

Industrial Managed Ethernet Switch

MS10GT8GX2-R User's Manual



Ver. 1.2
May 2019

Table of Content

Getting to Know Your Switch.....	6
1.1 About the MS10GT8GX2-R Managed Industrial Switch.....	6
2.1 Features	6
Hardware Overview.....	7
3.1 Front Panel	7
3.2 Front Panel LEDs.....	9
4.1 SFP.....	9
4.1.1 1000BASE-TX /100BASE-TX/10BASE-T Pin Assignments.....	10
4.2 Console Cable	11
WEB Management.....	12
5.1 Configuration using the Web Browser	12
5.1.1 About Web-based Management	12
5.1.2 System	14
5.1.2.1 System Information.....	14
5.1.2.2 Configuration	15
5.1.2.3 IP Configuration	15
5.1.2.4 Time Setting	17
5.1.2.5 Log Configuration.....	19
5.1.2.6 Software Upload	19
5.1.3 DHCP	20
5.1.3.1 DHCP server	20
5.1.3.2 DHCP snooping.....	22
5.1.3.3 DHCP Relay.....	22
5.1.4 Ports.....	23
5.1.4.1 Ports Configuration	23
5.1.4.2 Port state	24
5.1.5 Aggregation	25
5.1.5.1 Static	25
5.1.5.2 Static Status	26
5.1.5.3 LACP Port Configuration	26
5.1.5.4 System Status.....	27
5.1.6 Redundancy	28
5.1.6.1 Loop Protection Configuration.....	28
5.1.6.2 Loop Protection Status.....	29
5.1.6.3 Spanning Tree Bridge Setting.....	30
5.1.6.4 MSTI Mapping	31
5.1.6.5 MSTI Priority	32
5.1.6.6 CIST Ports	33
5.1.6.7 MSTI Ports.....	34
5.1.6.8 Ring	35
5.1.6.9 EPS	36
5.1.6.10 MEP.....	37
5.1.6.11 ERPS	38
5.1.7 LLDP	40
5.1.7.1 LLDP Configuration.....	40
5.1.7.2 LLDP Neighbor.....	41

	5.1.7.3.	LLDP-MED	41
5.1.8	GMRP		42
	5.1.8.1.	GMRP Configuration	42
	5.1.8.2.	Port Config	43
5.1.9	Diagnostics		44
	5.1.9.1.	Ping and Ping6	44
	5.1.9.2.	VeriPHY	45
	5.1.9.3.	Mirroring	45
5.1.10	VLANs		48
	5.1.10.1.	Global VLAN Configuration	48
	5.1.10.2.	VLAN Membership Status for Combined users	51
	5.1.10.3.	VLAN Port Status for Combined users	52
	5.1.10.4.	VLAN Translation	53
	5.1.10.5.	Private Vlan	55
	5.1.10.6.	VCL	57
	5.1.10.7.	Voice VLAN	61
5.1.11	QoS		63
	5.1.11.1.	QoS Ingress Port Classification	64
	5.1.11.2.	QoS Ingress Port Policers	66
	5.1.11.3.	QoS Ingress Queue Policers	68
	5.1.11.4.	QoS Egress Port Schedulers	68
	5.1.11.5.	QoS Egress Port Shapers	69
	5.1.11.6.	QoS Egress Port Tag Remarking	70
	5.1.11.7.	QoS Port DSCP Configuration	71
	5.1.11.8.	DSCP-Based QoS Ingress Classification	72
	5.1.11.9.	DSCP Translation	73
	5.1.11.10.	DSCP Classification	74
	5.1.11.11.		75
	5.1.11.12.	QoS Control List Configuration	75
	5.1.11.13.	Global Storm Policer Configuration	77
5.1.12	IGMP Snooping		77
	5.1.12.1.	IGMP Snooping Configuration&Port Related Configuration	78
	5.1.12.2.	IGMP Snooping VLAN Configuration	79
	5.1.12.3.	IGMP Snooping Status	81
	5.1.12.4.	IGMP Snooping Group Information	82
	5.1.12.5.	IGMP Snooping Port Filtering Profile Configuration	82
	5.1.12.6.	IGMP SFM Information	83
5.2	Security		84
5.2.1	Switch		85
	5.2.2.1.	Users Configuration	85
	5.2.2.2.	Privilege Level Configuration	85
	5.2.2.3.	Authentication Method Configuration	88
	5.2.2.4.	SSH Configuration	90
	5.2.2.5.	HTTPS Configuration	90
	5.2.2.6.	Access Management Configuration	92
	5.2.2.7.	Management Statistics	93
	5.2.2.8.	Alarm Configuration	94
	5.2.2.9.	SNMP	95
	5.2.2.1.	SNMP System Configuration	95
	5.2.2.2.	Trap Configuration	97
	5.2.2.3.	SNMPv3 Community Configuration	100
	5.2.2.4.	SNMPv3 User Configuration	101
	5.2.2.5.	SNMPv3 Group Configuration	102
	5.2.2.6.	SNMPv3 View Configuration	103
	5.2.2.7.	SNMPv3 Access Configuration	104
	5.2.2.10.	RMON	105
	5.2.2.8.	RMON Statistics Configuration	105

5.2.2.9.	RMON Statistics Status Overview	105
5.2.2.10.	RMON History Configuration	106
5.2.2.11.	RMON History Overview	107
5.2.2.12.	RMON Alarm Configuration	108
5.2.2.13.	RMON Alarm Overview	110
5.2.2.14.	RMON Event Configuration	110
5.2.2.15.	RMON Event Overview	111
5.2.2	Network	112
5.2.2.16.	Port Security	112
5.2.2.17.	Limit Control	112
5.2.2.18.	Switch	114
5.2.2.19.	Port Security Port Status Port 1	115
5.2.2.20.	Network Access Server Configuration	116
5.2.2.21.	Network Access Server Switch Status	123
5.2.2.22.	NAS Statistics Port 1	124
5.2.2.23.	ACL	125
5.2.2.24.	ACL Ports Configuration	125
5.2.2.25.	ACL Rate Limiter Configuration	126
5.2.2.26.	Access Control List Configuration	127
5.2.2.27.	ACL Status	129
5.2.2.28.	IP Source Guard	130
5.2.2.29.	IP Source Guard Configuration	130
5.2.2.30.	Static IP Source Guard Table	131
5.2.2.31.	Dynamic IP Source Guard Table	131
5.2.2.32.	ARP Inspection	132
5.2.2.33.	ARP Inspection Configuration	132
5.2.2.34.	VLAN Mode Configuration	134
5.2.2.35.	Static ARP Inspection Table	135
5.2.2.36.	Dynamic ARP Inspection Table	135
5.2.2.37.	Dynamic ARP Inspection Table	136
5.3	AAA	137
5.3.1	RADIUS Server Configuration	137
5.3.2	RADIUS Server Status Overview	138
5.3.3	RADIUS Authentication Statistics for Server #1	140
5.3.4	TACACS+ Server Configuration	143
5.4	MAC Table	144
5.4.1	MAC Address Table	147
5.5	Configuration	147
5.5.1	Save Running Configuration to startup-config	147
5.5.2	Download Configuration	148
5.5.3	Upload Configuration	149
5.5.4	Activate Configuration	150
5.5.5	Delete Configuration File	150
5.6	Factory Default	150
5.7	Restart Device	151
	Command Line Interface Management	152
6.1	About CLI Management	152
6.2	Commands Set List—System Commands Set	156
6.3	Commands Set List—Port Commands Set	157
6.4	Commands Set List—Trunk command set	158
6.5	Commands Set List—VLAN command set	158
6.6	Commands Set List—Spanning Tree command set	159
6.7	Commands Set List—QoS command set	160
6.8	Commands SetList—IGMP snooping command set	161
6.9	Commands Set List—MAC/Filter Table command set	161

6.10	Commands Set List—SNMP command set	161
6.11	Commands Set List—Port Mirroring command set	162
6.12	Commands Set List—TFTP command set	162
6.13	Commands Set List—LOG command set	162
6.14	Commands Set List—NTP command set.....	163
6.15	Commands Set List—M-Ring command set	163
Notes:		164

Getting to Know Your Switch

1.1 About the MS10GT8GX2-R Managed Industrial Switch

The Meridian MS10GT8GX2-R rack card is a managed redundant ring Ethernet switch with 8x10/100/1000Base-TX and 2x1000Base-F(X) Ports. With complete support of auto negotiation, 10/100/1000M transmission, full/half duplex and auto MDI/MDIX control this switch will provide stable operation in any mission-critical application. MS10GT8GX2-R can be managed by web interface, browser or optional, Windows® utility, SpectraVISION.

MS10GT8GX2-R switches are designed to work in wide operating temperature from -40°C to 75°C, to make them completely suitable for harsh environments.

2.1 Features

- 8x10/100/1000Base-T(X) ports and 2x100/1000Base-X SFP ports
- M-Ring (recovery time≤15ms), RSTP/STP and MSTP for network redundancy
- Supports IPv4/IPv6
- Supports STP/RSTP/MSTP/ITU-T G.8032 Ethernet Ring Protection
- Supports IGMP v1/v2/v3 Snooping, MLD v1/v2 Snooping
- Supports IEEE802.1Q VLAN/MAC based VLAN/Protocol based VLAN /IP subnet based VLAN/GVRP/MVR
- Supports DHCP Client/Relay/snooping/option 82Support IGMPV1/V2/ V3 Snooping. MLD v1/v2 Snooping
- Supports Port-based IEEE802.1X/Single and multiple IEEE802.1X/MAC- based authentication/VLAN Assignment/ IP source guard/ RADIUS/ TACACS+/ACL/SSH v2/HTTPS
- Supports web interface management CLI-Console/Telnet, SNMPv1/v2/v3, ROMN/System syslog
- Supports DNS client/proxy
- Supports LACP/Link Aggregation Static
- Supports port trunking, port speed limit, broadcast storm control
- Supports two 2.5G per port, can be configured 1G per port
- IETF RFC 1213 MIB-II (Management Information Base)

- Enclosure: Two Slot Rack Card
- Optional redundant power inputs with SR-2001/AR1 chassis
- Wide Operating Temperature: -40 to 75°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- EMC performance meets industrial level 4
- Green industrial series, without fan, low power consumption
- 10/100/1000Base-T(X) Gigabit Ethernet port
- 100/1000Base-X on SFP port
- Console Port
- Dimensions (W x D x H): 40mm(1.6 inch) x 160mm (6.3 inch) x 127mm (5.0 inch)

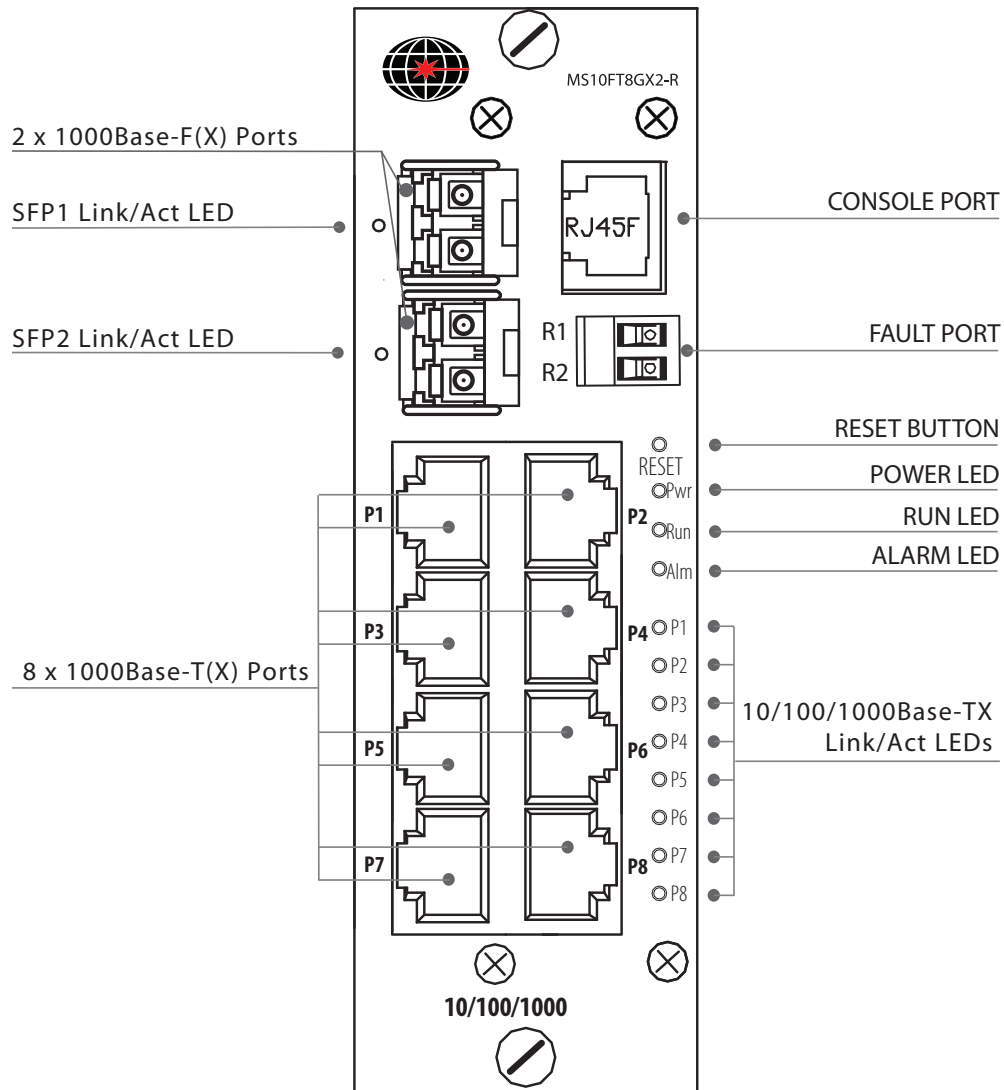
Hardware Overview

3.1 Front Panel

The front panel of MS10GT8GX2-R has following labels.

