



User Manual

ES-5816PHG



Gigabit 16-Port 802.3at PoE Web Smart Switch

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Content.....	I
Introduction.....	1
Product Overview.....	1
General Feature.....	1
L2 switching.....	1
Quality of Service.....	2
Security.....	2
Specification.....	3
Mechanical.....	3
Package Contents.....	4
Hardware Description.....	5
Physical Dimensions / Weight.....	5
Front Panel.....	5
LEDs Indicators.....	5
Rear Panel.....	6
Hardware Installation.....	6
Software Description.....	7
Login.....	7
Configuration.....	8
System	8
Ports	10
Vlan.....	11
Aggregation.....	12
LACP.....	13
RSTP.....	14
802.1x	16
Snopping.....	17
Mirrioring.....	18
QoS.....	19
Filter.....	22
Power over Ethernet	23
Rate Limit.....	24
Storm Control.....	24
Monitoring.....	26
Statistic Overview.....	26

Detailed Statistic.....	26
LACP Status.....	27
RSTP Status.....	28
IGMP Status.....	30
VeriPHY.....	30
Ping.....	31
Maintenance.....	34
Warm Restart.....	34
Factory Default.....	34
Software Upload.....	34
Configuration File Transfer.....	34
Logout.....	35

Introduction

Product Overview

This switch is a Web Management Switch equipped with 16-ports 10/100/1000BaseT(X) with 4-port gigabit SFP open slots. It was 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 desktop size was specifically designed for small to medium workgroups. It can be installed where space is limited; moreover, it provides smooth network migration and easy upgrade to network capacity.

In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

General Features

- 16 Gigabit Ethernet ports with non-blocking wire-speed performance
- 16 tri-speed 10/100/1000 Mbps Gigabit Ethernet Media Access Controllers (MACs)
- Eight tri-speed (10/100/1000 Mbps) integrated copper transceivers (PHY's)
- Sixteen integrated SGMII ports
- Buffer Memory 500K Bytes
- 8,192 IP multicast groups supported
- Jumbo frame support at all speed (10/100/1000 Mbps) of up to 9.6K bytes
- Wire-speed automatic learning and CPU-based learning configurable per port
- Support up to 24 trunks with up to 16 ports in a trunk

Layer-2 Switching

- 16 Giga Ethernet ports with non-blocking wire-speed performance
- 8,192 MAC addresses with wire-speed automatic learning and CPU-based learning configurable per port
- Rapid Spanning Tree Protocol support (IEEE std 802.1w)

- Multiple Spanning Tree support (IEEE std 802.1s)
- IGMP, GARP, GMRP, and GVRP support

Quality of Service

- Programmable multi-layer classifier with four QoS classes per port
- Strict priority or weighted round-robin forwarding with guaranteed bandwidth allocation
- Traffic class assignment based on port
- DSCP (IPv4 & IPv6) and 802.1p support
- DSCP remarking for both IPv4 & IPv6 packets
- Provide Bridge support with multiple VLAN tags (Q-in Q)
- Broadcast and multicast storm control
- Full-duplex flow control (IEEE 802.3x) and half-duplex back pressure
- Traffic shaping and policing per port in sites
- Link aggregation support based on layer 2-4 information (IEEE Std 802.3ad)

Security

- Port-based access control support
- 4,096 VLAN support
- VLAN awareness on a per port basis
- Independent and share VLAN learning
- VLAN Q-in Q support (VLAN stacking)
- Source IP filter per port to block unwanted access
- Extensive snooping : BPDU, GARP, ARP, IPMC, IGMP, TCP/UDP
- TCP/UDP filter for CPU copy/redirect, frame snooping and frame eradication
- DHCP filter to block unwanted DHCP servers on a per-port basis
- Multiple ARP filters for detection of ARP intrusion scans
- Extensive storm control: broadcast, multicast, uni-cast, ICMP and CPU (ARP, BPDU) traffic control
- Per port CPU based learning option
- CPU mirroring per port and per VLAN

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 802.3 Auto Negotiation
IEEE 802.3 Auto-MDI/MDI-X
IEEE 802.1ad Provider Bridge (Q in Q)
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
IEEE 802.3af- 2003 Power over Ethernet
IEEE 802.3at- 2009 Power over Ethernet

