

LevelOne

GES-2452

24 GE + 2GE SFP

Web Smart Switch

User Manual

Version 1.0-1109

FCC Certifications



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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

CE Mark Warning

CE

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class A for ITE, the essential protection requirement of Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks: All trade names and trademarks are the properties of their respective companies.

Copyright © 2011, All Rights Reserved.

Table of Contents

Chapter 1 Introduction to the Web Smart Switch	6
1.1 General Description ·····	6
1.2 The Front Panel ·····	7
1.3 LEDs Definition ·····	7
1.4 The Rear Panel ·····	7
1.5 Installation	9
Chapter 2 Basic Web Management Information1	1
2.1 System login······1	1
2.2 The Graphic User Interface1	2
2.3 Logging Out of the Web Configurator1	6
Chapter 3 Web Management Configuration1	7
3.1 Status ······1	7
3.1.1 System Information ······1	7
3.1.2 Log ······1	8
3.1.3 Port2	20
3.1.3.1 Port Statistics 2	20
3.1.3.2 Port Counters ······2	21
3.1.3.3 Port Error Disabled ······2	23
3.1.3.4 Bandwidth Utilization ······ 2	23
3.1.4 Trunk Group······2	24
3.1.5 MAC Address Table ······2	25
3.1.5.1 Dynamic Learned ······2	25
3.1.5.2 Static MAC 2	26
3.2 Network ······2	27
3.2.1 IP Address ······2	27
3.2.2 IPv6 Address······2	28
3.2.3 Time2	29
3.3 Switching ······3	\$1
3.3.1 Port Setting······3	51
3.3.2 Port Mirroring ······3	32
3.3.3 Trunk ······3	3
3.3.3.1 Trunk Group 3	33
3.3.3.2 LACP	35
3.3.4 VLAN3	6
3.3.4.1 VLAN Setting······ 3	36

3.3.4.2 VLAN Port Setting ······	• 37
3.3.4.3 VLAN Port Mode Setting	• 38
3.3.4.4 VLAN Ingress Filter	- 39
3.3.5 SVLAN	-39
3.3.5.1 SVLAN Setting	- 39
3.3.5.2 SVLAN Member Setting	• 40
3.3.5.3 SVLAN PVID Setting	• 41
3.3.5.4 SVLAN Service Port	• 41
3.3.6 Bandwidth Control	•42
3.3.6.1 Preamble Setting	• 42
3.3.6.2 Port Rate Setting ······	• 43
3.3.7 IGMP Snooping ······	•45
3.3.7.1 IGMP Setting ······	• 45
3.3.7.2 IGMP VLAN Setting ·····	• 46
3.3.7.3 Multicast Database ·····	• 47
3.3.7.4 Router Table ······	- 48
3.3.8 Jumbo Frame	•48
3.3.9 STP	-49
3.3.9.1 STP Global Setting ·····	• 49
3.3.9.2 STP Port Setting ·····	• 51
3.3.9.3 MST Configuration	• 52
3.3.9.4 MST Instance Setting	• 54
3.3.9.5 MST Port Setting ·····	• 54
3.4 Security ·····	•56
3.4.1 Storm Control	•56
3.4.2 MAC Filtering ·····	•57
3.4.3 802.1X ·····	•58
3.4.3.1 802.1X Setting	- 58
3.4.3.2 802.1X Port Setting·····	• 60
3.4.4 Port Security	•61
3.4.5 Protected Ports	•62
3.4.6 Access	•62
3.4.6.1 Console ······	• 62
3.4.6.2 Telnet	• 63
3.4.6.3 SSH	• 64
3.4.6.4 HTTP	• 65
3.4.6.5 HTTPS	• 65
3.5 ACL	-66
3.5.1 ACL Setting·····	•66

3.5.2 ACL Tomplato Sotting	60
2.5.2 ACL Index Denge Setting	70
3.5.3 ACL Index Range Setting	······/0
3.5.4 ACL Policy Setting	
	······/1
3.6.1 Port-based Priority	
3.6.2 802.1 p- based Priority	/2
3.6.3 DSCP - based Priority	73
3.6.4 Priority to Queue Mapping ······	74
3.6.5 Packet Scheduling ·····	76
3.6.6 Queue Weight Setting ·····	76
3.6.7 Queue Remarking Status	77
3.6.8 Queue Remarking Table	78
3.7 Management ·····	79
3.7.1 SNMP	79
3.7.1.1 SNMP Setting ·····	79
3.7.1.2 SNMP Community ·····	
3.7.1.3 SNMP Trap	
3.8 Diagnostics	82
3.8.1 Ping Test ·····	82
3.8.2 Ping6 Test ·····	83
3.8.3 Log Setting ·····	84
3.8.3.1 Local Log·····	
3.8.3.2 Remote Log ·····	85
3.8.4 Factory Default ·····	
3.8.5 Reboot Switch	
3.9 Maintenance	87
3.9.1 Backup Manager·····	87
3.9.2 Upgrade Manager ·····	
3.9.3 Configuration Manager	90
3.9.4 Account Manager ·····	91
3.9.5 Enable Password ·····	92
Product Specifications	94

Chapter 1 Introduction to the Web Smart Switch

1.1 General Description

High Performance

GES-2452 is a powerful, high-performance Gigabit Ethernet switch with 24*10/100/1000Mbps ports and 2*SFP (mini GBIC) ports, providing you a cost-effective, space-saving solution for expanding your network. The gigabit ports can lead you to a real gigabit connection, making you be able to transfer high bandwidth-needed files larger and faster in an easy way. And the four mini gigabit ports allow you to add fiber-optic connectivity for connecting to other network switches to obtain long-distance communication.

This device provides the easy management function through the Ethernet Web. The network administrator can configure the status and the port function setting of the device through the Web-Based UI. When installing the auto-discovery management tool helps network managers to search and access those switches on LAN easily. Therefore, network managers can access switches that support auto-discovery on LAN without memorizing IP address.

Smart Features

GES-2452 provides rich features including Link Aggregation, VLANs, IGMP Snooping, Port Trunking, Spanning Tree, Security (Port Security and 802.1x authentication) and other network management to meet the requirements evolving medium and small-sized enterprises. QoS secures the bandwidth for some bandwidth-demanded applications including VoIP or video conference. Additionally, IEEE 802.3az Energy Efficient Ethernet ability is supported to promise operation in Low Power Idle Mode and save power consumption.

Easy Installation and Management

This switch is plug & play and hassle-free in installation. Auto-MDI/MDI-X crossover on all ports eliminates the need for crossover cables for connection to another switch or hub. Auto-Negotiation on each port senses the link speed of a network device and intelligently adjusts for compatibility and optimal performance. This switch also features diagnostic LEDs, which display the status and activities of the LEDs, allowing you to quickly detect and correct problems on the network.

1.2 The Front Panel

The following figure shows the front panel of the switch.



The following table describes the port labels on the front panel.

LABEL	DESCRIPTON
24 10/100 RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router
Four Mini-GBIC Slots:	Use mini-GBIC transceivers in these slots for connections to backbone Ethernet switches.

1.3 LEDs Definition

This device provides extensive leds to show the activities on power, system and ports. See the following description for your reference:

LED	Status	Operation
Power	Steady Green	The switch is powered on.
	Off	The switch is powered off.
	Steady Green	Valid port connection.
Link/ACT	Blinking Green	Valid port connection and there is data transmitting/ receiving.
	Off	Port disconnected.

The RESET Button

Reset the switch to its factory default configuration via the RESET button. Press the RESET button for one second and release. The switch automatically reboots and reloads its factory configuration file. The RESET button is on the front panel of the switch.

1.4 The Rear Panel

The following figure shows the rear panel of the switch:



Power Receptacle

To be compatible with the electric service standards around the world, the switch is designed to afford the power supply in the range from 100 to 240 VAC, 50/60 Hz. Please make sure that your outlet standard to be within this range.

To power on the switch, please plug the female end of the power cord firmly into the receptacle of the switch and the other end into an electric service outlet. After the power cord installation, please check if the power LED is lit for a normal power status.

1.5 Installation

This switch can be placed on your desktop directly, or mounted in a rack. Please refer to the instructions for installation.

Before installing the switch, we recommend:

- 1. The switch is placed with appropriate ventilation environment. A minimum 25 mm space around the unit is recommended.
- 2. The switch and the relevant components are away from sources of electrical noise such as radios, transmitters and broadband amplifiers
- 3. The switch is away from environments beyond recommend moisture

Desktop Installation

- 1. Install the switch on a level surface that can support the weight of the unit and the relevant components.
- 2. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet.

Rack-mount Installation

The switch may be standalone, or mounted in a rack. Rack mounting facilitate to an orderly installation when you are going to install series of networking devices.

Procedures to Rack-mount the switch:

- 1. Disconnect all the cables from the switch before continuing.
- 2. Place the unit the right way up on a hard, flat surface with the front facing you.
- 3. Locate a mounting bracket over the mounting holes on one side of the unit.
- 4. Insert the screws and fully tighten with a suitable screwdriver.
- 5. Repeat the two previous steps for the other side of the unit.
- 6. Insert the unit into the rack and secure with suitable screws.
- 7. Reconnect all the cables.

Installing Network Cables

1. Crossover or straight-through cable: All the ports on the switch support Auto-MDI/MDI-X functionality. Both straight-through or crossover cables can be used as the media to connect the switch with PCs as well as other devices like switches, hubs or router.

2. Category 3, 4, 5 or 5e, 6 UTP/STP cable: To make a valid connection and obtain the optimal performance, an appropriate cable that corresponds to different transmitting/receiving speed is required. To choose a suitable cable, please refer to the following table.

Media	Speed	Wiring
	10 Mbps	Category 3,4,5 UTP/STP
10/100/1000 Mbps copper	100 Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP
1000 Mbps Fiber (mini-GBIC required)1000 MbpsT re		The cable type differs from the mini-GBIC you choose. Please refer to the instruction came with your mini-GBIC.

Chapter 2 Basic Web Management Information

2.1 System login

- 1. Start your web browser.
- 2. Type "http://"and the IP address of the switch (for example, the default management IP address is 192.168.1.1) in the Location or Address field. Press [ENTER].



3. The login screen appears. The default username and password are **admin**, so you can click **OK** and go to the web configuration screen directly.



2.2 The Graphic User Interface

After the password authorization, the information page shows up. You may click on each folder on the left column of each page to get access to each configuration page. The Graphic User Interface is as follows:

level one		8 10 12 14 16 18 20 22 24 0 0 0 0 0 0 0 0	8 B B B B B B B B B B B B B B B B B B B
LOGOUT REBOOT REFRES	н		
~	System Information		
k v			
ing 🗢	System Setting		
ly ⇒	System Name	GF5-2452	1.1
	System name		-
~	System Location	LevelOne	
ement 👳	System Contact		C
stics 👳			
nance 👳	Apply		
Α	• System Information		
	Information Name	Information Value	
	System Name	GE3-2452	
	System Location	Televac	
	MAC Address	DE AD RE EE 01-02	
	IP Address	192 169 1 1	
	Subnet Mask	255 255 255 0	
	Gateway	192 168 1 254	
	Loader Version	1.3.0.16735	
	Loader Date	Sat Apr 23 17:26:50 CST 20	11
	and the second se	Provident Contract Contract Contracts	
	Firmware Version	1.0.0	
	Firmware Version Firmware Date	1.0.0 Set Apr 23 17:21 52 CST 20	11
	Firmware Version Firmware Date System Object ID	1.0.0 Set Apr 23 17:21:52 CST 20 1.3.6.1.4.1.27282.3.2.10	11

A –Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B –It shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down.

C –Displays system information such as MAC address and firmware version.

