no password. Password can be set and changed as following Fig. 23



System Password

Old Password	
New Password	
Confirm New Password	

Fig. 23 System Password Setting Interface

2.5 Green Ethernet

This page allows the user to configure the port power savings features. What is EEE? EEE stands for “Energy-Efficient Ethernet” and is a power savings option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE capable, the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for them. The EEE port settings relate to the currently selected stack unit, as reflected by the page header.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

PATH

Web	GreenEthernet
CLI	**GreenEthernet>**

PARAMETERS

These parameters are displayed:

■**Led timers** - Set or show the time and intensity for the LEDs.

■**Port Power** - Set or show the port PHY power mode.

■**Led delete_timer** - Deletes a timer.

■**Port EEE Configuration** - Show EEE configuration.

■**Led maintenance** - Set or show the maintenance settings.

■**Port EEE Mode** - Set or show the EEE mode.

■**Led configuration** - Show Led Power Reduction configuration.

■**Port EEE Optimize** - Set or show the EEE optimize settings. EEE can be set to optimize for most power saving or least traffic latency.

■**Port EEE Urgent_queues** - Set or show EEE Urgent queues.

■**Port Status** - Showing current power savings status.

WEB INTERFACE

To configure global and port-specific Port Power Savings settings:

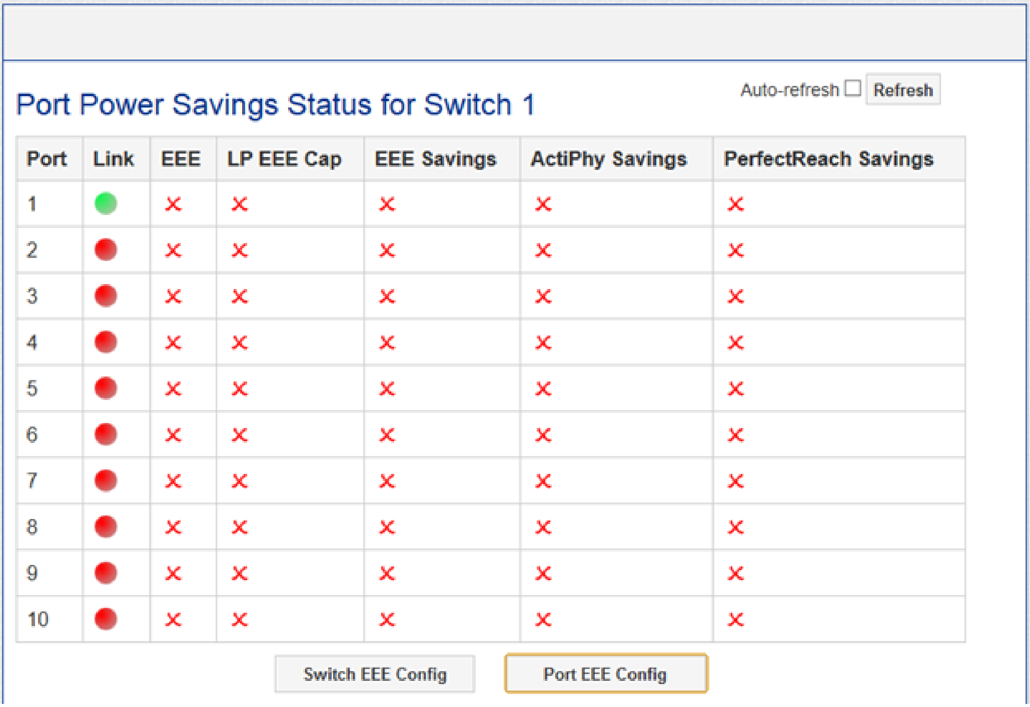
1. Click GreenEthernet, and then click the Port EEE Config button.

2. Set the global GreenEthernet parameters, including the method used for optimizing EEE by Power or Latency to determine port power savings.

3. Specify the Port Power Savings port power allocation priority by selecting (checking) the, ActiPHY, PerfectReach, EEE, and EEE Urgent Queues options for each or all of the ports as desired.

4. Click Save.

Port Power Saving Status Page Fig 24:



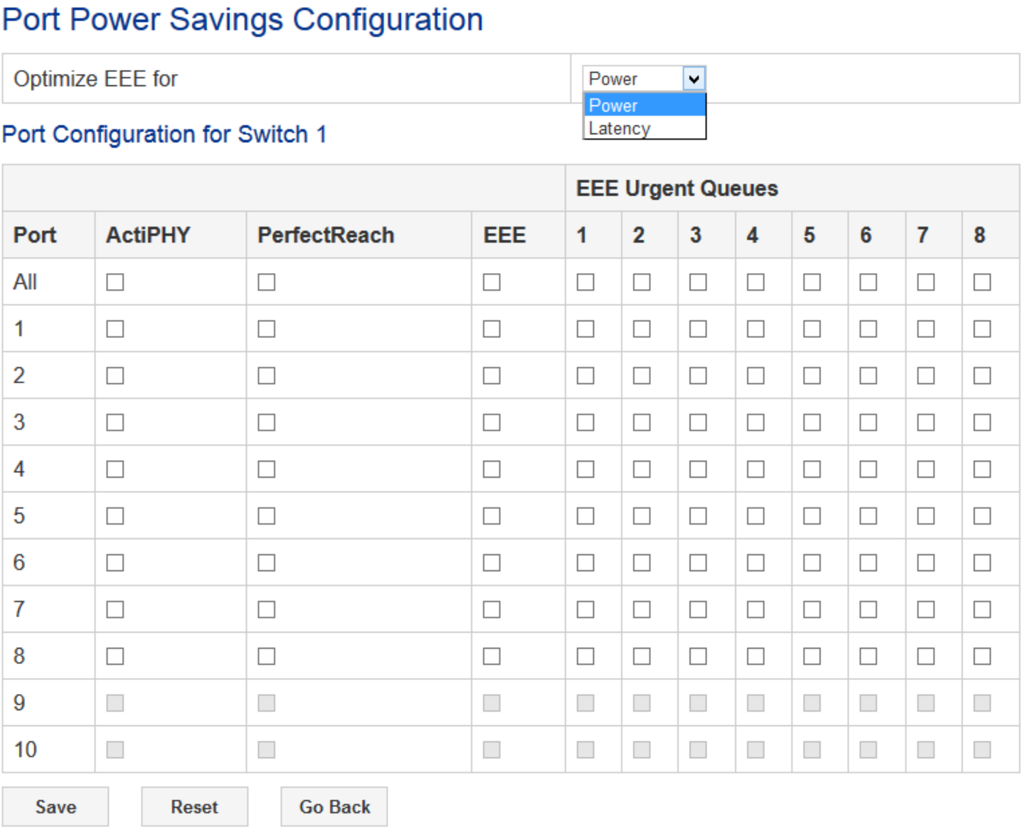
Auto-refresh □

Port Power Savings Status for Switch 1

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	🟢	✗	✗	✗	✗	✗
2	🔴	✗	✗	✗	✗	✗
3	🔴	✗	✗	✗	✗	✗
4	🔴	✗	✗	✗	✗	✗
5	🔴	✗	✗	✗	✗	✗
6	🔴	✗	✗	✗	✗	✗
7	🔴	✗	✗	✗	✗	✗
8	🔴	✗	✗	✗	✗	✗
9	🔴	✗	✗	✗	✗	✗
10	🔴	✗	✗	✗	✗	✗

Fig 24 Port Power Saving Status Page:

Configuring GreenEthernet Settings seen the following Fig. 24



Port Power Savings Configuration

Optimize EEE for	Power ▾

Port Configuration for Switch 1

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
All	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□	□	□	□

Fig. 24 Configuring GreenEthernet Settings seen the following

■**Port** – The switch port number of the logical port.

■**ActiPHY** – Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for short moment in order to determine if a cable is inserted.

■**PerfectReach** – Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.

■**EEE** – Controls whether EEE is enabled for this switch port.

2.6 PoE

Use the Power over Ethernet Configuration page to set the maximum PoE power provided to a port, the maximum power budget for the switch (power available to all RJ-45 ports), and the port PoE operating mode, power allocation priority, and the maximum power allocated to each port. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

Command Usage of PoE

■The switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-compliant devices (IEEE 802.3af or 802.3at).

■This switch supports both the IEEE 802.3af PoE and IEEE 802.3at-2009 PoE Plus standards. To ensure that the correct power is supplied to powered devices (PD) compliant with these standards, the first detection pulse from the switch is based on 802.3af to which the 802.3af PDs will respond normally. It then sends a second PoE Plus pulse that causes an 802.3at PD to respond as a Class 4 device and with the PD such as duty-cycle, peak and average power needs.

■ All the RJ-45 ports support both the IEEE 802.3af and IEEE 802.3at standards. The total PoE power delivered by all ports cannot exceed the maximum power budget of 80W.

■The switch’s power management enables individual port power to be controlled within the switch’s power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

■ Ports can be set to one of four power priority levels, critical, high, medium, or low. To control the power supply within the switch’s budget, ports set at critical to medium priority have power enabled in preference to those ports set at low priority. For example, when a device connected to a port is set to critical priority, the switch supplies the required power, if necessary by denying power to ports set for a lower priority during boot up.

NOTE: For more information on using the PoE provided by this switch refer to the Installation Guide.

PATH

Web	PoE
CLI	**POE>**

PARAMETERS

These parameters are displayed:

■ Reserved Power determined by - There are three modes for configuring how the ports or attached Powered Devices (PD) may reserve power:

◇ Class – Each port automatically determines how much power to reserve according to the class to which the connected PD belongs, and reserves power accordingly. Four different port classes exist, including 4, 7, 15.4 or 34.2 Watts. In this mode, the Maximum Power fields have no effect.

◇Allocation – The amount of power that each port may reserve is specified. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

◇LLDP-MED – This mode is similar to the Class mode expect that each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect For all modes, if a port uses more power than the power reserved for that port, it is shut down.

■ Power Management Mode – There are two modes for configuring when to shut down the ports:

◇Actual Consumption – Ports are shut down when actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the power reserved for that port. The ports are shut down according to port priority. If two ports have the same priority, the port with the highest port number is shut down.

◇Reserved Power – Ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

■ Primary Power Supply - The power budget for the switch. If devices connected to the switch require more power than the switch's budget, the port power priority settings are used to control the supplied power. (Range: 0-80 Watts)

■ Port – Port identifier.

■PoE Mode – The PoE operating mode for a port includes these options:

◇ Disabled – PoE is disabled for the port.