Ports / Buttons	Description
Gigabit RJ-45 ports	8x 10/100/1000Base-T(X) Gigabit ports
SFP ports	2 x 100/1000Base-FX on SFP port
Console	To manage switch via RJ-45 connector.
Fault contact	2-pin Screw Terminals. Relay output to carry capacity of 1A @ 24VDC
Reset	Reset to Factory defaults

MS10GT8GX2-R



3.2 Front Panel LEDs

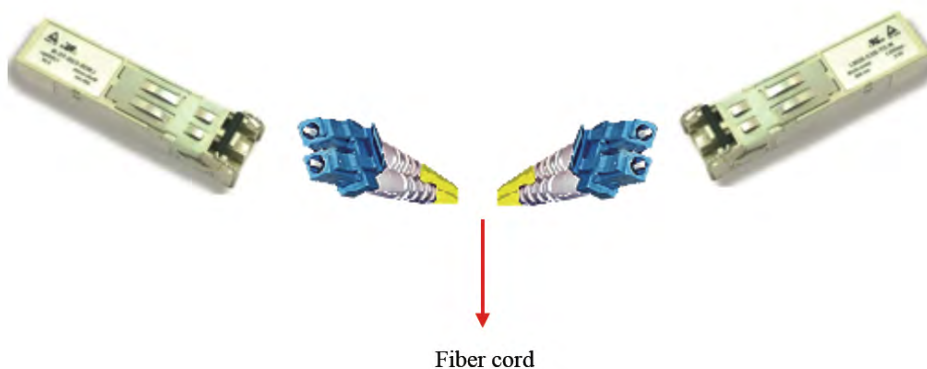
LED	Color	Status	Description
Pwr	Green	On	DC power input activated.
Alm	Green	On	Alarm activated
Run	Green	On	Slow flash: system run Quick flash: Ring Master
10/100/1000Base-TX Ethernet ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.
100/1000Base-FX SFP ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.

4.1 SFP

This switch is also equipped with two SFP fiber optic ports. These are available in a variety of configurations including single-mode, multimode, one fiber, two fibers, long reach & short reach. Please consult the SFP data sheet for a complete listing of the available SFP devices.

Switch A

Switch B



4.1.1 1000BASE-TX /100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-TX RJ-45 Pin Assignments

Pin Number	Assignment
1	TD +
2	TD -
3	RD +
4	Not used
5	Not used
6	RD -
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The MS10GT8GX2-R switch also supports auto MDI/MDI-X operation. As such, you can use a straight-through cable to connect a standard computer to the switch using the computer's RJ45 Ethernet port. The tables below show the 10BASE-T/ 100/1000BASE-TX MDI and MDI-X port pin outs.

10/100 Base-TX MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 Console Cable

The MS10GT8GX2-R switch can be managed from the console port. Enclosed console cable with RJ-45 and DB9 connectors can be used to connect console port (RJ-45 connector) on the switch and the RS-232 port (DB9 connector) on the computer.

PC pin out (male) assignment	RS-232 with DB9 female connector	RJ-45 connector
Pin #2 RD	Pin #2 TD	Pin #3
Pin #3 TD	Pin #3 RD	Pin #6
Pin #5 GD	Pin #5 GD	Pin #5

WEB Management

5.1 Configuration using the Web Browser

This section introduces the switch configuration using a standard Web browser.

5.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Windows Internet Explorer. The Web-Based Management function supports Internet Explorer 9.0 or later.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.0.2**

Subnet Mask: **255.255.255.0**

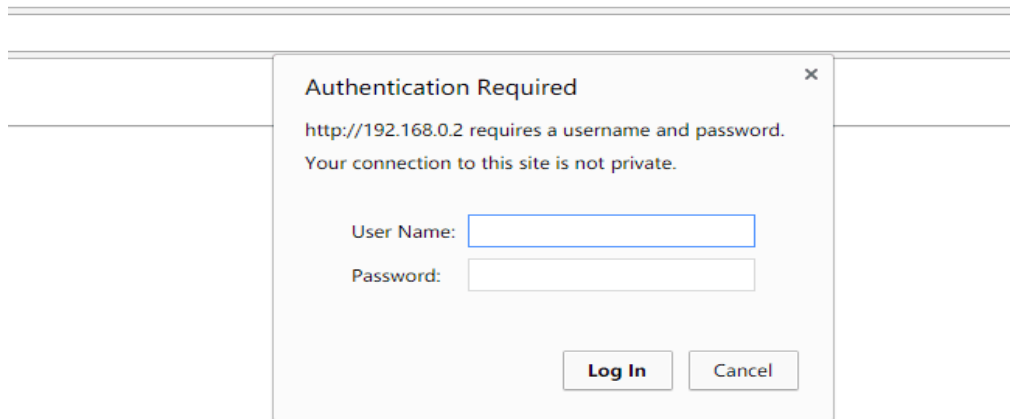
Default Gateway: **192.168.0.1**

User Name: **admin**

Password: **123**

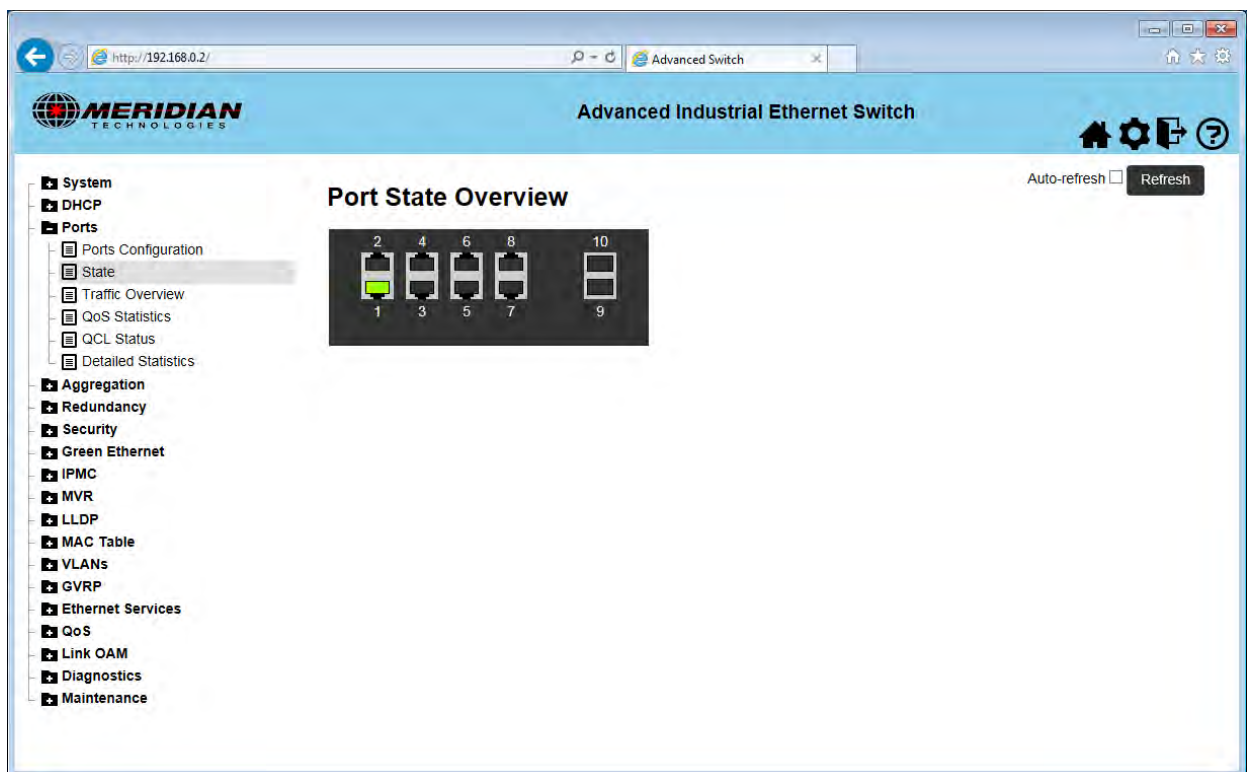
System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press "**Enter**".
3. The login screen appears.
4. Key in the username and password. The default username is admin and password is 123.
5. Click "Enter" or "OK" button, then the main interface of the Web-based management appears.

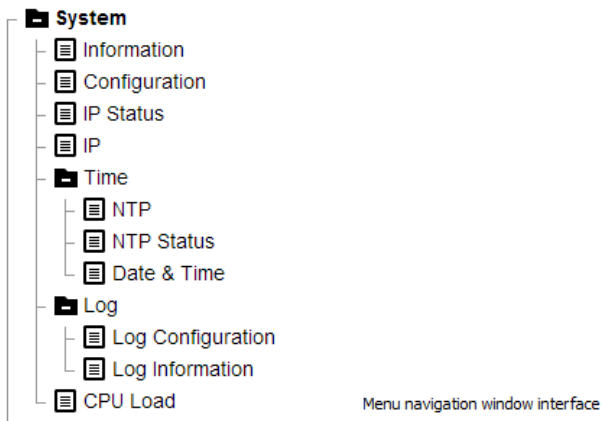


Login screen

Main interface

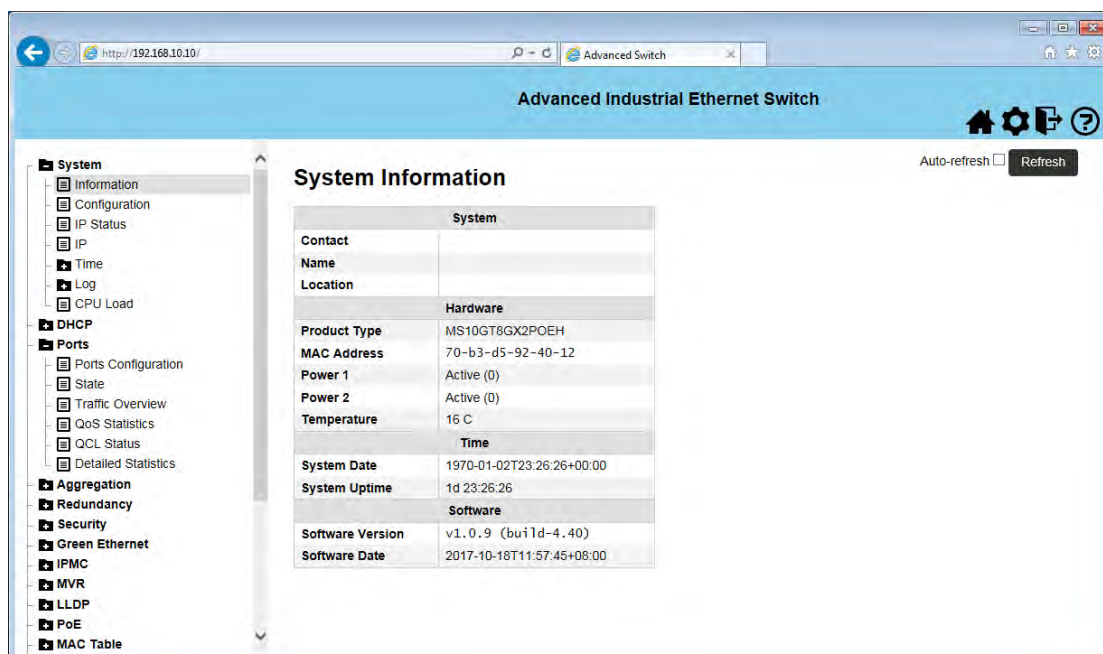


5.1.2 System



5.1.2.1. System Information

System Information interface. The system information will display the configuration of Basic Settings



Switch Setting page.

Label	Description
System Contact	Display the name of contact person or organization
System Name	Display the name of switch
System Location	Display the switch physical location.
Product Type	Display the model of the switch
Software Version	Display the switch's firmware version
MAC Address	Display the unique hardware address assigned by manufacturer

5.1.2.2. Configuration

The switch system information is provided here.

System Information Configuration

System Contact	
System Name	
System Location	

switch system information setting interface

The following table describes the labels in this screen.

Label	Description
System Contact	The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	Assign the name of switch.
System Location	Assign the switch physical location. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

5.1.2.3. IP Configuration

You can configure the IP Settings and DHCP client function through IP configuration function.

IP Configuration

Mode: Host

DNS Server 0: No DNS server

DNS Server 1: No DNS server

DNS Server 2: No DNS server

DNS Server 3: No DNS server

DNS Proxy: ☐

IP Interfaces

DHCPv4				IPv4			DHCPv6			IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐			192.168.0.2	24	☐	☐			

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
Add Route				

IP Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Configure whether the IP stack should act as a Host or a Router.
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface.
IPv4 DHCP Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.0.2.
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask.
DHCPv6 Enable	Enable the DHCPv6 client by checking this box.
DHCPv6 Rapid Commit	Enable the DHCPv6 Rapid-Commit option by checking this box.
DHCPv6 Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
IPv6 Address	The IPv6 address of the interface.
IPv6 Mask	The IPv6 network mask, in number of bits (prefix length).
DNS Server 0	Assign the primary DNS IP address
DNS Server 1	Assign the secondary DNS IP address
DNS Server 2	Assign the third DNS IP address
DNS Server 3	Assign the fourth DNS IP address
DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported.
Save	Click "Save" to activate the configurations.

5.1.2.4. Time Setting

NTP

The NTP (Network Time Protocol) settings allow you to synchronize switch clocks over the Internet.

NTP Configuration

Mode	Disabled ▼
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

NTP Configuration interface

The following table describes the labels in this screen.

Label	Description
NTP mode	Enable or disable NTP function to get the time from the NTP server.
Server 1-5	Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.
Save	Click " Save " to activate the configurations.

Date & Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Date & Time Configuration

Date & Time Configuration(UTC)	
Date	1970-01-01 (yyyy-mm-dd)
Time	05:03:48 (hh:mm:ss)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097

Time Zone Configuration interface

This page allows you to configure the Time Zone. The following table describes the labels in this screen.

Label	Description
Time Zone	Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone.
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration.
Save	Click " Save " to activate the configurations.

5.1.2.5. Log Configuration

System Log Configuration

Server Mode	Disabled ▼
Server Address	
Syslog Level	Informational ▼

Log Configuration interface

The following table describes the labels in this screen.

Label	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server.
Server Address	Indicates the IPv4 host address of syslog server.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: Error: Send the specific messages which severity code is less or equal than Error (3). Warning: Send the specific messages which severity code is less or equal than Warning (4). Notice: Send the specific messages which severity code is less or equal than Notice (5). Informational: Send the specific messages which severity code is less or equal than Informational (6).

5.1.2.6. Software Upload

This function allows you to update the firmware of the switch.

Update Firmware interface

5.1.3 DHCP

DHCP



5.1.3.1. DHCP server

Enable this DHCP server function will cause the switch system to function as a DHCP server.

DHCP Server Mode Configuration

Global Mode

Mode

VLAN Mode

Delete	VLAN Range	Mode
Add VLAN Range		

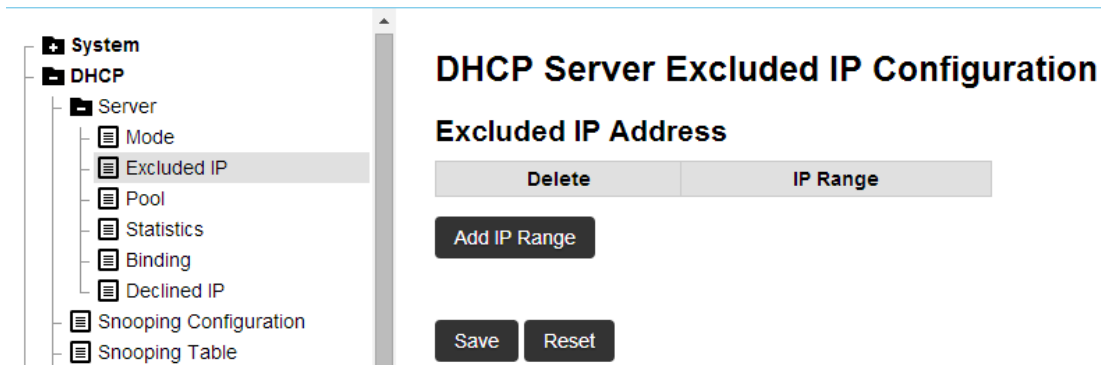
Add VLAN Range

Save **Reset**

DHCP Server Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Server Mode	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network
VLAN Mode	Configure operation mode to enable/disable DHCP server per VLAN.
VLAN Range	Indicate the VLAN range in which DHCP server is enabled or disabled.