In the navigation panel, click a main link to reveal a list of submenu links shown as the following:

Status	Network	Switching
Status 🗢	Network 🗢	Switching 🗢
System Information Log Port ⊅ Trunk Group MAC Address Table ♪	IP Address IPv6 Address Time	Port SettingPort MirroringTrunk▷VLAN▷SVLAN▷Bandwidth Control▷IGMP Snooping▷Jumbo Frame▷
Security	ACL	QoS
Security✓Storm ControlMAC Filtering802.1X▷Port SecurityProtected PortsAccess▷	ACL Setting ACL Template Setting ACL Index Range Setting ACL Policy Setting	QoSPort-based Priority802.1p-based PriorityDSCP-based PriorityPriority to QueueMappingPacket SchedulingQueue Weight SettingQoS Remarking StatusQoS Remarking Table
Management	Diagnostics	Maintenance
Management ⊽ SNMP Þ	DiagnosticsPing TestPing6 TestLog SettingFactory DefaultReboot Switch	MaintenanceBackup ManagerUpgrade ManagerConfiguration ManagerAccount ManagerEnable Password

The following table describes the links in the navigation panel.

LINKS DESCRIPTION		
Status	•	
System Information	This link takes you to a screen that displays general system information.	
Log	This sub-menu takes you to screens where you can view and setup system logs.	
Port	This link takes you to a screen where you can configure the port information.	
Trunk Group	This link takes you to a screen where you can configure the trunk settings on a port.	
MAC Address Table	This link takes you to screens where you can configure MAC address options.	
Network		
IP Address	This link takes you to a screen where you can configure the IP information.	
IPv6 Address	This link takes you to a screen where you can configure the IPv6 information.	
Time	This link takes you to a screen where you can configure the switch's time settings.	
Switching		
Port Setting	This link takes you to a screen where you can configure settings for individual switch ports.	
Port Mirroring	This sub-menu takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.	
Trunk	This link takes you to a screen where you can configure the trunk settings on a port.	
VLAN	This link takes you to a screen where you can configure the VLAN (IEEE 802.1Q) settings on a port.	
SVLAN	This link takes you to a screen where you can configure the SVLAN settings on a port.	
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the switch.	
IGMP Snooping	This sub-menu takes you to screens where you can configure and revising the information of IGMP Snooping.	
Jumbo Frame	This link takes you to a screen where you can configure the Jumbo Frame size.	
STP	This sub-menu takes you to screens where you can configure the STP to prevent network loops.	
Security		
Storm Control	This link takes you to a screen where you can limit the number of broadcast, multicast and unknown unicast and multicast packets the Switch receives per second on the	

	ports.	
MAC Filtering	This sub-menu takes you to screens where you can configure the accessed MAC address.	
802.1X	This sub-menu takes you to screens where you can configure IEEE 802.1x port authentication for clients communicating via the switch.	
Port Security	This link takes you to a screen where you can configure the port security setting.	
Protected Ports	This link takes you to a screen to setting and revising the protected ports.	
Access	This link takes you a way to access the switch.	
ACL		
ACL Setting	This link takes you to a screen to setting and revising the basic setting of ASL.	
ACL Template Setting	This link takes you to a screen to setting and revising the template setting of ASL.	
ACL Index Range Setting	This link takes you to a screen to setting and revising the index range setting of ASL.	
ACL Policy Setting	This link takes you to a screen to setting and revising the policy setting of ASL.	
QoS		
Port-based Priority	This link takes you to a screen where you can assign a IEEE 802.1p priority to packets based on the ingress (incoming) port of the packet.	
802.1p-based Priority	This link takes you to a screen where you can assign a IEEE 802.1p-based priority to packets based on the ingress (incoming) port of the packet.	
DSCP-based Priority	This link takes you to a screen where you can assign priority to packets based on their Differentiated Services Code Points (DSCPs).	
Priority to Queue Mapping	This link takes you to a screen where you can configure the priority level-to-physical queue mapping.	
Packet Scheduling	Packet Scheduling is used to help solve performance degradation when there is network congestion. Use this screen to configure queuing algorithms for outgoing traffic.	
Queue Weight Setting	This link takes you to a screen where you can assign a queue weight to packets based on the ingress (incoming) port of the packet.	
QoS Remarking Status	This link takes you to a screen where you can assign a QoS remarking status to packets based on the ingress (incoming) port of the packet.	
QoS Remarking Table	This link takes you to a screen where you can assign a QoS remarking table to packets based on the ingress (incoming) port of the packet.	
Management		
SNMP	This link takes you to a screen where you can set and revise the SNMP.	
Diagnostics		
Ping Test	This link takes you to a screen where you can do Ping test.	

Ping6 Test	This link takes you to a screen where you can do Ping6 test.	
Log Setting	This link takes you to a screen where you can configure log settings.	
Factory Default	This link takes you back to the factory default configuration.	
Reboot Switch	This link takes you to a screen where you can reboot the switch.	
Maintenance		
Backup Manager This link takes you to a screen where you can back settings you have made.		
Upgrade Manager	This link takes you to a screen where you can upgrade the switch settings.	
Configuration Manager	This link takes you to a screen where you can save all the configurations you have made to the switch.	
Account Manager	This link takes you to a screen where you can change the web configurator login account.	
Enable Password	This link takes you to a screen where you can change the login password.	

2.3 Logging Out of the Web Configurator

Click **Logout** in the navigation panel to exit the web configurator. You have to log in with your password again after you log out, if there is any. This is recommended after you finish a management session for security reasons.



Chapter 3 Web Management Configuration

3.1 Status

Use the Status pages to view system information and status.

3.1.1 System Information

In the navigation panel, click **Status** > **System Information** to display the screen as shown below. This page allow user to configure and browse some system information such as MAC address, IP address, loader version and firmware version and so on.

System Information

System Name	GES-2452
System Location	LevelOne
System Contact	

Apply

Information Name	Information Value	
System Name	GES-2452	
System Location	LevelOne	
System Contact		
MAC Address	DE:AD:BE:EF:01:02	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Gateway	192.168.1.254	
Loader Version	1.3.0.16735	
Loader Date	Sat Apr 23 17:26:50 CST 2011	
Firmware Version	1.0.0	
Firmware Date	Sat Apr 23 17:21:52 CST 2011	
System Object ID	1.3.6.1.4.1.27282.3.2.10	
System Up Time	O days, O hours, 4 mins, 25 secs	

LABEL	DESCRIPTION	
System Name	This field displays the descriptive name of the switch for identification purposes.	
System Location	This field displays the system location of the switch.	
System Contact	This field displays the system contact of the switch.	
MAC Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.	
IP Address	This field displays the IP address of the switch.	
Subnet Mask	This field displays the subnet mask of the switch.	
Gateway	This field displays the IP address of the gateway.	
Loader Version	This field displays the loader version of the switch.	
Loader Date	This field displays the loader date of the switch.	
Firmware Version	This field displays the version number of the switch's current firmware.	
Firmware Date	This field displays the switch's firmware created date.	
System Object ID	This field displays the system object ID of the switch.	
System Up Time	This field displays the system up time.	

3.1.2 Log

Use this screen to display the switch logs. Click **Status** > **Log** in the navigation panel to display the screen as shown below.

Log

Log Information Select



View

Log Information		
Information Name	Information Value	
Information Name	Information value	
Target	RAM	
Severity	error, warning, notice, info	
Category	ACL, Common, DAI, DEF_ENGINE, DoS, Dot1X, EEE, IGMP, L2, LACP, LLDP, Log, Mirror, POE, Port, QoS, QinQ, Rate, SNMP, STP, SVLAN, Switch, System, TFTP, Trunk, UDLD, VLAN, LOOP_PROT, DHCP_SNOOPING	
Total Entries	2	

Log				
CI	ear 👘	Refresh		
	PREV 1			
No.	Severity	Category	Timestamp	Message
	notice	Port	Jan 01 00:00:15	Port 8 link un
1		1 011	10411 01 00.00.10	r on o min ap

LABEL	DESCRIPTION		
Target	Select RAM to display only the logs stored in the RAM. Select Flash to display only the logs stored in the Flash memory.		
Severity	 Select severity level(s) to filter log messages. The possible severity levels are: Error - to record system failures, such as events which will cause the switch to malfunction and events such as invalid user input in the web configurator. Warning - to record non critical errors on the Switch. The Switch will continue to function when warnings are recorded. Info - to record regular system events, such as configuration changes or logins. 		

	Notice- to record the error which need to be noticed.		
Category	Select category to filter log messages. The categories are based on software and hardware features of the switch. For example the category MIRROR records events which deal with the Port Mirroring features you set up and the category SYSTEM records events which deal with the overall operation of the switch.		
View	iew Click the View button to display the logs according the criteria specified in fields above.		
No.	This is the index number for the log entry.		
Severity	This field displays the severity level of the log entry.		
Category	This field displays what category the log entry fits into.		
Timestamp	This field specifies the time when the switch recorded the log event. The switch resets its internal clock when it is restarted.		
Message	This field displays an explanation for the log entry.		

3.1.3 Port

The Port configuration page displays port summary and status information.

3.1.3.1 Port Statistics

Use this screen to display the Switch port statistics. Click **Status->Port > Port Statistics** to view the screen as shown next.

Port Statistics

Clear					
Port	Link Status	TX Good Packets	TX Bad Packets	RX Good Packets	RX Bad Packets
Port 01	DOWN	0	0	0	0
Port 02	DOWN	0	0	0	0
Port 03	DOWN	0	0	0	0
Port 04	DOWN	0	0	0	0
Port 05	DOWN	0	0	0	0
Port 06	DOWN	0	0	0	0
Port 07	DOWN	0	0	0	0
Port 08	UP	3422	0	2628	0
Port 09	DOWN	0	0	0	0

runk Statistics				
Frunk	TX Good Packets	TX Bad Packets	RX Good Packets	RX Bad Packets
Frunk 1	112			
Frunk 2				
Trunk 3				
Trunk 4			1	
Trunk 5				
Trunk 6				
Trunk 7				555
Trunk 8				

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
Port	This identifies the Ethernet port.	
Link Status	This field displays Link Up if the port is currently in use. Otherwise it displays Link Down .	
Tx Good Pkt	This field shows the number of frames successfully transmitted on this port.	
Tx Bad Pkt	This field shows the number of frames unsuccessfully transmitted on this port.	
Rx Good Pkt	This field shows the number of frames successfully received on this port.	
Rx Bad Pkt	This field shows the number of frames unsuccessfully received on this port.	
Clear	Click the Clear button to reset the port statistics.	

3.1.3.2 Port Counters

Click Status->Port > Port Counters to view the screen as shown next.

This page displays standard counters on network traffic from the Interface, Etherlike and RMON MIB. Interface and Etherlike counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.

Port Counters

Port MIB Counters Settings

▼ Port1 mib Counters

IF mib Counter Name	mib Counter Value
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Ether-Like mib Counter Name	mib Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Rmon mib Counter Name	mib Counter Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0
IngressLackPktBufDrop	0

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Mode	You have four choices: All, Interface, Etherlike and RMON.

3.1.3.3 Port Error Disabled

This page allow user to browse ports which disabled by some protocols such as BPDU Guard, Loopback and UDLD.

P	ort	Error	Disab	led

Port Name	Error Disabled Reason	E
-----------	-----------------------	---

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port Name	This shows the disabled Ethernet port.
Error Disabled	Here shows the reasons of these error.
Reason	
Recover	Click this button to enable those error disabled ports.

3.1.3.4 Bandwidth Utilization

Web Smart Switch

	Gbp	S	1	OOMb	ps		10Mb	ps	_ L	.ink D)own		Re	fresh	perio	d: 5	1	se 🖌	с	IFG:	Enable	•					
%											Тх																
P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28
		0%		0%			0%		U%		U%	U%	0%										U%	0%	υ%	υ%	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Refresh Period	This shows the period interval between last and next refresh. You have three choices: 2 sec, 5 sec and 10 sec
IFG	You can enable or disable this function.

3.1.4 Trunk Group

Click Status > Trunk Group in the navigation panel to view the screen as shown below.