◇PoE – Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)

◇PoE+ – Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 34.2W)

■ Priority - Port priority is used when remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

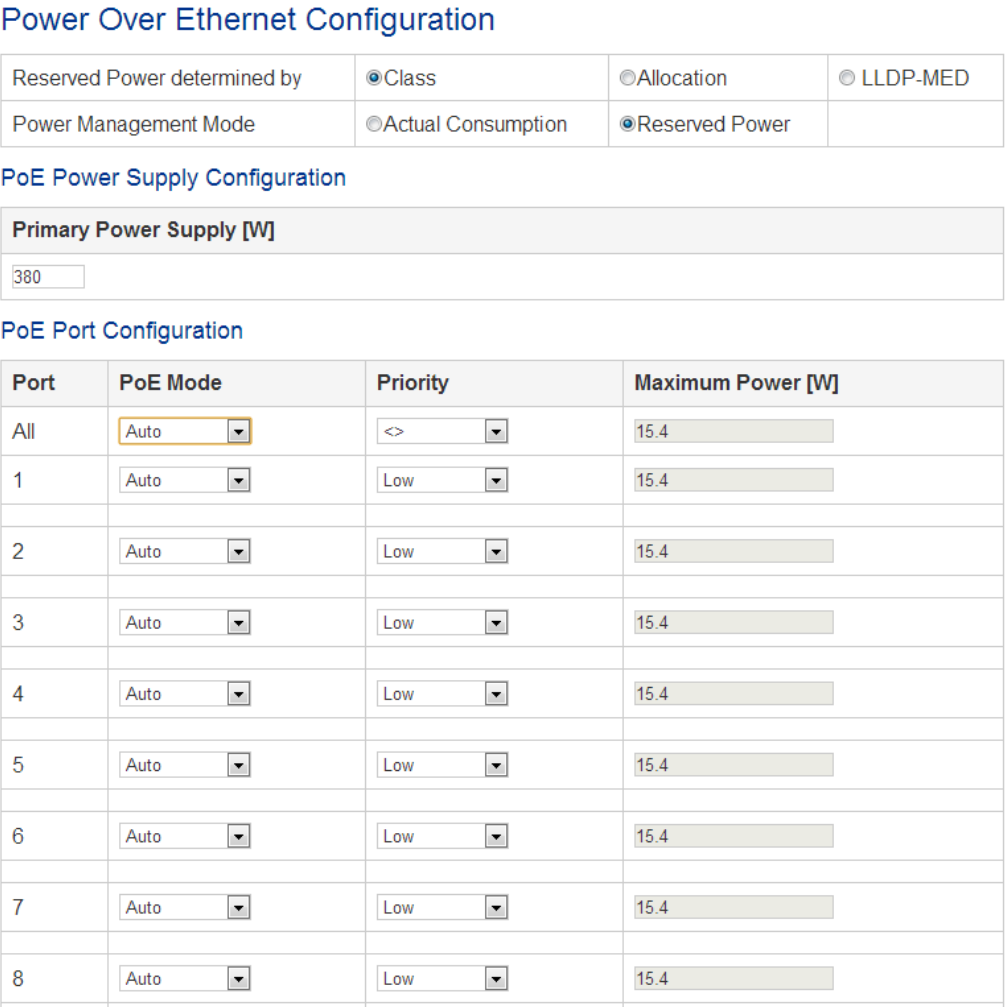
■ Maximum Power - The maximum power that can be delivered to a remote device.(Range: 0-34.2 Watts depending on the PoE mode)

WEB INTERFACE

To configure global and port-specific PoE settings:

1. Click PoE.
2. Set the global PoE parameters, including the method used to determine reserved port power, the method by which port power is shut down, and the switch’s overall power budget.
3. Specify the port PoE operating mode, port power allocation priority, and the port power budget.
4. Click Save.

Configuring PoE Settings seen the following Fig. 25



Power Over Ethernet Configuration

Reserved Power determined by	●Class	○Allocation	○ LLDP-MED
Power Management Mode	○Actual Consumption	●Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]
380

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
All	Auto	<>	15.4
1	Auto	Low	15.4
2	Auto	Low	15.4
3	Auto	Low	15.4
4	Auto	Low	15.4
5	Auto	Low	15.4
6	Auto	Low	15.4
7	Auto	Low	15.4
8	Auto	Low	15.4

Fig. 25 Configuring PoE

2.7 Displaying PoE Status

Use the Power Over Ethernet Status to display the status for all PoE ports, including the PD class, requested power, allocated power, power and current used, and PoE priority.

PATH

Web	PoE
CLI	**PoE>Status>**

PARAMETERS

These parameters are displayed:

■ Local Port – The port on this switch which received the LLDP frame.

■ PD class – Each PD is classified according to the maximum power it will use. The PD classes include:

◇ Class 0: Max. power 15.4 W

◇ Class 1: Max. power 4.0 W

◇ Class 2: Max. power 7.0 W

◇ Class 3: Max. power 15.4 W

◇ Class 4: Max. power 30.0 W

■ Power Requested – Amount of power the PD wants to be reserved.

■ Power Allocated – Amount of power the switch has allocated for the PD.

■ Power Used – How much power the PD is currently using.

■ Current Used – How much current the PD is currently using

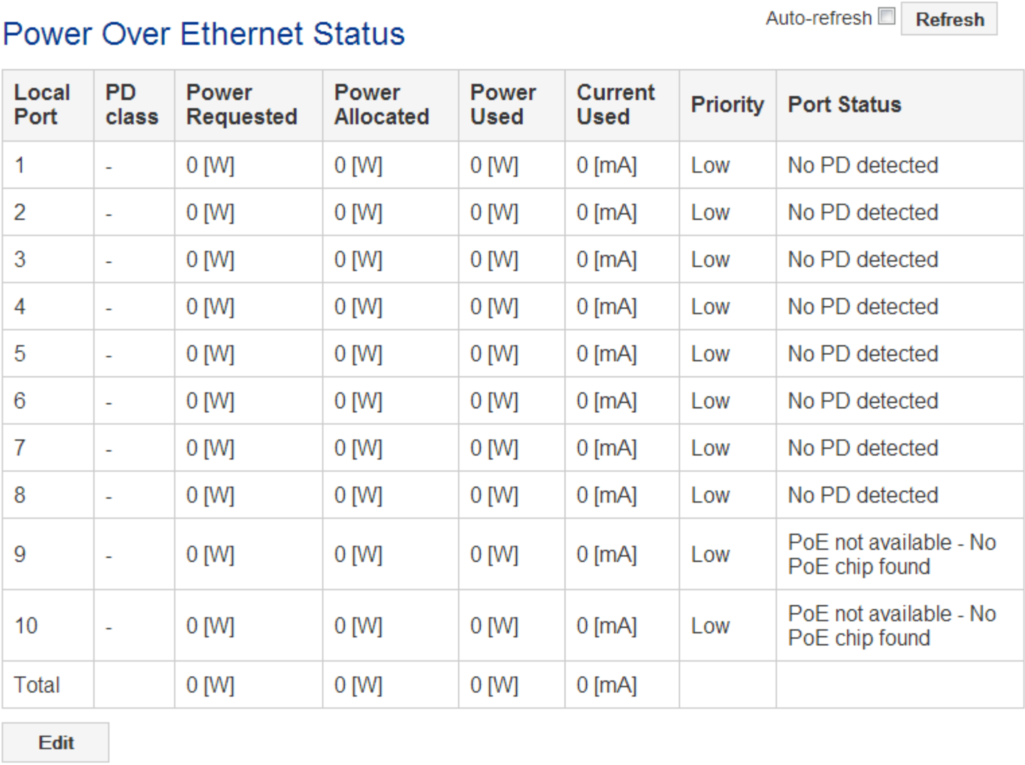
■ Priority – The port's configured priority level (see page 155).

■Port Status – PoE service status for the attached device.

WEB INTERFACE

To display the status for all PoE ports, click PoE.

Power over Ethernet Status seen as following Fig. 26



Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Fig. 26 Power over Ethernet Status

2.8 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

6.4.1 Configuring Link Layer Discovery Protocol

Use the LLDP Configuration page to set the timing attributes used for the transmission of LLDP advertisements, and the device information which is advertised.

PATH

Web	LLDP
CLI	**LLDP>**

PARAMETERS

These parameters are displayed:
LLDP Timing Attributes

■Tx Interval – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds) This attribute must comply with the following rule: (Transmission Interval * Transmission Hold Time) ≤ 65536, and Transmission Interval ≥ (4 * Transmission Delay)
■Tx Hold – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 3) the time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: (Transmission Interval * Transmission Hold Time) ≤ 65536. Therefore, the default TTL is 30*3 = 90 seconds.
■Tx Delay – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds) The transmit delay is used to prevent

a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission. This attribute must comply with the rule: (4 * Transmission Delay) ≤ Transmission Interval

■TxReinit – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds) When LLDP is re-initialized on a port, all information in the remote system's LLDP MIB associated with this port is deleted. LLDP Interface Attributes

■ Port – Port identifier.

■ Mode – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Disabled, Enabled – Tx Rx, Rx only, Tx only; Default: Disabled)

■ CDP Aware – Enables decoding of Discovery Protocol frames. (Default: Disabled) If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

◇ CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field.

◇ CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

◇ CDP TLV "Port ID" is mapped into the LLDP "Port ID" field.

◇ CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field.

◇ Both the CDP and LLDP support "system capabilities," but the CDP capabilities cover capabilities that are not part of LLDP. These capabilities are shown as "others" in the LLDP neighbors table. If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch. When CDP awareness for a port is disabled, the CDP information is not removed immediately, but will be removed when the hold time is exceeded.

Optional TLVs - Configures the information included in the TLV field of advertised messages.

■ Port Descr – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

■ Sys Name – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see page 41.

■ Sys Descr – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

■ Sys Capa – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

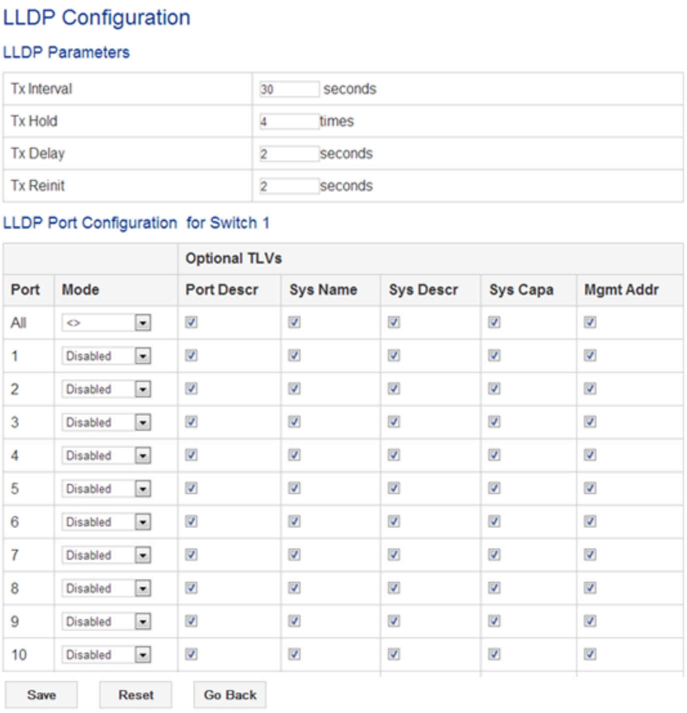
■MgmtAddr – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

WEB INTERFACE

To configure LLDP timing and advertised TLVs:

1. Click LLDP.
2. Modify any of the timing parameters as required.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Enable or disable decoding CDP frames.
5. Specify the information to include in the TLV field of advertised messages.
6. Click Save.