➤ Number of Port

16-port 10/100/1000BaseT(X) + 4 Gigabit SFP Open Slots

➤ LEDs Indicator

Per Port: Link/ Act, 1000M

Per Unit: Power

➤ Power Consumption: 130 Watts (Max)

➤ Power Input: 100~240V/AC, 50~60HZ

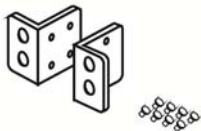
➤ Product Dimensions/ Weight

45 x 330 x 440 mm (H x W xD) / 4.4kg

Package Contents

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

- One Switch
- One Power Cord
- One User Manual
- One pair Rack-mount kit + 8 Screws



Hardware Description

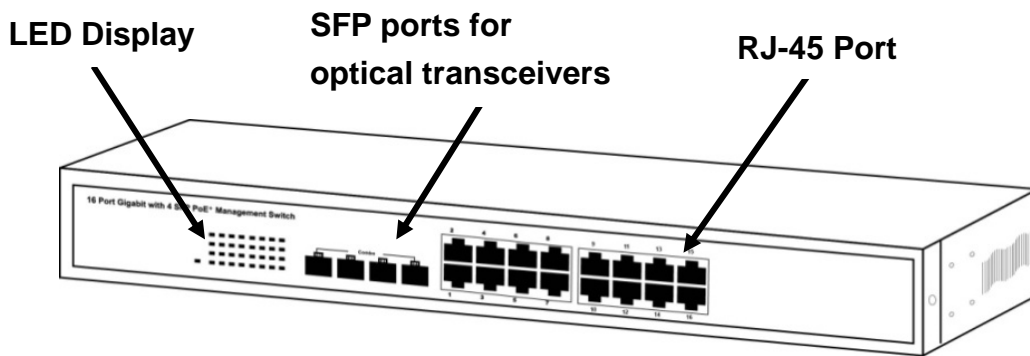
This part primarily presents hardware of the web-smart switch, physical dimensions and functional overview would be described.

Physical Dimensions/ Weight

45 × 440 × 330 mm (H × W × D) / 4.4KG

Front Panel

The front Panel of the web-smart Switch consists of 16 gigabit RJ-45 ports + 4 gigabit SFP open slot. The LED Indicators are also located on the front panel.

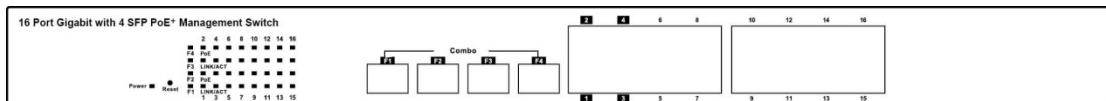


LED Indicators

The LED Indicators present real-time information of systematic operation status. This table provides description of LED status and the meaning.

Table 1-1 LED Indicators

LED	Status	Description
Power	On	Power on
	Off	Disconnect from Power Source
	Blink	Reset button for 3 seconds
Link/ ACT	On	Link
	Flashing	Data activating
	Off	No device is attached
PoE	On	Port is linked to Power Device
	Off	No Power Device is connected



Note: The SFP ports are shared with normal RJ-45 ports 1,2,3 and 4. The RJ-45 can not be used when SFP port link up.

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 clearance around the switch to allow attachment of cables, power cord and allow air circulation. The last, use twisted pair cable to connect this switch to your PC then user could start to operate the switch.

Software Description

This part instructs user how to set up and manage the switch through the web user interface. Please follow the description to understand the procedure.

At the first, open the web browser, and go to 192.168.2.1 site then the user will see the login screen. Key in the password to pass the authentication then clicks the **Apply**. The login process is completed and comes out the sign “Password successfully entered”.

Login

Password: **1234**

Please enter password to login

Password:	<input type="password"/>
-----------	--------------------------

Apply

Password Successfully Entered

Figure 1-1

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

Configuration

- System
- Ports
- VLANs
- Aggregation
- LACP
- RSTP
- 802.1X
- IGMP Snooping
- Mirroring
- Quality of Service
- Filter
- Power over Ethernet
- Rate Limit
- Storm Control

Monitoring

- Statistics Overview
- Detailed Statistics
- LACP Status
- RSTP Status
- IGMP Status
- VeriPHY
- Ping

Maintenance

- Warm Restart
- Factory Default
- Software Upload
- Configuration File
- Transfer
- Logout

Figure 1-2

Configuration

System

System Configuration

This page shows system configuration information. User can configure information as below:

System Configuration

MAC Address	00-03-ce-08-10-d6
S/W Version	G24 V110407
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	<input type="checkbox"/>
Fallback IP Address	<input type="text" value="192.168.2.1"/>
Fallback Subnet Mask	<input type="text" value="255.255.255.0"/>
Fallback Gateway	<input type="text" value="192.168.2.254"/>
Management VLAN	<input type="text" value="1"/>
Name	<input type="text"/>
Password	<input type="text"/>
Inactivity Timeout (secs)	<input type="text" value="0"/>
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	<input type="text" value="0.0.0.0"/>
SNMP Read Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
SNMP Trap Community	<input type="text" value="public"/>

Figure 2-1

- MAC Address: Displays the unique hardware address assigned by manufacturer (default).
- S/W Version: Displays the switch's firmware version.
- H/W Version: Displays the switch's Hardware version.
- DHCP Enabled: Click the box to enable DHCP

- Fallback IP address: Manually assign the IP address that the network is using. 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 for industrial switch. The default gateway is 0.0.0.0.
- Management VLAN: ID of a configured VLAN (1-4094) through which you can 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 must be attached to a port belonging to this VLAN.
- Name: Type in the new user name (The default value is 'admin').
- Password: Type in the new password (The default value is 'admin').
- SNMP Enabled: Enables or disables SNMP on the switch. Supports SNMP version 1 and 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. You must specify trap managers so that key events are reported by this switch to your management station.
- SNMP Read Community: A community string that acts like a password and permits access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects.
- SNMP Trap Community: Community string sent with the notification operation.

Ports

Port configuration ensures access to a switch port based on MAC address, limits the total number of devices from 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 such as Auto, 10 half, 10 Full, 100 Half, 100 Full, 1000 Full or Disabled. User may press Apply button to complete the configuration procedure.



Figure 2-2

Vlan

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting 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 64 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

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: The port number.
- Enabled: Enables LACP on the associated port.
- Key Value: Configures a port's LACP administration key. The port administrative key must be set to the same value for ports that belong 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 will automatically be set to the same value as that used by the LAG.

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto
9	<input type="checkbox"/>	auto
10	<input type="checkbox"/>	auto
11	<input type="checkbox"/>	auto
12	<input type="checkbox"/>	auto
13	<input type="checkbox"/>	auto
14	<input type="checkbox"/>	auto
15	<input type="checkbox"/>	auto
16	<input type="checkbox"/>	auto

Apply Refresh

Figure 2-5

RSTP

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. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 16 distinct 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. That 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 will wait 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	0
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 pathcost on the port. Number between 0 - 200000000. 0 means auto generated pathcost.

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

Apply Refresh

802.1X Configuration

IEEE802.1X provides a security standard for network access control, specially in Wi-Fi wireless networks. 802.1x holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANS to exchange authentication protocol client identity with the client,

and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contain the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

802.1X Configuration

Mode:

RADIUS IP:

RADIUS UDP Port:

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
13	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics

By default, 802.1x is disabled. To use EAP for security, select enabled and set the 802.1X Global Settings for the Radius Server and applicable authentication information.

RADIUS server IP: The IP ADDRESS OF THE EXTERNAL Radius Server, you need to specify an RADIUS server to enable 802.1s authentication.

IGMP Snooping

IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping, as implied by the name, is a feature that 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 in a switch 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. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

Prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to only the subscribers.

IGMP Configuration

- IGMP Enabled: When enabled, the switch will monitor 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 will flood when enabled, and forward to router-ports only when disabled.
- IGMP Snooping Enabled: When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.
- IGMP Querying Enabled: When enabled, the port can serve as the 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

Unregistered IPMC Flooding enabled

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 2-7

Mirroring

Port Mirroring is used on a network switch 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 will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be 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 will be mirrored when the “Mirroring Enabled” check-box is checked.

Mirroring Configuration

Port	Mirror Source
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>

Mirror Port:

- 1
- 2
- 3
- 4

Figure 2-8

QoS

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

QoS Mode: QoS Disabled
802.1p
DSCP

APPLY CANCEL

Figure 2-9-1

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

Queue Mode: Strict WRR
Note : WRR is not supported in Jumbo Frame mode.