Trunk	Grouj	ormation				
Trunk	Туре	Master Port	Member	Active/Passive	Aggregated	Delete

LABEL	DESCRIPTION
Trunk	This field displays the trunk to identify a trunk group, that is, one logical link containing multiple ports.
Туре	This field displays the type of the trunk group: a static trunk or an LACP trunk.
Master port	This field displays which ports are master ports of the trunk. The port with lowest port ID is choosed to be master port of the trunk. To synchronize the settings of trunk member ports, the configuration to trunk master port would be applied to all trunk member ports. Other member ports are slave ports that can not be configured individually in most settings (such as VLAN, port ability and so on.) but to follow the configuration of master port.
Member	This field shows the member ports of the trunk.
Active/ Passive	If the trunk is an LACP trunk, this field shows the LACP active and passive ports. The LACP active port would send LACP PDU periodically.
Aggregated	This field displays the ports that aggregated in a trunk group. A static trunk would be aggregated immediately; an LACP trunk exchanges LACP PDU to link partner to aggregate.
Delete	Click this button to delete the trunk.

3.1.5 MAC Address Table

Use the MAC Address Table pages to show dynamic MAC table and configure settings for static MAC entries.

3.1.5.1 Dynamic Learned

Click **Status > MAC Address Table > Dynamic Learned** in the navigation panel to bring up the screen as shown next.

Port Port 01 VLAN default MAC Address 00:00:00:00 View Clear	• • 0.00			
MAC Address Inform FIRST PREV 1 NEXT	nation			
MAC Address	VLAN	Туре	Port	
00:0E:A6:03:0D:44	default(1)	Dynamic	8	Add to Static MAC table
Total Entries:1				

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
VLAN	This is the VLAN group to which the MAC address belongs. Select the VLAN to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
MAC Address	This field displays the MAC address that will be forwarded. Select the MAC address to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
View	Click the View button to display the logs according the criteria specified in the fields above.
Clear	Click this button to remove any dynamically learned MAC address forwarding entries.
Туре	This shows whether the MAC address is Dynamic (learned by the Switch) or Static Unicast (manually entered in the Static MAC Forwarding screen).
Port	This field displays the port where the MAC address will be forwarded.
Add to Static MAC table	Click this button to add any port into the static MAC table.

3.1.5.2 Static MAC

Click **Status > MAC Address Table > Static MAC** in the navigation panel to bring up the screen as shown next.

Static MAC

Static MAC Setting

MAC Address	VLAN	Туре	Port
00:00:00:00:00	default 🖌 🖌	Unicast 🗸 🗸 🗸	Port 01

Add

lo.	MAC Address	VLAN	Туре	Port	Delete
	DE:AD:BE:EF:01:02	default(1)	Unicast	CPU	

LABEL	DESCRIPTION
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VLAN	Enter the VLAN identification number the MAC address belongs to.
Туре	 There are two types of MAC entry: Unicast: add a unicast MAC entry. Multicast: add a multicast MAC entry.
Port	If Type is unicast, select the port number of the MAC entry; If Type is multicast, select the port list of the MAC entry.
Add	Click Add to add any port into the static MAC address table.
No.	This is the index number for the MAC address forwarding entries.
Delete	To delete any selected MAC address entries.

3.2 Network

Use the Network pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

3.2.1 IP Address

Use the IP Setting screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic.

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

Click **Network** > **IP Address** in the navigation panel to display the screen as shown below.

IP Address

IP Address Setting

Mode	⊙Static ○DHCP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

Apply

nformation Name	Information Value
DHCP State	Disabled
Static IP Address	192.168.1.1
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.1.254

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Mode	Select Static from the drop-down box if you don't have a DHCP server or if you wish to assign static IP address information to the switch. You need to fill in the following fields when you select this option. Select DHCP option if you have a DHCP server that can assign the switch an IP address, subnet mask and a gateway IP address automatically.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1. If static mode is enabled, enter IP address in this field.
Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field.
Gateway	Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field.
Apply	Click Apply to save your changes to the switch.

3.2.2 IPv6 Address

Click **Network**> **IPv6 Address** in the navigation panel to display the screen as shown below.

IPv6 Address

Pv6 Address Setting				
Auto Configuration	ODisable 🖲 Enable			
IPv6 Address	<u></u> , 1 <u>0</u>			
Gateway	ii .			

Apply

Information Name	Information Value	
Auto Configuration	Enabled	
IP∨6 In Use Address	fe80::dcad;beff;feef;102 \ 64	
IPv6 In Use Router	н	
IPv6 Static Address	:: \ 0	
IPv6 Static Router		

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Auto	Select Enable or Disable this function.
Configuration	
IPv6 Address	Enter the IPv6 address of your switch. If auto configuration mode is
Gateway	configuration mode is disabled, enter IPv6 gateway address in this field.
Apply	Click Apply to save your changes to the switch.
Auto	It displays whether the auto configuration function is opened or not.
Configuration	
IPv6 In Use	It displays the in use address information of IPv6.
Address	
IPv6 In Use	It displays the in use router information of IPv6.
Router	
IPv6 Static	It displays the static address of IPv6.
Address	
IPv6 Static	It displays the static router of IPv6.
router	

3.2.3 Time

Click **Network> Time** in the navigation panel to display the screen as shown below.

Time

SNTP Configuration

SNTP State	⊙Enabled ⊙Disabled		
SNTP Server Address	0.0.0.0		
SNTP Server Port	123		
Time (HH:MM:SS)	0 🔹 : 11 🔹 : 55 💌		
Date (YYYY-MM-DD)	2000 🗸 . 1 🗸 . 1 🗸		
Time Zone (+/- HH:MM)	+ • 0 • : 0 •		

Apply

Information Name	Information Value	
SNTP State	Disabled	
SNTP Server	0.0.0	
SNTP Port	123	
Current Time	00:11:55	
Current Date	2000-01-01	
Time Zone	GMT + 0 0	

LABEL	DESCRIPTION
SNTP State	Select Enable to use Simple Network Time Protocol (SNTP) or Disable
	to set the time manually.
SNTP Server	If SNTP is enabled, enter the IP address of the time server you will use.
Address	
SNTP Server	It shows the Port Number of SNTP server.
Port	
Time	If SNTP is disabled, enter the new time in hour, minute and second
(HH:MM:SS)	format.
Date	If SNTP is disabled, enter the new date in year, month and day format.
(YYYY-MM-DD)	
Time Zone	Select system time zone by hours and minutes. "+" means after-UTC and
	"-" means before-UTC.
Apply	Click Apply to save your changes to the switch.

3.3 Switching

Use the Switching pages to configure settings for the switch ports, trunk and other switch features.

3.3.1 Port Setting

This page allow user to configure switch port settings and show port current status. Click **Switching** > **Port Setting** in the navigation panel to display the screen as shown below.

P	ort Select		Name	Enabled	Speed	d Duplex	Flow Control
ect Port	5	•		⊙Enabled ○Dis	sabled Auto	Auto 🗸	⊙Enabled ○Disabled
Apply Port Sta	tus						
Port	Name	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
01		Enabled	DOWN	Auto	Auto	Disabled	Disabled
02		Enabled	DOWN	Auto	Auto	Disabled	Disabled
02				0		Disabled	Disabled
03		Enabled	DOWN	AUTO	Auto	Disabled	Disabled
03		Enabled Enabled	DOWN	Auto	Auto	Disabled	Disabled
03 04 05		Enabled Enabled Enabled	DOWN DOWN DOWN	Auto Auto	Auto Auto Auto	Disabled Disabled Disabled	Disabled Disabled Disabled
03 04 05 06		Enabled Enabled Enabled Enabled	DOWN DOWN DOWN DOWN	Auto Auto Auto Auto Auto	Auto Auto Auto Auto	Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled
03 04 05 06 07		Enabled Enabled Enabled Enabled Enabled	DOWN DOWN DOWN DOWN DOWN	Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto	Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled
03 04 05 06 07 08		Enabled Enabled Enabled Enabled Enabled Enabled	DOWN DOWN DOWN DOWN DOWN UP	Auto Auto Auto Auto Auto A-1000M	Auto Auto Auto Auto Auto Auto A-Full	Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled

LABEL	DESCRIPTION			
Port Select	Select the port(s) from the list box that you will change the port settings			
	for.			
Name	It allows you to give a description for the port.			
Enabled	Select Enable from the drop-down box to enable a port. The factory			
	default for all ports is enabled. A port must be enabled for data			
	transmission to occur. Select Disable to not use a port.			
Speed	Port speed capabilities:			
	Auto: Auto speed with all capabilities.			
	Auto-10M: Auto speed with 10M ability only.			
	Auto-100M: Auto speed with 100M ability only.			
	Auto-1000M: Auto speed with 1000M ability only.			
	Auto-10/100M: Auto speed with 10/100M ability.			
	10M: Force speed with 10M ability.			
	100M: Force speed with 100M ability.			
	1000M: Force speed with 1000M ability.			
	Selecting Auto (auto-negotiation) allows one port to negotiate with a peer			
	port automatically to obtain the connection speed and duplex mode that			

	both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Duplex	Port duplex capabilities:
	Auto: Auto duplex with all capabilities.
	Full: Auto speed with 100M ability only. Full: Auto speed with 100M ability only.
Flow Control	A concentration of traffic on a port decreases port bandwidth and
	overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select " Enabled " to enable it. Or select " Disabled " to disable it.
Apply	Click Apply to save your changes to the switch.
Flow Control	The Config column displays if Flow Control has been configured to be
Config	turned On or Off for the port.
Flow Control	The column displays the port's current Flow Control status.
Status	

3.3.2 Port Mirroring

The Mirror function copies all the packets that are transmitted by the source port to the destination port. It allows administrators to analyze and monitor the traffic of the monitored ports.

The Mirror Configuration steps are as follows:

1. Choose "enable " or "disable" this function in "State" column

2. Select those ports that are going to be monitored by marking the checkboxes in "**Monitoring Port**" column.

3. Click the **"TX"** or **"RX"** or **"Both"** in the drop list of **"Sniffer Mode"** column. Select the packet types that are going to be monitored (transferred or received packets or both).

4. Click "**Apply**" to activate.

Port Morriring

Mirroring Port
01
iffer Mode
K Ports Both
K Port Source RX Port N/A

(a) Destination port: Theoretically it's possible to set more than one destination port in a network. Actually the port mirroring function will lower the network throughput, and therefore it's recommended to set "only one" destination port in a network.

(b) Mirroring Port: (1)RX: means copy the incoming packets of the selected source port to the selected destination port. (2)TX: means copy the outgoing packets of the selected source port to the selected destination port. (3)Rx & Tx: means the combination of Rx and Tx.

(c) Source port: the traffic source that will be copied to the destination port.

3.3.3 Trunk

3.3.3.1 Trunk Group

Click **Switching**> **Trunk** > **Trunk Group** in the navigation panel to view the screen as shown below.

Trunk Group

Trunk Group Setting

Trunk	Туре	Ports	LACP Active
Trunk 1 🔽	⊙Static ○LACP	Select Ports 👻	Select Ports 👻

Apply

Trunk G	roup In	formation				
Trunk	Туре	Master Port	Member	Active/Passive	Aggregated	Delete
	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					201010

LABEL	DESCRIPTION
Trunk	This field displays the trunk group number to identify a trunk group, that is,
	one logical link containing multiple ports.
Туре	Select the type of the trunk group: a static trunk or an LACP trunk. A static
	trunk would be aggregated immediately; an LACP trunk exchanges LACP
	PDU to link partner to aggregate.
Ports	Select the ports to be added to the trunk group. There are the following
	limitations for choosing the member ports:
	A member port can not be bandwidth limited.
	A member port can not be a mirroring port.
	Member ports should join the same VLANs.
	A member port can not join more than one trunk group.
	A member port can not be in 802.1x force-authed or auth mode.
	There could be at most 8 member ports in a trunk.
LACP Active	Select the LACP active ports to be added to the trunk group. This field is
	active when LACP is selected as the Type.
Apply	Click Apply to save your changes to the switch.
Trunk	This field displays the trunk number to identify a trunk group, that is, one
	logical link containing multiple ports.
Туре	Here displays the type of the trunk group: a static trunk or an LACP trunk.
Master Port	This field displays the master port's information.
	The port with lowest port ID is choosed to be master port of the trunk. To
	synchronize the settings of trunk member ports, the configuration to trunk
	master port would be applied to all trunk member ports. Other member ports
	are slave ports that can not be configured individually in most settings (such
	as VLAN, port ability and so on.) but to follow the configuration of master
	port.
Member	This field displays the ports that are part of the trunk group.
Active/	If the trunk is an LACP trunk, this field shows the LACP active and passive
Passive	ports. The LACP active port would send LACP PDU periodically.