LLDP Configuration seen as following Fig. 27



LLDP Configuration

LLDP Parameters

Tx Interval	30 seconds
Tx Hold	4 times
Tx Delay	2 seconds
Tx Reinit	2 seconds

LLDP Port Configuration for Switch 1

		Optional TLVs				
Port	Mode	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
All	<>	☑	☑	☑	☑	☑
1	Disabled	☑	☑	☑	☑	☑
2	Disabled	☑	☑	☑	☑	☑
3	Disabled	☑	☑	☑	☑	☑
4	Disabled	☑	☑	☑	☑	☑
5	Disabled	☑	☑	☑	☑	☑
6	Disabled	☑	☑	☑	☑	☑
7	Disabled	☑	☑	☑	☑	☑
8	Disabled	☑	☑	☑	☑	☑
9	Disabled	☑	☑	☑	☑	☑
10	Disabled	☑	☑	☑	☑	☑

Fig. 27 LLDP Configuration

6.4.2 Displaying LLDP Information

Use the monitor pages for LLDP to display information advertised by LLDP neighbors and statistics on LLDP control frames.

Use the LLDP Neighbor Information page to display information about devices connected directly to the switch’s ports which are advertising information through LLDP.

PATH

Web	LLDP, Neighbors
CLI	**LLDP>Info**

PARAMETERS

These parameters are displayed:

■ Local Port – The local port to which a remote LLDP-capable device is attached.

■ Chassis ID – An octet string indicating the specific identifier for the particular chassis in this system.

■ Remote Port ID – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

■ System Name – A string that indicates the system’s assigned name.

■ Port Description – A string that indicates the port’s description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

■ System Capabilities – The capabilities that define the primary function(s) of the system as shown in the following table:

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Table 13: System Capabilities

ID Basis	Reference
Other	–
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011

DOCSIS cable Device	IETF RFC 2669 and IETF RFC 2670
Station only	IETF RFC 2011

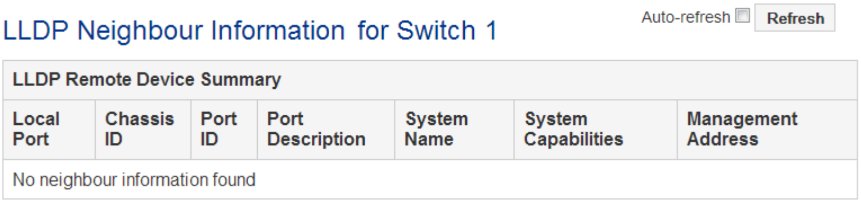
When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

■ Management Address – The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser to the neighbor's management interface.

WEB INTERFACE

To display information about LLDP neighbors; click LLDP, Neighbors.

LLDP Neighbor Information seen as following Fig. 28



LLDP Neighbour Information for Switch 1

LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

Fig. 28 LLDP Neighbor Information

2.9 Ports

Port Configuration

Use the Port Configuration page to configure the connection parameters for each port. This page includes options for enabling auto-negotiation or manually setting the speed and duplex mode, enabling flow control, setting the maximum frame size, specifying the response to excessive collisions, or enabling power saving mode.

PATH

Web	Ports
CLI	**Port>**

PARAMETERS

These parameters are displayed:

■**Link** – Indicates if the link is up or down.

■**Speed**–Sets the port speed and duplex mode using auto-negotiation or manual selection. The following options are supported:

◇Disabled - Disables the interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.

◇Auto - Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities.

◇1Gbps FDX - Supports 1 Gbps full-duplex operation

◇ 100Mbps FDX - Supports 100 Mbps full-duplex operation

◇ 100Mbps HDX - Supports 100 Mbps half-duplex operation

◇ 10Mbps FDX - Supports 10 Mbps full-duplex operation

◇ 10Mbps HDX - Supports 10 Mbps half-duplex operation

(Default: Auto negotiation enabled; Advertised capabilities for RJ-45: 1000BASE-T - 10half, 10full, 100half, 100full, 1000full; SFP: 1000BASE-SX/LX/LH - 1000full)

NOTE: The 1000BASE-T standard does not support forced mode. Auto negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

■**Flow Control**–Flow control can eliminate frame loss by “blocking”traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full duplex operation. (Default: Disabled)

When auto-negotiation is used, this parameter indicates the flow
control capability advertised to the link partner. When the speed and duplex mode are manually set, the Current Rx field indicates whether pause frames are obeyed by this port, and the Current Tx field indicates if pause frames are transmitted from this port.

Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

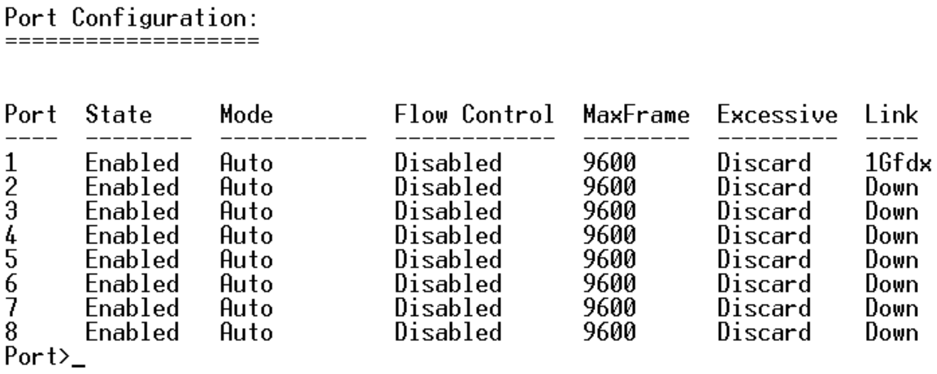
■ Maximum Frame Size–Sets the maximum transfer unit for traffic crossing the switch. Packets exceeding the maximum frame size are dropped. (Range: 9600-1518 bytes; Default: 9600 bytes)

■ Excessive Collision Mode–Sets the response to take when excessive transmit collisions are detected on a port.

◇ Discard - Discards a frame after 16 collisions (default).
◇ Restart - Restarts the back-off algorithm after 16 collisions.

CLI COMMANDS

Configuration, overall information for all the ports on the switch seen as following Fig. 29 and Fig. 30



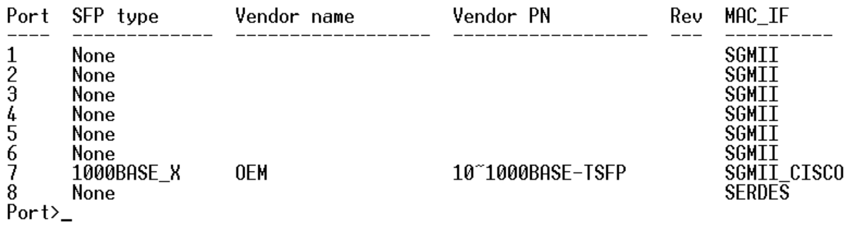
```
Port Configuration:
===================

Port  State     Mode         Flow Control  MaxFrame  Excessive  Link
----  --------  -----------  ------------  --------  ---------  ----
1     Enabled   Auto         Disabled      9600      Discard    1Gfdx
2     Enabled   Auto         Disabled      9600      Discard    Down
3     Enabled   Auto         Disabled      9600      Discard    Down
4     Enabled   Auto         Disabled      9600      Discard    Down
5     Enabled   Auto         Disabled      9600      Discard    Down
6     Enabled   Auto         Disabled      9600      Discard    Down
7     Enabled   Auto         Disabled      9600      Discard    Down
8     Enabled   Auto         Disabled      9600      Discard    Down
Port>_
```

Fig. 29 Overall information for all the ports

Configuration	Set or show the port speed and duplex mode. Syntax: Configuration [<port_list>] [up|down] Port_list is used to specified the ports that apply for this command, e.g. to show the ports 1 4,5,6 configuration, the syntax like this: Configuration 1, 4-5
Mode	Set or show the port speed and duplex mode Syntax: Mode[<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx|sfp_auto_ams|1000x_ams|100fx_ams|1000x|100fx]
Flow Control	Set or show the port flow control mode as in Fig. 23 flow control column

MaxFrame	Set or show the port MTU as in Fig.23 max frame column
Excessive	Set or show the port excessive collision mode as in Fig.23 excessive column
SFP	show the detected SFP type



```
Port  SFP type       Vendor name         Vendor PN           Rev  MAC_IF
----  -------------  ------------------  ------------------  ---  ----------
1     None                                                        SGMII
2     None                                                        SGMII
3     None                                                        SGMII
4     None                                                        SGMII
5     None                                                        SGMII
6     None                                                        SGMII
7     1000BASE_X     OEM                 10~1000BASE-TSFP         SGMII_CISCO
8     None                                                        SERDES
Port>_
```

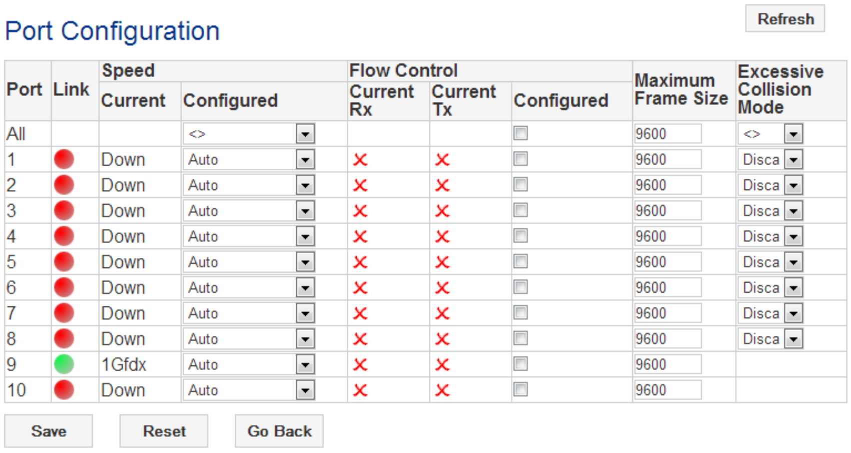
Fig. 30 Overall information for all the ports

WEB INTERFACE

To configure port connection settings:

1. Click Ports.
2. Make any required changes to the connection settings.
3. Click Save.

Port Configuration seen as following Fig. 31



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
All			<>			□	9600	<>
1	🔴	Down	Auto	✗	✗	□	9600	Disca
2	🔴	Down	Auto	✗	✗	□	9600	Disca
3	🔴	Down	Auto	✗	✗	□	9600	Disca
4	🔴	Down	Auto	✗	✗	□	9600	Disca
5	🔴	Down	Auto	✗	✗	□	9600	Disca
6	🔴	Down	Auto	✗	✗	□	9600	Disca
7	🔴	Down	Auto	✗	✗	□	9600	Disca
8	🔴	Down	Auto	✗	✗	□	9600	Disca
9	🟢	1Gfdx	Auto	✗	✗	□	9600	
10	🔴	Down	Auto	✗	✗	□	9600	

Fig. 31 Port Configuration

6.5.2 Loop Protection

This page is used to configure Loopback Detection function for each port. Loopback on port will cause packet storm in switch.