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

APPLY CANCEL

Figure 2-9-2

QoS Configuration

Queue Mode	<input checked="" type="radio"/> Strict <input type="radio"/> WRR <small>Note : WRR is not supported in Jumbo Frame mode.</small>
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	medium	1	low	2	low	3	normal
4	medium	5	low	6	high	7	high

APPLY CANCEL

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. User 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

Queue Mode	<input checked="" type="radio"/> Strict <input type="radio"/> WRR <small>Note : WRR is not supported in Jumbo Frame mode.</small>
QoS Mode	DSCP
Prioritize Traffic	All High Priority

Custom
All Low Priority
All Normal Priority
All Medium Priority
All High Priority

DSCP Value(0..63)	Priority
-------------------	----------

Figure 2-9-4

DSCP Configuration	
DSCP Value(0..63)	Priority
	high
	low
	normal
	medium
	high
	high
	high
	high
	high
	high
All others	high

APPLY CANCEL

Figure 2-9-5

Filter Configuration

There are 3 mode that you can choice for filter configuration:

Disabled: this mode is protected from potential threats like hackers, if the traffic from illegal MAC addresses will not be forwarded by the switch.

Static: This table displays the static MAC addresses connected, as well as the VID

DHCP:

Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			<input checked="" type="checkbox"/>
2	Disabled			<input checked="" type="checkbox"/>
3	Disabled			<input checked="" type="checkbox"/>
4	Disabled			<input checked="" type="checkbox"/>
5	Disabled			<input checked="" type="checkbox"/>
6	Disabled			<input checked="" type="checkbox"/>
7	Disabled			<input checked="" type="checkbox"/>
8	Disabled			<input checked="" type="checkbox"/>
9	Disabled			<input checked="" type="checkbox"/>
10	Disabled			<input checked="" type="checkbox"/>
11	Disabled			<input checked="" type="checkbox"/>
12	Disabled			<input checked="" type="checkbox"/>
13	Disabled			<input checked="" type="checkbox"/>
14	Disabled			<input checked="" type="checkbox"/>
15	Disabled			<input checked="" type="checkbox"/>
16	Disabled			<input checked="" type="checkbox"/>

Figure 2-10

PoE (Power over Ethernet) Configuration

PoE technology is a system to pass electrical power safely, along with data, on Ethernet cabling. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE enabled networking device such as Switch or can be injected into a cable run with a midspan power supply.

This figure shows all the PoE 's status when connect or disconnect to the PD device.

- PoE Enabled: POE of the port is able to supply power to the attached PD (Powered Device)
- PD Class: Detect the class of PD
- Delivering Power (W): Output power.
- Current (mA): The status of the port current
- Power output voltage per port
- Power Budget Percentage of PoE power has been used

PoE (Power over Ethernet) Configuration

Port	PoE Enabled	PD Class	Delivering Power [W]	Current [mA]	Voltage [V]	Power Budget [%] (total power = 130W)
1	<input checked="" type="checkbox"/>	--	0	0	0	10.1
2	<input checked="" type="checkbox"/>	3	5.217	101.504	51.395	
3	<input checked="" type="checkbox"/>	--	0	0	0	
4	<input checked="" type="checkbox"/>	0	2.079	40.504	51.33	
5	<input checked="" type="checkbox"/>	--	0	0	0	
6	<input checked="" type="checkbox"/>	--	0	0	0	
7	<input checked="" type="checkbox"/>	--	0	0	0	
8	<input checked="" type="checkbox"/>	3	5.801	113.216	51.237	
9	<input checked="" type="checkbox"/>	--	0	0	0	
10	<input checked="" type="checkbox"/>	--	0	0	0	
11	<input checked="" type="checkbox"/>	--	0	0	0	
12	<input checked="" type="checkbox"/>	--	0	0	0	

Rate Limit Configuration

Type of Port: You can define the certain port as Policer and Shaper before you set up the rate limit.

No Limit: This drop-down menu allows you to specify that the selected port will have no bandwidth limit.

Rate Limit: There is also allow you to enter the data rate, in Kbits per second, this can limit for the selected port. The value is between 128kbps – 3968kbps.

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 ▼

Figure 2-11

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 will then be dropped.

Storm Control Configuration

There are three type of traffic which can be rate limited, including broadcast multicast frame and Flooded Uncast Rate.