Aggregated	This field displays the ports that aggregated in a trunk group. A static trunk would be aggregated immediately; an LACP trunk exchanges
	LACP PDU to link partner to aggregate.
Delete	Click this button to delete the trunk.

3.3.3.2 LACP

Click **Switching** > **Trunk** > **LACP** to display the screen shown next.

LACP: Link Aggregation Control Protocol.

Note: Do not configure this screen unless you want to enable dynamic link aggregation.

LACP

LACP Setting

LACP Enable	🔿 Enable 💿 Disable
System Priority	32768 (0-65535)

Apply

- LACP Information

LABEL	DESCRIPTION
LACP Enable	Select Enable from the drop down box to enable Link Aggregation
	Control Protocol (LACP). Select Disable to not to use LACP.
System Priority	LACP system priority is a number between 0 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Apply	Click Apply to save your changes to the Switch.

3.3.4 VLAN

Each VLAN in a network has a associated VLAN ID, which displays in the IEEE 802.1Q tag in the L2 header of packets transmitted on a VLAN.

3.3.4.1 VLAN Setting

This page allow user to add, edit or delete VLAN settings.

Click **Switching** > **VLAN** > **VLAN Setting** to access this screen below to configure and view VLAN parameters for the switch.

LAN ID	VLAN Name	Untagged Ports Select	Tagged Ports Select	
(1-4094)		Select Untagged Ports 🔹	Select Tagged Ports 🔹	
/LAN Status				
/LAN Status	1			
LAN Status [VLAN ID	1 VLAN Name	Untagged Ports	Tagged Ports	Modify

LABEL	DESCRIPTION
VLAN ID	A unique number (between 1 and 4094) that identifies a particular VLAN.
VLAN Name	A 32-character alphanumeric name associated with a VLAN ID. The VLAN
	Name is intended to make user-defined VLANs easier to identify and remember.
Untagged	Select Untagged to make the port a permanent member of this VLAN
Ports Select	group. All outgoing frames will be transmitted without a VLAN Group ID
	tag.
Tagged Ports	Select Tagged to make the port a permanent member of this VLAN group.
Select	All outgoing frames will be transmitted with the VLAN Group ID tag.
Add	Click Add to save your changes to the Switch.
VLAN ID	This field displays the unique identification number of the VLAN group.
VLAN Name	This field displays the descriptive name for this VLAN group.
Untagged	This field displays all the ports that will transmit outgoing frames without a
Ports	VLAN group ID tag.
Tagged Ports	This field displays all the ports that will transmit outgoing frames with a
	VLAN group ID tag.
Modify	Click Edit to modify the tagged and untagged ports.
3.3.4.2 VLAN Port Setting

This page allow user to configure VLAN port related settings.

Click Switching > VLAN > VLAN Port Setting to access the screen below.

A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.

VLAN Port Setting

VLAN Port settings

Port Select	PVID	Accepted Type
Select Ports 👻	1 (1 - 4094)	⊙All ○Tag Only ○Untag Only

Apply

- Port VLAN Status

Port	PVID	Accept Frame Type
Port 01	1	ALL
Port 02	1	ALL
Port 03	1	ALL
Port 04	1	ALL
Port 05	1	ALL
Port 06	1	ALL
Port 07	1	ALL
Port 08	1	ALL
Port 09	1	ALL
Port 10	1	ALL
Port 11	1	ALL

LABEL	DESCRIPTION
Port Select	Select the ports to change the PVID for.
PVID	Enter a number between 1 and 4094 as the port VLAN ID (PVID).
Accepted Type	 Select the accepted type of the VLAN port: All: Accept tagged and untagged frames. Tag only: Only accept tagged frame. Untag only: Only accept untagged frame.
Apply	Click Apply to save your changes to the switch.
Port	This field displays the port number.
PVID	This field displays the port VLAN ID (PVID).

Accepted Frame	This field displays the accepted frame type of the VLAN port.
Туре	

3.3.4.3 VLAN Port Mode Setting

This page allow user to configure VLAN port tag mode setting.

Click Switching > VLAN > VLAN Port Mode Setting to access the screen below.

VLAN Port Mode Setting

VLAN Port Mode Settings

Port Select	Tag Mode
Select Ports 🔹	⊙Original ○Keep-Format ○Priority-Tag

Apply

Port	Tag Mode	
Port 01	Original	
Port 02	Original	
Port 03	Original	
Port 04	Original	
Port 05	Original	
Port 06	Original	
Port 07	Original	
Port 08	Original	
Port 09	Original	

LABEL	DESCRIPTION
Port Select	Select the ports to change this settings for.
Tag Mode	 Port tag mode: Original: Tag depends on VLAN settings. Keep-Format: Keep tag as packet received. Priority-Tag: Always append priority-tag on packet.
Apply	Click Apply to save your changes to the switch.
Port	This field displays the port number.
Tag Mode	It displays the tag mode you have choosed.

3.3.4.4 VLAN Ingress Filter

This page allow user to configure VLAN ingress filter setting.

Click Switching > VLAN > VLAN Ingress Filter to access the screen below.

VLAN In	gress Filter Setting	
VLAN ingress	filter settings	
State	⊙Enabled ○Disabled	

Apply

VLAN Ingress Filter Informatio	n	
Information Name	Information Value	
VLAN Ingress Filter	Enabled	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
State	Select Enabled from the drop down box to enable VLAN Ingress Filter. Select Disabled to not to use VLAN Ingress Filter.
Apply	Click Apply to save your changes to the switch.

3.3.5 SVLAN

3.3.5.1 SVLAN Setting

This page allow user to configure VLAN stacking tag protocol identifier.

Click Switching->SVLAN->SVLAN Setting to access the screen below.

SVLAN Setting

SVLAN TPID Setting

Apply

SVLAN Informations		
Information Name	Information Value	
TPID	0x0	

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
TPID	VLAN stacking tag protocol identifier (0x0000~0xFFFF).	
Apply	Click Apply to save your changes to the switch.	

3.3.5.2 SVLAN Member Setting

This page allow user to configure VLAN stacking members.

Click Switching->SVLAN->SVLAN Member Setting to access the screen below.

SVLAN Setting



LABEL	DESCRIPTION
SVLAN ID	Stacking VLAN ID.
Member Port	Select one or multiple ports as member ports of the SVLAN.
Add	Click Add to add any member port into the SVLAN.

3.3.5.3 SVLAN PVID Setting

This page allow user to add or set port VLAN stacking entry in the VLAN stacking table.

Click Switching->SVLAN->SVLAN PVID Setting to access the screen below.

SVLAN PVID Setting

SVLAN PVID settings

Port		PVID	
Select Ports 👻	1	(1 - 4094)	

Apply

Port 01	1	
Port 02	1	
Port 03	1	
Port 04	1	
Port 05	1	

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
Port	Select the port(s) to configure the SVLAN PVID settings for.	
PVID Set VLAN ID for selected ports.		
Apply	Click Apply to save your changes to the switch.	

3.3.5.4 SVLAN Service Port

This page allow user to configure VLAN stacking-aware ports.

Click Switching->SVLAN->SVLAN Service Port to access the screen below.

SVLAN Service Port Setting

SVLAN Service Port settings

Port	Enabled	
Select Ports 🔹	⊙Enabled ○Disabled	

Apply

- SVLAN Service Port Status

Port	State	
Port 01	Disabled	
Port 02	Disabled	
Port 03	Disabled	
Port 04	Disabled	
Port 05	Disabled	
Port 06	Disabled	
Port 07	Disabled	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the port(s) to configure this settings for.
Enabled	 Set VLAN stacking aware state: Enabled: Set as VLAN stacking aware. Disabled: Set as VLAN stacking unaware.
Apply	Click Apply to save your changes to the switch.

3.3.6 Bandwidth Control

3.3.6.1 Preamble Setting

Click **Switching** > **Bandwidth Control**->**Preamble Setting** in the navigation panel to bring up the screen as shown next.

Preamble Setting

	Bandwidth Control Preamble Setting		
Ingress Preamble & IFG		Egress Preamble & IFG	
	⊙Excluded ○Included	⊙Excluded ○Included	

Apply

-	Prea	ımbl	e St	atus

Information Name	Information Value	
Ingress Preamble & IFG	Excluded	
Egress Preamble & IFG	Excluded	

The following table describes the labels in this screen.

LABEL	DESCRIPTION		
Ingress Preamble	Select the mode of ingress preamble & IFG:		
& IFG	 Excluded: exclude preamble & IFG (20 bytes) when count ingress bandwidth rate. 		
	 Included: include preamble & IFG (20 bytes) when count ingress bandwidth rate. 		
Egress Preamble	Select the mode of egress preamble & IFG:		
& IFG	 Excluded: exclude preamble & IFG (20 bytes) when count egress bandwidth rate. 		
	 Included: include preamble & IFG (20 bytes) when count egress bandwidth rate. 		
Apply	Click Apply to save your changes to the switch.		

3.3.6.2 Port Rate Setting

Click **Switching** > **Bandwidth Control**-> **Port Rate Setting** in the navigation panel to bring up the screen as shown next.

Port Rate Setting

Port Rate Settings

Port	Туре	State	Rate(Kbit/sec)
Select Ports 👻	⊙Ingress ○Egress	⊙Disabled ○Enabled	Unlimited (0-1048544, must be a multiple of 16)

Apply

🝷 Port Rate Status

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 01	Unlimited	Unlimited
Port 02	Unlimited	Unlimited
Port 03	Unlimited	Unlimited
Port 04	Unlimited	Unlimited
Port 05	Unlimited	Unlimited
Port 06	Unlimited	Unlimited
Port 07	Unlimited	Unlimited
Port 08	Unlimited	Unlimited
Port 09	Unlimited	Unlimited
Port 10	Unlimited	Unlimited

LABEL	DESCRIPTION
Port	Select the ports to enable bandwidth control on.
Туре	Select the type of traffic to control, Ingress (incoming) or Egress (outgoing).
State	Select Enable to activate bandwidth control on the selected ports. Select Disable to turn off bandwidth control on the selected ports.
Rate (Kbit/sec)	Configure the desired bandwidth available to the port's traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is dropped. Specify the bandwidth in kilobit per second (Kbps). Enter a number between 0 and 1048544. The number must be a multiple of 16.
Apply	Click Apply to save your changes to the switch.
Port	This field displays the port number.
Ingress Rate (Kbit/sec)	This field displays the maximum bandwidth allowed for incoming traffic on the port in kilobits per second (Kbps). The default setting is Unlimited .
Egress Rate (Kbit/sec)	This field displays the maximum bandwidth allowed for outgoing traffic on the port in kilobits per second (Kbps). The default setting is Unlimited .

3.3.7 IGMP Snooping

Use the Switching pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

3.3.7.1 IGMP Setting

Click Switching > IGMP Snooping > IGMP Setting to access the screen below.

IGMP Setting

IGMP	Global	Setting

IGMP Snooping	⊙Disable ○Enable
Fastleave	⊙Disable ○Enable
Unknown Multicast Action	⊙Drop ○Flood
Query Interval	125 (60-600 Sec)
Response Time	10 (10-25 Sec)
Router Timeout	125 (60-600 Sec)
Last Member Query Interval	1 (1-25 Sec)
Robustness Variable	2 (1-255)

Apply

IGMP Informations

Information Name	Information Value	
IGMP Snooping	Disabled	
Fastleave	Disabled	
Unknown Multicast Action	Drop	
Query Interval	125 Secs	
Response Time	10 Secs	
Last Member Query Interval	1 Secs	
Robustness Variable	2 Secs	
Host Timeout	260 Sec	
Querier Election Time	255 Sec	

LABEL	DESCRIPTION
IGMP Snooping	Select Enable from the drop down box to enable IGMP Snooping. Select Disable to not to use IGMP Snooping. When enabled, it simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
Fastleave	Select Enable from the drop down box to enable IGMP Fast-Leave. Select Disable to not to use IGMP Fast-Leave.
Unknown Multicast Action	Unknown multicast message to the switch. Enable Drop will throw away the unknown multicast message. Enable Flood will flood the packets.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). You can also click the scroll arrows to select a new setting. The default query interval is 125 seconds.
Response Time	The time a generic system or functional unit takes to react to a given input. The default value is 10s.
Router Timeout	Save the time of the router port timer in the form. The default value is 125s.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queriers when it receives a Leave Group message for a group.
Robustness Variable	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Apply	Click Apply to save your changes to the switch.
Host Timeout	Save the timer related the host and its member. The default value is 260s.
Querier Election Time	It displays the querier election time.