For each port, if Loopback Detection is enabled and Tx Mode is enable, the port is actively generating loop protection PDU's. If loopback is found, the action could be shutdown port or log it. The shutdown time could be configured for some period.

PATH

Web	Loop Protection
CLI	**Loop>Protect>Loop/Protect>**

PARAMETERS

General Settings

■Enable Loop Protection

◇Disabled – Disable the Loop Protection (as a whole)

◇ Enabled - Enable the Loop Protection (as a whole)

■Transmission Time - The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

■Shutdown Time - The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

■ Port - The switch port number of the port.

■Enable - Controls whether loop protection is enabled on this switch port.

■Action – while the congestion occur on the port, following activity apply

◇Shutdown Port – Shutdown port while congestion

◇Shutdown Port and Log – Shutdown port and log this information

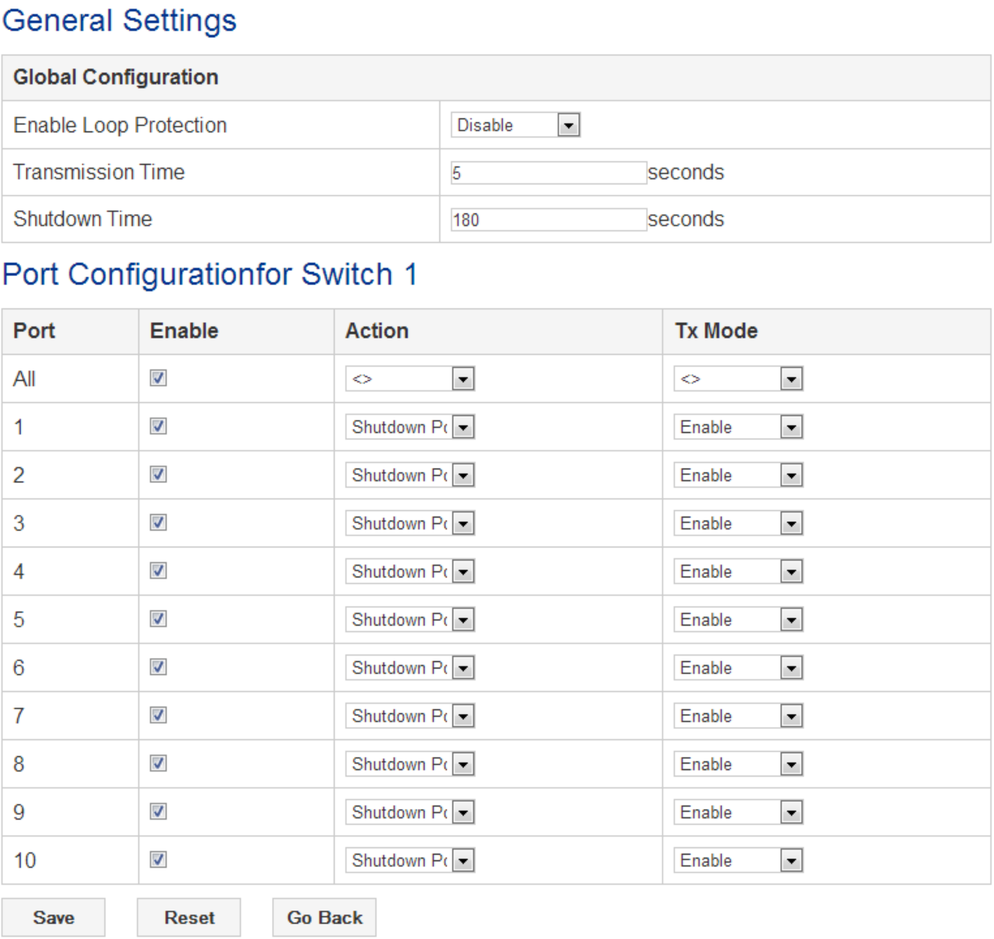
◇Log Only – Log only

WEB INTERFACE

To configure port connection settings:

1. Click Ports.
2. Make any required changes to the connection settings.
3. Click Save.

Interface of port configuration seen as following Fig. 32



General Settings

Global Configuration	
Enable Loop Protection	Disable ▾
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configurationfor Switch 1

Port	Enable	Action	Tx Mode
All	☑	<> ▾	<> ▾
1	☑	Shutdown P(▾	Enable ▾
2	☑	Shutdown P(▾	Enable ▾
3	☑	Shutdown P(▾	Enable ▾
4	☑	Shutdown P(▾	Enable ▾
5	☑	Shutdown P(▾	Enable ▾
6	☑	Shutdown P(▾	Enable ▾
7	☑	Shutdown P(▾	Enable ▾
8	☑	Shutdown P(▾	Enable ▾
9	☑	Shutdown P(▾	Enable ▾
10	☑	Shutdown P(▾	Enable ▾

Fig. 32 Port Configuration

CLI COMMANDS

Configuration	Show loop protection of the switch

Mode	Set or show the loop protection mode of the sw
Transmit	Set or show the loop protection transmit interv
Shutdown	Set or show loop protection shutdown time

2.106.6Aggregation

Aggregation or Link Aggregation is a technology that by setting multiple ports to server one physical or virtual link to increase the throughput and reliability. Aggregation or Link Aggregation short as LAG as well.

Schematic diagram shows as following Fig. 33

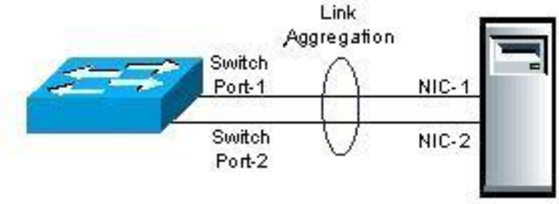


Fig. 33 Schematic Diagram

6.6.1 Aggregation Mode Configuration

Use the Aggregation Mode Configuration page to configure the aggregation mode and members of each static trunk group.

PATH

Web	LACP & Aggregation, Static
CLI	**Aggr>**

USAGE GUIDELINES

■When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Ether Channel compatible.

■To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

■When incoming data frames are forwarded through the switch to a trunk, the switch must determine to which port link in the trunk an outgoing frame should be sent. To maintain the frame sequence of various traffic flows between devices in the network, the switch also needs to ensure that frames in each "conversation" are mapped to the same trunk link. To achieve this requirement and to distribute a balanced load across all links in a trunk, the switch uses a hash algorithm to calculate an output link number in the trunk. However, depending on the device to which a trunk is connected and the traffic flows in the network, this load-balance algorithm may result in traffic being distributed mostly on one port in a trunk. To ensure that the switch traffic load is distributed evenly across all links in a trunk, the hash method used in the load-balance calculation can be selected to provide the best result for trunk connections. The switch provides four load-balancing modes as described in the following section.

■ Aggregation Mode Configuration also applies to LACP

PARAMETERS

These parameters are displayed:

Aggregation Mode Configuration

■**Hash Code Contributors** – Selects the load-balance method to apply to all trunks on the switch. If more than one option is selected, each factor is used in the hash algorithm to determine the port member within the trunk to which a frame will be assigned. The following options are supported:

◇**Source MAC Address** – All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts. (One of the defaults.)

◇**Destination MAC Address** – All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.

◇**IP Address** – All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch to- server trunk links where the destination IP address is the same for all traffic. (One of the defaults.)

◇**TCP/UDP Port Number** – All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk. Avoid using his mode as a lone option. It may overload a single port member of the trunk for application traffic of a specific type, such as web browsing. However, it can be used effectively in combination with the IP Address option. (One of the defaults.)

6.6.2 Aggregation Group Configuration

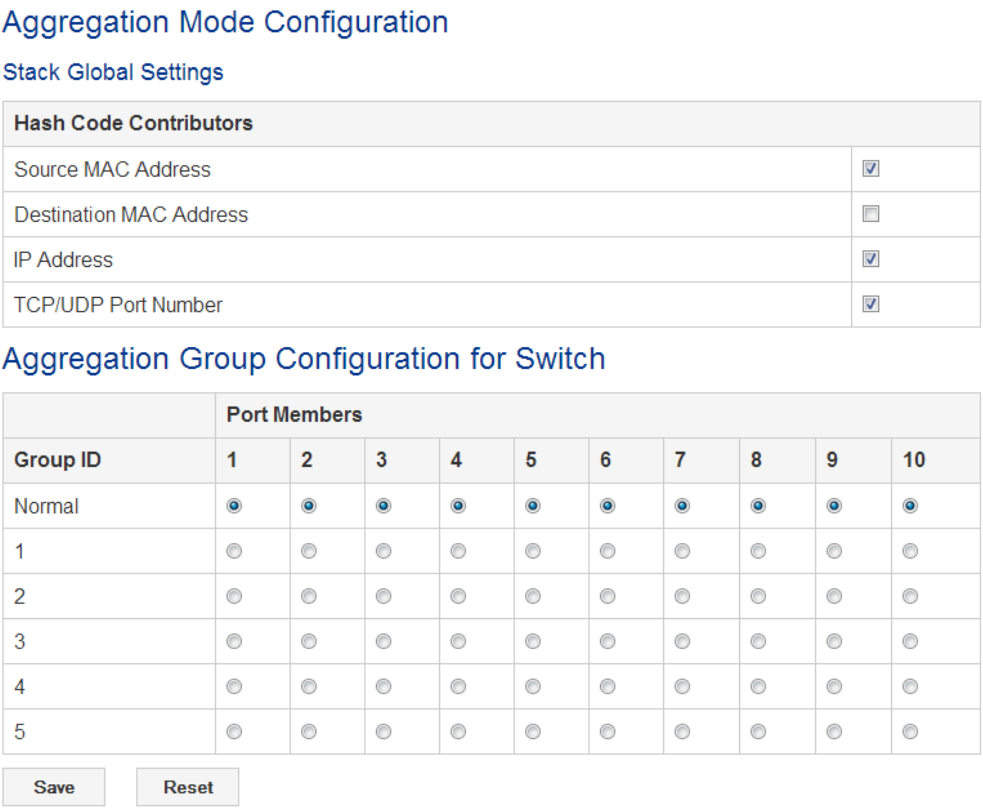
■**Group ID** – Trunk identifier. (Range: 1-5)
■**Port Members** – Port identifier.