DHCP Server Excluded IP Configuration interface

The following table describes the labels in this screen.

Label	Description
IP Range	Define the IP range to be excluded IP addresses.
Save	Click “Save” to activate the configurations.

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
Add New Pool					
Save Reset					

DHCP Server Pool Configuration interface

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client. The following table describes the labels in this screen.

Label	Description
Name	Configure the pool name that accepts all printable characters, except white space.
Type	Display which type of the pool is “network” or “Host”
IP	Display network number of the DHCP address pool.
Subnet Mask	Display subnet mask of the DHCP address pool.
Lease Time	Display lease time of the pool.
Save	Click “Save” to activate the configurations.

DHCP Server Binding IP

Auto-refresh ☐ Refresh Clear Selected Clear Automatic Clear Manual Clear Expired

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID
--------	----	------	-------	-----------	-----------

DHCP Server Binding IP

The following table describes the labels in this screen.

Label	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

5.1.3.2. DHCP snooping

DHCP Snooping Configuration

Snooping Mode Disabled ▼

Port Mode Configuration

Port	Mode
*	<> ▼
1	Trusted ▼
2	Trusted ▼
3	Trusted ▼

DHCP Snooping Configuration interface

The following table describes the labels in this screen.

Label	Description
Snooping Mode	Enable or Disable DHCP Snooping function.
Port Mode	Configures the port as trusted or untrusted source of the DHCP messages.

5.1.3.3. DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

DHCP Relay Configuration

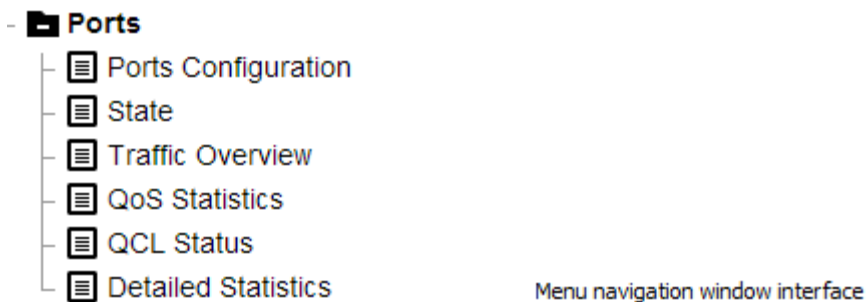
Relay Mode	Disabled ▼
Relay Server	0.0.0.0
Relay Information Mode	Disabled ▼
Relay Information Policy	Keep ▼

DHCP Relay Configuration interface

The following table describes the labels in this screen.

Label	Description
Relay Mode	Enable or Disable DHCP Relay function.
Relay Server	Indicates the DHCP relay server IP address.
Relay Information Mode	Enable or Disable DHCP Relay information function. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client.
Relay Information Policy	Indicates the DHCP relay information option policy.

5.1.4 Ports



Menu navigation window interface

5.1.4.1. Ports Configuration

By this function, you can set the state, speed/duplex, flow control, and security of the port, and so on.

Port Configuration

[Refresh](#)

Port	Description	Link	Current	Speed	Adv Duplex		Adv speed			Flow Control			Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx			
*				<>	☒	☒	☒	☒	☒	☐			9600	<>	☐
1			1Gfdx	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
2			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
3			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
4			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
5			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
6			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
7			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐
8			Down	Auto	☒	☒	☒	☒	☒	☐	☒	☒	9600	Discard	☐

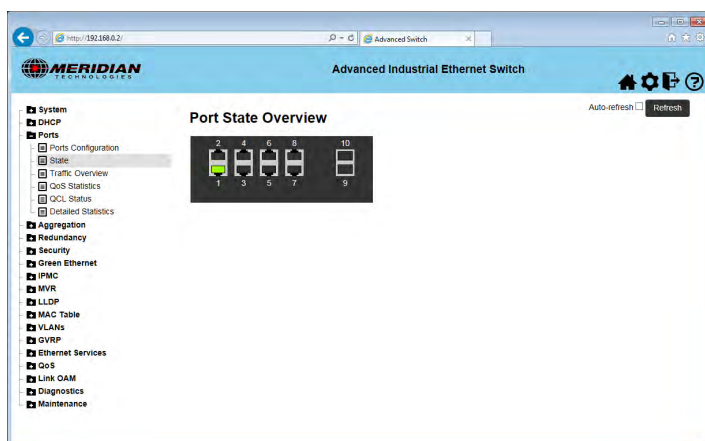
Ports configuration interface

The following table describes the labels in this screen.

Label	Description
Port	This is the logical port number for this row.
Description	Configure description of the port.
Link	The current link state is displayed graphically.
Current Link Speed	Display the current link speed of the port.
Configured Link Speed	Selects any available link speed for the given switch port. such as 1Gbps FDX.
Advertise Duplex	Configure "Fdx" or "Hdx" of the port.
Advertise Speed	Configure "10M", "100M", "1000M" of the port.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS.
Excessive Collision Mode	Configure port transmit collision behavior.
Frame Length Check	Configures if frames with incorrect frame length in the EtherType Length field shall be dropped.
Save	Click "Save" to activate the configurations.

5.1.4.2. Port state

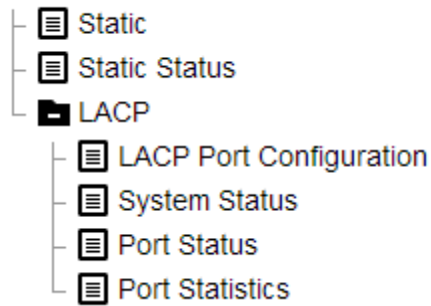
This page provides an overview of the current switch port states.



Ports state interface

5.1.5 Aggregation

Aggregation



Menu navigation window interface

5.1.5.1. Static

This function is used to configure the Aggregation hash mode and the aggregation group.

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☒
Destination MAC Address	☐
IP Address	☒
TCP/UDP Port Number	☒

Aggregation Group Configuration

Group ID	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Normal	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Ports Aggregation interface

The following table describes the labels in this screen.

Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame.
IP Address	The IP address can be used to calculate the destination port for the frame.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame.
Group ID	Indicates the group ID for the settings contained in the same row.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation.
Save	Click "Save" to activate the configurations.

5.1.5.2. Static Status

This page is used to see the status of ports in Aggregation group.

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

Aggregation status interface

The following table describes the labels in this screen.

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group(Static or LACP).
Speed	Speed of the Aggregation group.
Configured ports	Configured member ports of the Aggregation group.
Aggregated ports	Aggregated member ports of the Aggregation group.
Save	Click "Save" to activate the configurations.

5.1.5.3. LACP Port Configuration

This page allows the user to inspect the current LACP port configurations.

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<> ▼		<> ▼	<> ▼	32768
1	☐	Auto ▼		Active ▼	Fast ▼	32768
2	☐	Auto ▼		Active ▼	Fast ▼	32768
3	☐	Auto ▼		Active ▼	Fast ▼	32768
4	☐	Auto ▼		Active ▼	Fast ▼	32768
5	☐	Auto ▼		Active ▼	Fast ▼	32768
6	☐	Auto ▼		Active ▼	Fast ▼	32768

LACP Port Configuration interface

The following table describes the labels in this screen.

Label	Description
Port	The switch port number.
LACP Enabled	Controls whether LACP is enabled on this switch port.
Key	The Key value incurred by the port, range 1-65535.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions.
Prio	The Prio controls the priority of the port, range 1-65535.
Save	Click "Save" to activate the configurations.

5.1.5.4. System Status

This page provides a status overview for all LACP instances.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

LACP System Status interface

The following table describes the labels in this screen.

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance.
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed
Local Ports	Shows which ports are a part of this aggregation for this switch.
Refresh	Click "Refresh" button to refresh the configurations.

5.1.6 Redundancy

Redundancy

- └─ Loop Protection
 - └─ Configuration
 - └─ Status
- └─ Spanning Tree
 - └─ Bridge Settings
 - └─ MSTI Mapping
 - └─ MSTI Priorities
 - └─ CIST Ports
 - └─ MSTI Ports
 - └─ Bridge Status
 - └─ Port Status
 - └─ Port Statistics
- └─ Ring
- └─ EPS
- └─ MEP
- └─ ERPS

Menu navigation window interface

5.1.6.1. Loop Protection Configuration

This page allows the user to inspect the current Loop Protection configurations.

Loop Protection Configuration

General Settings

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

Port Configuration

Port	Enable	Action	Tx Mode
*	☒	<> ▾	<> ▾
1	☒	Shutdown Port ▾	Enable ▾
2	☒	Shutdown Port ▾	Enable ▾
3	☒	Shutdown Port ▾	Enable ▾

Loop Protection Configuration interface

The following table describes the labels in this screen.

Label	Description
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected.
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action performed when a loop is detected on a port.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

5.1.6.2. Loop Protection Status

This page displays the loop protection port status the ports of the switch.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

Loop Protection Status interface

The following table describes the labels in this screen.

Label	Description
Port	The switch port number of the port.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

5.1.6.3. Spanning Tree Bridge Setting

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the switch.

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▼
Bridge Priority	128 ▼
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

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

Save

Reset

STP Bridge Setting Configuration interface

The following table describes the labels in this screen.

Label	Description
Protocol Version	The MSTP / RSTP / STP protocol version setting.
Bridge Priority	Controls the bridge priority.
Hello Time	The interval between sending STP BPDU's.
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode).
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region.
Transmit Hold Count	The number of BPDU's a bridge port can send per second.
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU.
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time.
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled.

5.1.6.4. MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	bc-9c-c5-00-10-00
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	

MSTI Configuration interface

The following table describes the labels in this screen.

Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping.
Configuration Revision	The revision of the MSTI configuration named above.
MSTI	The bridge instance of MSTP.
VLANs Mapped	The list of VLANs mapped to the MSTI.

5.1.6.5. MSTI Priority

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<> ▼
CIST	128 ▼
MSTI1	128 ▼
MSTI2	128 ▼
MSTI3	128 ▼

STP MSTI Priority Configuration interface

The following table describes the labels in this screen.

Label	Description
Priority	Controls the bridge priority. Lower numeric values have better priority.

5.1.6.6. CIST Ports

This page allows the user to inspect the current STP CIST port configurations.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
-	☐	Auto ▼	128 ▼	Non-Edge ▼	☒	☐	☐	☐	Forced True ▼

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
*	☐	<> ▼	<> ▼	<> ▼	☒	☐	☐	☐	<> ▼
1	☐	Auto ▼	128 ▼	Non-Edge ▼	☒	☐	☐	☐	Auto ▼
2	☐	Auto ▼	128 ▼	Non-Edge ▼	☒	☐	☐	☐	Auto ▼

STP CIST Port Configuration interface

The following table describes the labels in this screen.

Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the port priority. This can be used to control priority of ports having identical port cost.
operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices.
AdminEdge	Controls whether the operEdge flag should start as set or cleared.
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium.

5.1.6.7. MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.

MSTI Port Configuration

Select MSTI

MST1 ▼

Get

MSTI Port Configuration interface

The following table describes the labels in this screen.

Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.

5.1.6.8. Ring

The Ring instances can be configured in here.

Ring Configuration

Global Configuration

Version

Ring v2 ▾

Delete	ID	Type	State	Root IP	Role	Priority	CRC Threshold	East Port			West Port			Backup Port		
								Port	State	CRC	Port	State	CRC	Port	State	CRC
Add New Ring Save Reset																

Ring Configuration interface

The following table describes the labels in this screen.

Label	Description
Version	Ring Version, v1 or v2.
Delete	This box is used to mark a Ring Domain for deletion in next Save operation.
ID	The ID of the created Ring Domain, It must be an integer value between 1 and 32. The maximum number of Ring Domain ID that can be created are 32
State	Indicates The current state of Ring.
Root IP	Indicates the IP address of master(root) station in the domain. Only normal station show it.
Role	Indicates the role state of this switch in the domain.
Priority	The role priority of this switch.
CRC Threshold	The port will be automatically disabled when specified number of error frames that received from the port is detected by switch, triggering Ring protocol to readjust transmission path for message.
East Port	East Port of the switch in the ring.
West Port	West Port of the switch in the Ring.
Backup Port	Backup port of the switch in the Ring.
Port	Port ID of east/west/backup port.
State	Interconnected State of port 0/port 1/backup port.
CRC	CRC error rate.
Add New Ring	Click "Add New Ring " to add a new Ring instance entry.
Save	Click to save changes.

5.1.6.9. EPS

The Ethernet (Linear) Protection Switch instances can be configured in here.

Ethernet Protection Switching

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
--------	--------	--------	--------------	--------	--------	----------	----------	---------	-------

Ethernet Protection Switching Configuration interface

The following table describes the labels in this screen.

Label	Description
Delete	This box is used to mark an MEP for deletion in next Save operation.
EPS ID	The ID of the EPS. Click on the ID of an EPS to enter the configuration page. The range is 1-100.
Domain	Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.
Architecture	Port: This will create a 1+1 EPS. Port: This will create a 1:1 EPS.
W Flow	The working flow for the EPS - See 'Domain'.
P Flow	The protecting flow for the EPS - See 'Domain'.
W SF MEP	The working Signal Fail reporting MEP.
P SF MEP	The protecting Signal Fail reporting MEP.
APS MEP	The APS PDU handling MEP.
Alarm	There is an active alarm on the EPS.
Add New EPS	Click "Add New EPS" to add a new EPS entry.

5.1.6.10. MEP

The Maintenance Entity Point instances can be configured in here.

Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
--------	----------	--------	------	-----------	----------------	-------	---------------	------------	----------	-------

MEP Configuration interface

The following table describes the labels in this screen.

Label	Description
Delete	This box is used to mark an EPS for deletion in next Save operation.
Instance	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
Domain	Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.
Mode	MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point. Port: This will create a 1:1 EPS.
Direction	Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Up: This is an Up MEP - monitoring egress OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
Tagged VID	Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. EVC MEP: This is not used. VLAN MEP: This is not used. EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.
Add New MEP	Click "Add New EPS" to add a new EPS entry.

5.1.6.11. ERPS

The ERPS instances can be configured in here.