3.3.7.2 IGMP VLAN Setting

Click Switching > IGMP Snooping > IGMP VLAN Setting to access the screen below.

IGMP Snooping VLAN Setting

IGMP Vlan Setting

VLAN ID	Snooping State	Querier State
Select VLANs 👻	⊙Disable ○Enable	⊙Disable ○Enable

Apply

VLAN ID	Snooping State	Querier State	Querier Status	Querier IP
1	Enabled	Disabled	Non-Querier	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
VLAN ID	Select the VLANs to configure.
Snooping State	Select Enable from the drop down box to enable IGMP. Select Disable to not to use IGMP.
Querier State	Select Enable from the drop down box to enable IGMP Querier Election. Select Disable to not to use IGMP Querier Election.
Apply	Click Apply to save your changes to the switch.
Querier Status	It displays the status of querier.
Querier IP	It shows the Querier IP of IGMP VLAN.

3.3.7.3 Multicast Database

Click Switching > IGMP Snooping > Multicast Database to access the screen below.

Multicast Database

	a second	and the second second second second	and the second second
--	----------	-------------------------------------	-----------------------

LABEL	DESCRIPTION
DIP Address	This field displays IP address of this group.
VID	This field displays ID of configured VLAN (1~4094).
Member Port	This field displays the ports that selected in the group address.
Life(Sec)	This field displays the life time of this group.

3.3.7.4 Router Table

Click Switching > IGMP Snooping > Router Table to access the screen below.

Router Table				
Router Ta	ıble			

The following table describes the labels in this screen.

LABEL	DESCRIPTION
VID	The VLAN ID that has router port.
Port	Router port (i.e. the port ID where IGMP Query message received).
Expiry Time(Sec)	This field displays the expiry time of the router port.

3.3.8 Jumbo Frame

This page allow user to configure switch port jumbo frame settings.

Click **Switching** > **Jumbo Frame** in the navigation panel to bring up the screen as shown next.

Jumbo Frame			
Jumbo Frame Setting			
Jumbo Frame (Bytes)	⊙1522 Bytes ◯1536 Bytes ◯1552 Bytes	○9216 Bytes	
Apply			
→ Jumbo Frame Informa	tion		
Information Name		Information Value	
Jumbo Frame		1522 Bytes	

LABEL	DESCRIPTION
Jumbo Frame (Bytes)	Specify the maximum Jumbo Frame size in bytes from 0~9216 .
Apply	Click Apply to save any changes to the switch.

3.3.9 STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

3.3.9.1 STP Global Setting

Use the SPT Global Setting screen to activate one of the STP modes on the switch.

Click Switching > STP > STP Global Setting.

STP Global Setting

Global Settings

Enabled	⊙Enabled ○Disabled
Force Version	STP-Compatible
Max Hops	20 (1-40)
Forward Delay	15 (4-30)
Max Age	20 (6-40)
Tx Hold Count	6 (1-10)
Hello Time	2 (1-10)

Apply

STP Informations

Information Name	Information Value	
STP	Enabled	
Force Version	STP-Compatible	
Max Hops	20	
Forward Delay	15	
Max Age	20	
Tx Hold Count	6	
Hello Time	2	

LABEL	DESCRIPTION
Enabled	Select Enabled to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). Select Disabled to not use STP or RSTP.
Force Version	 Select the operating mode of STP. STP-Compatible: 802.1D STP operation. RSTP-Operation: 802.1w operation. MSTP-Operation: 802.1s operation.
Max Hops	Set the value of the maximum number of hops in the region. Enter a number between 1 and 40 as the max hops.
Forward Delay	Set the delay time an interface takes to coverage from blocking state to forwarding state. This is the maximum time (in seconds) the switch will wait before changing states. This delay is required because every switch 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 blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

	As a general rule: Note: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Max Age	Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.
Tx Hold Count	Set the Transmit Hold Count used to limit BPDU transmission rate. Enter a number between 1 and 10 as the Tx hold count.
Hello Time	Set the interval between periodic transmissions of BPDU by Designated Ports. This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forward Delay.
Apply	Click Apply to save your changes to the switch.

3.3.9.2 STP Port Setting

Click Switching > STP > STP Port Setting.

STP Port Setting

STP Port Configuration

Port Select	External Cost (0 = Auto)	Edge Port	BPDU Filter	BPDU Guard	P2P MAC	Migrate
Select Ports 👻	0	Auto	No	No	Auto	

Apply

Port	External Cost Conf/Oper	Edge Port Conf/Oper	BPDU Filter	BPDU Guard	P2P MAC Conf/Oper
Port 01	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 02	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 03	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 04	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 05	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 06	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 07	0/ 0	Auto/Yes	No	No	Auto/Yes
Port 08	0/ 20000	Auto/Yes	No	No	Auto/Yes
Port 09	0/ 0	Auto/Yes	No	No	Auto/Yes

LABEL	DESCRIPTION
Port Select	Select the port(s) to change spanning tree protocol settings for.
External	Path cost is the cost of transmitting a frame on to a LAN through that port. It is

Cost	recommended to assign this value according to the speed of the bridge. The		
	slower the media, the higher the cost. Entering 0 means the switch will		
	automatically assign a value.		
	Set the edge port configuration:		
Edge Port	• No: Force to false state (as link to a bridge).		
	Yes: Force to true state (as link to a host).		
	Auto: Auto detect.		
	Set the BPDU Filter configuration:		
	No: Disable BPDU Filter function.		
DF DO TIILEI	Yes: Enable BPDU Filter function.		
	To avoid transmitting BPDU from the specified ports		
	Set the BPDU Guard configuration:		
BPDU	No: Disable BPDU Guard function.		
Guard	Yes: Enable BPDU Guard function.		
	To drop directly the received BPDU from the specified ports		
	Set the Point-to-Point port configuration:		
	• No: Force to false state.		
PZP WAC	Yes: Force to true state.		
	Auto: Auto detect (according to duplex).		
	Click the square choice box to enable this function.		
Misseta	Force to try to use the new MST/RST BPDUs, and hence to test the		
wigrate	hypothesis that all legacy systems that do not understand the new BPDU		
	formats have been removed from the LAN segment on the port(s).		
Apply	Click Apply to save your changes to the switch.		

3.3.9.3 MST Configuration

MST is the acronym of Minimum Spanning Tree.

Click Switching > STP > MST Configuration.

MST Configuarion

onfiguration Name		
nfiguration Revision	0	
pply		
nce ID Settings		
MSTI ID (1-15)		
Action Type	Add VID	
VLAN List (1-4094)		
nnly		
(1997) (1997)		
ST Instance Configura	ation	
ICTI	NI AN L	VI AN Court
1511	VLAN LIST	VLAN Count
O.T. (O)	1 4004	1001

LABEL	DESCRIPTION		
Configuration Name	You can manually set the configuration name for identification.		
Configuration Revision	You can manually set the configuration revision for identification. (Range: 0-65535)		
Apply	Click Apply to save your changes to the switch.		
MSTI ID	MSTI is MST Configuration ID. Enter a number between 1 and 15 as the MSTI ID.		
Action Type	 Select the action type: Add VID: Add the VLANs in VLAN list to the specified MST instance. Remove VID: Remove the VLANs in VLAN list from the specified MST instance. 		
VLAN List	Enter a number between 1 and 4094 as the VLAN List		
MSTI	It displays the CIST's number.		
VLAN List	It displays the list of VLAN.		
VLAN Count	It displays the count number of VLAN.		

3.3.9.4 MST Instance Setting

Click Switching > STP > MST Instance Setting.

MST Instance Setting

MST Priority Settings			
MST ID Priority			
	32768		

Apply

AST Insta	nce Information		
MSTI	Instance Status	Instance Priority	View Status
CIST (O)	Enabled	32768 (Bridge Priority: 32768, SYS ID Ext: 0)	View

The following table describes the labels in this screen.

LABEL	DESCRIPTION		
MST ID	You can manually set the MST ID to specify MST instance.		
Priority	You can manually set the Bridge Priority in the specified MST instance.		
Apply	Click Apply to save your changes to the switch.		
MSTI	It displays the CIST's number.		
Instance Status	It displays the status of MST instance.		
Instance Priority	It displays the priority of MST instance.		
View Status	Click View to view the status of MST instance.		

3.3.9.5 MST Port Setting

Click Switching > STP > MST Port Setting.

MST Port Setting

MST Port Configuration

Port Select	MST ID	Internal Path Cost (0 = Auto)	Priority	
Select Ports 👻		0	128 💌	

Apply

→ S	TP Po	rt Statu	5
	Port	мяті	Designated Bridge

Port	MSTI ID	Designated Bridge	Internal Path Cost Conf/Oper	Port Priority	Port Role	Port State
Port 01	0	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 02	O	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 03	0	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 04	0	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 05	0	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 06	0	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 07	O	0/00:00:00:00:00:00	0/ 0	128	Disabed	Disabled
Port 08	0	32768/DE:AD:BE:EF:01:02	0/ 20000	128	Designated	Forwarding

LABEL	DESCRIPTION		
Port Select	Select the port(s) which will use MST setting.		
MST ID	You can manually set the MST ID to specify MST instance.		
Internal Path Cost	You can manually set the internal path cost to the selected ports in the specified MST instance. (0 means "Auto")		
Priority	You can manually set the priority to the selected ports in the specified MST instance.		
Apply	Click Apply to save your changes to the switch.		
Port	It displays the port which you have choosed.		
MSTI ID	It displays the MSTI ID of the choosed port.		
Designed Bridge	It displays the designed bridge of the choosed port.		

Internal Path CostIt displays the internal path cost of the choosed port.	
Port Priority	It displays the port priority you have set.
Port Role It displays the port role of the choosed port.	
Port State It displays the port state of the choosed port.	

3.4 Security

3.4.1 Storm Control

Storm Control

Storm Control Setting					
Port	Storm Type	State	Rate (pps)		
Select Ports 👻	Broadcast 💌	⊙Off ◯On	Unlimited (0-1000000)		

Apply

Storm Control Information					
Port	Broadcast (pps)	Multicast (pps)	Unknown Unicast (pps)	Unknown Multicast (pps)	
Port 01	Off	Off	Off	Off	
Port 02	Off	Off	Off	Off	
Port 03	Off	Off	Off	Off	
Port 04	Off	Off	Off	Off	
Port 05	Off	Off	Off	Off	
Port 06	Off	Off	Off	Off	
Port 07	Off	Off	Off	Off	
Port 08	Off	Off	Off	Off	
Port 09	Off	Off	Off	Off	
Port 10	Off	Off	Off	Off	

LABEL	DESCRIPTION
Port	Select the port(s) which will use storm control.
Storm Type	 Select the type of packets to be limited with the Storm Control feature. Broadcast: Broadcast packet Multicast: All multicast packet, include known and unknown multicast., Unknown Unicast: Unknown unicast packet. Unknown Multicast: Unknown multicast packet.
State	Select On to enable traffic storm control on the Switch. Select Off to disable this feature.
Rate (pps)	Type a packet per second (pps) rate between 0 and 1000000. This is the maximum amount of packets of the type selected previously that are allowed to be transferred to the Switch per second. Any subsequent packets are discarded.