WEB INTERFACE

To configure a static trunk:

1. Click LACP & Aggregation, Static.
2. Select one or more load-balancing methods to apply to the configured trunks.
3. Assign port members to each trunk that will be used.
4**.** Click Save.

Aggregation Mode Configuration seen as following Fig. 34



Aggregation Mode Configuration

Stack Global Settings

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration for Switch

	Port Members									
Group ID	1	2	3	4	5	6	7	8	9	10
Normal	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○

Fig. 34 Aggregation Mode Configuration

CLI COMMANDS

Configuration	Show link aggregation configuration
Add	Add group of port to an aggregation configuration
Delete	Delete link aggregation
Lookup	Show the aggregation id

Mode	Set or show the link aggregation traffic distribution mode

6.6.3 LACP Port Configuration

Use the LACP Port Configuration page to enable LACP on selected ports, configure the administrative key, and the protocol initiation mode.

PATH

Web	LACP & Aggregation, Static
CLI	**LACP>**

Configuration, Aggregation, LACP

USAGE GUIDELINES

■To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

■If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

■A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.

■If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

■All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

■ Trunks dynamically established through LACP will be shown on the

LACP System Status page by path Monitor, LACP, System Status.

■ Ports assigned to a common link aggregation group (LAG) must meet the following criteria:

◇ Ports must have the same LACP Admin Key. Using auto configuration of the Admin Key will avoid this problem.

◇ One of the ports at either the near end or far end must be set to active initiation mode.

■ Aggregation Mode Configuration located under the Static Aggregation menu (see "Configuring Static Trunks" on section 6.3.2) also applies to LACP.

PARAMETERS

These parameters are displayed:

■**Port** – Port identifier.

■**LACP Enabled** – Controls whether LACP is enabled on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can form up to 12 LAGs per switch.

■**Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: Auto) Select the Specific option to manually configure a key. Use the Auto selection to automatically set the key based on the actual link speed, where 10Mb = 1, 100Mb = 2, and 1Gb = 3.

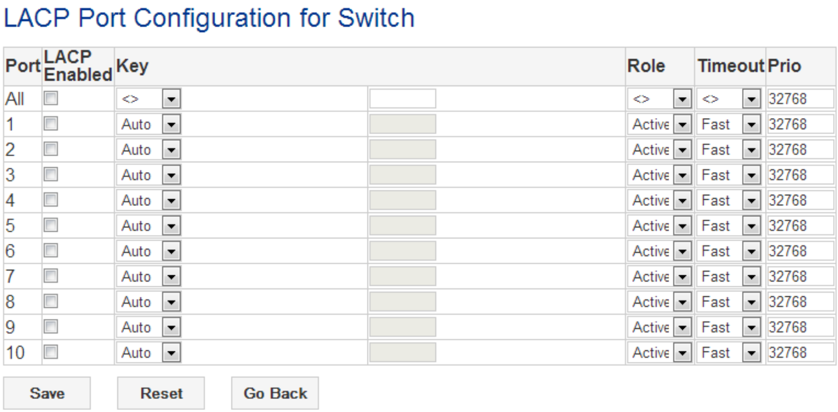
■**Role** – Configures active or passive LACP initiation mode. Use Active initiation of LACP negotiation on a port to automatically send LACP negotiation packets (once each second). Use Passive initiation mode on a port to make it wait until it receives an LACP protocol packet from a partner before starting negotiations.

WEB INTERFACE

To configure a dynamic trunk:

1. Click LACP & Aggregation, Port Status, then click the Edit button.
2. Enable LACP on all of the ports to be used in an LAG.
3. Specify the LACP Admin Key to restrict a port to a specific LAG.
4. Set at least one of the ports in each LAG to Active initiation mode, either at the near end or far end of the trunk.
5.Click Save.

LACP Port Configuration seen as following Fig. 35



LACP Port Configuration for Switch

Port	LACP Enabled	Key		Role	Timeout	Prio
All	□	<>		<>	<>	32768
1	□	Auto		Active	Fast	32768
2	□	Auto		Active	Fast	32768
3	□	Auto		Active	Fast	32768
4	□	Auto		Active	Fast	32768
5	□	Auto		Active	Fast	32768
6	□	Auto		Active	Fast	32768
7	□	Auto		Active	Fast	32768
8	□	Auto		Active	Fast	32768
9	□	Auto		Active	Fast	32768
10	□	Auto		Active	Fast	32768

Fig. 35 LACP Port Configuration

CLI COMMANDS

Configuration	Shows LACP configuration, following information will

	be show, Mode, Key, Role, Timeout, Priority, for more information of those parameter, please refer previous section.
Mode	Set or show the LACP mode of the switch
Key	Configure LACP key
Role	Configure LACP role
Timeout	Configure LACP timeout
Prior	Set or show specified ports LACP parameter respectively, as show in the LACP configuration command
System Prior	Set or show LACP system priority
Status	LACP Status for the specified port, default shows all
Statistics	LACP statistics information, including Rx Frames, Tx Frames, Rx unknown and Rx Illegal

6.7Redundancy

The Ethernet network redundancy assures the networking could continue work when single cable fails in switch-to-switch links by providing backup links. Spanning Tree Algorithm (STA) is introduced to support this functionality, such as detect and disable network loops, provide backup links between switches and select alternative path while the error occur.

PATH

Web	Spanning Tree, Bridge Status
CLI	STP>

6.7.1 Spanning Tree Algorithm (STA) Configuration

Basic Settings

■ Protocol Version– Specifies the type of spanning tree used on this switch. (Options: STP, RSTP; Default: RSTP)

◇ STP: Spanning Tree Protocol (IEEE 802.1D); i.e., the switch will use RSTP set to STP forced compatibility mode.

◇ RSTP: Rapid Spanning Tree (IEEE 802.1w)

■ Bridge Priority– Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

◇ Default: 128

◇ Range: 0-240, in steps of 16

◇ Options: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240

■ Forward Delay – The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

■ Max Age –Maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and*MaxAge must be <= (FwdDelay-1)*2.

■ Transmit Hold Count – The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. (Range: 1-10; Default: 6)

■ Max Hop Count– The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 6-40; Default: 20) An MST region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MST region is never changed. However, each spanning tree instance within a region and the common internal spanning tree (CIST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop counts by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Advanced Settings

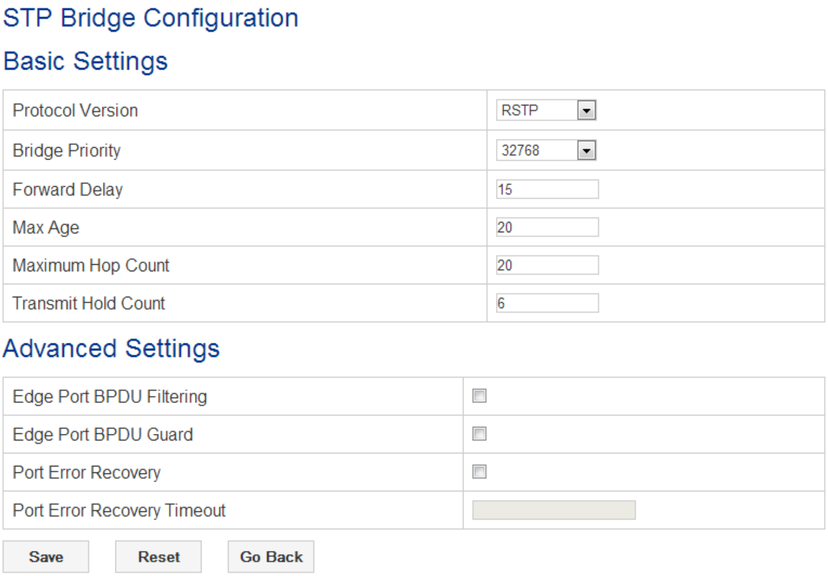
- Edge Port BPDU Filtering – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BDPU filtering is configured on a per-port basis. (Default: Disabled)
- Edge Port BPDU Guard – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU, an invalid configuration exists, such as a connection to an unauthorized device.
- The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
- Port Error Recovery – Controls whether a port in the error-disabled state will be automatically enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STA operation. The condition is also cleared by a system reboot.
- Port Error Recovery Timeout – The time that has to pass before a port in the error-disabled state can be enabled. (Range: 30-86400 seconds or 24 hours)

WEBINTERFACE

To configure global settings for STP:

1. Click Spanning Tree, Bridge Status, then the Edit button.
2. Modify the required attributes.
3. Click Save.

STP bridge configuration seen as following Fig. 36



STP Bridge Configuration

Basic Settings

Protocol Version	RSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Fig. 36 STP Bridge Configuration

CLI COMMANDS

Configuration	STP bridge level configuration information, such as RSTP, max age, and so on. For the detail, please refer Fig.30.
Recovery	Set the every parameter which show by the command STP configuration command, please refer the STP configuration for more detail

Status	STP Bridge status
Bridge Priority	Set or show the bridge instance priority, the priority value could start from 0, step 4096, till 61440

6.7.2 STP/RSTP/CIST Interface Configuration

Use the CIST Ports Configuration page to configure STA attributes for interfaces when the spanning tree mode is set to STP or RSTP, or for interfaces in the CIST. STA interface attributes include path cost, port priority, edge port (for fast forwarding), automatic detection of an edge port, and point-to-point link type.

You may use a different priority or path cost for ports of the same media type to indicate the preferred path, edge port to indicate if the attached device can support fast forwarding, or link type to indicate a point-to-point connection or shared-media connection. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

PATH

Web	Spanning Tree, Status
CLI	**STP>Port>STP/Port>**

CIST Aggregated Port Configuration &CIST Normal Port Configuration

PARAMETERS

These parameters are displayed:

■Port– Port Identifier.

This field is not applicable to static trunks or dynamic trunks created through LACP. Also, note that only one set of interface configuration settings can be applied to all trunks.

■ STP Enabled– Sets the interface to enable STA, disable STA, or disable STA with BPDUtransparency. (Default: Enabled) BPDU transparency is commonly used to support BPDU tunneling, passing BPDUs across a service provider's network without any changes, thereby combining remote network segments into a single spanning tree. As implemented on this switch, BPDU transparency allows a port which is not participating in the spanning tree (such as an uplink port to the service provider's network) to forward BPDU packets to other ports instead of discarding these packets or attempting to process them.