TIP: ERPS will automatically add the relevant MEP instances, but you need to manually configure the peer MEP and CCM.

Ethernet Ring Protection Switching

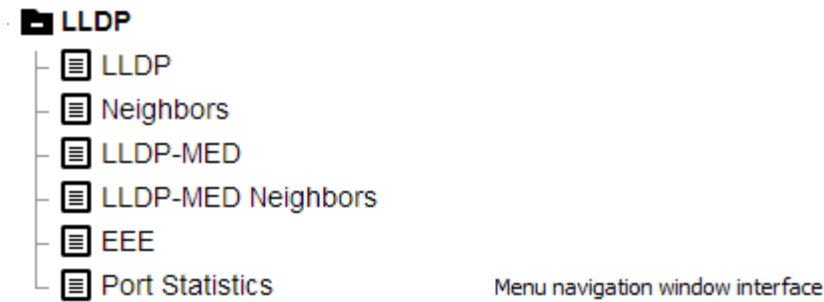
Delete	ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconn Node	Virtual Channel	Major Ring ID	Alarm
Add New Protection Group Save Reset												

ERPS Configuration interface

The following table describes the labels in this screen.

Label	Description
Delete	This box is used to mark an ERPS for deletion in next Save operation.
ERPS ID	The ID of the created Protection group, It must be an integer value between 1 and 64.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create "Port 1" of the switch in the Ring.
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP.
Port 0 APS MEP	The Port 0 APS PDU handling MEP.
Port 1 APS MEP	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
Ring Type	Type of Protecting ring. It can be either major ring or sub-ring.
Interconnected Node	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.
Virtual Channel	Sub-rings can either have virtual channel or not on the interconnected node.
Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
Alarm	There is an active alarm on the ERPS.
Add New Protection Group	Click to add a new Protection group entry.
Refresh	Click to refresh the page immediately
Save	Click to save changes.

5.1.7 LLDP



5.1.7.1. LLDP Configuration

LLDP Configuration

LLDP Parameters

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

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/1	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/2	Enabled	☐	☒	☒	☒	☒	☒

LLDP configuration interface

The following table describes the labels in this screen.

Label	Description
LLDP Mode	“Enable” or “Disable” LLDP function.
LLDP	The interval of resend LLDP (by default at 30 seconds)
Tx Hold	Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. Valid values are restricted to 2 - 10 times.
Tx delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

5.1.7.2. LLDP Neighbor

This page provides a status overview for all LLDP neighbors.

LLDP Neighbor Information

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

LLDP Neighbor interface

The following table describes the labels in this screen.

Label	Description
Local Interface	The interface on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities.
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management.

5.1.7.3. LLDP-MED

This page allows you to configure the LLDP-MED.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4
-------------------------	--------------------------------

Transmit TLVs

Interface	Capabilities	Policies	Location	PoE
*	☒	☒	☒	☒
GigabitEthernet 1/1	☒	☒	☒	☒
GigabitEthernet 1/2	☒	☒	☒	☒
GigabitEthernet 1/3	☒	☒	☒	☒

LLDP-MED Configuration interface

The following table describes the labels in this screen.

Label	Description
Interface	The interface name to which the configuration applies.
Capabilities	When checked the switch's capabilities is included in LLDP-MED information transmitted.
Policies	When checked the configured policies for the interface is included in LLDP-MED information transmitted.
Location	When checked the configured location information for the switch is included in LLDP-MED information transmitted.

5.1.8 GMRP

GMRP

-  Global config
-  Port config

Menu navigation window interface

5.1.8.1. GMRP Configuration

GMRP Configuration

Enable GMRP	☐
-------------	--------------------------

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Save

GMRP Configuration interface

The following table describes the labels in this screen.

Label	Description
Enable GMRP globally	The GMRP feature is globally enabled by setting the check mark in the checkbox named Enable GMRP and pressing the Save button.
GMRP protocol timers	Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs. Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs. LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.
Max number of VLANs	When GMRP is enabled, a maximum number of VLANs supported by GMRP is specified. By default this number is 20.

5.1.8.2. Port Config

This page allows you to enable or disable a port for GMRP operation.

This configuration can be performed either before or after GMRP is configured globally - the protocol operation will be the same.

GMRP Port Configuration

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼

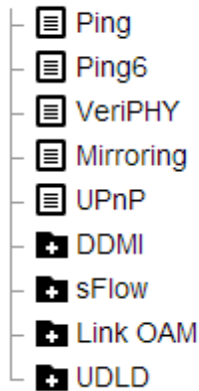
Port Configuration interface

The following table describes the labels in this screen.

Label	Description
Port	The logical port that is to be configured.
Mode	Mode can be either 'Disabled' or 'GMRP enabled'. These values turn the GMRP feature off or on respectively for the port in question.

5.1.9 Diagnostics

Diagnostics



Menu navigation window interface

5.1.9.1. Ping and Ping6

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

ICMP Ping interface

The following table describes the labels in this screen.

Label	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (Only for IPv6)	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

5.1.9.2. VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

VeriPHY Cable Diagnostics

Port

All ▼

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

VeriPHY configuration interface

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports. Press Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

5.1.9.3. Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

Mirroring & Remote Mirroring Configuration

Mode	Disabled ▼
Type	Mirror ▼
VLAN ID	200
Reflector Port	Port 1 ▼

Source VLAN(s) Configuration

Source VLANs	
--------------	--

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled ▼	☐	☐
2	Disabled ▼	☐	☐
3	Disabled ▼	☐	☐

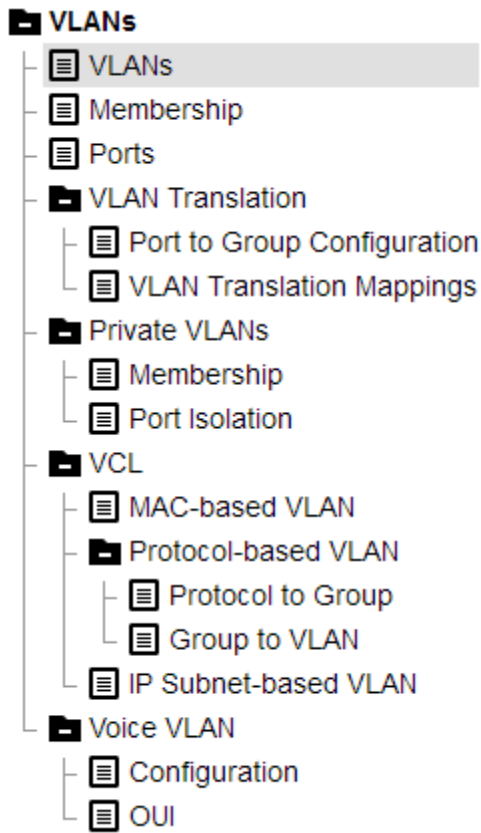
Mirroring Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	To Enabled/Disabled the mirror or Remote Mirroring function.
Type	Select switch type. Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch. Source: The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch. Intermediate: The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch. Destination: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.
VLAN ID	The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.
Reflector Port	The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the remote mirror function cannot work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port only supports on pure copper ports.
Source VLAN(s) Configuration	The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.
Port	The logical port for the settings contained in the same row.
Source	Select mirror mode. Disabled Neither frames transmitted nor frames received are mirrored. Both Frames received and frames transmitted are mirrored on the Intermediate/Destination port. Rx only Frames received on this port is mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.
Intermediate	Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. Note: The intermediate port needs to disable MAC Table learning.
Destination	Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning.

5.1.10 VLANS

Virtual Local Area Network (VLAN) is a new technology that can realize Virtual working group by logically dividing the equipment in the LAN into a Network segment.



Menu navigation window interface

5.1.10.1. Global VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☒	<>	<>	1	
1	Access	1	Edge	☒	Tagged and Untagged	Untagged	1	
2	Access	1	Edge	☒	Tagged and Untagged	Untagged	1	
3	Access	1	Edge	☒	Tagged and Untagged	Untagged	1	

Save Reset

Global VLAN Configuration interface

The following table describes the labels in this screen.

Label	Description
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.
Ethertype for Custom Port	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Port	This is the logical port number of this row
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 Accepts untagged and C-tagged frames Discards all frames not classified to the Access VLAN On egress all frames are transmitted untagged Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: By default, a trunk port is member of all VLANs (1-4095) The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs Frames classified to a VLAN that the port is not a member of are discarded By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware Ingress filtering can be controlled Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. S-Port: On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If the port is configured to accept either Untagged Only or Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag. If frames must be tagged on egress, they will be tagged with an S-tag. S-Custom-Port: On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If the port is configured to accept either Untagged Only or Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. Tagged and Untagged Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. Tagged Only Only frames tagged with the corresponding Port Type tag are accepted on ingress. Untagged Only Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. Untag Port VLAN Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. Tag All All frames, whether classified to the Port VLAN or not, are transmitted with a tag. Untag All All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs	A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.10.2. VLAN Membership Status for Combined users

VLAN Membership Status for Combined users

Combined ☐ Auto-refresh

Start from VLAN with entries per page.

Port Members												
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
1	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

VLAN Membership Status for Combined users interface

The following table describes the labels in this screen

Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the following image will be displayed: ☒ If a port is in the forbidden port list, the following image will be displayed: ☒ If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ☒ . The port will not be a member of the VLAN in this case.
Refresh	Click to refresh the page immediately.

5.1.10.3. VLAN Port Status for Combined users

VLAN Port Status for Combined users

Combined

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☒	All	1	Untag All		No
2	C-Port	☒	All	1	Untag All		No
3	C-Port	☒	All	1	Untag All		No
4	C-Port	☒	All	1	Untag All		No
5	C-Port	☒	All	1	Untag All		No
6	C-Port	☒	All	1	Untag All		No
7	C-Port	☒	All	1	Untag All		No
8	C-Port	☒	All	1	Untag All		No
9	C-Port	☒	All	1	Untag All		No
10	C-Port	☒	All	1	Untag All		No
11	C-Port	☒	All	1	Untag All		No
12	C-Port	☒	All	1	Untag All		No

VLAN Port Status for Combined users interface

The following table describes the labels in this screen

Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.
Frame Type	Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Port VLAN ID	Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.

Tx Tag	Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.
Untagged VLAN ID	If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
Conflicts	Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.
Refresh	Click to refresh the page immediately.

5.1.10.4. VLAN Translation

VLAN Translation Port Configuration

VLAN Translation Port Configuration

Auto-refresh ☐ **Refresh**

Port	Group Configuration	
	Default	Group ID
*	☐	<> ▼
1	☐	1 ▼
2	☐	2 ▼
3	☐	3 ▼

VLAN Translation Port Configuration interface

The following table describes the labels in this screen

Label	Description
Port	The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.
Default	To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.

Group ID	The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 12. Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to the previously saved values.

VLAN Translation Mapping Table

VLAN Translation Mapping Table

Auto-refresh ☐ **Refresh** **Remove All**

Group ID	VID	TVID	
			⊕

Mapping Configuration

Mapping Parameters

Group ID	0
VID	0
TVID	0

Save
Reset
Cancel

VLAN Translation Mapping Table interface

The following table describes the labels in this screen

Label	Description
Group ID	The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 12. Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.
VID	Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.
TVID	Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the
Modification Buttons	You can modify each VLAN Translation mapping in the table using the following buttons:  : Edits the mapping row.  : Deletes the mapping.  : Adds a new mapping.
Refresh	Click to refresh the page.
Remove All	Click to remove all VLAN Translation mappings.

5.1.10.5. Private Vlan

Private VLAN Membership Configuration

Auto-refresh ☐ Refresh

Private VLAN Membership Configuration

Port Members													
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
☐	1	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Add New Private VLAN

Save
Reset

Private VLAN Membership Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Private VLAN	Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save".
Delete	The Delete button can be used to undo the addition of new Private VLANs.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Port Isolation Configuration

Port Isolation Configuration

Auto-refresh ☐ **Refresh**

Port Number											
1	2	3	4	5	6	7	8	9	10	11	12
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save **Reset**

Port Isolation Configuration interface

The following table describes the labels in this screen

Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.10.6. VCL

MAC-based VLAN Membership Configuration

MAC-based VLAN Membership Configuration

Auto-refresh ☐ **Refresh**

Port Members			
Delete	MAC Address	VLAN ID	123456789101112
Currently no entries present			

Add New Entry

Save **Reset**

MAC-based VLAN Membership Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.
MAC Address	Indicates the MAC address of the mapping.
VLAN ID	Indicates the VLAN ID the above MAC will be mapped to.
Port Members	A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add a new Entry	Click to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save".
Delete	The button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries are limited to 256.
save	Click to save changes.
Reset :	Click to undo any changes made locally and revert to previously saved values.
Refresh	Refreshes the displayed table.

Protocol-based VLAN

Protocol to Group Mapping Table

Protocol to Group Mapping Table

Auto-refresh ☐ **Refresh**

Delete	Frame Type	Value	Group Name
☐	No Group entry found!		

Add New Entry**Save****Reset**

Protocol to Group Mapping Table interface

The following table describes the labels in this screen

Label	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.
Frame Type	Frame Type can have one of the following values: 1. Ethernet 2. LLC 3. SNAP Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.
Value	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for the three different Frame Types:
Group Name	A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). Note: Special characters and underscores (_) are not allowed.
Add a new Entry	Click to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed.
Delete	The button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.
save	Click to save changes.
Reset :	Click to undo any changes made locally and revert to previously saved values.
Refresh	Refreshes the displayed table.

Group Name to VLAN mapping Table

Group Name to VLAN mapping Table

Auto-refresh ☐ Refresh

		Port Members												
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
Currently no entries present in the switch														

Add New Entry

Save Reset

Group Name to VLAN mapping Table interface

The following table describes the labels in this screen

Label	Description
Delete	To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.
Group Name	A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).
VLAN ID	Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add a new Entry	Click to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port id members can be configured as needed. Legal values for a VLAN ID are 1through 4095.
Delete	The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 256.
Save	Click to save changes.
Reset :	Click to undo any changes made locally and revert to previously saved values.
Refresh	Refreshes the displayed table.

IP Subnet-based VLAN Membership Configuration

IP Subnet-based VLAN Membership Configuration

Auto-refresh ☐ **Refresh**

Port Members			
Delete	IP Address	Mask Length	VLAN ID
123456789101112			
Currently no entries present			

Add New Entry

Save **Reset**

IP Subnet-based VLAN Membership Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	To delete a mapping, check this box and press save. The entry will be deleted in the stack.
IP Address	Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically)
Mask Length	Indicates the subnet's mask length.
VLAN ID	Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.
Port Members	A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.
Add a new Entry	Click to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095.
Delete	The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The button can be used to undo the addition of new mappings.
Save	Click to save changes.
Reset :	Click to undo any changes made locally and revert to previously saved values.
Refresh	Refreshes the displayed table.