Apply	Click Apply to save your changes to the Switch.
Port	This field displays the port number.
Broadcast (pps)	This field displays how many broadcast packets can the port receive per second.
Multicast (pps)	This field displays how many multicast packets can the port receive per second.
Unknown Unicast (pps)	This field displays how many unknown unicast packets can the port receive per second.
Unknown Multicast (pps)	This field displays how many unknown multicast packets can the port receive per second.

3.4.2 MAC Filtering

Use this screen to create rules for traffic going through the switch.

Click **Security**> **MAC Filtering** in the navigation panel to display the screen as shown.

MAC Filtering

MAC Filtering Setting

00:00:00:00 Add	Add Static MAC Status	MAC Address	VLAN	Filter	Name	
Add Static MAC Status	Add Static MAC Status	00:00:00:00:00	default 🖌 🗸	Source MAC 🛛 🗸		
		Add				

LABEL	DESCRIPTION
MAC Address	Type a MAC address to which packets will be filtered in valid MAC address format, that is, six hexadecimal character pairs. And this must be a unicast MAC address.
VLAN	The VLAN ID number of the VLAN on which the above MAC address resides This function is set default in this switch.
Filter	Select Source MAC to drop the frames with the source MAC address (specified in the MAC Address field). Select Destination MAC to drop the frames with the destination MAC address (specified in the MAC Address field). Select Both to drop frames with the source MAC address and destination MAC address which specified in the MAC Address field.

Web Smart Switch

Name	Type a descriptive name (up to 32 printable ASCII characters) for this filtering rule. This is for identification only.
Add	Click Add to add any port into the MAC filtering table.
No.	This is the index number for the MAC filtering rules.
MAC Address	This field displays the MAC address that will be filtered.
VLAN	This is the VLAN group to which the MAC address belongs.
Filter	This field displays the action of the filter.
Name	This field displays the descriptive name for this rule. This is for
	identification purpose only.
Select	Click on the checkbox for the MAC filtering rule you want to delete.

3.4.3 802.1X

3.4.3.1 802.1X Setting

Use this screen to activate IEEE 802.1x security and configure RADIUS server settings.

Click **Security** > **802.1x** > **802.1x** Setting to display the configuration screen as shown

802.1x Setting

802.1x Setting

802.1X	💿 Disable 🔿 Enable
Radius Server IP	192.168.1.99
Server Port (1024-65535)	1812
Shared Key (max. 30 characters)	****
Retype Shared Key	****
Reauthentication Enable	🔿 Disable 💿 Enable
Reauthentication Period (30~65535 sec)	3600

Apply

- 802.1x Informations

Information Name	Information Value	
802.1X	Disabled	
Radius Server IP	192.168.1.99	
Server Port	1812	
Reauthentication Enable	Enabled	
Reauthentication Period	3600	

LABEL	DESCRIPTION
802.1X	Select Enable from the drop-down list box to activate IEEE 802.1x port authentication. Select Disable to disable this function.
Radius Server IP	Enter the IP address of an external RADIUS server in dotted decimal notation.
Server Port (1024-65535)	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Key (max. 30 characters)	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Retype Shared Key	Retype the key specified above to ensure it has been entered correctly.
Reauthentication enable	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port. Select Enable means the user has to re-enter his/her username and

	password.
Reauthentication	Specify how often a client has to re-enter his or her username and
Period	password to stay connected to the port.
(30-65535 sec)	Set the reauthentication period of 802.1X if reauthentication is enabled.
Apply	Click Apply to save your changes to the switch.

3.4.3.2 802.1X Port Setting

Click **Security** > 802.1x > 802.1x Port Setting to display the configuration screen as shown.

802.1x Port Setting

802.1x Port Setting



Apply

D	Mar die Volume	Cardina (mark)	
Pon	Mode (pps)	Status (pps)	
Port 01	802.1X Disabled	-	
Port 02	802.1X Disabled		
Port 03	802.1X Disabled		
Port 04	802.1X Disabled	-	
Port 05	802.1X Disabled	2	
Port 06	802.1X Disabled	-	
Port 07	802 1X Disabled	-	

LABEL	DESCRIPTION	
Port	Specify the ports to activate IEEE 802.1x port authentication on.	
Mode	Select Force Unauthorized to always force this port to be unauthorized. Select Force Authorized to always force this port to be authorized. Select Authorization to enable 802.1x port authentication. Select No Authorization to disable 802.1x port authentication.	
Apply	Click Apply to save your changes to the Switch.	
Port	This field displays the port number.	
Mode	This field displays the port's current 802.1x setting.	
Status	This field displays the current stage of the 802.1x port authentication procedure.	

3.4.4 Port Security

Click **Security** > **Port Security** to display the configuration screen as shown.

Port Security

Port Security Settings

Port Select	Security	Max L2 Entry
Select Ports 🔹 👻	©Enabled ⊙Disabled	Unlimited

Apply

Port Name	Enable State	L2 Entry Num	Action
Port 01	Disabled	Unlimited	forward
Port 02	Disabled	Unlimited	forward
Port 03	Disabled	Unlimited	forward
Port 04	Disabled	Unlimited	forward
Port 05	Disabled	Unlimited	forward
Port 06	Disabled	Unlimited	forward
Port 07	Disabled	Unlimited	forward
Port 08	Disabled	Unlimited	forward

LABEL	DESCRIPTION
Port Select	Select the port(s) to configure this setting
Security	 Port security function. It constraint how many MAC addresses can be learned by a port and drop new one when reach the limitation. Enable: Enable port security function. Disable: Disable port security function.
Max L2 Entry	Maximum number of Layer 2 entries that assign the MAC address to the port.
Apply	Click Apply to save your changes to the Switch.
Port Name	This field displays the port number.
Enable State	This field displays the state of this function whether it has been enabled or not.
L2 Entry Num	This field displays the status of maximum number of Layer 2 entries of the MAC addresses.
Action	This field displays the action of the port.

3.4.5 Protected Ports

This page allow user to configure protected port setting to prevent the selected ports from communicate with each other.

Click **Security** > **Protected Ports** to display the configuration screen as shown.

Protected Ports

Protected Ports Settings

Port List	Port Type
Select Protected Ports 🔹	⊙Unprotected ○Protected

Apply

Protected Type	Port List
Protected Ports	
Unprotected Ports	all

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port List	To select the port to be protected.
Port Type	 Configure port protect type: Unprotected: Unprotected port can communicate with all ports. Protected: Prevent protected ports from communicate with each other.
Apply	Click Apply to save your changes to the Switch.

3.4.6 Access

3.4.6.1 Console

Console Settings			
Console Settings			
Session Timeout	15 (0-1440) minu	tes	
Apply			
- Console Information			
Information Name		Information Va	lue
Session Timeout		15	

LABEL	DESCRIPTION
Session Timeout	Set session timeout minutes for user access CLI from console line. If user doesn't response after session timeout minute, CLI will logout automatically. Enter a number between 0 and 1440 as the session timeout. 0 minutes means never timeout.
Apply	Click Apply to save your changes to the Switch.

3.4.6.2 Telnet

Telnet is the TCP/IP standard protocol for remote terminal service. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's keyboard and display connected directly to the remote machine.

Settings	
ession Timeout 10 (0-1440) minutes
lγ	
net Information	
ormation Name	Information Value

LABEL	DESCRIPTION
Session Timeout	Set session timeout minutes for user access CLI from telnet line. If user doesn't response after session timeout minute, CLI will logout automatically. Enter a number between 0 and 1440 as the session timeout. 0 minutes means never timeout.
Apply	Click Apply to save your changes to the Switch.

3.4.6.3 SSH

SSH is the acronym of Secure Shell.

SSH Settings

SSH Settings
Session Timeout
10 (0-1440) minutes

Apply

SSH Information		
Information Name	Information Value	
Session Timeout	10	

LABEL	DESCRIPTION
Session Timeout	Set session timeout minutes for user access CLI from SSH line. If user doesn't response after session timeout minute, CLI will logout automatically. Enter a number between 0 and 1440 as the session timeout. 0 minutes means never timeout.
Apply	Click Apply to save your changes to the Switch.

3.4.6.4 HTTP

HTTP is the acronym of Hyper Text Transfer Protocol.

P Settings			
Session Timeout	15 (0-1440) minut	es	
and			
аррту			
ITTP Information			
Information Name		Information Value	
ант		4.5	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Session Timeout	Set session timeout minutes for user access WEB from HTTP protocol. If user doesn't response after session timeout minute, WEB UI will logout automatically. Enter a number between 0 and 1440 as the session timeout. 0 minutes means never timeout.
Apply	Click Apply to save your changes to the Switch.

3.4.6.5 HTTPS

HTTPS is the acronym of Hypertext Transfer Protocol over Secure Socket Layer.

HTTPS Settings HTTPS Settings Session Timeout 15 (0-1440) minutes Apply • HTTPS Information Information Name Information Value Session Timeout 15

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Session Timeout	Set session timeout minutes for user access WEB from HTTPS protocol. If user doesn't response after session timeout minute, WEB UI will logout automatically. Enter a number between 0 and 1440 as the session timeout. 0 minutes means never timeout.
Apply	Click Apply to save your changes to the Switch.

3.5 ACL

Use the ACL pages to configure settings for the Access Control List.

3.5.1 ACL Setting

ACL Setting								
ACL Set	ting					_		
ACLI	ndex	1			Add			
Index	Name	Port List	VLAN List	Policy Index	Modify	Delete		

LABEL	DESCRIPTION
ACL Index	You can manually set the ACL Index.
Add	Click Add to add the basic information of ACL Index.
Index	It displays the index information.
Name	It displays the name of the index.
Port List	It displays the list of the port.
VLAN List	It displays the list of the VLAN.
Policy Index	It displays the policy index.
Modify	Click Modify to modify any setting.
Delete	Click Delete to delete any setting.

Click **ACL->ACL Setting->Add** button, the ACL Content web page pops out.

ACL Content

ACL Content

Index	1	
Name		
Comment		

Apply

ACL Binding

		P	ort list				
		VI	AN list				
	Policy index						
	4	4					
Interface	Port nu	mber 🗸 📔			B	ind	Unbind
ACE Setti	a d						
ACE Settii	ng						
ACE Settii ACE Ind	ng dex	1					Add
ACE Settii ACE Ind	ng dex	1					Add
ACE Settin ACE Inc	ng dex	1					Add
ACE Settii	ng dex	1					Add
ACE Settii ACE Ind ACE Index	ng dex Co	1 mment	Action	Modify	Delete		Add
ACE Settii ACE Ind ACE Index	ng dex Co	1 mment	Action	Modify	Delete		Add

Name	Enter ACL name in this field
Comment	Enter ACL comment in this field.
Interface	Select the interface to bind:
	Port number: Enter port number.
	VLAN ID: Enter VLAN ID.
	Policy: Enter policy index.
ACE Index	Enter ACE index in this field to configure ACE.

Click ACL->ACL Setting->Add->Add (in ACE Setting) button, the ACE Content web page pops out.

ACE Content

ACL Index	1	
ACE Index	1	
Comment		
src-mac	00:00:00:00:00:00	mask 00:00:00:00:00
dst-mac	00:00:00:00:00:00	mask 00:00:00:00:00
ethertype	0	
src-ip	0.0.0.0	mask 0.0.0.0
dst-ip	0.0.0.0	mask 0.0.0.0
ip-protocol	0	
tos	0	
l4-src-port	0	
l4-dst-port	0	
tcp-flag	0	
Action	Permit 🐱	

Apply

LABEL	DESCRIPTION
Comment	Enter ACE comment in this field.
src-mac	Enter source MAC data and mask in this field.
dst-mac	Enter destination MAC data and mask in this field.
ethertype	Enter ethernet type in this field.
src-ip	Enter source IP data and mask in this field.
dst-ip	Enter destination IP data and mask in this field.
ip-protocol	Enter IP protocol in this field.

tos	Enter ToS in this field.
14-src-port	Enter Layer 4 source port in this field.
14-dst-port	Enter Layer 4 destination port in this field.
tcp-flag	Enter TCP flag in this field.
Action	Select the action to take:
	 Permit: permit packet to pass through.
	Deny: drop packet.
	Note: system will automatically add one "deny any any" rule in the last
	rule of this ACL.