■ Path Cost– This parameter is used by the STA 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. (Path cost takes precedence over port priority.) By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Recommended STA Path Cost Range

■Priority– Defines the priority used for this port in the Spanning Tree Algorithm. If the path costs for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

(Range: 0-240, in steps of 16; Default: 128)

■ Admin Edge(Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying edge ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that this feature should only be enabled for ports connected to an end-node device. (Default: Edge)

■ Auto Edge– Controls whether automatic edge detection is enabled on a bridge port. When enabled, the bridge can determine that a port is at the edge of the network if no BPDU's are received on the port.
(Default: Enabled)

■ Restricted Role– If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, this can cause a lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know as Root Guard.

■ Restricted TCN– If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports. TCN messages can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent incorrectly learned station location information. TCN messages can be restricted by a network administrator to prevent bridges external to a core region of the network from causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state for the attached LANs transitions frequently.

■ BPDU Guard– This feature protects ports from receiving BPDUs. It can prevent loops by shutting down an port when a BPDU is received instead of putting it into the spanning tree discarding state. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)

If enabled, the port will disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well (see "Configuring Global Settings for STA" on pervious section).

■ Point-to-Point– The link type attached to an interface can be set to automatically detect the link type, or manually configured as point-to-point or shared medium. Transition to the forwarding state is faster for point-to-point links than for shared media. These options are described below:

◇ Auto– The switch automatically determines if the interface is attached to a point-to-point link or to shared medium. (This is the default setting.)

When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

◇ Forced True– A point-to-point connection to exactly one other bridge.

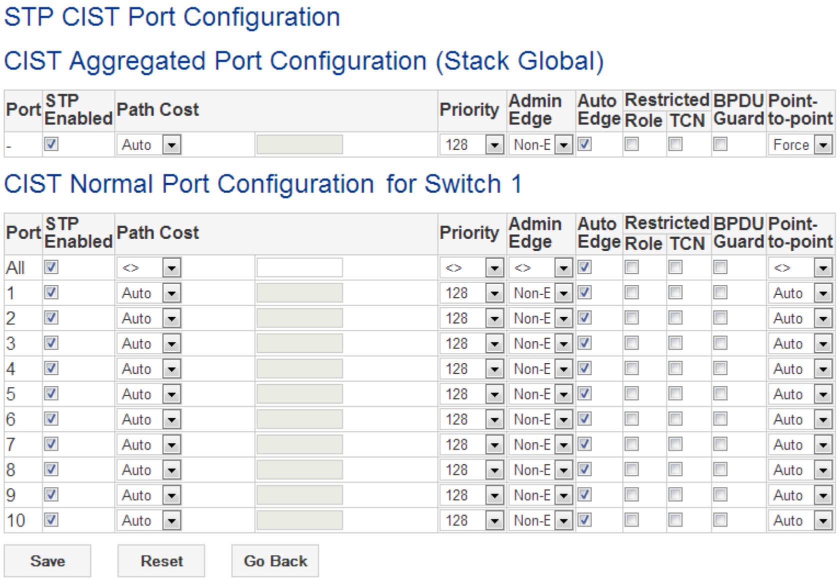
◇ Forced False– A shared connection to two or more bridges.

WEBINTERFACE

To configure global settings for STA:

1. Click Spanning Tree, Port Status.
2. Modify the required attributes.
3. Click Save.

STP CIST port configuration is seen as following Fig. 37.



STP CIST Port Configuration

CIST Aggregated Port Configuration (Stack Global)

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☑	Auto	128	Non-E	☑	□	□	□	Force

CIST Normal Port Configuration for Switch 1

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
All	☑	<>	<>	<>	☑	□	□	□	<>
1	☑	Auto	128	Non-E	☑	□	□	□	Auto
2	☑	Auto	128	Non-E	☑	□	□	□	Auto
3	☑	Auto	128	Non-E	☑	□	□	□	Auto
4	☑	Auto	128	Non-E	☑	□	□	□	Auto
5	☑	Auto	128	Non-E	☑	□	□	□	Auto
6	☑	Auto	128	Non-E	☑	□	□	□	Auto
7	☑	Auto	128	Non-E	☑	□	□	□	Auto
8	☑	Auto	128	Non-E	☑	□	□	□	Auto
9	☑	Auto	128	Non-E	☑	□	□	□	Auto
10	☑	Auto	128	Non-E	☑	□	□	□	Auto

Fig. 37 STP COST Port Configuration

CLI COMMANDS

onfiguration	Port level STP configuration parameter, including

	mode, Admin edge, auto edge and so on, please refer Fig.31 for more detail information
Statistics	Configure the STP parameter of the ports be specified
Migration check	Set the STP Migration Check variable for ports
Cost	Set or show the port instance path cost for the port be specified, the path cost could range 1-200000000, or auto
Priority	Set or show the instance priority for the port be specified, the priority could range from 0 to 240 with step 16

6.8 SNMP System Configuration

■ Mode- Enables or disables SNMP service. (Default: Disabled)

■ Version- Specifies the SNMP version to use. (Options: SNMP v1, SNMP v2c, SNMP v3; Default: SNMP v2c)

■ Read **Community** - The community used for read-only access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only; Default: public) This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 Communities table (page 69).

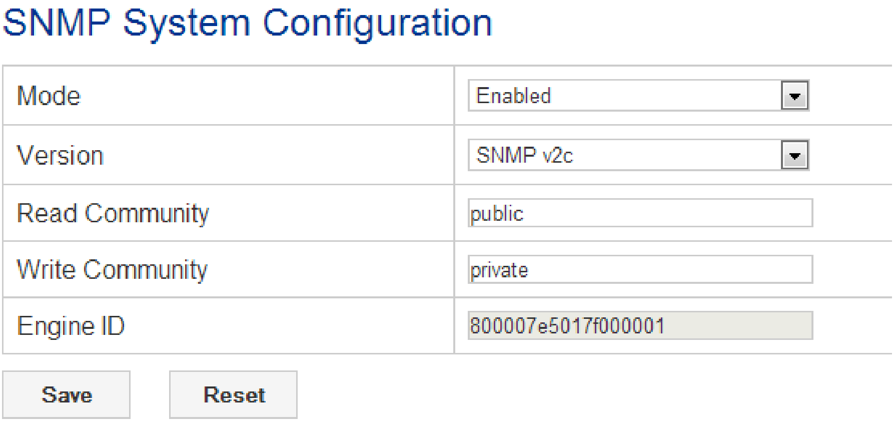
■**Write Community** - The community used for read/write access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only; Default: private) This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 Communities table (page 69).

■**Engine ID** - The SNMPv3 engine ID. (Range: 10-64 hex digits, excluding a string of all 0's or all F's; Default: 800007e5017f000001) A SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets. A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all local SNMP users will be cleared. You will need to reconfigure all existing users.

To configure SNMP system:

1. Click Security, SNMP, and System.
2. In the SNMP System Configuration table, set the Mode to Enabled to enable SNMP service on the switch, specify the SNMP version to use, change the community access strings if required, and set the engine ID if SNMP version 3 is used.
3. Click Save.

SNMP System Configuration seen as following Fig. 38



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Fig. 38 SNMP System Configuration

6.9 Port Status

Use the Port Statistics Overview page to display a summary of basic information on the traffic crossing each port.

PATH

Web	Ports, Traffic Overview
CLI	**Port>**

PARAMETERS

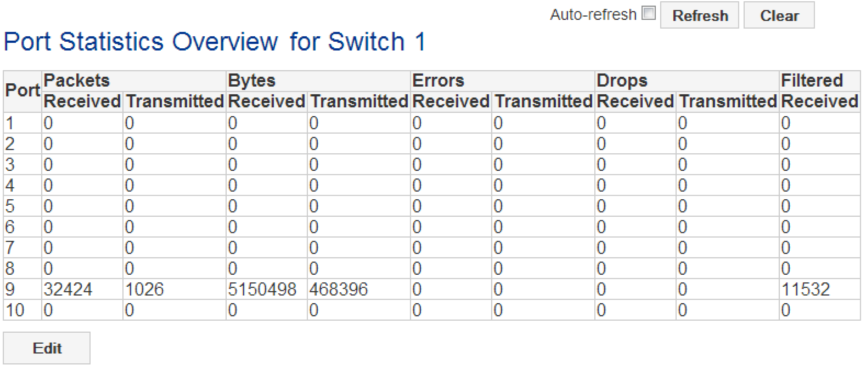
These parameters are displayed:

■**Packets Received/Transmitted** – The number of packets received and transmitted.
■**Bytes Received/Transmitted** – The number of bytes received and transmitted.
■**Errors Received/Transmitted** – The number of frames received with errors and the number of incomplete transmissions.
■**Drops Received/Transmitted** – The number of frames discarded due to ingress or egress congestion
■**Filtered Received** – The number of received frames filtered by the forwarding process.

WEB INTERFACE

To display a summary of port statistics, click Monitor, Ports, and Traffic Overview

Figure Port Statistics Overview seen as following Fig. 39.



Auto-refresh □ Refresh Clear

Port Statistics Overview for Switch 1

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	32424	1026	5150498	468396	0	0	0	0	11532
10	0	0	0	0	0	0	0	0	0

Edit

Fig. 39 Port Statistics Overview

CLI COMMANDS

Please refer 6.2.1

6.10MAC Table List

Use the MAC Address Table Configuration page to configure dynamic address learning or to assign static addresses to specific ports. Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

PATH

Web	MAC Table
CLI	**MAC>**

PARAMETERS

These parameters are displayed:

Aging Configuration

■**Disable Automatic Aging** - Disables the automatic aging of dynamic entries. (Address aging is enabled by default.)
■**Aging Time** - The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

MAC Table Learning

■**Auto** - Learning is done automatically as soon as a frame with an unknown source MAC address is received. (This is the default.)
■**Disable** - No addresses are learned and stored in the MAC address table.
■**Secure** - Only static MAC address entries are used, all other frames are dropped. Make sure that the link used for managing the switch is added to the Static MAC Table before changing to secure learning mode. Otherwise the management link will be lost, and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

NOTE: If the learning mode for a given port in the MAC Learning Table is grayed out, another software module is in control of the mode and cannot be changed by the user. An example of such a module is the MAC Based Authentication under 802.1X.