Storm Control Configuration

Storm Control Number of frames per second	
Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾
Flooded unicast Rate	No Limit ▾

Figure 2-12-1

- Enable Rate Limit: Click the check box to enable storm control.
- Rate (number of frames per second): The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.
- Web: Click PORTS, Storm Control. This page enables you to set the broadcast storm control parameters for every port on the switch.

Storm Control Configuration

Storm Control Number of frames per second	
Broadcast Rate	9910 ▾
Multicast Rate	1982
Flooded unicast Rate	3964

Apply Refresh

- 5946
- 7928
- 9910
- 11892
- 13874
- 15856
- 17838
- 19820
- 21802
- 23874
- 25766
- 27748
- 29730
- 31712
- No Limit

Figure 2-12-2

Monitoring

Statistic Overview

Statistic Overview for all ports

User can mirror traffic from any source port to a target port for real-time analysis the following figures shows clearly the statistics overview.

Statistics Overview for all ports

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	45635	70	59380	583	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	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	1088	17	200	4	0	1

Figure 3-1

Detailed Statics

To view the statistics of individual ports, click one of the linked port numbers for details.

Clear: To renew the details collected and displayed.

Refresh: To reset the details displayed.

Statistics for Port 1

Clear Refresh

Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8
Port 9 Port 10 Port 11 Port 12 Port 13 Port 14 Port 15 Port 16

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 Broadcast and Multicast	0	Tx Broadcast 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 allows for the automatic detection of links in a Port Trunking Group

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
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

Refresh

LACP Port Status

Figure 3-3-1

- Port: The 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 at the remote end of this LAG link member.
- Operational Port Key: Current operational value of the key used by this LAG.

LACP Port Status

Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs requires.

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational 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		

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
<input type="button" value="Refresh"/>						

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

Figure 3-4

- Hello Time: Interval (in seconds) at which the root device transmits a configuration message.
- Max Age: The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that age 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 among the device ports attached to the network.
- Fwd Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- 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 this switch has accepted as the root device, and the port connected to the root device.

RSTP Port Status

- 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 the media, the higher 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 will instead function as a point-to-point connection.
- P2P Port: Shows if this port is functioning as a Point-to-Point connection to exactly one other bridge. 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 will assume that it is connected to two or more bridges.
- Protocol: Shows the spanning tree protocol functioning on this port, either RSTP or STP (that is, STP-compatible mode).

IGMP Status

IGMP Status

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

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

Refresh

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 5
Mode	Full
	Full
	Anomaly
	Anomaly w/o X-pair

Apply

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. (Range: 1-20)
- Time Out: setting the time period of host will be Ping

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	<input type="text"/>
Count	1 ▾
Time Out (in secs)	1 ▾

Apply

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

Refresh

Figure 3-7-1

Ping Parameters

Target IP address	192.168.0.1
Count	1
Time Out (in secs)	1

Apply

Ping Results	
Target IP address	192.168.0.1
Status	Test starting...
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 3-7-2

Ping Parameters

Target IP address	192.168.0.1
Count	1
Time Out (in secs)	1

Apply

Ping Results	
Target IP address	192.168.0.1
Status	Test starting...
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 3-7-3

Maintenance

Warm Restart

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

Warm Restart

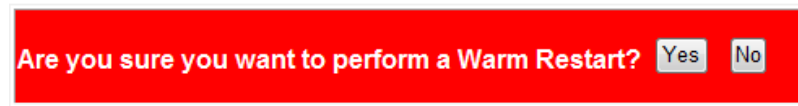


Figure 4-1

Factory Default

Forces the switch to restore the original factory settings. To reset the switch, select "Reset to Factory Defaults" from the drop-down list and click Apply. The LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory

Factory Default



Figure 4-2

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. User can download firmware files for user's switch from the Support section of your local supplier.

Software Upload

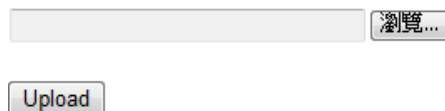


Figure 4-3

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. To 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

 瀏覽...

Configuration Download

Figure43-4

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:	<input type="text"/>
-----------	----------------------

Figure 4-5

Reset button for the factory default setting

Please take the following steps to reset the Web Smart Switch back to the original default:

Step 1:

Turn on the Web Smart Switch

Step 2:

Press and hold the reset button continuously for 5 seconds and release the reset button.

Step 3:

The switch will reboot for 20 seconds and the configuration of switch will back to the default setting.