3.5.2 ACL Template Setting

ACL	Templ	ate S	etting
			· · · · · · · · · · · · · · · · · · ·

Temp	ate	Setting	
remp	are	Setting	

Template Index	1 🗸	Get	
Template Field			
src-mac			
dst-mac			
ethertype			
src-ip			
dst-ip			
ip-protocol			
tos			
l4-src-port			
l4-dst-port			
tcp-flag			

Apply

LABEL	DESCRIPTION
Template Index	You can choose the template index.
Get	To get the basic information of the policy index.
src-mac	Click in the square box to set source MAC into Template.
dst-mac	Click in the square box to set destination MAC into Template.
ethertype	Click in the square box to set ethernet type into Template.
src-ip	Click in the square box to set source IP into Template.
dst-ip	Click in the square box to set destination IP into Template.
ip-protocol	Click in the square box to set IP protocol into Template.
tos	Click in the square box to set ToS into Template.

14-src-port	Click in the square box to set Layer 4 source port into Template.
14-dst-port	Click in the square box to set Layer 4 destination port into Template.
tcp-flag	Click in the square box to set TCP flag into Template.
Apply	Click Apply to save your changes to the switch.

3.5.3 ACL Index Range Setting

ACL Index Range Setting

ACL Index Range Setting

ACL Index Range	Template Index(1-16)
1-1000	1
1001-2000	2
2001-3000	3
3001-4000	4
4001-5000	0
5001-6000	0
6001-7000	0
7001-8000	0
8001-9000	0
9001-10000	0
10001-11000	0
11001-12000	0
12001-13000	0
13001-14000	0
14001-15000	0
15001-16000	0

Apply

LABEL	DESCRIPTION
ACL Index Range	It displays the 16 types of ACL index range.
Template Index	Enter Template index mapping to specify range of ACL index in this field. Enter a number between 1 and 16 as the template index.

3.5.4 ACL Policy Setting

ACL Policy Setting				
Policy Setting				
Policy Index 1 🐱			Get	
olicy Content	P			
VLAN ID(1-4094)				
Port Number				
Action	Mirror in	ıdex	*	0
Apply				

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Policy Index	You can choose the policy index.
Get	To get the basic information of the policy index.
VLAN ID	Enter VLAN ID and check it to care specified VLAN ID.
Port Number	Enter port number and check it to care specified port number.
Action	 Select the action to take: Mirror Index: mirror packet via the configuration of specified mirror index. Rate Limit: limit packet rate, the unit is 16kbps. Priority: change packet priority.
Apply	Click Apply to save your changes to the switch.

3.6 QoS

Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

3.6.1 Port-based Priority

You can configure the switch to assign an IEEE 802.1p priority to packets based on the ingress (incoming) port of the packet.

Click **QoS > Port-based Priority** in the navigation panel to display the screen as shown below.

Port-based Priority

Port-based Priority Setting

Port	Priority (0-7)	
Select Ports 👻	0	

Apply

- Port Based Priority Status

Port	Priority	
Port 01	0	
Port 02	0	
Port 03	0	
Port 04	0	
Port 05	0	
Port 06	0	
Port 07	0	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the number of the port for which you want to assign IEEE 802.1p priority to incoming frames.
Priority	Select the QoS port-based priority you want to assign to the packets coming into the switch on the ports specified in the port field.
Apply	Click Apply to save your changes to the switch.
Port	This field displays the port number.
Priority	This field indicates what IEEE 802.1p priority is assigned to the incoming packets from the port.

3.6.2 802.1 p- based Priority

Click **QoS > 802.1 p-based Priority** in the navigation panel to display the screen as shown below.
802.1p-based Priority

802.1p-based Priority Remapping Setting

802.1p	Priority (0-7)	
0 🗸	0	

Apply

802.1p	Priority	
0	1	
1	0	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
802.1 p	Select the 802.1p value to mapping to the priority and drop precedence. The 802.1p range is 0 to 7.	
Priority	Select the IEEE 802.1p priority you want to assign to the packets coming into the switch on the ports specified in the port field. The priority range is 0 to 7.	
Apply	Click Apply to save your changes to the switch.	
802.1 p	This field displays the 802.1p priority level which you've choosed	
Priority	This field indicates what IEEE 802.1p priority is assigned to the incoming packets from the port.	

3.6.3 DSCP - based Priority

You can configure the switch to assign an IEEE 802.1p priority to packets coming into the switch with DSCPs assigned to them.

Click **QoS** > **DSCP-based Priority** to display the screen as shown next.

DSCP-based Priority

OSCP-based Priority Rema	pping Setting
DSCP	Priority (0-7)
Select DSCP 🔹	0 🗸

Apply

DSCP-based Priority Remapping Status

DSCP	Priority	
0	0	
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
DSCP	Select the DSCP value to mapping to the priority and drop precedence. The DSCP range is 0 to 63.	
Priority	Select the priority value that the DSCP mapped to. The priority range is 0 to 7.	
Apply	Click Apply to save your changes to the switch.	
DSCP	This field displays the DSCP classification identification numbers.	
Priority	This field displays the DSCP classification identification number's IEEE 802.1p Priority.	

3.6.4 Priority to Queue Mapping

Click QoS > Priority to Queue Mapping to display the screen as shown next.

IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next screen to configure the priority level-to-physical queue mapping.

The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch,

traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Priority to Queue Mapping

Priority to Queue Mapping Setting

Priority	Queue ID (1-8)
0	1

Apply

•	Priority to Queue Mapping Status		
	Priority	Queue ID	
	0	1	
	1	2	
	2	3	
	3	4	

LABEL	DESCRIPTION	
Priority	Select the priority value to mapping to the Queue ID. The priority range is 0 to 7.	
0	Typically used for best-effort traffic.	
1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.	
2	This is for "spare bandwidth".	
3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.	
4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.	
5	Typically used for video that consumes high bandwidth and is sensitive to jitter.	
6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).	
7	Typically used for network control traffic such as router configuration messages.	
Queue ID	Select the Queue ID for which the Priority should be applied. The Queue ID range is 1 to 8.	
Apply	Click Apply to save your changes to the Switch.	
Priority	This field displays the priority for each Queue ID.	
Queue ID	This field displays the Queue ID.	

3.6.5 Packet Scheduling

Click **QoS** > **Packet Scheduling** to display the screen as shown next.

Packet Scheduling is used to help solve performance degradation when there is network congestion. Use this screen to configure queuing algorithms for outgoing traffic.

Packet	Scheduling	Algorithm
Tachet	Schedding	Algorithm

Per Port Setting	
Port	Scheduling Algorithm
Select Ports 🔹	⊖WFQ ⊙WRR

Apply

Packet Scheduling Algorithm Status		
Port	Scheduling Algorithm	
Port 01	WFQ	
Port 02	WFQ	
Port 03	WFQ	
Dort 04	WEO	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the number of the port for which you want to assign IEEE 802.1p priority to incoming frames.
Scheduling Algorithm	 Select the algorithm of packet scheduling: WFQ: Weighted Fair Queuing, octet-based egress scheduling method depend on queue weighted. WRR: Weighted Round Robin, packet-based egress scheduling method depend on queue weighted. Note: Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue weight field). Queues with smaller weights.
Apply	Click Apply to save your changes to the switch.

3.6.6 Queue Weight Setting

Click **QoS** > **Queue Weight Setting** to display the screen as shown next.

Queue Weight

Queue Weight Setting

Port	Queue ID	Weight
Select Ports 👻	Select Queue ID 👻	0 (0 - 127, 0: Strict)

Apply

- Queue Weight Information

Port	Q1 Weight	Q2 Weight	Q3 Weight	Q4 Weight	Q5 Weight	Q6 Weight	Q7 Weight	Q8 Weight
Port 01	1	2	3	4	5	6	7	8
Port 02	1	2	3	4	5	6	7	8

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the number of the port for which you want to assign IEEE 802.1p priority to incoming frames.
Queue ID	Select the Queue ID for configuration it's weighted. The Queue ID range is 1 to 8.
Weight	 Configure the queue scheduling weight of specified ports. Range is valid as following: 0: mean the queue is strict mode. 1~127: mean the queue weight of the scheduling.
Apply	Click Apply to save your changes to the switch.
Weight	This field displays the weight of the queue.

3.6.7 Queue Remarking Status

Click **QoS** > **Queue Remarking Status** to display the screen as shown next.

QoS Remarking Status

QoS Remarking	Status Setting
---------------	----------------

Port	802.1p Priority Remarking	DSCP Remarking
Select Ports 👻	⊙Enabled ⊙Disabled	⊙Enabled ⊙Disabled

Apply

- QoS Remarking Status

Port	802.1p Remarking	DSCP Remarking	
Port 01	Disabled	Disabled	
Port 02	Disabled	Disabled	
Port 03	Disabled	Disabled	
Port 04	Disabled	Disabled	
Port 05	Disabled	Disabled	
Port 06	Disabled	Disabled	
Port 07	Disabled	Disabled	
Port 08	Disabled	Disabled	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the number of the port for which you want to assign IEEE 802.1p priority to incoming frames.
802.1 p Priority Remarking	Click Enabled to enable this function in specified ports. Click Disabled to disable this function in specified ports.
DSCP Remarking	Click Enabled to enable this function in specified ports. Click Disabled to disable this function in specified ports.
Apply	Click Apply to save your changes to the switch.

3.6.8 Queue Remarking Table

Click **QoS** > **Queue Remarking Table** to display the screen as shown next.

QoS Remarking Table

QoS Remarking Table Setting

Priority	New 802.1p Priority (0-7)	New DSCP Value (0-63)
0	0	0

Apply

Priority	New 802.1p Priority (0-7)	New DSCP Value (0-63)
0	1	0
1	0	0
2	2	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Priority	Select the priority value to mapping to new 802.1p, new 802.1ad and DSCP value. The priority range is 0 to 7.
New 802.1 p Priority	Remark to the new 802.1p priority that the priority and drop precedence mapped to. The new 802.1p priority is 0 to 7.
New DSCP Value	Remark to the new DSCP priority that the priority and drop precedence mapped to. The new DSCP priority is 0 to 63.
Apply	Click Apply to save your changes to the switch.

3.7 Management

3.7.1 SNMP

3.7.1.1 SNMP Setting

Click Management > SNMP->SNMP Setting to display the screen as shown next.

SNMP Setting

State	💿 Disabled 🔘 Enabled		
Apply			
	1		
SNMP Inf	ormations		
		In foremention, Malue	
Informat	ion Name	Information value	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
State	SNMP daemon state: Select Enabled to activate SNMP daemon. Select Disabled to not use SNMP daemon.

3.7.1.2 SNMP Community

Click **Management > SNMP->SNMP Community** to display the screen as shown next.

SNMP Community

Community Setting

Community	Туре
] ③Read-Only ○Read-Write

Add

No.	Community	Access Type	Delete
1	public	read-only	Delete
2	private	read-write	Delete

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Community	Enter a Community string, this will act as a password for requests from the management station.
Туре	 SNMP community type: Read-Only: Read all objects only, it can allow the SNMP manager using this string to collect information from the switch. Read-Write: Read and write all objects, it can allow the SNMP manager using this string to create or edit MIBs (configure settings on the switch).
Add	Click Add to add any other community.
No	It displays the port number which in the community.
Community	This field displays the community strings.
Access Type	This field displays the community string's type. This will either be read-only or read-write.
Delete	Click Delete to remove any selected community strings.

3.7.1.3 SNMP Trap

This page allow user to add or delete SNMP trap receiver IP address and community name.

Click **Management** > **SNMP**->**SNMP Trap** to display the screen as shown next.

SNMP Trap

Trai	n R	ece	iver	Setting	
Πa	5 IX		ve	Setting	

IP Address	Community
Add	

No.	IP Address	Community Type	Delete

LABEL	DESCRIPTION
IP Address	Enter the IP addresses to send your SNMP traps to.
Community	Enter a Community string, which is the password sent with each trap to

	the SNMP manager.
Add	Click Add to add any trap receiver.
IP Address	This field displays the IP address where the traps from the switch are sent.
Community Type	This field displays the password which is sent with each trap to the SNMP manager.
Delete	Click Delete to remove any selected trap receiver entries.