Static MAC Table Configuration

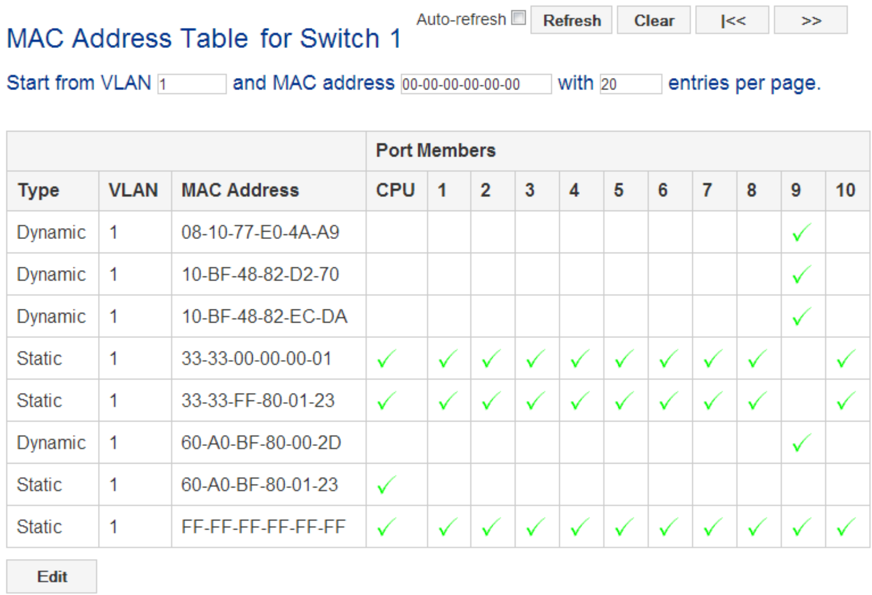
■**VLAN ID** - VLAN Identifier. (Range: 1-4095)
■**MAC Address** - Physical address of a device mapped to a port. A static address can be assigned to a specific port on this switch. Static addresses are bound to the assigned port and will not be moved. When a static address is seen on another port, the address will be ignored and will not be written to the address table.
■**Port Members** - Port identifier.

WEB INTERFACE

To configure the MAC Address Table:

1. Click MAC Table.
2. Change the address aging time if required.
3. Specify the way in which MAC addresses are learned on any port.
4. Add any required static MAC addresses by clicking the Add New Static Entry button, entering the VLAN ID and MAC address, and marking the ports to which the address is to be mapped.
5. Click Save.

MAC Address Table Configuration seen as following Fig. 40



MAC Address Table for Switch 1

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members										
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10
Dynamic	1	08-10-77-E0-4A-A9										✓	
Dynamic	1	10-BF-48-82-D2-70										✓	
Dynamic	1	10-BF-48-82-EC-DA										✓	
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Static	1	33-33-FF-80-01-23	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Dynamic	1	60-A0-BF-80-00-2D										✓	
Static	1	60-A0-BF-80-01-23	✓										
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Fig. 40 MAC Address Table

CLI COMMANDS

Configuration	MAC configuration of specified port list, learning method could be AUTO, DISABLE or SECURE as configured by Learning command
Add	Add MAC address
Delete	Delete MAC address
Lookup	Maintain or show the Mac address for the specified ports manually
Age time	Specified the how long the MAC address entry will expire
Learning	Set or show the port learn mode, could be assigned as auto, disable or secure for the specified port.

Dump	Show sorted list of MAC address entries for the specified ports, for every entry
Statistics	Show MAC address table statistics information, such as how many dynamic addresses or static addresses have been learned on the specified port or switch
Flush	Flush the current MAC address on the port

MAC Dump looks like

```
Type         VID     MAC Address                  Ports
------      ---      -----------------            -----
Dynamic    1          00-18-82-d5-18-97     10
```

Type means the current entry is dynamic or static, static usual configure by manual;

The VID means current entry belong which VLAN;

MAC address and ports mean on switch port list in the entry, which MAC address has been detected automatically or configured manually

6.11 IEEE 802.1Q VLANS

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections.

VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing). VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

◆ Up to 256 VLANs based on the IEEE 802.1Q standard
◆ Distributed VLAN learning across multiple switches using explicit or implicit tagging
◆ Port overlapping, allowing a port to participate in multiple VLANs

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP.

However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

6.12 PROTOCOL VLANS

6.12.1 ASSIGNING PORTS TO VLANS

Use the VLAN Membership Configuration page to enable VLANs for this switch by assigning each port to the VLAN group(s) in which it will participate.

PATH

Web	VLANs, VLAN Membership
CLI	**VLAN>**

PARAMETERS

These parameters are displayed:

◆**VLAN ID** - VLAN Identifier. (Range: 1-4095)
◆**VLAN Name** - The name of a VLAN. (Range: 1-32 alphanumeric characters)
◆**Port Members** - Port identifier. Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you must connect them

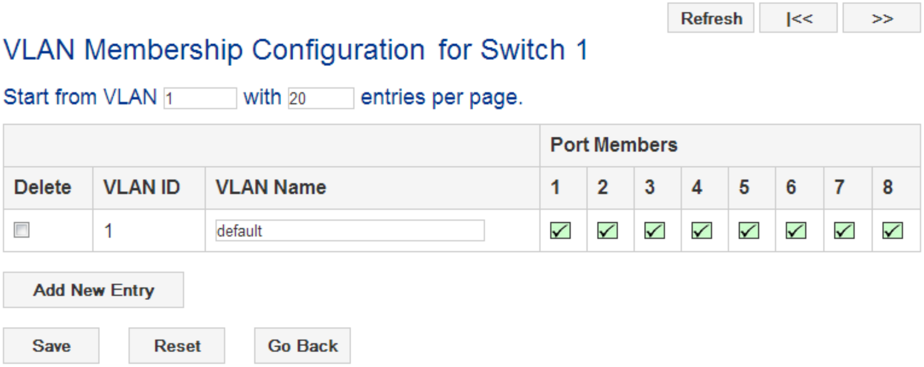
through a router.

WEB INTERFACE

To configure IEEE 802.1Q VLAN groups:

1. Click Configuration, VLANs, and VLAN Membership.
2. Change the ports assigned to the default VLAN (VLAN 1) if required.
3. To configure a new VLAN, click Add New VLAN, enter the VLAN ID, and then mark the ports to be assigned to the new group.
4. Click Save.

VLAN Membership Configuration seen as following Fig. 41



VLAN Membership Configuration for Switch 1

Start from VLAN 1 with 20 entries per page.

			Port Members							
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑

Fig. 41 VLAN Membership Configuration

6.12.2 CONFIGURING VLAN ATTRIBUTES FOR PORT MEMBERS

Use the VLAN Port Configuration page to configure VLAN attributes for specific interfaces, including processing Queue-in-Queue frames with embedded tags, enabling ingress filtering, setting the accepted frame types, and configuring the default VLAN identifier (PVID).

PATH

Web	VLANs, VLAN Port
CLI	**VLAN>**

PARAMETERS

These parameters are displayed:

◆Ethertype for Custom S-ports - When Port Type is set to S-custom port, the EtherType (also called the Tag Protocol Identifier or TPID) of all frames received on the port is changed to the specified value. By default, the EtherType is set to 0x88a8 (IEEE 802.1ad). IEEE 802.1ad outlines the operation of Queue-in-Queue tagging which allows a service provider to use a Virtual Bridged Local Area Network to provide separate VLAN instances to multiple independent customers over the same medium using double tagged frames. When Port Type is set to S-port or S-custom-port, the port will change the EtherType of all frames received to indicate that double-tagged frames are being forwarded across the switch. The switch will pass these frames on to the VLAN indicated in the outer tag. It will not strip the outer tag, nor change any components of the tag other than the EtherType field.

◆ Port - Port identifier.

◆ Port Type – Configures how a port processes the VLAN ID in ingress frames. (Default: Unaware)

■ C-port – For customer ports, each frame is assigned to the VLAN indicated in the VLAN tag, and the tag is removed.

■ S-port – For service ports, the EtherType of all received frames is changed to 0x88a8 to indicate that double-tagged frames are being forwarded across the switch. The switch will pass these frames on to the VLAN indicated in the outer tag. It will not strip the outer tag, nor change any components of the tag other than the EtherType field.

■ S-custom-port – For custom service ports, the EtherType of all received frames is changed to value set in the Ethertype for Custom S-ports field to indicate that double-tagged frames are being forwarded across the switch. The switch will pass these frames on to the VLAN indicated in the outer tag. It will not strip the outer tag, nor change any components of the tag other than the EtherType field.

■ Unaware – All frames are classified to the Port VLAN ID and tags are not removed.

◆ Ingress Filtering - Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

■ Ingress filtering only affects tagged frames.

■If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

■If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports.

■ Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

◆ Frame Type - Sets the interface to accept all frame types, including tagged or untagged frames, only tagged frames, or only untagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. When set to receive only tagged frames, all untagged frames received on the interface are discarded. (Option: All, Tagged, Untagged; Default: All)

◆ Port VLAN Mode - Determines how to process VLAN tags for ingress and egress traffic. (Options: None, Specific; Default: Specific)

■None - The ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port. The assigned VLAN ID can be based on the ingress tag for tagged frames, or the default PVID for untagged ingress frames. Note that this mode is normally used for ports connected to VLAN-aware switches.

■ Specific - A Port VLAN ID can be configured (as described below). Untagged frames received on the port are classified to the Port VLAN ID. If Port Type is Unaware, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along with a path that does not contain any VLAN-aware devices (including the destination host), the switch should first strips off the VLAN tag before forwarding the frame.

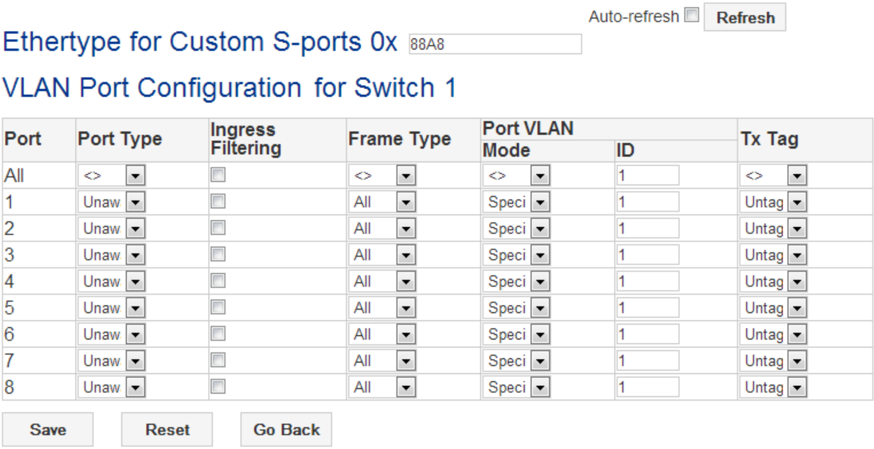
◆ Port VLAN ID - VLAN ID assigned to untagged frames received on the interface. (Range: 1-4095; Default: 1) the port must be a member of the same VLAN as the Port VLAN ID.