5.1.10.7. Voice VLAN

Voice VLAN Configuration

Voice VLAN Configuration

Mode	Disabled ▼
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High) ▼

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	OUI ▼
2	Disabled ▼	Disabled ▼	OUI ▼
3	Disabled ▼	Disabled ▼	OUI ▼

Save

Reset

Voice VLAN Configuration interface

The following table describes the labels in this screen

Label	Description
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. Possible port modes are: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced: Force join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: Enabled: Enable Voice VLAN security mode operation. Disabled: Disable Voice VLAN security mode operation.
Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP.
Save	Click to save changes.
Reset :	Click to undo any changes made locally and revert to previously saved values.

Voice VLAN OUI Table

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Add New Entry

Save **Reset**

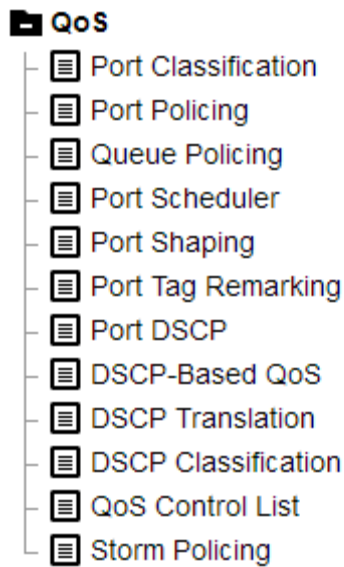
Voice VLAN OUI Table interface

The following table describes the labels in this screen

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Add New Entry	Click to add a new access management entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11 QoS

Refers to a network can use a variety of basic technology, to provide better services for the specified network communication ability, is a kind of network security mechanism, is used to solve the problem of network delay and blocking a technology.



Menu navigation window interface

5.1.11.1. QoS Ingress Port Classification

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<> ▼	<> ▼	<> ▼	<> ▼		☐	<> ▼
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼

QoS Ingress Port Classification interface

The following table describes the labels in this screen

Label	Description
Port	The port number for which the configuration below applies.
CoS	Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class.	Shows the classification mode for tagged frames on this port. Disabled: Use default CoS and DPL for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.2. QoS Ingress Port Policers

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	500	kbps	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐

Save

Reset

QoS Ingress Port Policers interface

The following table describes the labels in this screen

Label	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the port policer for this switch port.
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.
Unit	Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

Label	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.3. QoS Ingress Queue Policers

QoS Ingress Queue Policers

	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
Port	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐

Save **Reset**

QoS Ingress Queue Policers interface

The following table describes the labels in this screen

5.1.11.4. QoS Egress Port Schedulers

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

QoS Egress Port Schedulers interface

The following table describes the labels in this screen

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

5.1.11.5. QoS Egress Port Shapers

QoS Egress Port Shapers

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-

QoS Egress Port Shapers interface

The following table describes the labels in this screen

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Qn	Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".
Port	Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

5.1.11.6. QoS Egress Port Tag Remarking

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

QoS Egress Port Tag Remarking interface

The following table describes the labels in this screen

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
Mode	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

5.1.11.7. QoS Port DSCP Configuration

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable
11	☐	Disable	Disable
12	☐	Disable	Disable

QoS Port DSCP Configuration interface

The following table describes the labels in this screen

Label	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate 2. Classify
Translate	To Enable the Ingress Translation click the checkbox.

Classify	Classification for a port have 4 different values. Disable: No Ingress DSCP Classification. DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of - Disable: No Egress rewrite. Enable: Rewrite enabled without remapping. Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.8. DSCP-Based QoS Ingress Classification

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<> ▼	<> ▼
0 (BE)	☐	0 ▼	0 ▼
1	☐	0 ▼	0 ▼
2	☐	0 ▼	0 ▼
3	☐	0 ▼	0 ▼
4	☐	0 ▼	0 ▼
5	☐	0 ▼	0 ▼
6	☐	0 ▼	0 ▼
7	☐	0 ▼	0 ▼
8 (CS1)	☐	0 ▼	0 ▼

Save

Reset

DSCP-Based QoS Ingress Classification interface

The following table describes the labels in this screen

Label	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS Class
DPL	Drop Precedence Level (0-1)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.9. DSCP Translation

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)

Save **Reset**

DSCP Translation interface

The following table describes the labels in this screen

Label	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - 1. Translate 2. Classify
Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side - 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.
Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.10. DSCP Classification

DSCP Classification

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

5.1.11.11.

DSCP Classification interface

The following table describes the labels in this screen

Label	Description
QoS Class	Actual QoS class.
SCP DP0	Select the classified DSCP value (0-63) for Drop Precedence Level 0.
DSCP DP1	Select the classified DSCP value (0-63) for Drop Precedence Level 1.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11.12. QoS Control List Configuration**QoS Control List Configuration**

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
															

QCE Configuration

Port Members											
1	2	3	4	5	6	7	8	9	10	11	12
☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Key Parameters		Action Parameters	
DMAC	Any	CoS	0
SMAC	Any	DPL	Default
Tag	Any	DSCP	Default
VID	Any	PCP	Default
PCP	Any	DEI	Default
DEI	Any	Policy	
Frame Type	Any		

QoS Control List Configuration interface

The following table describes the labels in this screen

Label	Description
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE or 'Any'.
DMAC	Indicates the destination MAC address. Possible values are: Any: Match any DMAC. Unicast: Match unicast DMAC. Multicast: Match multicast DMAC. Broadcast: Match broadcast DMAC. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on destination addresses, this field indicates the DMAC.
Tag Type	Indicates tag type. Possible values are: Any: Match tagged and untagged frames. Untagged: Match untagged frames. Tagged: Match tagged frames. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.
Frame Type	Indicates the type of frame. Possible values are: Any: Match any frame type. Ethernet: Match EtherType frames. LLC: Match (LLC) frames. SNAP: Match (SNAP) frames. IPv4: Match IPv4 frames. IPv6: Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: CoS: Classify Class of Service. DPL: Classify Drop Precedence Level. DSCP: Classify DSCP value. PCP: Classify PCP value. DEI: Classify DEI value. Policy: Classify ACL Policy number.
Modification Buttons	You can modify each QCE (QoS Control Entry) in the table using the following buttons: Add: Inserts a new QCE before the current row. Edit: Edits the QCE. Up: Moves the QCE up the list. Down: Moves the QCE down the list. Delete: Deletes the QCE. Add: The lowest plus sign adds a new entry at the bottom of the QCE listings.

5.1.11.13. Global Storm Policer Configuration

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☐	1	fps ▼
Multicast	☐	1	fps ▼
Broadcast	☐	1	fps ▼

Global Storm Policer Configuration interface

The following table describes the labels in this screen

Label	Description
Frame Type	The frame type for which the configuration below applies.
Enable	Enable or disable the global storm policer for the given frame type.
Rate	Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.
Unit	Controls the unit of measure for the global storm policer rate as fps or kfps.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.12 IGMP Snooping

Igmp Snooping, short for Internet Group Management Protocol Snooping, is a multicast constraint that runs on two-level devices for Management and control multicast groups.

- IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - Status
 - Groups Information
 - Port Filtering Profile
 - IPv4 SFM Information

Menu navigation window interface

5.1.12.1. IGMP Snooping Configuration&Port Related Configuration

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv4 Flooding Enabled	☒
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited

The following table describes the labels in this screen

Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting

IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.12.2. IGMP Snooping VLAN Configuration

IGMP Snooping VLAN Configuration

Refresh << >>

Start from VLAN with entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	------------------	-----------------	---------------	-----	----	----------	---------------	----------------	-----------

Add New IGMP VLAN

Save Reset

IGMP Snooping VLAN Configuration interface

The following table describes the labels in this screen

Label	Description
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.
Refresh	Refresh: Refreshes the displayed table starting from the "VLAN" input fields.
 <<	<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
 <<	Updates the table, starting with the entry after the last entry currently displayed.
add new IGMP VLAN	Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.12.3. IGMP Snooping Status

IGMP Snooping Status

Auto-refresh ☐

Refresh

Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

IGMP Snooping Status interface

The following table describes the labels in this screen

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.

5.1.12.4. IGMP Snooping Group Information

IGMP Snooping Group Information

 Auto-refresh ☐ Refresh |<< >>

 Start from VLAN and group address with entries per page.

		Port Members											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12
No more entries													

IGMP Snooping Group Information interface

The following table describes the labels in this screen

Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.
Refresh:	Refreshes the displayed table starting from the input fields.
<<	Updates the table, starting with the first entry in the IGMP Group Table.
>> :	Updates the table, starting with the entry after the last entry currently displayed.

5.1.12.5. IGMP Snooping Port Filtering Profile Configuration

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile		
1			- ▼
2			- ▼
3			- ▼
4			- ▼
5			- ▼
6			- ▼

IGMP Snooping Port Filtering Profile Configuration interface

The following table describes the labels in this screen

Label	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile Management Button	You can inspect the rules of the designated profile by using the following button: Navigate: List the rules associated with the designated profile.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.12.6. IGMP SFM Information

Auto-refresh ☐ Refresh << >>

IGMP SFM Information

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

IGMP SFM Information interface

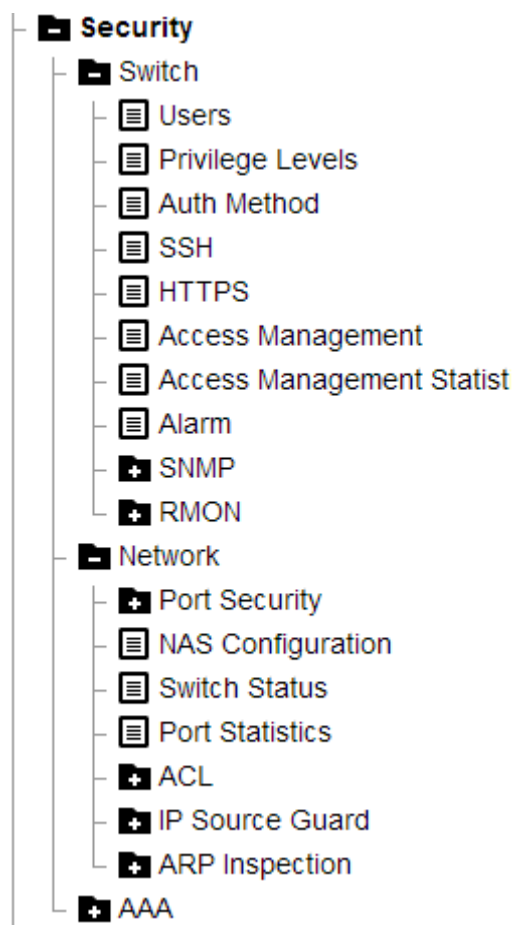
The following table describes the labels in this screen

Label	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address	IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.
Refresh	Refreshes the displayed table starting from the input fields.
<< :	Updates the table starting from the first entry in the IGMP SFM Information Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.2 Security

Three useful features can improve the security of switches: switch security, network security, AAA..



Menu navigation window interface

5.2.1 Switch

5.2.2.1. Users Configuration

Users Configuration

User Name	Privilege Level
admin	15

Add New User

Users Configuration interface

The following table describes the labels in this screen

Label	Description
User Name	The name identifying the user. This is also a link to Add/Edit User.
Privilege Level	The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Add New User	Click to add a new user.

5.2.2.2. Privilege Level Configuration

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
DDMI	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
DHCP	5 ▼	10 ▼	5 ▼	10 ▼
DHCPv6_Client	5 ▼	10 ▼	5 ▼	10 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
EEE	5 ▼	10 ▼	5 ▼	10 ▼
EPS	5 ▼	10 ▼	5 ▼	10 ▼
ERPS	5 ▼	10 ▼	5 ▼	10 ▼

Save

Reset

Privilege Level Configuration interface

The following table describes the labels in this screen

Label	Description
Group Name	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: System: Contact, Name, Location, Timezone, Daylight Saving Time, Log. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. IP: Everything except 'ping'. Port: Everything except 'VeriPHY'. Diagnostics: 'ping' and 'VeriPHY'. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI.
Privilege Levels	Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.3. Authentication Method Configuration

Authentication Method Configuration

Client	Methods		
console	local ▼	no ▼	no ▼
telnet	local ▼	no ▼	no ▼
ssh	local ▼	no ▼	no ▼
http	local ▼	no ▼	no ▼

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no ▼	0	☐
telnet	no ▼	0	☐
ssh	no ▼	0	☐

Accounting Method Configuration

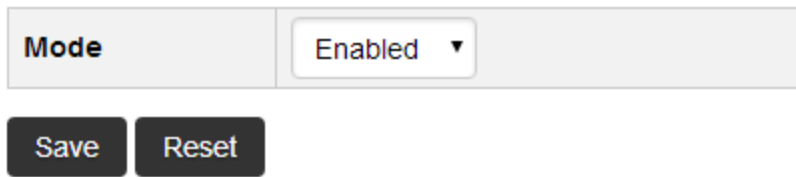
Client	Method	Cmd Lvl	Exec
console	no ▼		☐
telnet	no ▼		☐
ssh	no ▼		☐

The following table describes the labels in this screen

Label	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: no: Authentication is disabled and login is not possible. local: Use the local user database on the switch for authentication. radius: Use remote RADIUS server(s) for authentication. tacacs: Use remote TACACS+ server(s) for authentication. Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.
Label	Description
Client	The management client for which the configuration below applies.
Method	Method can be set to one of the following values: no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level. tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
Cmd Lvl	Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
Cfg Cmd	Also authorize configuration commands.
Label	Description
Client	The management client for which the configuration below applies.
Method	Method can be set to one of the following values: no: Accounting is disabled. tacacs: Use remote TACACS+ server(s) for accounting.
Cmd Lvl	Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
Exec	Enable exec (login) accounting.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.4. SSH Configuration

SSH Configuration



Mode: Enabled ▼

Save Reset

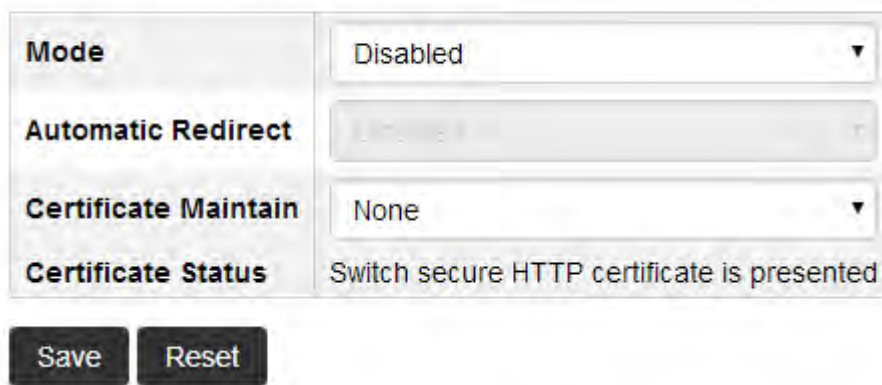
SSH Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.5. HTTPS Configuration

HTTPS Configuration



Mode: Disabled ▼

Automatic Redirect: Disable ▼

Certificate Maintain: None ▼

Certificate Status: Switch secure HTTP certificate is presented

Save Reset

HTTPS Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Indicate the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation.
Certificate Maintain	The operation of certificate maintenance. Possible operations are: None: No operation. Delete: Delete the current certificate. Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL. Generate: Generate a new self-signed RSA certificate.
Certificate Pass Phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload	Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: Web Browser: Upload a certificate via Web browser. URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
Certificate Status	Display the current status of certificate on the switch. Possible statuses are: Switch secure HTTP certificate is presented. Switch secure HTTP certificate is not presented. Switch secure HTTP certificate is generating ...
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

5.2.2.6. Access Management Configuration

Access Management Configuration

Mode Disabled ▼

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	☐	☐	☐

Add New Entry

Save Reset

Access Management Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP address	Indicates the start IP address for the access management entry.
End IP address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
Add New Entry	Click to add a new access management entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.7. Management Statistics

Access Management Statistics

Auto-refresh ☐ [Refresh](#) [Clear](#)

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Access Management Statistics interface

The following table describes the labels in this screen.