3.8 Diagnostics

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

3.8.1 Ping Test

IP Address	192.168.1.100	(x.x.x.x)	
Count	1	(1 - 5 Default : 1)	
nterval (in sec)	1	(1 - 5 Default : 1)	
Size (in bytes)	0	(0-5120 Default:0)	
Ping Results			< >

LABEL	DESCRIPTION
IP Address	Enter the IP addresses of the test destination.
Count	It displays how many times to send ping request packet.

	Enter a number between 1 and 5 as the count and the default configuration is 1.
Interval	It displays time interval between each ping request packet.
	Enter a number between 1 and 5 as the interval and the default configuration is 1.
Size	It displays the size of ping packet.
	Enter a number between 0 and 5120 as the size and the default configuration is 0.
Ping Results	After ping finished, results will show in this field.
Apply	Click Apply to save your changes to the switch.

3.8.2 Ping6 Test

Ping Test

Ping test Settin	g
IPv6 Address	000000000
Count	1 (1 - 5 Default : 1)
Interval (in sec)	1 (1 - 5 Default : 1)
Size (in bytes)	0 (0-5120 Default:0)
Ping Results	
Apply	

LABEL	DESCRIPTION		
IPv6 Address	Enter the IPv6 addresses of the test destination.		
Count	It displays how many times to send ping request packet.		
	Enter a number between 1 and 5 as the count and the default configuration is 1.		
Interval	It displays time interval between each ping request packet.		
	Enter a number between 1 and 5 as the interval and the default configuration is 1.		

Size	It displays the size of ping packet.		
	Enter a number between 0 and 5120 as the size and the default configuration is 0.		
Ping Results	After ping finished, results will show in this field.		
Apply	Click Apply to save your changes to the switch.		

3.8.3 Log Setting

3.8.3.1 Local Log

Use this screen to display the switch logs.

Click **Diagnostics** > **Log Setting** > **Local Log** to view the screen as shown next.

Local Log

Local Log Target Setting

Target	Severity	
Select Targets 🔹	Select Levels 👻	

Apply

Local Log S	etting Status		
Status	Target	Severity Action	
enabled	local-ram	error, warning, notice, Disable	
disabled	local-flash	error, warning, notice, Enable	

LABEL	DESCRIPTION
Target	 Select the target to store log message: RAM: store the log messages in the RAM disk. All log messages will disappear after system reboot. Flash: store the log messages in the Flash memory. All log messages will not disappear after system reboot.
Severity	 Select the severity level(s) of the log entries you want to display. The possible severity levels are: Error - to record system failures, such as events which will cause the switch to malfunction and events such as invalid user input in the web configurator. Warning - to record non critical errors on the Switch. The Switch will continue to function when warnings are recorded. Info - to record regular system events, such as configuration changes or

	logins.				
	• Debug - to record events which can be helpful for engineering				
	debugging of the switch's function. This field is not recommended				
	to track as it creates many messages not helpful to typical users.				
	Notice- to record the error which need to be noticed.				
Apply	Click Apply to save your changes to the switch.				
Status	It displays the status of local log settings.				
Target	It displays the target you've choosed.				
Severity	It displays the severity status.				
Action	Click enable to enable this function.				
ACTION	Click disable to disable this function.				

3.8.3.2 Remote Log

Click **Diagnostics** > **Log Setting** > **Remote Log** to view the screen as shown next.

Remote Log

Remote Log Target Setting

Server Index	Server IP	Server Port	Severity
server1		514 (1-65535)	Select Levels 👻

Apply

Status	Server Info	Severity	Action
disabled	server1 - 0.0.0.0 : 0		N/A
disabled	server2 - 0.0.0.0 : 0		N/A
disabled	server3 - 0.0.0.0 : 0		N/A
disabled	server4 - 0.0.0.0 : 0		N/A

LABEL	DESCRIPTION			
Server Index	Select the index of remote log server. System supports 4 remote log servers. When a server is set and enabled, log messages will send to this server.			
Server IP	The IP address of remote log server.			
Server Port	Enter a number between 1 and 65535 as the server port.			
Severity	Select the severity level(s) of the log entries you want to display. The possible severity levels are:			

	 Error - to record system failures, such as events which will cause the switch to malfunction and events such as invalid user input in the web configurator. Warning - to record non critical errors on the Switch. The Switch will continue to function when warnings are recorded. Info - to record regular system events, such as configuration changes or logins. Debug - to record events which can be helpful for engineering debugging of the switch's function. This field is not recommended 			
	 to track as it creates many messages not helpful to typical users. Notice- to record the error which need to be noticed. 			
Apply	Click Apply to save your changes to the switch.			
Status	It displays the status of local log settings.			
Server Information	It displays the server information.			
Severity	It displays the severity status.			
Action	It displays the action status.			

3.8.4 Factory Default

Follow the steps below to restore the switch back to the factory defaults.

1. Click Diagnostics->Factory Default to view the screen as shown next.



2. Click the **Restore** button, then the **confirm** interface pops up.



3. Click **OK** to restore all switch configurations to the factory defaults and the switch will reboot.

3.8.5 Reboot Switch

Reboot allows you to restart the switch without physically turning the power off.

Follow the steps below to reboot the switch.

1. Click **Diagnostics->Reboot Switch** to view the screen as shown next.

	Reboot	Switch
	Reboot	
2. Click Reboot button, then the	following interfac	e pops up.
Re	booting	now

3. When it finished, the switch has been restarted.

3.9 Maintenance

3.9.1 Backup Manager

This page allow user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.

Click Maintenance->Backup Manager to view the screen as shown next.



Backup Manager	
Backup Method	TFIP
Server IP	(IPv4 or IPv6 Address)
Backup Type	⊙Image ○Configuration
Backup	

Backup Image with TFTP Page

Backup Manager

Backup Manager	
Backup Method	TFIP
Server IP	(IPv4 or IPv6 Address)
Васкир Туре	Olmage Oconfiguration
Configuration	startup-config.cfg

Backup

Backup Config with TFTP Page

Backup Manager

Backup Manager

Backup Method	HTTP
Backup Type	

Backup

Backup Image with HTTP Page

Backup Manager

Backup Manager

Backup Method	НТІР
Backup Type	Olmage 💿 Configuration
Configuration	startup-config.cfg

Backup

Backup Config with HTTP Page

LABEL	DESCRIPTION
Backup	Select backup method:

Method	 TFTP: Use TFTP to backup. HTTP: Use HTTP to backup.
Server IP	IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.
Backup Type	 Select backup type: Image: Firmware image of current system. Configuration: Configuration file.
Configuration	If the Configuration backup type is selected, one of the configuration file in current system can select to backup.
Backup	Click Backup to save the current switch configuration to the local address specified.

3.9.2 Upgrade Manager

This page allow user to upgrade new firmware image or configuration file to the switch from remote TFTP server or select file from web browser.

Click Maintenance->Upgrade Manager to view the screen as shown next.

Upgrade Manager

grade Method TFTP 🖌	
Server IP (IF	Pv4 or IPv6 Address)
File Name	
pgrade Type Image Configuration	

Upgrade

Upgrade with TFTP Page

Upgrade Manager

Upgrade Manager

Upgrade Method	HTIP
Browse file	Browse
Upgrade Type	Image ○ Configuration

Upgrade

Upgrade with HTTP Page

LABEL DESCRIPTION Select upgrade method: Upgrade **TFTP:** Use TFTP to upgrade. Method HTTP: Use HTTP to upgrade. IP address of the TFTP server. If the TFTP upgrade method is selected, the Server IP IP address of the TFTP server must be assigned. Firmware image or configuration file name on remote TFTP server. If the File Name TFTP upgrade method is selected, the file name must be specified. If the HTTP upgrade method is selected, the browse file field allow you to **Browse File** select any file on host operating system. Select upgrade type: Upgrade Image: Firmware image of current system. Туре Configuration: Configuration file. Click Upgrade to update the file specified above and install the new Upgrade firmware.

The following table describes the labels in this screen.

3.9.3 Configuration Manager

This page allow user to save running configurations to any file which user specified by pushing the "Save Configuration" button. And use "Set Startup" button to select any existing configuration file as startup configuration. The "Delete" button allow user to delete the selected configuration file.

Click Maintenance-> Configuration Manager to view the screen as shown next.



Configuration Manager Page

Configuration Manager

Save Configuration

Configuration	New Configuration	*
New Config Name	.cfg	
Save Configuration	Set Startup	

File Name File Size startup-config.cfg (selected) 8933 Bytes

Configuration Manager with new file name Page

LABEL	DESCRIPTION
Configuration	You have two choice: startup-config.cfg and New Configuration
New Config Name	Configuration file name. Our system will save it with sub file name .cfg automatically.
Save	Click Save Configuration to save running configurations to any file which
Configuration	user specified
Set Startup	Click Set startup to select any existing configuration file as startup
	configuration.
File Name	It displays the name of the file.
File Size	It displays the size of the file.
Delete	Click Delete to delete the selected configuration file.

3.9.4 Account Manager

This page allow user to add or delete switch local user database for authenticating.

Click **Maintenance** > **Account Manager** in the navigation panel to display the screen as shown below.

Local User Information

New User

User Name	Password Type	Password	Retype Password	Privilege Type
	Clear Text 🔽			Admin 💌

Apply

Local Users			
User Name	Password Type	Privilege Type	Modify
	Encrypted	Admin	Delete

The following table describes the labels in this screen.

LABEL	DESCRIPTION
User name	Enter your user name for new account.
Password Type	Select password type for new account:
	Clear Text: Password without encryption.
	 Encrypted: Password with encryption.
	 No Password: No password for new account.
Password	If the password type is not "No Password", the password must be
	specified.
Retype Password	Retype password to make sure the password is exactly you typed before
	in "Password" field.
Privilege Type	Select privilege level for new account:
	 Admin: Allow to change switch settings.
	 User: See switch settings only. Not allow to change it.
Apply	Click Apply to save your changes to the switch.
Modify	Click Delete to modify any configuration.

3.9.5 Enable Password

This page allow user to modify the enable password. In command line interface, user can use "enable" command to change their privilege level to "Admin". After "enable" command is issued, user need to type the enable password to change their privilege level.

Click **Maintenance** > **Enable Password** in the navigation panel to display the screen as shown below.

Note: It is highly recommended that you change the default password.

Admin Enable Password

Setup Enable Password

Password Type	Clear Text 🐱
Password	
Retype Password	

Apply

LABEL	DESCRIPTION
Password Type	Select password type for enable password:
	Clear Text: Password without encryption.
	 Encrypted: Password with encryption.
Password	Enter your new system password.
Retype Password	Retype password to make sure the password is exactly you typed
	before in "Password" field.
Apply	Click Apply to save your changes to the switch.

Product Specifications

Standard	IEEE 802.3/802.3u/802.3ab IEEE 802.3x flow control IEEE 802.3az Energy Efficient Ethernet IEEE 802.1D spanning tree protocol IEEE 802.1p class of service, priority protocols IEEE 802.1Q VLAN tagging IEEE 802.1x port authentication IEEE 802.3ad VLAN stacking IEEE 802.3ad LACP aggregation
Interface	24* 10/100/1000Mbps ports 2* SFP ports
Transmission Mode	10/100Mbps: Full-duplex, Half-duplex 1000Mbps: Full-duplex
MAC Address Table	16K
Jumbo Frame	9K Bytes
Buffer Memory	448K Bytes
Temperature	Operating: 0°C ~ 40°C (32°F ~104°F) Storage: -40°C ~ 70°C (-40°F ~158°F)
Humidity	Operating: 10% ~ 90% RH, non-condensing Storage: 5%~90% RH, non-condensing
LED Indications	1*Power LED(Green) 24*Gigabit port LEDs(Link/Act: Green) 2*SFP port LEDs(Link/Act: Green)
Power Supply	Internal power supply 5V/6A
Dimensions	266*185*44 mm
Case Material	Metal
Certification	FCC, CE, VCCI Class A