WEB INTERFACE

To configure attributes for VLAN port members:

1. Click Configuration, VLANs, and VLAN Port.
2. Configure in the required settings for each interface.
3. Click Save.

VLAN Port Configuration seen as following Fig. 42



Auto-refresh □ Refresh

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration for Switch 1

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
All	<>	□	<>	<>	1	<>
1	Unaw	□	All	Speci	1	Untag
2	Unaw	□	All	Speci	1	Untag
3	Unaw	□	All	Speci	1	Untag
4	Unaw	□	All	Speci	1	Untag
5	Unaw	□	All	Speci	1	Untag
6	Unaw	□	All	Speci	1	Untag
7	Unaw	□	All	Speci	1	Untag
8	Unaw	□	All	Speci	1	Untag

Fig. 42 VLAN Port Configuration

6.13System Log Information

Use the System Log Information page to scroll through the logged system and event messages.

PATH

Web	System, Log
CLI	**System>Log>System/log>**

PARAMETERS

These parameters are displayed:

Display Filter

■**Level** – Specifies the type of log messages to display.

◇ Info – Informational messages only.

◇ Warning – Warning conditions.

◇ Error – Error conditions.

◇ All – All levels.

■ Start from ID – The error ID from which to start the display.

■with # entries per page – The number of entries to display per page. *Table Headings*

■**ID** – Error ID.

■**Level** – Error level as described above.

■**Time** – The time of the system log entry.

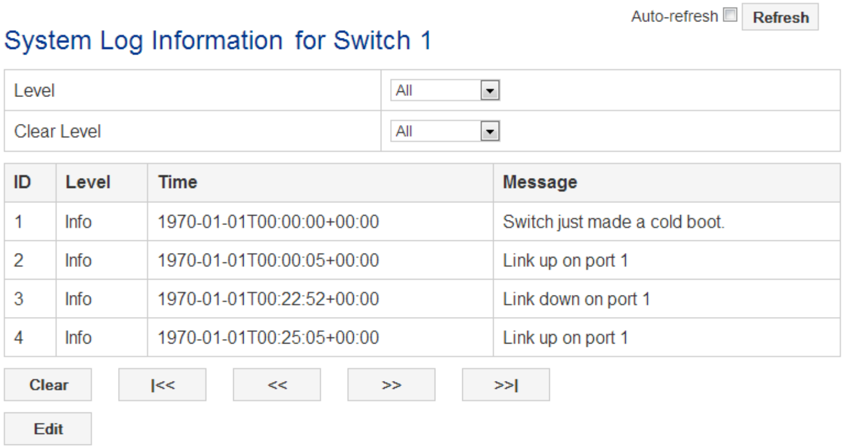
■**Message** – The message text of the system log entry.

WEB INTERFACE

To display the system log:

1. Click System, Log.
2. Specify the message level to display, the starting message ID, and the number of messages to display per page.
3. Use Auto-refresh to automatically refresh the page at regular intervals, Refresh to update system log entries starting from the current entry ID, or clear to flush all system log entries. Use the arrow buttons to scroll through the log messages. |<< updates the system log entries, starting from the first available entry ID, << updates the system log entries, ending at the last entry currently displayed, >> updates the system log entries, starting from the last entry currently displayed, and >>| updates the system log entries, ending at the last available entry ID.

System Log Information seen as following Fig. 43



System Log Information for Switch 1

Level	All
Clear Level	All

ID	Level	Time	Message
1	Info	1970-01-01T00:00:00+00:00	Switch just made a cold boot.
2	Info	1970-01-01T00:00:05+00:00	Link up on port 1
3	Info	1970-01-01T00:22:52+00:00	Link down on port 1
4	Info	1970-01-01T00:25:05+00:00	Link up on port 1

Fig. 43 System Log Information

CLI COMMANDS

Configuration	Show the system log configu
Server Mode	Set or show the system lo disable
Server Address	Configure system log server
Level	Configure system log level
Lookup [log_id] [all | info|warning|error]	Show system log, e.g. looku first ten logs with level error.
Clear	Clear system log entry

6.14Profile Configuration

6.14.1 Configuration Save

Use the Configuration Save page to save the current configuration settings to a file on your local management station.

PATH

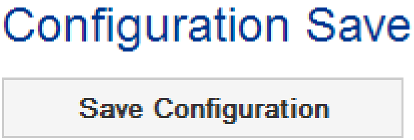
Web	Configuration, Save
CLI	**Config>**

WEB INTERFACE

To save your current configuration settings:

1. Click Configuration, Save.
2. Click the “Save configuration” button.
3.Specify the directory and name of the file under which to save the current configuration settings. The configuration file is in XML format. The configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may be modified using an editor and loaded to a switch

Configuration Save seen as following Fig. 44


Configuration Save

Save Configuration

Fig. 44 Configuration Save Interface

6.14.2 Configuration Upload

Use the Configuration Upload page to restore previously saved configuration settings to the switch from a file on your local management station.

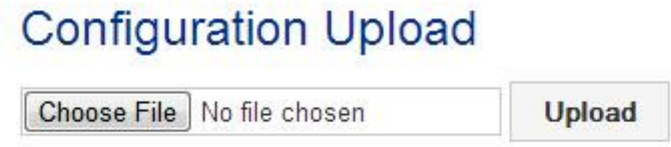
PATH

Web	Configuration, Upload
CLI	**Config>**

WEB INTERFACE

To restore your current configuration settings:
1. Click Configuration, Upload.
2. Click the Browse button, and select the configuration file.
3. Click the Upload button to restore the switch’s settings.

Configuration Upload seen as following Fig. 45



Configuration Upload

Fig. 45 Configuration Upload Interface

CLI COMMANDS

Save	Saved configuration settings from your local management station
Load	Upload the configuration you saved before

6.15Firmware Update

Use the Software Upload page to upgrade the switch's system firmware by specifying a file provided by SMC/Edge-Core. You can download firmware files for your switch from the Support section of the SMC/Edge-Core web site.

PATH

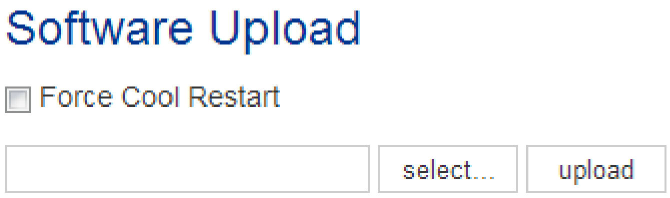
Web	Software, Upload
CLI	**Firmware>**

WEB INTERFACE

To upgrade firmware:

1. Click Maintenance, Software Upload.
2. Click the Browse button, and select the firmware file.
3. Click the Upload button to upgrade the switch’s firmware. After the software image is uploaded, a page announces that the firmware update has been initiated. After about a minute, the firmware is updated and the switch is rebooted.

CAUTION: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off at a frequency of 10 Hz while the firmware update is in progress. Do not reset or power off the device at this time or the switch may fail to function afterwards.
Software Upload seen as following Fig. 46


Software Upload

□ Force Cool Restart

Fig. 46 Software Upload Interface

CLI COMMANDS

Load	load a new firmware from TFTP server for the firmware upgrading
Net Load	net load upgrading the firmware via

	http
Upgrading	Upgrading the firmware via http
Information	show the current firmware information of this switch

6.16Factory Defaults

Use the Factory Defaults page to restore the original factory settings. Note that the LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

PATH

Web	Factory Defaults
CLI	**System>Restore Default>**

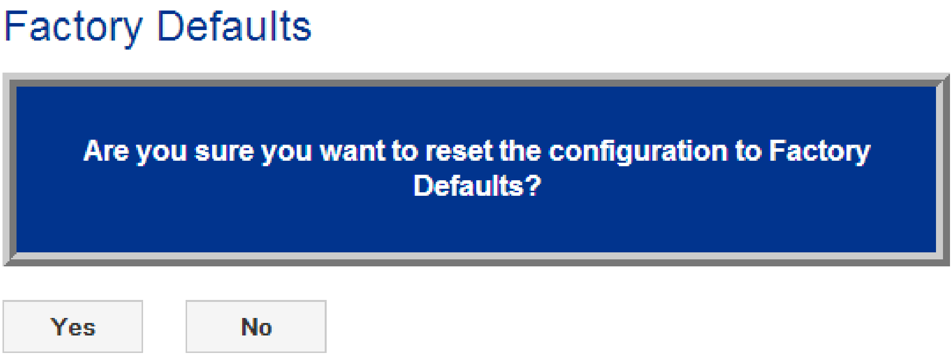
WEB INTERFACE

To restore factory defaults:

1. Click Maintenance, Factory Defaults.

2.Click Yes. The factory defaults are immediately restored, which means that no reboot is necessary.

Factory Defaults seen as following Fig. 47



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Fig. 47 Factory Defaults Interface

CLI COMMANDS

Restore factory default configuration and keep IP address if the keep_ip parameter specified

System>restore default
Restore factory default configuration.
Restore Default [keep_ip]

6.17Restart Device

Use the Restart Device page to restart the switch.

PATH

Web	Restart Device
CLI	**System>Reboot>**

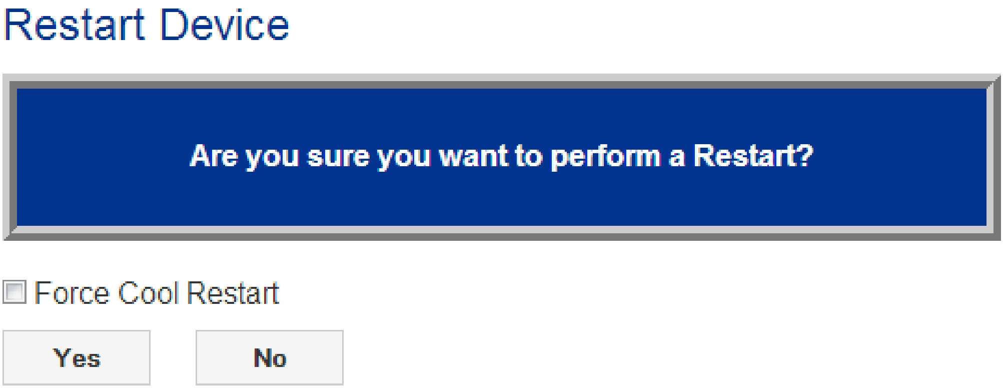
WEB INTERFACE

To restart the switch

1. Click Restart Device.

2.Click Yes. The reset will be complete when the user interface displays the login page.

Restart Device seen as following Fig. 48



Restart Device

Are you sure you want to perform a Restart?

□ Force Cool Restart

Fig. 48 Restart Device Interface

CLI COMMANDS

Reboot the default configuration of the switch.

SHANGHAI SUN TELECOMMUNICATION CO., LTD.
Building No.145 Lane 666, Xianing Rd.
Jinshan Industrial Zone, Jinshan District
ShangHai, China 201506
Tel: +86 21 60138638 Fax: +86 21 60138635-401
E-mail: ics@suntelecom.cn
http://www.suntelecom.cn