Label	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.
Refresh	Click to refresh the page immediately.
Clear	Clear all statistics.

5.2.2.8. Alarm Configuration

Alarm Configuration

Dual Power Alarm	Disabled ▼
------------------	------------

Port Link Down Alarm

Port	Link Down Alarm
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼



Alarm Configuration interface

The following table describes the labels in this screen.

Label	Description
Dual Power Alarm	Indicates the alarm mode operation. Possible modes are: Enabled: Enable alarm mode operation. Disabled: Disable alarm mode operation. If enabled, when any one of the power loss, the alarm LED is on, and the alarm relay is change.
Port Link Down Alarm	Indicates the alarm mode operation. Possible modes are: Enabled: Enable alarm mode operation. Disabled: Disable alarm mode operation. If enabled, when port link-down, the alarm LED is on, and the alarm relay is change.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.9. SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems identify network problems by receiving traps or change notices from network devices implementing SNMP.

5.2.2.1. SNMP System Configuration

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	1.3.6.1.4.1.12345.1.1

Save Reset

SNMP System Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled : Enable SNMP mode operation. Disabled : Disable SNMP mode operation.
SNMP Version	Indicates the SNMP supported version. Possible versions are: SNMP v1 : Set SNMP supported version 1. SNMP v2c : Set SNMP supported version 2c. SNMP v3 : Set SNMP supported version 3.
Read Community Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.
Save	Save: Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.2. Trap Configuration

A trap manager is a management station that receives traps or system alerts generated by the switch. If no trap manager is defined, no traps will be issued. You can create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager enter the SNMP community strings and select the SNMP version.

Trap Configuration

Global Settings

Mode	Disabled ▼
------	------------

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
Add New Entry Save Reset					

Trap Configuration interface

SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled ▼
Trap Version	SNMP v2c ▼
Trap Community	Public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled ▼
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled ▼
Trap Security Engine ID	
Trap Security Name	None ▼

SNMP Trap Event

System	☐ *	Power ☐ Power 1 ☐ Power 2	☐ Cold Start
Interface	☐ *	Link up ☒ none ☐ specific ☐ all switches	
		Link down ☒ none ☐ specific ☐ all switches	
		LLDP ☒ none ☐ specific ☐ all switches	
Authentication	☐ *	☐ SNMP Authentication Fail	
Switch	☐ *	☐ STP	☐ RMON

The following table describes the labels in this screen.

Label	Description
Mode	Indicates the trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Config Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Trap Mode	Indicates the trap destination mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMPv1: Set SNMP trap supported version 1. SNMPv2c: Set SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3.
Trap Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.
Trap Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.
System	Enable/disable that the Interface group's traps. Possible traps are: Warm Start: Enable/disable Warm Start trap. Cold Start: Enable/disable Cold Start trap.
Interface	Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Link Up: Enable/disable Link up trap. Link Down: Enable/disable Link down trap. LLDP: Enable/disable LLDP trap.
Authentication	Indicates that the authentication group's traps. Possible traps are: SNMP Authentication Fail : Enable/disable SNMP trap authentication failure trap.
Switch	Indicates that the Switch group's traps. Possible traps are: STP: Enable/disable STP trap. RMON: Enable/disable RMON trap.
Add New Entry	Click to add a new user.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.3. SNMPv3 Community Configuration

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0
Delete		0.0.0.0	0.0.0.0

SNMPv3 Community Configuration interface

The following table describes the labels in this screen

Label	Description
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask
Delete	Check to delete the entry. It will be deleted during the next save.
Add New Entry	Click to add a new user.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.4. SNMPv3 User Configuration

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete			Auth, Priv	MD5		DES	

SNMPv3 User Configuration interface

The following table describes the labels in this screen

Label	Description
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: No authentication protocol. MD5: An optional flag to indicate that this user uses MD5 authentication protocol. SHA: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists.
Authentication Password	A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: No privacy protocol. DES: An optional flag to indicate that this user uses DES authentication protocol. AES: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.
Delete	Check to delete the entry. It will be deleted during the next save.
Add New Entry	Click to add a new user.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.5. SNMPv3 Group Configuration

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

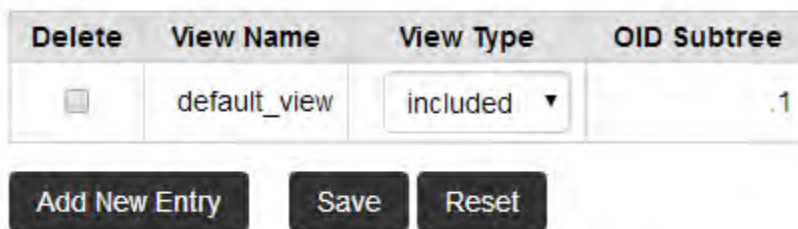
SNMPv3 Group Configuration interface

The following table describes the labels in this screen

Label	Description
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Delete	Check to delete the entry. It will be deleted during the next save.
Add New Entry	Click to add a new user.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.6. SNMPv3 View Configuration

SNMPv3 View Configuration



The screenshot shows the SNMPv3 View Configuration interface. It features a table with four columns: Delete, View Name, View Type, and OID Subtree. The 'Delete' column contains a checkbox. The 'View Name' column contains the text 'default_view'. The 'View Type' column contains a dropdown menu with 'included' selected. The 'OID Subtree' column contains the text '.1'. Below the table are three buttons: 'Add New Entry', 'Save', and 'Reset'.

SNMPv3 View Configuration interface

The following table describes the labels in this screen

Label	Description
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
Delete	Check to delete the entry. It will be deleted during the next save.
Add New Entry	Click to add a new view entry.

Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.7. SNMPv3 Access Configuration

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
☐	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

SNMPv3 Access Configuration interface

The following table describes the labels in this screen

Label	Description
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Any security model accepted(v1 v2c usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Delete	Check to delete the entry. It will be deleted during the next save.
Add New Entry	Click to add a new access entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.10. RMON

5.2.2.8. RMON Statistics Configuration

RMON Statistics Configuration

Delete	ID	Data Source
Add New Entry Save Reset		

RMON Statistics Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
Add New Entry	Click to add a new community entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.9. RMON Statistics Status Overview

Auto-refresh ☐

Refresh

<<

>>

RMON Statistics Status Overview

Start from Control Index with entries per page.

Data Source ID (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Bytes	64 ~ 127	65 ~ 128	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

RMON Statistics Status Overview interface

The following table describes the labels in this screen

Label	Description
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address

Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.
Frag	The number of frames which size is less than 64 octets received with invalid CRC
Jabb	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll	The best estimate of the total number of collisions on this Ethernet segment.
64	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.
Refresh	Click to refresh the page immediately.
<<	Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
<<	Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

5.2.2.10. RMON History Configuration

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

RMON History Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
Buckets Granted	The number of data shall be saved in the RMON.
Add New Entry	Click to add a new community entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.11. RMON History Overview

Auto-refresh ☐ Refresh << >>

RMON History Overview

Start from Control Index and Sample Index with entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

RMON History Overview interface

The following table describes the labels in this screen

Label	Description
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.

CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
Refresh	Click to refresh the page immediately.
 <<	Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.2.2.12. RMON Alarm Configuration

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold
Delete		30	.1.3.6.1.2.1.2.2.1.0.0	Delta	0	RisingOrFalling	0	0	0

RMON Alarm Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2 ³¹ -1.

Variable	Indicates the particular variable to be sampled, the possible variables are: InOctets: The total number of octets received on the interface, including framing characters. InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded even the packets are normal. InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit. OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. OutDiscards: The number of outbound packets that are discarded event the packets is normal. OutErrors: The The number of outbound packets that could not be transmitted because of errors. OutQLen: The length of the output packet queue (in packets).
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: Absolute: Get the sample directly. Delta: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: RisingTrigger alarm when the first value is larger than the rising threshold. FallingTrigger alarm when the first value is less than the falling threshold. RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling	Falling event index (1-65535).
Add New	Click to add a new community entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.13. RMON Alarm Overview

RMON Alarm Overview

 Auto-refresh ☐ **Refresh** |<< >>

 Start from Control Index with entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

RMON Alarm Overview interface

The following table describes the labels in this screen

Label	Description
ID	Indicates the index of Alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds
Value	The value of the statistic during the last sampling period.
Startup Alarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	Rising threshold value.
Rising Index	Rising event index.
Falling Threshold	Falling threshold value
Falling Index	Falling event index.
Refresh	Click to refresh the page immediately.
<<	Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.2.2.14. RMON Event Configuration

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
Add New Entry Save Reset					

RMON Event Configuration interface

The following table describes the labels in this screen

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event, the possible types are: none: No SNMP log is created, no SNMP trap is sent. log: Create SNMP log entry when the event is triggered. snmptrap: Send SNMP trap when the event is triggered. logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.
Community	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.
Add New Entry	Click to add a new community entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.15. RMON Event Overview

RMON Event Overview

Auto-refresh ☐ Refresh << >>

Start from Control Index and Sample Index with entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

RMON Event Overview interface

The following table describes the labels in this screen

Label	Description
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
LogTime	Indicates Event log time
LogDescription	Indicates the Event description
Refresh	Click to refresh the page immediately.
<<	Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.2.2 Network

5.2.2.16. Port Security

5.2.2.17. Limit Control

Port Security Limit Control Configuration

System Configuration

Mode	Disabled ▼
Aging Enabled	☐
Aging Period	seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<> ▼	4	<> ▼		
1	Disabled ▼		None ▼	Disabled	Reopen
2	Disabled ▼		None ▼	Disabled	Reopen
3	Disabled ▼		None ▼	Disabled	Reopen

Port Security Limit Control Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode	Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period

Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.
Port	The port number to which the configuration below applies.
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses
Action	If Limit is reached, the switch can take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action. Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button. Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: Disabled: Limit Control is either globally disabled or disabled on the port. Ready: The limit is not yet reached. This can be shown for all actions. Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown
Re-open Button	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.
Refresh	Click to refresh the page. Note that non-committed changes will be lost.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.18. Switch

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-

Port Security Switch Status interface

The following table describes the labels in this screen.

Label	Description
User Module Name	The full name of a module that may request Port Security services
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
MAC Count (Current, Limit)	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).
Refresh	Click to refresh the page immediately.

5.2.2.19. Port Security Port Status Port 1

Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Port Security Port Status Port 1 interface

The following table describes the labels in this screen.

Label	Description
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.
Refresh	Click to refresh the page immediately.

5.2.2.20. Network Access Server Configuration

Network Access Server Configuration

System Configuration

Mode	Disabled ▼
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<> ▼	☐	☐	☐			
1	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

The following table describes the labels in this screen.

Label	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames
Reauthentication Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Guest VLAN ID	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
Max. Reauth. Count	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X, Multi 802.1X, MAC-based Auth.,

RADIUS-Assigned QoS Enabled	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: • All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].
------------------------------------	--

RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
-------------------------------------	---

Guest VLAN Enabled	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • Port-based 802.1X • Single 802.1X • Multi 802.1X For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
Port State	The current state of the port. It can undertake one of the following values: Globally Disabled: NAS is globally disabled. Link Down: NAS is globally enabled, but there is no link on the port. Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.
Refresh	Click to refresh the page.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.21. Network Access Server Switch Status

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	

Network Access Server Switch Status interface

The following table describes the labels in this screen.

Label	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.
Refresh	Click to refresh the page immediately.

5.2.2.22. NAS Statistics Port 1

NAS Statistics Port 1

Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

NAS Statistics Port 1 interface

The following table describes the labels in this screen.

Label	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.

5.2.2.23. ACL

5.2.2.24. ACL Ports Configuration

ACL Ports Configuration Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
+	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	+
1	0	Permit	Disabled	Disabled		Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled		Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled		Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Save Reset

ACL Ports Configuration interface

The following table describes the labels in this screen.

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".
EVC Policer	Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.
EVC Policer ID	Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled.
State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the number of frames that match this ACE.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear the counters.

5.2.2.25. ACL Rate Limiter Configuration

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps

Save

Reset

ACL Rate Limiter Configuration interface

The following table describes the labels in this screen.

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
Rate	The valid rate is 0-3276700 in pps. or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	Specify the rate unit. The allowed values are: pps: packets per second. kbps: Kbits per second.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.26. Access Control List Configuration

Access Control List Configuration

Auto-refresh ☐ **Refresh** **Clear** **Remove All**

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	Actions
									

Access Control List Configuration interface

The following table describes the labels in this screen.

Label	Description
ACE	Indicates the ACE ID.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE

Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons: Add: Inserts a new ACE before the current row. Edit: Edits the ACE row. Up: Moves the ACE up the list. Down: Moves the ACE down the list. Delete: Deletes the ACE. Add: The lowest plus sign adds a new entry at the bottom of the ACE listings.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear the counters.
Remove All	Click to remove all ACEs.

5.2.2.27. ACL Status

ACL Status

combined ☐ Auto-refresh ☐ Refresh

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
ring	1	SNAP	Deny	Disabled	Disabled	No	0	No

ACL Status interface

The following table describes the labels in this screen.

Label	Description
User	Indicates the ACL user.
ACE	Indicates the ACE ID on local switch.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled
CPU	Forward packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.
Refresh	Click to refresh the page.

5.2.2.28. IP Source Guard

5.2.2.29. IP Source Guard Configuration

IP Source Guard Configuration

Mode

Disabled ▼

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<> ▼	<> ▼
1	Disabled ▼	Unlimited ▼
2	Disabled ▼	Unlimited ▼
3	Disabled ▼	Unlimited ▼

Save

Reset

The following table describes the labels in this screen.

Label	Description
Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Translate dynamic to static	Click to translate all dynamic entries to static entries.

5.2.2.30. Static IP Source Guard Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
--------	------	---------	------------	-------------

Add New Entry

Save

Reset

Static IP Source Guard Table interface

The following table describes the labels in this screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next
Port	The logical port for the settings.
VLAN ID	The vlan id for the settings.
IP Address	Allowed Source IP address.
MAC address	Allowed Source MAC address.
Add New Entry	Click to add a new entry to the Static IP Source Guard table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.31. Dynamic IP Source Guard Table

Dynamic IP Source Guard Table

Start from , VLAN and IP address with entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Dynamic IP Source Guard Table interface

The following table describes the labels in this screen.

Label	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the IP traffic is permitted.
IP Address	User IP address of the entry.
MAC Address	Source MAC address.
Refresh	Refreshes the displayed table starting from the input fields.
Clear	Flushes all dynamic entries.
 << :	Updates the table starting from the first entry in the Dynamic IP Source Guard Table.
>> :	Updates the table, starting with the entry after the last entry currently displayed.

5.2.2.32. ARP Inspection

5.2.2.33. ARP Inspection Configuration

ARP Inspection Configuration

Mode

Disabled ▼

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	None ▼
2	Disabled ▼	Disabled ▼	None ▼
3	Disabled ▼	Disabled ▼	None ▼

Save

Reset

ARP Inspection Configuration interface

The following table describes the labels in this screen.

Label	Description
Mode of ARP Inspection Configuration	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port Mode Configuration	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are: Enabled: Enable ARP Inspection operation. Disabled: Disable ARP Inspection operation. If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: Enabled: Enable check VLAN operation. Disabled: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Translate dynamic to static	Click to translate all dynamic entries to static entries.

5.2.2.34. VLAN Mode Configuration

VLAN Mode Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Log Type
Add New Entry Save Reset		

VLAN Mode Configuration interface

The following table describes the labels in this screen.

Label	Description
VLAN Mode Configuration	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.
Add New Entry	Click to add a new VLAN to the ARP Inspection VLAN table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.35. Static ARP Inspection Table

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Add New Entry				
Save		Reset		

Static ARP Inspection Table interface

The following table describes the labels in this screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save
Port	The logical port for the settings.
VLAN ID	The vlan id for the settings.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.
Add New Entry	Click to add a new entry to the Static ARP Inspection table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2.36. Dynamic ARP Inspection Table

Dynamic ARP Inspection Table

Auto-refresh ☐
Refresh
|<<
>>

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Save
Reset

Dynamic ARP Inspection Table interface

The following table describes the labels in this screen.

Label	Description
Port	Switch Port Number for which the entries are displayed

VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.
Translate to static	Select the checkbox to translate the entry to static entry.
Refresh	Refreshes the displayed table starting from the input fields.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
 << :	Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>> :	Updates the table, starting with the entry after the last entry currently displayed.

5.2.2.37. Dynamic ARP Inspection Table

Dynamic ARP Inspection Table Auto-refresh ☐ Refresh |<< >>

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Dynamic ARP Inspection Table interface

The following table describes the labels in this screen.

Label	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.
Refresh	Refreshes the displayed table starting from the input fields.
Clear	Flushes all dynamic entries.
 <<	Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.3 AAA

5.3.1 RADIUS Server Configuration

RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Add New Server						
Save Reset						

RADIUS Server Configuration interface

The following table describes the labels in this screen.

Label	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
NAS-IP-Address (Attribute 4)	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95)	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier (Attribute 32)	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server
Auth Port	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key
Add New Server	Click Add New Server to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.
Delete	The Delete button can be used to undo the addition of the new server.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.3.2 RADIUS Server Status Overview

RADIUS Server Status Overview

Auto-refresh ☐ **Refresh**

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

RADIUS Server Status Overview interface

The following table describes the labels in this screen.

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address of this server.
Authentication Port	UDP port number for authentication.
Authentication Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Accounting Port	UDP port number for accounting.
Accounting Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Refresh	Click to refresh the page immediately.

5.3.3 RADIUS Authentication Statistics for Server #1

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State	Disabled		
Round-Trip Time	0 ms		

The following table describes the labels in this screen.

Label	Description
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Unknown Types	The number of RADIUS packets that were received with unknown types
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Access Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Timeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
IP Address	IP address and UDP port for the authentication server in question
State	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Responses	The number of RADIUS packets (valid or invalid) received from the server.
Malformed Responses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Unknown Types	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason
Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Pending Requests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
IP Address	IP address and UDP port for the accounting server in question.
State	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

5.3.4 TACACS+ Server Configuration

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key
Add New Server				
Save Reset				

TACACS+ Server Configuration interface

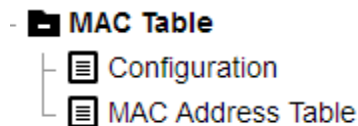
The following table describes the labels in this screen.

Label	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

5.4 MAC Table

The switching of frames is based on the source MAC address in the frame. The switch creates a table that maps the MAC address to the switch port, which contains static and dynamic MAC addresses. If you want to make a fixed mapping between the DMAC address and the switch port, you need to configure a static MAC.

The switch automatically updates the dynamic MAC address table according to the source MAC address of the frame. If the MAC address is not received after the aging time, the dynamic mac address is removed from the MAC table



Menu navigation window interface

MAC Address Table Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging. Change aging time to 200 seconds

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	☐
Aging Time	200 seconds

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
Add New Static Entry														

Change aging time to 200 seconds interface

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

The following table describes the labels in this screen.

Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Add a static MAC address entry to the MAC address table. Add static MAC address:

00:00:00:00:00:0f to port 3 of VLAN 2

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
Delete	2	00-00-00-00-00-00	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐
Add New Static Entry														
Save Reset														

Add static MAC address: 00:00:00:00:00:0f in VLAN 2 on port 3

The following table describes the labels in this screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add New Static Entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.1 MAC Address Table

MAC Address Table

 Auto-refresh ☐ Refresh Clear |<< >>

 Start from VLAN and MAC address with entries per page.

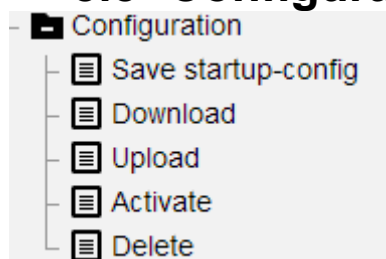
			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00-E0-4C-77-3A-9E					✓								
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-10-00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	80-EE-73-3A-33-AA								✓					
Dynamic	1	84-79-73-21-4B-30								✓					
Static	1	BC-9C-C5-00-10-00	✓												
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

MAC Address Table interface

The following table describes the labels in this screen.

Label	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.
Refresh	Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
Clear	Flushes all dynamic entries.
<<	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>	Updates the table, starting with the entry after the last entry currently displayed.

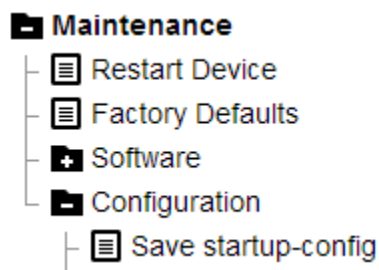
5.5 Configuration



Menu navigation window interface

5.5.1 Save Running Configuration to startup-config

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.



Menu navigation window interface

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

Save Running Configuration to startup-config interface

5.5.2 Download Configuration

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
☐ running-config
☐ default-config
☐ startup-config

Download Configuration

Download Configuration interface

Download: It is possible to download any of the files on the switch to the web browser.

Select the file and click Download Configuration.

Download of running-config may take a little while to complete, as the file must be prepared for download.

5.5.3 Upload Configuration

Upload Configuration

File To Upload

Destination File

File Name	Parameters
☐ running-config	☒ Replace ☐ Merge
☐ startup-config	
☐ Create new file	

Upload Configuration interface

It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

Select the file to upload, select the destination file on the target, then click Upload Configuration.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

Merge mode: The uploaded file is merged into running-config.

If the flash file system is full (i.e. contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

5.5.4 Activate Configuration

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

Activate Configuration interface

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

5.5.5 Delete Configuration File

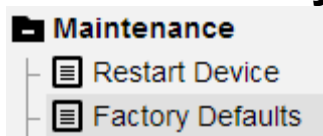
Delete Configuration File

Select configuration file to delete.

Delete Configuration File interface

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

5.6 Factory Default



Menu navigation window interface

Factory Defaults

Factory Default interface

The following table describes the labels in this screen.

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

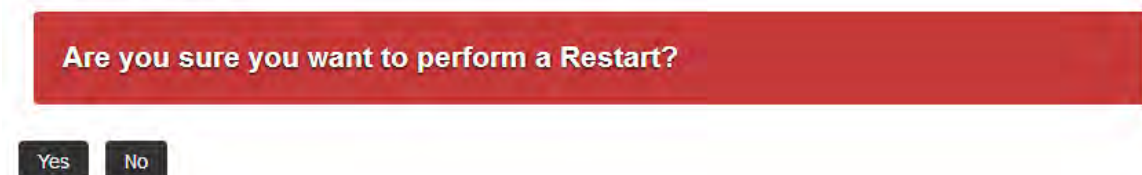
5.7 Restart Device

Maintenance

Restart Device

Menu navigation window interface

Restart Device



Restart Device interface

The following table describes the labels in this screen.

Label	Description
Yes	Click to restart device.
No	Click to return to the Port State page without restarting.

Command Line Interface Management

6.1 About CLI Management

Besides WEB-based management, the MS10GT8GX2-R also supports CLI management.

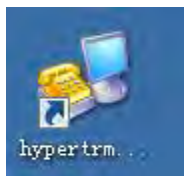
You can use console or telnet to manage the switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

To configure the switch via RS-232 serial console, use an enclosed RJ-45 to DB9 cable to connect the Console port on the switch to COM port on the computer.

Follow the steps below to access the console via RS-232 serial cable. The following is an example of opening Windows XP with HyperTerminal.

Step 1. Click on the HyperTerminal



Step 2. Input a name for new connection



Step 3. Select the appropriate COM port number.



Step 4. The COM port should be set to the following:

Bits per second: 115200

data bits: 8

Parity: None

Stop bits: 1

Flow control: None



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press “Enter”.

```
Username: admin
Password:
#
```

CLI Management by Telnet

Users can use “TELNET” to configure the switches.

IP Address: **192.168.0.2**

Subnet Mask: **255.255.255.0**

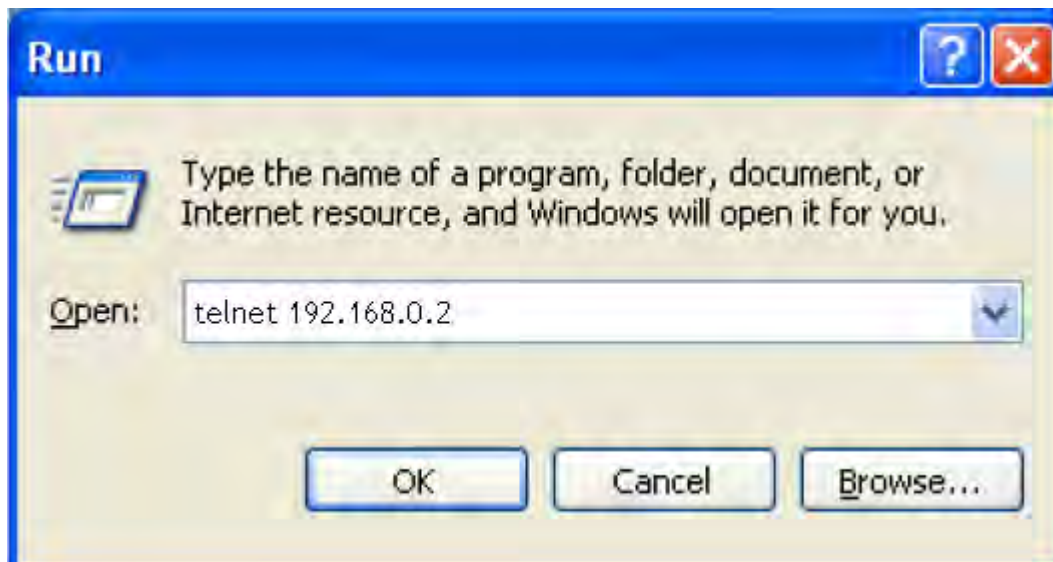
Default Gateway: **192.168.0.1**

User Name: **admin**

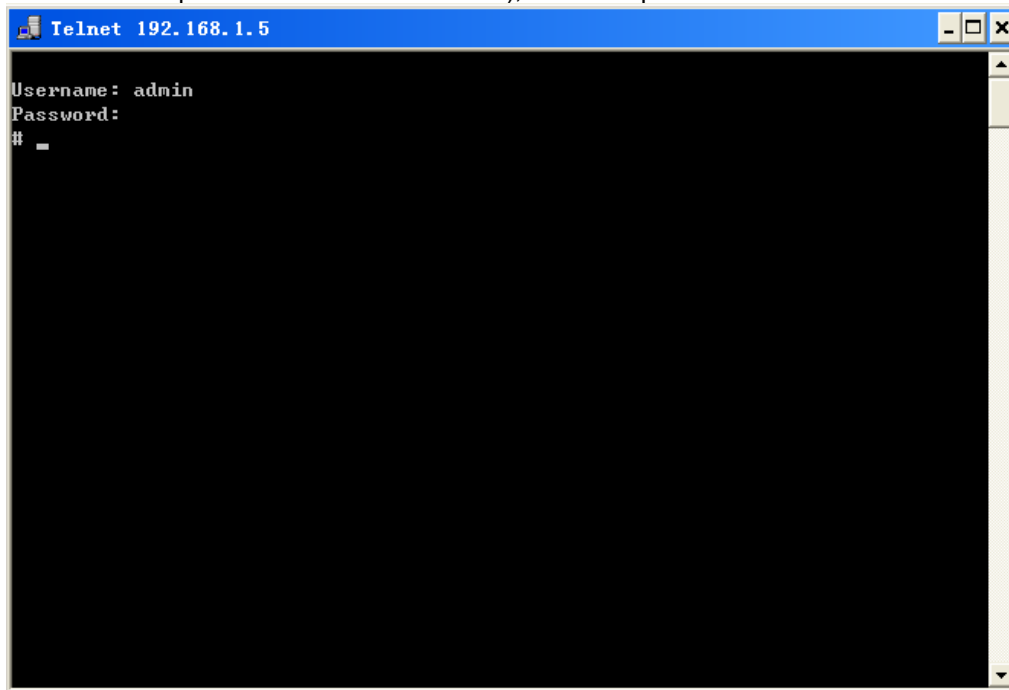
Password: **123**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows “Run” command as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press "Enter".



Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
Privileged EXEC	Begin a session with your switch.	#	To exit to User EXEC mode, enter disable	The privileged command is advance mode Privileged this mode to Display advance function status save configures
User EXEC	Enter the disable command while in Privileged EXEC mode.	>	Enter exit or logout	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to Enter menu mode. Display system information.
Global configuration	Enter the configure terminal command while in privileged EXEC mode.	(config)#	To exit to privileged EXEC mode, enter exit .	Use this mode to configure parameters that apply to your Switch as a whole.
VLAN configuration	Enter the interface vlan command while Global configuration mode.	(config-if-vlan)#	To exit to Global configuration mode, enter exit .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in Global configuration mode	(config-if)#	To exit to global configuration mode, Enter exit . To exist privileged EXEC mode or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level.

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

6.2 Commands Set List—System Commands Set

MS10GT8GX2 Commands	Level	Description	Example
show	P	Show running system information	#show
configure terminal	P	Enter global configuration mode	# configure terminal
username <username> privilege <priv> password encrypted <encry_password>	G	Add or modify the user and password of the privileged user configuration mode	(config)# username admin privilege 15 password unencrypted 123
exit	G	From the current mode, enter the previous mode,	(config)# exit
?	P	Outputs a brief description of the command interpreter help system	# show ?
hostname <hostname>	G	Sets the prompt for the switch's command line interface.	Set the prompt to Test. (Config)#hostname Test
reload cold	P	Reboot the switch	# reload cold
reload default	P	Restore the factory settings of the switch	# reload default
copy running-config startup-config	P	Save the current runtime configuration parameters to Flash Memory.	# copy running-config startup-config Building configuration... % Saving 1522 bytes to flash:startup-config
ping	P	The switch sends an ICMP request packet to the remote device to check whether the switch is reachable with the remote device.	#ping ip 192.168.0.200
hostname [hostname]	G	Configure system name	(config)# hostname
show system[cpu leb] status	P	Display system information	# show system cpu status

ip address <ipv4_addr> <ipv4_netmask>	v	Configure the IP address of switch	(config-if-vlan)# ip address 192.168.0.2 255.255.255.0
ip dhcp server	v	Enable DHCP client function of switch	(config-if-vlan)# ip dhcp server
show interface vlan <vlan_list>	p	Show IP information of switch	# show interface vlan 1
no ip dhcp server	G	Disable DHCP client function of switch	(config)# no ip dhcp server

6.3 Commands Set List—Port Commands Set

MS10GT8GX2 Commands	Level	Description	Example
interface GigabitEthernet <port_type_list>	I	Choose the port for modification.	(config)# interface GigabitEthernet 1/1
Duplex { half full auto }	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	(config-if)# duplex half
speed [10 100 1000 auto]	I	Sets the rate of the specified port. Parameters: auto for the automatic negotiation rate; 10 for the mandatory 10Mbit / s; 100 for the mandatory 100Mbit / s; 1000 for the mandatory 1000Mbit / s.	(config-if)# speed 1000
flowcontrol {on off }	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	(config-if)# flowcontrol on
no flowcontrol	I	Disable flow control of interface	(config-if)# flowcontrol off
shutdown	I	shutdown	(config-if)# shutdown
no shutdown	I	no shutdown	(config-if)# no shutdown
show interface GigabitEthernet <port_type_list> statistics	p	Displays information about the specified switch port	# show interface GigabitEthernet 1/1 statistics
clear statistics GigabitEthernet <port_type_list>	p	Clear the Ethernet port statistics	# clear statistics GigabitEthernet 1/2
show monitor session all	p	Displays information about the mirror source, destination port	# show monitor session all
show interface GigabitEthernet <port_type_list> status	p	show interface actual status	# show interface GigabitEthernet 1/2 status

6.4 Commands Set List—Trunk command set

MS10GT8GX2 Commands	Level	Description	Example
aggregation mode { [smac] [dmac] [ip] [port] }	G	Aggregation mode can be selected The source MAC address Destination MAC address The IP address One or more of the four TCP/UDP port Numbers	(config)# aggregation mode ip
aggregator group <uint>	I	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The	(config-if)#aggregator group 1
show aggregation	P	Show the information of trunk group	# show aggregation
no aggregation group <uint>	G	Remove a trunk group	(config-if)# no aggregation group 1

6.5 Commands Set List—VLAN command set

MS10GT8GX2 Commands	Level	Description	Example
vlan <vlan_list ISL VLAN IDs 1~4095 >	G	Enter VLAN configure mode	(config)# vlan 1
gvrp	I	To set switch VLAN mode.	(config-if)# gvrp
name <vlan-name>	V	Specify the VLAN name	(config-vlan)# name 2
No name <vlan-name>	V	Delete the VLAN name	(config-vlan)# no name 2
no vlan <vlan_list>	G	Disable vlan group(by VID)	(config)# no vlan 1
no gvrp	G	Disable GVRP	(config)# no gmrp
IEEE 802.1Q VLAN			
switchport mode { access trunk hybrid }	I	Sets the current port mode.	(config-if)# switchport mode trunk
switchport trunk allowed vlan { all none [add remove except] <vlan_list> }	I	Set or modify the trunk port to allow VLANs. The no operation of this command is to restore the default.	(config-if)# switchport trunk allowed vlan 1,3,5-20
no switchport trunk allowed vlan { all none [add remove except] <vlan_list> }	I	Delete the vlans allowed by the main port	(config-if)#no switchport trunk allowed vlan 1,3,5-20

switchport access vlan <vlan-id>	I	switchport access vlan 3	(config-if)# switchport mode access (config-if)# switchport access vlan 3
no switchport access vlan <vlan-id>	I	The operation of this command removes the current port from the VLAN	(config-if)# no switchport access vlan 3
switchport trunk native vlan <vlan-id>	I	Set the PVID of the trunk port. The no operation of this command is to restore the default value	(config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 100
show vlan <vlan-id>	P	Show VLAN information	#show vlan 2

6.6 Commands Set List—Spanning Tree command set

MS10GT8GX2 Commands	Level	Description	Example
spanning-tree mst <instance> priority <prio>	G	Configure spanning tree priority parameter	(config)# spanning-tree mst 0 priority 128
spanning-tree	I	Set the port to enable	(config-if)# spanning-tree
no spanning-tree	I	Set port disable	(config-if)# no spanning-tree
spanning-tree mst hello-time < hello-time >	G	Set the RSTP hello time. <Hello-time> is the hello time value, in seconds. The default value is 2, in the range of 1 to 10.	(config)# spanning-tree mst hello-time 3
spanning-tree mst forward-time <fwdtime>	G	Set the RSTP forward delay time. <Fwdtime> is the forward delay time value, in seconds. The default value is 15, in the range of 4 to 30.	(config)# spanning-tree mst forward-time 5
spanning-tree mst max-age <maxage> [forward-time <fwdtime>]	G	Set RSTP maximum lifetime. <Maxage> is the maximum lifetime value in seconds. The default value is 20, in the range of 6 to 40.	(config)# spanning-tree mst max-age 7
spanning-tree mode { stp rstp mstp }	G	Set the STP version. <Stp rstp mstp> for the STP version number, select rstp mode, in the mode behind the input rstp	(config)# spanning-tree mode stp
show spanning-tree	P	View RSTP information.	# show spanning-tree

6.7 Commands Set List—QoS command set

MS10GT8GX2 Commands	Level	Description	Example
qos trust [dscp tag] no qos trust [dscp tag]	I	Configure the port trust mode. The no operation of this command is to disable the current trust mode of the switch port.	(config-if)# qos trust tag
qos cos <cos> no qos cos <cos>	I	Configure the default CoS value for the port. The no operation of this command is to restore the default.	(config-if)# qos cos 2
qos dei <dei> no qos dei <dei>	I	Configure the port default DEI value. The no operation of this command is to restore the default.	(config-if)# qos dei 1
qos dpl <dpl> no qos dpl <dpl>	I	Configure the port default DPL value. The no operation of this command is to restore the default.	(config-if)# qos dpl 1
qos pcp <pcp> no qos pcp <pcp>	I	Configure the port default PCP value. The no operation of this command is to restore the default.	(config-if)# qos pcp 3
qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>	I	Configure the port PCP-CoS mapping. The no operation of this command is to restore the default.	(config-if)# qos map tag-cos pcp 7 dei 1 cos 7 dpl 0
qos policer <rate> [kbps mbps fps kfps] [flowcontrol] no qos policer	I	Configure the inbound direction rate of the port. The no operation of this command is to restore the default configuration.	(config-if)# qos policer 20 mbps
qos queue-policer queue <queue> <rate> [kbps mbps] no qos queue-policer queue <queue>	I	Configure the port inbound queue rate control. The no operation of this command restores the default configuration.	(config-if)# qos queue-policer queue 0 20 mbps
qos tag-remark { pcp <pcp> dei <dei> mapped } no qos tag-remark	I	Rewrite the port outbound priority; the no operation of this command is to restore the default configuration.	(config-if)# qos tag-remark pcp 7 dei 0
qos queue-shaper queue <queue> <rate> [kbps mbps] [excess] no qos queue-shaper queue <queue>	I	Configure the direction of the queue rate; the command no operation to restore the default configuration.	(config-if)#qos queue-shaper queue 1 200 mbps excess
qos wrr <weight0 weight1 weight2 weight3 weight4 weight5 > no qos wrr	I	Set the WRR weight of the switch port queue. The no operation of this command is to restore the default value.	(config-if)# qos wrr 1 2 4 4 8 8
show qos	P	Display the information of QoS configuration	# show qos

6.8 Commands SetList—IGMP snooping command set

MS10GT8GX2 Commands	Level	Description	Example
ip igmp snooping no ip igmp snooping	G	Enable IGMP snooping on the switch. The no operation of this command is to disable IGMP Snooping	(config)# ip igmp snooping
ip igmp snooping vlan <vlan_list> no ip igmp snooping vlan <vlan_list>	G	Enable IGMP snooping on the specified VLAN. The no operation of this command is to disable IGMP Snooping for the specified VLAN	(config)# ip igmp snooping vlan 100
show ip igmp snooping	P	Displays the details of an IGMP configuration.	#show ip igmp snooping

6.9 Commands Set List—MAC/Filter Table command set

MS10GT8GX2 Commands	Level	Description	Example
mac address-table static <v_mac_addr> vlan <v_vlan_id> interface <port_type>[<v_port_type _list>]	G	Configure MAC address table of interface (static)	(config)#mac-address-table static 11-22-33-44-55-66 valn 1 interface GigabitEthernet 1/2
show mac-address-table	P E	Show all MAC address table	#show mac-address-table Or another way in the following : #disable >show mac-address-table
show mac-address-table static	P	Show static MAC address table	#show mac-address-table static
no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface <port_type> [<v_port_type_list>]	G	Remove an entry of MAC address table of interface (static)	switch(config-if)# no mac-address-table static 11-22-33-44-55-66 vlan 1 interface GigabitEthernet 1/2
clear mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.10 Commands Set List—SNMP command set

MS10GT8GX2 Commands	Level	Description	Example
snmp server- vision {v1 v2c v3}	G	Select the server mode of SNMP	(config)#snmp server-version v1
snmp-server community v2c <comm>[ro rw] snmp-server community v3 <v3_comm> <v_ipv4_addr> <v_ipv4_netmask>	G	Configure SNMP server community information and community string	(config)#snmp-server community v2c public rw (config)#snmp-server community v3 public 192.168.0.5 255.255.255.0

show snmp	P	Show SNMP configuration	#show snmp
show snmp host	P	Show specified trap host information	#show snmp host
no snmp-server community { v2c v3 }	G	Remove the specified community.	(config)#no snmp community v2c
no snmp-server host [Host-name]	G	Remove the SNMP server host.	(config)#no snmp-server host [Host-name]

6.11 Commands Set List—Port Mirroring command set

MS10GT8GX2 Commands	Level	Description	Example
monitor session 1	G	Enable mirroring mode	(config)#monitor session 1
monitor session 1 destination interface <port_type> <di_list>	G	Set destination port of monitor function	(config)#monitor monitor session 1 destination interface GigabitEthernet 1/3
monitor session 1 source interface <port_type> <di_list> rx	G	Set TX source port of monitor function	(config)# monitor session 1 source interface GigabitEthernet 1/2 rx
show monitor session 1	P	Show port monitor information	#show monitor session 1
monitor session 1 source interface <port_type> <di_list>{rx\tx\both}	G	Configure source port of monitor function	(config)#monitor monitor session 1 source interface GigabitEthernet 1/2 both
no monitor session 1	G	Disable source port of monitor function	(config)#no monitor session 1

6.12 Commands Set List—TFTP command set

MS10GT8GX2 Commands	Level	Description	Defaults Example
copy running-config startup-config	P	Get configuration from running-config to startup-config and save.	# copy running-config startup-config
copy startup-config running-config	P	Get configuration from startup-config to running-config and save.	# copy startup-config running-config
copy <source_path> <destination_path>	P	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	

6.13 Commands Set List—LOG command set

MS10GT8GX2 Commands	Level	Description	Defaults Example
log level {error\ informational\ notice \warning}	G	Specified the log mode	(config)# log level error

show logging {error\ informational\ notice\ warning} d	P	Display system log.	#show logging error
log on	G	Enable log function	(config)#log on
no log on	G	Disable log function	(config)#log on
log host <ipv4_ucast>	G	Enable log function and set ip address to the log server	(config)#log host 192.168.0.6
show logging <Logging ID>	P	Use the show logging command with logging ID to display the detail logging message.	#show logging 1

6.14 Commands Set List—NTP command set

MS10GT8GX2-R Commands	Level	Description	Defaults Example
ntp	G	Enable NTP function	(config)#ntp
ntp server <1-5> ip-address < ip-address>	G	Enable NTP server And need to specify the IP of NTP server	(config)#ntp server 1 ip address 192.168.0.10
no ntp	G	Disable NTP function	(config)#no ntp
no ntp server	G	Disable NTP server function	(config)#no ntp server
show ntp server status	P	Display NTP server status	#show ntp server status
show ntp status	P	Display all NTP server status	#show ntp status
show ntp system status	P	Display NTP system status	#show ntp system status

6.15 Commands Set List—M-Ring command set

MS10GT8GX2 Commands	Level	Description	Example
ring version {v1 v2}	G	Enable Ring v1 v2	(config)# ring version v1
ring <1-32>	G	Configure specific ring	(config)# ring 1
ring <1-32> <ring-type>	G	Configure specific type which belongs to this ring	(config)# ring 1 dual-homing
ring <id> <ring type>[priority <priority>] east-port <port_type> <port0> west-port <port_type> <port1>	G	Configuring specific ring types and occupied ports, when there are several loops at the same time, the data transmission will be determined by priority	(config)# ring 1 dual-homing priority 128 east-port GigabitEthernet 1/2 west-port GigabitEthernet 1/3
show ring version	P	Display ring versions which are configured	# show ring version
Show ring <1-32>	P	Display specific ring number configuration information	#show ring 1

Notes:



Meridian Technologies, Inc.
700 Elmont Road, Elmont NY 11003, USA
Telephone: +1-516-285-1000 Fax: +1-516-285-6300
E-mail: support@meridian-tech.com
Web: www.meridian-tech.com